ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

Кваліфікаційна наукова
праця на правах рукопису

ІГНАТЕНКО СЕРГІЙ МИХАЙЛОВИЧ

УДК 003.26:004.056.55

ДИСЕРТАЦІЯ

МЕТОДИ РОЗВ'ЯЗАННЯ ЗАДАЧІ LPN НАД СКІНЧЕННИМИ КІЛЬЦЯМИ ДЛЯ ОЦІНЮВАННЯ СТІЙКОСТІ СИМЕТРИЧНИХ ПОСТКВАНТОВИХ ШИФРОСИТЕМ

05.13.21 – «Системи захисту інформації»

Подається на здобуття наукового ступеня
кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____

Науковий керівник:
КУЗНЕЦОВ Олександр Олександрович,
доктор технічних наук, професор

Харків – 2020

АНОТАЦІЯ

Ігнатенко С.М. Методи розв’язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Харківський національний університет імені В. Н. Каразіна, Харків, 2021.

Дисертаційна робота присвячена вирішенню актуальної наукової задачі розробки більш ефективних (в порівнянні з перебірним) методів розв’язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем.

На основі проведеного аналізу доступних наукових публікацій показано, що не дивлячись на помітний прогрес у розробці швидких (більш ефективних в порівнянні з перебірним) алгоритмів розв’язання задачі LPN над полем з двох елементів або деякими кільцями лишків, питання про існування таких алгоритмів для випадку довільного скінченного кільця R залишається відкритим. На сьогодні відсутні навіть неасимптотичні оцінки обсягу матеріалу, достатнього для надійного розв’язання задачі LPN над довільним скінченним кільцем. Залишається також не вирішеною задача про неасимптотичну часову складність узагальненого алгоритму BKW, який являє собою природне розширення на випадок довільного скінченного кільця одного з найкращих на сьогодні алгоритмів розв’язання задачі LPN над полем з двох елементів. Як наслідок, стійкість багатьох симетричних шифросистем, які будуються над скінченними кільцями (по аналогії з відомими шифросистемами, що базуються на складності розв’язання класичної задачі LPN над полем $\mathbf{GF}(2)$), залишається не визначеною, що стримує практичне застосування цих шифросистем у сучасних спеціальних інформаційно-телекомунікаційних системах.

У дисертаційній роботі вирішено важливу й актуальну наукову задачу розробки більш ефективних (в порівнянні з перебірним) методів розв’язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем.

Наведено класифікацію задач LPN в залежності від числа рівнянь та алгебраїчної структури кільця, над яким вона розглядається. Підкреслено роль симетричних шифросистем, що будуються на основі задачі LPN над скінченними кільцями, показано актуальність задачі оцінювання стійкості таких шифросистем. Сформульовано задачу отримання оцінок часової складності узагальненого алгоритму BKW розв’язання задачі LPN над скінченними кільцями.

Вперше отримано аналітичні оцінки обсягу матеріалу, достатнього для розв’язання із заданою достовірністю задачі LPN над довільним скінченним кільцем, які узагальнюють аналогічну оцінку, відому для випадку класичної задачі LPN та дозволяють визначити часову складність узагальненого алгоритму BKW, відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв’язання класичної задачі LPN.

Удосконалено метод максимуму правдоподібності розв’язання задачі LPN над скінченними фробеніусовими кільцями на основі використання швидкого перетворення Фур’є, що дозволяє помітно зменшити часову складність розв’язання задачі LPN над фробеніусовими кільцями як за допомогою самого ММП, так і інших алгоритмів, що використовують ММП як допоміжну процедуру.

Удосконалено метод максимуму правдоподібності розв’язання задачі LPN над кільцем лишків за модулем 2^N на основі використання числового перетворення Ферма, що надає можливість суттєво зменшити часову складність розв’язання задачі LPN за допомогою узагальненого алгоритму BKW.

Вперше розроблено послідовний метод побудови нових алгоритмів розв'язання задачі LPN над кільцем лишків за модулем 2^N за довільною скінченною сукупністю вхідних таких алгоритмів. Суттєву перевагу послідовного методу демонструють отримані оцінки стійкості шифросистем типу LPN-C над кільцем лишків за модулем 2^N відносно атак на основі підібраних відкритих повідомлень. Послідовний метод відновлення ключа шифросистеми є набагато більш ефективним (як за обчислювальною складністю, так і за обсягом матеріалу) в порівнянні з методом, що базується на застосуванні узагальненого алгоритму BKW. В цілому, шифросистема LPN-C над кільцем лишків за модулем 2^N забезпечує майже таку ж стійкість, що і N «паралельно працюючих» шифросистем LPN-C над полем $\mathbf{GF}(2)$. Це свідчить про недоцільність використання кілець лишків за модулем 2^N для побудови шифросистем зазначеного типу.

Доведено, що заміна в схемі генератора гами шифру SNOW 2.0 порозрядного булевого додавання арифметичним додаванням за модулем 2^{32} приводить до суттєвого підвищення стійкості шифру відносно кореляційних атак.

Показано, що можливість застосування узагальненого алгоритму BKW є суттєвим фактором для визначення стійкості постквантових шифросистем типу Ring-LWE відносно атак на основі підібраних відкритих повідомлень. Це надає можливість цілеспрямовано вибирати значення параметрів шифросистем типу Ring-LWE, виходячи з вимог до їх стійкості відносно відомих атак.

У першому розділі показано, що задача LPN є перспективним кандидатом на роль універсальної основи для побудови постквантових криптосистем і протоколів. Проаналізовано сучасний стан та перспективи розвитку шифросистем, стійкість яких базується на складності розв'язання задачі LPN, при різних припущеннях щодо структури кільця, кількості

рівнянь у системі або закону розподілу ймовірностей у правих частинах її рівнянь.

Серед усіх криптосистем, стійкість яких базується на складності розв'язання задачі LPN, перспективний клас утворюють симетричні шифросистеми, створення яких обумовлено, перш за все, потребою у практичних системах шифрування із секретним ключем, стійкість яких базується на складності розв'язання лише однієї обчислювально складної задачі. Відомі конструкції таких шифросистем будуються, головним чином, над полем з двох елементів. Проте, як правило, вони допускають природні узагальнення на випадок довільного скінченного кільця. При цьому вирішення задач оцінювання стійкості цих шифросистем потребує додаткових досліджень.

У другому розділі вперше отримано аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем. Перша з них встановлює явну залежність потрібного обсягу матеріалу від основних параметрів системи (порядку кільця, числа невідомих та розподілу спотворень у правих частинах рівнянь у системі). Друга оцінка базується на застосуванні центральної граничної теореми і встановлює наближений вираз обсягу матеріалу в термінах квантилів нормального розподілу ймовірностей.

Як відомо, ММП характеризується найбільшою достовірністю (найменшою середньою ймовірністю помилки) серед усіх методів розв'язання задачі LPN над довільним скінченним кільцем R. Проте зазначений метод є найбільш трудомістким, оскільки потребує перебору всіх можливих розв'язків. Відомо, що у випадку, коли R є полем порядку 2^N, трудомісткість ММП можна зменшити, використовуючи алгоритми швидкого перетворення Фур'є. Поряд з тим, питання про те, наскільки широким є клас скінченних кілець із зазначеною властивістю є на сьогодні відкритим.

У третьому розділі показано, що таким є клас скінченних фробеніусових кілець. Цей клас є дуже потужним і включає в себе, зокрема, будь-які кільця головних (лівих чи правих) ідеалів. Розроблено два методи підвищення ефективності розв'язання задачі LPN за допомогою ММП. Перший з них є застосовним для довільного скінченного фробеніусова кільця R та базується на використанні швидкого перетворення Фур'є допоміжних функцій, що визначаються на цьому кільці. Другий метод є застосовним до задачі LPN над кільцем лишків за модулем 2^N і базується на використанні числового перетворення Ферма. Розроблені методи узагальнюють відомий спосіб застосування швидкого перетворення Фур'є для розв'язання задачі LPN над скінченним полем порядку 2^N.

У четвертому розділі викладено метод побудови нових алгоритмів розв'язання системи рівнянь зі спостереженими правими частинами над кільцем $R_N = \mathbf{Z}/(2^N)$ за довільною скінченною сукупністю вхідних таких алгоритмів. Зазначений (послідовний) метод запропоновано вперше. Отримано аналітичні вирази оцінок достовірності та часової складності алгоритмів розв'язання систем рівнянь, які будуються за допомогою розробленого методу, через відповідні характеристики вхідних алгоритмів. Запропоновано також процедуру побудови оптимальних (у певному класі) алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_N.

Зауважимо, що ідея послідовного методу є достатньо природною і може бути використана для розв'язання систем лінійних рівнянь зі спотвореними правими частинами над більш широкими класами скінченних кілець, зокрема, кільцями Галуа (відмінними від скінченних полів). В цілому, запропонований метод дозволяє забезпечити гарний «баланс» між основними показниками ефективності (достовірністю і трудомісткістю) алгоритмів шляхом належного вибору композиції (тобто впорядкованого розбиття на доданки) числа *N*.

Практичне значення результатів дисертаційної роботи полягає у появі можливості отримувати науково обгрунтовані оцінки стійкості симетричних постквантових шифросистем шляхом більш ефективного розв'язання задачі LPN над скінченними кільцями та, як наслідок, суттєвому підвищенні криптографічної стійкості симетричних постквантових шифросистем.

Представлені в дисертаційній роботі нові наукові та практичні результати дозволяють:

– цілеспрямовано вибирати значення параметрів симетричних постквантових шифросистем над скінченними кільцями, що гарантують їх стійкість відносно відомих атак;

– зменшити (від декількох разів до декількох десятків порядків) часову складність розв'язання задачі LPN над скінченними кільцями за допомогою методу максимуму правдоподібності, а також узагальненого алгоритму BKW;

– встановити та обґрунтувати недоцільність (з погляду криптографічної стійкості) практичного застосування шифросистем типу LPN-C над кільцем лишків за модулем 2^N при $N > 1$;

– підвищити ефективність відомих атак на шифросистеми типу Ring-LWE від $2^{55,71}$ до $2^{1408,73}$ разів (в залежності від параметрів шифросистем).

– підвищити ефективність кореляційних атак на SNOW 2.0-подібні потокові шифри над кільцями лишків за модулем 2^N від $2^{8,24}$ до $2^{28,54}$ разів (в залежності від значення N та довжини накопичувача генератора гами);

– будувати SNOW 2.0-подібні потокові шифри над кільцями лишків за модулем 2^N, що є обґрунтовано стійкими відносно відомих кореляційних атак, зокрема, підвищити стійкість шифру SNOW 2.0 з $2^{164,15}$ до $2^{302,31}$ операцій (при збільшенні обсягу потрібного матеріалу з $2^{163,59}$ до $2^{301,31}$) шляхом повної заміни порозрядного булевого додавання у схемі генератора гами додаванням за модулем 2^{32}.

Наукові та практичні результати дисертаційної роботи реалізовані в Службі зовнішньої розвідки України – в результаті виконання НДР “Баракуда”, в Службі безпеки України в результаті виконання НДР “Самсон” та в навчальному процесі Харківського національного університету імені В. Н. Каразіна.

Ключові слова: симетричні постквантові шифросистеми, задача LPN, часова складність алгоритму, метод максимуму правдоподібності, оцінки обсягу матеріалу, узагальнений алгоритм BKW, скінченні кільця, обґрунтування стійкості, системи лінійних рівнянь зі спотвореними правими частинами.

ABSTRACT

Ihnatenko S. Methods for solving the LPN problem over finite rings to evaluate the security of symmetric post-quantum cryptosystems. – Qualifying scientific research as a manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 «Information protection systems». – V.N. Karazin Kharkiv National university, Kharkiv, 2020.

This thesis is devoted to solving the actual scientific problem of development more effective methods (in comparison with brute force method) of solving the LPN problem over finite rings for evaluation of the security of post-quantum symmetric cryptosystems.

Analysis of available scientific publications was carried out. It showed that in spite of the considerable progress in the development of fast methods (more effective in comparison with brute force method) for solving the LPN problem over a field of two elements or some residue rings, the question of the existence of such methods in case of arbitrary finite ring remains open. To date, there are not

even noasymptotic estimates of the amount of material sufficient to solve the LPN problem over an arbitrary finite ring properly. The problem of the noasymptotic time complexity of the generalized BKW algorithm, which is a natural extension of one of the best methods for solving the LPN problem over a two-element field in case of arbitrary finite ring, remains unresolved. As a result, the security of many symmetric cryptosystems over finite rings (by analogy with known cryptosystems based on the complexity of the classical LPN problem solving over the $\mathbf{GF}(2)$ field) remains undefined, which holds back the practical application of these cryptosystems in modern special information and telecommunication systems.

In the thesis the important and actual scientific problem of development more effective (in comparison with bruteforce) methods of the solving of LPN problem over finite rings for an evaluation the security of symmetric post-quantum cipher systems is solved.

The classification of LPN problems depending on the number of equations and the algebraic structure of the ring over which it is considered is given. The role of symmetric cipher systems built on the basis of the LPN problem over finite rings is emphasized, the topicality of the problem of evaluation the security of such cipher systems is shown. The problem of obtaining estimates of the time complexity of the generalized BKW algorithm for solving the LPN problem over finite rings is formulated.

Analytical estimates of the amount of material sufficient to solve the LPN problem over an arbitrary finite ring properly, that generalize a similar estimate known for the classical LPN problem and allow to determine the time complexity of the generalized BKW algorithm, a known prototype of which is currently one of the most effective algorithms for solving the classical LPN problem are obtained for the first time.

The maximum likelihood method (MLM) for solving the LPN problem over finite Frobenius rings has been improved based on the fast Fourier transform using, which allows to significantly reduce the time complexity of the LPN problem

solving over Frobenius rings, using both the MLM itself and other algorithms that use MLM as an auxiliary procedure.

The maximum likelihood method for solving the LPN problem over residue rings modulo 2^N has been improved based on the Fermat number transforms, which enables to significantly reduce the time complexity of the LPN solving using a generalized BKW algorithm.

For the first time, a sequential method of constructing new algorithms for solving the LPN problem over residue rings modulo 2^N by an arbitrary finite set of incoming such algorithms has been developed. A significant advantage of the sequential method is demonstrated by the obtained estimates of the security of LPN-C type cipher systems over residue rings modulo 2^N against chosen plaintext attacks. The sequential method of recovering the key of the cipher system is much more efficient (both in terms of computational complexity and the amount of material) in comparison with the method based on the use of the generalized BKW algorithm. In general, the LPN-C cipher system over residue rings modulo 2^N provides almost the same security as the "parallel" LPN-C cipher systems over the field $\mathbf{GF}(2)$. This indicates the inexpediency of using residue rings modulo 2^N to build cipher systems of this type.

It is proved that the replacement of the SNOW 2.0 cipher gamma generator bitwise Boolean addition by arithmetic modular 2^{32} addition leads to a significant increasing the security of the cipher against correlation attacks.

It is shown that the possibility of using the generalized BKW algorithm is an essential factor for determining the security of post-quantum cipher systems like as Ring-LWE against chosen plaintext attacks. This makes it possible to purposefully select the values of the parameters of cryptosystems like Ring-LWE, based on the requirements for their security against known attacks.

The first section shows that the LPN problem is a promising candidate for the role of a universal basis for building post-quantum cryptosystems and protocols. The current state and prospects of development of cipher systems, the security of

which is based on the complexity of solving the LPN problem, with different assumptions about the structure of the ring, the number of equations in the system or the law of probability distribution in the right parts of its equations.

Among all cryptosystems, the security of which is based on the complexity of solving the LPN problem, a promising class is formed by symmetric cipher systems, the creation of which is due primarily to the need for practical encryption systems with secret keys, the security of which is based on the complexity of solving only one computationally complex task. Known designs of such cipher systems are built mainly over a field of two elements. However, as a rule, they allow natural generalizations on the case of an arbitrary finite ring. At the same time, solving the problems of evaluation the security of these cipher systems requires additional research.

In the second section, for the first time, analytical estimates of the amount of material sufficient to solve a given LPN problem over an arbitrary finite ring are obtained. The first of them establishes a clear dependence of the required amount of material on the basic parameters of the system (the order of the ring, the number of unknowns and the distribution of errors in the right parts of the equations in the system). The second estimate is based on the application of the central limit theorem and establishes an approximate expression of the amount of material in terms of quantiles of the normal probability distribution.

As you know, the maximum likelihood method is characterized by the highest reliability (lowest average probability of error) among all methods of solving the LPN problem over an arbitrary finite ring R. However, this method is the most time consuming, as it requires a search of all possible solutions. It is known that in the case when R is an order 2^N field, the complexity of the MLM can be reduced using fast Fourier transform algorithms. At the same time, the question of how wide is the class of finite rings with this property is currently open.

The third section shows that this is a class of finite frobenius rings. This class is very powerful and includes, in particular, any rings of main (left or right) ideals.

Two methods have been developed to increase the efficiency of solving the LPN problem using MLM. The first is applicable to an arbitrary finite Frobenius ring R and is based on the use of the fast Fourier transform of auxiliary functions defined on this ring. The second method is applicable to the LPN problem over the modulus 2^N ring and is based on the use of the Fermat numerical transformation. The developed methods generalize the known method of applying the fast Fourier transform to solve the LPN problem over a finite 2^N order field.

The fourth section describes the method of constructing new algorithms for solving a corrupted system of equations over ring $R_N = \mathbf{Z}/(2^N)$ with an arbitrary finite set of input such algorithms. This (sequential) method was proposed for the first time. Analytical expressions for estimating the reliability and time complexity of algorithms for solving systems of equations are obtained. These systems of equations are constructed using the developed method, through the corresponding characteristics of the input algorithms. A procedure for constructing optimal (in a certain class) algorithms for solving corrupted systems of linear equations over a R_N ring is also proposed.

Note that the idea of a sequential method is qui te natural and can be used to solve corrupted systems of linear equations over wider classes of finite rings, in particular, Galois rings (other than finite fields). In general, the proposed method allows to ensure a good «balance» between the main indicators of efficiency (reliability and complexity) of algorithms by proper selection of the composition (ie orderly division into terms) of the number *N*.

The practical significance of the results of the thesis is the possibility of obtaining scientifically sound estimates of the security of symmetric post-quantum cipher systems by more efficient solution of the LPN problem over finite rings and, as a consequence, a significant increase in cryptographic security of symmetric post-quantum cipher systems.

New scientific and practical results presented in this thesis allow:

– to purposefully choose the values of the parameters of post-quantum

symmetric cryptosystems over finite rings, which guarantee their security against known attacks;

– to reduce (from several times to several dozen orders) the time complexity of solving the LPN problem over finite rings using the maximum likelihood method, as well as the generalized BKW algorithm;

– to establish and prove the inexpediency (from the cryptographic security point of view) of the practical application of LPN-C type encryption systems over the residue ring modulo 2^N where $N > 1$;

– to increase the effectiveness of known attacks on the Ring-LWE encryption system from $2^{55,71}$ to $2^{1408,73}$ times (depending on the encryption system parameters);

– to increase the effectiveness of correlation attacks on SNOW 2.0-like stream ciphers over residue rings modulo 2^N from $2^{8,24}$ to $2^{28,54}$ times (depending on the N value and gamma generator length);

– to build SNOW 2.0-like stream ciphers over residue rings modulo 2^N, which are reasonably secure against known correlation attacks, in particular, to increase the resistance of SNOW 2.0 cipher from $2^{164,15}$ to $2^{302,31}$ operations (with increasing of the amount of required material from $2^{163,59}$ to $2^{301,31}$) by completely replacement from boolean bitwise addition in the gamma generator scheme to addition modulo 2^{32}.

The scientific and practical results of the thesis were implemented at the Foreign Intelligence Service of Ukraine (in the research scientific work «Baracuda») and at the Security Service of Ukraine (in the research scientific work «Samson») and in the educational process of V.N. Karazin Kharkiv National University.

Keywords: post-quantum symmetric cryptosystems, LPN problem, time complexity of the algorithm, maximum likelihood method, material amount estimations, generalized BKW algorithm, finite rings, security proving, systems of linear equations corrupted by noise.

Список основних публікацій здобувача:

1. Алексейчук А. Н., Игнатенко С. М. Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N. *Збірник наукових праць ІПМЕ НАН України*. 2003. Вип. 20, С. 40-48.

2. Алексейчук А. Н., Игнатенко С. М. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Реєстрація, зберігання і обробка даних*. 2005. № 1, т. 7. С. 11-23.

3. Алексейчук А. Н., Игнатенко С. М. Нижняя граница вероятности восстановления истинного решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2006. № 4, т. 8. С. 5-12.

4. Игнатенко С. М. Модификация метода максимума правдоподобия решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2007. № 1, т. 9. С. 63-72.

5. Ігнатенко С. М. Аналіз кореляційних атак на потокові шифри. *Спеціальні телекомунікаційні системи та захист інформації*. 2008. Вип. 1. С. 55-65.

6. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2017. Вип. 15. С. 150-155.

7. Олексійчук А. М., Ігнатенко С. М. Застосування швидкого перетворення Фур'є для розв'язання задачі LPN над скінченними фробеніусовими кільцями. *Захист інформації*. 2017. № 4, т. 19. С. 271-277.

8. Олексійчук А. М., Ігнатенко С. М. Алгоритми оцінювання стійкості SNOW 2.0-подібних потокових шифрів над кільцями лишків відносно кореляційних атак. *Радіотехніка*. 2018. Вип. 193, С. 28 – 34.

9. Ігнатенко С. М. Застосування послідовного методу для побудови статистичної атаки на шифросистему LPN-C над кільцем лишків за модулем 2^N. *Захист інформації*. 2018. № 3, т. 20. С. 149-154.

10. Kuznetsov A., Potii O., Poluyanenko N., Ihnatenko S., Stelnyk I., Mialkovsky D. Opportunites to minimize hardware and software costs for implementing Boolean functions in stream ciphers. *International Journal of Computing*. 2019. Vol. 18, Issue 4. P. 443-452.

11. Игнатенко С. М., Алексейчук А. Н. Алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю 2^N с использованием быстрого преобразования Ферма. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. VI міжнар. наук.-практ. конф. Київ, 2003. С. 42-43.

12. Игнатенко С. М., Алексейчук А. Н. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. VII міжнар. наук.-практ. конф. Київ, 2004. С. 58-59.

13. Игнатенко С. М., Алексейчук А. Н. Итеративный алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю модулю 2^N. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. VIII міжнар. наук.-практ. конф. Київ, 2005. С. 46-47.

14. Игнатенко С. М., Алексейчук А. Н. Оценка надежности метода максимума правдоподобия решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. IX міжнар. наук.-практ. конф. Київ, 2006. С. 29-30.

15. Игнатенко С. М., Алексейчук А. Н. Быстрый алгоритм восстановления искаженных линейных рекуррентных последовательностей над кольцом вычетов по модулю 2^N. *Безпека інформації в інформаційно-*

телекомунікаційних системах: тези доп. X міжнар. наук.-практ. конф. Київ, 2007. С. 36-37.

16. Алексейчук А. Н., Игнатенко С. М., Конюшок С. Н. Быстрая корреляционная атака на генераторы гаммы над кольцом вычетов по модулю 2^N. *Питання оптимізації обчислень* (ПОО-XXXV): праці міжнар. симп. Україна, Крим, Велика Ялта, смт. Кацивелі, 2009. С. 14-18.

17. Ігнатенко С. М., Олексійчук А. М. Послідовна статистична атака на шифросистему LPN-C над кільцем лишків за модулем 2^N. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. XX міжнар. наук.-практ. конф. м. Буча Київської обл, 2018. С. 35-36.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕОМ – електронно-обчислювальна машина;

ЛРЗ – лінійний регістр зсуву;

ММП – метод максимуму правдоподібності;

НДР – науково-дослідна робота;

ОС – операційна система;

ПК – персональний комп’ютер;

СР – система рівнянь;

ETSI – Європейський Інститут Телекомунікаційних Стандартів;

MLM – maximum likelihood method.

ВСТУП

Актуальність теми. Протягом останнього часу спостерігається помітне зростання вимог до стійкості криптографічних систем і протоколів. Зокрема, у зв'язку з можливою появою квантових комп'ютерів криптографія переживає етап створення шифросистем, стійких до квантових атак. У 2016 році США та ЄС розпочали активні роботи з організації конкурсів на нові стандарти квантово-захищених криптографічних алгоритмів. Крім того, Національний інститут стандартів і технологій США оголосив, що державні установи повинні бути готові до впровадження до 2025 р. постквантових алгоритмів шифрування. Таким чином, виникає потреба у шифросистемах, стійкість яких базується на задачах, що є обчислювально складними навіть у моделі квантових обчислень.

Однією з таких задач є задача LPN (learning parity with noise), яка у найбільш загальному випадку полягає в розв'язанні системи лінійних рівнянь зі спотвореними правими частинами та випадковою рівноймовірною матрицею коефіцієнтів над довільним скінченним кільцем R. Зазначена задача рівносильна задачі декодування випадкового лінійного коду над кільцем R та має важливе значення для криптографії в цілому. Зокрема, відомо чимало конструкцій генераторів псевдовипадкових послідовностей, алгоритмів шифрування, протоколів автентифікації та протоколів узгодження ключів, стійкість яких базується на складності розв'язання задачі LPN над полем з двох елементів або над скінченним полем великого простого порядку. Крім того, до розв'язання цієї задачі зводиться побудова кореляційних атак на деякі потокові шифри. У всіх зазначених випадках практична стійкість відповідних криптосистем і протоколів залежить безпосередньо від часової складності найкращих з відомих алгоритмів розв'язання задачі LPN, причому для випадку симетричних шифросистем допускаються алгоритми розв'язання цієї задачі за умови необмеженої кількості даних (рівнянь у системі).

Не дивлячись на помітний прогрес у розробці швидких (більш ефективних в порівнянні з перебірним) алгоритмів розв'язання задачі LPN над полем з двох елементів або деякими кільцями лишків, питання про існування таких алгоритмів для випадку довільного скінченного кільця R залишається відкритим. На сьогодні відсутні навіть неасимптотичні оцінки обсягу матеріалу, достатнього для надійного розв'язання задачі LPN над довільним скінченним кільцем. Залишається також не вирішеною задача про неасимптотичну часову складність узагальненого алгоритму BKW, який являє собою природне розширення на випадок довільного скінченного кільця одного з найкращих на сьогодні алгоритмів розв'язання задачі LPN над полем з двох елементів. Як наслідок, стійкість багатьох симетричних шифросистем, які будуються над скінченними кільцями (по аналогії з відомими шифросистемами, що базуються на складності розв'язання класичної задачі LPN над полем $\mathbf{GF}(2)$), залишається не визначеною, що стримує практичне застосування цих шифросистем у сучасних спеціальних інформаційно-телекомунікаційних системах.

Таким чином, є актуальною *наукова задача розробки більш ефективних (в порівнянні з перебірним) методів розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем*. Вирішенню цієї задачі присвячено дану дисертаційну роботу.

Зв'язок роботи з науковими програмами, планами, темами. Робота над дисертацією проводилася в рамках науково-дослідних робіт (НДР) "Баракуда" (№ держреєстрації 0108U000007д) на замовлення Служби зовнішньої розвідки України та НДР "Самсон" на замовлення Служби безпеки України.

Мета та задачі досліджень. *Метою дисертаційної роботи є отримання науково обґрунтованих оцінок стійкості симетричних шифросистем, які базуються на складності розв'язання задачі LPN над скінченними кільцями, на основі застосування більш ефективних методів розв'язання зазначеної задачі.*

Для досягнення поставленої мети в дисертаційній роботі сформульовано та вирішено наступні взаємозв'язані *окремі задачі досліджень*.

1. Провести аналіз відомих методів розв'язання задачі LPN та методів побудови шифросистем, стійкість яких базується на складності розв'язання цієї задачі.

2. Отримати аналітичні оцінки обсягу матеріалу, достатнього для розв'язання задачі LPN над довільним скінченним кільцем за допомогою методу максимуму правдоподібності.

3. Отримати аналітичну оцінку та розробити алгоритм обчислення часової складності узагальненого алгоритму BKW для розв'язання задачі LPN над довільним скінченним кільцем.

4. Розробити методи підвищення ефективності розв'язання задачі LPN за допомогою швидкого перетворення Фур'є та числового перетворення Ферма над скінченними фробеніусовими кільцями та над кільцями лишків за модулем 2^N відповідно. Провести порівняння часової складності узагальненого алгоритму BKW та його модифікацій із застосуванням запропонованих методів.

5. Розробити послідовний метод розв'язання задачі LPN над кільцем лишків за модулем 2^N.

6. Застосувати розроблені методи розв'язання задачі LPN до оцінювання стійкості симетричних постквантових шифросистем Ring-LWE та LPN-C над кільцем лишків за модулем 2^N відносно атак на основі підібраних відкритих повідомлень, а також SNOW 2.0-подібних потокових шифрів над кільцями лишків за модулем 2^N відносно кореляційних атак.

Об'єктом дослідження в дисертаційній роботі є процес перетворення інформації за допомогою симетричних шифросистем, стійкість яких базується на складності розв'язання задачі LPN над скінченними кільцями, а *предметом дослідження* – методи розв'язання зазначеної задачі LPN над скінченними кільцями.

Методи дослідження. Основу дисертаційних досліджень складають теоретичні дослідження. При розв'язанні окремих задач 2, 3, 6 використано методи лінійної алгебри, теорії кодування, теорії ймовірностей та математичної статистики, а при розв'язанні окремих задач 4, 5 – методи лінійної алгебри, теорії скінченних кілець і теорії обчислювальних алгоритмів. Чисельні розрахунки на ЕОМ виконувалися з використанням середовища розробки Microsoft Visual Studio 2013 (компонент Visual C++).

Наукова новизна отриманих результатів. Підсумком вирішення перелічених вище окремих задач є такі нові наукові результати, що висуваються на захист.

1. Вперше отримано аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем, які узагальнюють аналогічну оцінку, відому для випадку класичної задачі LPN та дозволяють визначити часову складність узагальненого алгоритму BKW, відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN.

2. Удосконалено метод максимуму правдоподібності розв'язання задачі LPN над скінченними фробеніусовими кільцями на основі використання швидкого перетворення Фур'є, що дозволяє помітно зменшити часову складність розв'язання задачі LPN над фробеніусовими кільцями як за допомогою самого ММП, так і інших алгоритмів, що використовують ММП як допоміжну процедуру.

3. Удосконалено метод максимуму правдоподібності розв'язання задачі LPN над кільцем лишків за модулем 2^N на основі використання числового перетворення Ферма, що надає можливість суттєво зменшити часову складність розв'язання задачі LPN за допомогою узагальненого алгоритму BKW.

4. Вперше розроблено метод побудови нових алгоритмів розв'язання задачі LPN над кільцем лишків за модулем 2^N за довільною скінченною

сукупністю вхідних таких алгоритмів, що надає можливість підвищити ефективність розв'язання цієї задачі шляхом належного вибору композиції числа N.

Практичне значення отриманих результатів. Представлені в дисертаційній роботі нові наукові та практичні результати дозволяють:

– цілеспрямовано вибирати значення параметрів симетричних постквантових шифросистем над скінченними кільцями, що гарантують їх стійкість відносно відомих атак;

– зменшити (від декількох разів до декількох десятків порядків) часову складність розв'язання задачі LPN над скінченними кільцями за допомогою методу максимуму правдоподібності, а також узагальненого алгоритму BKW;

– встановити та обґрунтувати недоцільність (з погляду криптографічної стійкості) практичного застосування шифросистем типу LPN-C над кільцем лишків за модулем 2^N при $N > 1$;

– підвищити ефективність відомих атак на шифросистеми типу Ring-LWE від $2^{55,71}$ до $2^{1408,73}$ разів (в залежності від параметрів шифросистем);

– підвищити ефективність кореляційних атак на SNOW 2.0-подібні потокові шифри над кільцями лишків за модулем 2^N від $2^{8,24}$ до $2^{28,54}$ разів (в залежності від значення N та довжини накопичувача генератора гами);

– будувати SNOW 2.0-подібні потокові шифри над кільцями лишків за модулем 2^N, що є обґрунтовано стійкими відносно відомих кореляційних атак, зокрема, підвищити стійкість шифру SNOW 2.0 з $2^{164,15}$ до $2^{302,31}$ операцій (при збільшенні обсягу потрібного матеріалу з $2^{163,59}$ до $2^{301,31}$) шляхом повної заміни порозрядного булевого додавання у схемі генератора гами додаванням за модулем 2^{32}.

Наукові та практичні *результати дисертаційної роботи реалізовані* в Службі зовнішньої розвідки України – в результаті виконання НДР

“Баракуда” (акт від 06.11.2008) та в Службі безпеки України в результаті виконання НДР “Самсон” (акт від 19.12.2017).

Особистий внесок здобувача. В статті [1] автором отримано оцінку ймовірності правильного відновлення справжнього розв’язку системи лінійних рівнянь зі спотвореними правими частинами над кільцем лишків по модулю 2^N з фіксованою матрицею коефіцієнтів методом максимальної правдоподібності; в статті [2] та тезах доповідей [12] автору належить метод побудови нових алгоритмів розв’язування системи лінійних рівнянь зі спотвореними правими частинами над кільцем лишків по модулю 2^N; в статті [3] та тезах доповідей [14] автором отримано аналітичні оцінки числа рівнянь, необхідних для розв’язання зазначених систем із заданою ймовірністю; в статті [6] автором отримано оцінку ймовірності відновлення істинного розв’язку системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями з випадковою рівноймовірною матрицею коефіцієнтів; в статті [7] автором запропоновано модифікацію методу максимуму правдоподібності із застосуванням швидкого перетворення Фур’є для розв’язування задачі LPN над довільним скінченним фробеніусовим кільцем; в статті [8] автором проведені розрахунки часової складності узагальненого алгоритму BKW та його модифікацій; в статті [10] автором обґрунтовано критерії та показники ефективності окремих шифросистем; в тезах доповідей [11] автором запропоновано модифікацію методу максимуму правдоподібності розв’язування систем лінійних рівнянь зі спотвореними правими частинами над кільцем лишків по модулю 2^N із застосуванням числового перетворення Ферма допоміжних функцій; в тезах доповідей [13] автору належить алгоритм побудови перевірочних співвідношень малої ваги для знаків лінійної рекурентної послідовності над кільцем лишків по модулю 2^N; в тезах доповідей [15] автором запропоновано процедуру “підйому” поліномів заданої ваги над полем $\mathbf{GF}(2)$ до поліномів над кільцем $\mathbf{Z}/2^N$; в тезах доповідей [16] автору належить ідея застосування

алгоритмів швидкого перетворення Фур'є для зменшення трудомісткості обчислення значень апостеріорної ймовірності на другому етапі "векторної" кореляційної атаки; в тезах доповідей [17] автором проведені розрахунки часової складності узагальненого алгоритму BKW та послідовного методу розв'язання системи рівнянь зі спотвореними правими частинами над кільцем лишків за модулем 2^N при застосуванні статистичної атаки на шифросистему LPN-C.

Апробація результатів дисертації. Результати дисертаційних досліджень доповідалися та обговорювалися *на* 8 *міжнародних наукових та науково-практичних конференціях*: VI – X, XX Міжнародних науково-практичних конференціях "Безпека інформації в інформаційно-телекомунікаційних системах" (м. Київ, 2003 – 2007 рр.; м. Буча Київської обл., 2018 р.), міжнародному симпозіумі "Питання оптимізації обчислень (ПОО-XXXV)" (Крим, Велика Ялта, смт. Кацивелі, 2009 рік) та міжнародній науковій конференції "Питання оптимізації обчислень (ПОО-XLIV)" (м. Кам'янець-Подільський Хмельницької обл., 2017 р.).

Публікації. Основні наукові результати дисертаційної роботи опубліковано в 17 наукових працях: з них 10 наукових статей [1 – 10] в наукових спеціалізованих виданнях України та інших країн (3 видання індексуються міжнародними наукометричними базами), 7 тез доповідей на наукових та науково-практичних конференціях [11 – 17].

Структура роботи та її обсяг. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел (в кінці кожного розділу основної частини дисертації) і має 130 сторінок основного тексту, 15 рисунків, 12 таблиць, 28 сторінок додатків. Список використаних джерел містить 159 найменування і займає 16 сторінок. Загальний обсяг дисертаційної роботи – 187 сторінок.

РОЗДІЛ 1

АНАЛІЗ ВІДОМИХ МЕТОДІВ РОЗВ'ЯЗАННЯ ЗАДАЧІ LPN ДЛЯ ПОБУДОВИ ТА ОЦІНЮВАННЯ СТІЙКОСТІ ПОСТКВАНТОВИХ СИМЕТРИЧНИХ ШИФРОСИСТЕМ

1.1. Аналіз ролі постквантових криптосистем і протоколів в сучасних системах захисту інформації

Останнім часом у зв'язку з можливістю створення квантових комп'ютерів надзвичайно актуальною стає проблема значного зниження стійкості окремих сучасних криптосистем у квантовій моделі обчислень.

У 1985 році Д. Дойч запропонував використовувати закони квантової фізики для побудови комп'ютерних систем нового типу – квантових комп'ютерів [1]. Робота квантового комп'ютера ґрунтується на принципі суперпозиції. Роль бітів у традиційному комп'ютері відіграють квантові біти (quantum bits – кубіти). Так само як і біти, вони мають два стани – нуль та одиницю, але завдяки суперпозиції кубіт може приймати значення, отримані шляхом комбінування цих станів та знаходитися в них одночасно. Саме за рахунок цієї властивості кубітів досягається "паралельність" квантових обчислень, що приводить до відсутності необхідності перебору всіх можливих значень в окремих алгоритмах [2]. Як наслідок, продуктивність квантових комп'ютерів при розв'язанні перебірних задач (комівояжера, динамічного програмування тощо) значно перевищує продуктивність традиційних комп'ютерів.

Найважливішою характеристикою квантового комп'ютера з точки зору продуктивності обчислень є кількість кубітів. Створенню квантових комп'ютерів з великою кількістю кубітів перешкоджають помилки, які виникають зі збільшенням їх числа внаслідок електричних, магнітних, теплових завад та інших зовнішніх факторів. Іншими словами, час розпаду

суперпозиції системи швидко зменшується зі збільшенням її складових частин [3].

На сьогодні над створенням квантових комп'ютерів працюють провідні світові компанії, такі як IBM [4, 5], D-Wave Systems [6], Google [7], Intel [8] тощо. Компанія Microsoft інвестує не тільки в розробку квантових комп'ютерів. Нещодавно її співробітники створили мову програмування квантових обчислень Q# [9].

Актуальний список квантових процесорів можна побачити за посиланням [10]. Разом з тим, оскільки на сьогодні не існує єдиного стандарту квантового процесору, порівняння існуючих квантових комп'ютерів лише за кількістю кубітів є умовним. За оцінками експертів, кількість кубітів квантових комп'ютерів буде подвоюватися кожні 10 місяців [11].

Зрозуміло, що для ефективного розв'язання зазначених обчислювальних задач окрім самих квантових комп'ютерів необхідні відповідні алгоритми. Виявляється, що для задач криптоаналізу окремих криптосистем такі алгоритми вже існують. Так, алгоритм Шора [12] дозволяє за поліноміальний час розв'язувати задачі розкладання чисел на множники та дискретного логарифмування. Зокрема, алгоритм факторизації чисел Шора [13] виконує лише $O((\log n)^2 \log\log n \log\log\log n)$ кроків на квантовому комп'ютері. При цьому найкращі з відомих на сьогодні алгоритмів факторизації цілих чисел мають субекспоненційну складність. Таким чином, можливість застосування алгоритму Шора з появою повноцінного квантового комп'ютера несе загрозу класичним асиметричним криптографічним алгоритмам, таким як RSA, DSA, ECDSA, ECRSA тощо.

Квантовий алгоритм Гровера [14], у свою чергу, дозволяє розв'язувати задачі перебору ключів значно швидше, ніж звичайні алгоритми. Алгоритм Гровера дозволяє для заданої функції від n змінних розв'язувати задачу обчислення її аргументів за $(\pi\sqrt{2^n})/4$ кроків у порівнянні з 2^{n-1} кроками в

середньому при застосуванні класичних методів перебору. На відміну від алгоритма Шора, зазначений алгоритм дає лише квадратичний виграш у порівнянні з класичними перебірними методами. Але при великих значеннях n такий виграш змушує розробників криптосистем вже сьогодні замислитися над збільшенням довжини ключів шифрування. Зауважимо, шо часова складність задачі перебору ключів є еквівалентною за складністю задачі пошуку елементу в невідсортованій базі даних, та, як показано в [15], становить $\Theta(\sqrt{2^n})$.

Наведені факти свідчать про актуальність задачі створення нових *постквантових* (тобто стійких до атак з використанням квантових комп'ютерів та алгоритмів) криптосистем [16]. У зв'язку з цим Агентством національної безпеки США ще в 2015 році анонсовано план переходу до таких криптосистем [17]. Крім того, Національний Інститут Стандартів та Технологій (NIST) США рекомендував урядовим установам бути готовими до впровадження алгоритмів постквантового шифрування до 2025 року та оголосив відкритий конкурс з метою прийняття протягом найближчих п'яти-семи років нових постквантових криптостандартів [16, 18]. В свою чергу, Європейський Інститут Телекомунікаційних Стандартів (ETSI) в 2016 році також розпочав роботу над стандартизацією алгоритмів постквантової криптографії [19].

Таким чином, актуальною є задача розробки шифросистем, стійкість яких базується на задачах, що є обчислювально складними навіть у моделі квантових обчислень.

В залежності від математичної задачі, яка складно розв'язується як на класичному, так і на квантовому комп'ютері, розрізняють п'ять основних видів постквантових криптосистем (рис. 1.1) [20]:

– на завадостійких кодах;

– на ґеш-функціях;

– на решітках;

– на системах квадратичних булевих рівнянь;

– на основі ізогеній суперсингулярних еліптичних кривих.

Зауважимо також, що до постквантових відносять також сучасні потокові та блокові шифри (за умови збільшення довжини ключів) [21].

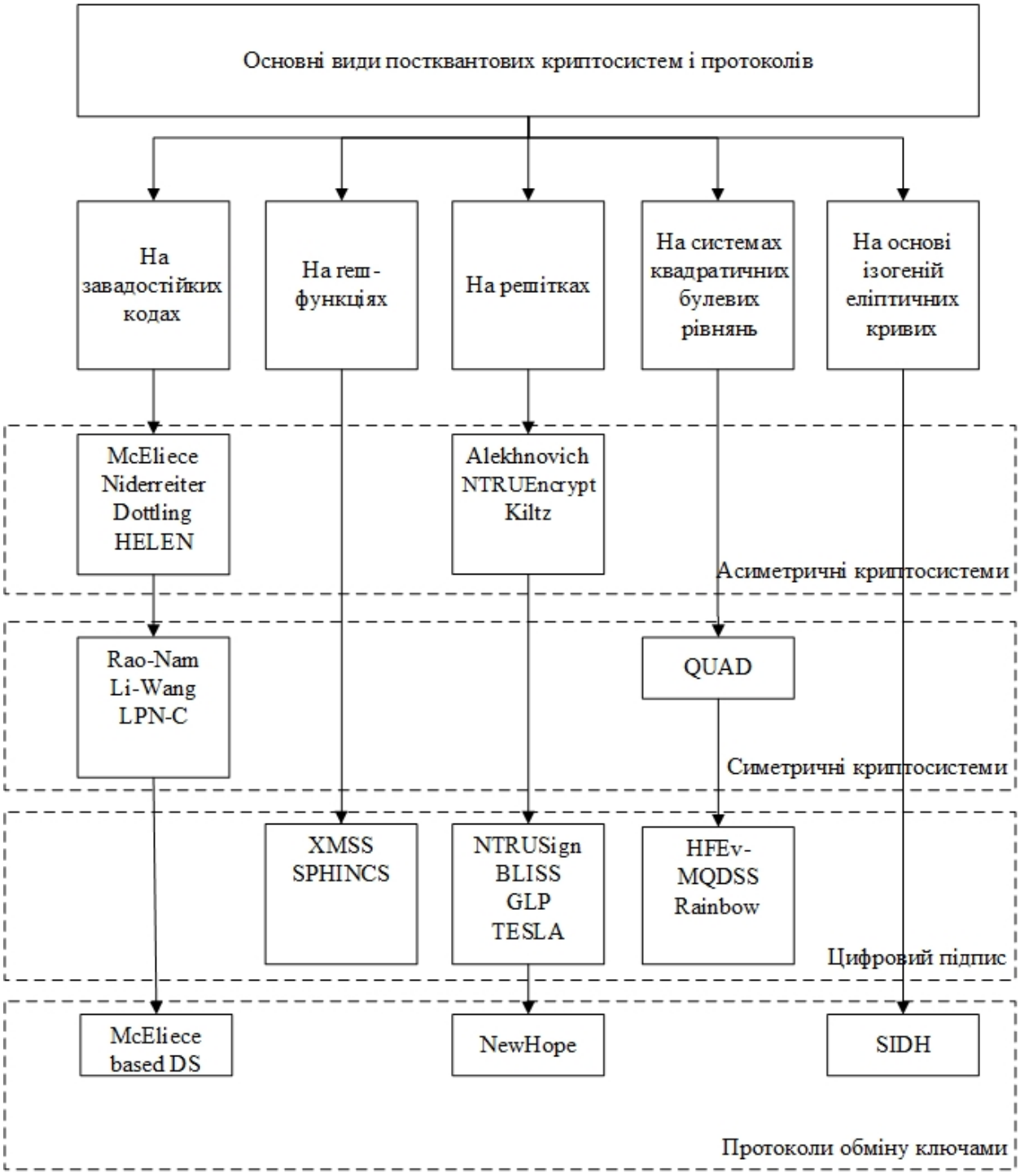

Рисунок 1.1. Основні види постквантових криптосистем і протоколів

Стійкість криптосистем на завадостійких кодах базується на складності розв’язання задачі декодування випадкового двійкового лінійного коду. Не відомо алгоритмів, зокрема, у квантовій моделі обчислень, які здатні розв’язати цю задачу за поліноміальний час [22].

Першою асиметричною кодовою криптосистемою є шифросистема Мак-Еліса [23]. Шифросистема Нідеррайтера [24], так само як і Мак-Еліса, використовує двійкові коди Гоппи, але при цьому потребує значно меншої довжини ключів (близько 1 МБ замість 4 МБ). Існують також інші криптопримітиви, побудовані на завадостійких кодах, зокрема, кодові ґеш-функції [25], генератори псевдовипадкових послідовностей [26] та алгоритми цифрового підпису [27].

Одну з найперших симетричних шифросистем, LPN-C, стійкість якої базується на складності декодування випадкового двійкового лінійного коду, запропоновано в [28]. Зауважимо, що на відміну від інших кодових шифросистем [23, 24, 29-31], зазначена шифросистема є обґрунтовано стійкою відносно атак на основі підібраних відкритих повідомлень (CPA-стійкою). Проте це не виключає необхідності оцінювання стійкості шифросистеми відносно конкретних атак з метою належного вибору її параметрів.

Стійкість шифросистем на ґеш-функціях базується на складності розв’язання задач пошуку прообразу значення ґеш-функції або обчислення її колізії [32]. У порівнянні з повним перебором всіх можливих значень квантовий алгоритм Гровера дає виграш лише в $\sqrt{2^n}$ для задачі пошуку прообразу [33] та в $\sqrt[3]{2^n}$ для пошуку колізії ґеш-функції [34]. На основі ґеш-функцій побудовані такі алгоритми цифрового підпису як XMSS [35] та SPHINCS [36]. Варто зазначити, що алгоритм XMSS пропонується міжнародним співтовариством вчених (IETF) до стандартизації для використання у протоколах мережі Інтернет [37]. Недоліками зазначених

схем цифрового підпису є необхідність зберігати стан ключа у випадку XMSS або розмір значення цифрового підпису (близько 40 КБ).

Криптографічні системи на решітках будуються на основі двох близько пов'язаних між собою обчислювально складних задачах: знаходження найкоротшого вектору в решітці у евклідовому просторі (SVP, shortest vector problem) або найближчого вектору решітки до заданого вектору (CVP, closest vector problem) та задачі LWE (learning with errors). Відомі також численні модифікації обох задач, для яких на сьогодні не існує алгоритмів розв'язання за поліноміальний час (зокрема, постквантових) [38, 39].

Перші криптосистеми на решітках запропоновано в 90-і роки. Зокрема, як альтернативу асиметричним алгоритмам RSA та іншим, побудованим на еліптичних кривих, створено шифросистему NTRUEncrypt [40], стійкість якої базується на складності розв'язання задачі SVP. Окрім асиметричних шифросистем, відомі також алгоритми цифрового підпису на решітках: NTRUSign [41], BLISS [42], GLP [43], TESLA [44] та протокол обміну ключами NewHope [45], що базується на задачі LWE.

Перша криптосистема, стійкість якої базується на складності розв'язання довільних систем квадратичних булевих рівнянь, запропонована в [46]. На відміну від систем лінійних рівнянь, не відомо ефективних алгоритмів розв'язання випадкових систем квадратичних рівнянь над скінченним полем [47]. Зауважимо, що алгоритм Гровера дозволяє розв'язувати системи квадратичних рівнянь на квантовому комп'ютері лише за $\sqrt{2^n}$ кроків у порівнянні з 2^n при повному переборі всіх можливих значень [48]. Серед криптографічних алгоритмів на квадратичних рівняннях відзначимо схеми цифрового підпису HFEv [49, 50], Rainbow [51], MQDSS [52], а також потоковий шифр QUAD [53].

Криптосистеми на ізогеніях еліптичних кривих утворюють наймолодший серед усіх перерахованих класів (див. рис. 1.1). На відміну від класичних алгоритмів, де обчислення відбуваються в групі точок однієї

еліптичної кривої, вводяться операції відображення однієї кривої на іншу – ізогенії. Відповідні шифросистеми з відкритим ключем запропоновано в [54, 55]. Пізніше запропоновано використовувати ізогенії звичайних еліптичних кривих на суперсингулярні криві [56], що дозволяє підвищити стійкість та дещо зменшити час виконання операцій шифрування та розшифрування даних.

Як видно з рис. 1.1, більшість постквантових криптосистем належить до асиметричних. Це обумовлено лише частковим зниженням стійкості традиційних симетричних шифросистем відносно квантових атак, оскільки для протидії алгоритму Гровера достатньо вдвічі збільшити довжину ключа.

В рамках проекту PQCRYPTO опубліковано мінімальні значення параметрів шифросистем, стійкість яких залишиться достатньо високою в квантовій моделі обчислень [21]. Зокрема, наведено довжини ключів для симетричних алгоритмів шифрування AES, Salsa20, схем автентифікації GCM та Poly1305, шифросистеми Мак-Еліса та схем цифрового підпису XMSS та SPHINCS-256.

В цілому, постквантові криптосистеми та протоколи програють традиційним криптопримітивам за такими характеристиками як довжина ключа, швидкість передачі інформації у системі та час, необхідний для виконання обчислень. Це можна розглядати як платню за стійкість відносно квантових атак. Разом з тим, беззаперечною перевагою симетричних постквантових шифросистем є обґрунтована залежність їх стійкості від складності розв’язання лише однієї математичної задачі.

Таким чином, можлива поява у найближчому майбутньому повноцінних квантових комп’ютерів потребує переходу до постквантових криптосистем і протоколів, стійкість яких базується на математичних задачах, що є складними як у традиційній, так і у квантовій моделях обчислень. Зокрема, на сьогодні є актуальними задачі розробки методів побудови та оцінювання стійкості постквантових (зокрема, симетричних) шифросистем.

1.2 Аналіз методів побудови та оцінювання стійкості симетричних постквантових шифросистем, що базуються на складності розв'язання задачі LPN

Однією з найбільш відомих та добре вивчених обчислювальних задач є задача LPN (learning parity with noise) [57]. Разом з задачею SVP, LPN є одним з найкращих кандидатів на роль універсальної основи для побудови постквантових криптографічних примітивів [58, 59]. Основними перевагами шифросистем, що будуються на основі класичної задачі LPN, є простота реалізації та можливість застосування у пристроях з обмеженими технічними характеристиками [58, 59].

Класична задача LPN полягає у відновленні невідомого вектора $a \in \mathbf{Z}_2^n$ за m незалежними випадковими рівноймовірними двійковими векторами A_i довжини n та значеннями b_i, які обчислюються за формулою

$$b_i = A_i a \oplus \xi_i,\ i \in \overline{1,m}, \tag{1.1}$$

де ξ_i є незалежними випадковими величинами, розподіленими за законом

$$\mathbf{P}(\xi_i = 1) = 1 - \mathbf{P}(\xi_i = 0) = p < 1/2,\ i \in \overline{1,m}. \tag{1.2}$$

Таким чином, класична задача LPN характеризується трьома параметрами: числом n невідомих, числом m рівнянь у системі (1.1) та ймовірністю p спотворень у правих частинах рівнянь цієї системи.

При $p = 0$ задача легко розв'язується за допомогою методу Гаусса, але з ростом параметрів n та p розв'язати задачу LPN стає практично неможливим.

У пострадянській літературі LPN розглядається як задача розв'язання системи лінійних рівнянь зі спотвореними правими частинами, яку іноді записують у вигляді

$$Ax = b = Aa + \xi, \tag{1.3}$$

де A – $m \times n$-матриця, сформована з рядків $A_i, i \in \overline{1,m}$ (а + позначає додавання в полі з двох елементів) [60 – 65]. Ця задача є окремим випадком більш загальної обчислювальної задачі – LWE (learning with errors), яка полягає у розв'язанні системи рівнянь (1.3) за модулем простого числа q, причому вважається, що координати вектора ξ мають дискретний гауссів розподіл [66]. Відомо, що задача LWE є обчислювально складною, оскільки зводиться до пошуку найкоротшого вектора у довільних решітках [66 – 68].

На сьогодні немає доведення, що класична задача LPN є складною у квантовій моделі обчислень. Разом з тим, вона рівносильна задачі декодування випадкового лінійного коду, яка, в свою чергу, є NP-повною [69]. Крім того, задача LPN близько пов'язана з теорією вивідування інформації (learning theory). Зокрема, якщо задача LPN може бути розв'язана за поліноміальний час, то деякі концептуальні класи обчислювально складних задач також можуть бути розв'язані за поліноміальний час [70].

Зауважимо про окремий випадок задачі LPN, який полягає у розв'язанні СР (1.3) від $n = 1$ змінних над факторкільцем $\mathbf{Z}_q[x]/(f(x))$, де $f(x)$ – поліном над кільцем $\mathbf{Z}_q$. Зазначену задачу називають Ring-LWE [71]. Перевагами криптосистем, що будуються на її основі, є менша довжина ключів та вища швидкість роботи алгоритмів шифрування [72]. В [72 – 74] показано, що задача LPN над кільцем поліномів $\mathbf{Z}_q[x]/(f(x))$ є поліноміально еквівалентною задачі пошуку найкоротшого вектора в ідеалах кільця $\mathbf{Z}_q[x]/(f(x))$, яка є NP-складною.

На рис. 1.2 наведено класифікацію задач LPN та атак, що будуються на її основі в залежності від числа рівнянь в системі (1.3) та алгебраїчної структури кільця, над яким розглядається задача. Враховуючи спільність у формулюванні цих задач, доцільно називати *задачею LPN над* (*скінченним*) *кільцем* R будь-яку задачу розв'язання системи рівнянь (1.3) над цим кільцем, незалежно від виду кільця або розподілу ймовірностей спотворень у правих частинах рівнянь системи (вимагаючи тільки, щоб цей розподіл був відмінним від рівномірного розподілу ймовірностей на R). Зауважимо також, що кількість рівнянь у системі (1.3) суттєво впливає на вибір методу її розв'язання. Потенційно необмежена кількість рівнянь виникає, як правило, при побудові атак на симетричні шифросистеми або протоколи ідентифікації типу HB [75 – 78].

На сьогодні відомо чимало конструкцій асиметричних шифросистем та протоколів, стійкість яких базується на складності розв'язання задач LPN над різними видами кілець (як, правило, це кільця лишків цілих чисел або факторкільця вигляду $\mathbf{Z}_q[x]/(f(x))$) [66, 68, 79 – 87].

Одну з найперших асиметричних криптосистем на базі задачі LPN запропоновано в [88]. Секретним ключем криптосистеми є вектор a, а відкритим – пара $(A, b = Aa \oplus \xi)$ (тут і далі використовуються позначення з формул (1.1) – (1.3)).

Для зашифрування символу $v \in \{0,1\}$ необхідно згенерувати випадковий вектор-стовпець f з незалежними координатами, розподіленими за законом Бернуллі з параметром $p < 1/2$, та обчислити шифротекст (u, c), де

$$u = f^T A,\ c = f^T b \oplus v.$$

Розшифрування відбувається за формулою $v' = c \oplus u^T a$. При цьому можливі помилки розшифрування, для зменшення ймовірності яких пропонується багаторазово зашифровувати та передавати кожен біт відкритого тексту.

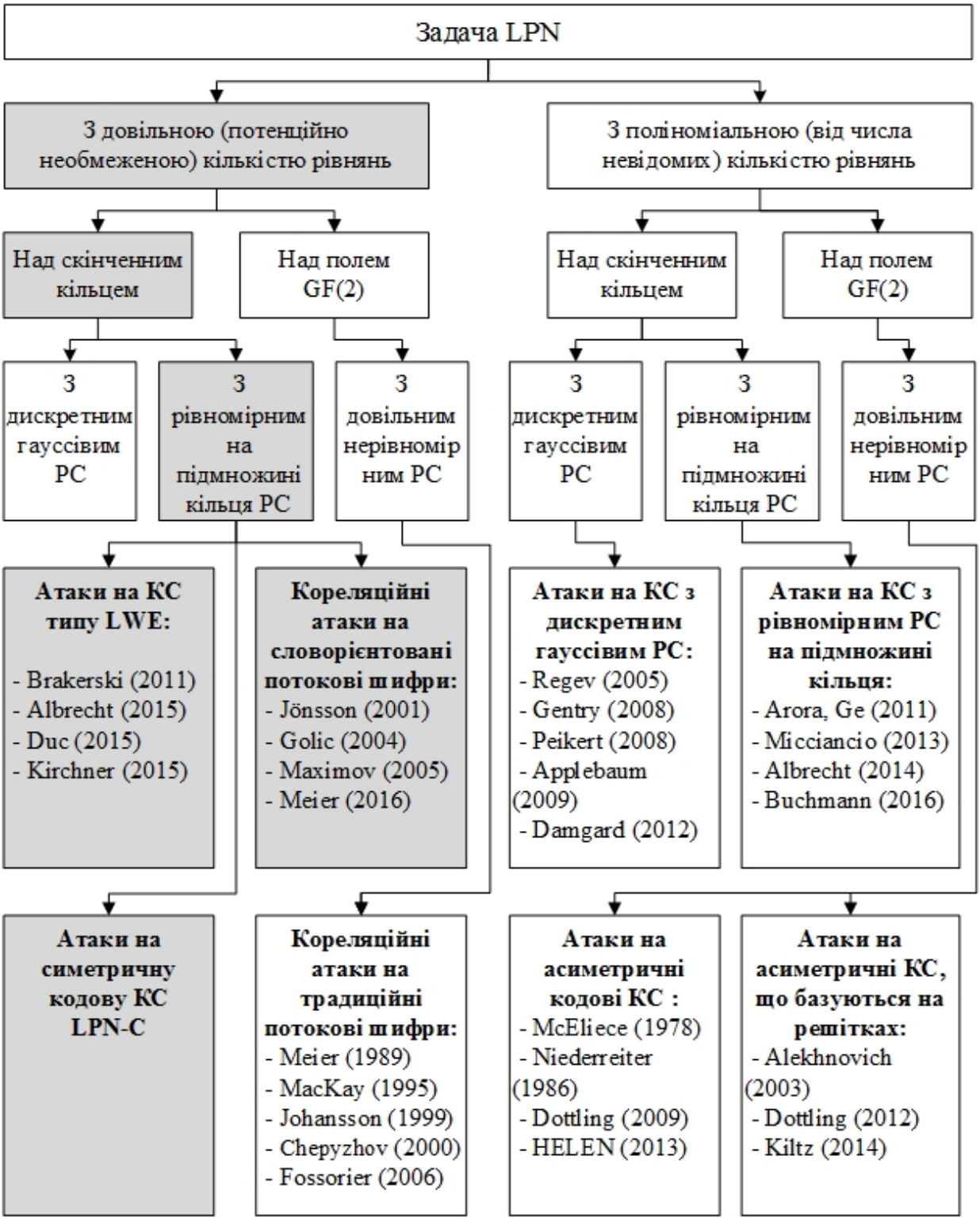

Рисунок 1.2. Класифікація задач LPN та атак, що будуються на її основі

Відомі численні вдосконалення зазначеної шифросистеми, що є більш практичними, але усі вони будуються на тому ж самому принципі: задача відновлення секретного ключа за відкритим зводиться до розв’язання СР (1.3) над скінченним полем або кільцем лишків [58, 89], причому кількість m

рівнянь у системі є фіксованою і не може бути збільшена за бажанням супротивника при проведення атаки на шифросистему. Найкращі алгоритми розв'язання задачі LPN в цьому випадку базуються на синдромному декодуванні блокових кодів (для випадку поля з двох елементів) або на пошуку коротких векторів у певних решітках (у випадку кільця лишків за модулем цілого числа або полінома) [58].

Поряд з тим, для симетричних шифросистем, що будуються на основі задачі LPN, супротивник може будувати системи вигляду (1.3), які складаються з довільної кількості рівнянь зі спотвореними правими частинами, що суттєво збільшує можливості супротивника при проведенні атак.

Як приклад, розглянемо шифросистему LPN-C [28], яка, за умови належного вибору параметрів, є стійкою відносно атак з адаптивно вибраним відкритим текстом (IND-P2-C0). Для її побудови вибирається двійковий лінійний $[L, K, D]$-код C, що дозволяє виправляти будь-яку комбінацію з $t \le \left\lfloor \frac{D-1}{2} \right\rfloor$ помилок.

В ролі ключа використовується випадкова рівноймовірна $n \times L$-матриця M, а шифроване повідомлення, що отримується в результаті зашифрування відкритого тексту x на ключі M визначається за формулою $(a, y = xG \oplus aM \oplus \xi)$, де G – твірна матриця коду C, a – випадковий рівноймовірний вектор довжини n, ξ – випадковий рівноймовірний вектор довжини L та ваги t. Законний отримувач, знаючи ключ M, отримує спотворене кодове слово $xG \oplus \xi$, за яким може швидко відновити відкритий текст x, використовуючи алгоритм декодування коду C. Зрозуміло, що супротивник може реалізувати на шифросистему атаку з підібраним відкритим повідомленням, зашифровуючи m разів нульове повідомлення $x = 0$ та формуючи L систем лінійних рівнянь зі спотвореними правими частинами $a_i M_j + \xi_{i,j} = y_{i,j}$, $i \in \overline{1,m}$, відносно стовпців M_j невідомої

матриці M, $j \in \overline{1, L}$. При цьому, на відміну від асиметричних шифросистем, кількість рівнянь в зазначених СР може бути як завгодно великою, що надає супротивнику можливість застосовувати для розв'язання цих СР відомі субекспоненційні алгоритми [90 – 92].

Зауважимо, що конструкція шифросистеми LPN-C [28] допускає природне узагальнення на випадок довільного скінченного кільця. Як правило, таке узагальнення, пов'язане з ускладненням алгебраїчної структури об'єкту, на основі якого будується та чи інша шифросистема, збільшує її стійкість відносно відомих атак, проте в даному випадку це питання залишається відкритим. На сьогодні відсутні неасимптотичні оцінки обсягу матеріалу, достатнього для надійного розв'язання задачі LPN над довільним скінченним кільцем. Залишається також не вирішеною задача про неасимптотичну часову складність узагальненого алгоритму BKW, який являє собою природне розширення на випадок довільного скінченного кільця одного з найкращих відомих алгоритмів розв'язання задачі LPN над полем з двох елементів [90]. Як наслідок, стійкість багатьох симетричних шифросистем, які будуються над скінченними кільцями (по аналогії з відомими шифросистемами, що базуються на складності розв'язання класичної задачі LPN), залишається не визначеною, що стримує практичне застосування цих шифросистем у сучасних спеціальних інформаційний і телекомунікаційних системах.

Ще одним напрямом сучасної криптології, близько пов'язаним із задачею LPN, є розробка кореляційних атак на потокові, зокрема, словоорієнтовані, шифри (див. рис. 1.2). Кожна кореляційна атака фактично полягає у складанні та розв'язанні певної системи лінійних рівнянь зі спотвореними правими частинами, яка звичайно будується над полем з двох елементів [93, 94]. Протягом останніх років з'явилися атаки на словоорієнтовані шифри (зокрема, SNOW 2.0; рис. 1.3 [95]), де СР зі спотвореними правими частинами будуються над скінченними полями

порядку 2^r, де $r > 1$. Як показано в [96], ефективність таких атак може бути помітно більшою в порівнянні з ефективністю звичайних (двійкових) кореляційних атак. Зазначений факт стимулює подальший розвиток методів розв'язання задачі LPN над полями або скінченними кільцями загального вигляду.

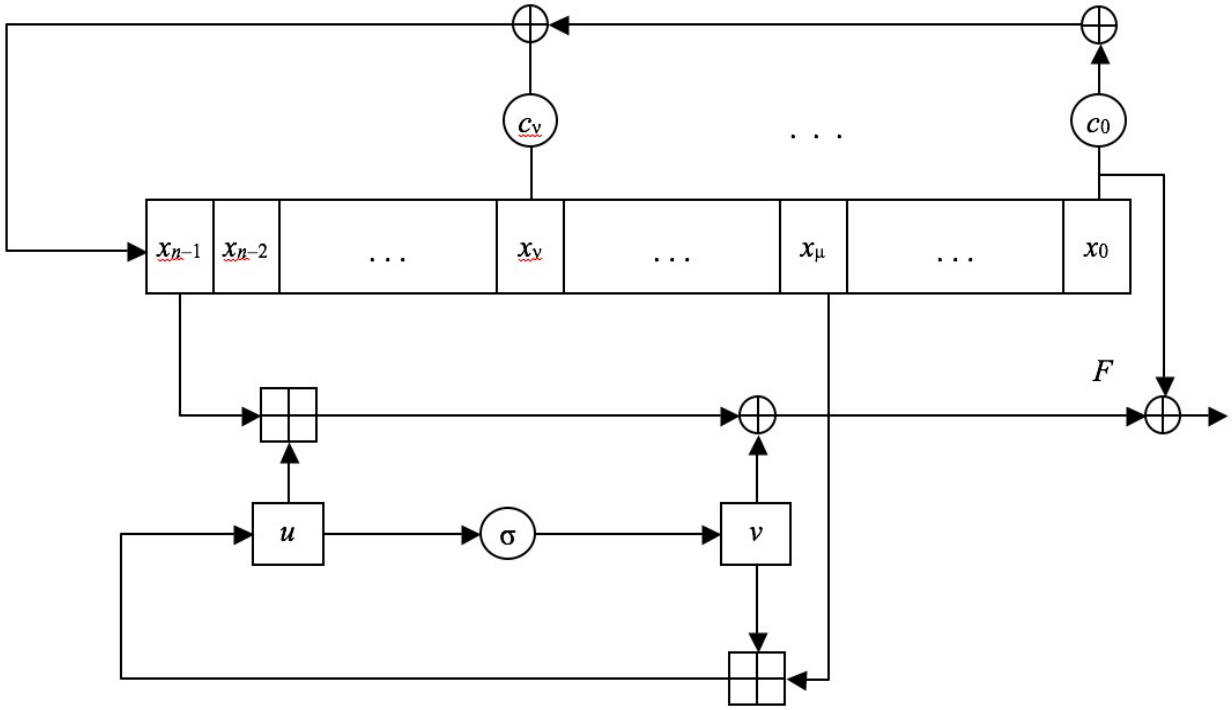

Рисунок 1.3. Схема генератора гами SNOW 2.0-подібного потокового шифру

В цілому, задача LPN є перспективним кандидатом на роль універсальної основи для побудови постквантових криптосистем і протоколів. Відомо чимало шифросистем, зокрема, симетричних, стійкість яких базується на складності розв'язання цієї задачі при різних припущеннях щодо структури кільця, над яким розв'язується задача, кількості рівнянь у системі або законі розподілу ймовірностей у правих частинах її рівнянь [28, 75 – 78, 87, 88, 97]. Разом з тим, деякі з запропонованих шифросистем виявляються слабкими, а окремі алгебраїчні структури – непридатними для використання [98, 99], що призводить до необхідності окремо досліджувати стійкість новостворених шифросистем. У свою чергу, це потребує

удосконалення відомих та розробки нових методів розв'язання задачі LPN над більш широкими класами скінченних кілець.

1.3. Аналіз методів та алгоритмів розв'язання задачі LPN

Як показано вище, задача LPN зводиться до розв'язання системи лінійних рівнянь зі спотвореними правими частинами (1.3).

Одним з найвідоміших методів розв'язання цієї задачі є *метод максимуму правдоподібності* (ММП) [60, 61], викладений спочатку для СР зі спотвореними правими частинами над полем з двох елементів [60, 61]. Цей метод природнім чином узагальнюється на системи лінійних рівнянь зі спотвореними правими частинами над довільними скінченними кільцями. Його сутність полягає в наступному.

Кожному вектору $x \in \mathbf{Z}_2^n$ ставиться у відповідність вектор спотворень $\varepsilon(x) = b \oplus Ax \in \mathbf{Z}_2^m$. В якості оцінки істинного розв'язку a системи рівнянь вважається найбільш правдоподібний вектор $x^* \in \mathbf{Z}_2^m$, тобто такий, що задовольняє умові $\mathbf{P}\{\varepsilon = \varepsilon(x^*)\} = \max\{\mathbf{P}\{\varepsilon = \varepsilon(x)\} : x \in \mathbf{Z}_2^n\}$. В теорії кодування [100] аналогічна процедура, що застосовується для декодування блокових кодів, називається методом декодування у найближче кодове слово. У випадку, коли система лінійних рівнянь розв'язується над скінченним (асоціативним) кільцем R з одиницею, $|R| = q$, оцінка істинного розв'язку обчислюється за правилом $\mathbf{P}\{\varepsilon = \varepsilon(x^*)\} = \max\limits_{x \in R^n} \mathbf{P}\{\varepsilon = \varepsilon(x)\}$, де $\varepsilon(x) = b - Ax$ для будь-якого $x \in R^n$.

Таким чином, фактично ММП полягає в повному переборі всіх можливих розв'язків системи лінійних рівнянь та виборі такого з них, що найбільше відповідає вектору спотворень для заданого розподілу ймовірностей його координат.

Відомо [60, 101], що у випадку, коли вектор a є рівномірно розподіленим на множині всіх можливих векторів довжини n випадковим вектором, ММП має найбільшу надійність (забезпечує найменшу середню ймовірність помилки при відновленні вектору a) серед усіх методів розв'язання СР (1.3).

В [60] отримані аналітичні оцінки надійності ММП для випадку булевої системи рівнянь відповідно з випадковою рівноймовірною та фіксованою лівою частиною. Зокрема, для випадку фіксованої матриці коефіцієнтів СР (1.3) ймовірність обчислення правильного розв'язку такої системи методом максимуму правдоподібності обчислюється за формулою [60]:

$$\mathbf{P}\{x^* = a\} \geq 1 - \sum_{k \geq 1} | X_k | \, p(k), \tag{1.4}$$

де X_k – множина $n-$мірних векторів $x \in \mathbf{Z}_2^n$, при підстановці яких до СР (1.3) виявляється точно k рівнянь, яким не задовольняє вектор x,

$$p(k) = \sum_{i \geq k/2} C_k^i p^i (1-p)^{k-i} \leq \sigma^k, \;\; \sigma = \sqrt{4p(1-p)}, \;\; k \in \{0,...,t\}.$$

В [60] також наведена умова, за якої ймовірність правильного розв'язку СР (1.3) спрямовується до 1:

$$\sum_{k \geq 1} | X_k | \, (\sqrt{4p(1-p)})^k = o(1) \text{ при } n, t \to \infty.$$

Наведена оцінка (1.4) надійності ММП є асимптотичною, вона дозволяє лише отримати уяву про поведінку ймовірності правильного розв'язку СР (1.3). Разом з тим, її складно застосовувати на практиці, оскільки вона не містить явної залежності від конкретних параметрів системи рівнянь. Крім

того, залишається відкритим питання як оцінити ймовірність відновлення істинного розв'язку СР зі спотвореними правими частинами методом максимуму правдоподібності у випадку, коли такі системи розглядаються над довільними полями характеристики 2 або скінченними кільцями. В [96, 102] та деяких інших роботах використовуються лише евристичні оцінки надійності ММП для випадку скінченного поля порядку 2^r.

Основним недоліком методу максимуму правдоподібності є його висока часова складність, оскільки істинний розв'язок вибирається шляхом перебору усіх векторів довжини n. Відомо (див., наприклад, [103, 104]), що трудомісткість ММП розв'язання систем лінійних рівнянь зі спотвореними правими частинами над полем з двох елементів можна зменшити, застосовуючи алгоритми швидкого перетворення Адамара допоміжної псевдобулевої функції.

Нехай

$$g(x) = \begin{cases} (-1)^{b_i}, \text{ якщо } x = A_i; \\ 0 - \text{інакше.} \end{cases} \qquad (1.5)$$

Перетворення Адамара функції g обчислюється таким чином:

$$\hat{g}(\alpha) = \sum_{x \in \mathbf{Z}_2^n} (-1)^{\alpha x} g(x) = \sum_{i=1}^{t} (-1)^{b_i \oplus \alpha A_i} = t - \sum_{i=1}^{t} (b_i \oplus \alpha A_i) =$$

$$= t - |\varepsilon(\alpha)|, \ \alpha \in \mathbf{Z}_2^n.$$

Значення числа рівнянь, яким не задовольняє вектор $\alpha \in \mathbf{Z}_2^n$, обчислюється як $t - \hat{g}(\alpha)$, де $\hat{g}(\alpha)$ – коефіцієнт Адамара функції g з номером α.

Тоді, за умови, що всі стовпці матриці A є попарно різними, зокрема, виконується умова $t < 2^n$, алгоритм розв'язання системи рівнянь (1.3) над полем з двох елементів виглядає таким чином:

1. Побудувати функцію g за формулою (1.5) та обчислити її перетворення Адамара.

2. В якості оцінки істинного розв'язку СР вибрати такий вектор $x \in \mathbf{Z}_2^n$, для якого значення $\hat{g}(x)$ є максимальним.

Зменшення часової складності ММП у випадку наведеного алгоритму розв'язання СР (1.3) досягається за рахунок застосування алгоритмів швидкого перетворення Адамара [103].

В [104] запропоновано векторний варіант швидкої кореляційної атаки на комбінувальні генератори гами двійкових потокових шифрів. А саме, аналізується кореляція між вихідною послідовністю генератора гами та множиною всіх лінійних рекурентних регістрів, що в ньому використовуються. Такий підхід приводить до розв'язання задачі LPN над полями порядку 2^r. Для зменшення часової складності обчислення значень апостеріорних ймовірностей на другому етапі кореляційної атаки автори пропонують застосовувати алгоритм швидкого перетворення Фур'є розподілів ймовірностей. Зокрема, розподіл ймовірностей та його перетворення Фур'є над полем $R = \mathbf{GF}(2^r)$ пов'язані такими рівностями [104]:

$$P(\omega) = \sum_{x \in R} P(x)(-1)^{\omega x},$$

$$P(x) = 2^{-r} \sum_{\omega \in R} P(\omega)(-1)^{\omega x},$$

де $x, \omega \in R$, $\omega = (\omega_1, ..., \omega_r)$, $x = (x_1, ..., x_r)$ – векторний вигляд елементів поля R.

Застосування алгоритмів швидкого перетворення Фур'є дозволяє зменшити часову складність обчислення всіх значень апостеріорної ймовірності з $O(q^2)$ до $O(q \log q)$ операцій, де $q = 2^r$. Варто зазначити, що векторна кореляційна атака може бути також застосована і до словоорієнтованих потокових шифрів. Разом з тим, відкритим залишається питання про можливість застосування швидкого перетворення Фур'є для зменшення часової складності розв'язання задачі LPN над довільним скінченним кільцем.

В залежності від кількості наявних рівнянь в системі (1.3) алгоритми розв'язання задачі LPN над полем з двох елементів поділяються на такі класи:

– системи з субекспоненційною (від числа невідомих) кількістю рівнянь;

– системи з поліноміальною кількістю рівнянь;

– системи з лінійною кількістю рівнянь.

У випадку наявності субекспоненційної кількості рівнянь найкращі на сьогоднішній день з алгоритмів розв'язання задачі LPN мають також субекспоненційну часову складність. Вперше такий алгоритм запропоновано в 1988 році академіком І. М. Коваленком [105], який показав, що за певних умов таку систему рівнянь можна розв'язати з високою надійністю при $n \to \infty$, використовуючи при цьому, в середньому, $2^{O(n/\log n)}$ операцій.

Алгоритм Коваленка [105] фактично було повторно відкрито в [90], де він отримав назву BKW за першими літерами прізвищ його авторів. Алгоритм BKW [90] складається з двох етапів: редукції та розв'язання. Задачею етапу редукції є зменшення числа невідомих з n до n_1, де $n = n_1 a$. Для цього m рівнянь системи поділяються на певні класи еквівалентності. Два рівняння потрапляють до одного класу, якщо вони мають однакові

значення n_1 останніх коефіцієнтів. Для кожного класу еквівалентності обирається випадковий вектор – представник цього класу, для якого по черзі виконується операція додавання за модулем 2 з іншими векторами класу. Після цього обраний вектор вилучається з класу еквівалентності. В результаті отримуємо нову, зменшену систему рівнянь від $n - n_1$ невідомих, оскільки останні n_1 коефіцієнтів тепер дорівнюють 0. Повторюючи зазначену процедуру $a - 1$ разів, отримаємо n_1 перших невідомих. Далі в системі залишаються лише ті рівняння, вага Гемінга яких (число ненульових елементів вектора) дорівнює одиниці. Отримана система рівнянь розв'язується послідовно для кожної невідомої за мажоритарним правилом.

Фактично успішність етапу редукції базується на ефективності розв'язання задачі про адитивне представлення [91, 92], суть якої полягає в знаходженні для заданого списку L, який складається з l випадкових незалежних та рівноймовірних векторів $z_1, \ldots, z_l \in R^{n-n_1}$, k не обов'язково різних чисел $\nu_1, \ldots, \nu_k \in \{1, 2, \ldots, l\}$ таких, що $z_{\nu_1} \oplus \cdots \oplus z_{\nu_k} = 0$. Відомі ефективні алгоритми розв'язання задачі про адитивне представлення для випадків $R = \mathbf{GF}(2)$ [90, 106, 107] та $R = \mathbf{GF}(2^r)$, де $r \geq 2$ [108].

В [59] запропоновано дві модифікації алгоритму BKW, які покращують його ефективність. По-перше, на етапі розв'язання пропонується замість мажоритарного правила застосовувати алгоритми швидкого перетворення Адамара допоміжної функції. Такий підхід дозволяє відновлювати одразу n_1 невідомих. По-друге, на етапі редукції пропонується замість вибору представника класу еквівалентності попарно додавати за модулем 2 усі вектори одного класу. Зазначене дозволяє збільшити число рівнянь у випадку, якщо їх недостатньо для застосування алгоритму BKW.

В роботах [109 – 111] запропоновано нові підходи, які покращують ефективність етапу редукції алгоритму BKW. Наприклад, в [111] вводиться

додатковий етап попередніх обчислень, який дозволяє зменшити трудомісткість безпосередньо етапу редукції.

Одна з найбільш ефективних на сьогоднішній день модифікацій алгоритму BKW наведена в [96]. Авторами пропонується кореляційна атака на словоорієнтовані потокові шифри, такі як SNOW 2.0, SNOW 3G, Sosemanuk та інші, які розглядаються над полем $\mathbf{GF}(2^r)$. В [96] наведено еврістичну оцінку числа рівнянь, необхідних для надійного розв'язання СР (1.3) над полем з 2^r елементів. Крім того, в цій роботі пропонується алгоритм побудови рекурентних перевірочних співвідношень, який також базується на задачі про адитивне представлення. Разом з тим, зазначений алгоритм достатньо простий для реалізації та, на перший погляд, може бути узагальнений для застосування на етапі редукції алгоритму BKW над довільними скінченними кільцями. На другому етапі кореляційної атаки в [96] з метою підвищення ефективності при обчисленні статистичної відмінності між розподілом спотворень у правих частинах рівнянь та рівномірним розподілом запропоновано застосовувати алгоритм швидкого перетворення Адамара [112].

Таким чином, за наявності великої (субекспоненційної) кількості рівнянь розв'язання задачі LPN за допомогою алгоритму BKW або його модифікацій фактично зводиться до задачі про адитивне представлення та може бути розв'язана за допомогою субекспоненційного від n числа операцій.

Для систем з поліноміальним числом рівнянь алгоритми типу BKW не можуть бути застосовані у чистому вигляді. В [113] показано, як задача розв'язання системи з $n^{1+\alpha}$ лінійних рівнянь (1.3) з рівноймовірною матрицею коефіцієнтів може бути зведена до аналогічної задачі з $2^{O(n/\log n)}$ лінійних рівнянь. Крім того, запропоновано алгоритм розв'язання систем з поліноміальною кількістю рівнянь за $2^{O(n/\log\log n)}$ операцій. Таким чином, алгоритм [113] дозволяє збільшити число рівнянь шляхом побудови нових векторів за допомогою лінійних комбінацій випадково обраних з існуючих.

Такий підхід дозволяє “добудовувати” необхідну кількість рівнянь в системі, що, в свою чергу, дає можливість застосовувати звичайні алгоритми типу BKW. Зрозуміло, що поява додаткового етапу збільшення числа рівнянь призводить до збільшення часу, необхідного для розв’язання задачі в цілому [58, 92].

Для систем з лінійним числом рівнянь системи (1.3) на сьогодні існують алгоритми розв’язання задачі LPN лише з експоненційною складністю [114, 115].

Таким чином, найкращим на сьогодні з точки зору часової складності алгоритмом розв’язання задачі LPN є алгоритм BKW із запропонованими до нього модифікаціями. Але його застосування вимагає наявності субекспоненційної кількості рівнянь. Такі умови можуть бути створені, наприклад, при використанні симетричних постквантових шифросистем.

Алгоритм BKW адаптований також для розв’язання задачі LWE [116 – 118] або систем лінійних рівнянь вигляду (1.3) над полем $\mathbf{GF}(2^r)$ [96]. Разом з тим, в контексті дослідження стійкості шифросистем над окремими алгебраїчними структурами важливою науковою задачею є узагальнення алгоритму BKW на випадок довільного скінченного кільця.

Наведені факти свідчать про певне протиріччя між потребами в практичному застосуванні у сучасних спеціальних інформаційно-телекомунікаційних системах симетричних постквантових шифросистем, що базуються на складності розв’язання задачі LPN над довільними скінченними кільцями, з одного боку, та відсутністю методів оцінювання стійкості таких шифросистем, з іншого. Зазначене протиріччя визначає напрямок, характер та окремі задачі дисертаційного дослідження.

1.4. Основні напрями та окремі задачі дисертаційного дослідження

Вище показана актуальність наукової задачі дисертаційної роботи, що полягає в розробці більш ефективних (в порівнянні з перебірними) методів розв’язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем.

Метою дисертаційної роботи є отримання науково обґрунтованих оцінок стійкості симетричних шифросистем, які базуються на складності розв’язання задачі LPN над скінченними кільцями, на основі застосування більш ефективних методів розв’язання зазначеної задачі.

Об’єктом дослідження в дисертаційній роботі є симетричні постквантові шифросистеми, стійкість яких базується на складності розв’язання задачі LPN над скінченними кільцями, а предметом дослідження – методи розв’язання зазначеної задачі.

У відповідності до поставленої мети, наукова задача дисертаційної роботи включає в себе ряд взаємопов’язаних окремих задач, порядок розв’язання яких визначає основні напрями дисертаційних досліджень (рис. 1.4).

Перший напрям полягає в оцінюванні часової складності узагальненого алгоритму BKW для розв’язання задачі LPN над довільним скінченним скінченним кільцем (задачі 2 – 3 на рис. 1.4). Крім того, задачею цього напряму є підвищення ефективності існуючих та розробка нових методів розв’язання задачі LPN над скінченними кільцями (задачі 4 – 5 на рис. 1.4). Основною задачею другого напряму є застосування розроблених методів розв’язання задачі LPN до оцінювання стійкості конкретних постквантових шифросистем над кільцями лишків (задача 6 на рис. 1.4).

Вирішення перелічених окремих задач дозволяє вирішити наукову задачу дисертаційної роботи та досягнути поставленої в роботі мети.

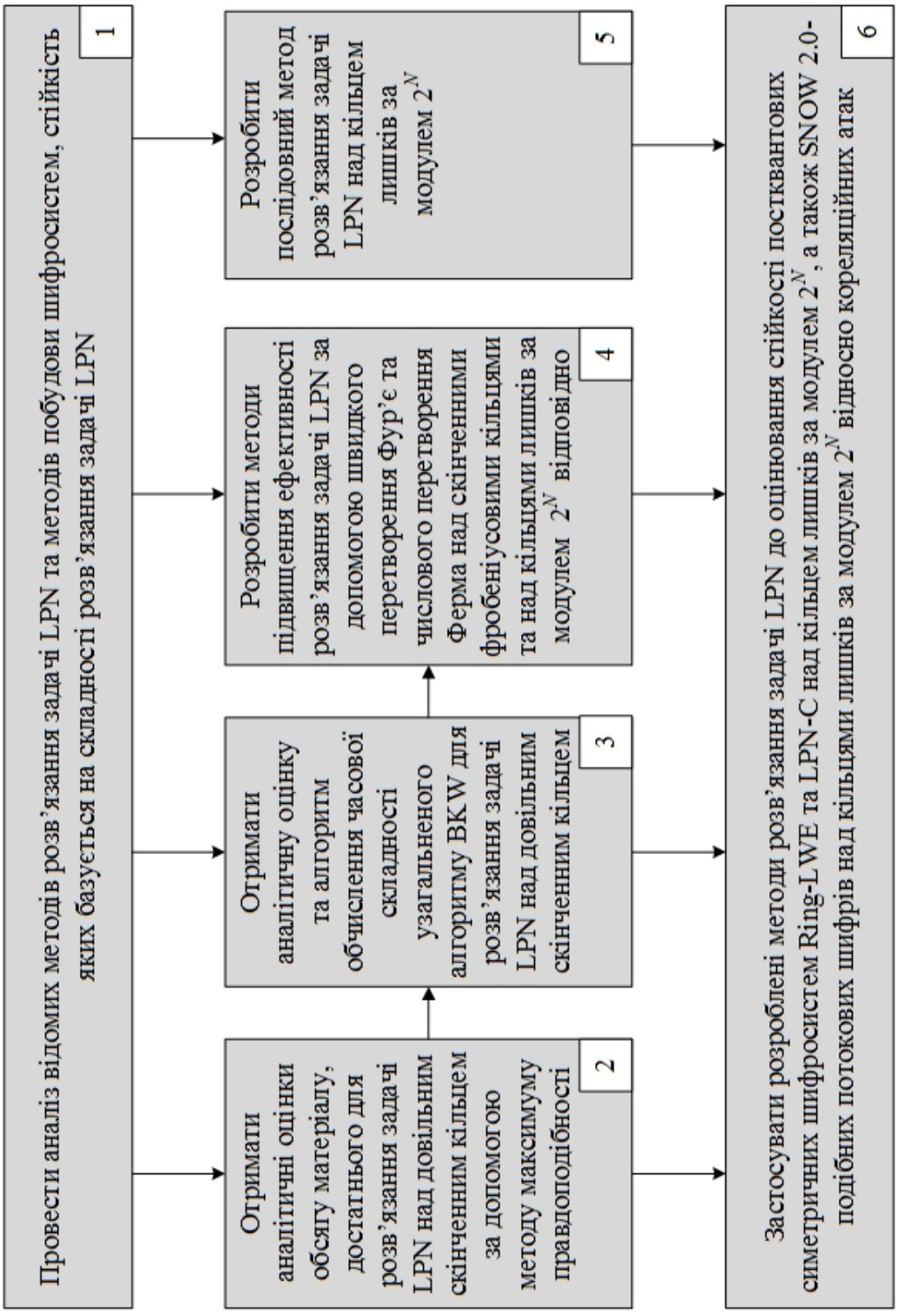

Рисунок 1.4. Окремі задачі досліджень

Висновки

1. Задача LPN є перспективним кандидатом на роль універсальної основи для побудови постквантових криптосистем і протоколів. Відомо

чимало шифросистем, зокрема, симетричних, стійкість яких базується на складності розв’язання цієї задачі при різних припущеннях щодо структури кільця, над яким розв’язується задача, кількості рівнянь у системі або законі розподілу ймовірностей у правих частинах її рівнянь. Разом з тим, деякі з запропонованих шифросистем виявляються слабкими, а окремі алгебраїчні структури – непридатними для використання, що призводить до необхідності окремо досліджувати стійкість новостворених шифросистем. У свою чергу, це потребує удосконалення відомих та розробки нових методів розв’язання задачі LPN над більш широкими класами скінченних кілець. Крім того, залишається відкритим питання як оцінити ймовірність відновлення істинного розв’язку CP зі спотвореними правими частинами методом максимуму правдоподібності у випадку, коли такі системи розглядаються над довільними полями характеристики 2 або скінченними кільцями.

2. Найкращими на сьогодні (з точки зору часової складності) алгоритмами розв’язання задачі LPN є алгоритм BKW та його модифікації. На сьогодні відсутні неасимптотичні оцінки обсягу матеріалу, достатнього для надійного розв’язання задачі LPN над довільним скінченним кільцем. Залишається також не вирішеною задача про неасимптотичну часову складність узагальненого алгоритму BKW, який являє собою природне розширення одного з найкращих відомих алгоритмів розв’язання задачі LPN над полем з двох елементів. Як наслідок, стійкість багатьох симетричних шифросистем, які будуються над скінченними кільцями (по аналогії з відомими шифросистемами, що базуються на складності розв’язання класичної задачі LPN), залишається не визначеною, що стримує практичне застосування цих шифросистем у сучасних спеціальних інформаційно-телекомунікаційних системах.

3. Для симетричних шифросистем, що будуються на основі задачі LPN, супротивник може будувати системи лінійних рівнянь зі спотвореними правими частинами, які складаються з довільної кількості рівнянь, що суттєво збільшує можливості супротивника при проведенні атак. Зокрема,

наявність субекспоненційного числа рівнянь дозволяє застосовувати алгоритми сімейства BKW, які мають найменшу трудомісткість з усіх відомих на сьогодні методів розв'язання задачі LPN.

4. У відповідності до поставленої мети, розв'язання наукової задачі дисертаційної роботи включає в себе дослідження за двома напрямами. Перший напрям полягає в оцінюванні часової складності узагальненого алгоритму BKW для розв'язання задачі LPN над довільним скінченним кільцем та розробці нових ефективних методів розв'язання цієї задачі. Основною задачею другого напряму є застосування розроблених методів розв'язання задачі LPN до оцінювання стійкості конкретних постквантових шифросистем над кільцями лишків.

Список використаних джерел у першому розділі

1. Deutsch D. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London. Mathematical, Physical and Engineering Sciences.* 1985. Vol. 400, № 1818. P. 97-117.

2. Bernstein D. J., Buchmann J., Dahmen E. Post-Quantum Cryptography : Springerlink, 2009. 246 с.

3. Nielsen M. A., Chuang I. L. Quantum computation and quantum information : Cambridge university press, 2000. 702 с.

4. *IBM's Test-Tube Quantum Computer Makes History* : веб-сайт. URL: https://www-03.ibm.com/press/us/en/pressrelease/965.wss (дата звернення: 06.08.2020).

5. *IBM Unveils World's First Integrated Quantum Computing System for Commercial Use* : веб-сайт. URL: https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System-for-Commercial-Use (дата звернення: 06.08.2020).

6. *Temporal Defense Systems Purchases the First D-Wave 2000Q Quantum Computer* : веб-сайт. URL: https://www.dwavesys.com/press-releases/temporal-defense-systems-purchases-first-d-wave-2000q-quantum-computer (дата звернення: 06.08.2020).

7. *A Preview of Bristlecone, Google's New Quantum Processor* : веб-сайт. URL: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html (дата звернення: 06.08.2020).

8. *2018 CES: Intel Advances Quantum and Neuromorphic Computing Research* : веб-сайт. URL: https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/ (дата звернення: 06.08.2020).

9. *Microsoft Quantum Development Kit* : веб-сайт. URL: https://www.microsoft.com/en-us/quantum/development-kit (дата звернення: 06.08.2020).

10. *List of quantum processors* : веб-сайт. URL: https://en.wikipedia.org/wiki/List_of_quantum_processors (дата звернення: 06.08.2020).

11. Aggarwal D., Brennen G. K., Lee T., Santha M., Tomamichel M. Quantum attacks on Bitcoin, and how to protect against them. *Cryptology ePrint Archive*. URL: https://eprint.iacr.org/2018/213 (дата звернення: 06.08.2020).

12. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Foundations of Computer Science:* Conference Publications, 1997. P. 1484-1509.

13. Shor P. W. Algorithms for quantum computer: Discrete logarithms and factoring. *Proceedings of 35th Annual Symposium of Foundations of Computer Science:* IEEE Computer Society Press, 1994. P. 124-134.

14. Grover L. K. A fast quantum mechanical algorithm for database search. *Proceedings of 28th Annual ACM Symposium on the Theory of Computing*, 1996. P. 212-219.

15. Dohotaru C., Hoyer P. Exact quantum lower bound for grover's problem. *Quantum Information and Computation*. 2009. Vol 9, № 5. P. 533-540.

16. *Report on Post-Quantum Cryptography. National Institute of Standards and Technology* : веб-сайт. URL: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (дата звернення: 06.08.2020).

17. *NSA preps quantum-resistant algorithms to head off crypto-apocalypse* : веб-сайт. URL: https://arstechnica.com/information-technology/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/ (дата звернення: 06.08.2020).

18. Moody D. Post Quantum Cryptography: NIST's Plan for the Future. *National Institute of Standards and echnology* : веб-сайт. URL: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf (дата звернення: 06.08.2020).

19. *European Telecommunications Standards Institute (ETSI). Quantum-Safe Cryptography* : веб-сайт. URL: https://www.etsi.org/technologies/quantum-safe-cryptography (дата звернення: 06.08.2020).

20. Niederhagen R., Waidner M. Practical Post-Quantum Cryptography. *Fraunhofer Institute for secure information technology* : веб-сайт. URL: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Practical.PostQuantum.Cryptography_WP_FraunhoferSIT.pdf (дата звернення: 06.08.2020).

21. Augot D. et al. Initial recommendations of long-term secure post-quantum systems : веб-сайт. URL: http://pqcrypto.eu.org/docs/initial-recommendations.pdf (дата звернення: 06.08.2020).

22. Overbeck R., Sendrier N. Code-based cryptography. *PostQuantum Cryptography, Springer*. 2009. P. 95-146.

23. McEliece R. J. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *The Deep Space Network Progress Report 42-44*. 1978. P. 114-116.

24. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory.* 1986. Vol. 15. P. 19-34.

25. Augot D., Finiasz M., Sendrier N. A Family of Fast Syndrome Based Cryptographic Hash Functions. *Progress in Cryptology, LNCS, Springer*. 2005. Vol. 3715. P. 64-83.

26. Fischer J.-B., Stern J. An Efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding. *Advances in Cryptology - EUROCRYPT 1996*, *LNCS, Springer*. 1996. Vol. 1070. P. 245-255.

27. Courtois N. T., Finiasz M., Sendrier N. How to Achieve a McElieceBased Digital Signature Scheme. *Advances in Cryptology - ASIACRYPT 2001*, *LNCS, Springer*. 2001. Vol. 2248. P. 157-174.

28. Gilbert H., Mattew J.B., Robshaw M.J.B., Seurin Y. How to Encrypt with the LPN Problem. *ICALP, Part 2, LNCS, Springer Verlag*. 2008. Vol. 5126. P. 679-690.

29. Duc A., Vaudenay S. HELEN: A public-key cryptosystem based on the LPN and the decisional minimal distance problems. *Progress in Cryptology – AFRICACRYPT 2013*, *LNCS*. 2013. Vol. 7918. P. 286-296.

30. Hooshmand R., Eghlidos T., Aref M.R. Improving the Rao-Nam secret key cryptosystem using regular EDF-QC-LDPC codes. *ISeCure Journal*. 2012. Vol. 4, № 1. P. 3-14.

31. Li Y.X., Wang X.M. A joint authentication and encryption scheme based on algebraic coding theory, applied algebra, algebraic algorithms and error correcting codes. *LNCS, Springer Verlag*. 1991. Vol. 539. P. 241-245.

32. Merkle R. C. Secrecy, authentication, and public key systems: technical report № 1971-1, Electrical Engineering, Stanford. 1979, URL: https://www.merkle.com/papers/Thesis1979.pdf (дата звернення: 06.08.2020).

33. Amy M., Matteo O. D., Gheorghiu V., Mosca M., Parent A., Schanck J. Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2016/992 (дата звернення: 06.08.2020).

34. Oorschot P. C., Wiener M. J. Parallel Collision Search with Cryptanalytic Applications. *Journal of Cryptology*. 1999. Vol. 12, № 1. P. 1-28.

35. Buchmann J., Dahmen E., Hülsing A. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. *Post-Quantum Cryptography, PQCrypto 2011, LNCS, Springer*. 2011. Vol. 7071. P. 117-129.

36. Bernstein D. J., Hopwood D., Hülsing A., Lange T., Niederhagen R., Papachristodoulou L., Schneider M., Schwabe P., Wilcox-O'Hearn Z. SPHINCS: practical stateless hash-based signatures. *Advances in Cryptology - EUROCRYPT 2015, LNCS, Springer*. 2015. Vol. 9056. P. 368-397.

37. Butin D., Hülsing A., Mohaisen A., Gazdag S.-L. XMSS: Extended Hash-Based Signatures. RFC 8391. *Crypto Forum Research Group, IETF*. 2018. URL: https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/ (дата звернення: 06.08.2020).

38. *IEEE P1363.1: Draft standard for Public-Key Cryptographic Techniques Based on Hard Problems over Lattices*, URL: https://pdfs.semanticscholar.org/4e23/5fd5671971d913f4daee4903ab2aaf84f796.pdf (дата звернення: 06.08.2020).

39. Ajtai M. Generating Hard Instances of Lattice Problems. *ACM Symposium on Theory of Computing - STOC'96. ACM*, 1996. P. 99-108.

40. Hoffstein J., Pipher J., Silverman J. H. NTRU: A ring-based public key cryptosystem. *Algorithmic Number Theory: Third International Symposiun, ANTS-III, LNCS, Springer*. 1998. Vol. 1423. P. 267-288.

41. Hoffstein J., Howgrave-Graham N., Pipherv J., Silverman J. H., Whyte W. NTRUSign: digital signatures using the NTRU lattice. *CT-RSA LNCS, Springer*. 2003. Vol. 2612. P. 122-140.

42. Ducas L., Durmus A., Lepoint T., Lyubashevsky V. Lattice Signatures and Bimodal Gaussians. *Advances in Cryptology - CRYPTO 2013, LNCS, Springer*. 2013. Vol. 8042. P. 40-56.

43. Güneysu T., Lyubashevsky V., Pöppelmann T. Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems. *Cryptographic*

Hardware and Embedded Systems - CHES 2012, LNCS, Springer. 2012. Vol. 7428. P. 530-547.

44. Alkim E., Bindel N., Buchmann J., Dagdelen Ö., Schwabe P. TESLA: Tightly-Secure Efficient Signatures from Standard Lattices. *IACR Cryptology ePrint Archive.* URL: https://eprint.iacr.org/2015/755/20150730:095248 (дата звернення: 06.08.2020).

45. Alkim E., Ducas L., Pöppelmann T., Schwabe P. Post-quantum key exchange - a new hope. *IACR Cryptology ePrint Archive.* URL: https://eprint.iacr.org/2015/1092 (дата звернення: 06.08.2020).

46. Matsumoto T., Imai H. Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. *Advances in Cryptology - EUROCRYPT 1988, LNCS, Springer*. 1988. Vol. 330. P. 419-453.

47. Bouillaguet C., Cheng C.-M., Chou T., Niederhagen R., Yang B.-Y. Fast Exhaustive Search for Quadratic Systems in F2 on FPGAs. *Selected Areas in Cryptography - SAC 2013, LNCS, Springer*. 2013. Vol. 8282. P. 205-222.

48. Schwabe P., Westerbaan B. Solving Binary MQ with Grover's Algorithm. *Security, Privacy, and Applied Cryptography Engineering – SPACE 2016, LNCS, Springer*. 2016. Vol. 10076. P. 303-322.

49. Patarin J. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. *Advances in Cryptology - EUROCRYPT '96, LNCS, Springer*. 1996. Vol. 1070. P. 33-48.

50. Kipnis A., Patarin J., Goubin L. Unbalanced Oil and Vinegar Signature Schemes. *Advances in Cryptology - EUROCRYPT '99, LNCS, Springer.* 1999. Vol. 1592. P. 206-222.

51. Ding J., Schmidt D. Rainbow, a New Multivariable Polynomial Signature Scheme. *Applied Cryptography and Network Security - ACNS 2005, LNCS, Springer*. 2005. Vol. 3531. P. 164-175.

52. Hülsing A., Rijneveld J., Samardjiska S., Schwabe P. From 5-pass MQ-based identification to MQ-based signatures. *Advances in Cryptology - Asiacrypt 2016, LNCS, Springer*. 2016. Vol. 10032. P. 135-165.

53. Berbain C., Gilbert H., Patarin J. QUAD: A Practical Stream Cipher with Provable Security. *Advances in Cryptology - EUROCRYPT 2006, LNCS, Springer*. 2006. Vol. 4004. P. 109-128.

54. Rostovtsev A., Stolbunov A. Public-key Cryptosystem Based on Isogenies. *IACR Cryptology ePrint Archive.* URL: https://eprint.iacr.org/2006/145 (дата звернення: 06.08.2020).

55. Stolbunov A. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications.* 2010. Vol. 4, № 2. P. 215-235.

56. Jao D., De Feo L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. *Post-Quantum Cryptography – PQCrypto, LNCS, Springer*. 2011. Vol. 7071. P. 19-34.

57. Blum A., Furst M. L., Kearns M. J., Lipton R. J. Cryptographic primitives based on hard learning problems. *CRYPTO 1993, LNCS*. 1993. Vol. 773. P. 278-291.

58. Bogos S. LPN in cryptography: an algorithmic study : PhD thesis: *Ecole Polytechnique Federale de Lausanne,* 2017. 157 p. URL: https://infoscience.epfl.ch/record/228977/files/EPFL_TH7800.pdf (дата звернення: 06.08.2020).

59. Levieil E., Fouque P.-A. An Improved LPN Algorithm. *Security and Cryptography for Networks, 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006, Proceedings, LNCS, Springer*. 2006. Vol. 4116. P. 348-359.

60. Балакин Г. В. Введение в теорию случайных систем уравнений. *Труды по дискретной математике.* 1997. т. 1. С. 1-18.

61. Балакин Г. В. О вероятностном подходе к решению систем уравнений с целочисленными неизвестными. *Дискретная математика*. 1995. т. 7, Вып. 1. С. 88-98.

62. Алексейчук А. Н. Системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2001. № 4. С. 12-19.

63. Алексейчук А. Н., Лукъянов В. В. Метод декодирования блоковых кодов в канале с аддитивным по модулю 2^N шумом по частично известным входным и выходным сообщениям. *Моделювання та інформаційні технології. Збірник наукових праць ІПМЕ НАН України*. 2001. Вип. 10. С. 88-93.

64. Балакин Г. В. Оценка истинного решения системы уравнений над кольцом вычетов при аддитивной помехе. *Проблемы теоретической кибернетики:* тез. докл. XII Междунар. конф.: Нижний Новгород, 1999. С. 15.

65. Смирнов В. Г. Системы булевых уравнений рекуррентного типа. *Обозрение прикл. промышл. матем.* 1995. т. 2, Вып. 3. С. 477-482.

66. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*: Baltimore, MD, USA, 2005. P. 84-93.

67. Brakerski Z., Langlois A., Peikert C., Regev O., Stehlé D. Classical hardness of learning with errors. *45th ACM STOC*: Palo Alto, CA, USA, June 1–4, 2013, P. 575-584.

68. Peikert C. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. *Proceedings of the 41st annual ACM symposium on theory of computing, STOC 2009*: Bethesda, MD, USA, 2009. P. 333-342.

69. Berlekamp E.R., McEliece R.J., van Tilborg H.C.A. On the inherent intractability of certain coding problems. *IEEE Trans. Information Theory IT.* 1978. Vol. 24. P. 384-386.

70. Feldman V., Gopalan P., Khot S., Ponnuswami A.K. New results for learning noisy parities and halfspaces. *In 47th FOCS*: Berkeley, CA, USA, October 21–24, 2006, IEEE Computer Society Press, 2006. P. 563-574.

71. Lyubashevsky V., Peikert C., Regev O. On ideal lattices and learning with errors over rings. *Eurocrypt 2010, LNCS, Springer.* 2010. Vol. 6110. P. 1-23.

72. Damgard I., Park S. How practical is public-key encryption based on LPN and Ring-LPN? *IACR Cryptology ePrint Archive.* URL: https://eprint.iacr.org/2012/699 (дата звернення: 06.08.2020).

73. Peikert C., Rosen A. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. *TCC 2006, LNCS, Springer*. 2006. Vol. 3876. P. 145-166.

74. Stehl´e D., Steinfeld R., Tanaka K., Xagawa K. Efficient public key encryption based on ideal lattices. *ASIACRYPT 2009, LNCS, Springer, Heidelberg*. 2009. Vol. 5912. P. 617-635.

75. Hopper N. J., Blum M. Secure Human Identification Protocols. *Advances in Cryptology - ASIACRYPT 2001, Proceedings of Lecture Notes in Computer Science, Springer*. 2001. Vol. 2248. P. 52-66.

76. Juels A. and Weis S. A. Authenticating Pervasive Devices with Human Protocols. *Advances in Cryptology - CRYPTO 2005, Proceedings, LNCS, Springer*. 2005. Vol. 3621. P. 293-308.

77. Bringer J., Chabanne H., Dottax E. HB++: a Lightweight Authentication Protocol Secure against Some Attacks. *Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing:* 29 June 2006, Lyon, France, IEEE Computer Society, 2006. P. 28-33.

78. Gilbert H., Robshaw M. J. B., Seurin Y. HB#: Increasing the Security and Efficiency of HB+. *Advances in Cryptology - EUROCRYPT 2008, Proceedings, LNCS, Springer*. 2008. Vol. 4965. P. 361-378.

79. Peikert C., Vaikuntanathan V., Waters B. A framework for efficient and composable oblivious transfer. *Proceedings of the 28th Annual conference on Cryptology: Advances in Cryptology*, *CRYPTO 2008: Berlin, Heidelberg: Springer-Verlag*, 2008. P. 554-571.

80. Peikert C., Waters B. Lossy trapdoor functions and their applications. *Proceedings of the 40th annual ACM symposium on Theory of computing*, *STOC '08*: New York, NY, USA: ACM, 2008. P. 187-196.

81. Goldwasser S., Kalai Y. T., Peikert C., Vaikuntanathan V. Robustness of the learning with errors assumption. *Innovations in Computer Science ICS'10*, 2010. P. 230-240.

82. Gentry C. Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st annual ACM symposium on Theory of computing*, *STOC '09*: New York, USA: ACM, 2009. P. 169-178.

83. Brakerski Z., Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) lwe. *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, *FOCS '11*: Washington, 98 DC, USA: IEEE Computer Society, 2011. P. 97-106.

84. Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. *Proceedings of the 40th annual ACM symposium on Theory of computing*: New York, USA: ACM, 2008. P. 197-206.

85. Ding J. New cryptographic constructions using generalized learning with errors problem. *Cryptology ePrint Archive.* URL: https://eprint.iacr.org/2012/387 (дата звернення: 06.08.2020).

86. Banerjee A., Peikert C., Rosen A. Pseudorandom functions and lattices. *Proceedings of the 31st Annual international conference on Theory and Applications of Cryptographic Techniques*, *EUROCRYPT'12,* Berlin, Heidelberg: Springer-Verlag, 2012. P. 719-737.

87. Heyse S. et al. Lapin: an efficient authentication protocol based on Ring-LPN. *FSE, LNCS, Springer*. 2012. Vol. 7549. P. 346-365.

88. Alekhnovich M. More on average case vs approximation complexity. *FOCS, IEEE Computer Society*. 2003, P. 298-307.

89. Kuebler R. J. Time-memory trade-offs for the learning parity with noise problem: PhD thesis, Ruhr-University, Bochum, Chair for Cryptology, 2018. URL: https://d-nb.info/116345169X/34 (дата звернення: 06.08.2020).

90. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. 2003. Vol. 50, № 3. P. 506-519.

91. Bogos S., Tramer F., Vaudenay S. On solving LPN using BKW and variants. Implementation and analysis. *Cryptology ePrint Archive.* URL: http://eprint.iacr.org/2015/049 (дата звернення: 06.08.2020).

92. Олексійчук А.М. Субекспоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. *Прикладная радиоэлектроника.* 2012. Т. 11, № 2. С. 3-11.

93. Canteaut A. Fast correlation attacks against stream ciphers and related open problems. *The 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, ITW 2005, E-Proc*, 2005. P. 49-54.

94. Meier W. Fast correlation attacks: methods and countermeasures. *LNCS, FSE'2011, Proceedings, Springer Verlag*, 2011. P. 55-67.

95. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. *Selected Areas in Cryptography, SAC 2002, LNCS, Springer-Verlag*. 2002. Vol. 2295. P. 47-61.

96. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive.* URL: http://eprint.iacr.org/2016/311 (дата звернення: 06.08.2020).

97. Katz J., Shin J. S., Smith A. Parallel and concurrent security of HB and HB^{+} protocols. *Journal Cryptology.* 2010. Vol. 23, № 3. P. 402-421.

98. Eisenträger K., Hallgren S., Lauter K. E. Weak instances of PLWEK. *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal*: QC, Canada, August 14-15, 2014, LNCS, Springer, 2014. Vol. 8781. P. 183-194.

99. Elias Y., Lauter K. E., Ozman E., Stange K. E.Provably weak instances of ring-lwe. *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference*: Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, LNCS, Springer, 2015. Vol. 9215. P. 63-92.

100. Месси Дж. Пороговое декодирование. М.: Мир, 1966. 208 с.

101. Chechyota S. I. Introduction to discrete information and coding theory: a training edition. M.: MCCME Press, 2011. 224 p.

102. Cateaut A., Naya-Plasencia M. Correlation attacks on combination generators. *Cryptography and Communications*. 2012. Vol. 4, № 3-4. P. 147-171.

103. Fino B. J., Algazi V.R. Unified matrix treatment of the Walsh-Hadamard transform. *IEEE transactions on computers*. 1976. Vol. 25, № 11. P. 1142-1146.

104. Golić J. D., Morgari G. Vectorial fast correlation attacks. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2004/247 (дата звернення: 06.08.2020).

105. Коваленко І.М. Про алгоритм субекспоненційної складності декодування сильно спотворених лінійних кодів. *Доп. АН УРСР, Сер. А*. 1988. № 10. С. 16-17.

106. Wagner D. A generalized birthday problem. *Advances in Cryptology – CRYPTO'02, Proceedings, Springer,* 2002. P. 288 – 303.

107. Bhattacharyya A., Indyk P., Woodruff D. P., Xie N. The complexity of linear dependence problems in vector spaces. *Innovations in Computer Science – ICS 2010*: Bijing, China, Jan 7 – 9, Proceedings, 2011. P. 496-508.

108. Minder L., Sinclair A. The extended k-tree algorithm. *The 19th Annual ACM-SIAM Sympposium on Discrete Algorithms, Proceedings*, 2009. P. 586-595.

109. Fossorier M. P. C., Mihaljevic M. J., Imai H., Cui Y., Matsuura K. An Algorithm for Solving the LPN Problem and Its Application to Security Evaluation of the HB Protocols for RFID Authentication. *INDOCRYPT, LNCS, Springer*. 2006. Vol. 4329. P. 48-62.

110. Guo Q., Johansson T., Londahl C. Solving LPN Using Covering Codes. *20th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt),* 2014. Vol. 8873. P. 1-20.

111. Zhang B., Jiao L., Wang M. Faster algorithms for solving LPN. *Advances in Cryptology – EUROCRYPT 2016: 35th Annual International*

Conference on the Theory and Applications of Cryptographic Techniques: Vienna, Austria, May 8-12, 2016, Proceedings, Part I, 2016. P. 168-195.

112. Yarlagadda R. R., Hershey J. E. Hadamard matrix analysis and synthesis with applications to communications and signal/image processing. Kluwer academic publishers, 1997. 120 p.

113. Lyubashevsky V. The Parity Problem in the Presence of Noise, Decoding Random Linear Codes, and the Subset Sum Problem. *APPROX 2005, RANDOM 2005*: Berkeley, CA, USA, August 22-24, 2005, Proceedings, LNCS, Springer, 2005. Vol. 3624. P. 378-389.

114. May A., Meurer A., Thomae E. Decoding Random Linear Codes in O(2ˆ{0.054n}). *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security*: Seoul, South Korea, December 4-8, 2011. Proceedings, LNCS, Springer, 2011. Vol. 7073. P. 107-124.

115. Stern J. A method for finding codewords of small weight. *Coding Theory and Applications, 3rd International Colloquium*: Toulon, France, November 2-4, 1988, Proceedings, LNCS, Springer, 1988. Vol. 388. P. 106-113.

116. Albrecht M. R., Cid C., Faug`ere J.-C., Fitzpatrick R., Perret L. On the complexity of the BKW algorithm on LWE. *Des. Codes Cryptography*. 2015. Vol. 74, Issue 2. P. 325-354.

117. Duc A., Tram`er F., Vaudenay S. Better algorithms for LWE and LWR. *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques:* Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I, LNCS, Springer, 2015. Vol. 9056. P. 173-202.

118. Paul Kirchner P., Fouque P.-A. An improved BKW algorithm for LWE with applications to cryptography and lattices. *CRYPTO 2015, LNCS, Springer*. 2015. Vol. 9215. P. 43-62.

РОЗДІЛ 2

АНАЛІТИЧНІ ОЦІНКИ ОБСЯГУ МАТЕРІАЛУ, ДОСТАТНЬОГО ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ LPN МЕТОДОМ МАКСИМУМУ ПРАВДОПОДІБНОСТІ

В попередньому розділі зазначено, що універсальним методом розв'язання задачі LPN є добре відомий в теорії статистичних рішень та її застосуваннях метод максимуму правдоподібності. За певних умов цей метод забезпечує найменшу (середню) ймовірність помилки серед усіх статистичних процедур розв'язання СР зі спотвореними правими частинами та часто використовується як допоміжний алгоритм в сучасних швидких алгоритмах розв'язання класичної задачі LPN над полем з двох елементів (див., наприклад, [1]).

Поряд з тим, за винятком класичної задачі LPN [2], на сьогодні відсутні неасимптотичні оцінки обсягу матеріалу (числа рівнянь у системі зі спотвореними правими частинами), достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем.

В даному розділі отримані такі аналітичні оцінки. Перша з них доводиться за допомогою нерівності Гефдінга [3] і встановлює явну залежність потрібного обсягу матеріалу від основних параметрів системи (порядку кільця, числа невідомих та розподілу спотворень у правих частинах рівнянь у системі). Друга, наближена, оцінка базується на застосуванні центральної граничної теореми і встановлює вираз обсягу матеріалу в термінах квантилів нормального розподілу ймовірностей.

Шляхом порівняння отриманих оцінок з відомою нижньою межею обсягу матеріалу [4] показано, що обидві оцінки надають можливість визначати за порядком величини фактичний обсяг матеріалу, достатній для надійного розв'язання задачі LPN над довільним скінченним кільцем.

Показано також, що отримані оцінки дозволяють визначити часову складність узагальненого алгоритму BKW [5], відомий прототип якого [6] є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN.

2.1. Аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем

Позначимо R довільне скінченне кільце з одиницею, $|R| = q$.
Розглянемо систему рівнянь зі спотвореними правими частинами

$$Ax = b, \tag{2.1}$$

де A – $m \times n$-матриця над кільцем R, b – вектор довжини m з координатами

$$b_i = A_i a + \xi_i,\ i \in \overline{1,m}, \tag{2.2}$$

де $A_1, \dots, A_m$ – рядки матриці A, $a = (a_1,\dots,a_n)^{\mathrm{T}}$ – невідомий вектор-стовпець над кільцем R (істинний розв'язок СР (2.1)), $\xi_1, \dots, \xi_m$ – незалежні випадкові величини, розподілені за законом $\mathbf{P}\{\xi_i = z\} = p(z)$, де $p(z) \geq 0$ для кожного $z \in R$, $\sum_{z \in R} p(z) = 1$. Задача LPN полягає у відновленні вектора a за відомими матрицею A, вектором b і розподілом ймовірностей $p_\xi = (p(z) : z \in R)$.

Для будь-якого $x \in R^n$ позначимо $\varepsilon(x) = b - Ax$. Нагадаємо (див., наприклад, [2, 7]), що розв'язання СР (2.1) методом максимуму правдоподібності полягає в знаходженні "оцінки" a^* вектора a за правилом $\mathbf{P}\{\xi = \varepsilon(a^*)\} = \max_{x \in R^n} \mathbf{P}\{\xi = \varepsilon(x)\}$, де $\xi = (\xi_1, \dots, \xi_m)$. Якщо вектор a є

рівномірно розподіленим на множині R^n, то метод максимуму правдоподібності має найменшу (середню) ймовірність помилки серед усіх методів розв'язання СР (2.1) (див., наприклад, [8], с. 141).

При практичному застосуванні ММП звичайно виконують такий алгоритм [2, 7]:

1) для кожного $x \in R^n$ обчислюють значення функції

$$\lambda(x) = \sum_{z \in N_\xi(R)} n(z \mid \varepsilon(x)) \log qp(z), \ x \in R^n, \tag{2.3}$$

де $N_\xi(R) = \{z \in R : p(z) > 0\}$, $n(z \mid \varepsilon(x))$ – частота зустрічальності елемента z у векторі $\varepsilon(x)$;

2) знаходять вектор a^* за правилом $\lambda(a^*) = \max\{\lambda(x) : x \in R^n\}$ (якщо існує декілька таких векторів, то вибирають будь-який з них).

Оскільки $\lambda(x) = \log \mathbf{P}\{\xi = \varepsilon(x)\} + q \log q$, $x \in R^n$, то вектор a^*, який отримується з використанням наведеного алгоритму, співпадає з розв'язком СР (2.1) за допомогою ММП. При цьому часова складність алгоритму дорівнює

$$T(n) = 2nmq^n \tag{2.4}$$

операцій додавання та множення в кільці R.

На сьогодні аналітичні оцінки обсягу матеріалу, достатнього для відновлення істинного розв'язку СР (2.1) методом максимуму правдоподібності відомі лише для випадку, коли кільце R є полем з двох елементів [2]. В [9, 10] та деяких інших роботах використовуються евристичні оцінки надійності ММП для випадку скінченного поля порядка 2^r. Наступне твердження уточнює та узагальнює зазначені результати.

Твердження 2.1. Нехай матриця A має рівномірний розподіл ймовірностей на множині усіх матриць розміру $m \times n$ над кільцем R та не залежить від випадкового вектора $\xi = (\xi_1, \dots, \xi_m)$. Позначимо $N_\xi(R) = \{z \in R : p(z) > 0\}$, $p_{\max} = \max\limits_{z \in R} p(z)$, $p_{\min} = \min\limits_{z \in N_\xi(R)} p(z)$ та припустимо, що $p_{\max} \neq p_{\min}$. Тоді для будь-якого $a \in R^n$ справедлива нерівність

$$\mathbf{P}_{A,\xi}\{a^* = a\} \geq 1 - q^n \exp\left\{ - \frac{m(D(p \,\|\, \omega) + D(\omega \,\|\, p))^2}{2(\log p_{\max} - \log p_{\min})^2} \right\},$$

де

$$D(p \,\|\, \omega) = \sum_{z \in N_\xi(R)} p(z) \log qp(z), \tag{2.5}$$

$$D(\omega \,\|\, p) = - q^{-1} \sum_{z \in N_\xi(R)} \log qp(z). \tag{2.6}$$

Доведення. Перш за все, нагадаємо відому нерівність Гефдінга [3], яка використовується надалі: якщо $\xi_1, \dots, \xi_t$ є незалежними випадковими величинами такими, що $\alpha_i \leq \xi_i \leq \beta_i$, де $\alpha_i, \beta_i \in \mathbf{R}$, $i \in \overline{1,m}$, то для будь-якого $u > 0$ має місце нерівність

$$\mathbf{P}\{\sum_{i=1}^{m} (\xi_i - \mathbf{E}\xi_i) \geq mu\} \leq \exp\left\{ - \frac{2m^2u^2}{\sum\limits_{i=1}^{m} (\beta_i - \alpha_i)^2} \right\}. \tag{2.7}$$

Згідно з наведеним вище описом ММП для будь-якого $c \in \mathbf{R}$ справедливе співвідношення

$$\{a^* \neq a\} \subseteq \{\lambda(a) < c\} \cup \left(\bigcup_{x \neq a} \{\lambda(x) \geq c\} \right),$$

з якого випливає, що

$$\mathbf{P}\{a^* \neq a\} \leq \mathbf{P}\{\lambda(a) < c\} + (q^n - 1) \max_{x \neq a} \mathbf{P}\{\lambda(x) \geq c\}. \quad (2.8)$$

Для будь-яких $x \in R^n$, $z \in N_\xi(R)$, $i \in \overline{1,m}$ розглянемо випадкову величину $\xi_{i,z}(x)$, яка приймає значення 1, якщо i-та координата випадкового вектора $\varepsilon(x) = A(a - x) + \xi$ дорівнює z, та значення 0 – у протилежному випадку. На підставі формули (2.3) справедлива рівність

$$\lambda(x) = \sum_{i=1}^{m} \eta_i(x), \quad (2.9)$$

де

$$\eta_i(x) = \sum_{z \in N_\xi(R)} \xi_{i,z}(x) \log qp(z), \; i \in \overline{1,m}. \quad (2.10)$$

Зауважимо, що для будь-якого $x \in R^n$ випадкові величини (2.10) є незалежними в сукупності та однаково розподіленими.

Знайдемо математичне сподівання $\mathbf{E}\eta_i(x)$ випадкової величини $\eta_i(x)$ для кожного $x \in R^n$. Якщо $x = a$, то на підставі рівності (2.10)

$$\mathbf{E}\eta_i(a) = \sum_{z \in N_\xi(R)} \mathbf{E}\xi_{i,z}(a) \log qp(z) = \sum_{z \in N_\xi(R)} \mathbf{P}\{\xi_i = z\} \log qp(z) = D(p \,\|\, \omega). \quad (2.11)$$

Якщо $x \neq a$, то

$$\mathbf{E}\eta_i(x) = \sum_{z \in N_\xi(R)} q^{-1} \log qp(z) = -D(\omega \,\|\, p). \qquad (2.12)$$

Підставимо у нерівність (2.8) значення $c = 1/2 \cdot m(D(p \,\|\, \omega) - D(\omega \,\|\, p))$. Тоді на підставі співвідношень (2.9), (2.11), (2.12) отримаємо такі рівності:

$$\mathbf{P}\{\lambda(a) < c\} = \mathbf{P}\{\lambda(a) - \mathbf{E}\lambda(a) < c - mD(p \,\|\, \omega)\} =$$

$$= \mathbf{P}\{\lambda(a) - \mathbf{E}\lambda(a) < 1/2 \cdot m(D(p \,\|\, \omega) + D(\omega \,\|\, p))\},$$

$$\mathbf{P}\{\lambda(x) \geq c\} = \mathbf{P}\{\lambda(x) - \mathbf{E}\lambda(x) \geq c + mD(\omega \,\|\, p)\} =$$

$$= \mathbf{P}\{\lambda(x) - \mathbf{E}\lambda(x) \geq 1/2 \cdot m(D(p \,\|\, \omega) + D(\omega \,\|\, p))\}, \; x \neq a.$$

Для оцінювання виразу в правій частині нерівності (2.8) застосуємо нерівність (2.7) до випадкових величин $\xi_i = \eta_i(x)$, $i \in \overline{1,m}$. Помітимо, що на підставі формули (2.10) $\log qp_{\min} \leq \eta_i(x) \leq \log qp_{\max}$, $i \in \overline{1,m}$, звідки випливає, що

$$\mathbf{P}\{\lambda(a) < c\} \leq \exp\left\{-\frac{mD((p \,\|\, \omega) + D(\omega \,\|\, p))^2}{2(\log p_{\max} - \log p_{\min})^2}\right\},$$

$$\mathbf{P}\{\lambda(a) \geq c\} \leq \exp\left\{-\frac{mD((p \,\|\, \omega) + D(\omega \,\|\, p))^2}{2(\log p_{\max} - \log p_{\min})^2}\right\}, \; x \neq a.$$

Підставляючи наведені оцінки у формулу (2.8), отримаємо нерівність

$$\mathbf{P}\{a^* = a\} \geq 1 - q^n \exp\left\{ - \frac{m(D(p \,\|\, \omega) + D(\omega \,\|\, p))^2}{2(\log p_{\max} - \log p_{\min})^2} \right\}.$$

Отже, твердження доведено.

Наслідок 2.1. За умови твердження 2.1 метод максимуму правдоподібності надає можливість відновити істинний розв'язок СР (2.1) з ймовірністю помилки не більше ніж $\delta \in (0, 1/2)$ (відносно сумісного розподілу матриці A та вектора ξ), якщо число m рівнянь у системі є не менше ніж

$$m_1 = \frac{2n \ln(q\delta^{-1})(\log p_{\max} - \log p_{\min})^2}{(D(p \,\|\, \omega) + D(\omega \,\|\, p))^2}. \qquad (2.13)$$

Отримаємо зараз іншу, наближену оцінку ймовірності $\mathbf{P}\{a^* = a\}$, яка базується на нормальній апроксимації ймовірностей в лівій частині нерівності (2.8).

Позначимо $D_x = \mathbf{D}\eta_i(x)$ дисперсію випадкової величини $\eta_i(x)$, $x \in R^n$, $i \in \overline{1, m}$. На підставі формул (2.10) – (2.12) справедливі рівності

$$D_a = \sum_{z \in N_\xi(R)} p(z) \log^2(qp(z)) - D(p \,\|\, \omega)^2, \qquad (2.14)$$

$$D_x = q^{-1} \sum_{z \in N_\xi(R)} \log^2(qp(z)) - D(\omega \,\|\, p)^2, \; x \neq a, \qquad (2.15)$$

де параметри $D(p \,\|\, \omega)$ і $D(\omega \,\|\, p)$ визначаються за формулами (2.5) і (2.6) відповідно.

Твердження 2.2. Нехай $\alpha, \beta > 0$ та число m рівнянь у системі (2.1) є не менше ніж

$$m_2 = \left(\frac{u_\alpha \sqrt{D_a} + u_\beta \sqrt{D_x}}{D(p \,\|\, \omega) + D(\omega \,\|\, p)} \right)^2, \tag{2.16}$$

де u_α, u_β – квантилі нормального розподілу, що визначаються за формулами

$$\alpha = \Phi(-u_\alpha),\ \beta = 1 - \Phi(u_\beta),\ \Phi(u) \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-\frac{t^2}{2}} dt,\ u \in \mathbf{R}. \tag{2.17}$$

Тоді справедлива наближена оцінка

$$\mathbf{P}\{a^* = a\} \geq 1 - (\alpha + (q^n - 1)\beta)). \tag{2.18}$$

Доведення. Підставимо у формулу (2.8)

$$c = m_2 D(p \,\|\, \omega) - u_\alpha \sqrt{m_2 D_a}\ . \tag{2.19}$$

На підставі рівності (2.16) отримаємо, що

$$c = -m_2 D(\omega \,\|\, p) + u_\beta \sqrt{m_2 D_x}\ . \tag{2.20}$$

Помітимо, що, оскільки доданки в формулі (2.9) є незалежними та однаково розподіленими випадковими величинами, то на підставі центральної граничної теореми та формул (2.11), (2.12), (2.14), (2.15), (2.19) і (2.20) справедливі наступні (наближені) рівності:

$$\mathbf{P}\{\lambda(a) < c\} = \mathbf{P}\{\frac{\lambda(a) - m_2\mathbf{E}\eta_1(a)}{\sqrt{m_2 D_a}} < \frac{c - m_2\mathbf{E}\eta_1(a)}{\sqrt{m_2 D_a}}\} = \Phi(-u_\alpha) = \alpha, \quad (2.21)$$

$$\mathbf{P}\{\lambda(x) \geq c\} = \mathbf{P}\{\frac{\lambda(x) - m_2\mathbf{E}\eta_1(x)}{\sqrt{m_2 D_x}} \leq \frac{c - m_2\mathbf{E}\eta_1(x)}{\sqrt{m_2 D_x}}\} = 1 - \Phi(u_\beta) = \beta. \quad (2.22)$$

Підставляючи вирази (2.21), (2.22) в формулу (2.8), отримаємо нерівність (2.18).

Твердження доведено.

Наслідок 2.2. Нехай $\alpha, \beta > 0$, $\alpha + (q^n - 1)\beta \leq \delta$. Тоді метод максимуму правдоподібності надає можливість відновити істинний розв'язок СР (2.1) з ймовірністю помилки не більше ніж $\delta \in (0, 1)$ (відносно сумісного розподілу матриці A та вектора ξ), якщо число m рівнянь у системі є не менше ніж m_2, що визначається за формулою (2.16).

Як видно з твердження 2.1 при фіксованих q і n ймовірність правильного розв'язання задачі LPN за допомогою ММП експоненційно швидко прямує до 1 з ростом числа m рівнянь у системі. За умови фіксованого числа рівнянь зазначена ймовірність експоненційно зростає із збільшенням параметра $D^2 = \left(D(\overline{p} \,||\, \overline{\omega}) + D(\overline{\omega} \,||\, \overline{p})\right)^2$, який характеризує статистичну відмінність між розподілом спотворень у правих частинах системи (2.1) та рівномірним розподілом ймовірностей на кільці R.

Проілюструємо отримані результати на важливому окремому випадку задачі LPN, коли розподіл ймовірностей $p_\xi = (p(z) : z \in R)$ визначається за законом

$$p(0) = q^{-1}(1 + (q-1)\varepsilon),\ p(z) = q^{-1}(1 - \varepsilon),\ z \neq 0, \quad (2.23)$$

де $\varepsilon \in (0,1)$. Зауважимо, що такий варіант задачі (при $R = \mathbf{GF}(q)$) розглядається в [11] при побудові кореляційних атак на словоорієнтовані потокові шифри.

На підставі формул (2.5), (2.6), (2.14), (2.15) і (2.23), справедливі такі рівності:

$$D(p \,||\, \omega) = q^{-1}(1+(q-1)\varepsilon)\log(1+(q-1)\varepsilon) + q^{-1}(q-1)(1-\varepsilon)\log(1-\varepsilon), \qquad (2.24)$$

$$D(\omega \,||\, p) = -q^{-1}(\log(1+(q-1)\varepsilon) + (q-1)\log(1-\varepsilon)), \qquad (2.25)$$

$$D_a = q^{-1}\left((1+(q-1)\varepsilon)\log^2(1+(q-1)\varepsilon) + (q-1)(1-\varepsilon)\log^2(1-\varepsilon)\right) - D(p \,||\, \omega)^2, \qquad (2.26)$$

$$D_x = q^{-1}\left(\log^2(1+(q-1)\varepsilon) + (q-1)\log^2(1-\varepsilon)\right) - D(\omega \,||\, p)^2, \; x \neq a. \qquad (2.27)$$

На рисунках 2.1 – 2.4 показані залежності оцінок (2.13) і (2.16) від параметра ε, отримані для деяких значень n, q і $\delta \in (0, 1/2)$, де останній параметр позначає верхню межу ймовірності помилки при розв'язанні СР (2.1) за допомогою ММП. Для порівняння показані також значення нижньої оцінки найменшого числа рівнянь у системі (2.1), для якого існує алгоритм її розв'язання з ймовірністю помилки не більше ніж $\delta \in (0, 1/2)$ [4]:

$$m_0 = \frac{n(1-\delta)\log q - h(\delta)}{\Delta(p_\xi)} \ln 2, \qquad (2.28)$$

де $h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$, $\Delta(p_\xi) = q^{-1}\sum_{z \in R}(qp(z)-1)^2$.

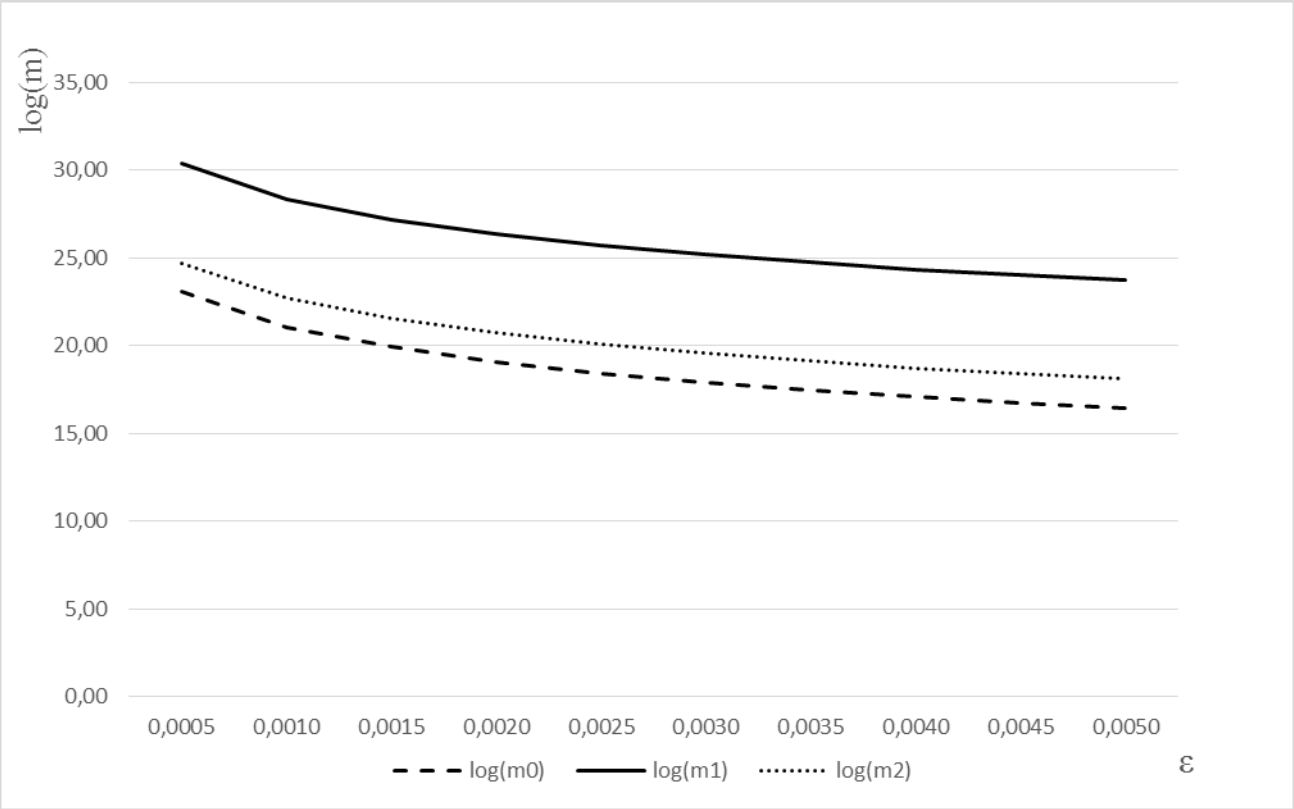

Рисунок 2.1. Залежності оцінок обсягу матеріалу в задачі LPN від розподілу спотворень у правих частинах рівнянь при $\delta = 0{,}01$, $n = 20$, $q = 2^5$

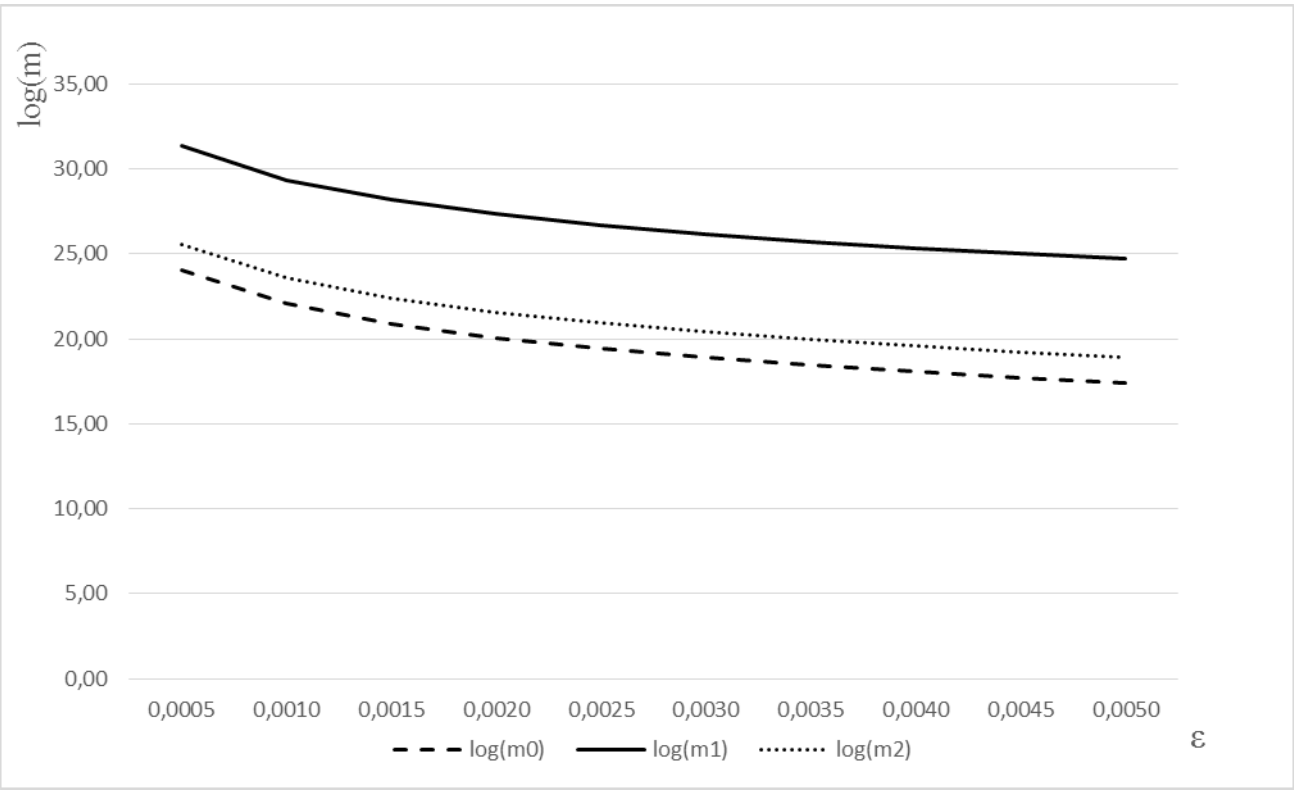

Рисунок 2.2. Залежності оцінок обсягу матеріалу в задачі LPN від розподілу спотворень у правих частинах рівнянь при $\delta = 0{,}01$, $n = 40$, $q = 2^5$

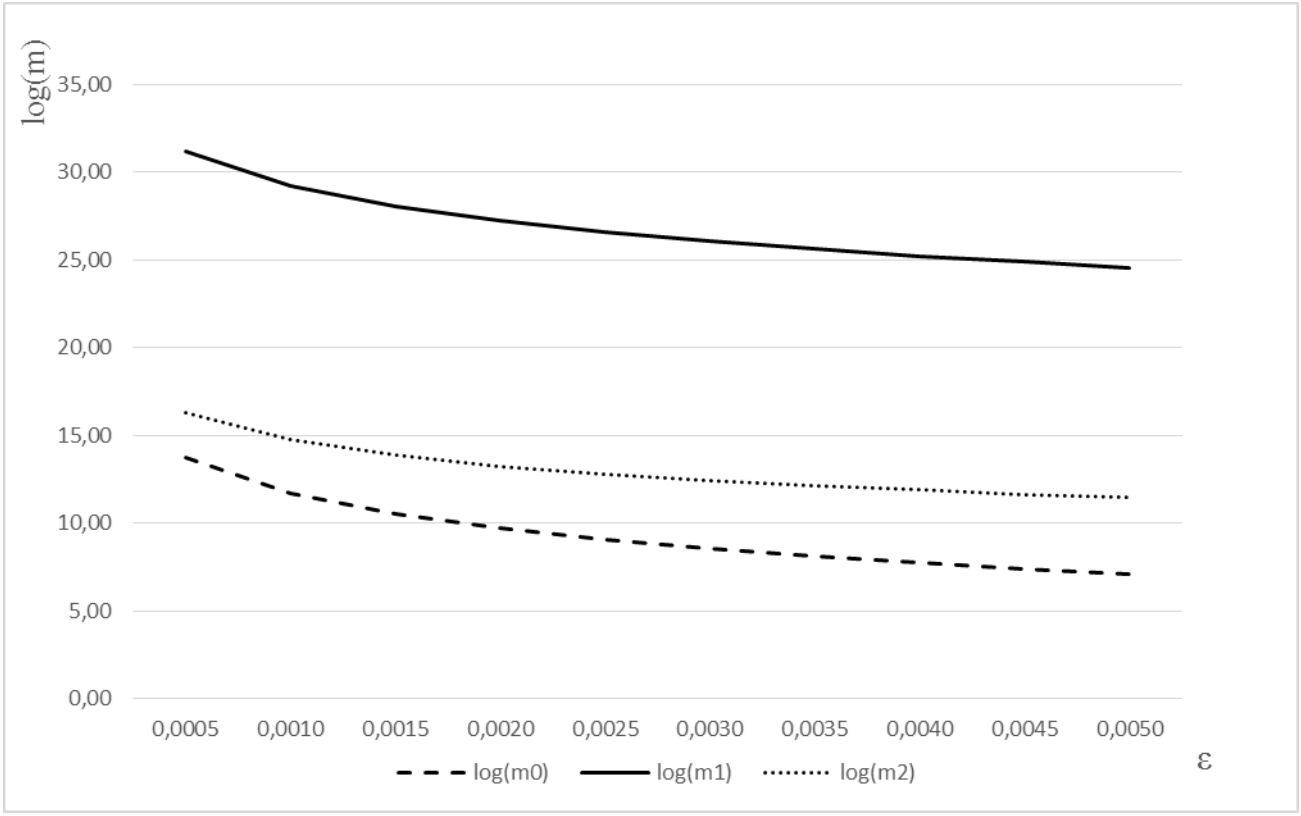

Рисунок 2.3. Залежності оцінок обсягу матеріалу в задачі LPN від розподілу спотворень у правих частинах рівнянь при $\delta = 0{,}01$, $n = 20$, $q = 2^{16}$

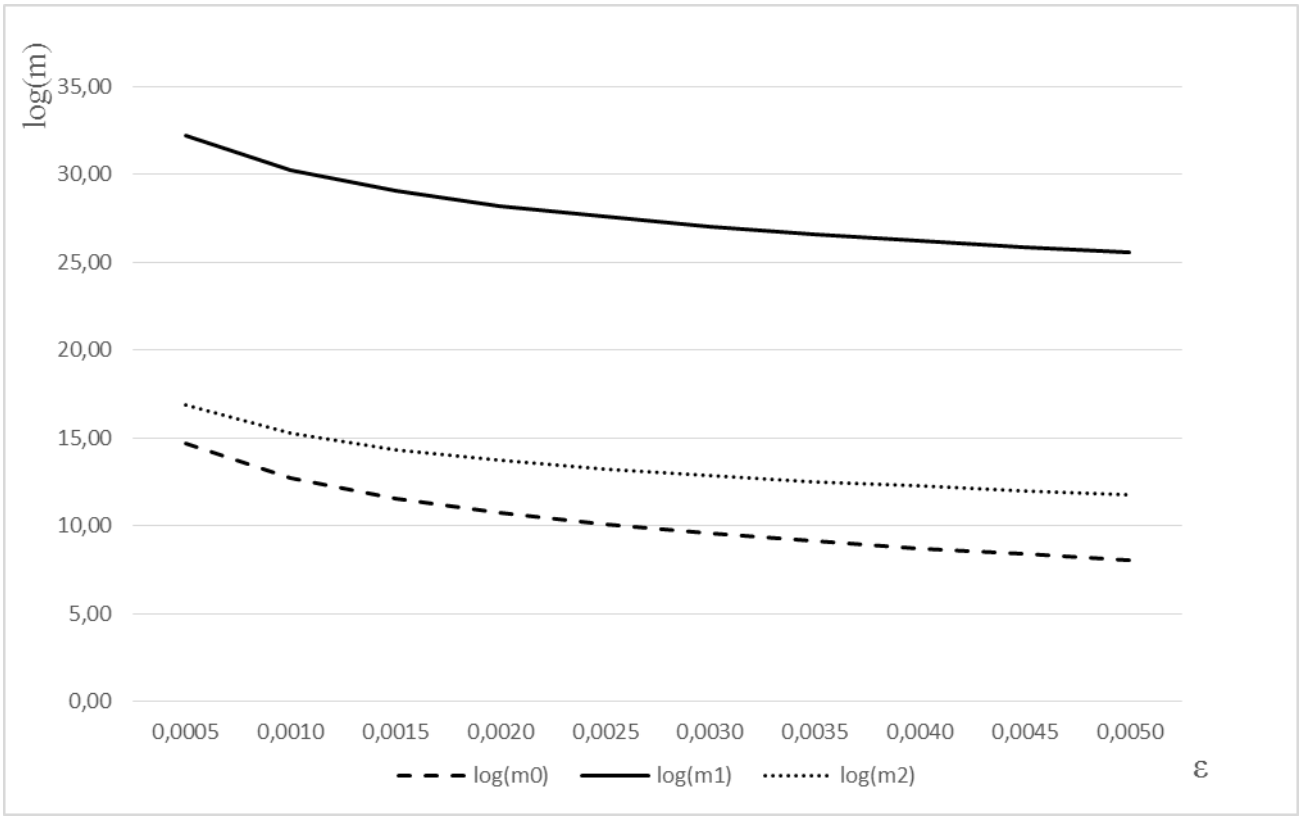

Рисунок 2.4. Залежності оцінок обсягу матеріалу в задачі LPN від розподілу спотворень у правих частинах рівнянь при $\delta = 0{,}01$, $n = 40$, $q = 2^{16}$

Як видно з рисунку 2.1, при $n = 20$, $q = 2^5$ верхня оцінка m_1 набуває значень від $2^{23,71}$ до $2^{30,36}$ в залежності від параметра ε. При цьому значення іншої оцінки m_2 є приблизно в 50 разів менше в усьому зазначеному діапазоні зміни ε та перевищують значення нижньої оцінки m_0 не більше ніж у 3,18 разів. Зі збільшенням числа n (рисунок 2.2) значення усіх трьох оцінок збільшуються приблизно на однакову величину, що дорівнює 1,93. Аналогічний характер залежності спостерігається зі збільшенням параметра q при тих самих n і δ (рисунки 2.3, 2.4), проте в цьому випадку різниця $m_2 - m_0$ є більшою в порівнянні з попереднім випадком. Зокрема, при $\delta = 0{,}01$, $n = 40$, $q = 2^{16}$ і $\varepsilon = 0{,}0025$ для розв'язання СР (2.1) з ймовірністю не менше ніж $1 - \delta$ достатньо 9675 та необхідно не менше ніж 1075 рівнянь зі спотвореними правими частинами.

Таким чином, отримані аналітичні оцінки надають можливість визначати верхні межі обсягу матеріалу, достатнього для надійного розв'язання задачі LPN над довільним скінченним кільцем.

2.2. Застосування отриманих оцінок до визначення часової складності узагальненого алгоритму BKW

У попередньому розділі зазначено, що найефективнішими на сьогодні алгоритмами розв'язання класичної задачі LPN (над полем з двох елементів) є алгоритм BKW [6] та його модифікації [1, 12]. Ці алгоритми мають субекспоненційну часову складність і базуються на розв'язанні задачі про адитивне представлення.

Як показано в [5], алгоритм BKW допускає природне узагальнення на випадок довільного скінченного кільця, проте для визначення часової складності узагальненого алгоритму необхідно мати аналітичні оцінки обсягу

матеріалу, достатнього для розв'язання допоміжних СР зі спотвореними правими частинами над заданим кільцем R.

Нижче показано, як скористатися отриманими оцінками (2.13) і (2.16) для визначення часової складності та оптимізації узагальненого алгоритму BKW.

Перш за все, нагадаємо, що узагальнений алгоритм [5] складається з двох етапів, на першому з яких за вхідною СР (2.1) будується нова система рівнянь зі спотвореними правими частинами від $n_1 < n$ змінних. Потім, на другому етапі отримана система рівнянь розв'язується за допомогою ММП.

Більш точно, узагальнений алгоритм BKW (алгоритм **B**) [5] залежить від натуральних параметрів n_1, l, t, де $1 \le n_1 \le n-3$, $m \ge lt$, та допоміжного алгоритму **A** розв'язання задачі про адитивне представлення з параметрами $n-n_1, k, l$ і за певних умов дозволяє відновлювати перші n_1 координат істинного розв'язку СР (2.1).

Задача про адитивне представлення полягає в знаходженні для вхідного списку L, який складається з l випадкових незалежних та рівноймовірних векторів $z_1, \dots, z_l \in R^{n-n_1}$, k не обов'язково різних чисел $\nu_1, \dots, \nu_k \in \{1, 2, \dots, l\}$ та $\varepsilon_1, \dots, \varepsilon_k \in \{1, -1\}$ таких, що $\varepsilon_1 z_{\nu_1} + \dots + \varepsilon_k z_{\nu_k} = 0$.

Для будь-якого $z \in R^n$ позначимо z' та z'' підвектори вектора z, що складаються з його перших n_1 та останніх $n-n_1$ координат відповідно. Запишемо СР (1) у вигляді $A_i' x' + A_i'' x'' = b_i$, $i = \overline{1,m}$.

Алгоритм **B** має такий вигляд [5].

1. Розіб'ємо систему рядків $A_1'', \dots, A_m''$ на t списків L_j довжини l кожний та застосуємо для кожного $j \in \overline{1,t}$ алгоритм **A** до списку L_j. Якщо хоча б в одному випадку алгоритм **A** завершується неуспішно, то алгоритм **B** припиняє роботу. Інакше отримаємо рівності вигляду

$\varepsilon_1(j)A''_{\nu_1(j)} + \cdots + \varepsilon_k(j)A''_{\nu_k(j)} = 0$, де $A''_{\nu_1(j)},\ldots, A''_{\nu_k(j)} \in L_j$,

$\varepsilon_1(j),\ldots, \varepsilon_k(j) \in \{1, -1\}$, $j \in \overline{1,t}$.

2. Складемо СР зі спотвореними правими частинами

$$A'(j)x' = b(j),\ j \in \overline{1,t}, \tag{2.29}$$

де

$$A'(j) = \varepsilon_1(j)A'_{\nu_1(j)} + \cdots + \varepsilon_k(j)A'_{\nu_k(j)},$$

$$b(j) = \varepsilon_1(j)b_{\nu_1(j)} + \cdots + \varepsilon_k(j)b_{\nu_k(j)} = A'(j)a' + (\varepsilon_1(j)\xi_{\nu_1(j)} + \cdots + \varepsilon_k(j)\xi_{\nu_k(j)}),$$

та розв’яжемо її методом максимуму правдоподібності.

В [5] показано, що часова складність алгоритму **B** визначається за формулою

$$T_{\mathrm{BKW}}(n_1) = 2n_1tq^{n_1} + ult \tag{2.30}$$

де

$$u = \left\lceil \frac{\log(n-n_1)}{2} \right\rceil,\ v = \left\lceil \frac{2(n-n_1)}{\log(n-n_1)} \right\rceil,\ k = 2^{u-1},$$

$$l = (u\ +\ \left\lceil \ln(2t\delta^{-1}) \right\rceil\ -\ 1)q^v,$$

$$m = lt, \tag{2.31}$$

а t позначає кількість рівнянь у системі (2.29), яка є достатньою для відновлення її істинного розв'язку з ймовірністю не менше ніж $1-\delta/2$, де $\delta \in (0, 1/2)$. При цьому розподіл ймовірностей спотворень у правій частині рівнянь системи (2.29) співпадає з розподілом випадкової величини $\xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, де $\xi_1, ..., \xi_k$ є незалежними в сукупності випадковими величинами, розподіленими на кільці R за законом p_ξ.

Таким чином, для визначення часової складності алгоритму **B** слід для кожного $n_1 \in \overline{1, n-3}$ обчислити t за формулою $t = \min\{m_1, m_2\}$, де m_1 і m_2 визначаються за формулами (2.13) і (2.16) відповідно з заміною в них n на n_1, δ на $\delta/2$, а розподілу p_ξ на розподіл $p_\xi^{(k)}$ ймовірностей випадкової величини $\xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, та скористатися рівністю (2.30). Для оптимізації алгоритму **B** слід вибрати таке $n_1 \in \overline{1, n-3}$, що мінімізує значення (2.30).

Як приклад, розглянемо важливий окремий випадок задачі LPN, коли розподіл ймовірностей $p_\xi = (p(z) : z \in R)$ визначається за законом (2.23). В цьому випадку за допомогою індукції по k неважко переконатися в тому, що розподіл ймовірностей $p_\xi^{(k)} = (p^{(k)}(z) : z \in R)$ має такий вигляд:

$$p^{(k)}(0) = q^{-1}(1 + (q-1)\varepsilon^k),\ p^{(k)}(z) = q^{-1}(1 - \varepsilon^k),\ z \neq 0.$$

Отже, згідно з формулами (2.13) і (2.16)

$$t = \min\{m_1, m_2\}, \tag{2.32}$$

де

$$m_1 = \frac{2n_1 \ln(2q\delta^{-1}) \log^2\left(\dfrac{1 + (q-1)\varepsilon^k}{1 - \varepsilon^k}\right)}{(D(p^{(k)} \,\|\, \omega) + D(\omega \,\|\, p^{(k)}))^2}. \tag{2.33}$$

$$m_2 = \left(\frac{u_\alpha \sqrt{D_a} + u_\beta \sqrt{D_x}}{D(p^{(k)} \,||\, \omega) + D(\omega \,||\, p^{(k)})} \right)^2, \qquad (2.34)$$

u_α, u_β – квантилі нормального розподілу, що визначаються за формулами (2.17), $\alpha, \beta > 0$, $\alpha + (q^{n_1} - 1)\beta \le \delta/2$,

$$D(p^{(k)} \,||\, \omega) = q^{-1}(1 + (q-1)\varepsilon^k)\log(1 + (q-1)\varepsilon^k) + q^{-1}(q-1)(1-\varepsilon^k)\log(1-\varepsilon^k), \qquad (2.35)$$

$$D(\omega \,||\, p^{(k)}) = -q^{-1}(\log(1 + (q-1)\varepsilon^k)) + (q-1)\log(1-\varepsilon^k)), \qquad (2.36)$$

$$D_a = q^{-1}((1 + (q-1)\varepsilon^k)\log^2(1 + (q-1)\varepsilon^k) +$$

$$+ (q-1)(1-\varepsilon^k)\log^2(1-\varepsilon^k)) - D(p^{(k)} \,||\, \omega)^2, \qquad (2.37)$$

$$D_x = q^{-1}(\log^2(1 + (q-1)\varepsilon^k) + (q-1)\log^2(1-\varepsilon^k)) - D(\omega \,||\, p^{(k)})^2, \; x \ne a. \qquad (2.38)$$

В табл. 2.1 наведені результати розрахунків часової складності (оптимізованого) узагальненого алгоритму BKW за формулами (2.30) – (2.38) при $q = 2^8$, $\delta = 0{,}01$ для різних значень n і ε. Символом m у таблиці позначена кількість рівнянь у системі (2.1), потрібних для її розв'язання з ймовірністю помилки не вище ніж δ за допомогою узагальненого алгоритму BKW (див. формулу (2.31)).

В табл. 2.2 наведені оцінки часової складності та обсягу матеріалу, достатнього для розв'язання аналогічної СР зі спотвореними правими частинами за допомогою ММП. Отримані результати свідчать про помітну перевагу в трудомісткості узагальненого алгоритму BKW в порівнянні з

методом максимуму правдоподібності. (Зауважимо, що узагальнений алгоритм BKW дозволяє відновити тільки n_1 довільних невідомих СР (2.1), використовуючи час та обсяг даних, зазначені в табл. 2.1.

Таблиця 2.1

Характеристики ефективності розв'язання задачі LPN з використанням узагальненого алгоритму BKW

n	ε	n_1	$\log T_{\mathrm{BKW}}(n_1)$	$\log m$
32	2^{-2}	9	109,46	107,88
32	2^{-3}	9	117,59	116,00
32	2^{-4}	9	125,89	124,31
32	2^{-5}	9	134,12	132,53
32	2^{-6}	9	142,34	140,76
32	2^{-7}	9	150,51	148,93
64	2^{-2}	16	166,02	164,43
64	2^{-3}	16	174,19	172,60
64	2^{-4}	16	182,50	180,92
64	2^{-5}	16	190,76	189,17
64	2^{-6}	16	198,95	197,37
64	2^{-7}	16	207,14	205,56
80	2^{-2}	18	190,18	188,60
80	2^{-3}	18	198,42	196,83
80	2^{-4}	18	206,67	205,08
80	2^{-5}	18	214,93	213,35
80	2^{-6}	18	223,12	221,53
80	2^{-7}	18	231,28	229,70
128	2^{-2}	28	287,64	285,64
128	2^{-3}	28	304,12	302,12
128	2^{-4}	28	320,44	318,44
128	2^{-5}	28	336,71	334,71
128	2^{-6}	28	352,94	350,94
128	2^{-7}	28	369,13	367,13

Таблиця 2.2

Характеристики ефективності розв’язання задачі LPN методом максимуму правдоподібності

n	ε	$\log T(n)$	$\log m_1$	$\log m_2$
32	2^{-2}	268,41	13,35	6,41
32	2^{-3}	270,07	15,35	8,07
32	2^{-4}	271,74	17,35	9,74
32	2^{-5}	273,46	19,36	11,46
32	2^{-6}	275,25	21,36	13,25
32	2^{-7}	277,09	23,35	15,09
64	2^{-2}	525,97	14,36	6,97
64	2^{-3}	527,69	16,35	8,69
64	2^{-4}	529,43	18,36	10,43
64	2^{-5}	531,21	20,36	12,21
64	2^{-6}	533,05	22,36	14,05
64	2^{-7}	534,93	24,35	15,93
80	2^{-2}	654,48	14,68	7,16
80	2^{-3}	656,22	16,68	8,90
80	2^{-4}	657,97	18,68	10,65
80	2^{-5}	659,77	20,68	12,45
80	2^{-6}	661,62	22,67	14,30
80	2^{-7}	663,52	24,68	16,20
128	2^{-2}	1039,55	15,35	7,55
128	2^{-3}	1041,33	17,35	9,33
128	2^{-4}	1043,12	19,36	11,12
128	2^{-5}	1044,95	21,36	12,95
128	2^{-6}	1046,82	23,35	14,82
128	2^{-7}	1048,73	25,36	16,73

Для відновлення усіх n невідомих треба використати зазначений алгоритм $\lceil n/n_1 \rceil$ разів, застосовуючи його до нових вхідних даних, що збільшить в таку ж саму кількість разів значення, логарифми яких наведені в табл. 2.1). Отже, згідно з табл. 2.1, 2.2, виграш у трудомісткості узагальненого алгоритму розв’язання СР (2.1) становить від $2^{124,58}$ до $2^{749,59}$ в залежності від числа n невідомих в системі та параметра ε, який визначає

близькість розподілу спотворень у правій частині СР до рівномірного розподілу ймовірностей на кільці R. Зі зменшенням ε виграш у трудомісткості змінюється від $2^{156,95}$ до $2^{124,58}$ при $n = 32$ та від $2^{749,59}$ до $2^{677,28}$ при $n = 128$.

Висновки

1. Основним науковим результатом розділу є аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем. Зазначені оцінки отримані вперше та узагальнюють аналогічну оцінку, відому для випадку класичної задачі LPN [2].

Перша аналітична оцінка (2.13) встановлює явну залежність потрібного обсягу матеріалу від основних параметрів системи (порядку кільця, числа невідомих та розподілу спотворень у правих частинах рівнянь у системі). Друга, наближена, оцінка (2.16) базується на застосуванні центральної граничної теореми і встановлює вираз обсягу матеріалу в термінах квантилів нормального розподілу ймовірностей.

2. Обсяг матеріалу, достатнього для розв'язання СР (2.1) з достовірністю не менше ніж $1-\delta$, залежить лінійно від числа n невідомих СР, логарифмічно від порядку q кільця R та величини δ^{-1} і збільшується зі зменшенням параметра $D^2 = \left(D(\overline{p} \,||\, \overline{\omega}) + D(\overline{\omega} \,||\, \overline{p})\right)^2$, який характеризує статистичну відмінність між розподілом спотворень у правих частинах системи (2.1) та рівномірним розподілом ймовірностей на кільці R.

При фіксованих q і n ймовірність правильного розв'язання задачі LPN за допомогою ММП експоненційно швидко прямує до 1 з ростом числа рівнянь у системі. За умови фіксованого числа рівнянь зазначена ймовірність експоненційно зростає із збільшенням параметра D^2.

3. Отримані аналітичні оцінки надають можливість визначати за порядком величини фактичний обсяг матеріалу, достатнього для надійного розв'язання задачі LPN над довільним скінченним кільцем. Зокрема, при $\delta = 0{,}01$, $n = 40$, $q = 2^{16}$ і $\varepsilon = 0{,}0025$ (див. формулу (2.23)) для розв'язання СР (2.1) з ймовірністю не менше ніж $1 - \delta$ достатньо 9675 та необхідно не менше ніж 1075 рівнянь зі спотвореними правими частинами.

4. При $n = 20$, $q = 2^5$ за умови (2.23) верхня оцінка m_1 набуває значень від $2^{23{,}71}$ до $2^{30{,}36}$ в залежності від параметра ε. При цьому значення оцінки m_2 є приблизно в 50 разів менше в усьому зазначеному діапазоні зміни ε та перевищують значення відомої нижньої оцінки (2.28) не більше ніж у 3,18 разів. Зі збільшенням числа n значення усіх трьох оцінок збільшуються приблизно на однакову величину, що дорівнює 1,93. Аналогічний характер залежності спостерігається зі збільшенням параметра q при тих самих n і δ (рисунки 2.1 – 2.4).

5. Отримані аналітичні оцінки дозволяють визначити часову складність узагальненого алгоритму BKW [5], відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN. Зокрема, згідно з табл. 2.1, 2.2, виграш у трудомісткості узагальненого алгоритму розв'язання СР (2.1) в порівнянні з ММП становить від $2^{124{,}58}$ до $2^{749{,}59}$ в залежності від числа n невідомих в системі та параметра ε, який визначає близькість розподілу спотворень у правій частині СР до рівномірного розподілу ймовірностей на кільці. Зі зменшенням ε виграш у трудомісткості змінюється від $2^{156{,}95}$ до $2^{124{,}58}$ при $n = 32$ та від $2^{749{,}59}$ до $2^{677{,}28}$ при $n = 128$. Це свідчить про помітну перевагу в трудомісткості узагальненого алгоритму BKW в порівнянні з методом максимуму правдоподібності.

Список використаних джерел у другому розділі

1. Bogos S., Tramer F., Vaudenay S. On solving LPN using BKW and variants. Implementation and analysis. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2015/049 (дата звернення: 06.08.2020).

2. Балакин Г. В. Введение в теорию случайных систем уравнений. *Труды по дискретной математике*. 1997. т. 1. С. 1-18.

3. Hoeffding W. Probability inequalities for sums of bounded random variables. *Journal of American Statistical Association*. 1963. № 58. P. 13-30.

4. Алексейчук А. Н. Неасимптотические нижние границы информационной сложности статистических атак на симметричные криптосистемы. *Кибернетика и системный анализ*. 2018. № 1, т. 54. С. 1-13.

5. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Сер. Технічні науки*. 2017. Вип. 15. С. 150-155.

6. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. 2003. Vol. 50, № 3. P. 506-519.

7. Левитская А. А. Системы случайных уравнений над конечными алгебраическими структурами. *Кибернетика и системный анализ*. 2005. № 1, т. 41. С. 82-116.

8. Чечёта С. И. Введение в дискретную теорию информации и кодирования : учебное издание. М.: МЦНМО, 2011. 224 с.

9. Cateaut A., Naya-Plasencia M. Correlation attacks on combination generators. *Cryptography and Communications*. 2012. Vol. 4, Issue (3-4). P. 147–171.

10. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2016/311 (дата звернення: 06.08.2020).

11. Jönsson F. Some results on fast correlation attacks: PhD Thesis / Land University, Sweden, 2002. 151 p.

12. Олексійчук А. М. Субекспоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. *Прикладная радиоэлектроника*. 2012. т. 11, № 2. С. 3–11.

13. Алексейчук А. Н., Игнатенко С. М. Нижняя граница вероятности восстановления истинного решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2006. № 4, Т. 8. С. 5-12.

14. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2017. Вип. 15. С. 150-155.

15. Игнатенко С. М., Алексейчук А. Н. Оценка надежности метода максимума правдоподобия решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. IX міжнар. наук.-практ. конф. Київ, 2006. С. 29-30.

РОЗДІЛ 3

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗВ'ЯЗАННЯ ЗАДАЧІ LPN НА ОСНОВІ ШВИДКИХ ПЕРЕТВОРЕНЬ ФУР'Є ТА ФЕРМА

Як зазначено вище, метод максимуму правдоподібності характеризується найбільшою достовірністю (найменшою середньою ймовірністю помилки) серед усіх методів розв'язання задачі LPN над довільним скінченним кільцем R. Проте зазначений метод є найбільш трудомістким, оскільки потребує перебору всіх векторів довжини n над кільцем R. Відомо, що у випадку, коли R є полем порядку 2^N, трудомісткість ММП можна зменшити, використовуючи алгоритми швидкого перетворення Фур'є (див., наприклад, [1, 2]). Поряд з тим, питання про те, наскільки широким є клас скінченних кілець із зазначеною властивістю є на сьогодні відкритим.

В даному розділі показано, що таким є клас скінченних фробеніусових кілець. Цей клас є дуже потужним і включає в себе, зокрема, будь-які кільця головних (лівих чи правих) ідеалів [3]. Розроблено два методи підвищення ефективності розв'язання задачі LPN за допомогою ММП. Перший метод є застосовним для довільного скінченного фробеніусова кільця R та базується на використанні швидкого перетворення Фур'є допоміжних функцій, що визначаються на цьому кільці. Другий метод є застосовним до задачі LPN над кільцем лишків за модулем 2^N і базується на використанні числового перетворення Ферма (яке можна розглядати як спеціальний окремий випадок дискретного перетворення Фур'є [4]).

Показано, що за певних умов розроблені методи дозволяють помітно зменшити часову складність розв'язання задачі LPN як за допомогою самого

ММП, так і інших алгоритмів (узагальненого алгоритму BKW [5]), що використовують ММП як допоміжну процедуру.

3.1. Метод підвищення ефективності розв'язання задачі LPN над скінченним фробеніусовим кільцем за допомогою швидкого перетворення Фур'є

Нехай R – скінченне кільце порядку q. Нагадаємо, що (адитивним комплексним) характером кільця R називається гомоморфізм його адитивної групи в мультиплікативну групу поля $\mathbf{C}$ комплексних чисел. Характери кільця R утворюють мультиплікативну групу $\hat{R}$, ізоморфну групі $(R,+)$; при цьому зазначений ізоморфізм $a \mapsto \chi_a$, $a \in R$ можна задати таким чином, щоби для будь-яких $a, x \in R$ виконувалась рівність $\chi_a(x) = \chi_x(a)$ [6].

Перетворенням Фур'є функції $f : R^n \to \mathbf{C}$ називається функція $\hat{f}(a) = \sum_{x \in R^n} f(x)\overline{\chi_a(x)}$, $a \in R^n$, де χ_a – характер групи $(R^n,+)$, що відповідає елементу a при заданому ізоморфізмі цієї групи в групу $\hat{R}^n$, $\overline{\chi_a(x)}$ – число, комплексно спряжене до $\chi_a(x)$. Функція f відновлюється за її перетворенням Фур'є за формулою $f(x) = q^{-1} \sum_{a \in R^n} \hat{f}(a)\chi_a(x)$, $x \in R^n$ (див., наприклад, [3]).

Кільце R називається фробеніусовим, якщо існує його утворюючий справа характер, тобто такий елемент $\chi \in \hat{R}$, що $\hat{R} = \{r\chi : r \in R\}$. Кожен утворюючий справа характер кільця R є також утворюючим зліва, тобто задовольняє умові $\hat{R} = \{\chi r : r \in R\}$, і в подальшому називається просто утворюючим характером (фробеніусова) кільця R [3].

Наведемо найважливіші, з практичного погляду, приклади фробеніусових кілець [3].

1. Скінченне поле $R = \mathbf{GF}(q)$, де $q = p^r$, p – просте число, є фробеніусовим кільцем. При цьому утворюючим є характер $\chi(x) = \omega^{\mathrm{Tr}(x)}$, $x \in R$, де ω – примітивний корінь степеня p з одиниці, $\mathrm{Tr}(x) = x \oplus x^p \oplus \cdots \oplus x^{p^{r-1}}$, $x \in R$.

2. Кільце лишків $R = \mathbf{Z}/(q)$ є фробеніусовим кільцем з утворюючим характером $\chi(x) = \omega^x$, $x \in R$, де $\omega = \exp\{-2\pi i q^{-1}\}$, $i^2 = -1$.

3. Будь-яке скінченне кільце головних (лівих чи правих) ідеалів є фробеніусовим кільцем.

4. Пряма сума кілець $R_1,...,R_n$ є фробеніусовим кільцем тоді й тільки тоді, коли кожне кільце R_i, $i \in \overline{1,n}$, є фробеніусовим. Якщо при цьому χ_i є утворюючим характером кільця R_i, то $\chi(x_1,...,x_n) = \chi_1(x_1) \cdots \chi_n(x_n)$, $x_i \in R_i$, $i \in \overline{1,n}$, є утворюючим характером кільця $R = R_1 \oplus \cdots \oplus R_n$.

5. Кільце матриць $R_{n\times n}$ над фробеніусовим кільцем R є фробеніусовим. При цьому для будь-якого утворюючого характера χ кільця R відображення $\widetilde{\chi}(X) = \chi(\mathrm{tr}(X))$, де $\mathrm{tr}(X)$ – сума діагональних елементів матриці $X \in R_{n\times n}$, є утворюючим характером кільця $R_{n\times n}$.

Наступна лема, доведення якої випливає безпосередньо з наведених означень, надає опис усіх характерів абелевої групи $(R^n, +)$ для фробеніусова кільця R.

Лема 3.1. Нехай R є фробеніусовим кільцем характеристики l з утворюючим характером χ. Тоді $\chi(x) = \omega^{G(x)}$, $x \in R$, де ω – примітивний корінь степеня l з одиниці, $G : R \to \mathbf{Z}/(l)$ – гомоморфізм абелевих груп, ядро якого не містить ненульових правих (лівих) ідеалів кільця R. При цьому всі

різні характери абелевої групи $(R^n,+)$ мають вигляд $\chi_a(x)=\chi(ax)$, $x\in R^n$, де $a\in R^n$, ax – скалярний добуток векторів a та x над кільцем R.

Розглянемо зараз СР (2.1) над фробеніусовим кільцем R та покажемо, як скористатися швидким перетворенням Фур'є для обчислення усіх значень $n(z\,|\,\varepsilon(x))$ у виразі (2.3).

Твердження 3.1. Нехай R – фробеніусове кільце порядку q з утворюючим характером χ, $A\in R_{m\times n}$, $b\in R^m$. Тоді для кожного $z\in R$ частота зустрічальності $n(z\,|\,\varepsilon(x))$ елемента z у векторі $\varepsilon(x)=b-Ax$ задовольняє рівності

$$n(z\,|\,\varepsilon(x))=q^{-1}(\hat{g}_z(x)+m),\ x\in R^n, \tag{3.1}$$

де

$$g_z(y)=\sum_{\substack{(r\in R\setminus\{0\},\,j\in\overline{1,m}):\\ rA_j=y}}\chi(r(b_j-z)),\ y\in R^n. \tag{3.2}$$

Доведення. На підставі означення перетворення Фур'є функції (3.2) та леми 3.1 справедливі рівності

$$\hat{g}_z(x)=\sum_{y\in R^n}g_z(y)\overline{\chi_y(x)}=\sum_{y\in R^n}\ \sum_{\substack{(r\in R\setminus\{0\},\,j\in\overline{1,m}):\\ rA_j=y}}\chi(r(b_j-z))\chi(-yx)=$$

$$=\sum_{(r\in R\setminus\{0\},\,j\in\overline{1,m})}\chi(r(b_j-z))\chi(-rA_jx)=\sum_{(r\in R\setminus\{0\},\,j\in\overline{1,m})}\chi(r(b_j-z-A_jx))=$$

$$=\sum_{j\in\overline{1,m}}\ \sum_{r\in R\setminus\{0\}}\chi(r(b_j-z-A_jx))=\sum_{j\in\overline{1,m}}(q\delta(z,b_j-A_jx)-1)=qn(z\,|\,\varepsilon(x))-m,$$

де передостання рівність випливає зі співвідношення ортогональності для характерів: $\sum_{r\in R}\chi(ru)=q\delta(u,0)$, δ є символом Кронекера (див., наприклад, [6]).

Отже, справедлива формула (3.1). Твердження доведено.

Таким чином, на підставі отриманого твердження при розв'язанні СР (2.1) над фробеніусовим кільцем R за допомогою ММП достатньо обчислити для кожного $z\in R$ перетворення Фур'є функції (3.2) та знайти (шляхом повного перебору) точку максимуму функції (2.3).

Покажемо, як скористатися для обчислення усіх значень (3.1) швидким алгоритмом, наведеним в додатку А.1.

Перш за все, сформулюємо наступну лему, доведення якої міститься в додатку А.2.

Лема 3.2. Суму t невід'ємних цілих чисел, кожне з яких не перевищує M, можна обчислити, використовуючи не більше ніж $5(t-1)(\log tM+2)$ двійкових операцій.

Розглянемо матрицю $H_1=(\omega^{-G(yx)})_{x,y\in R}$, де $G:R\to\mathbf{Z}/(l)$ – гомоморфізм, зазначений у формулюванні леми 3.1.

Твердження 3.2. За умови твердження 3.1 двійкова часова складність обчислення всіх значень (3.1) не перевищує

$$T_q(n)=5T_q(1)q^n nl(\log(T_q(1)q^n nm)+2)+q(q-1)m((n+1)C_\times+C_++C_G), \quad (3.3)$$

де $T_q(1)$ – число арифметичних операцій в полі $\mathbf{C}$, що використовуються для множення векторів довжини q на матрицю H_1, l – характеристика кільця R, C_+, $C_\times$ і C_G – двійкові складності операцій додавання, множення елементів кільця R та обчислення значення гомоморфізму G відповідно.

Доведення. З наведених означень випливає, що обчислення перетворення Фур'є функції (3.2) рівносильно множенню вектора її значень

на матрицю $H_n = (\chi(-yx))_{x,y \in R^n}$, яка є n-м тензорним степенем матриці H_1. Отже, перетворення Фур'є функції (3.2) можна обчислити за допомогою алгоритму A_n зі складністю

$$T'_q(n) = T_q(1) q^{n-1} n \tag{3.4}$$

операцій додавання комплексних чисел та їх множення на степені елемента ω, причому число $T_q(1)$ дорівнює складності множення векторів довжини q на матрицю H_1 (див. підрозділ А.1).

Далі, елементи матриці H_n як і значення кожної функції (3.2) є многочленами від ω з цілими коефіцієнтами, тобто належать кільцю $\mathbf{Z}[\omega]$. Отже, обчислення можна проводити в цьому кільці. Кожен елемент кільця має (не обов'язково однозначне) представлення у вигляді $\sum_{i=0}^{l-1} c_i \omega^i$, де $c_i \in \mathbf{Z}$. Додавання двох таких елементів зводиться до додавання цілочисельних векторів довжини l, а множення такого елемента на елемент ω^k – до циклічного зсуву вектора $(c_0,...,c_{l-1})$ праворуч на k позицій. Крім того, величина коефіцієнтів c_i, $i \in \overline{0, l-1}$, у представленнях значень функції (3.2) як елементів кільця $\mathbf{Z}[\omega]$ не перевищує числа доданків у виразі, який визначає цю функцію, тобто $m(q-1)$. Звідси на підставі леми 3.2 випливає, що двійкова часова складність обчислення перетворення Фур'є кожної окремої функції (3.2) не перевищує $5T'_q(n) l(\log(T'_q(n) m(q-1)) + 2)$, де $T'_q(n)$ є складністю обчислення перетворення Фур'є цієї функції в операціях над полем $\mathbf{C}$ (див., формулу (3.4)). Отже, двійкова складність обчислення перетворень Фур'є усіх q функцій (3.2) не перевищує

$$T_1 = 5T'_q(n) q l(\log(T'_q(n) mq) + 2). \tag{3.5}$$

Далі, для визначення кожної функції (3.2) як елемента кільця $\mathbf{Z}[\omega]$ треба виконати не більше ніж $m(q-1)(n+1)$ операцій множення, $m(q-1)$ операцій додавання елементів кільця R та $m(q-1)$ операцій звернення до гомоморфізму G. Отже, двійкова складність визначення усіх функцій (3.2) не перевищує

$$T_2 = q(q-1)l((n+1)C_{\times} + C_{+} + C_G). \tag{3.6}$$

Підсумовуючи вирази (3.5) і (3.6), отримаємо формулу (3.3). Твердження доведено.

На рисунку 3.1 наведено докладний опис алгоритму, про який йдеться у доведенні твердження 3.2. Алгоритм складається з двох етапів, на першому з яких обчислюється вектор значень функції (3.2). Потім, на другому етапі здійснюється множення цього вектора на матрицю H_n за допомогою алгоритму A_n, описаного в підрозділі А.1. Значення функцій (3.2) зберігаються у двовимірному масиві, рядки якого занумеровані (розташованими в лексикографічному порядку) векторами $y \in R^n$, а стовпці – числами $0, 1, \ldots, l-1$; при цьому значення $g_z(y)$ ототожнюється з набором $(g_z[y,0], \ldots, g_z[y,l-1])$ коефіцієнтів многочлена $\sum_{i=0}^{l-1} g_z[y,i]\omega^i$, який представляє це значення в кільці $\mathbf{Z}[\omega]$. Зауважимо, при практичній реалізації алгоритму 3.1 в результаті обчислень, виконаних в кільці $\mathbf{Z}[\omega]$, кожне значення $\hat{g}_z(x)$, $x \in R^n$, також буде отримано у вигляді певного многочлена від ω: $\hat{g}_z(x) = \sum_{i=0}^{l-1} c_i(x)\omega^i$, де $c_i(x) \in \mathbf{Z}$, $i \in \overline{0,l-1}$, і на підставі формули (3.1) для знаходження частоти $n(z \mid \varepsilon(x))$ достатньо обчислити значення $\sum_{i=0}^{l-1} c_i(x)\,\mathrm{Re}(\omega^i)$. Це є єдиним випадком, коли доведеться мати справу з

числами з плаваючою комою, що, однак, не призведе до втрати точності обчислень, якщо заздалегідь визначити значення $\mathrm{Re}(\omega^i)$, $i \in \overline{0,l-1}$, з потрібною точністю.

Вхідні дані:

– фробеніусове кільце R порядку q і характеристики l з утворюючим характером $\omega^{G(x)}$, $x \in R$;

– $m \times n$-матриця A над кільцем R;

– вектор $b \in R^m$.

Результат: набір чисел $(qn(z \mid \varepsilon(x)) - m : z \in R,\ x \in R^n)$.

Алгоритм обчислень.

Для кожного $z \in R$:

1. Обчислити усі значення функції (3.2) таким чином:

   1.1. Для будь-яких $y \in R^n$, $i \in \overline{0,l-1}$ покласти $g_z[y,i] = 0$.

   1.2. Для будь-яких $r \in R \setminus \{0\}$, $j \in \overline{1,m}$ покласти

$$g_z[rA_j, G(r(b_j - z))] = g_z[rA_j, G(r(b_j - z))] + 1.$$

2. Обчислити перетворення Фур'є $\hat{g}_z(x)$, $x \in R^n$ побудованої функції (3.2) за допомогою алгоритму A_n (див. підрозділ А.1) та покласти

$$qn(z \mid \varepsilon(x)) - m = \hat{g}_z(x),\ x \in R^n.$$

Рисунок 3.1. Алгоритм обчислення значень (3.1) з використанням швидкого перетворення Фур'є

Як приклад, що ілюструє отримані результати, розглянемо задачу LPN над кільцем $R_N = \mathbf{Z}/(2^N)$. Тоді $q = l = 2^N$, $G(x) = x$ для кожного $x \in R_N$. Крім того, $C_+ = 5(N-1)$, $C_\times = N(6N-5)$ (див. твердження А.2),

$T_q(1) = (2N-1)2^N + 1$ [4] і на підставі твердження 3.2 двійкова часова складність знаходження істинного розв'язку СР (2.1) за допомогою швидкого перетворення Фур'є не перевищує

$$T_{2^N}(n) = 5 \cdot 2^{(n+2)N+1} Nn \log(2^{N+1} Nnm) +$$

$$+ 2^{2N} m((n+1)N(6N-5) + 5(N-1)).$$

В той же час, двійкова складність знаходження цього розв'язку за допомогою звичайного алгоритму (див. підрозділ 2.1) дорівнює $T = nm2^{Nn}(6N^2 - N)$.

В табл. 3.1 для низки значень n, N і m наведені значення двійкового логарифму виграшу $\tau = \log(T \cdot T_{2^N}(n)^{-1})$ в часовій складності, який отримується в результаті застосування швидкого перетворення Фур'є.

Таблиця 3.1

Чисельні значення логарифму виграшу у часовій складності при розв'язанні задачі LPN над кільцем $\mathbf{Z}/(2^N)$ за допомогою швидкого перетворення Фур'є

(n, N) $\log m$	20	25	30	35	40	45	50	55
(20, 4)	8,23	13,02	17,83	22,67	27,52	32,39	37,26	42,15
(30, 4)	8,21	13,00	17,81	22,65	27,50	32,37	37,25	42,14
(40, 4)	8,19	12,98	17,80	22,64	27,49	32,36	37,24	42,13
(60, 4)	8,16	12,96	17,78	22,62	27,48	32,35	37,23	42,12
(20, 8)	1,05	5,86	10,70	15,55	20,42	25,29	30,18	35,08
(30, 8)	1,03	5,84	10,68	15,54	20,40	25,28	30,17	35,07
(40, 8)	1,01	5,83	10,67	15,52	20,39	25,27	30,16	35,06
(60, 8)	0,99	5,81	10,65	15,51	20,38	25,26	30,15	35,05
(80, 8)	0,97	5,80	10,64	15,50	20,37	25,25	30,14	35,04

Як видно з таблиці, при фіксованому N значення виграшу практично не залежить від числа невідомих та швидко зростає з ростом числа m рівнянь у

системі (2.1). Зокрема, при $m \geq 2^{25}$ виграш в трудомісткості складає від $2^{5,80}$ до $2^{42,15}$ разів в залежності від значень параметрів N і m.

3.2. Метод підвищення ефективності розв'язання задачі LPN над кільцем лишків за модулем 2^N за допомогою швидкого перетворення Ферма

Викладений вище метод, що базується на використанні алгоритмів швидкого перетворення Фур'є, є застосовним до розв'язання задачі LPN над довільним скінченним фробеніусовим кільцем. У важливому окремому випадку кільця лишків за модулем 2^N можна використовувати інше перетворення, яке має назву числового перетворення Ферма.

Позначимо $R_N = \mathbf{Z}/(2^N)$, $\Re_N = \mathbf{Z}/(2^{2^{N-1}}+1)$. За означенням [4], с. 196, перетворення Ферма $\hat{f}$ довільної функції $f : {R_N}^n \to \Re_N$ визначається за формулою

$$\hat{f}(x) = (\sum_{y \in {R_N}^n} 2^{-xy} f(y)) \bmod(2^{2^{N-1}}+1),$$

де xy означає скалярний добуток векторів x та y над кільцем R_N. Позначимо $\chi(x) = 2^x \bmod(2^{2^{N-1}}+1)$, $x \in R_N$. Функція χ є гомоморфізмом адитивної групи кільця R_N в мультиплікативну групу кільця $\Re_N$. При цьому, оскільки порядок елемента 2 в останній групі дорівнює 2^N, то справедливі такі співвідношення ортогональності:

$$\sum_{r \in R_N} \chi(ru) \equiv 2^N \delta(u, 0) \bmod(2^{2^{N-1}}+1),\ u \in R_N, \qquad (3.7)$$

де δ є символом Кронекера [7], с. 662.

Наступне твердження показує як скористатися числовим перетворенням Ферма для обчислення усіх значень $n(z \mid \varepsilon(x))$ у виразі (2.3).

Твердження 3.3. Припустимо, що число рівнянь у системі (2.1) над кільцем R_N задовольняє умові $m \le 2^{2^{N-1}}$. Тоді для кожного $z \in R_N$ частота зустрічальності $n(z \mid \varepsilon(x))$ елемента z у векторі $\varepsilon(x) = b - Ax$ дорівнює

$$n(z \mid \varepsilon(x)) = 2^{2^N - N}(\hat{g}_z(x) + m) \bmod(2^{2^{N-1}} + 1),\ x \in {R_N}^n, \tag{3.8}$$

де

$$g_z(y) = \sum_{\substack{(r \in R_N \setminus \{0\},\, j \in \overline{1,m}): \\ rA_j = y}} \chi(r(b_j - z)) \bmod(2^{2^{N-1}} + 1),\ y \in {R_N}^n. \tag{3.9}$$

Доведення. На підставі означення перетворення Ферма функції (3.9) справедливі такі порівняння:

$$\hat{g}_z(x) \equiv \sum_{y \in {R_N}^n} g_z(y)\chi(-xy) \equiv \sum_{y \in {R_N}^n} \sum_{\substack{(r \in R_N \setminus \{0\},\, j \in \overline{1,m}): \\ rA_j = y}} \chi(r(b_j - z))\chi(-xy) \equiv$$

$$\equiv \sum_{(r \in R_N \setminus \{0\},\, j \in \overline{1,m})} \chi(r(b_j - z))\chi(-rA_j x) \equiv \sum_{(r \in R_N \setminus \{0\},\, j \in \overline{1,m})} \chi(r(b_j - z - A_j x)) \equiv$$

$$\equiv \sum_{j \in \overline{1,m}} \sum_{r \in R_N \setminus \{0\}} \chi(r(b_j - z - A_j x)) \equiv \sum_{j \in \overline{1,m}} (2^N \delta(z, b_j - A_j x) - 1) \equiv$$

$$\equiv (2^N n(z \mid \varepsilon(x)) - m) \bmod(2^{2^{N-1}} + 1),$$

де передостаннє порівняння випливає з формули (3.7). Отже,

$$n(z \mid \varepsilon(x)) \equiv 2^{2^N - N}(\hat{g}_z(x) + m) \bmod (2^{2^{N-1}} + 1).$$

Оскільки за умови твердження $n(z \mid \varepsilon(x)) \le m < 2^{2^{N-1}} + 1$ для будь-яких $z \in R_N$, $x \in {R_N}^n$, то $n(z \mid \varepsilon(x)) \bmod (2^{2^{N-1}} + 1) = n(z \mid \varepsilon(x))$. Звідси випливає формула (3.8).

Твердження доведено.

Таким чином, за умови отриманого твердження при розв'язанні СР (2.1) над кільцем R_N за допомогою ММП достатньо обчислити для кожного $z \in R_N$ перетворення Ферма функції (3.9) та знайти (шляхом повного перебору) точку максимуму функції (2.3).

Для обчислення перетворення Ферма функції (3.9) можна скористатися швидким алгоритмом, наведеним в підрозділі А.1, вважаючи при цьому $\Re = \Re_N$, $H = (h_{ij})_{i,j \in R_N}$, де $h_{ij} = 2^{-ij} \bmod (2^{2^{N-1}} + 1)$, $i, j \in R_N$ та використовуючи в ролі допоміжного алгоритму A алгоритм швидкого перетворення Ферма, наведений в [4], с. 197. Зауважимо, що часова складність останнього алгоритму складає

$$T_N(1) = (2N - 1)2^N + 1 \qquad (3.10)$$

операцій додавання та зсуву (множення на степені числа 2) в кільці $\Re_N$.

На рисунку 3.2 наведено опис алгоритму обчислення усіх значень (3.1) за допомогою швидкого перетворення Ферма. Наступне твердження дозволяє оцінити часову складність цього алгоритму.

Твердження 3.4. За умови твердження 3.3 двійкова часова складність обчислення всіх значень (3.1) не перевищує

$$\widetilde{T}_{2^N}(n) = 26 \cdot 2^{N(n+1)} Nn + 2^{2N} m((n+1)N(6N-5) + 5(N-1) + 7 \cdot 2^{N-1} + 2) \quad (3.11)$$

Вхідні дані:

– натуральне число $N \geq 2$;

– $m \times n$-матриця A над кільцем R_N, де $m \leq 2^{2^{N-1}}$;

– вектор $b \in {R_N}^m$.

Результат: набір чисел $(n(z \mid \varepsilon(x)) : z \in R_N,\ x \in {R_N}^n)$.

Алгоритм обчислень.

Для кожного $z \in R_N$:

1. Обчислити усі значення функції (3.9) таким чином:

1.1. Для будь-якого $y \in {R_N}^n$ покласти $g_z(y) = 0$.

1.2. Для будь-яких $r \in R_N \setminus \{0\}$, $j \in \overline{1,m}$ покласти

$$g_z(rA_j) = (g_z(rA_j) + 2^{r(b_j - z)}) \bmod (2^{2^{N-1}} + 1).$$

2. Обчислити перетворення Ферма $\hat{g}_z(x)$, $x \in {R_N}^n$ побудованої функції (3.9) за допомогою алгоритму A_n (див. підрозділ А.1) та покласти

$$n(z \mid \varepsilon(x)) = 2^{2^N - N}(\hat{g}_z(x) + m) \bmod (2^{2^{N-1}} + 1),\ x \in {R_N}^n.$$

Рисунок 3.2. Алгоритм обчислення значень (3.1) з використанням швидкого перетворення Ферма

Доведення. Для визначення кожної функції (3.9) на кроці 2.2 наведеного вище алгоритму треба виконати не більше ніж $2^N m(n+1)$ операцій множення, $2^N m$ операцій додавання елементів кільця R_N та $2^N m$ операцій

додавання в кільці $\Re_N$. Отже, двійкова складність визначення усіх функцій (3.9) не перевищує

$$T' = 2^{2N} m((n+1)C_{\times}(R_N) + C_{+}(R_N) + C_{+}(\Re_N)), \qquad (3.12)$$

де $C_{\times}(R_N)$ та $C_{+}(R_N)$ є відповідно двійкові складності операцій множення та додавання в кільці R_N, $C_{+}(\Re_N)$ – двійкова складність операції додавання в кільці $\Re_N$.

Далі, на підставі твердження А.1 перетворення Ферма функції (3.9) можна обчислити за допомогою алгоритму A_n, використовуючи не більше ніж $T_N(1)2^{N(n-1)}n$ операцій додавання та зсуву в кільці $\Re_N$, де число $T_N(1)$ визначається за формулою (3.10). Отже двійкова часова складність обчислення усіх значень $\hat{g}_z(x)$, $x \in {R_N}^n$, $z \in R_N$, на кроці 3 алгоритму не перевищує

$$T'' = ((2N-1)2^N + 1)2^{N(n-1)+1} n \max\{C_{+}(\Re_N), C_{>>}(\Re_N)\}, \qquad (3.13)$$

де $C_{+}(\Re_N)$ та $C_{>>}(\Re_N)$ є відповідно двійкові складності операцій додавання та зсуву в кільці $\Re_N$.

Підсумовуючи вирази (3.12), (3.13) та використовуючи формули (див. твердження А.2 та А.4)

$$C_{+}(R_N) = 5(N-1),\ C_{\times}(R_N) = N(6N-5),$$

$$C_{+}(\Re_N) = 7 \cdot 2^{N-1} + 2\ \ C_{>>}(\Re_N) = 13 \cdot 2^{N-1},$$

отримаємо рівність (3.11). Твердження доведено.

В табл. 3.2 для низки значень n, N і m наведені значення двійкового логарифму виграшу $\tau = \log(T \cdot \widetilde{T}_{2^N}(n)^{-1})$ в часовій складності, який отримується в результаті застосування швидкого перетворення Ферма при розв'язанні СР (2.1) в порівнянні зі звичайним алгоритмом, двійкова часова складність якого дорівнює $T = nm2^{Nn}(6N^2 - N)$.

Таблиця 3.2

Чисельні значення логарифму виграшу у часовій складності при розв'язанні задачі LPN над кільцем $\mathbf{Z}/(2^N)$ за допомогою швидкого перетворення Ферма

(n, N) $\log m$	20	25	30	35	40	45	50	55
(20, 8)	12,85	17,85	22,85	27,85	32,85	37,85	42,85	47,85
(30, 8)	12,85	17,85	22,85	27,85	32,85	37,85	42,85	47,85
(40, 8)	12,85	17,85	22,85	27,85	32,85	37,85	42,85	47,85
(60, 8)	12,85	17,85	22,85	27,85	32,85	37,85	42,85	47,85
(20, 10)	11,18	16,18	21,18	26,18	31,18	36,18	41,18	46,18
(30, 10)	11,18	16,18	21,18	26,18	31,18	36,18	41,18	46,18
(40, 10)	11,18	16,18	21,18	26,18	31,18	36,18	41,18	46,18
(60, 10)	11,18	16,18	21,18	26,18	31,18	36,18	41,18	46,18
(80, 10)	11,18	16,18	21,18	26,18	31,18	36,18	41,18	46,18

Як видно з таблиці, при фіксованому N значення виграшу практично не залежить від числа невідомих (відмінності спостерігаються лише у молодших розрядах) та швидко зростає з ростом числа рівнянь у системі (2.1). При цьому збільшення кількості рівнянь у 2^5 разів призводить до 32-разового збільшення виграшу. Зокрема, при $N = 8$ виграш в трудомісткості складає від $2^{12,85}$ до $2^{47,85}$ разів в залежності від числа рівнянь у системі (2.1).

В табл. 3.3 для низки значень N і m наведені значення логарифму часової складності розв'язання задачі LPN для $n = 20$ невідомих над кільцем $\mathbf{Z}/(2^N)$ за допомогою швидкого перетворення Фур'є та швидкого перетворення Ферма відповідно.

Таблиця 3.3

Порівняння часової складності розв'язання задачі LPN над кільцем $\mathbf{Z}/(2^N)$ за допомогою швидких перетворень Фур'є та Ферма

$\log m$		50	100	150	200	250	300
$N=12$	$\log T_{2^N}(n)$	281,38	282,15	282,65	283,02	288,10	338,05
	$\log \tilde{T}_{2^N}(n)$	264,61	264,61	264,61	264,61	288,93	338,93
$N=16$	$\log T_{2^N}(n)$	369,88	370,61	371,10	371,46	371,75	371,99
	$\log \tilde{T}_{2^N}(n)$	349,02	349,02	349,02	349,02	349,02	350,59
$N=20$	$\log T_{2^N}(n)$	458,28	458,98	459,46	459,81	460,09	460,33
	$\log \tilde{T}_{2^N}(n)$	433,34	433,34	433,34	433,34	433,34	433,34
$N=24$	$\log T_{2^N}(n)$	546,62	547,29	547,75	548,10	548,38	548,61
	$\log \tilde{T}_{2^N}(n)$	517,61	517,61	517,61	517,61	517,61	517,61

Як видно з таблиці, трудомісткість обох алгоритмів збільшується з ростом параметрів m та N. При цьому, з погляду трудомісткості, для розв'язання задачі LPN над кільцем $\mathbf{Z}/(2^N)$ вигідніше використовувати алгоритм, наведений на рисунку 3.2. Поряд з тим, алгоритм на рисунку 3.1 не накладає обмежень щодо кількості рівнянь у системі (2.1) та є застосовним для розв'язання задачі LPN над довільним скінченним фробеніусовим кільцем.

3.3. Застосування розроблених методів до підвищення ефективності узагальненого алгоритму BKW

Наведені вище результати надають можливість за певних умов зменшити трудомісткість узагальненого алгоритму BKW, відомий прототип якого [8] є на сьогодні одним з найкращих алгоритмів розв'язання задачі LPN над полем з двох елементів.

Позначимо R довільне скінченне фробеніусове кільце порядку q. Нагадаємо (див. підрозділ 2.2), що узагальнений алгоритм BKW складається з двох етапів, на першому з яких за вхідною СР (2.1) над кільцем R будується нова система рівнянь (2.29) зі спотвореними правими частинами

від $n_1 \le n-3$ змінних. Потім, на другому етапі отримана система рівнянь розв'язується за допомогою ММП.

Оцінимо трудомісткість модифікації узагальненого алгоритму BKW, вважаючи, що на другому етапі, замість традиційного, використовується запропонований алгоритм 3.1, який базується на застосуванні швидкого перетворення Фур'є. Згідно з результатами підрозділу 2.2, часова складність зазначеного алгоритму визначається за формулою

$$T_{\mathrm{BKW}}(n_1) = T_{\mathrm{MMP}}(n_1, t) + ult \tag{3.14}$$

де

$$u = \left\lceil \frac{\log(n-n_1)}{2} \right\rceil,\ v = \left\lceil \frac{2(n-n_1)}{\log(n-n_1)} \right\rceil,\ k = 2^{u-1}, \tag{3.15}$$

$$l = (u\ +\ \left\lceil \ln(2t\delta^{-1}) \right\rceil\ -\ 1)q^v, \tag{3.16}$$

$$m(n_1) = lt, \tag{3.17}$$

а t позначає кількість рівнянь у системі (2.29), яка є достатньою для відновлення її істинного розв'язку з ймовірністю не менше ніж $1-\delta/2$, де $\delta \in (0, 1/2)$. При цьому розподіл ймовірностей спотворень у правій частині рівнянь системи (2.29) співпадає з розподілом випадкової величини $\xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, де $\xi_1, ..., \xi_k$ є незалежними в сукупності випадковими величинами, розподіленими на кільці R за законом p_ξ.

При розв'язанні СР (2.29) за допомогою традиційного алгоритму маємо $T_{\mathrm{MMP}}(n_1, t) = 2n_1 t q^{n_1}$, проте у випадку фробеніусова кільця R значення $T_{\mathrm{MMP}}(n_1, t)$ визначається за формулою (3.3) із заміною в ній n на n_1 та m на t відповідно.

Для проведення розрахунків розглянемо конкретний випадок, коли R є кільцем лишків за модулем 2^N, а розподіл ймовірностей спотворень у правих частинах рівнянь системи (2.1) визначається за законом (2.23).

Виконуючи процедуру, наведену на рисунку 3.3, отримаємо чисельні оцінки трудомісткості, зазначені в табл. 3.4.

Вхідні дані:

– натуральні числа $N \geq 2$, $n \geq 3$;

– числа $\varepsilon \in (0,1)$, $\delta \in (0,1/2)$.

Алгоритм обчислень.

Для кожного $n_1 \in \overline{1, n-3}$:

1. Обчислити значення u, v, k за формулами (3.15).
2. Обчислити значення t за формулами (2.32) – (2.38).
3. Обчислити значення (3.16) і (3.17).
4. Обчислити

$$T_{\text{MMP}}(n_1, t) = \quad 5 \cdot 2^{(n_1+2)N+1} N n_1 \log(2^{N+1} N n_1 t) +$$

$$+ 2^{2N} t((n_1+1)N(6N-5) + 5(N-1))$$

та визначити $T_{\text{BKW}}(n_1)$ за формулою (3.14).

Результат: число n_1^* таке, що $T_{\text{BKW}}(n_1^*) = \min\{T_{\text{BKW}}(n_1) : n_1 \in \overline{1, n-1}\}$ та відповідні значення $T_{\text{BKW}}(n_1^*)$, $m(n_1^*)$.

Рисунок 3.3. Процедура обчислення трудомісткості модифікації узагальненого алгоритму BKW, що базується на швидкому перетворенні Фур'є

Таблиця 3.4

Характеристики ефективності розв'язання задачі LPN за допомогою модифікації узагальненого алгоритму BKW, що базується на швидкому перетворенні Фур'є ($N = 8,\ \delta = 0{,}01$)

n	ε	n_1*	$\log T_{\mathrm{BKW}}(n_1^*)$	$\log m(n_1^*)$
32	2^{-10}	13	158,23	156,65
32	2^{-15}	16	160,55	128,58
32	2^{-20}	16	160,89	148,94
32	2^{-25}	16	170,22	169,22
32	2^{-30}	16	190,47	189,47
64	2^{-10}	21	214,95	213,36
64	2^{-15}	25	247,73	246,14
64	2^{-20}	28	280,28	278,69
64	2^{-25}	32	312,77	311,18
64	2^{-30}	35	345,15	343,56
80	2^{-10}	22	247,01	245,43
80	2^{-15}	26	279,78	278,20
80	2^{-20}	33	304,54	302,93
80	2^{-25}	33	344,81	343,23
80	2^{-30}	41	369,40	367,79
128	2^{-10}	42	385,29	383,29
128	2^{-15}	50	450,09	448,09
128	2^{-20}	58	514,70	512,70
128	2^{-25}	64	548,10	384,19
128	2^{-30}	64	548,34	424,44

Аналогічним чином, за умови твердження 3.3 можна підвищити ефективність узагальненого алгоритму BKW, використовуючи на другому етапі швидке перетворення Ферма (див. алгоритм на рисунку 3.2).

Для оцінки трудомісткості модифікованого таким чином узагальненого алгоритму BKW скористаємося процедурою, наведеною на рисунку 3.4.

Результати чисельних розрахунків, отримані за допомогою цієї процедури, представлено в табл. 3.5.

Порівнюючи результати, наведені в табл. 3.4 та 3.5 з даними, зазначеними в табл. 3.6, можна побачити, що запропоновані модифікації узагальненого алгоритму BKW мають меншу часову складність у порівнянні з його традиційною версією (див. підрозділ 2.2).

Вхідні дані:

– натуральні числа $N \geq 2$, $n \geq 3$;

– числа $\varepsilon \in (0,1)$, $\delta \in (0,1/2)$.

Алгоритм обчислень.

Для кожного $n_1 \in \overline{1, n-3}$:

5. Обчислити значення u, v, k за формулами (3.15).
6. Обчислити значення t за формулами (2.32) – (2.38).
7. Обчислити значення (3.16) і (3.17).
8. Обчислити

$$T_{\text{MMP}}(n_1, t) = 26 \cdot 2^{N(n_1+1)} N n_1 +$$

$$+ 2^{2N} t((n_1+1)N(6N-5) + 5(N-1) + 7 \cdot 2^{N-1} + 2)$$

та визначити $T_{\text{BKW}}(n_1)$ за формулою (3.14).

Результат: число $\widetilde{n}_1^*$ таке, що $T_{\text{BKW}}(\widetilde{n}_1^*) = \min\{T_{\text{BKW}}(n_1) : n_1 \in \overline{1, n-1}\}$ та відповідні значення $T_{\text{BKW}}(\widetilde{n}_1^*)$, $m(\widetilde{n}_1^*)$.

Рисунок 3.4. Процедура обчислення трудомісткості модифікації узагальненого алгоритму BKW, що базується на швидкому перетворенні Ферма

Таблиця 3.5

Характеристики ефективності розв'язання задачі LPN за допомогою модифікації узагальненого алгоритму BKW, що базується на швидкому перетворенні Ферма ($N = 8,\ \delta = 0{,}01$)

n	ε	$\widetilde{n}_1^*$	$\log T_{\mathrm{BKW}}(\widetilde{n}_1^*)$	$\log m(\widetilde{n}_1^*)$
32	2^{-10}	13	158,23	156,64
32	2^{-15}	16	147,70	128,58
32	2^{-20}	16	150,22	148,94
32	2^{-25}	16	170,21	169,22
32	2^{-30}	16	190,47	189,47
64	2^{-10}	21	214,95	213,36
64	2^{-15}	25	247,73	246,14
64	2^{-20}	28	280,28	278,69
64	2^{-25}	32	312,77	311,18
64	2^{-30}	39	337,38	335,72
80	2^{-10}	22	247,01	245,43
80	2^{-15}	26	279,78	278,20
80	2^{-20}	33	304,52	302,93
80	2^{-25}	33	344,81	343,23
80	2^{-30}	41	369,38	367,79
128	2^{-10}	42	385,29	383,29
128	2^{-15}	50	450,09	448,09
128	2^{-20}	58	514,70	512,70
128	2^{-25}	64	533,70	384,19
128	2^{-30}	65	541,72	424,46

Зокрема, застосування швидкого перетворення Фур'є на другому етапі узагальненого алгоритму BKW зменшує його складність від $2^{122,79}$ до $2^{754,07}$ разів в залежності від числа невідомих в системі та відстані між розподілом спотворень у правих частинах її рівнянь і рівномірним розподілом ймовірностей. При застосуванні швидкого перетворення Ферма виграш є майже таким же і змінюється від $2^{122,79}$ до $2^{754,07}$ разів.

Таблиця 3.6

Характеристики ефективності розв'язання задачі LPN з використанням звичайного узагальненого алгоритму BKW ($N = 8,\ \delta = 0{,}01$)

n	ε	n_1	$\log T_{\mathrm{BKW}}(n_1)$	$\log m(n_1)$
32	2^{-10}	28	281,61	56,12
32	2^{-15}	28	291,61	66,50
32	2^{-20}	28	301,61	76,84
32	2^{-25}	28	311,61	87,12
32	2^{-30}	28	321,61	97,35
64	2^{-10}	60	539,81	57,22
64	2^{-15}	60	549,81	67,65
64	2^{-20}	60	559,81	77,99
64	2^{-25}	60	569,81	88,26
64	2^{-30}	60	579,81	98,48
80	2^{-10}	76	668,49	57,63
80	2^{-15}	76	678,49	67,99
80	2^{-20}	76	688,49	78,33
80	2^{-25}	76	698,49	88,60
80	2^{-30}	76	708,49	98,82
128	2^{-10}	124	1139,95	58,34
128	2^{-15}	124	1149,95	68,75
128	2^{-20}	124	1159,95	79,08
128	2^{-25}	124	1169,95	89,34
128	2^{-30}	124	1179,95	99,56

Зазначимо також, що значення $n_1{}^*$ та $\widetilde{n}_1{}^*$ в табл. 3.4 та 3.5, які визначають, відповідно, кількість невідомих СР (2.1), що відновлюються за допомогою відповідних модифікацій узагальненого алгоритму, не збігаються зі значеннями n_1 з табл. 2.1. При цьому виявляється, що інколи на другому етапі узагальненого алгоритму BKW вигідніше розв'язувати систему рівнянь від більшої кількості змінних, використовуючи модифікацію Ферма замість модифікації Фур'є. Так, згідно з даними в табл. 3.4, 3.5, при $\varepsilon = 2^{-30}$ та $n = 128$ системи рівнянь зі спотвореними правими частинами від 65 змінних над кільцем лишків за модулем 2^8 розв'язуються швидше за допомогою

модифікацій ММП на базі швидкого перетворення Ферма, ніж аналогічні системи рівнянь від 64 невідомих з використанням швидкого перетворення Фур'є.

В цілому, запропоновані методи підвищення ефективності розв'язання задачі LPN доцільно використовувати у випадку сильноспотворених систем лінійних рівнянь над кільцями помірного порядку (зокрема, при $N = 8$ значення ε повинно бути не більше ніж 2^{-10}). Зокрема, це може бути корисним при побудові швидких кореляційних атак на потокові шифри над скінченним кільцями або полями.

Висновки

1. Основними науковими результатами розділу є два методи підвищення ефективності розв'язання задачі LPN за допомогою ММП. Перший з них є застосовним для довільного скінченного фробеніусова кільця R та базується на використанні швидкого перетворення Фур'є допоміжних функцій, що визначаються на цьому кільці. Другий метод є застосовним до задачі LPN над кільцем лишків за модулем 2^N і базується на використанні числового перетворення Ферма. Розроблені методи узагальнюють відомий спосіб застосування швидкого перетворення Фур'є для розв'язання задачі LPN над скінченним полем порядку 2^N.

2. Застосування швидкого перетворення Фур'є для розв'язання задачі LPN над кільцем лишків за модулем 2^N надає можливість зменшити трудомісткість ММП від $2^{5,80}$ до $2^{42,15}$ разів в залежності від параметра N та числа рівнянь у системі (2.1). При цьому застосування швидкого перетворення Ферма дозволяє отримати ще більший виграш у трудомісткості: від $2^{11,18}$ до $2^{47,85}$ разів (див. табл. 3.1, 3.2).

3. Модифікації узагальненого алгоритму BKW, побудовані на основі запропонованих методів, мають меншу часову складність у порівнянні з традиційною версією цього алгоритму. Зокрема, застосування швидкого перетворення Фур'є на другому етапі узагальненого алгоритму BKW зменшує складність останнього до 2^{754} разів в залежності від числа невідомих в системі та відстані між розподілом спотворень у правих частинах її рівнянь і рівномірним розподілом ймовірностей. При застосуванні швидкого перетворення Ферма виграш змінюється аналогічним чином: від 2^{122} до 2^{754} разів (див. табл. 3.4 – 3.6).

4. В цілому, розроблені методи підвищення ефективності розв'язання задачі LPN доцільно використовувати у випадку сильноспотворених систем лінійних рівнянь над кільцями помірного порядку, зокрема, при побудові швидких кореляційних атак на потокові шифри над скінченним кільцями або полями. В цьому випадку зазначені методи дозволяють помітно зменшити часову складність розв'язання задачі LPN як за допомогою самого ММП, так і інших алгоритмів (узагальненого алгоритму BKW), що використовують ММП як допоміжну процедуру.

Список використаних джерел у третьому розділі

1. Golić J. Dj., Morgari G. Vectorial fast correlation attacks. *Cryptology ePrint Archive.* URL: http://eprint.iacr.org/2004/247 (дата звернення: 06.08.2020).

2. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive.* URL: http://eprint.iacr.org/2016/311 (дата звернення: 06.08.2020).

3. Wood J. A. Duality for modules over finite rings and application to coding theory. *American Journal of Mathematics.* 1999. Vol. 121, № 3. P. 555-575.

4. Блейхут Р. Быстрые алгоритмы цифровой обработки сигналов : пер. с англ. Москва: Мир, 1989. 448 с.

5. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Сер. Технічні науки*. 2017. Вип. 15. С. 150-155.

6. Лидл Р., Нидеррайтер Г. Конечные поля : пер. с англ. Москва: Мир, 1988. 818 с.

7. Ноден П., Китте К. Алгебраическая алгоритмика : пер. с франц., Москва: Мир, 1999. 720 с.

8. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. 2003. Vol. 50, № 3. P. 506-519.

9. Игнатенко С. М. Модификация метода максимума правдоподобия решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2007. № 1, т. 9. С. 63-72.

10. Олексійчук А. М., Ігнатенко С. М. Застосування швидкого перетворення Фур'є для розв'язання задачі LPN над скінченними фробеніусовими кільцями. *Захист інформації*. 2017. № 4, т. 19. С. 271-277.

11. Игнатенко С. М., Алексейчук А. Н. Алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю 2^N с использованием быстрого преобразования Ферма. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. VI міжнар. наук.-практ. конф. Київ, 2003. С. 42-43.

12. Алексейчук А. Н., Игнатенко С. М. Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N. *Збірник наукових праць ІПМЕ НАН України*. 2003. Вип. 20, С. 40-48.

13. Ігнатенко С. М. Аналіз кореляційних атак на потокові шифри. *Спеціальні телекомунікаційні системи та захист інформації*. 2008. Вип. 1. С. 55-65.

РОЗДІЛ 4

ПОСЛІДОВНИЙ МЕТОД РОЗВ'ЯЗАННЯ ЗАДАЧІ LPN НАД КІЛЬЦЕМ ЛИШКІВ ЗА МОДУЛЕМ 2^N ТА ПРАКТИЧНІ ЗАСТОСУВАННЯ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

У підрозділі 4.1 викладено метод побудови нових алгоритмів розв'язання СР (2.1) над кільцем $R_N = \mathbf{Z}/(2^N)$ за довільною скінченною сукупністю вхідних таких алгоритмів. Зазначений (послідовний) метод запропоновано вперше і базується на ідеї послідовного розв'язання статистичних задач, що пристосована до розв'язання булевих СР із заважаючими параметрами [1], а також на формальному підході до побудови оптимальних за трудомісткістю обчислювальних алгоритмів, який запропоновано в [2]. Наведено аналітичні вирази оцінок надійності та часової складності алгоритмів розв'язання СР (2.1), які будуються за допомогою розробленого методу, через відповідні характеристики вхідних алгоритмів. Описано також процедуру побудови оптимальних (у певному класі) алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_N. Зауважимо, що ідея послідовного методу є достатньо природною і може бути використана для розв'язання систем лінійних рівнянь зі спотвореними правими частинами над більш широкими класами скінченних кілець, зокрема, кільцями Галуа (відмінними від скінченних полів).

У п. 4.2 наведено приклади практичного застосування розроблених методів до оцінювання або обґрунтування стійкості сучасних шифросистем, що базуються на складності розв'язання задачі LPN.

Як перший приклад, отримано (позитивну) відповідь на запитання про те, чи можна підвищити стійкість шифру SNOW 2.0 [3] відносно відомих

кореляційних атак [4 – 7] шляхом заміни у схемі його генератора гами порозрядного булевого додавання арифметичним додаванням за модулем 2^{32}, а також нелінійної підстановки іншим швидким перетворенням. Отримані практичні результати свідчать про можливість безпосереднього застосування розроблених у попередніх розділах методів до вирішення задачі оцінювання стійкості потокових шифрів над кільцями лишків за модулем 2^N відносно кореляційних атак та надають можливість цілеспрямовано вибирати компоненти зазначених шифрів для підвищення їх стійкості.

Як другий приклад, отримано чисельні оцінки стійкості шифросистем типу LPN-C [8] над кільцем R_N відносно атак на основі підібраних відкритих повідомлень. Показано, що послідовний метод відновлення ключа шифросистеми є набагато більш ефективним у порівнянні з методом, що базується на застосуванні узагальненого алгоритму BKW. Отримані результати свідчать про недоцільність застосування для побудови шифросистем LPN-C кілець R_N при $N \geq 2$, оскільки це не призводить до суттєвого підвищення стійкості у порівнянні з випадком $N = 1$.

Нарешті, як третій приклад, отримано чисельні оцінки стійкості шифросистеми, запропонованої в [9], за менш жорстких обмежень щодо її параметрів (зауважимо, що в [9] та інших доступних публікаціях таких оцінок не наводиться). Отримані результати надають можливість безпосередньо вибирати значення параметрів таких шифросистем, виходячи з вимог до їх стійкості відносно атаки на основі підібраних відкритих повідомлень.

4.1. Послідовний метод розв’язання задачі LPN над кільцем R_N

Позначимо $R_N = \mathbf{Z}/(2^N)$, P_N – сукупність усіх розподілів ймовірностей на кільці R_N. Кожний розподіл $p_N \in P_N$ являє собою стохастичний вектор

довжини 2^N з координатами $p_N(a)$, $a \in R_N$. Ототожнимо СР (2.1) з упорядкованим набором (A, a, b, p_N), де a є істинним розв'язком, а $p_N \in P_N$ – розподілом ймовірностей спотворень у правих частинах рівнянь системи (2.1).

Надалі під алгоритмом розв'язання СЛР (2.1) розумітимемо довільну частково обчислювану функцію $\wp$, що задана на певній підмножині $D_\wp$ множини всіх упорядкованих наборів (A, b, p_N) таких, що $A \in (R_N)_{m\times n}$, $p_N \in P_N$, $b = Aa + \xi$, яка ставить у відповідність кожному зазначеному набору деякий вектор $a^* \in R_N{}^n$ – оцінку істинного розв'язку a СР (2.1). Запис $a^* = \wp(A, b, p_N)$ означає, що вектор a^* є результатом застосування алгоритму $\wp$ до вхідних даних $(A, b, p_N) \in D_\wp$.

Позначимо Λ_N клас усіх алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_N. Символами $\pi_\wp = \pi_\wp(A, a, p_N)$ та $T_\wp = T_\wp(N, n, m, p_N)$ позначатимемо відповідно функції достовірності та трудомісткості алгоритму $\wp \in \Lambda_N$.

За означенням (див., наприклад, [11]) достовірність алгоритму $\wp$ визначається за формулою

$$\pi_\wp = \mathbf{P}\{\wp(A, b, p_N) = a\}, \tag{4.1}$$

де ймовірність в правій частині рівності (4.1) визначається відносно закону розподілу p_N координат випадкового вектора ξ. Зауважимо, що задана таким чином достовірність залежить від матриці $A \in (R_N)_{m\times n}$ та вектора $a \in R_N{}^n$. Можна визначити середню достовірність $\overline{\pi_\wp}$ алгоритму $\wp$, вважаючи $\overline{\pi_\wp} = 2^{-Nmn} \sum_{A\in(R_N)_{m\times n}} \mathbf{P}\{\wp(A, b, p_N) = a\}$. Нарешті, можна усереднити

значення (4.1) за всіма $A \in (R_N)_{m\times n}$, $a \in R_N{}^n$ і отримати таким чином середню достовірність алгоритму $\wp$ розв'язання СР (2.1), яка формується шляхом незалежного, випадкового та рівноймовірного вибору істинного розв'язку і матриці коефіцієнтів, які не залежать від вектора ξ.

Трудомісткість $T_\wp$ алгоритму $\wp \in \Lambda_N$ визначимо як бітову часову складність (в найгіршому випадку за рівномірним ваговим критерієм) цього алгоритму, використовуючи рівнодоступну адресну машину як модель обчислювального пристрою, на якому реалізуються алгоритми (див., наприклад, [3, 11]).

Перейдемо до викладення методу побудови нових алгоритмів розв'язання систем лінійних рівнянь вигляду (2.1).

Нехай задані довільні натуральні числа N_1, N_2. Позначимо $N = N_1 + N_2$ та визначимо відображення

$$\theta_{N_1,N_2} : \Lambda_{N_1} \times \Lambda_{N_2} \to \Lambda_N, \tag{4.2}$$

яке ставить у відповідність кожній упорядкованій парі $(\wp_1, \wp_2)$ алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцями R_{N_1}, R_{N_2} відповідно новий алгоритм

$$\wp = \theta_{N_1,N_2}(\wp_1, \wp_2),\ \wp \in \Lambda_N. \tag{4.3}$$

Сформулюємо точне означення алгоритму (4.3). Попередньо введемо низку додаткових позначень. Ототожнимо елементи кільця R_N з N-вимірними двійковими векторами, вважаючи

$$r = \sum_{i=0}^{N-1} 2^i r_i = (r_{N-1},...,r_1,r_0),\ r_i \in \{0,1\},\ i \in \overline{0, N-1}.$$

Для заданих N_1, N_2 задамо відображення $\delta_0, \delta_1 : R_N \to R_N$ за формулами

$$\delta_0(r) = (0,...,0,r_{N_1-1},...,r_0),\ \delta_1(r) = (0,...,0,r_{N-1},...,r_{N_1}), \tag{4.4}$$

де $r = (r_{N-1},...,r_1,r_0) \in R_N$. На підставі рівностей (4.4) маємо

$$r = \delta_0(r) + 2^{N_1}\delta_1(r),\ r \in R_N. \tag{4.5}$$

Вважаючи, що множини R_{N_1}, R_{N_2} канонічно вкладені в множину R_N, можна записати

$$\delta_0(r) \in R_{N_1},\ \delta_1(r) \in R_{N_2}. \tag{4.6}$$

Зауважимо, що співвідношення (4.5), (4.6) однозначно визначають функції δ_0, δ_1 в наступному сенсі: для будь-яких $a_0 \in R_{N_1}$, $a_1 \in R_{N_2}$ таких, що $r = a_0 + 2^{N_1}a_1$, справедливі рівності $a_0 = \delta_0(r)$, $a_1 = \delta_1(r)$. Ця властивість функцій δ_0, δ_1 використовується далі.

Нарешті, для будь-якої матриці $U = \| u_{\mu\nu} \|$ над кільцем R_N позначимо $\delta_1(U) = \| \delta_1(u_{\mu\nu}) \|$; зрозуміло, що $U = \delta_0(U) + 2^{N_1}\delta_1(U)$.

Перейдемо до визначення алгоритму $\wp = \theta_{N_1,N_2}(\wp_1,\wp_2)$. Розглянемо СР (2.1) над кільцем R_N. Для розв'язання цієї СР за допомогою алгоритму $\wp$, що визначається, перш за все, побудуємо таку систему лінійних рівнянь зі спотвореними правими частинами над кільцем R_{N_1}:

$$\delta_0(A)y = \delta_0(b) = \delta_0(A)\delta_0(a) + \delta_0(\xi). \tag{4.7}$$

Відзначимо, що закон розподілу $p_{N_1} \overset{\text{def}}{=} \delta_0(p_N)$ координат випадкового вектору $\delta_0(\xi)$ визначається за формулою

$$p_{N_1}(a_{N_1-1},...,a_0) = \sum_{(u_{N-1},...,u_{N_1})\in R_{N_2}} p_N(u_{N-1},...,u_{N_1},a_{N_1-1},...,a_0),\ (a_{N_1-1},...,a_0)\in R_{N_1}.$$

Якщо впорядкований набір $(\delta_0(A),\delta_0(b),p_{N_1})$ належить області визначення $D_{\wp_1}$ алгоритму $\wp_1$ (тобто СР (4.7) може бути розв'язана за допомогою цього алгоритму), то, розв'язуючи її, отримаємо оцінку

$$a_{0,1}* = \wp_1(\delta_0(A),\delta_0(b),p_{N_1}) \tag{4.8}$$

вектора $a_{0,1} \overset{\text{def}}{=} \delta_0(a)$.

Таким чином, на першому кроці алгоритму $\wp$ вигляду (4.3) здійснюється побудова СР (4.7), перевірка умови

$$(\delta_0(A),\delta_0(b),p_{N_1})\in D_{\wp_1} \tag{4.9}$$

та обчислення оцінки істинного розв'язку $a_{0,1}$ СР (4.7) за формулою (4.8).

На другому кроці алгоритму $\wp$ за системою рівнянь (2.1) та вектором (4.8) складається така СР над кільцем R_{N_2}:

$$A_2 z = \delta_1(b) - \delta_1(Aa_{0,1}* + \xi_1*), \tag{4.10}$$

де $A_2 = A \bmod(2^{N_2})$,

$$\xi_1^* = \delta_0(b - Aa_{0,1}^*). \tag{4.11}$$

Зауважимо, що у загальному випадку СР (4.10) не є системою рівнянь зі спотвореними правими частинами. Проте, справедливо таке твердження.

Твердження 4.1. Нехай виконується рівність

$$a_{0,1}^* = a_{0,1}. \tag{4.12}$$

Тоді СР (4.10) є системою лінійних рівнянь зі спотвореними правими частинами над кільцем R_{N_2}, яка має істинний розв'язок $a_{0,2} \overset{\text{def}}{=} \delta_1(a)$ і визначається впорядкованим набором $(A_2, a_{0,2}, d, p_{N_2})$, де вектор $d \overset{\text{def}}{=} \delta_1(b) - \delta_1(Aa_{0,1}^* + \xi_1^*)$ задовольняє такій рівності над кільцем R_{N_2}:

$$d = A_2 a_{0,2} + \xi_2, \tag{4.13}$$

а закон розподілу випадкового вектора $\xi_2 \overset{\text{def}}{=} \delta_1(\xi)$ визначається за формулою

$$p_{N_2}(a_{N_2-1},...,a_0) = \sum_{(u_{N_1-1},...,u_0)\in R_{N_1}} p_N(a_{N_2-1},...,a_0,u_{N_1-1},...,u_0),\ (a_{N_2-1},...,a_0) \in R_{N_2}.$$

Доведення. Достатньо показати, що за умови виконання співвідношень (2.1), (4.12) справедлива рівність (4.13).

Відповідно до означення вектора *d* та рівності (4.11) на підставі формули (4.12) справедлива така рівність над кільцем R_{N_2}:

$$d = \delta_1(b) - \delta_1(Aa_{0,1}^* + \delta_0(\xi)). \tag{4.14}$$

З іншого боку, на підставі рівності (2.1), маємо

$$b = Aa + \xi = A(a_{0,1} + 2^{N_1} a_{0,2}) + \delta_0(\xi) + 2^{N_1}\delta_1(\xi) =$$

$$= Aa_{0,1} + \delta_0(\xi) + 2^{N_1}(Aa_{0,2} + \delta_1(\xi)) = \delta_0(Aa_{0,1} + \delta_0(\xi)) +$$

$$+ 2^{N_1}(Aa_{0,2} + \delta_1(\xi) + \delta_1(Aa_{0,1} + \delta_0(\xi))),$$

звідки, згідно відзначеній вище властивості функцій δ_0, δ_1, випливає рівність

$$\delta_1(b) \equiv Aa_{0,2} + \delta_1(\xi) + \delta_1(Aa_{0,1} + \delta_0(\xi)) \pmod{2^{N_2}}. \qquad (4.15)$$

З формул (4.14), (4.15) знаходимо, що $d \equiv Aa_{0,2} + \delta_1(\xi) \pmod{2^{N_2}}$, тобто над кільцем R_{N_2} виконується рівність (4.13), що і треба було довести.

Отримане твердження показує, що у випадку, коли оцінка (4.8) істинного розв'язку $a_{0,1}$ СР (4.7) співпадає з самим розв'язком, СР (4.10) являє собою систему рівнянь зі спотвореними правими частинами над кільцем R_{N_2}. Ця система рівнянь визначається набором $(A_2, a_{0,1}, d, p_{N_2})$, який зазначено у формулюванні твердження 4.1.

Отже, на підставі наведеного вище другий крок алгоритму $\wp$ описується таким чином. Спочатку будується СР (4.10), яка інтерпретується як система рівнянь зі спотвореними правими частинами над кільцем R_{N_2}. Далі перевіряється умова

$$(A_2, d, p_{N_2}) \in D_{\wp_2}. \qquad (4.16)$$

Якщо співвідношення (4.16) виконується, то СР (4.10) розв'язується за допомогою алгоритму $\wp_2$, тобто обчислюється оцінка

$$a_{0,2}^* = \wp_2(A_2, d, p_{N_2}) \tag{4.17}$$

істинного розв'язку $a_{0,2}$ СР зі спотвореними правими частинами

$$A_2 z = d = A_2 a_{0,2} + \xi_2 \tag{4.18}$$

над кільцем R_{N_2}.

Нарешті, на третьому кроці алгоритму $\wp$ обчислюється оцінка $a_0^* = \wp(A, b, p_N)$ істинного розв'язку СР (2.1), яка знаходиться за формулою $a_0^* = a_{0,1}^* + 2^{N_1} a_{0,2}^*$.

Відзначимо, що відповідно до наведеного опису алгоритму $\wp$ його область визначення $D_\wp$ складається з тих і тільки тих упорядкованих наборів (A, b, p_N), для яких виконуються умови (4.9) та (4.16). Таким чином, відображення θ_{N_1,N_2} вигляду (4.2) визначено коректно.

Отримаємо аналітичні вирази оцінок достовірності та трудомісткості алгоритму $\wp = \theta_{N_1,N_2}(\wp_1, \wp_2)$ через відповідні характеристики алгоритмів $\wp_1$ та $\wp_2$.

Твердження 4.2. Нехай (A, a, b, p_N) є СР вигляду (2.1) над кільцем R_N та $(A, b, p_N) \in D_\wp$, де алгоритм $\wp$ визначається за формулою (4.3). Позначимо $\pi_{\wp_1} = \pi_{\wp_1}(\delta_0(A), a_{0,1}, p_{N_1})$, $\pi_{\wp_2} = \pi_{\wp_2}(A_2, a_{0,2}, p_{N_2})$ значення функцій достовірності алгоритмів $\wp_1$, $\wp_2$ відповідно (від аргументів $(\delta_0(A), a_{0,1}, p_{N_1})$ і $(A_2, a_{0,2}, p_{N_2})$, що відповідають СР зі спотвореними

правими частинами (4.7) та (4.18) відповідно). Позначимо також $\pi_{\wp} = \pi_{\wp}(A, a, p_N)$. Тоді справедливі нерівності

$$\pi_{\wp_1} + \pi_{\wp_2} - 1 \le \pi_{\wp} \le \min\{\pi_{\wp_1}, \pi_{\wp_2}\}. \tag{4.19}$$

Крім того, якщо випадкові вектори $\xi_1 = \delta_0(\xi)$ та $\xi_2 = \delta_1(\xi)$ є незалежними, то

$$\pi_{\wp} = \pi_{\wp_1}\pi_{\wp_2}. \tag{4.20}$$

Доведення. Розглянемо події U_1 та U_2, що визначаються за формулами

$$U_1 = \{\xi \in {R_N}^m : \wp_1(\delta_0(A), \delta_0(b), p_{N_1}) = a_{0,1}\},$$

$$U_2 = \{\xi \in {R_N}^m : \wp_2(A_2, d, p_{N_2}) = a_{0,2}\}.$$

Позначимо символом $\Pr^{(m)}$ розподіл ймовірностей на множині ${R_N}^m$ значень випадкового вектора ξ. З означення параметрів $\pi_{\wp_1}$, $\pi_{\wp_2}$ випливають рівності

$$\pi_{\wp_1} = \Pr^{(m)}\{U_1\},\ \pi_{\wp_2} = \Pr^{(m)}\{U_2\}. \tag{4.21}$$

З іншого боку, згідно з означенням алгоритму $\wp$ виконується рівність

$$\pi_{\wp} = \Pr^{(m)}\{U_1U_2\}. \tag{4.22}$$

Безпосередньо з формул (4.21), (4.21) випливають співвідношення (4.19), (4.20). Твердження доведено.

Отримаємо оцінку трудомісткості $T_{\wp} = T_{\wp}(N, n, m, p_N)$ алгоритму $\wp$. На першому кроці цього алгоритму побудова СР (4.7) не потребує обчислень (за виключенням, можливо, знаходження розподілу ймовірностей p_{N_1} за розподілом p_N). Отже, трудомісткість першого кроку дорівнює $T_{\wp_1}(N_1, n, m)$.

На другому кроці для обчислення вектора ξ_1* за формулою (4.11) достатньо виконати nm множень та $(n-1)m + m = nm$ додавань (віднімань) у кільці R_{N_1}. Далі, обчислення вектора d у правій частині СР (4.10) потребує виконання nt множень та $(n+1)m$ додавань (віднімань) у кільці R_N. Таким чином, сумарна складність другого кроку алгоритму $\wp$ складе не більше ніж

$$T_2 = T_{\wp_2}(N_2, n, m) + 2nmC_{\times}(N) + 2(n+1)mC_{+}(N)$$

двійкових операцій, де символи $C_{\times}(N)$ та $C_{+}(N)$ означають відповідно двійкові часові складності алгоритмів множення та додавання (віднімання) N-розрядних двійкових цілих чисел.

Нарешті, на третьому кроці алгоритму $\wp$ обчислень фактично не відбувається. Отже, доведено наступне твердження.

Твердження 4.3. Трудомісткість алгоритму $\wp = \theta_{N_1,N_2}(\wp_1, \wp_2)$, що визначається за формулою (4.3), оцінюється зверху величиною

$$T_{\wp} = T_{\wp_1}(N_1, n, m, p_{N_1}) + T_{\wp_2}(N_2, n, m, p_{N_2}) + 2(n+1)m(C_{\times}(N) + C_{+}(N)). \quad (4.23)$$

Розглянемо задачу оптимізації алгоритмів розв’язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_N. Дотримуючись

загальної ідеї підходу [2] до побудови оптимальних обчислювальних алгоритмів, визначимо рекурсивно відображення

$$\theta_{N_1,N_2,\ldots,N_k} : \Lambda_{N_1} \times \Lambda_{N_2} \times \ldots \times \Lambda_{N_k} \to \Lambda_N ,$$

де $k \geq 3$, $N = N_1 + N_2 + \ldots + N_k$, $N_i \geq 1$, $i \in \overline{1,k}$, вважаючи для будь-яких $\wp_i \in \Lambda_{N_i}$ $(i \in \overline{1,k})$

$$\theta_{N_1,N_2,\ldots,N_k}(\wp_1, \wp_2, \ldots, \wp_k) = \theta_{N-N_k,N_k}(\theta_{N_1,N_2,\ldots,N_{k-1}}(\wp_1, \wp_2, \ldots, \wp_{k-1}), \wp_k).$$

Нехай для кожного натурального $j \in \overline{1,N}$ задано деякий алгоритм $\wp(j)$ розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_j. Функції достовірності π_j та трудомісткості T_j алгоритму $\wp(j)$ ($j \in \overline{1,N}$) вважаються відомими. Позначимо $\Theta = \Theta(\wp(1), \ldots, \wp(N))$ клас усіх алгоритмів $\wp \in \Lambda_N$, що мають вигляд:

$$\wp = \theta_\nu \overset{\text{def}}{=} \theta_{N_1,N_2,\ldots,N_k}(\wp(N_1), \wp(N_2), \ldots, \wp(N_k)),$$

де $\nu = (N_1, N_2, \ldots, N_k)$ пробігає усі можливі композиції (впорядковані розбиття) числа N.

Зафіксуємо СР вигляду (2.1) над кільцем R_N та припустимо, що двійкові розряди координат випадкового вектора ξ є незалежними в сукупності випадковими величинами. Розглянемо задачу побудови алгоритму $\wp^* \in \Theta$, який має при фіксованій верхній межі трудомісткості найбільшу достовірність серед усіх алгоритмів розв'язання СР (2.1), що належать класу Θ:

$$\pi_{\wp}(A, a, p_N) \to \max,\ T_{\wp}(N, n, m, p_N) \le T_0,\ \wp \in \Theta. \qquad (4.24)$$

Зауважимо, що, оскільки Θ містить точно 2^{N-1} різних алгоритмів, то тривіальна процедура розв'язання задачі (4.24) зводиться до перебору таких алгоритмів та обчисленню їх достовірності та трудомісткості з використанням співвідношень (4.20), (4.23). Відзначимо також, що за деяких додаткових обмежень щодо розподілу ймовірностей координат випадкового вектора ξ задача (4.24) може бути розв'язана більш ефективно. Розглянемо, наприклад, окремий випадок, в якому

$$p_N(a) = p^{\|a\|}(1-p)^{N-\|a\|}, a = (a_{N-1},...,a_0) \in R_N, \qquad (4.25)$$

де $\|a\| = a_0 + ... + a_{N-1}$, $p \in (0, 1/2)$. Позначимо φ_j канонічний гомоморфізм кільця R_N в кільце R_j, $j \in \overline{1, N}$. Продовжимо відображення φ_j зазначеним вище чином на множини всіх матриць над кільцем R_N та розподілів ймовірностей на цьому кільці відповідно.

На підставі тверджень 4.2, 4.3 та рівності (4.25) для будь-якої композиції ν числа N достовірність і трудомісткість алгоритму $\wp = \theta_\nu$ визначаються за формулами

$$\pi_{\wp}(A, a, p_N) = \prod_{j=1}^{N} (\pi_j)^{\alpha_j},$$

$$T_{\wp}(N, n, m, p_N) = \sum_{j=1}^{N} \alpha_j T_j + 2(n+1)m(C_{\times}(N) + C_{+}(N))(\sum_{j=1}^{N} \alpha_j - 1),$$

де α_j – число доданків, що дорівнюють j, у композиції ν, $\pi_j = \pi_j(\varphi_j(A), \varphi_j(x^{(0)}), \varphi_j(p_N))$, $T_j = T_j(N, n, m, \varphi_j(p_N))$, $j \in \overline{1, N}$. Звідси випливає, що за умови (4.25)

задача (4.24) рівносильна наступній задачі цілочисельного лінійного програмування:

$$\sum_{j=1}^{N} \alpha_j \ln \pi_j \to \max,$$

$$\sum_{j=1}^{N} \alpha_j (T_j + 2(n+1)m(C_{\times}(N) + T_{+}(N))) \le T_0 + 2(n+1)m(T_{\times}(N) + T_{+}(N)),$$

$$\alpha_j \in \mathbf{Z},\ \alpha_j \ge 0,\ j \in \overline{1, N},\ \alpha_1 + 2\alpha_2 + \ldots + N\alpha_N = N.$$

Для розв'язання останньої задачі можна застосовувати відомі алгоритми [12].

Наведемо результати експериментального дослідження ефективності алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_5. В табл. 4.1 представлені чисельні оцінки середньої достовірності та трудомісткості семи програмно реалізованих алгоритмів розв'язання СР (2.1) над кільцем лишків за модулем 32, які відповідають семи композиціям числа $N = 5$. Дані в таблиці отримані з використанням програми для ПЕОМ типу Celeron 1100 MHz, 256 Mb ОЗП, яка для кожної пари значень n, m (числа невідомих та рівнянь відповідно) розв'язує 100 систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_5.

Істинний розв'язок та елементи матриці коефіцієнтів кожної системи лінійних рівнянь формуються з використанням лінійного конгруентного генератора за модулем 32. Вектори спотворень у правих частинах СР утворюються з символів, що представлені в коді ASCII, які вибираються послідовно, з інтервалом у 10 знаків, із осмислених україно- або англомовних текстів. В ролі вхідного алгоритму $\wp(j)$ розв'язання СР зі спотвореними правими частинами над кільцем R_j ($j \in \overline{1, 5}$) використовується традиційний метод максимуму правдоподібності (див. підрозділ 2.1). Параметри P і T у

таблиці позначають відповідно відношення числа СР, що розв'язані правильно, до їх загальної кількості (тобто 100) та сумарний час (у секундах) розв'язання всіх СР без врахування часу на їх формування.

Таблиця 4.1

Характеристики ефективності алгоритмів розв'язання СР зі спотвореними правими частинами над кільцем лишків за модулем 32

		(1,1,1,1,1)		(2, 2, 1)		(2, 3)		(3, 1, 1)		(3, 2)		(4, 1)		(5)	
n	*m*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*	*P*	*T*
3	7	0,01	0	0,01	0	0,01	0	0,03	0	0,03	0	0,03	1	0,09	20
	25	0,04	0	0,10	0	0,13	0	0,22	0	0,39	0	0,39	2	0,86	28
	40	0,15	0	0,21	0	0,27	0	0,34	0	0,59	0	0,78	3	0,99	34
	60	0,17	0	0,38	0	0,48	0	0,48	1	0,79	0	0,94	4	1	42
	80	0,30	0	0,57	0	0,64	0	0,63	1	0,88	0	0,95	6	1	50
	100	0,47	0	0,66	0	0,78	0	0,77	1	0,99	0	1	7	1	58
	150	0,67	0	0,88	0	0,92	1	0,90	2	1	1	1	10	1	79
4	25	0	0	0,02	0	0,04	1	0,08	2	0,20	1	0,22	42	0,72	919
	80	0,18	0	0,33	1	0,45	3	0,38	5	0,79	3	0,93	98	1	1717
	150	0,49	0	0,81	1	0,88	4	0,81	10	1	5	1	168	1	2744

Як видно з табл. 4.1, діапазон зміни значень характеристик ефективності алгоритмів, що розглядаються, є достатньо широким. Так, середня достовірність розв'язання системи з 25 рівнянь зі спотвореними правими частинами від 3 невідомих змінюється від 0,04 до 0,86. При цьому на розв'язання 100 таких систем витрачається від 1 до 28 секунд. Система з тим самим числом невідомих, яка складається з 60 рівнянь зі спотвореними правими частинами, розв'язується з середньою достовірністю від 0,17 до 1. Час розв'язання 100 зазначених СР складає від 1 до 42 секунд. Зрозуміло, що з ростом відношення m/n достовірність кожного з семи алгоритмів збільшується.

Результати, наведені в табл. 4.1, дозволяють впорядкувати алгоритми, що розглядаються, за незростанням їх середньої достовірності. Так, для всіх значень параметрів n та m з таблиці найбільшу середню достовірність має алгоритм $\theta_{(5)}$; далі слідують алгоритми $\theta_{(4,1)}$ и $\theta_{(3,2)}$. При помірних (у

порівнянні з n) значеннях m наступними в списку виявляються алгоритми $\theta_{(3,1,1)}$ та $\theta_{(2,3)}$. З ростом m середні достовірності цих алгоритмів вирівнюються, і при $m >> n$ порядок їх розміщення змінюється на протилежний: $\theta_{(2,3)}$, $\theta_{(3,1,1)}$. Нарешті, замикають список алгоритми $\theta_{(2,2,1)}$ та $\theta_{(1,1,1,1,1)}$.

Зауважимо, що алгоритм $\theta_{(1,1,1,1,1)}$ співпадає з послідовним алгоритмом розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем R_5, який наведено в [13]. Як видно з табл. 4.1, цей алгоритм має найменшу середню достовірність та найменшу трудомісткість серед усіх семи алгоритмів. З іншого боку, алгоритм $\theta_{(5)}$ реалізує стандартний метод максимуму правдоподібності (див. п. 2.1) та характеризується найбільшими достовірністю та трудомісткості серед усіх алгоритмів, що розглядаються.

В цілому, як видно з даних, приведених у таблиці, викладений метод оптимізації алгоритмів розв'язання СР зі спотвореними правими частинами над кільцем R_N дозволяє забезпечити гарний "баланс" між основними показниками ефективності (достовірністю і трудомісткістю) алгоритмів шляхом належного вибору композиції числа N. Зрозуміло також, що з розширенням сукупності вхідних алгоритмів з'являється додаткова можливість цілеспрямовано змінювати значення цих показників в залежності від конкретної прикладної задачі, яка приводить до розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем лишків за модулем 2^N.

4.2. Застосування отриманих наукових результатів до оцінювання та обґрунтування стійкості сучасних шифросистем

4.2.1. Оцінювання стійкості SNOW 2.0-подібних шифрів над кільцями лишків відносно кореляційних атак.

Розглянемо генератор гами SNOW 2.0-подібного потокового шифру, який складається з лінійного регістру зсуву над кільцем R_N та підстановки $\sigma: R_N \to R_N$, поєднаних між собою як зазначено на рисунку 4.1. Вважатимемо, що многочлен зворотного зв'язку ЛРЗ $g(z) = z^n - (c_{n-1}z^{n-1} + ... + c_0)$ над кільцем R_N є многочленом максимального періоду (який дорівнює $2^{N-1}(2^n - 1)$ [14]), а ЛРЗ виробляє лінійну рекурентну послідовність $x_0, x_1, ...,$ знаки якої пов'язані співвідношенням $x_{i+n} = c_{n-1}x_{i+n-1} + ... + c_0 x_i$, $i = 0, 1, ...$ Генератор гами являє собою скінченний автономний автомат з множиною внутрішніх станів ${R_N}^n \times {R_N}^2$, функцією переходів

$$h((z_{n-1}, z_{n-2}, ..., z_0), u, v) = ((z_n, z_{n-1}, ..., z_1), z_\mu + v, \sigma(u))$$

та функцією виходів

$$f((z_{n-1}, z_{n-2}, ..., z_0), u, v) = z_0 + F = z_0 + (z_{n-1} + u + v),$$

де $z_0, ..., z_{n-1}, u, v \in R_N$, $x_n = c_{n-1}x_{n-1} + ... + c_0 x_0$. Отже, знак гами в i-му такті визначається за початковим станом $((x_{n-1}, x_{n-2}, ..., x_0), u_0, v_0)$ генератора за допомогою таких рекурентних співвідношень:

$$\gamma_i = x_i + x_{i+n-1} + u_i + v_i,\ u_{i+1} = x_{i+\mu} + v_i,\ v_{i+1} = \sigma(u_i),\ i = 0, 1, ... \qquad (4.26)$$

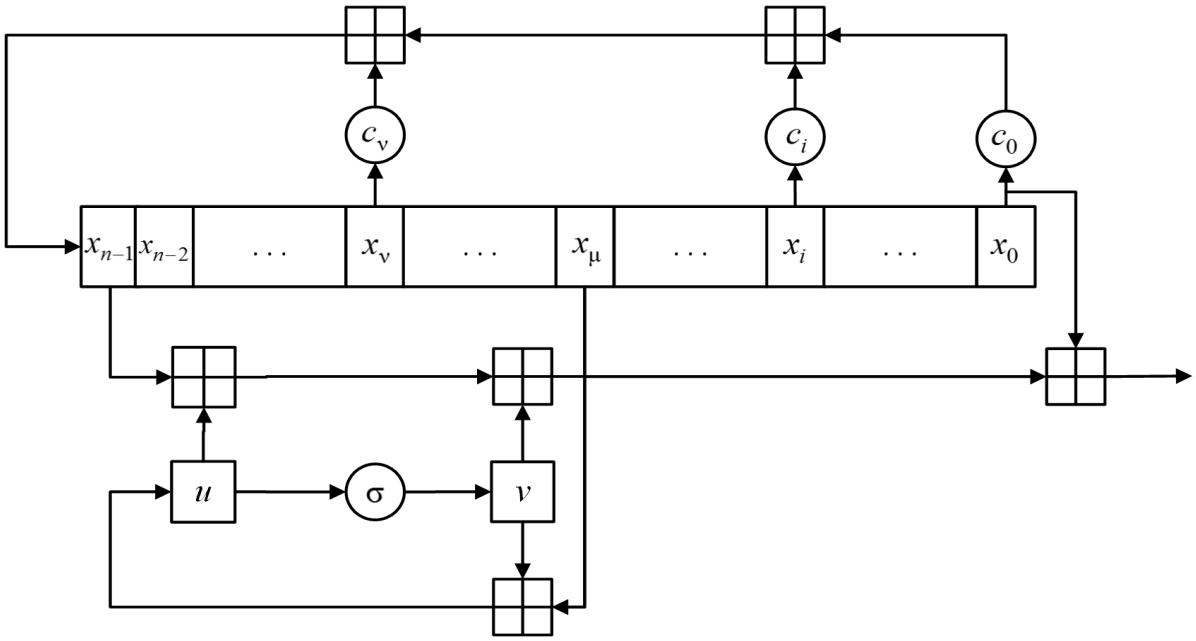

Рисунок 4.1. Схема генератора гами SNOW 2.0-подібного шифру

Зауважимо, що головною відмінністю генератора, що розглядається, від генераторів гами звичайних SNOW 2.0-подібних потокових шифрів [15] є застосування операції + додавання в кільці R_N замість операції $\oplus$ порозрядного додавання двійкових векторів за модулем 2.

Використовуючи розвинуті вище методи, отримуємо оцінки стійкості генератора на рисунку 4.1 відносно кореляційних атак [4 – 7], що є застосовними до шифру SNOW 2.0. Як зазначено у підрозділі 1.2, усі ці атаки базуються на тому, що сума (за модулем 2) знаків гами в будь-яких суміжних тактах є результатом спотворення знаку певної лінійної рекуренти з характеристичним многочленом $g(z)$.

Для генератора, що розглядається, на підставі співвідношень (4.26) справедливі такі рівності:

$$\gamma_{i+1} - \gamma_i = x_{i+1} + x_{i+n} - x_i - x_{i+n-1} + x_{i+\mu} + \xi_i,\ i = 0, 1, \ldots, \qquad (4.27)$$

де

$$\xi_i = \sigma(u_i) - u_i,\ i = 0, 1, \ldots. \qquad (4.28)$$

Вважаючи, що змінні $u_0, u_1, \ldots$ є незалежними випадковими величинами з рівномірним розподілом на кільці R_N та виражаючи знаки $x_i, x_{i+1}, x_{i+\mu}, x_{i+n-1}, x_{i+n}$ лінійної рекуренти через початковий стан ЛРЗ на рисунку 4.1, на підставі рівностей (4.27) отримаємо систему лінійних рівнянь зі спотвореними правими частинами над кільцем R_N, де спотворення є випадковими величинами (4.28).

Позначимо $\sigma'(u) = \sigma(u) - u$, $u \in R_N$. Тоді

$$p(z) = \mathbf{P}\{\xi_i = z\} = 2^{-N} \mid \{u \in R_N : \sigma'(u) = z\} \mid,\ z \in R_N,\ i = 0, 1, \ldots. \qquad (4.29)$$

Отже, з погляду спроможності генератора протистояти кореляційним атакам, що базуються на розв'язанні СР (4.27), найкращим способом вибору підстановки σ є такий, коли розподіл (4.29) є рівномірним або, що те ж саме, відображення σ' є підстановкою на кільці R_N. Поряд з тим, при $N \geq 2$ таких підстановок σ не існує [16]. Проте існують підстановки σ, для яких розподіл (4.29) відрізняється від рівномірного розподілу ймовірностей на кільці R_N лише у двох точках:

$$p(0) = 0,\ p(2^{N-1}) = 2^{1-N}\ p(z) = 2^{-N}\ z \in R_N \setminus \{0, 2^{N-1}\}. \qquad (4.30)$$

Як приклад, зазначимо підстановку σ, значення якої в точці $z \in R_N$ дорівнює циклічному зсуву двійкового запису числа z в бік старших розрядів [16].

Отже, вважатимемо, що підстановка σ вибрана таким чином, що розподіл ймовірностей (4.29) має вигляд (4.30).

Зауважимо, що на підставі формул (4.29), (4.30) для будь-яких $i = 0, 1, \ldots$, $z \in R_{N-1}$ справедлива рівність $\mathbf{P}\{\xi_i (\mathrm{mod}\, 2^{N-1}) = z\} = 2^{-(N-1)}$. Отже, випадкові

величини $\xi_i \pmod{2^l}$, $i = 0, 1, ...,$ є рівномірно розподіленими на кільці R_l для кожного $l \in \overline{0, N-1}$, і послідовний метод, викладений в п. 4.1, є незастосовним для побудови кореляційних атак на генератор гами, що розглядається.

Поряд з тим, викладені в розділах 2, 3 результати надають можливість оцінити обсяг матеріалу, потрібного для розв'язання СР (4.27) із заданою достовірністю, а також обчислювальну складність розв'язання цієї СР за допомогою узагальненого алгоритму BKW та його модифікацій (табл. 4.2).

Символом T в таблиці позначено нижню межу часової складності ММП: $T = nm_0 2^{Nn}(6N^2 - N)$, де m_0 визначається за формулою (2.28); символи $T_{\mathrm{BKW}}(n_1)$, $T_{\mathrm{BKW}}(n_1{*})$ та $T_{\mathrm{BKW}}(\widetilde{n}_1{*})$ позначають трудомісткості узагальненого алгоритму BKW та його модифікацій із застосуванням швидкого перетворення Фур'є та швидкого перетворення Ферма відповідно, а символи $m(n_1)$, $m(n_1{*})$ і $m(\widetilde{n}_1{*})$ позначають обсяг матеріалу (кількість рівнянь в системі (4.27)), потрібного для успішного застосування узагальненого алгоритму BKW та його модифікацій з використанням швидкого перетворення Фур'є та швидкого перетворення Ферма відповідно.

При проведенні розрахунків використано інформацію про розподіл (4.30), а також розподіл ймовірностей $p_\xi^{(k)}$ (див. зауваження за формулою (2.31)), що має такий вигляд:

$$p_\xi^{(k)}(0) = 2^{-N}(1 + 2^{-(N-1)(k-1)}),\ p_\xi^{(k)}(2^{N-1}) = 2^{-N}(1 - 2^{-(N-1)(k-1)}),$$

$$p_\xi^{(k)}(z) = 2^{-N},\ z \in R_N \setminus \{0, 2^{N-1}\}.$$

Таблиця 4.2

Результати оцінювання стійкості SNOW 2.0-подібних шифрів над кільцем лишків відносно кореляційних атак

Параметр	$n = 64,\ N = 8$	$n = 16,\ N = 32$
$\log T$	542,01	568,03
n_1	17	7
n_1 *	21	7
$\widetilde{n}_1$ *	21	7
$\log T_{\mathrm{BKW}}(n_1)$	200,93	329,26
$\log T_{\mathrm{BKW}}(n_1^*)$	199,20	304,65
$\log T_{\mathrm{BKW}}(\widetilde{n}_1^*)$	192,69	300,72
$\log m(n_1)$	199,04	299,72
$\log m(n_1^*)$	191,04	299,72
$\log m(\widetilde{n}_1^*)$	191,04	299,72

Як видно з таблиці, за умов (4.28), (4.30) для розв'язання СР (4.27) від $n = 64$ невідомих над кільцем $R_N = \mathbf{Z}/(2^8)$ за допомогою ММП необхідно не менше ніж $2^{542,01}$ двійкових операцій. При цьому для відновлення будь-яких $n_1 = 17$ невідомих з цієї системи рівнянь за допомогою узагальненого алгоритму BKW потрібно лише $2^{200,93}$ операцій та $2^{199,04}$ рівнянь, а при застосуванні швидкого перетворення Ферма – тільки $2^{192,69}$ операцій та $2^{191,04}$ рівнянь. Отже, складність найкращої (з відомих на сьогодні) кореляційних атак на SNOW 2.0-подібний шифр, що розглядається, складає $\left\lceil \frac{64}{21} \right\rceil \cdot 2^{192,69} = 2^{194,69}$ операцій при обсязі матеріалу $\left\lceil \frac{64}{21} \right\rceil \cdot 2^{191,04} = 2^{193,04}$ знаків вихідної послідовності генератора.

При $n = 16$, $N = 32$ (параметри шифру SNOW 2.0) найкраща з відомих кореляційних атак на шифр потребує $\left\lceil \frac{16}{7} \right\rceil \cdot 2^{300,72} = 2^{302,31}$ операцій та $\left\lceil \frac{16}{7} \right\rceil \cdot 2^{299,72} = 2^{301,31}$ знаків гами (при цьому довжина ЛРЗ генератора складає 512 біт). Зауважимо також, що найкраща з відомих кореляційних атак на оригінальну версію шифру SNOW 2.0 має обчислювальну складність $2^{164,15}$ операцій та потребує $2^{163,59}$ знаків гами [7].

Отримані результати свідчать про можливість безпосереднього застосування розроблених методів до вирішення задачі оцінювання стійкості потокових шифрів над кільцями лишків відносно кореляційних атак. Вони надають також можливість цілеспрямовано вибирати компоненти зазначених шифрів для підвищення їх стійкості відносно таких атак.

4.2.2. Оцінювання стійкості шифросистем типу LPN-C над кільцями лишків. Як приклад ефективного застосування послідовного методу розв'язання систем лінійних рівнянь зі спотвореними правими частинами (підрозділ 4.1), розглянемо атаки на шифросистему LPN-C, побудовану над кільцем $R_N = \mathbf{Z}/(2^N)$, де $N \geq 2$.

Нагадаємо, що шифросистема LPN-C запропонована в [8] для випадку $N = 1$, проте вона природним чином узагальнюється на випадок довільного скінченного кільця R (див. підрозділ 1.2). Для побудови шифросистеми вибирається $[L, K, D]$-код C, тобто вільний підмодуль вимірності K лівого модуля R^L такий, що мінімальна вага (Гемінга) будь-якого ненульового слова $c \in C$ є не менше ніж D. Вважається, що зазначений код допускає швидкий алгоритм декодування у межах коригувальної здатності, тобто дозволяє ефективно, з обчислювальної точки зору, виправляти будь-яку комбінацію з $t \leq \left\lfloor \frac{D-1}{2} \right\rfloor$ помилок. У ролі ключа використовується випадкова

рівноймовірна $n \times L$-матриця M над кільцем R, а шифроване повідомлення, що отримується в результаті зашифрування відкритого тексту $x \in R^K$ на ключі M визначається за формулою $(a, y = xG + aM + \xi)$, де G – твірна матриця коду C, a – випадковий рівноймовірний вектор довжини n над кільцем R, ξ – випадковий рівноймовірний вектор довжини L та ваги t над цим кільцем. Законний отримувач, знаючи ключ M, отримує спотворене кодове слово $xG + \xi$, за яким може швидко відновити відкритий текст x, використовуючи алгоритм декодування коду C (рисунок 4.2). При цьому супротивник може реалізувати на шифросистему атаку з підібраним відкритим повідомленням, зашифровуючи m разів певне фіксоване, наприклад, нульове, повідомлення $x = 0$ та формуючи L систем лінійних рівнянь зі спотвореними правими частинами

$$a_i M_j + \xi_{i,j} = y_{i,j},\ i \in \overline{1,m} \tag{4.31}$$

відносно стовпців M_j невідомої матриці M, $j \in \overline{1,L}$.

Зауважимо, що внаслідок незалежно випадкового вибору векторів a_i, ξ_i при кожному зашифруванні матриця коефіцієнтів СР (4.31), яка складається з рядків $a_1,...,a_m$ над кільцем R, є суто випадковою (але відомою супротивнику), а величини $\xi_{1,j}, ..., \xi_{m,j}$ є незалежними в сукупності та розподілені за законом

$$\mathbf{P}\{\xi_{i,j} = z\} = \frac{\binom{L-1}{t-1}(q-1)^{t-1}}{\binom{L}{t}(q-1)^t} = \frac{t}{L(q-1)},\ z \in R \setminus \{0\},\ \mathbf{P}\{\xi_{i,j} = 0\} = 1 - \frac{t}{L},$$

де $i \in \overline{1,m}$, $j \in \overline{1,L}$, $q = |R|$. Зазначений закон розподілу має вигляд (2.23):

$$p(0) = q^{-1}(1+(q-1)\varepsilon),\ p(z) = q^{-1}(1-\varepsilon),\ z \neq 0, \tag{4.32}$$

де

$$\varepsilon = 1 - \frac{qt}{L(q-1)}. \tag{4.33}$$

Отже, для оцінювання складності розв'язання СР (4.31), яка визначає стійкість шифросистеми LPN-C відносно зазначеної атаки, можна використовувати запропоновані вище методи.

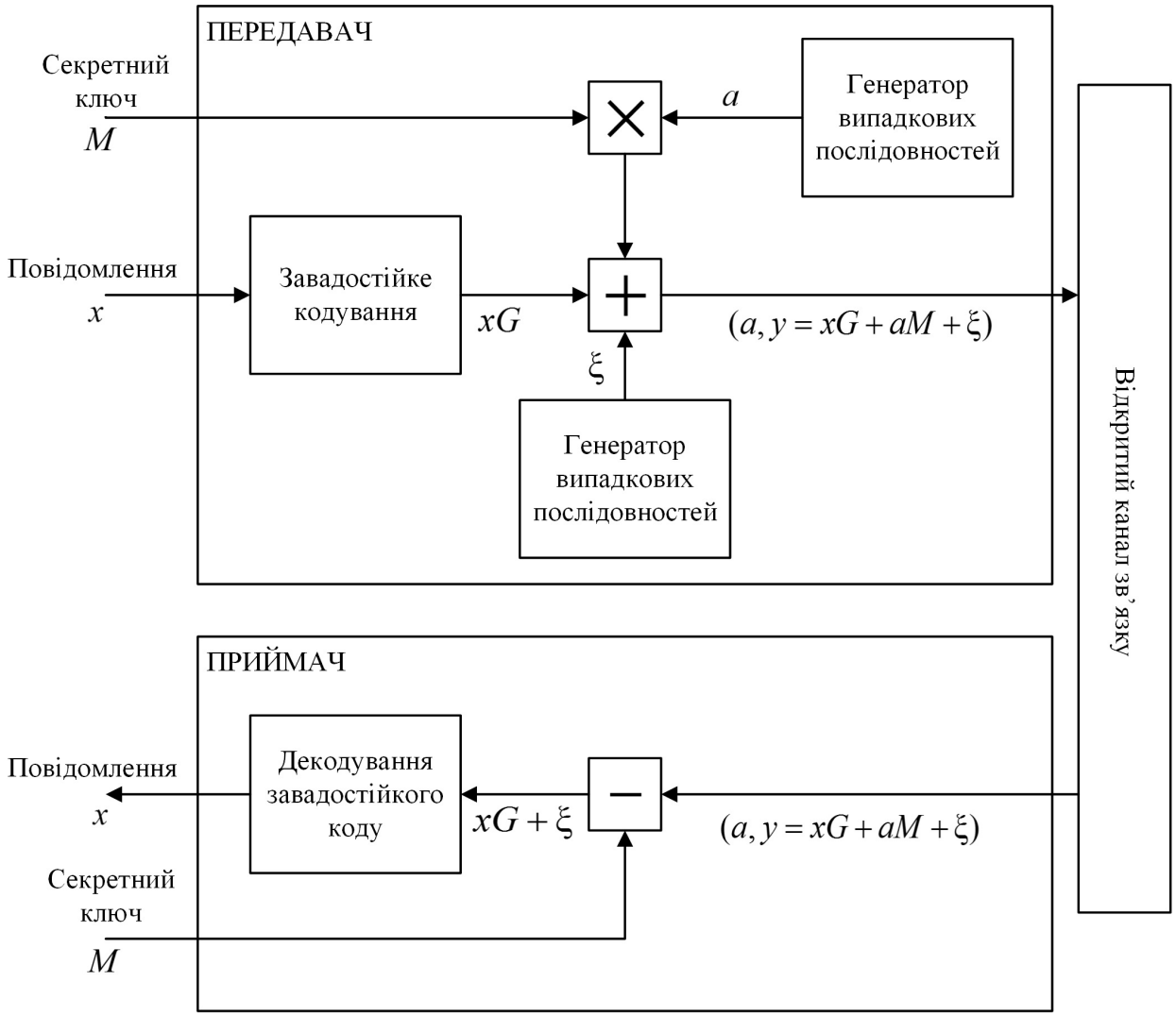

Рисунок 4.2. Схема конфіденційної передачі повідомлень за допомогою шифросистеми LPN-C

В табл. 4.3 наведено результати оцінювання часової складності та обсягу матеріалу, потрібного для розв'язання L систем вигляду (4.31) над кільцем $R = R_N$ за допомогою узагальненого алгоритму BKW та послідовного методу відповідно (зауважимо, що при $N = 1$ останній метод по суті зводиться до виконання узагальненого алгоритму).

Значення параметрів n, K, L, t в табл. 4.3 взяті з роботи [8], де їх запропоновано використовувати для побудови шифросистем LPN-C над полем з двох елементів. Параметри $\log T_{\mathrm{BKW}}$ та $\log m$ у табл. 4.3 позначають двійкові логарифми часової складності та, відповідно, обсягу матеріалу, потрібного для розв'язання усіх СР (4.31) із достовірністю не менше ніж $1 - \delta = 0{,}99$; для їх обчислення використано формули (2.30) – (2.38).

Для обчислення трудомісткості послідовного методу використані результати підрозділів 4.1 і 2.2.

Нагадаємо, що при застосуванні цього методу (для тривіальної композиції числа $N = \underbrace{1 + \cdots + 1}_{N}$, $N \geq 2$) за вхідною СР вигляду (2.1) будуються дві нові системи рівнянь: вигляду (4.7) та (4.10) відповідно. Перша з них є системою рівнянь зі спотвореними правими частинами над полем $\mathbf{Z}_2$; при цьому на підставі твердження 4.1 та рівностей (4.32) закон спотворень у правих частинах її рівнянь має такий вигляд:

$$p(1) = 1 - p(0) = 1/2 \cdot (1 - \varepsilon), \tag{4.34}$$

де ε визначається за формулою (4.33) при $q = 2^N$. Друга система будується над кільцем R_{N-1}; при цьому закон розподілу спотворень у правих частинах її рівнянь має вигляд (4.32) при $q = 2^{N-1}$, де ε визначається за формулою (4.33), але при $q = 2^N$. Цю систему рівнянь можна розв'язувати далі, будуючи нові СР вигляду (4.7) та (4.10) і т.д.

Таблиця 4.3

Порівняння ефективності атак на шифросистеми LPN-C над кільцями лишків за модулем 2^N

N	n	K	L	t	$\log T_{\text{BKW}}$	$\log m$	$\log T'$	$\log m'$
1	512	27	80	10	134,07	122,11	134,07	122,11
4	512	27	80	10	412,31	400,94	136,07	122,11
8	512	27	80	10	793,27	782,03	137,07	122,11
16	512	27	80	10	1550,81	1536,54	138,07	122,11
1	512	42	160	5	124,57	111,45	124,57	111,45
4	512	42	160	5	408,31	395,92	126,57	111,45
8	512	42	160	5	789,97	777,73	127,57	111,45
16	512	42	160	5	1551,81	1536,72	128,57	111,45
1	768	53	80	4	165,94	154,69	165,94	154,69
4	768	53	80	4	572,46	561,24	167,94	154,69
8	768	53	80	4	1115,53	1103,39	168,94	154,69
16	768	53	80	4	2206,81	2192,80	169,94	154,69
1	768	99	160	8	167,03	154,78	167,03	154,78
4	768	99	160	8	573,56	561,33	169,03	154,78
8	768	99	160	8	1116,61	1103,87	170,03	154,78
16	768	99	160	8	2207,92	2192,47	171,03	154,78
1	768	75	160	12	169,79	157,54	169,79	157,54
4	768	75	160	12	574,90	562,67	171,79	157,54
8	768	75	160	12	1116,69	1104,23	172,79	157,54
16	768	75	160	12	2207,93	2193,04	173,79	157,54

Таким чином, послідовний метод розв'язання СР вигляду (4.31) складається з N кроків, на кожному з яких формується система з m лінійних рівнянь від n невідомих над полем $\mathbf{Z}_2$, закон розподілу спотворень у правих частинах яких має вигляд (4.34), де ε визначається за формулою (4.33) при $q = 2^N$. Звідси на підставі тверджень 4.2, 4.3 і А.2 випливає такий результат.

Твердження 4.4. Нехай існує алгоритм $\mathbf{A}$, який для довільних $\varepsilon \in (0,1)$, $\delta \in (0,1/2)$ і $n \in \mathbf{N}$ розв'язує з достовірністю не менше ніж $1-\delta$ будь-яку систему з $m = m(n,\varepsilon,\delta)$ лінійних рівнянь зі спотвореними правими частинами від n невідомих над полем $\mathbf{Z}_2$ і законом розподілу спотворень (4.34), використовуючи $T(n,\varepsilon,\delta)$ двійкових операцій. Тоді існує атака на

шифросистему LPN-C з параметрами L, K, t, n над кільцем R_N, яка дозволяє відновити ключ з достовірністю не менше ніж $1-\delta$, використовуючи не більше ніж

$$T' = NL \cdot \left(T\left(n, 1 - \frac{2^N t}{L(2^N - 1)}, \delta N^{-1} L^{-1} \right) + 2(n+1)m(C_{\times}(N) + C_{+}(N)) \right) \quad (4.35)$$

двійкових операцій та

$$m' = m\left(n, 1 - \frac{2^N t}{L(2^N - 1)}, \delta N^{-1} L^{-1} \right) \quad (4.36)$$

зашифровувань, де $C_{\times} = N(6N-5)$, $C_{+} = 5(N-1)$.

Значення параметрів T' і m' в табл. 4.3 обчислені за формулами (4.35) і (4.36) відповідно при $\delta = 0{,}01$ за умови, що в ролі **A** використовується узагальнений алгоритм BKW при $N = 1$ (див. підрозділ 2.2).

Як видно з таблиці, при $N \geq 2$ послідовний метод є суттєво більш ефективним (як за трудомісткістю, так і за обсягом матеріалу) в порівнянні з узагальненим алгоритмом BKW. Зокрема, при $N = 4$, $n = 512$, $K = 27$, $L = 80$ і $t = 10$ часова складність відновлення ключа шифросистеми LPN-C за допомогою послідовного методу складає $2^{136{,}07}$, в той час як узагальнений алгоритм BKW потребує $2^{412{,}31}$ операцій. При $N = 16$ та наведених вище значеннях решти параметрів складність послідовного методу дорівнює $2^{138{,}07}$, а складність алгоритму BKW – $2^{1550{,}81}$ (при практично такому ж обсязі матеріалу).

Зауважимо, що згідно з формулою (4.35) і даними табл. 4.3, часова складність послідовного методу майже лінійно залежить від параметра N. Іншими словами, шифросистема LPN-C над кільцем R_N забезпечує майже

таку ж стійкість відносно розглянутої атаки, що і N "паралельно працюючих" шифросистем LPN-C над полем $R_1 = \mathbf{GF}(2)$. Це свідчить про недоцільність використання кілець лишків за модулем 2^N, $N \geq 2$, для побудови шифросистем зазначеного типу.

4.2.3. Оцінювання стійкості симетричної шифросистеми типу Ring-LWE. Розглянемо схему шифрування на рисунку 4.3, яка є окремим випадком частково гомоморфної шифросистеми, запропонованої в [9]. У цій схемі шифрування обчислення здійснюються в кільці $R_{n,q}$ поліномів степеня не вище n з коефіцієнтами з кільця лишків за модулем q. Зашифрування та розшифрування відбуваються за формулами (4.37) та (4.38) відповідно, де обидва значення c_2, $c_2 - c_1 s$ обчислюються в кільці $R_{n,q}$. Коректність розшифрування випливає з того, що за умови (4.37) поліном $c_2 - c_1 s = u + 2e \in R_{n,q}$ співпадає з сумою поліномів u і $2e$ над кільцем $\mathbf{Z}$, оскільки максимальний коефіцієнт цієї суми знаходиться в межах від 0 до $1 + 2(q' - 1) \leq q - 1$. Отже, $D_s(c_1, c_2) = (u + 2e) \bmod 2 = u$.

В [9] проаналізовано стійкість шифросистеми за умови, що q є простим числом, $f(x) = x^n + 1$, де n є степенем двійки таким, що $2n$ ділить $q - 1$, а випадковий поліном e на рисунку 4.3 має дискретний гауссів розподіл ймовірностей. Показано, що в цьому випадку будь-яка атака на шифросистему на основі підібраних відкритих повідомлень може бути обчислювально ефективно трансформована в алгоритм розв'язання задачі Ring-LWE (тобто задачі LPN над кільцем $R_{n,q}$), яка на сьогодні вважається обчислювально складною. Поряд з тим в [9], а також інших доступних публікаціях не наведено оцінок стійкості шифросистем цього типу відносно конкретних атак, що надавало б можливість вибирати їх параметри для забезпечення належного рівня стійкості.

Параметри:

– натуральне число $n > 1$,

– непарне число $q \geq 5$;

– унітарний поліном $f(x)$ над кільцем $\mathbf{Z}_q$, $\deg f(x) = n$;

Множина відкритих повідомлень:

$$U = \{u_0 + u_1 x + \ldots + u_{n-1} x^{n-1} : u_i \in \{0,1\}, i \in \overline{0, n-1}\}.$$

Множина ключів: $R_{n,q} = \mathbf{Z}_q[x]/(f(x))$.

Алгоритм зашифрування. Нехай $u \in U$, $s \in R_{n,q}$; тоді шифротекст, який отримується при зашифруванні відкритого повідомлення u на ключі s, має вигляд

$$E_s(u) = (c_1 = a, c_2 = as + 2e + u), \tag{4.37}$$

де a – випадковий рівноймовірний елемент кільця $R_{n,q}$, e – поліном степеня не вище n, коефіцієнти якого є незалежними випадковими величинами з рівномірним розподілом ймовірностей на множині $\mathbf{Z}_{q'}$, $q' = 1/2 \cdot (q-1)$.

Алгоритм розшифрування. Для відновлення відкритого повідомлення u за шифротекстом (c_1, c_2) за допомогою ключа s слід обчислити

$$D_s(c_1, c_2) = (c_2 - c_1 s) \bmod 2. \tag{4.38}$$

Рисунок 4.3. Опис симетричної шифросистеми Ring-LWE

Отримаємо такі оцінки стійкості для шифросистеми на рисунку 4.3, вважаючи, що супротивник проводить традиційну атаку з підібраним відкритим повідомленням, зашифровуючи m разів на тому ж самому (невідомому) ключі $s \in R_{n,q}$ відкрите повідомлення $u = 0$. В результаті

супротивник отримує систему рівнянь $a_i s + 2e_i = c_{2,i}$, $i \in \overline{1,m}$, над кільцем $R_{n,q}$, яку, враховуючи непарність числа q, можна записати у вигляді

$$\widetilde{a}_i s + e_i = \widetilde{c}_{2,i},\ i \in \overline{1,m}, \tag{4.39}$$

де $\widetilde{a}_i = 2^{-1} a_i$, $\widetilde{c}_{2,i} = 2^{-1} c_{2,i}$, $a_1,...,a_m$ та $e_1,...,e_m$ є незалежними випадковими рівноймовірними елементами кільця $R_{n,q}$ та множини $\mathbf{Z}_{q'}$ відповідно.

Для розв'язання СР (4.39) можна використовувати наступний природний метод. Зафіксуємо число $i \in \overline{1,m}$, для якого елемент $\widetilde{a}_i$ є оборотним в кільці $R_{n,q}$. Далі, перебираючи усі $\left(\frac{q-1}{2}\right)^n$ значень полінома e_i, обчислимо поліном $s = \widetilde{a}_i(\widetilde{c}_{2,i} - e_i)$ та перевіримо для кожного $j \in \overline{1,m} \setminus \{i\}$, чи належать коефіцієнти полінома $e_j = \widetilde{c}_{2,i} - \widetilde{a}_j s$ множині $\mathbf{Z}_{q'}$. Зрозуміло, що трудомісткість такого перебірного методу розв'язання СР (4.39) складає у найгіршому випадку не менше ніж

$$T(n,q) = \left(\frac{q-1}{2}\right)^n \tag{4.40}$$

операцій.

Для розв'язання СР (4.39) можна застосувати також інший відомий метод (див., наприклад, [17]).

Для будь-якого полінома $a = a(x) \in R_{n,q}$ позначимо $M(a)$ матрицю розміру $n \times n$, j-й стовпець якої дорівнює вектору коефіцієнтів полінома $(x^j a(x)) \bmod f(x)$, $j \in \overline{0,n-1}$. Тоді вектор коефіцієнтів полінома $\widetilde{a}_i s$ дорівнює добутку матриці $M(\widetilde{a}_i)$ на вектор-стовпець коефіцієнтів полінома s. Отже, позначаючи останній тим самим символом, отримаємо як наслідок

системи (4.39) систему рівнянь зі спотвореними правими частинами вигляду (2.1) над кільцем $\mathbf{Z}_q$:

$$A_i s + \xi_i = b_i,\ i \in \overline{1,m}, \tag{4.41}$$

де A_i є рядком з номером 0 матриці $M(\widetilde{a}_i)$, b_i – координатою з тим самим номером вектора $\widetilde{c}_{2,i}$, а ξ_i – випадковою величиною, що розподілена рівномірно на множині $\mathbf{Z}_{q'}$. Підкреслимо, що $A_1,...,A_m$ є незалежними випадковими рівноймовірними векторами довжини n над кільцем $\mathbf{Z}_q$, а випадкові величини $\xi_1,...,\xi_m$ є незалежними в сукупності та не залежать від векторів $A_1,...,A_m$.

Для оцінки складності розв'язання СР (4.41) за допомогою одного з найкращих на сьогодні алгоритмів, а саме, узагальненого алгоритму BKW, можна скористатися формулами (2.13), (2.16), (2.30), (2.31). Проте для цього треба знайти розподіл ймовірностей випадкової величини $\eta_k = \xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$. Скористаємося таким твердженням, доведення якого міститься в додатку А.

Твердження 4.5. Справедливі рівності

$$\mathbf{P}(\eta_k = l) = \frac{2^{k/2}}{(q-1)^k q} \sum_{j=0}^{q-1} \frac{\cos(2\pi q^{-1} jl)}{\left(1 + \cos(\pi q^{-1}(q-1)j)\right)^{k/2}}, \tag{4.42}$$

$$\Delta(p_{\eta_k}) \stackrel{\text{def}}{=} q^{-1} \sum_{l=0}^{q-1} (q\mathbf{P}(\eta_k = l) - 1)^2 = \frac{2^k}{(q-1)^{2k}} \sum_{j=0}^{q-1} \frac{1}{\left(1 + \cos(\pi q^{-1}(q-1)j)\right)^k}. \tag{4.43}$$

Зауважимо, що, згідно з формулою (2.28), параметр (4.43) визначає нижню межу кількості рівнянь, які необхідно побудувати на першому етапі узагальненого алгоритму BKW для розв'язання СР (4.41).

Отже, використовуючи формули (2.13), (2.16), (2.30), (2.31) оцінимо часову складність T_{BKW} та обсяг m матеріалу, потрібного для відновлення ключа шифросистеми на рисунку 4.3 за допомогою узагальненого алгоритму BKW (табл. 4.4).

Таблиця 4.4

Характеристики ефективності атак на шифросистему Ring-LWE на основі підібраних відкритих повідомлень ($\delta = 0{,}01$)

n	q	$\log T(n,q)$	$\log T_{\mathrm{BKW}}$	$\log m$
32	37	133,44	75,53	71,94
32	57	153,84	82,66	79,08
32	107	183,29	93,05	89,47
64	71	328,27	130,41	126,82
64	91	351,48	136,97	133,38
64	141	392,27	148,52	144,93
80	121	472,55	165,98	162,07
80	141	490,34	170,67	166,76
80	191	525,59	179,97	176,07
128	131	770,86	245,34	241,01
128	151	797,29	251,75	247,43
128	201	850,41	264,67	260,34
256	257	1791,99	454,04	448,61
256	277	1819,78	459,80	454,37
256	327	1881,27	472,54	467,11

Як видно з таблиці, можливість застосування узагальненого алгоритму BKW є суттєвим фактором для визначення стійкості шифросистеми відносно атак на основі підібраних відкритих повідомлень. Зокрема, при $n = 128$, $q = 151$ складність відновлення ключа шифросистеми шляхом природного перебірного методу є не менше ніж $2^{797,29}$ операцій, в той час як складність узагальненого алгоритму BKW дорівнює $2^{251,75}$. Зі збільшенням параметра n або параметра q виграш у трудомісткості атаки за рахунок застосування

узагальненого алгоритму BKW збільшується (від $2^{55,71}$ при $n=32$, $q=37$ до $2^{1408,73}$ при $n=256$, $q=327$).

В цілому, наведені вище приклади свідчать про можливість практичного застосування розроблених методів до оцінювання чи обґрунтування стійкості сучасних шифросистем, що базуються на складності розв'язання задачі LPN. Розроблені методи також надають можливість безпосередньо вибирати значення параметрів цих шифросистем, виходячи з вимог до їх стійкості відносно відомих атак на основі підібраних відкритих повідомлень.

Висновки

1. Основним науковим результатом розділу є послідовний метод побудови нових алгоритмів розв'язання задачі LPN над кільцем лишків за модулем 2^N за довільною скінченною сукупністю вхідних таких алгоритмів. Цей метод запропоновано вперше і базується на ідеї послідовного розв'язання статистичних задач, що пристосована до розв'язання булевих СР із заважаючими параметрами [2], а також на формальному підході до побудови оптимальних за трудомісткістю обчислювальних алгоритмів, який запропоновано в [3].

2. Суттєву перевагу послідовного методу демонструють отримані оцінки стійкості шифросистем типу LPN-C над кільцем $R_N=\mathbf{Z}/(2^N)$ відносно атак на основі підібраних відкритих повідомлень. Так, послідовний метод відновлення ключа шифросистеми є набагато більш ефективним (як за обчислювальною складністю, так і за обсягом матеріалу) в порівнянні з методом, що базується на застосуванні узагальненого алгоритму BKW. Зокрема, при $N=4$, $n=512$, $K=27$, $L=80$ і $t=10$ часова складність відновлення ключа шифросистеми LPN-C за допомогою послідовного методу складає $2^{136,07}$, в той час як узагальнений алгоритм BKW потребує $2^{412,31}$

операцій. При $N = 16$ та наведених вище значеннях решти параметрів складність послідовного методу дорівнює $2^{138,07}$, а складність алгоритму BKW – $2^{1550,81}$ (табл. 4.3).

В цілому, шифросистема LPN-C над кільцем R_N забезпечує майже таку ж стійкість, що і N "паралельно працюючих" шифросистем LPN-C над полем $R_1 = \mathbf{GF}(2)$. Це свідчить про недоцільність використання кілець лишків за модулем 2^N, $N \geq 2$, для побудови шифросистем зазначеного типу.

3. Отримані результати свідчать про можливість безпосереднього застосування розроблених методів до вирішення задачі оцінювання стійкості потокових шифрів над кільцями лишків відносно кореляційних атак. Зокрема, заміна в схемі генератора гами шифру SNOW 2.0 порозрядного булевого додавання арифметичним додаванням за модулем 2^{32} приводить (за умови належного вибору підстановки σ; див рисунок 4.1) до суттєвого підвищення стійкості шифру відносно відомих кореляційних атак. Найкраща з таких атак на модифіковану версію шифру потребує $2^{302,31}$ операцій та $2^{301,31}$ знаків гами, в той час як найкраща з відомих атак на SNOW 2.0 [7] має обчислювальну складність $2^{164,15}$ та потребує $2^{163,59}$ знаків гами.

4. Розроблені методи розв'язання задачі LPN над кільцем лишків за модулем 2^N із застосуванням швидких перетворень Фур'є або Ферма дозволяють будувати більш ефективні кореляційні атаки на SNOW 2.0-подібні шифри над цим кільцем. Зокрема, застосування швидкого перетворення Ферма зменшує складність звичайної кореляційної атаки на зазначені шифри від $2^{8,24}$ до $2^{28,54}$ разів в залежності від параметрів n та N (табл. 4.2).

5. Можливість застосування узагальненого алгоритму BKW є суттєвим фактором для визначення стійкості постквантових шифросистем типу Ring-LWE відносно атак на основі підібраних відкритих повідомлень. Зокрема, при $n = 128$, $q = 151$ складність відновлення ключа шифросистеми шляхом

природного перебірного методу є не менше ніж $2^{797,29}$ операцій, в той час як складність узагальненого алгоритму BKW дорівнює $2^{251,75}$. Зі збільшенням параметра n або параметра q виграш у трудомісткості атаки за рахунок застосування узагальненого алгоритму BKW збільшується (від $2^{55,71}$ при $n=32$, $q=37$ до $2^{1408,73}$ при $n=256$, $q=327$; табл. 4.4). Це надає можливість цілеспрямовано вибирати значення параметрів шифросистем типу Ring-LWE, виходячи з вимог до їх стійкості відносно відомих атак.

Список використаних джерел у четвертому розділі

1. Балакин Г. В., Никольский Ю. Б. Последовательное применение метода максимума правдоподобия к решению систем уравнений с мешающими параметрами. *Обозрение прикладной и промышленной математики*. 1995. № 3, т. 2. С. 468-476.

2. Гаврилкевич М. В., Солодовников В. И. Эффективные алгоритмы решения задач линейной алгебры над полем из двух элементов. *Обозрение прикладной и промышленной математики*. 1995. № 3, т. 2. С. 400-437.

3. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. *Selected Areas in Cryptography, LNCS, Springer-Verlag*. 2002. Vol. 2295. P. 47-61.

4. Nyberg K., Wallen J. Improved linear distinguishers for SNOW 2.0. *Fast Software Encryption, LNCS, Springer-Verlag*. 2006. Vol. 4047. P. 144-162.

5. Maximov A., Johansson T. Fast computation for large distribution and and its cryptographic application. *Advanced in Cryptology – ASIACRYPT 2005, LNCS, Springer-Verlag*. 2005. Vol. 3788. P. 313-332.

6. Lee J.-K., Lee D.H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks. *Advanced in Cryptology – ASIACRYPT 2008, LNCS, Springer-Verlag*. 2008. Vol. 5350. P. 524-538.

7. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2016/311 (дата звернення: 06.08.2020).

8. Gilbert H., Mattew J.B., Robshaw M.J.B., Seurin Y. How to Encrypt with the LPN Problem. *ICALP, Part 2, LNCS, Springer Verlag*. 2008. Vol. 5126. P. 679-690.

9. Brakerski Z., Vaikuntanathan V. Fully homomorphic encryption from Ring-LWE and security for key dependent messages. *Advanced in Cryptology – CRYPTO 2011, LNCS, Springer-Verlag*. 2011. Vol. 6841. P. 505-524.

10. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии, Москва: МЦНМО, 2004. 470 с.

11. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов : пер. с англ. Москва: Мир, 1979. 535 с.

12. Мину М. Математическое программирование : пер. с фр. Москва: Наука, 1990. 488с.

13. Алексейчук А. Н. Системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2001. № 4. С. 12-19.

14. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра : учебник в 2-х томах, Т. 2, М.: Гелиос АРВ, 2003. 416 с.

15. Олексійчук А. М. Достатня умова стійкості SNOW 2.0-подібних потокових шифрів відносно певних атак зі зв'язаними ключами. *Захист інформації*. 2016. № 3, т. 18. С. 261-268.

16.Vaudenay S. On the Lai-Massey scheme. *Advanced in Cryptology – ASIACRYPT 1999, LNCS, Springer-Verlag*. 1999. Vol. 1716. P. 8-19.

17. Lybashevsky V., Peikert C., Regev O. On ideal lattices and learning with errors over rings. *Advanced in Cryptology – EUROCRYPT 2010, LNCS, Springer-Verlag*. 2010. Vol. 6110. P. 1-23.

18. Алексейчук А. Н., Игнатенко С. М. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над

кольцом вычетов по модулю 2N. Реєстрація, зберігання і обробка даних. 2005. № 1, Т. 7. С. 11-23.

19. Олексійчук А. М., Ігнатенко С. М. Алгоритми оцінювання стійкості SNOW 2.0-подібних потокових шифрів над кільцями лишків відносно кореляційних атак. Радіотехніка. 2018. Вип. 193, С. 28–34.

20. Ігнатенко С. М. Застосування послідовного методу для побудови статистичної атаки на шифросистему LPN-C над кільцем лишків за модулем 2^N. Захист інформації. 2018. № 3, Т. 20. С. 149-154.

21. Kuznetsov A., Potii O., Poluyanenko N., Ihnatenko S., Stelnyk I., Mialkovsky D. Opportunites to minimize hardware and software costs for implementing Boolean functions in stream ciphers. International Journal of Computing. 2019. Vol. 18, Issue 4. P. 443-452.

18. Игнатенко С. М., Алексейчук А. Н. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. VII міжнар. наук.-практ. конф. Київ, 2004. С. 58-59.

22. Игнатенко С. М., Алексейчук А. Н. Итеративный алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю модулю 2^N. Безпека інформації в інформаційно-телекомунікаційних системах: тези доп. VIII міжнар. наук.-практ. конф. Київ, 2005. С. 46-47.

19. Игнатенко С. М., Алексейчук А. Н. Быстрый алгоритм восстановления искаженных линейных рекуррентных последовательностей над кольцом вычетов по модулю 2^N. *Безпека інформації в інформаційно-телекомунікаційних системах*: тези доп. X міжнар. наук.-практ. конф. Київ, 2007. С. 36-37.

20. Алексейчук А. Н., Игнатенко С. М., Конюшок С. Н. Быстрая корреляционная атака на генераторы гаммы над кольцом вычетов по модулю 2^N. *Питання оптимізації обчислень* (ПОО-XXXV): праці міжнар. симп. Україна, Крим, Велика Ялта, смт. Кацивелі, 2009. С. 14-18.

23. Ігнатенко С. М., Олексійчук А. М. Послідовна статистична атака на шифросистему LPN-C над кільцем лишків за модулем 2^N. Безпека інформації в інформаційно-телекомунікаційних системах: тези доп. XX міжнар. наук.-практ. конф. м. Буча Київської обл, 2018. С. 35-36.

ВИСНОВКИ

Протягом останнього часу спостерігається помітне зростання вимог до стійкості криптографічних систем і протоколів. Зокрема, у зв'язку з можливою появою квантових комп'ютерів криптографія переживає етап створення шифросистем, стійких до квантових атак. Таким чином, виникає потреба у шифросистемах, стійкість яких базується на задачах, що є обчислювально складними навіть у моделі квантових обчислень.

Однією з таких задач є задача LPN (learning parity with noise), яка у найбільш загальному випадку полягає в розв'язанні системи лінійних рівнянь зі спотвореними правими частинами та випадковою рівноймовірною матрицею коефіцієнтів над довільним скінченним кільцем. Зазначена задача рівносильна задачі декодування випадкового лінійного коду над кільцем та має важливе значення для криптографії в цілому. Зокрема, відомо чимало конструкцій генераторів псевдовипадкових послідовностей, алгоритмів шифрування, протоколів автентифікації та протоколів узгодження ключів, стійкість яких базується на складності розв'язання задачі LPN над полем з двох елементів або над скінченним полем великого простого порядку. Крім того, до розв'язання цієї задачі зводиться побудова кореляційних атак на деякі потокові шифри. У всіх зазначених випадках практична стійкість відповідних криптосистем і протоколів залежить безпосередньо від часової складності найкращих з відомих алгоритмів розв'язання задачі LPN, причому для випадку симетричних шифросистем допускаються алгоритми розв'язання цієї задачі за умови необмеженої кількості даних (рівнянь у системі).

Не дивлячись на помітний прогрес у розробці швидких (більш ефективних в порівнянні з перебірним) алгоритмів розв'язання задачі LPN над полем з двох елементів або деякими кільцями лишків, питання про існування таких алгоритмів для випадку довільного скінченного кільця R

залишається відкритим. На сьогодні відсутні навіть неасимптотичні оцінки обсягу матеріалу, достатнього для надійного розв'язання задачі LPN над довільним скінченним кільцем. Залишається також не вирішеною задача про неасимптотичну часову складність узагальненого алгоритму BKW, який являє собою природне розширення на випадок довільного скінченного кільця одного з найкращих на сьогодні алгоритмів розв'язання задачі LPN над полем з двох елементів. Як наслідок, стійкість багатьох симетричних шифросистем, які будуються над скінченними кільцями (по аналогії з відомими шифросистемами, що базуються на складності розв'язання класичної задачі LPN над полем $\mathbf{GF}(2)$), залишається не визначеною, що стримує практичне застосування цих шифросистем у сучасних спеціальних інформаційно-телекомунікаційних системах.

В дисертаційній роботі вирішено **актуальну наукову задачу** розробки більш ефективних (в порівнянні з перебірним) методів розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем.

Для вирішення поставленої наукової задачі **використано методи** лінійної алгебри, теорії кодування, теорії ймовірностей та математичної статистики, теорії скінченних кілець і теорії обчислювальних алгоритмів. Чисельні розрахунки на ЕОМ виконувалися з використанням середовища розробки Microsoft Visual Studio 2013 (мова програмування C++) на персональному комп'ютері з процесором Intel(R) Core(TM) i3-6100 CPU @ 3.7GHz та обсягом оперативної пам'яті 4 ГБ на базі 64-розрядної Windows 7 Service Pack 1.

Основні наукові результати, отримані в дисертації.

1. *Вперше* отримано аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем, які узагальнюють аналогічну оцінку, відому для випадку класичної задачі LPN та дозволяють визначити часову складність узагальненого

алгоритму BKW, відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN.

2. Удосконалено метод максимуму правдоподібності розв'язання задачі LPN над скінченними фробеніусовими кільцями на основі використання швидкого перетворення Фур'є, що дозволяє помітно зменшити часову складність розв'язання задачі LPN над фробеніусовими кільцями як за допомогою самого ММП, так і інших алгоритмів, що використовують ММП як допоміжну процедуру.

3. Удосконалено метод максимуму правдоподібності розв'язання задачі LPN над кільцем лишків за модулем 2^N на основі використання числового перетворення Ферма, що надає можливість суттєво зменшити часову складність розв'язання задачі LPN за допомогою узагальненого алгоритму BKW.

4. *Вперше* розроблено метод побудови нових алгоритмів розв'язання задачі LPN над кільцем лишків за модулем 2^N за довільною скінченною сукупністю вхідних таких алгоритмів, що надає можливість підвищити ефективність розв'язання цієї задачі шляхом належного вибору композиції числа N.

Достовірність результатів дисертаційної роботи забезпечується адекватністю припущень, які лежать в основі проведених наукових досліджень, а також коректним застосуванням відомих математичних методів. Результати проведених чисельних розрахунків узгоджуються з отриманими теоретичними висновками.

Значення наукових результатів дисертації для теорії полягає в тому, що вони утворюють наукову основу для отримання обґрунтованих оцінок стійкості симетричних шифросистем, які базуються на складності розв'язання задачі LPN над скінченними кільцями, з метою практичного застосування цих шифросистем у сучасних спеціальних інформаційно-телекомунікаційних системах.

Практичне значення роботи. Розроблено програмні реалізації алгоритмів оцінювання складності розв'язання задачі LPN з використанням запропонованих методів, які дозволяють безпосередньо отримувати науково обґрунтовані оцінки стійкості відповідних симетричних шифросистем над скінченними кільцями.

Крім того, результати дисертаційної роботи дозволяють:

– підвищити ефективність відомих атак на шифросистеми типу Ring-LWE від $2^{55,71}$ до $2^{1408,73}$ разів (в залежності від параметрів шифросистем);

– підвищити ефективність кореляційних атак на SNOW 2.0-подібні потокові шифри над кільцями лишків за модулем 2^N від $2^{8,24}$ до $2^{28,54}$ разів (в залежності від значення N та довжини накопичувача генератора гами);

– будувати SNOW 2.0-подібні потокові шифри над кільцями лишків за модулем 2^N, що є обґрунтовано стійкими відносно відомих кореляційних атак, зокрема, підвищити стійкість шифру SNOW 2.0 з $2^{164,15}$ до $2^{302,31}$ операцій (при збільшенні обсягу потрібного матеріалу з $2^{163,59}$ до $2^{301,31}$) шляхом повної заміни порозрядного булевого додавання у схемі генератора гами додаванням за модулем 2^{32}.

Висновки та рекомендації по науковому та практичному використанню наукових результатів. Отримані в дисертаційній роботі нові наукові та практичні результати мають універсальний характер і можуть бути використані як при створенні нових, так і при дослідженні стійкості відомих симетричних постквантових шифросистем, побудованих на складності розв'язання задачі LPN.

1. Отримані аналітичні оцінки надають можливість визначати за порядком величини фактичний обсяг матеріалу, достатнього для надійного розв'язання задачі LPN над довільним скінченним кільцем. Зокрема, при $\delta = 0{,}01$, $n = 40$, $q = 2^{16}$ і $\varepsilon = 0{,}0025$ з ймовірністю не менше ніж $1-\delta$ достатньо 9675 та необхідно не менше ніж 1075 рівнянь зі спотвореними правими частинами.

2. При $n = 20$, $q = 2^5$ за умови (2.23) верхня оцінка m_1 набуває значень від $2^{23,71}$ до $2^{30,36}$ в залежності від параметра ε. При цьому значення оцінки m_2 є приблизно в 50 разів менше в усьому зазначеному діапазоні зміни ε та перевищують значення відомої нижньої оцінки (2.28) не більше ніж у 3,18 разів. Зі збільшенням числа n значення усіх трьох оцінок збільшуються приблизно на однакову величину, що дорівнює 1,93. Аналогічний характер залежності спостерігається зі збільшенням параметра q при тих самих n і δ.

3. Отримані аналітичні оцінки дозволяють визначити часову складність узагальненого алгоритму BKW, відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN. Зокрема, виграш у трудомісткості узагальненого алгоритму розв'язання СР (2.1) в порівнянні з ММП становить від $2^{124,58}$ до $2^{749,59}$ в залежності від числа n невідомих в системі та параметра ε, який визначає близькість розподілу спотворень у правій частині СР до рівномірного розподілу ймовірностей на кільці. Зі зменшенням ε виграш у трудомісткості змінюється від $2^{156,95}$ до $2^{124,58}$ при $n = 32$ та від $2^{749,59}$ до $2^{677,28}$ при $n = 128$. Це свідчить про помітну перевагу в трудомісткості узагальненого алгоритму BKW в порівнянні з методом максимуму правдоподібності.

4. Застосування швидкого перетворення Фур'є для розв'язання задачі LPN над кільцем лишків за модулем 2^N надає можливість зменшити трудомісткість ММП від $2^{5,80}$ до $2^{42,15}$ разів в залежності від параметра N та числа рівнянь. При цьому застосування швидкого перетворення Ферма дозволяє отримати ще більший виграш у трудомісткості: від $2^{11,18}$ до $2^{47,85}$ разів.

5. Модифікації узагальненого алгоритму BKW, побудовані на основі запропонованих методів, мають меншу часову складність у порівнянні з традиційною версією цього алгоритму. Зокрема, застосування швидкого перетворення Фур'є на другому етапі узагальненого алгоритму BKW

зменшує складність останнього до 2^{754} разів в залежності від числа невідомих в системі та відстані між розподілом спотворень у правих частинах її рівнянь і рівномірним розподілом ймовірностей. При застосуванні швидкого перетворення Ферма виграш змінюється аналогічним чином: від 2^{122} до 2^{754} разів.

6. В цілому, розроблені методи підвищення ефективності розв'язання задачі LPN доцільно використовувати у випадку сильноспотворених систем лінійних рівнянь над кільцями помірного порядку, зокрема, при побудові швидких кореляційних атак на потокові шифри над скінченним кільцями або полями. В цьому випадку зазначені методи дозволяють помітно зменшити часову складність розв'язання задачі LPN як за допомогою самого ММП, так і інших алгоритмів (узагальненого алгоритму BKW), що використовують ММП як допоміжну процедуру.

7. Суттєву перевагу послідовного методу демонструють отримані оцінки стійкості шифросистем типу LPN-C над кільцем $R_N = \mathbf{Z}/(2^N)$ відносно атак на основі підібраних відкритих повідомлень. Так, послідовний метод відновлення ключа шифросистеми є набагато більш ефективним (як за обчислювальною складністю, так і за обсягом матеріалу) в порівнянні з методом, що базується на застосуванні узагальненого алгоритму BKW. Зокрема, при $N = 4$, $n = 512$, $K = 27$, $L = 80$ і $t = 10$ часова складність відновлення ключа шифросистеми LPN-C за допомогою послідовного методу складає $2^{136,07}$, в той час як узагальнений алгоритм BKW потребує $2^{412,31}$ операцій. При $N = 16$ та наведених вище значеннях решти параметрів складність послідовного методу дорівнює $2^{138,07}$, а складність алгоритму BKW – $2^{1550,81}$.

В цілому, шифросистема LPN-C над кільцем R_N забезпечує майже таку ж стійкість, що і N "паралельно працюючих" шифросистем LPN-C над полем $R_1 = \mathbf{GF}(2)$. Це свідчить про недоцільність використання кілець лишків за модулем 2^N, $N \geq 2$, для побудови шифросистем зазначеного типу.

8. Отримані результати свідчать про можливість безпосереднього застосування розроблених методів до вирішення задачі оцінювання стійкості потокових шифрів над кільцями лишків відносно кореляційних атак. Зокрема, заміна в схемі генератора гами шифру SNOW 2.0 порозрядного булевого додавання арифметичним додаванням за модулем 2^{32} приводить (за умови належного вибору підстановки σ) до суттєвого підвищення стійкості шифру відносно відомих кореляційних атак. Найкраща з таких атак на модифіковану версію шифру потребує $2^{302,31}$ операцій та $2^{301,31}$ знаків гами, в той час як найкраща з відомих атак на SNOW 2.0 має обчислювальну складність $2^{164,15}$ та потребує $2^{163,59}$ знаків гами.

9. Розроблені методи розв'язання задачі LPN над кільцем лишків за модулем 2^N із застосуванням швидких перетворень Фур'є або Ферма дозволяють будувати більш ефективні кореляційні атаки на SNOW 2.0-подібні шифри над цим кільцем. Зокрема, застосування швидкого перетворення Ферма зменшує складність звичайної кореляційної атаки на зазначені шифри від $2^{8,24}$ до $2^{28,54}$ разів в залежності від параметрів n та N.

10. Можливість застосування узагальненого алгоритму BKW є суттєвим фактором для визначення стійкості постквантових шифросистем типу Ring-LWE відносно атак на основі підібраних відкритих повідомлень. Зокрема, при $n=128$, $q=151$ складність відновлення ключа шифросистеми шляхом природного перебірного методу є не менше ніж $2^{797,29}$ операцій, в той час як складність узагальненого алгоритму BKW дорівнює $2^{251,75}$. Зі збільшенням параметра n або параметра q виграш у трудомісткості атаки за рахунок застосування узагальненого алгоритму BKW збільшується (від $2^{55,71}$ при $n=32$, $q=37$ до $2^{1408,73}$ при $n=256$, $q=327$). Це надає можливість цілеспрямовано вибирати значення параметрів шифросистем типу Ring-LWE, виходячи з вимог до їх стійкості відносно відомих атак.

11. Основні наукові та практичні результати реалізовані в НДР “Баракуда” та НДР “Самсон”. Вони також можуть бути використані для оцінки стійкості при виборі конкретних постквантових симетричних шифросистем для застосування, в тому числі, і для державних органів. Подальший розвиток наукових ідей та методів, які лежать в основі дисертаційного дослідження, є актуальним напрямом в галузі захисту інформації.

ДОДАТКИ

Додаток А.1 Швидкий алгоритм множення вектора на тензорний степінь матриці над комутативним кільцем

Нехай $\Re$ – довільне комутативне кільце, $H = (h_{ij})_{i,j\in\overline{0,q-1}}$ – матриця порядку q над кільцем $\Re$. Послідовність тензорних (або кронекерових) степенів матриці H визначається рекурсивно за формулами:

$$H^{[1]} = H,$$

$$H^{[n]} = \begin{pmatrix} h_{0,1}H^{[n-1]} & h_{0,2}H^{[n-1]} & \cdots & h_{0,q-1}H^{[n-1]} \\ \ldots & \ldots & \ldots & \ldots \\ h_{q-1,1}H^{[n-1]} & h_{q-1,2}H^{[n-1]} & \cdots & h_{q-1,q-1}H^{[n-1]} \end{pmatrix}, \; n \geq 2. \qquad \text{(A.1)}$$

Природний алгоритм множення вектора $g \in \Re^{q^n}$ на матрицю $H^{[n]}$ потребує порядку q^{2n} операцій додавання та множення в кільці $\Re$. Наступний, більш ефективний алгоритм A_n базується на результатах, викладених в [1], с. 314.

Алгоритм A_n визначається рекурсивно таким чином.

Вхідні дані:

– вектор-стовпець $g = (g_0, \ldots, g_{q-1})^T$, де

$$g_j = (g_{j,1}, \ldots, g_{j,q^{n-1}})^T \in \Re^{q^{n-1}}, \; j \in \overline{0, q-1};$$

– допоміжний алгоритм A множення вектор-стовпців над кільцем $\Re$ на матрицю H.

1. Якщо $n = 1$, то $A_n = A$.

2. Якщо $n \geq 2$, то для обчислення добутку $H^{[n]}g$ потрібно

– обчислити матрицю $F = \begin{pmatrix} f_{0,1} & f_{0,2} & \cdots & f_{0,q^{n-1}} \\ \ldots & \ldots & \ldots & \ldots \\ f_{q-1,1} & f_{q-1,2} & \cdots & f_{q-1,q^{n-1}} \end{pmatrix}$, домножаючи за допомогою алгоритму A кожен стовпець матриці $G = \begin{pmatrix} g_{0,1} & g_{0,2} & \cdots & g_{0,q^{n-1}} \\ \ldots & \ldots & \ldots & \ldots \\ g_{q-1,1} & g_{q-1,2} & \cdots & g_{q-1,q^{n-1}} \end{pmatrix}$ на матрицю H;

– сформувати з рядків матриці F вектор-стовпці $f_i = (f_{i,1}, \ldots, f_{i,q^{n-1}})^T$, $i \in \overline{0, q-1}$ та обчислити вектор $H^{[n]}g = \begin{pmatrix} H^{[n-1]}f_0 \\ H^{[n-1]}f_1 \\ \ldots \\ H^{[n-1]}f_{q-1} \end{pmatrix}$, використовуючи алгоритм A_{n-1}.

Твердження А.1. Для будь-якого натурального n алгоритм A_n обчислює добуток $H^{[n]}g$ за

$$T_q(n) = T_q(1)q^{n-1}n \qquad \text{(А.2)}$$

операцій додавання в кільці $\Re$ та множення елементів цього кільця на елементи матриці H, де $T_q(1)$ – число зазначених операцій, що використовуються в алгоритмі A.

Доведення. Для обґрунтування коректності алгоритму A_n помітимо, що на підставі рівності (А.1)

$$H^{[n]}g = \begin{pmatrix} h_{0,1}H^{[n-1]} & h_{0,2}H^{[n-1]} & \cdots & h_{0,q-1}H^{[n-1]} \\ \ldots & \ldots & \ldots & \ldots \\ h_{q-1,1}H^{[n-1]} & h_{q-1,2}H^{[n-1]} & \cdots & h_{q-1,q-1}H^{[n-1]} \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \\ \ldots \\ g_{q-1} \end{pmatrix} =$$

$$= \begin{pmatrix} H^{[n-1]}\left(\sum_{j=0}^{q-1} h_{0,j}g_j\right) \\ \ldots \quad \ldots\ldots \\ H^{[n-1]}\left(\sum_{j=0}^{q-1} h_{q-1,j}g_j\right) \end{pmatrix}.$$

Крім того, на підставі рівності $F = HG$ маємо $\sum_{j=0}^{q-1} h_{i,j}g_{j,l} = f_{i,l}$, $i \in \overline{0, q-1}$, $l \in \overline{1, q^{n-1}}$. Отже, $\sum_{j=0}^{q-1} h_{i,j}g_j = f_i$ для кожного $i \in \overline{0, q-1}$ і $H^{[n]}g = \begin{pmatrix} H^{[n-1]}f_0 \\ H^{[n-1]}f_1 \\ \ldots \\ H^{[n-1]}f_{q-1} \end{pmatrix}$,

що і треба було довести.

Далі, згідно з означенням алгоритму A_n справедлива рівність $T_q(n) = T_q(1)q^{n-1} + qT_q(n-1)$, $n = 1, 2, \ldots$, причому $T_q(1)$ дорівнює часовій складності алгоритму A. Звідси за допомогою індукції по n отримується формула (А.2). Твердження доведено.

Додаток А.2 Двійкова часова складність арифметичних операцій в деяких кільцях лишків

Розглянемо кільце $R_N = \mathbf{Z}/(2^N)$, елементи якого є N-розрядними двійковими цілими числами, що додаються та множаться за модулем 2^N.

Твердження А.2. Суму та добуток двох елементів кільця R_N можна обчислити, використовуючи не більше ніж $C_+ = 5(N-1)$ та $C_\times = N(6N-5)$ двійкових операцій відповідно.

Доведення. Нехай $a = \sum_{i=0}^{N-1} a_i 2^i$, $b = \sum_{i=0}^{N-1} b_i 2^i$, де $a_i, b_i \in \{0,1\}$, $i \in \overline{0, N-1}$, $s = (a+b) \bmod 2^N = \sum_{i=0}^{N-1} s_i 2^i$. Тоді справедливі рівності [1], с. 231:

$$s_i = a_i \oplus b_i \oplus c_{i-1},\ c_i = (a_i \oplus b_i)c_{i-1} \oplus a_i b_i,\ c_{-1} = 0,\ i \in \overline{0, N-1}. \qquad \text{(A.3)}$$

Помітимо, що для обчислення значень s_0, c_0 достатньо виконати одне додавання за модулем 2 та одне множення, для обчислення значень $s_1, c_1, ..., s_{N-2}, c_{N-2}$ – $3(N-2)$ додавань за модулем 2 та $2(N-2)$ множень, а для обчислення значення s_{N-1} – два додавання за модулем 2. Отже, загальна кількість двійкових операцій, що використовуються, дорівнює $5(N-2)+4 \le 5(N-1)$.

Для обчислення добутку елементів a та b в кільці R_N скористаємося формулою $ab = \sum_{i=0}^{N-1} a_i b 2^i = \sum_{i=0}^{N-1} a_i r_i(b)$, де $r_i(b)$ – циклічний зсув двійкового представлення елемента b на i позицій праворуч [1], с. 236. Таким чином, добуток можна обчислити, використовуючи не більше ніж N команд порівняння розрядів числа a з нулем, N додавань та N циклічних зсувів, що потребує не більше ніж

$$N + N(C_+ + N) \le N + N(5N - 6 + N) + N = N(6N - 5)$$

двійкових операцій.

Твердження доведено.

Аналогічно попередньому доводиться наступне твердження.

Твердження А.3. Суму двох N-розрядних невід'ємних цілих чисел можна обчислити, використовуючи не більше ніж $5N$ двійкових операцій.

Доведення леми 3.2. Позначимо $T(t)$ двійкову часову складність обчислення суми t невід'ємних цілих чисел, кожне з яких не перевищує M. Треба показати, що $T(t) \le 5(t-1)(\log tM + 2)$.

Перш за все, зазначимо, що розрядність (довжина двійкового запису) натурального числа, яке не перевищує M, є не більше ніж $N = \lfloor \log M \rfloor + 1$. Крім того, $T(1) = 0$. Далі за означенням для додавання i N-розрядних натуральних чисел треба виконати $T(i)$ двійкових операцій, а сума цих чисел не перевищує $i2^N$ і, отже, має розрядність не більше ніж $\log(i2^N) + 1$. Звідси на підставі твердження А.3 випливає, що

$$T(i+1) \le T(i) + 5(\log(i2^N) + 1),\ i = 1, 2, \ldots.$$

Таким чином,

$$T(t) \le T(1) + 5\sum_{i=1}^{t-1} (\log(i2^N) + 1) \le 5(t-1)(\log(t2^N) + 1) =$$

$$= 5(t-1)(\log t + N + 1) \le 5(t-1)(\log t + \log M + 2),$$

що і треба було довести.

Наведемо оцінки двійкової складності операцій додавання та зсуву (множення на степінь числа 2) в кільці $\Re_N = \mathbf{Z}/(2^m + 1)$, де $m = 2^{N-1},\ N \ge 2$

Попередньо доведемо два допоміжних твердження.

Лема А.1. Для будь-якого $a \in \Re_N$ число $a' = (a-1) \bmod (2^m + 1)$ можна обчислити, використовуючи не більше ніж $2m+1 = 2^N + 1$ двійкових операцій.

Доведення. Нехай $(a_0, ..., a_{m-1}, a_m)$ є двійковим представленням числа a (при цьому якщо $a_m = 1$, тобто $a = 2^m$, то $a_0 = ... = a_{m-1} = 0$). Визначимо число i_0, вважаючи $i_0 = \min\{i \in \overline{0,m} : a_i = 1\}$, якщо $a \neq 0$; $i_0 = -1$ – в протилежному випадку.

Зрозуміло, що $a' = 2^m$ при $a = 0$. В протилежному випадку двійковий запис числа a має вигляд $(0, 0, ..., 0, 1, a_{i_0+1}, ..., a_m)$. Отже, двійковий запис числа a' має такий вигляд: $(1, 1, ..., 1, 0, a_{i_0+1}, ..., a_m)$. Таким чином, при обчисленні a' треба виконати не більше ніж $m+1$ двійкових операцій для визначення i_0 та ще не більше ніж m операцій для формування результату, якщо i_0 відомо.

Лему доведено.

Лема А.2. Для будь-якого $a \in \overline{1, 2^m - 1}$ число $2^m + 1 - a$ можна обчислити, використовуючи не більше ніж $3m - 2 = 3 \cdot 2^{N-1} - 2$ двійкових операцій.

Доведення. Використовуючи формули (А.3), неважко переконатися в тому, що двійкові розряди числа $b = 2^m + 1 - a$ обчислюються таким чином:

$$b_0 = a_0 \oplus 1,\ c_0 = 0,\ b_i = a_i \oplus c_{i-1},\ c_i = a_i \oplus c_{i-1} \oplus a_i c_{i-1},\ i \in \overline{1, m-1}.$$

Отже, для знаходження числа b достатньо виконати $1 + 3(m-1)$ двійкових додавань та множень. Лему доведено.

Твердження А.4.

1. Суму в кільці $\Re_N$ елементів $a,b \in \Re_N$ можна обчислити, використовуючи не більше ніж $C_+(\Re_N) = 7 \cdot 2^{N-1} + 2$ двійкових операцій.

2. Добуток в кільці $\Re_N$ елемента a на число 2^l, де $l \in \overline{1, 2^N - 1}$, можна обчислити, використовуючи не більше ніж $C_{>>}(\Re_N) = 13 \cdot 2^{N-1}$ двійкових операцій.

Доведення.

1. Як і вище, позначимо $m = 2^{N-1}$, $x' = (x-1) \bmod (2^m + 1)$ для будь-якого $x \in \Re_N$.

Нехай $(a_0,...,a_{m-1},a_m)$ і $(b_0,...,b_{m-1},b_m)$ є двійковими представленнями елементів a і b кільця $\Re_N$ відповідно. Тоді суму $s = (a+b) \bmod (2^m + 1)$ можна обчислити, використовуючи такий алгоритм:

1) якщо $a_m = 1$ (тобто $a = 2^m$), то $s = b'$;

2) якщо $b_m = 1$ (тобто $b = 2^m$), то $s = a'$;

3) інакше обчислимо суму чисел a і b в кільці $\mathbf{Z}$: $a + b = u + 2^m v$, де $u \in \overline{0, 2^m - 1}$, $v \in \{0,1\}$; покладемо $s = u$; якщо $v = 1$, то покладемо $s = u'$.

З леми А.1 і твердження А.3 випливає, що число двійкових операцій, які використовуються на кроках 1), 2) і 3) наведеного алгоритму, не перевищує $1 + (2m+1)$, $1 + (2m+1)$ і $5m + 1 + (2m+1)$ відповідно. Отже, часова складність алгоритму є не вище ніж

$$\max\{1 + (2m+1), 1 + (2m+1), 5m + 1 + (2m+1)\} = 7m + 2$$

двійкових операцій, що й треба було довести.

2. Нехай $l \in \overline{1, 2^N - 1}$ і $(a_0,...,a_{m-1},a_m)$ є двійковими представленнями числа $a \in \Re_N$. Тоді двійкове представлення числа $a_{>>l} = (2^l a) \bmod (2^m + 1)$ можна обчислити, використовуючи такий алгоритм:

1) отримати вектор $(u_0,...,u_{m-1},v_0,\dots,v_{m-1})$ (та пов'язані з ним числа $u = \sum_{i=0}^{m-1} u_i 2^i$ і $v = \sum_{i=0}^{m-1} v_i 2^i$) шляхом циклічного зсуву вектора $(a_0,...,a_{m-1},a_m,0,\dots,0)$ довжини $2m$ на l позицій праворуч;

2) якщо $v = 0$, то покласти $a_{>>l} = u$; інакше – покласти $a_{>>l} = (u + (2^m - 1 - v)) \bmod (2^m + 1)$.

Зрозуміло, що двійкова складність кроку 1) алгоритму дорівнює $2m$, і на підставі леми А.2 двійкова складність кроку 2) не перевищує $m + C_+(\Re_N) + (3m - 2)$. Звідси, згідно з п. 1 твердження А.4, двійкова складність алгоритму не перевищує $2m + (m + (7m + 2) + (3m - 2)) = 13m$.

Твердження доведено.

Доведення твердження 4.5. Перш за все, знайдемо перетворення Фур'є розподілу ймовірностей випадкової величини $\xi = \xi_1$.

Позначимо $\omega = \exp\{2\pi i q^{-1}\}$, де $i^2 = -1$. Тоді

$$\hat{p}_\xi(\alpha) \stackrel{\text{def}}{=} \sum_{j=0}^{q-1} \mathbf{P}(\xi = j)\omega^{-\alpha j} = \frac{2}{q-1} \sum_{j=0}^{q'} \omega^{-\alpha j}, \ \alpha \in \mathbf{Z}_q.$$

Оскільки для ненульового числа α

$$0 = \sum_{j=0}^{q-1} \omega^{-\alpha j} = \sum_{j=0}^{q'} \omega^{-\alpha j} + \sum_{j=q'+1}^{q-1} \omega^{-\alpha j} = \frac{q-1}{2} \hat{p}_\xi(\alpha) + \sum_{j=1}^{q-q'-1} \omega^{-\alpha(j+q')} =$$

$$= \frac{q-1}{2} \hat{p}_\xi(\alpha) + \sum_{j=1}^{q'} \omega^{-\alpha(j+q')} = \frac{q-1}{2} \hat{p}_\xi(\alpha) + \omega^{-\alpha q'} \sum_{j=1}^{q'} \omega^{-\alpha j} =$$

$$= \frac{q-1}{2}\,\hat{p}_{\xi}(\alpha) + \omega^{-\alpha q'}\left(\frac{q-1}{2}\,\hat{p}_{\xi}(\alpha) - 1\right),$$

то

$$\hat{p}_{\xi}(\alpha) = \frac{2}{q-1}\left(\frac{\omega^{-\alpha q'}}{1+\omega^{-\alpha q'}}\right),\ \alpha \in \mathbf{Z}_q \setminus \{0\}. \qquad \text{(A.4)}$$

Крім того,

$$\hat{p}_{-\xi}(\alpha) \stackrel{\text{def}}{=} \sum_{j=0}^{q-1} \mathbf{P}(-\xi = j)\omega^{-\alpha j} = \sum_{j=0}^{q-1} \mathbf{P}(\xi = j)\omega^{\alpha j} = \hat{p}_{\xi}(-\alpha),\ \alpha \in \mathbf{Z}_q. \qquad \text{(A.5)}$$

Далі, оскільки $\eta_k = \xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, де $\xi_1, ..., \xi_k$ є незалежними випадковими величинами з тим самим законом розподілу, що і ξ, то на підставі теореми про згортку (див., наприклад [2]) та формул (A.4), (A.5) справедливі такі рівності:

$$\hat{p}_{\eta_k}(\alpha) = \left(\hat{p}_{\xi}(\alpha)\right)^{k/2}\left(\hat{p}_{\xi}(-\alpha)\right)^{k/2} = \frac{2^k}{(q-1)^k}\left(\frac{\omega^{-\alpha q'}}{1+\omega^{-\alpha q'}} \cdot \frac{\omega^{\alpha q'}}{1+\omega^{\alpha q'}}\right)^{k/2} =$$

$$= \frac{2^{k/2}}{(q-1)^k}\left(\frac{1}{1+\cos(\pi q^{-1}(q-1)\alpha)}\right),\ \alpha \in \mathbf{Z}_q \setminus \{0\}. \qquad \text{(A.6)}$$

Звідси, використовуючи формулу обернення для перетворення Фур'є і той факт, що значення ймовірності є дійсними числами, отримаємо, що

$$\mathbf{P}(\eta_k = l) = q^{-1}\sum_{j=0}^{q-1} \hat{p}_{\eta_k}(j)\omega^{lj} = \frac{2^{k/2}}{(q-1)^k q}\sum_{j=0}^{q-1} \frac{\omega^{lj}}{\left(1+\cos(\pi q^{-1}(q-1)j)\right)^{k/2}} =$$

$$= \frac{2^{k/2}}{(q-1)^k q} \sum_{j=0}^{q-1} \frac{\cos(2\pi q^{-1} jl)}{\left(1+\cos(\pi q^{-1}(q-1)j)\right)^{k/2}}.$$

Таким чином, справедлива рівність (4.42).

Справедливість рівності (4.43) випливає безпосередньо з формули (А.6) та рівності Парсеваля (див., наприклад, [2]):

$$\Delta(p_{\eta_k}) = \sum_{\alpha \neq 0} |\hat{p}_{\eta_k}(\alpha)|^2 = \frac{2^k}{(q-1)^{2k}} \sum_{j=0}^{q-1} \frac{1}{\left(1+\cos(\pi q^{-1}(q-1)j)\right)^k}.$$

Таким чином, твердження доведено.

Список використаних джерел в Додатку А

1. Сэвидж Дж. Э. *Сложность вычислений*, пер. с англ., М.: Факториал, 1998, 368 с.

2. Wood J.A. Duality for modules over finite rings and application to coding theory, *American Journal of Mathematics*, 1999. Vol. 121, P. 555-575.

Додаток Б Програмний код реалізації послідовного методу розв’язання системи рівнянь зі спотвореними правими частинами над кільцем $\mathbf{Z}/32$

Програмна реалізація послідовного методу розв’язання СР виконана на ПК з процесором Intel(R) Core(TM) i3-6100, 3.7GHz та обсягом оперативної пам’яті 4 ГБ на базі 64-розрядної ОС Windows 7 Service Pack 1. Мова програмування – C++. Середовище розробки – Microsoft Visual Studio 2013.

```
// Файл Posl_Adamar_32.cpp
#include<iostream.h>
#include<time.h>
#include<stdio.h>
#include<stdlib.h>
#include<math.h>
#include<dos.h>
#include<string.h>
#include <sys/timeb.h>

int fun_mod(int z,int x);
int* b_adam(int* sss);
int* fun_sort(int *p,int s);
int rand_my(int r1);
int fun_(int zz);
int *gps2;
int n,i;
int NN;

int main(int argc,char *argv[])
{
clock_t h,hh,hhh,h2;
double hhhh=0.0;
float ver;
int k,j,l,nn;
long d,ggg,jjj=0;
int   t;
int flag=0;
FILE *fp,*tp;
int max;
int *nz;
int *lrr;
int *x1;
int *fun;
int **s1;
int **si;
int **mat;
int *b;
int *bi;
int *g;
int *x0;
int *gps;
int *prov;
unsigned short data1;
struct _timeb timebuffer;
char *timeline;
int r1;
int s,s4,ind;
```

```
int b3[5]= {0};
int osh[5]={0};
int u1[3]= {1,0,1};
int u2[4]= {1,0,0,1};
int u3[5]= {1,0,0,1,0};
int u4[6]= {1,0,0,0,0,1};
int u5[7]= {1,0,0,0,0,0,1};
int u6[8]= {1,0,0,0,1,1,1,0};
int u7[9]= {1,0,0,0,0,1,0,0,0};
int u8[10]={1,0,0,0,0,0,0,1,0,0};
int u9[11]={1,0,0,0,0,0,0,0,0,1,0};

char sss[12];
float pp[32];
float raspr[5]={0.0};
int  nn2[32];

if(argc!=2)
{
 printf("USE: Posl_Adamar_32.EXE FILE_TXT");
 exit(1);
}
fp=fopen(argv[1],"rb+");
 strcpy(sss,argv[1]);
    sss[9]='p'; sss[10]='s';  sss[11]='l';
tp=fopen(sss,"wb+");
cout<< "Enter the number of variables (2<n<12): ";
cin >>n;
printf("Enter the number of equqtions (t<%d):",(int)pow(2,n)-1);
cin >>t;
cout<<"Enter the number of times the program is run:";
cin>>nn;
fprintf(tp,"\nThe program was run %d times with the following parameters:",nn);
fprintf(tp,"\nn= %d\nt= %d",n,t);
d=0;
NN=5;
for(i=0;i<32;i++)
 nn2[i]=0;

while((i=fgetc(fp))!=EOF)
{
          j=i%32;
          d+=1;
          nn2[j]++;
}
fseek(fp,0,SEEK_SET);

for(i=0;i<32;i++)
{
 pp[i]=(float)nn2[i]/(float)d;
 if(pp[i]==0.0)            pp[i]=(float)0.000001;
}

fprintf(tp,"\nPlaintext statistic is:");
for(i=0;i<32;i++)
  fprintf(tp,"\np(%d)=%f%",i,pp[i]);

for(i=0;i<32;i++)
{
          if(i%2)    raspr[0]+=pp[i];
          if(i>=16) raspr[4]+=pp[i];
          if(i>=8 && i<=15) raspr[3]+=pp[i];
          if(i>=24) raspr[3]+=pp[i];
}
```

```
raspr[1]=pp[2]+pp[3]+pp[6]+pp[7]+pp[10]+pp[11]+pp[14]+pp[15]+pp[18]+pp[19]+pp[22]+pp[23]+
pp[26]+pp[27]+pp[30]+pp[31];
raspr[2]=pp[4]+pp[5]+pp[6]+pp[7]+pp[12]+pp[13]+pp[14]+pp[15]+pp[20]+pp[21]+pp[22]+pp[23]+
pp[28]+pp[29]+pp[30]+pp[31];

fprintf(tp,"\nError distribution is:");
for(i=0;i<5;i++)
          fprintf(tp,"\n%d-j blank: %f",i,raspr[i]);

fseek(fp,0,SEEK_SET);

s1=new int*[n];
for(i=0;i<n;i++)
 { s1[i]=new int[n]; }
si=new int*[n];
for(i=0;i<n;i++)
 { si[i]=new int[n]; }
mat=new int*[t];
for(i=0;i<t;i++)
 { mat[i]=new int[n]; }
nz=new int[n];
lrr=new int[n];
fun=new int[n];
b=new int[t];
g=new int[t];
bi=new int[t];
x0=new int[n];
x1=new int[t];
gps=new int[(int)pow(2,n)];
gps2=new int[(int)pow(2,n)];
prov=new int[n];

_ftime( &timebuffer );
timeline = ctime( & ( timebuffer.time ) );
data1=timebuffer.millitm;
srand(data1);
r1=rand();
r1=1048;

for(ggg=0;ggg<nn;ggg++)
{
flag=0;
printf("\n\nProgram runs for the %d-nd time\n",ggg+1);
fprintf(tp,"\n\nProgram runs for the %d-nd time\n",ggg+1);
for(i=0;i<5;i++)  b3[i]=0;
k=0;

for(i=0;i<n;i++)
 {
          r1=rand_my(r1);
          nz[i]=fun_(r1%32);
 }

 for(i=0;i<n;i++)
  { lrr[i]=0; fun[i]=0; }
  fun[0]=1;

switch(n)  {
   case 3: for(i=0;i<n;i++)  lrr[i]=u1[i];          break;
   case 4: for(i=0;i<n;i++)  lrr[i]=u2[i];          break;
   case 5: for(i=0;i<n;i++)  lrr[i]=u3[i];          break;
   case 6: for(i=0;i<n;i++)  lrr[i]=u4[i];          break;
   case 7: for(i=0;i<n;i++)  lrr[i]=u5[i];          break;
   case 8: for(i=0;i<n;i++)  lrr[i]=u6[i];          break;
```

```
   case 9: for(i=0;i<n;i++)  lrr[i]=u7[i];           break;
   case 10:for(i=0;i<n;i++)  lrr[i]=u8[i];           break;
   case 11:for(i=0;i<n;i++)  lrr[i]=u9[i];           break;
   default: printf("Wrong parameters");     exit(1);
           }
printf(" nz=");
fprintf(tp,"H3: ");
for(i=0;i<n;i++)
 { printf ("%d ",nz[i]);
   fprintf(tp,"%d ",nz[i]); }
 printf("\nlrr=");     fprintf(tp,"\nf(x)= ");
 for(i=0;i<n;i++)
  { printf("%d ",lrr[i]);
    fprintf(tp,"%d ",lrr[i]); }
  printf("\nfun=");
 for(i=0;i<n;i++)
 { printf("%d ",fun[i]); }

for(i=0;i<t;i++)
{
          for(j=0;j<n;j++)
          {
              r1=rand_my(r1);
              mat[i][j]=fun_(r1%32);
          }
}

for(i=0;i<t;i++)
 { k=0;
  for(j=0;j<n;j++)
   {
    k=((mat[i][j]*nz[j])+k)%(int)pow(2,NN);  }
    b[i]=k;
 }

 for(i=0;i<t;i++)
  g[i]=0;
 for(i=0;i<5;i++)
  b3[i]=0;

ver=0;
int jkl;
for(i=0;i<t;i++)
{
          for(jkl=0;jkl<10;jkl++)  j=fgetc(fp)%32;
          bi[i]=(b[i]+j)%32;
}

fprintf(tp,"\n");
for(i=0;i<t;i++)
 {
   fprintf(tp,"|");
   for(j=0;j<n;j++)
    {
     fprintf(tp,"%2d",mat[i][j]);
    }
   if(i==ceil(t/2))
    { fprintf(tp,"| * "); }
   else
    { fprintf(tp,"|   "); }
   if(i<n)
    fprintf(tp,"|X%d|",i+1);
   else
    { for(j=0;j<4;j++)
```

```
    fprintf(tp," "); }
   if(i==ceil(t/2))
    fprintf(tp,"  =  |%2d|   |%2d|\n",b[i],bi[i]);
   else
    fprintf(tp,"     |%2d|   |%2d|\n",b[i],bi[i]);
 }

for(i=0;i<t;i++)
{ b[i]=bi[i]; bi[i]=0; x1[i]=0; g[i]=(b[i])%2; }

for(i=0;i<n;i++)   lrr[i]=0;
hh=clock();

for(int zz=0;zz<NN;zz++)
{
max=t;
for(j=0;j<n;j++)    prov[j]=0;
for(i=0;i<pow(2,n);i++)
{
          for(j=n-1,k=0;j>=0;j--,k++)
          {
                    if(i & (int)pow(2,j)) x0[k]=1;
                    else x0[k]=0;
          }
for(l=0;l<t;l++)
   {
    k=0;
    for(j=0;j<n;j++)
     {
              s=((mat[l][j])%2)*x0[j];
              k=(k+s)%2;
     }
    x1[l]=k;
   }

 s4=0;
 for(l=0;l<t;l++)
 {
           if((x1[l]+g[l])%2==1) s4++;
 }


 if(s4<max)  {
           max=s4;
           for(j=0;j<n;j++) prov[j]=x0[j];
                    }
}

fprintf(tp,"\nFound solution (Z/2): ");
 for(i=0;i<n;i++)   fprintf(tp," %d",prov[i]);
ind=0;
for(i=0;i<n;i++)
{
          if(prov[i]==fun_mod(zz,nz[i])) ind++;
}
if(ind==n)    { fprintf(tp,", MATCHS with the true "); }
else
{
          fprintf(tp,"\nTrue solution for this binary digit is:");
          for(j=0;j<n;j++)
              fprintf(tp,"%d ",fun_mod(zz,nz[j]));
          osh[zz]++;
          break;
}
```

```
for(l=0;l<n;l++)
 lrr[l]=(lrr[l]+(prov[l]*(int)pow(2,zz)));

if(zz!=NN-1)
{
for(i=0;i<t;i++)     /* Ax0 */
 { k=0;
  for(j=0;j<n;j++)
   {
     k=(mat[i][j]*lrr[j]+k)%(int)pow(2,NN);
  }
     x1[i]=k;
 }

for(i=0;i<t;i++)     /* e0  */
 { k=0;
  for(j=0;j<n;j++)
   { k=((mat[i][j])%2*prov[j]+k)%2; }
     bi[i]=(bi[i]+((k+g[i])%2)*(int)pow(2,zz))%(int)pow(2,NN);
}

for(i=0;i<t;i++)     /* Ax0 + e0 */
 {   x1[i]=(x1[i]+bi[i])%(int)pow(2,NN); }


for(i=0;i<t;i++)     /* (Ax0 + e0)i+1 */
  {  x1[i]=(fun_mod(zz+1,x1[i])); }


for(i=0;i<t;i++)     /* bi=bi+(Ax0 + e0)i+1 */
  { g[i]=(x1[i]+fun_mod(zz+1,b[i]))%2;  }

         }
}

if(flag==0)   h=clock();
hhh=h-hh;
hhhh=hhhh+hhh;
printf("\n");
fprintf(tp,"\n");
for(i=0;i<n;i++)
{ printf(" %d",lrr[i]); fprintf(tp," %d",lrr[i]); }
printf(" – found initial state ");
printf("\n");
fprintf(tp," - found initial state ");
fprintf(tp,"\n");
for(i=0;i<n;i++)
{  printf(" %d",nz[i]);  fprintf(tp," %d",nz[i]); }
printf(" - true initial state ");
fprintf(tp," – true initial state ");
   k=0;
for(i=0;i<n;i++)
 if(lrr[i]==nz[i]) k++;
if(k==n)   jjj++;

}
h2=clock();
printf("\nCommon time solving systems of equations: %1.f seconds",(hhhh/CLK_TCK));
printf("\nFrom %d true initial state: %d",nn,jjj);
fprintf(tp,"\n\nCommon time solving systems of equations: %1.f seconds",(hhhh/CLK_TCK));
fprintf(tp, "\nFrom %d true initial state: %d",nn,jjj);
hhhh=h2;
printf("\nCommon time working program: %1.f seconds",hhhh/CLK_TCK);
fprintf(tp,"\n Common time working program: %1.f seconds",hhhh/CLK_TCK);
```

```
fprintf(tp,"\nError distribution by digits:");
for(j=0;j<5;j++)
          fprintf(tp,"\n %d - %d",j,osh[j]);
return 0;
}
int fun_mod(int z,int x)
{
  int c;
  int vsp=x;
  if(z==0)
   { c=vsp%2; }
  else
  {
   for(int jj=NN-1;jj>=z;jj--)
    {
     if(vsp>=pow(2,jj))
      {
        vsp-=(int)pow(2,jj);
             c=1;
      }
     else  { c=0; }
    }
  }
return c;
}
int* b_adam(int* sss)
{int ee,qq;
 int tt;
 for(qq=n-1,ee=0;qq>=0;qq--,ee++)
  {
   for(int rr=0,tt=0;rr<pow(2,ee);tt+=(int)pow(2,qq+1),rr++)
    {
     for(int ww=0;ww<pow(2,qq);ww++)
      {
       int z1=sss[ww+tt]+sss[ww+tt+(int)pow(2,qq)];
       int z2=sss[ww+tt]-sss[ww+tt+(int)pow(2,qq)];
       sss[ww+tt]=z1;
       sss[ww+tt+(int)pow(2,qq)]=z2;
      }
    }
  }
 return sss;
}
int *fun_sort(int *p,int s)
{
 int i,j;
 int per,per2,per3;
 for(i=0;i<pow(2,n);i++)
  gps2[i]=i;
 for(i=s-1;i>=0;i--)
  {
   for(j=i;j>=0;j--)
    {
     per=i;
     if(p[per]>=p[j])
      {
       per2=p[j];   per3=gps2[j];
       p[j]=p[per]; gps2[j]=gps2[per];
       p[per]=per2; gps2[per]=per3;
      }
   }
  }
  return p;
}
```

```
int rand_my(int r1)
{
          int r;

          r=(2416*r1+374441)%1771875;

          return r;
}

int fun_(int zz)
{
 if(zz<0)
  zz=zz+32;
return zz;
}
```

Додаток В Програмний код реалізації модифікації ММП розв'язання систем рівнянь зі спотвореними правими частинами над кільцем $\mathbf{Z}/32$ з використанням алгоритму числового перетворення Ферма

Програмна реалізація модифікації ММП розв'язання СР виконана на ПК з процесором Intel(R) Core(TM) i3-6100, 3.7GHz та обсягом оперативної пам'яті 4 ГБ на базі 64-розрядної ОС Windows 7 Service Pack 1. Мова програмування – C++. Середовище розробки – Microsoft Visual Studio 2013.

```
// Файл FERMA_Adamar_32.exe
#include<iostream.h>
#include<time.h>
#include<stdio.h>
#include<stdlib.h>
#include<math.h>
#include<string.h>
#include<dos.h>

int fun_(int zz);
unsigned long mod(unsigned long step,unsigned long modal);
int * int_to_str(unsigned val,int *s);
void b_adam32(unsigned long** sss,FILE *sp);
void bpf_st_2(FILE *sp,char erteg);
int n,i,kk;
unsigned long mat_adam[32][32];
unsigned long buferr[32][32];
double bol,lll;
int NN;

main(int argc,char *argv[])
{
clock_t h,hh,hhh,h2;
double hhhh=0.0;

int  nn[32];
long ggg;
double pp[32];
int k,j,l;
int   t,d;
FILE *fp,*tp;
double max;
double min=0.0;
int per=0;
int *nz;
int *lrr;
int *x1;
int *fun;
int **s1;
int **si;
int **mat
int *b;
int *bi;
int *x0;
int nnn;
int u1[3]={1,0,1};
```

```
int u2[4]={1,0,0,1};
int u3[5]={1,0,0,1,0};
int u4[6]={1,0,0,0,0,1};
int u5[7]={1,0,0,0,0,0,1};
int u6[8]={1,0,0,0,1,1,1,0};
int u7[9]={1,0,0,0,0,1,0,0,0};
int u8[10]={1,0,0,0,0,0,0,1,0,0};
int u9[11]={1,0,0,0,0,0,0,0,0,1,0};
char sss[12];

if(argc!=2)
{
 printf("USE: FERMA_Adamar_32.exe FILE_TXT");
 exit(1);
}
fp=fopen(argv[1],"rb+");
strcpy(sss,argv[1]);
sss[9]='f'; sss[10]='r'; sss[11]='m';
tp=fopen(sss,"wb+");
cout<< "Enter the number of variables(2<n<12): ";
cin >>n;
cout<< "Enter the number of equations (t<2^n):";
cin >>t;
cout<<"Enter the number of times the program is run:";
cin>>nnn;
fprintf(tp,"\n The program was run %d times with the following parameters:",nnn);
fprintf(tp,"\nn= %d\nt= %d",n,t);

for(i=0;i<32;i++)
 nn[i]=0;
d=j=0;
NN=5;
while((i=fgetc(fp))!=EOF)
{  if(i>64&&i<91||i>96&&i<123||i==32||i==10||i==13)
    {
     d+=1;
     if(i==32||i==10||i==13)
      {
        if(i==32)
          nn[26]++;
        if(i==10)
          nn[27]++;
        if(i==13)
          nn[28]++;
      }
     else
      {
     if(i>96&&i<123)
        { i-=32; }
     nn[i-65]++;
      }
    }
}
if(d<t)
{
  printf("Filesize is too small for entered number of equations");
  fclose(fp);
  exit(1);
}
max=0.0;
min=0.0;
double maxx=0.0,maxx3;
int maxx2;
for(i=0;i<32;i++)
```

```
 { pp[i]=(float)((float)nn[i]/(float)d);
   if(pp[i]==0.0)  pp[i]=0.000001;
   if(pp[i]>maxx)  { maxx=pp[i];  maxx2=i; }
 }
maxx3=pp[0];
pp[0]=pp[maxx2];
pp[maxx2]=maxx3;

fprintf(tp,"\nPlaintext statistic is:");
for(i=0;i<32;i++)
 { fprintf(tp,"\np(%d)=%f%",i,pp[i]); }


fseek(fp,0,SEEK_SET);
s1=new int*[n];
for(i=0;i<n;i++)
 { s1[i]=new int[n]; }
si=new int*[n];
for(i=0;i<n;i++)
 { si[i]=new int[n]; }
mat=new int*[t];
for(i=0;i<t;i++)
 { mat[i]=new int[n]; }
nz=new int[n];
lrr=new int[n];
fun=new int[n];
b=new int[t];
bi=new int[t];
x0=new int[n];
x1=new int[t];
 for(i=0;i<n;i++)
  { lrr[i]=0; fun[i]=0; }
  fun[0]=1;
unsigned long **massive;
massive=new unsigned long*[32];

for(i=0;i<32;i++)
 { massive[i]=new unsigned long[(int)pow(32,n)];  }

for(i=0;i<32;i++)
{
for(j=0;j<pow(32,n);j++)
{
         massive[i][j]=0;
}}

for(ggg=0;ggg<nnn;ggg++)
{
 for(i=0;i<n;i++)
  { lrr[i]=0; fun[i]=0; }
  fun[0]=1;

switch(n)  {
   case 3: for(i=0;i<n;i++)  lrr[i]=u1[i];           break;
   case 4: for(i=0;i<n;i++)  lrr[i]=u2[i];           break;
   case 5: for(i=0;i<n;i++)  lrr[i]=u3[i];           break;
   case 6: for(i=0;i<n;i++)  lrr[i]=u4[i];           break;
   case 7: for(i=0;i<n;i++)  lrr[i]=u5[i];           break;
   case 8: for(i=0;i<n;i++)  lrr[i]=u6[i];           break;
   case 9: for(i=0;i<n;i++)  lrr[i]=u7[i];           break;
   case 10:for(i=0;i<n;i++)  lrr[i]=u8[i];           break;
   case 11:for(i=0;i<n;i++)  lrr[i]=u9[i];           break;
   default: printf("Wrong parameters");     exit(1);
           }
```

```
printf("\n\nProgram is running %d-nd time\n",ggg+1);
fprintf(tp,"\n\nProgram is running %d-nd time\n",ggg+1);
k=0;

srand((unsigned) time(NULL));
 while(k==0)
 {
 for(j=0;j<n;j++)                /* random initial state */
  { nz[j]=(int)rand()%32;
    if(nz[j]!=0)
    k=k+1; }
   }
fprintf(tp,"\n");
 printf(" nz=");
fprintf(tp,"H3: ");
for(i=0;i<n;i++)
 { printf ("%d ",nz[i]);
   fprintf(tp,"%d ",nz[i]); }
 printf("\nlrr=");     fprintf(tp,"\nf(x)= ");
 for(i=0;i<n;i++)
  { printf("%d ",lrr[i]);
    fprintf(tp,"%d ",lrr[i]); }
  printf("\nfun=");
 for(i=0;i<n;i++)
 { printf("%d ",fun[i]); }
                                 /* memory allocation for S1 */
for(i=0;i<n-1;i++)
for(j=0;j<n;j++)
 s1[i][j]=0;
                                 /* initializing  S1 */
for(i=0,j=1;i<n-1;i++,j++)
 { s1[i][j]=1; }
for(j=0;j<n;j++)
 { s1[n-1][j]=lrr[j]; }
                                 /* memory allocation for Si  */
for(i=0;i<n;i++)
for(j=0;j<n;j++)
 si[i][j]=0;
                                 /* memory allocation for Matrix */
for(i=0;i<t;i++)
 for(j=0;j<n;j++)
  { mat[i][j]=0; }

 for(i=0;i<t;i++)
   b[i]=0;

   for(i=0;i<n;i++)
    { k=0;
     for(j=0;j<n;j++)
      {
       k=((fun[j]*s1[j][i])+k)%(int)(pow(2,NN));
      }
      mat[0][i]=k;
    }

for(i=0;i<n-1;i++)       /* S2 matrix generation */
 {
  for(j=0;j<n;j++)
   {
    si[i][j]=s1[i+1][j];
 } }
for(i=0;i<n;i++)
 { k=0;
```

```
  for(j=0;j<n;j++)
   { k=((s1[n-1][j]*s1[j][i])+k)%(int)(pow(2,NN));}
     si[n-1][i]=k;
 }

for(l=1;l<t;l++)
 {
   for(i=0;i<n;i++)
    { k=0;
     for(j=0;j<n;j++)
      {
       k=((fun[j]*si[j][i])+k)%(int)pow(2,NN);
      }
      mat[l][i]=k;
    }

 for(i=0;i<n-1;i++)       /* Si+1 matrix generation for i+1 step */
 {
  for(j=0;j<n;j++)
   {
    si[i][j]=si[i+1][j];
  } }

  for(i=0;i<n;i++)
   { k=0;
    for(j=0;j<n;j++)
     { k=((si[n-1][j]*s1[j][i])+k)%(int)pow(2,NN); }
       lrr[i]=k;
   }
for(i=0;i<n;i++)
 { si[n-1][i]=lrr[i]; }
}

for(i=0;i<t;i++)
 { k=0;
  for(j=0;j<n;j++)
   {
    k=((mat[i][j]*nz[j])+k)%(int)pow(2,NN);  }
    b[i]=k;
 }

int jkl;
for(i=0;i<t;i++)
 {
  for(jkl=0;jkl<5;jkl++)
         j=fgetc(fp);
  if(j>64&&j<91||j>96&&j<123)
   {
    if(j>96&&j<123)
    j-=32;
    bi[i]=(b[i]+j-65)%32;
   }
  else
   {
  if(j==32)
   {
     bi[i]=(b[i]+26)%32;
   }
  else
  if(j==10)
    {
     bi[i]=(b[i]+27)%32;
   }
  else
```

```
  if(j==13)
  {
     bi[i]=(b[i]+28)%32;
  }
  else  i--;
  }
 }
fprintf(tp,"\n\n");
for(i=0;i<32;i++)
{
for(j=0;j<pow(32,n);j++)
{
          massive[i][j]=0;
}}

int xxx1,xxx;
unsigned long znach, znach1;
hh=clock();
          for(j=0;j<t;j++)
          {
              for(xxx1=0;xxx1<32;xxx1++)
              {
                     znach=0;
                     for(xxx=0;xxx<n;xxx++)
                     {
                     znach1=((xxx1*mat[j][xxx])%32)<<(5*(n-1-xxx));
                     znach+=znach1;
                     }
                     for(i=0;i<32;i++)
                             massive[i][znach]=mod(xxx1*(fun_(bi[j]-i)),16);
              }
          }

b_adam32(massive,tp);
 for(j=0;j<32;j++)
 {
  for(i=0;i<pow(32,n);i++)
  {
          massive[j][i]+=t;
          massive[j][i]=massive[j][i]%65537;
          massive[j][i]/=32;
  }
 }
 for(i=0;i<pow(32,n);i++)
           massive[maxx2][i]=massive[0][i];

 double lambda,sum;
 double ssss=1.0;
 int *ppp;
 ppp=new int[n];
 for(i=0;i<n;i++)   ppp[i]=0;
 min=pow(2,31);
 for(i=0;i<pow(32,n);i++)
 {
   lambda=0.0;
          for(j=1;j<32;j++)
          {
       sum=(double)massive[j][i]*log(pp[0]/pp[j]);
            lambda+=sum;
          }
          if (lambda<min)
          {
              min=lambda;
              ppp=int_to_str(i,ppp);
```

```
          }
 }
h=clock();
hhh=h-hh;
hhhh=hhhh+hhh;
fprintf(tp,"\nFound initial state: ");
for(i=0;i<n;i++)  {fprintf(tp,"%d ",ppp[i]); printf("%d ",ppp[i]); }
fprintf(tp,"function l(x) value: %f",min);
fprintf(tp,"\nTrue initial state:  ");
for(i=0;i<n;i++)  {fprintf(tp,"%d ",nz[i]); printf("%d ",nz[i]);}
fprintf(tp,"\n");   printf("\n");
  max=0;
  for(i=0;i<n;i++)
  {
           if(ppp[i]==nz[i])  max++;
  }
if(max==n)  per++;

}
h2=clock();
fprintf(tp,"\nFrom %d times %d true found initial states\n",nnn,per);
fprintf(tp,"\nTime is %1.f seconds",hhhh/CLK_TCK);
hhhh=h2;
fprintf(tp,"\nCommon time program running is %1.f seconds",hhhh/CLK_TCK);
return 0;
}

int* int_to_str(unsigned val,int *s)
{
          int one;
          int z,rr;
          rr=0;
              for(z=n-1;z>=0;z--)
              {
                     one=val/(int)pow(2,z*5);
                     s[rr]=one;
                     rr++;
                     val=val-(one*(int)pow(2,z*5));
              }
          return s;
}

int fun_(int zz)
{
 if(zz<0)
  zz+=32;
return zz;
}

// Calculating the value of pow(2,step)(mod(pow(2,modal)+1); step>modal
unsigned long mod(unsigned long step,unsigned long modal)
{
unsigned int pp=0;
if(step<(modal+1))
          step=(int)pow(2,step);
else
{
          pp=step/modal;   //n
          step=(int)pow(2,step-pp*modal);//n
          if(pp%2) { step=step*(-1); step+=(int)pow(2,modal)+1; }  //pow(2,n)+1
}
return step;
}
```

```
void b_adam32(unsigned long** sss,FILE *sp)
{int ee,qq;
 int ss;
 unsigned long tt;
 for(qq=n-1,ee=0;qq>=0;qq--,ee++)
  {
   for(int rr=0,tt=0;rr<pow(2,ee*5);tt+=(unsigned long)pow(2,5*(qq+1)),rr++)
    {
     for(int ww=0;ww<pow(2,qq*5);ww++)
      {
           for(ss=0;ss<32;ss++)
               {
                      for(char jk=0;jk<32;jk++)
                      buferr[jk][ss]=sss[jk][ww+tt+(ss<<(5*qq))];
               }
                     for(char jk=0;jk<32;jk++)
                           bpf_st_2(sp,jk);
           for(ss=0;ss<32;ss++)
               {
                      for(char jk=0;jk<32;jk++)
                           sss[jk][ww+tt+(ss<<(5*qq))]=buferr[jk][ss];
               }
           }
    }
  }
}

void bpf_st_2(FILE *sp,char erteg)
{
          unsigned long F[32];
          unsigned long g0,g1;
          int poc,m;
    int ch1,ch2;
          int ch, ch_0,ch_1;
  F[0]=buferr[erteg][0]; F[16]=buferr[erteg][1];
  F[8]=buferr[erteg][2]; F[24]=buferr[erteg][3];
  F[4]=buferr[erteg][4]; F[20]=buferr[erteg][5];
  F[12]=buferr[erteg][6]; F[28]=buferr[erteg][7];
  F[2]=buferr[erteg][8]; F[18]=buferr[erteg][9];
  F[10]=buferr[erteg][10]; F[26]=buferr[erteg][11];
  F[6]=buferr[erteg][12]; F[22]=buferr[erteg][13];
  F[14]=buferr[erteg][14]; F[30]=buferr[erteg][15];
  F[1]=buferr[erteg][16]; F[17]=buferr[erteg][17];
  F[9]=buferr[erteg][18]; F[25]=buferr[erteg][19];
  F[5]=buferr[erteg][20]; F[21]=buferr[erteg][21];
  F[13]=buferr[erteg][22]; F[29]=buferr[erteg][23];
  F[3]=buferr[erteg][24]; F[19]=buferr[erteg][25];
  F[11]=buferr[erteg][26]; F[27]=buferr[erteg][27];
  F[7]=buferr[erteg][28]; F[23]=buferr[erteg][29];
  F[15]=buferr[erteg][30]; F[31]=buferr[erteg][31];

   for(poc=0;poc<16;poc++)
             {
                    ch=poc<<1;  ch1=ch+1;
                      ch2=0;
                           ch_0=ch;   ch_1=ch1;
                           g0=F[ch_0];
                           if(F[ch_1])
                           {
                                  g1=F[ch_1];
                                  F[ch_0]=(g0+g1)%65537;
                                if(g1!=65536)
                                  g1=(g1<<16)%65537;
                                else g1=1;
```

```
                        F[ch_1]=(g0+g1)%65537;
                    }
                    else
                    {
                        F[ch_0]=g0;
                        F[ch_1]=g0;
                    }
        }
for(poc=0;poc<8;poc++)
        {
                ch=poc<<2;  ch1=ch+2;
                for(ch2=0;ch2<2;ch2++)
                {
                        ch_0=ch+ch2;
                        ch_1=ch1+ch2;
                        g0=F[ch_0];

                        if(F[ch_1])
                        {
       g1=(F[ch_1]<<(ch2<<3))%65537;

                         F[ch_0]=(g0+g1)%65537;
                            if(g1!=65536)
                               g1=(g1<<16)%65537;
                            else g1=1;
                               F[ch_1]=(g0+g1)%65537;
                        }
                        else
                        {
                               F[ch_0]=F[ch_1]=g0;
                        }
                }
        }
for(poc=0;poc<4;poc++)
        {
                ch=poc<<3;  ch1=ch+4;
                for(ch2=0;ch2<4;ch2++)
                {
                        ch_0=ch+ch2;   ch_1=ch1+ch2;
                        g0=F[ch_0];
                        if(F[ch_1])
                        {
                         g1=(F[ch_1]<<(ch2<<2))%65537;
                           F[ch_0]=(g0+g1)%65537;
                         if(g1!=65536)
                             g1=(g1<<16)%65537;
                         else g1=1;
                             F[ch_1]=(g0+g1)%65537;
                        }
                        else
                        {
                            F[ch_0]=g0;
                            F[ch_1]=g0;
                        }
                }
        }
for(poc=0;poc<2;poc++)
        {
                ch=poc<<4;  ch1=ch+8;
                for(ch2=0;ch2<8;ch2++)
                {
                        ch_0=ch+ch2;   ch_1=ch1+ch2;
                        g0=F[ch_0];
                        if(F[ch_1])
```

```
                        {
                         g1=(F[ch_1]<<(ch2<<1))%65537;
                         F[ch_0]=(g0+g1)%65537;
                             if(g1!=65536)
                                 g1=(g1<<16)%65537;
                             else g1=1;
                                F[ch_1]=(g0+g1)%65537;
                        }
                        else
                        {
                           F[ch_0]=g0;
                           F[ch_1]=g0;
                        }
                    }
            }
      poc=0;
                    ch=0;  ch1=16;
                    for(ch2=0;ch2<16;ch2++)
                    {
                           ch_0=ch+ch2;
                           ch_1=ch1+ch2;
                           g0=F[ch_0];

                           if(F[ch_1])
                           {
                            g1=(F[ch_1]<<ch2)%65537;
                              F[ch_0]=(g0+g1)%65537;
                            if(g1!=65536)
                                  g1=(g1<<16)%65537;
                            else g1=1;
                                F[ch_1]=(g0+g1)%65537;
                           }
                           else
                           {
                               F[ch_0]=g0;
                               F[ch_1]=g0;
                           }
                    }
               buferr[erteg][0]=F[0];
          for(poc=1;poc<32;poc++)
              buferr[erteg][poc]=F[32-poc];
}
```

Додаток Г Акти впровадження наукових результатів кандидатської дисертаційної роботи

“ЗАТВЕРДЖУЮ”

Директор Департаменту СЗР України
доктор технічних наук, доцент

М. Шелест

« 06 » 2008 р.

АКТ
впровадження результатів досліджень дисертаційної роботи
Ігнатенка Сергія Михайловича в науково-дослідній роботі „Сучасні методи аналізу потокових шифрів. Дослідження систем рівнянь зі спотвореннями”
(шифр „Баракуда”)

Комісія у складі голови комісії *Романовича К.О.* та членів комісії: *Дмитрука А.Ю., Смірнова О.Ю.* з’ясувала, що в результаті виконання науково-дослідної роботи „Сучасні методи аналізу потокових шифрів. Дослідження систем рівнянь зі спотвореннями” (шифр „Баракуда”, № держреєстрації 0108U000007д) впроваджені отримані Ігнатенко Сергієм Михайловичем такі наукові результати:

1. *Модифікації методу максимальної вірогідності розв’язання систем лінійних рівнянь із спотвореною правою частиною над кільцем* $\mathbf{Z}/(2^N)$, *що базуються на швидких перетвореннях Фур’є та Ферма допоміжних функцій.*
2. *Нижні оцінки ймовірності правильного відновлення справжнього розв’язку систем лінійних рівнянь із спотвореною правою частиною над кільцем лишків за модулем* 2^N *методом максимальної вірогідності.*
3. *Метод синтезу нових алгоритмів розв’язання систем лінійних рівнянь із спотвореною правою частиною над кільцем лишків за модулем* 2^N, *виходячи з довільної сукупності відомих алгоритмів.*

Зазначені наукові результати дозволяють: при великих значеннях числа невідомих розв’язувати системи лінійних рівнянь із спотвореною правою частиною над кільцем $\mathbf{Z}/(2^N)$ з меншою трудомісткістю (при тій самій надійності) у порівнянні з самим методом максимальної правдоподібності; оцінювати на практиці мінімальну кількість рівнянь, що необхідно для відновлення з потрібною надійністю справжнього розв’язку системи лінійних рівнянь з випадковою рівноймовірною матрицею коефіцієнтів та нижню межу ймовірності відновлення справжнього розв’язку зазначених систем рівнянь з фіксованою лівою частиною; забезпечити “баланс” між надійністю і трудомісткістю алгоритмів розв’язання систем лінійних рівнянь із спотвореною правою частиною над кільцем лишків за модулем 2^N в залежності від конкретної прикладної задачі шляхом належного вибору композиції числа N.

Голова комісії: К.Романович

Члени комісії: А. Дмитрук

О.Смирнов

Прим. №1

“ЗАТВЕРДЖУЮ”
Командир військової частини Р 9000

М. Ємел’яненко

“ 12 ” 12 2017 р.

АКТ
впровадження результатів досліджень дисертаційної роботи Ігнатенка Сергія Михайловича в науково-дослідній роботі “Розробка ефективних алгоритмів вирішення окремих задач криптографічного та стеганографічного аналізу” (шифр “Самсон”) у військовій частині Р 9000

Комісія у складі голови комісії *Острецова І.В.*, та членів комісії *Бредельова Б.А.*, *Кондратенка В.В.* встановила, що у військовій частині Р 9000 при виконанні деяких функціональних задач використовуються наступні результати, отримані Ігнатенком Сергієм Михайловичем в процесі виконання науково-дослідної роботи “Розробка ефективних алгоритмів вирішення окремих задач криптографічного та стеганографічного аналізу” (шифр “Самсон”):

1. Аналітичні оцінки надійності та оптимізовані за обчислювальною складністю модифікації методу максимуму правдоподібності розв’язання систем лінійних рівнянь із спотвореною правою частиною над кільцем $Z/(2^N)$, що базуються на швидких перетвореннях Фур’є та Ферма допоміжних функцій.

2. Метод побудови нових алгоритмів розв’язання систем лінійних рівнянь із спотвореною правою частиною над кільцем $Z/(2^N)$ за довільною скінченою сукупністю вхідних таких алгоритмів.

Зазначені наукові результати дозволяють обчислювати на практиці кількість рівнянь, необхідних для розв’язання систем лінійних рівнянь із спотвореною правою частиною над кільцем $Z/(2^N)$ із заданою надійністю; розв’язувати такі системи рівнянь за менший час (при тій самій надійності) у порівнянні з методом максимуму правдоподібності при великих значеннях числа невідомих; оптимізувати алгоритм розв’язування вказаних систем рівнянь з точки зору трудомісткості та ймовірності правильного розв’язку в залежності від умов конкретної прикладної задачі.

Голова комісії: І. Острецов

Члени комісії: Б. Бредельов

В. Кондратенко

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної
роботи Харківського національного
університету імені В. Н. Каразіна

_____ Микола АЗАРЄНКОВ
20 20 р.

АКТ

про використання результатів кандидатської дисертаційної роботи **Ігнатенка Сергія Михайловича** в навчальному процесі кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна

Комісія у складі: голови комісії – завідувача кафедри безпеки інформаційних систем і технологій, доктора технічних наук, доцента Рассомахіна С.Г. та членів комісії – професора кафедри безпеки інформаційних систем і технологій, доктора технічних наук, професора Кузнецова О.О., професора кафедри безпеки інформаційних систем і технологій, доктора технічних наук, доцента Олійникова Р.В. склала дійсний акт про те, що у навчальному процесі Харківського національного університету імені В.Н. Каразіна впроваджені наступні результати, що одержані Ігнатенком С.М. у процесі виконання його дисертаційної роботи:

1. Розроблені за участю Ігнатенка С.М. лекції «Методи підвищення ефективності розв'язання систем лінійних рівнянь із спотвореними правими частинами над кільцем лишків за модулем 2^N» (дисципліна «Математичні основи проектування та оптимізації інформаційно-комунікаційних систем»), що базуються на результатах, отриманих Ігнатенком С.М. (статті: Игнатенко С.М. Модификация метода максимума правдоподобия решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2007. № 1, т. 9. С. 63-72; Олексійчук А.М., Ігнатенко С.М. Застосування швидкого перетворення Фур'є для розв'язання задачі LPN над скінченними фробеніусовими кільцями. *Захист інформації*. 2017. № 4, т. 19. С. 271-277; Олексійчук А.М., Ігнатенко С.М., Поремський М.В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2017. Вип. 15. С. 150-155.)

2. Розроблене за участю Ігнатенка С. М. практичне заняття «Методи побудови нових алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем лишків за модулем 2^N за довільною скінченною сукупністю вхідних таких алгоритмів» (дисципліна «Математичні основи проектування та оптимізації інформаційно-

комунікаційних систем»). Теоретичною основою практичного заняття є статті: Алексейчук А.Н., Игнатенко С.М. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Реєстрація, зберігання і обробка даних*. 2005. № 1, т. 7. С. 11-23; Ігнатенко С. М. Застосування послідовного методу для побудови статистичної атаки на шифросистему LPN-C над кільцем лишків за модулем 2^N. *Захист інформації*. 2018. № 3, т. 20. С. 149-154.

Голова комісії
завідувач кафедри безпеки інформаційних
систем і технологій
доктор технічних наук, доцент Сергій РАССОМАХІН

Члени комісії:
професор кафедри безпеки інформаційних
систем і технологій
доктор технічних наук, професор Олександр КУЗНЕЦОВ

професор кафедри безпеки інформаційних
систем і технологій
доктор технічних наук, доцент Роман ОЛІЙНИКОВ

Додаток Д СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ КАНДИДАТСЬКОЇ ДИСЕРТАЦІЙНОЇ РОБОТИ

Наукові праці, у яких опубліковано основні наукові результати дисертації у фахових виданнях України:

1. Алексейчук А. Н., Игнатенко С. М. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Реєстрація, зберігання і обробка даних*. 2005. № 1, Т. 7. С. 11-23. *(особистий внесок здобувача - розроблено метод побудови нових алгоритмів розв'язування системи лінійних рівнянь зі спотвореними правими частинами над кільцем лишків по модулю 2^N)*
2. Алексейчук А. Н., Игнатенко С. М. Нижняя граница вероятности восстановления истинного решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2006. № 4, Т. 8. С. 5-12. *(особистий внесок здобувача - отримано аналітичні оцінки числа рівнянь, необхідних для розв'язання зазначених систем із заданою ймовірністю)*
3. Игнатенко С. М. Модификация метода максимума правдоподобия решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N. *Захист інформації*. 2007. № 1, Т. 9. С. 63-72.
4. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2017. Вип. 15. С. 150-155. *(особистий внесок здобувача - отримано оцінку ймовірності відновлення істинного розв'язку системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями з випадковою рівноймовірною матрицею коефіцієнтів)*
5. Олексійчук А. М., Ігнатенко С. М. Застосування швидкого перетворення Фур'є для розв'язання задачі LPN над скінченними фробеніусовими кільцями. *Захист інформації*. 2017. № 4, Т. 19. С. 271-277. *(особистий внесок здобувача - запропоновано модифікацію методу максимуму правдоподібності із застосуванням швидкого перетворення Фур'є для розв'язування задачі LPN над довільним скінченим фробеніусовим кільцем)*
6. Олексійчук А. М., Ігнатенко С. М. Алгоритми оцінювання стійкості SNOW 2.0-подібних потокових шифрів над кільцями лишків відносно кореляційних атак. *Радіотехніка*. 2018. Вип. 193. С. 28 – 34. *(особистий внесок здобувача - проведено розрахунки часової складності узагальненого алгоритму BKW та його модифікацій)*
7. Ігнатенко С. М. Застосування послідовного методу для побудови статистичної атаки на шифросистему LPN-C над кільцем лишків за модулем 2^N. *Захист інформації*. 2018. № 3, Т. 20. С. 149-154.

Наукові праці, в яких опубліковані основні наукові результати дисертації у зарубіжних спеціалізованих виданнях (входить до міжнародної наукометричної бази SCOPUS):

8. Kuznetsov A., Potii O., Poluyanenko N., Ihnatenko S., Stelnyk I., Mialkovsky D. Opportunites to minimize hardware and software costs for implementing Boolean functions in stream ciphers. *International Journal of Computing*. 2019. Vol. 18, Issue 4. P. 443-452. *(особистий внесок здобувача - обґрунтовано критерії та показники ефективності окремих шифросистем)*

Наукові праці, які засвідчують апробацію матеріалів дисертації:

9. Игнатенко С. М., Алексейчук А. Н. Алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю 2^N с использованием быстрого преобразования Ферма // Безпека інформації в інформаційно-телекомунікаційних системах: тези доповідей VI Міжнародної науково-практичної конференції, 13-16 травня 2003р., Київ, 2003. С. 42-43. *(особистий внесок здобувача - запропоновано модифікацію методу максимуму правдоподібності розв'язування систем лінійних рівнянь зі спотвореними правими частинами над кільцем лишків по модулю 2^N із застосуванням числового перетворення Ферма допоміжних функцій)*

10. Игнатенко С. М., Алексейчук А. Н. Метод оптимизации алгоритмов решения систем линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Безпека інформації в інформаційно-телекомунікаційних системах: тези доповідей VII Міжнародної науково-практичної конференції, 12-14 травня 2004р., Київ, 2004. С. 58-59. *(особистий внесок здобувача - розроблено метод побудови нових алгоритмів розв'язування системи лінійних рівнянь зі спотвореними правими частинами над кільцем лишків по модулю 2^N)*

11. Игнатенко С. М., Алексейчук А. Н. Итеративный алгоритм восстановления искаженной линейной рекурренты над кольцом вычетов по модулю модулю 2^N // Безпека інформації в інформаційно-телекомунікаційних системах: тези доповідей VIII Міжнародної науково-практичної конференції, 11-13 травня 2005р., Київ, 2005. С. 46-47. *(особистий внесок здобувача - розроблено алгоритм побудови перевірочних співвідношень малої ваги для знаків лінійної рекурентної послідовності над кільцем лишків по модулю 2^N)*

12. Игнатенко С. М., Алексейчук А. Н. Оценка надежности метода максимума правдоподобия решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю 2^N // Безпека інформації в інформаційно-телекомунікаційних системах: тези доповідей IX Міжнародної науково-практичної конференції, 17-19 травня 2006р., Київ, 2006. С. 29-30. *(особистий внесок здобувача - отримано аналітичні оцінки числа рівнянь, необхідних для розв'язання зазначених систем із заданою ймовірністю)*

13. Игнатенко С. М., Алексейчук А. Н. Быстрый алгоритм восстановления искаженных линейных рекуррентных последовательностей

над кольцом вычетов по модулю 2^N // Безпека інформації в інформаційно-телекомунікаційних системах: тези доповідей IX Міжнародної науково-практичної конференції, 15-18 травня 2007р., Київ, 2007. С. 36-37. *(особистий внесок здобувача - запропоновано процедуру «підйому» поліномів заданої ваги над полем* $\mathbf{GF}(2)$ *до поліномів над кільцем* $\mathbf{Z}/2^N$ *)*

14. Алексейчук А. Н., Игнатенко С. М., Конюшок С. Н. Быстрая корреляционная атака на генераторы гаммы над кольцом вычетов по модулю 2^N // Питання оптимізації обчислень (ПОО-XXXV): праці міжнародного симпозіуму, 24-29 вересня 2009р., Україна, Крим, Велика Ялта, смт. Кацивелі, 2009. С. 14-18. *(особистий внесок здобувача - запропоновано ідею застосування алгоритмів швидкого перетворення Фур'є для зменшення трудомісткості обчислення значень апостеріорної ймовірності на другому етапі «векторної» кореляційної атаки)*

15. Ігнатенко С. М., Олексійчук А. М. Послідовна статистична атака на шифросистему LPN-C над кільцем лишків за модулем 2^N // Безпека інформації в інформаційно-телекомунікаційних системах: тези доповідей IX Міжнародної науково-практичної конференції, 22-24 травня 2018р., Буча Київської обл, 2018. С. 35-36. *(особистий внесок здобувача - проведено розрахунки часової складності узагальненого алгоритму BKW та послідовного методу розв'язання системи рівнянь зі спотвореними правими частинами над кільцем лишків за модулем* 2^N *при застосуванні статистичної атаки на шифросистему LPN-C)*

Наукові праці, які додатково відображають наукові результати дисертації:

16. Алексейчук А. Н., Игнатенко С. М. Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N. *Збірник наукових праць ІПМЕ НАН України*. 2003. Вип. 20, С. 40-48. (*особистий внесок здобувача - отримано оцінку ймовірності правильного відновлення справжнього розв'язку системи лінійних рівнянь зі спотвореними правими частинами над кільцем лишків по модулю* 2^N *з фіксованою матрицею коефіцієнтів методом максимальної правдоподібності*)

17. Ігнатенко С. М. Аналіз кореляційних атак на потокові шифри. *Спеціальні телекомунікаційні системи та захист інформації*. 2008. Вип. 1. С. 55-65.