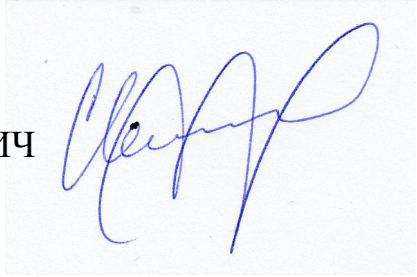
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА

ІГНАТЕНКО СЕРГІЙ МИХАЙЛОВИЧ



УДК 003.26:004.056.55

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

05.13.21 – системи захисту інформації

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2021

Дисертацією є рукопис.

Роботу виконано в Харківському національному університеті імені В. Н. Каразіна Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Кузнецов Олександр Олександрович,
Харківський національний університет імені В. Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій

Офіційні опоненти: доктор технічних наук, старший науковий співробітник
Кудін Антон Михайлович,
Національний технічний університет «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри математичних методів захисту інформації;

доктор технічних наук, професор
Василіу Євген Вікторович,
Одеська національна академія зв'язку імені О. С. Попова, директор навчально-наукового інституту Кібербезпеки, комп'ютерних і радіо технологій, професор кафедри кібербезпеки та технічного захисту інформації.

Захист відбудеться « 22 » квітня 2021 року о 15-00 годині на засіданні спеціалізованої вченої ради Д 64.051.29 Харківського національного університету імені В. Н. Каразіна за адресою: 61022, м. Харків, майдан Свободи, 6, ауд. 234.

З дисертацією можна ознайомитись у Центральній науковій бібліотеці Харківського національного університету імені В. Н. Каразіна за адресою: 61022, м. Харків, майдан Свободи, 4.

Автореферат розісланий « 17 » березня 2021 р.

Учений секретар
спеціалізованої вченої ради Євгенія КОЛОВАНОВА

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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 навіть 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 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, 2007 р.) на замовлення Служби зовнішньої розвідки України та НДР «Самсон» (держреєстрації не підлягає, 2011 р.) 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 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, 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.

Предмет дослідження – методи розв'язання 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 методу максимуму правдоподібності (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), в Службі безпеки України в результаті виконання НДР «Самсон» (акт від 19.12.2017) та в навчальному процесі кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна в рамках викладання дисципліни «Математичні основи проектування та оптимізації інформаційно-комунікаційних систем» (акт від 10.03.2020).

Апробація результатів дисертації. Результати дисертаційних досліджень доповідалися та обговорювалися на 7 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).

Публікації. Основні наукові результати дисертаційної роботи опубліковано в 17 наукових працях: з них 10 наукових статей [1 – 8], [16 – 17] в наукових спеціалізованих виданнях України та інших країн (3 видання індексуються міжнародними наукометричними базами), 7 тез доповідей на наукових та науково-практичних конференціях [9 – 15].

Структура роботи та її обсяг. Дисертація складається з вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел (в кінці кожного розділу основної частини дисертації). Повний обсяг дисертації складає 179 сторінок (7,4 д.а.). Робота ілюстрована 12 таблицями та 15 рисунками. Список використаних літературних джерел містить 142 найменування.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми, сформульовано мету та задачі досліджень, відображено наукову новизну і практичну значимість отриманих результатів, їх впровадження та апробацію.

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 (рисунок 1).

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.

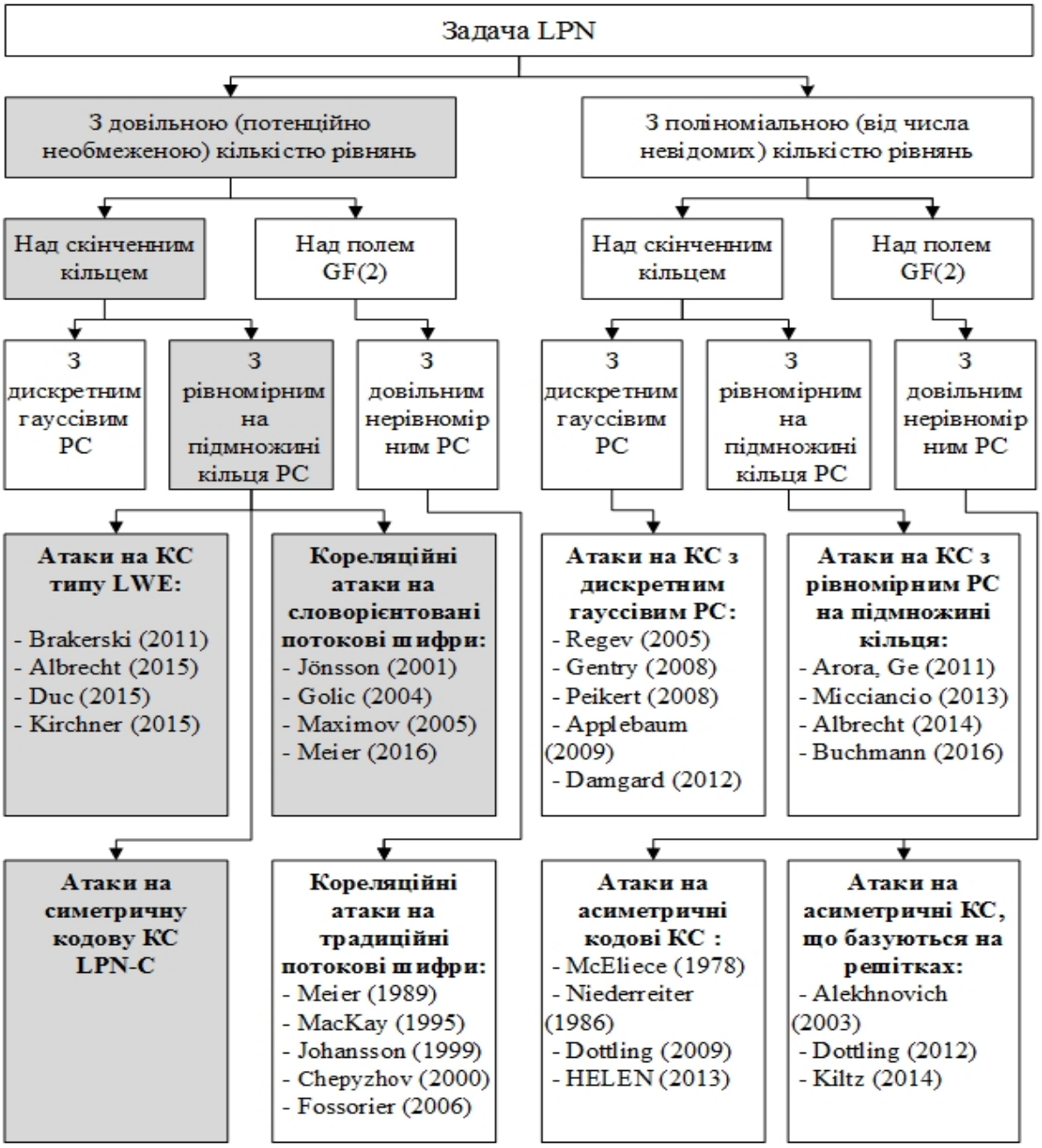


Рисунок 1 – Класифікація задач LPN та атак, що будуються на її основі

При цьому вирішення задач оцінювання стійкості цих шифросистем потребує додаткових досліджень. 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 **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.

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

$$Ax = b, \tag{1}$$

де A – $m \times n$-матриця над кільцем R, b – вектор довжини m з координатами $b_i = A_i a + \xi_i$, $i \in \overline{1,m}$, $A_1, \dots, A_m$ – рядки матриці A, $a = (a_1, \dots, a_n)^{\mathrm{T}}$ – невідомий вектор-стовпець над кільцем R (істинний розв'язок СР (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 $p_\xi = (p(z) : z \in R)$.

Розв'язання СР (1) методом максимуму правдоподібності (ММП) полягає в знаходженні «оцінки» a^* вектора a за правилом $\lambda(a^*) = \max\{\lambda(x) : x \in R^n\}$, де

$$\lambda(x) = \sum_{z \in N_\xi(R)} n(z \mid \varepsilon(x)) \log qp(z), \quad x \in R^n, \tag{2}$$

$N_\xi(R) = \{z \in R : p(z) > 0\}$, $n(z \mid \varepsilon(x))$ – частота зустрічальності елемента z у векторі $\varepsilon(x) = b - Ax$. При цьому часова складність ММП дорівнює

$$T(n) = 2nmq^n. \tag{3}$$

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 $p_{\max} = \max_{z \in R} p(z)$, $p_{\min} = \min_{z \in N_\xi(R)} p(z)$ та припустимо, що $p_{\max} \neq p_{\min}$.

У розділі доведено, що для будь-якого $a \in R^n$ справедлива нерівність

$$\mathbf{P}_{A,\xi}\{a^* = a\} \geq 1 - q^n \exp\left\{ - \frac{m(D(p \,\|\, \omega) + D(\omega \,\|\, p))^2}{2(\log p_{\max} - \log p_{\min})^2} \right\}, \tag{4}$$

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

Доведено також, що ММП надає можливість відновити істинний розв'язок СР (1) з ймовірністю помилки не більше ніж $\delta\in(0,1/2)$, якщо число m рівнянь у системі є не менше ніж

$$m_1=\frac{2n\ln(q\delta^{-1})(\log p_{\max}-\log p_{\min})^2}{(D(p\,\|\,\omega)+D(\omega\,\|\,p))^2}. \tag{5}$$

Окремим науковим результатом розділу є (отримана вперше) наближена оцінка ймовірності $\mathbf{P}\{a^*=a\}$, яка базується на застосуванні центральної граничної теореми і має такий вигляд:

$$\mathbf{P}\{a^*=a\}\ge 1-(\alpha+(q^n-1)\beta), \tag{6}$$

за умови, що число рівнянь у системі (1) є не менше ніж

$$m_2=\left(\frac{u_\alpha\sqrt{D_a}+u_\beta\sqrt{D_x}}{D(p\,\|\,\omega)+D(\omega\,\|\,p)}\right)^2, \tag{7}$$

де $\alpha,\beta>0$, u_α, u_β – квантилі нормального розподілу, що визначаються за формулами $\alpha=\Phi(-u_\alpha)$, $\beta=1-\Phi(u_\beta)$, $\Phi(u)\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u}e^{-\frac{t^2}{2}}dt$, $x\ne a$, $u\in\mathbf{R}$,

$D_a=\sum_{z\in N_\xi(R)} p(z)\log^2(qp(z))-D(p\,\|\,\omega)^2$, $D_x=q^{-1}\sum_{z\in N_\xi(R)}\log^2(qp(z))-D(\omega\,\|\,p)^2$.

Отримані результати проілюстровано на важливому окремому випадку задачі LPN, коли розподіл ймовірностей $p_\xi=(p(z):z\in R)$ визначається за законом $p(0)=q^{-1}(1+(q-1)\varepsilon)$, $p(z)=q^{-1}(1-\varepsilon)$, $z\ne 0$; див. рисунок 2, де для порівняння показана раніше відома нижня оцінка найменшого числа рівнянь у системі (1), для якої існує алгоритм її розв'язання з ймовірністю помилки не більше ніж $\delta\in(0,1/2)$: $m_0=\frac{n(1-\delta)\log q-h(\delta)}{\Delta(p_\xi)}\ln 2$.

Як видно з рисунку 2, верхня оцінка m_1 при $\delta=0{,}01$, $n=20$, $q=2^5$ набуває значень від $2^{23{,}71}$ до $2^{30{,}36}$ в залежності від параметра $\varepsilon\in(0,1)$. 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.

Отримані аналітичні оцінки дозволяють визначати часову складність узагальненого алгоритму BKW, відомий прототип якого є на сьогодні одним з найефективніших алгоритмів розв'язання класичної задачі LPN. Зокрема, показано, що виграш у трудомісткості узагальненого алгоритму розв'язання СР (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.

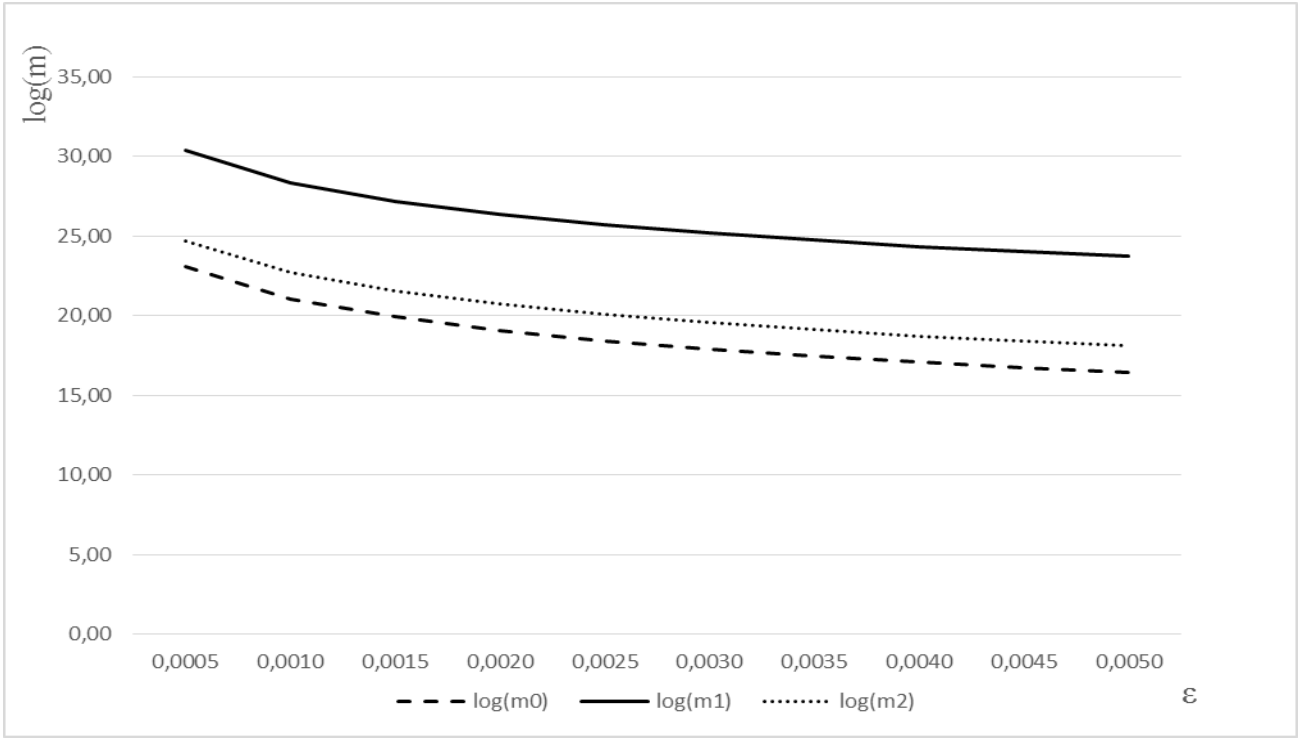


Рисунок 2 – Залежності оцінок обсягу матеріалу в задачі LPN від розподілу спотворень у правих частинах рівнянь системи

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 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. 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.

Швидке перетворення Фур'є або числове перетворення Ферма допоміжної функції застосовуються відповідно при розв'язанні СР (1) над фробеніусовим кільцем або кільцем лишків за модулем 2^N для отримання значень частоти зустрічальності елементів $n(z \mid \varepsilon(x))$ при обчисленні значення (2). Зменшення трудомісткості ММП досягається за рахунок застосування швидкого перетворення Фур'є з використанням алгоритму множення вектора на тензорний степінь матриці над комутативним кільцем. При цьому у першому випадку обчислення проводяться у кільці $\mathbf{Z}[\omega]$, де ω – примітивний корінь степеня l з одиниці, l – характеристика кільця R, а у другому – над кільцем лишків $\Re_N = \mathbf{Z}/(2^{2^{N-1}} + 1)$. Це надає можливість уникнути застосування операцій над числами з плаваючою комою, а отже, забезпечити стовідсоткову точність обчислень.

Отримано аналітичні оцінки двійкової часової складності алгоритмів обчислення всіх значень частоти зустрічальності елементів $n(z \mid \varepsilon(x))$. У випадку застосування швидкого перетворення Фур'є вона не перевищує

$$T_q(n) = 5T_q(1)q^n nl(\log(T_q(1)q^n nm) + 2) + q(q-1)m((n+1)C_\times + C_+ + C_G), \quad (8)$$

де $T_q(1)$ – число операцій у кільці $\mathbf{Z}[\omega]$, що використовуються для множення векторів довжини q на матрицю $H_1 = (\omega^{-G(yx)})_{x,y \in R}$, де $G: R \to \mathbf{Z}/(l)$ – гомоморфізм абелевих груп, ядро якого не містить ненульових правих (лівих) ідеалів кільця R, l – характеристика кільця R, C_+, $C_\times$ і C_G – двійкові складності операцій додавання, множення елементів кільця R та обчислення значення гомоморфізму G відповідно.

При застосуванні числового перетворення Ферма двійкова часова складність алгоритму обчислення всіх значень частоти зустрічальності елементів $n(z \mid \varepsilon(x))$ не перевищує

$$\widetilde{T}_{2^N}(n) = 26 \cdot 2^{N(n+1)} Nn + 2^{2N} m((n+1)N(6N-5) + 5(N-1) + 7 \cdot 2^{N-1} + 2). \quad (9)$$

Для окремого випадку, коли R є кільцем лишків за модулем 2^N та заданого розподілу ймовірностей спотворень у правих частинах рівнянь системи (1) розраховано трудомісткість узагальненого алгоритму BKW за умови, що на другому етапі, замість традиційного ММП, використовуються запропоновані методи, які базуються на застосуванні швидкого перетворення Фур'є та числового перетворення Ферма відповідно.

В таблиці 1 символами $\log T_{\mathrm{BKW}}(n_1)$, $\log T_{\mathrm{BKW}}(n_1{}^*)$ та $\log T_{\mathrm{BKW}}(\widetilde{n}_1{}^*)$ позначені трудомісткості узагальненого алгоритму BKW та його модифікацій, що базуються на швидкому перетворенні Фур'є та Ферма відповідно, а символами n_1, $n_1{}^*$, $\widetilde{n}_1{}^*$ – число рівнянь в СР (1), що складаються на першому етапі цього алгоритму. Як видно з таблиці 1, застосування швидкого перетворення Фур'є на другому етапі узагальненого алгоритму BKW зменшує його складність від $2^{131,06}$ до $2^{631,61}$ разів в залежності від числа невідомих в системі та відстані між

розподілом спотворень у правих частинах її рівнянь і рівномірним розподілом ймовірностей.

Таблиця 1

Часова складність розв'язання задачі LPN ($N = 8$, $\delta = 0{,}01$)

n	ε	n_1	$\log T_{\mathrm{BKW}}(n_1)$	$n_1{}^*$	$\log T_{\mathrm{BKW}}(n_1{}^*)$	$\widetilde{n}_1{}^*$	$\log T_{\mathrm{BKW}}(\widetilde{n}_1{}^*)$
32	2^{-15}	28	291,61	16	160,55	16	147,70
32	2^{-25}	28	311,61	16	170,22	16	170,21
64	2^{-30}	60	579,81	35	345,15	39	337,38
80	2^{-15}	76	678,49	26	279,78	26	279,78
128	2^{-25}	124	1169,95	64	548,10	64	533,70
128	2^{-30}	124	1179,95	64	548,34	65	541,72

При застосуванні швидкого перетворення Ферма виграш є ще більшим і змінюється від $2^{143,97}$ до $2^{638,23}$ разів. Встановлено також, що інколи на другому етапі узагальненого алгоритму BKW вигідніше розв'язувати систему рівнянь від більшої кількості змінних, використовуючи числове перетворення Ферма замість звичайного швидкого перетворення Фур'є. Так, згідно з даними в таблиці 1, при $\varepsilon = 2^{-30}$ та $n = 64$ системи рівнянь зі спотвореними правими частинами від 39 змінних над кільцем лишків за модулем 2^8 розв'язуються швидше за допомогою швидкого перетворення Ферма, ніж аналогічні СР від 35 невідомих з використанням швидкого перетворення Фур'є.

У **четвертому розділі** викладено метод побудови нових алгоритмів розв'язання СР (1) над кільцем $R_N = \mathbf{Z}/(2^N)$ за довільною скінченною сукупністю вхідних таких алгоритмів. Зазначений (послідовний) метод запропоновано вперше. Він базується на ідеї послідовного розв'язання статистичних задач, що пристосована до розв'язання булевих СР зі спотвореними правими частинами. Отримано аналітичні вирази оцінок достовірності та часової складності алгоритмів розв'язання СР (1), 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*.

В якості прикладу практичного застосування послідовного методу запропоновано ефективну атаку на симетричну шифросистему типу LPN-C над

кільцем R_N. Схема конфіденційної передачі повідомлень за допомогою шифросистеми LPN-C наведена на рисунку 3. Ключем шифрування є випадкова рівноймовірна $n \times L$-матриця M над кільцем R_N, а шифроване повідомлення, що отримується в результаті зашифрування відкритого тексту x на ключі M, визначається за формулою $(a, y = xG + aM + \xi)$, де G – твірна матриця завадостійкого (L, K)-коду C над кільцем R_N зі швидким алгоритмом декодування, a та ξ – випадкові вектори довжини n та L відповідно над кільцем R_N із певними законами розподілу.

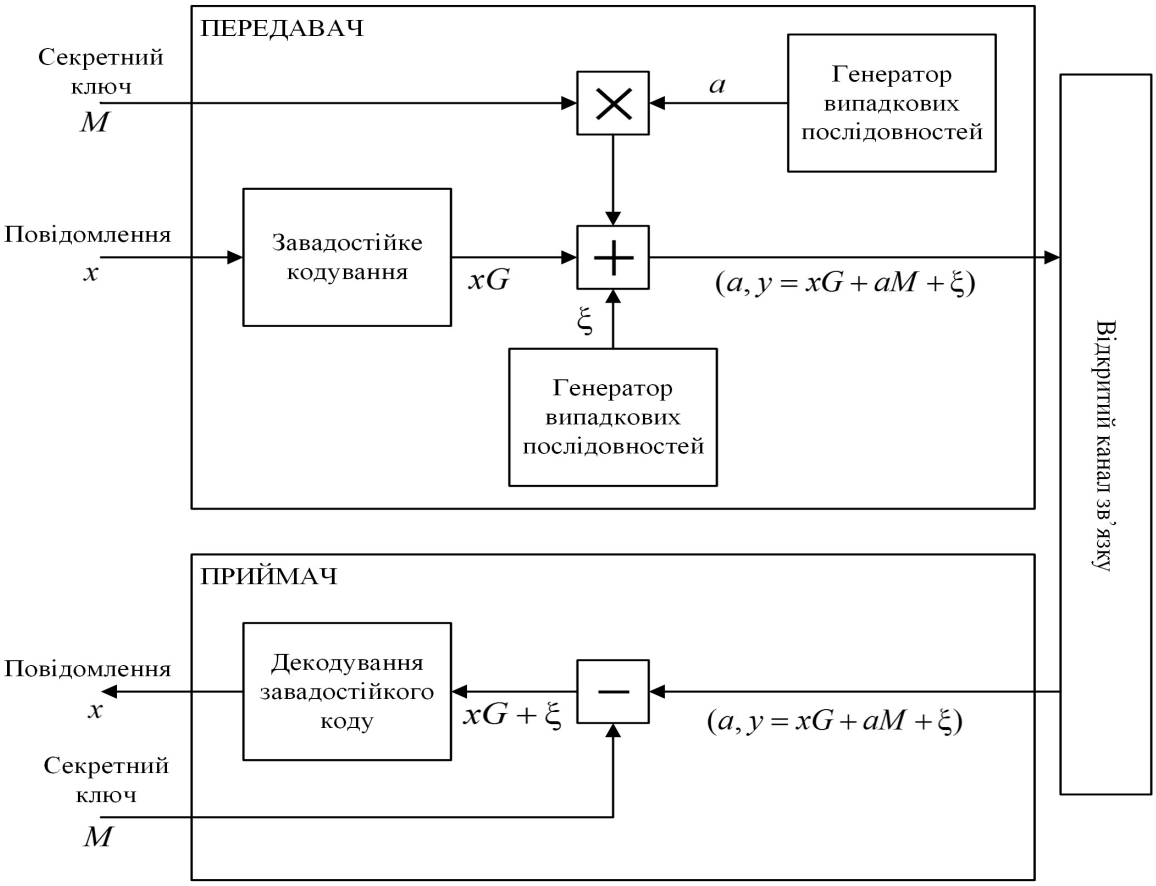


Рисунок 3 – Схема конфіденційної передачі повідомлень за допомогою шифросистеми LPN-C

Оцінено часову складність та обсяг матеріалу, потрібного для розв'язання зазначених СР над кільцем R_N за допомогою узагальненого алгоритму BKW та послідовного методу відповідно. Показано, що послідовний метод є суттєво більш ефективним (як за трудомісткістю, так і за обсягом матеріалу) в порівнянні з узагальненим алгоритмом BKW. Зокрема, при $n = 512, K = 27$ $L = 80$, $4 \le N \le 16$ часова складність відновлення ключа шифросистеми LPN-C за допомогою послідовного методу складає від $2^{136,07}$ до $2^{138,07}$ операцій, в той час як узагальнений алгоритм BKW потребує від $2^{412,31}$ до $2^{1550,81}$ операцій (при практично такому ж обсязі матеріалу).

Як другий важливий приклад практичного застосування отриманих наукових результатів, отримано (позитивну) відповідь на запитання про те, чи

можна підвищити стійкість шифру SNOW 2.0 відносно відомих кореляційних атак шляхом заміни у схемі його генератора гами порозрядного булевого додавання арифметичним додаванням за модулем 2^N (а також нелінійної підстановки іншим швидким перетворенням).

Генератор гами SNOW 2.0-подібного потокового шифру 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.

У розділі доведено, що у випадку, коли значення підстановки σ в точці $z \in R_N$ дорівнює циклічному зсуву двійкового запису числа z в бік старших розрядів, послідовний метод є незастосовним для побудови кореляційних атак на шифр.

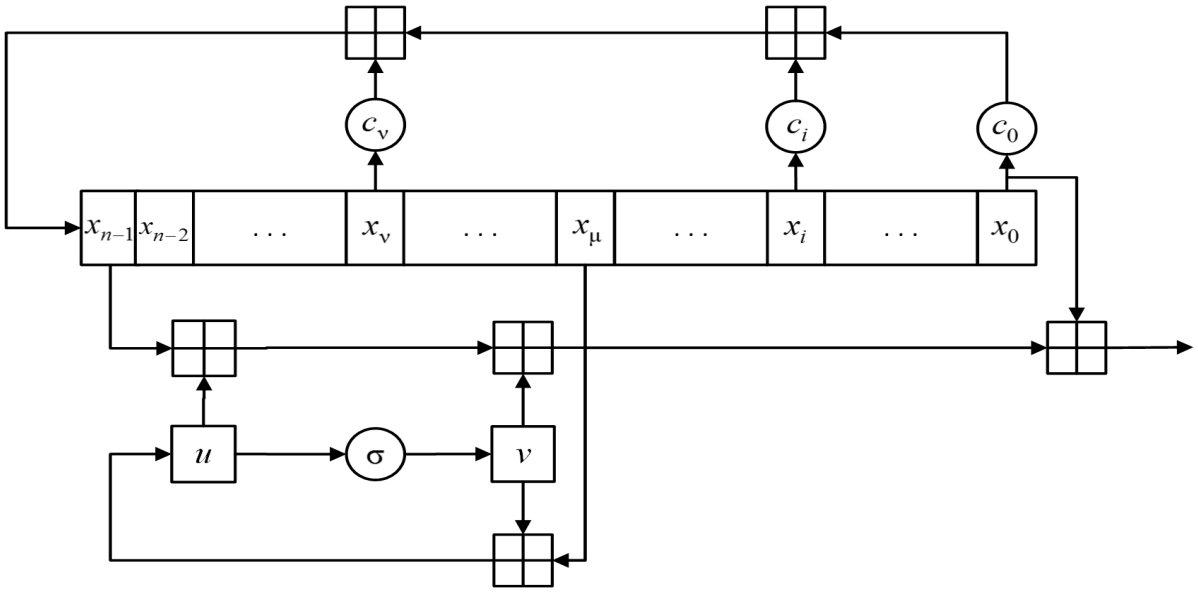


Рисунок 4 – Схема генератора гами SNOW 2.0-подібного шифру

Отже, зменшення стійкості шифру відносно таких атак за рахунок послідовного розв'язання СР зі спотвореними правими частинами є неможливим. Поряд з тим, отримано оцінки обчислювальної складності розв'язання СР за допомогою ММП, узагальненого алгоритму BKW та його модифікацій з використанням швидкого перетворення Фур'є та Ферма.

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. Показано також, що застосування швидкого

перетворення Ферма зменшує складність звичайної кореляційної атаки на SNOW 2.0-подібні шифри від $2^{8,24}$ до $2^{28,54}$ разів в залежності від параметрів n та N.

Як третій практично важливий приклад, отримано чисельні оцінки стійкості шифросистеми типу Ring-LWE (рисунок 5). Отримані результати надають можливість безпосередньо вибирати значення параметрів цієї шифросистеми, виходячи з вимоги її стійкості відносно атаки на основі підібраних відкритих повідомлень.

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:

$$U = \{u_0 + u_1 x + ... + u_{n-1} x^{n-1} : u_i \in \{0,1\}, i \in \overline{0, n-1}\}.$$

Множина ключів: $R_{n,q} = \mathbf{Z}_q[x]/(f(x))$.

Алгоритм зашифрування: шифротекст, який отримується при зашифруванні відкритого повідомлення $u \in U$ на ключі $s \in R_{n,q}$, має вигляд

$$E_s(u) = (c_1 = a, c_2 = as + 2e + u), \quad (10)$$

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

$$D_s(c_1, c_2) = (c_2 - c_1 s) \bmod 2. \quad (11)$$

Рисунок 5 – Опис симетричної шифросистеми Ring-LWE

У схемі шифрування Ring-LWE обчислення здійснюються в кільці $R_{n,q}$ поліномів степеня не вище n з коефіцієнтами з кільця лишків за модулем q. В розділі показано як супротивник може реалізувати на шифросистему атаку з підібраним відкритим повідомленням, формуючи СР зі спотвореними правими частинами. При цьому для оцінки складності розв'язання утвореної СР можна застосувати узагальнений алгоритм BKW. Оцінено часову складність та обсяг матеріалу, потрібного для відновлення ключа шифросистеми типу Ring-LWE за допомогою узагальненого алгоритму BKW та природного перебірного методу відповідно.

Результати розрахунків свідчать про те, що 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 $n=256$, $q=327$).

Додатки містять доведення окремих лем та тверджень, деяких формул, які мають значний обсяг; програмні коди реалізації модифікації методу максимуму правдоподібності з використанням швидкого перетворення Фур'є та послідовного методу розв'язання системи лінійних рівнянь над кільцем $\mathbf{Z}/(2^N)$; акти впровадження результатів дисертаційної роботи.

У **висновках** викладено найбільш важливі наукові та практичні результати дисертаційного дослідження, сформульовано розв'язану наукову задачу, розкрито методи її розв'язання, наукове та практичне значення роботи, обґрунтованість та достовірність отриманих результатів, подано висновки та рекомендації щодо їхнього подальшого використання.

ВИСНОВКИ

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.

1. 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.

2. Вперше отримано аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем. Зазначені оцінки надають можливість визначати фактичний обсяг матеріалу, достатнього для надійного розв'язання задачі LPN над довільним скінченним кільцем та часову складність узагальненого алгоритму BKW.

3. Розроблено два методи підвищення ефективності розв'язання задачі LPN за допомогою ММП. Перший з них є застосовним для довільного скінченного фробеніусова кільця 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. Застосування швидкого перетворення Фур'є або Ферма на другому етапі узагальненого алгоритму BKW в окремих випадках суттєво зменшує складність останнього.

4. 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 R_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 R_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 R_N для побудови шифросистем зазначеного типу.

5. 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. 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.

6. 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. 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 $2^{251,75}$.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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.

АНОТАЦІЯ

Ігнатенко С. М. Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Харківський національний університет імені В. Н. Каразіна, Міністерства освіти і науки України. – Харків, 2021.

У дисертації розв'язано актуальну наукову задачу розробки більш ефективних (в порівнянні з перебірним) методів розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем. Вперше отримано аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем, які дозволяють визначити часову складність узагальненого алгоритму BKW. Розроблено два методи підвищення ефективності розв'язання задачі LPN за допомогою ММП. Вперше розроблено метод побудови нових алгоритмів розв'язання СР над кільцем $\mathbf{Z}/(2^N)$ за довільною скінченною сукупністю вхідних таких алгоритмів. Наведено аналітичні вирази оцінок достовірності та часової складності алгоритмів розв'язання СР, які будуються за допомогою розробленого методу, через відповідні характеристики вхідних алгоритмів. Головним практичним результатом роботи є можливість оцінювати стійкість симетричних шифросистем, які будуються над скінченними кільцями та базуються на складності розв'язання задачі LPN.

Ключові слова: симетрична постквантова шифросистема, задача LPN, часова складність алгоритму, метод максимуму правдоподібності, узагальнений алгоритм BKW, скінченне кільце, обґрунтування стійкості, система лінійних рівнянь зі спотвореними правими частинами.

АННОТАЦИЯ

Игнатенко С. М. Методы решения задачи LPN над конечными кольцами для оценивания стойкости симметричных постквантовых шифрсистем. – Рукопись.

Диссертация на соискание научной степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. – Харьковский национальный университет имени В. Н. Каразина Министерства образования и науки Украины. – Харьков, 2021.

В диссертации решена актуальная научная задача разработки более эффективных (по сравнению с переборным) методов решения задачи LPN над конечными кольцами для оценивания стойкости симметричных постквантовых шифрсистем. Впервые получены аналитические оценки объема материала, достаточного для решения с заданной достоверностью задачи LPN над произвольным конченым кольцом, которые позволяют определить временную сложность обобщенного алгоритма BKW. Разработано два метода повышения эффективности решения задачи LPN с помощью ММП. Впервые разработан метод построения новых алгоритмов решения СР над кольцом $\mathbf{Z}/(2^N)$ по произвольной конечной совокупности исходных таких алгоритмов. Приведены аналитические выражения оценок достоверности и временной сложности алгоритмов решения СР, которые строятся с помощью разработанного метода, через соответствующие характеристики входных алгоритмов. Главным практическим результатом работы является возможность оценивать стойкость симметричных шифрсистем, которые строятся над конечными кольцами и базируются на сложности решения задачи LPN.

Ключевые слова: симметричная постквантовая шифрсистема, задача LPN, временная сложность алгоритма, метод максимума правдоподобия, обобщенный алгоритм BKW, конечное кольцо, обоснование стойкости, система линейных уравнений с искаженными правыми частями.

ABSTRACT

Ihnatenko S.M. Methods for solving the LPN problem over finite rings to evaluate the security of symmetric post-quantum cryptosystems. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 – Information protection systems. – V. N. Karazin Kharkiv National University of the Ministry of Education and Science of Ukraine. – Kharkiv, 2021.

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 information and telecommunication

systems.

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 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.

The method for developing new algorithms for solving the LPN problem over residue rings modulo 2^N for an arbitrary finite set of inputs of such algorithms obtained for the first time. It makes it possible to increase the effectiveness of solving this problem by properly selecting a composition of the N number.

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}.

Keywords: symmetric post-quantum cryptosystem, LPN problem, time complexity of the algorithm, maximum likelihood method, generalized BKW algorithm, finite ring, security proving, system of linear equations corrupted by noise.

Підписано до друку 15.03.2021 р.
Ум. др. арк. 0,9.Формат 60х84 1/16.
Наклад 100 прим. Папір офсетний. Зам. № 1503/2021.
Свідоцтво ДК 5941 від 11.01.2018 р.
03127 м. Київ, вул. Героїв Оборони 8.
Тел. (050)-411-66-51, (044)22-99-539

Видавництво «Наукова столиця»®
ДРУК НАУКОВОЇ ЛІТЕРАТУРИ
musetess@gmail.com
www.science.org.ua