**DOI: 10.18372/2410-7840.19.12109**
**УДК 621.391:519.2**

# ЗАСТОСУВАННЯ ШВИДКОГО ПЕРЕТВОРЕННЯ ФУР'Є ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ LPN НАД СКІНЧЕННИМИ ФРОБЕНІУСОВИМИ КІЛЬЦЯМИ

***Антон Олексійчук, Сергій Ігнатенко***

*Задача LPN є однією з найвідоміших обчислювально складних задач. В найбільш загальному формулюванні вона полягає в розв'язанні системи лінійних рівнянь зі спотвореними правими частинами над довільним скінченним кільцем і включає в себе, як окремий випадок, задачу декодування випадкового лінійного коду над скінченним полем. На сьогодні відомі (як симетричні, так і асиметричні) криптосистеми і протоколи, стійкість яких базується на складності розв'язання задачі LPN. Тому розробка більш ефективних, в порівнянні з відомими, алгоритмів вирішення цієї задачі є актуальним напрямом сучасної криптології. Найнадійнішим (та найбільш трудомістким) методом розв'язання задачі LPN є метод максимуму правдоподібності. Відомо, що для систем лінійних рівнянь зі спотвореними правими частинами над скінченним полем або кільцем лишків за модулем степеня двійки можна зменшити трудомісткість цього методу, 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. В даній статті 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. Отримані результати свідчать про те, що при розв'язанні задачі LPN над довільним скінченним фробеніусовим кільцем можна використовувати алгоритми швидкого перетворення Фур'є, добре відомі для випадку скінченного поля або кільця лишків за модулем степеня двійки. Це надає можливість помітно зменшити трудомісткість розв'язання цієї задачі методом максимуму правдоподібності.*

***Ключові слова:*** *криптологія, обґрунтована стійкість, задача LPN, система лінійних рівнянь зі спотвореними правими частинами, швидке перетворення Фур'є, скінченне фробеніусове кільце.*

**Вступ.**

Задача LPN (Learning Parity with Noise) є однією з найвідоміших обчислювально складних задач [9-12, 19]. В найбільш загальному формулюванні вона полягає у розв'язанні системи лінійних рівнянь зі спотвореними правими частинами над довільним скінченним кільцем і включає в себе, як окремий випадок, задачу декодування випадкового лінійного коду над скінченним полем (зауважимо, що часто-густо в літературі під задачею LPN розуміють її окремий випадок, коли кільце, над яким розглядається система рівнянь (СР), є полем з двох елементів; у випадку кільця лишків за натуральним модулем задачу LPN називають також задачею LWE (Learning With Errors) [9, 19]). Від складності розв'язання задачі LPN залежить стійкість сучасних потокових шифрів відносно кореляційних атак [15, 18, 22]. Більш того, відомі (як симетричні, так і асиметричні) криптосистеми і протоколи, стійкість яких безпосередньо базується на складності розв'язання задачі LPN [12, 13, 16, 17, 19]. Тому розробка більш ефективних, в порівнянні з відомими, алгоритмів вирішення цієї задачі є актуальним напрямом сучасної криптології.

Найнадійнішим (та найбільш трудомістким) методом розв'язання задачі LPN є метод максимуму правдоподібності [1, 3, 6]. Відомо, що для систем лінійних рівнянь зі спотвореними правими частинами над скінченним полем або кільцем лишків за модулем $2^N$ можна зменшити трудомісткість цього методу, використовуючи алгоритми швидкого перетворення Фур'є [2, 5, 14, 22]. Поряд з тим, питання про те, наскільки широким є клас скінченних кілець із зазначеною властивістю є на сьогодні відкритим.

В даній статті показано, що таким є клас скінченних фробеніусових кілець (при цьому з результатів, наведених в [20, 21], випливає, що цей клас є у певному сенсі найширшим). Отримані результати свідчать про те, що при розв'язанні задачі LPN над довільним скінченним фробеніусовим кільцем можна використовувати алгоритми швидкого перетворення Фур'є, добре відомі для випадку скінченного поля або кільця лишків за модулем $2^N$. Це надає можливість помітно зменшити трудомісткість розв'язання цієї задачі методом максимуму правдоподібності.

**1. Постановка задачі.**

Нехай $R$ – скінченне (асоціативне) кільце з одиницею, $|R| = q$. Розглянемо систему рівнянь зі спотвореними правими частинами

$$Ax = b, \qquad (1)$$

де $A$ – випадкова рівноймовірна $m \times n$-матриця над кільцем $R$, $b$ – вектор довжини $m$ з координатами $b_i = A_i a + \xi_i$, $i \in \overline{1,m}$, 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 (1)), $\xi_1, \dots, \xi_m$ – незалежні випадкові величини, розподілені за законом $\mathbf{P}\{\xi_i = z\} = p(z)$, де $p(z) \ge 0$ для кожного $z \in R$, $\sum_{z \in R} p(z) = 1$. Задача LPN полягає у відновленні вектора $a$ за відомими реалізаціями матриці $A$, вектора $b$ та розподілом ймовірностей $p_\xi = (p(z) : z \in R)$ [9-12, 19].

Одним з найвідоміших методів розв'язання цієї задачі є *метод максимуму правдоподібності* (ММП), який 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 $\xi = (\xi_1, \dots, \xi_m)$, $\varepsilon(x) = b - Ax$ для будь-якого $x \in R^n$. 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 (1) (див., наприклад, [8, с. 141]).

При практичному застосуванні ММП звичайно виконують такий алгоритм [1, 3, 6]:

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

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

де $N_\xi(R) = \{z \in R : p(z) > 0\}$, $n(z \mid \varepsilon(x))$ – частота зустрічаємості 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 (1) за допомогою ММП. При цьому двійкова часова складність алгоритму дорівнює

$$T = nmq^n (C_+ + C_\times), \qquad (3)$$

де $C_+$ і $C_\times$ є двійкові складності операцій додавання та множення елементів кільця $R$.

Відомо, що у випадку, коли $R$ є скінченним полем або кільцем лишків за модулем $q = 2^N$ для обчислення значень функції (2) можна використовувати перетворення Фур'є певних допоміжних функцій, заданих на групі $(R^n, +)$. При цьому застосування алгоритмів швидкого перетворення Фур'є дозволяє помітно скоротити трудомісткість розв'язання СР (1) за допомогою ММП [2, 5, 14, 22].

В зв'язку з цим є природним запитання про те, наскільки широким є клас скінченних кілець, для яких обчислення усіх значень $n(z \mid \varepsilon(x))$ у виразі (2) можна здійснити за допомогою перетворення Фур'є. Визначення такого класу кілець є основною задачею, що розв'язується далі в статті.

**2. Попередні відомості про перетворення Фур'є та фробеніусові кільця.**

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 $\chi_a(x) = \chi_x(a)$ [7].

*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 $\chi_a$ – 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 $f$ відновлюються 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, [20]).

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 $R$ [20].

Наведемо найважливіші, з практичного погляду, приклади фробеніусових кілець [20].

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 $\omega$ – примітивний корінь степеня $p$ з одиниці, $\mathrm{Tr}(x) = x \oplus x^p \oplus \dots \oplus x^{p^{r-1}}$, $x \in R$.

2. Кільце лишків $R = \mathbf{Z}/(q)$ є фробеніусовим кільцем с 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 $\chi_i$ 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 $\chi$ кільця $R$ відображення $\tilde{\chi}(X) = \chi(\mathrm{tr}(X))$, 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 1.** Нехай $R$ є фробеніусовим кільцем характеристики $l$ з утворюючим характером $\chi$. Тоді $\chi(x) = \omega^{G(x)}$, $x \in R$, де $\omega$ – 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 $R$.

**3. Основні результати.**

Розглянемо СР (1) над фробеніусовим кільцем $R$ та покажемо, як скористатися швидким перетворенням Фур'є для обчислення усіх значень $n(z\,|\,\varepsilon(x))$ у виразі (2).

**Теорема 1.** Нехай $R$ – фробеніусове кільце порядку $q$ з утворюючим характером $\chi$, $A \in R_{m\times n}$, $b \in R^m$. Тоді для кожного $z \in R$ частота зустрічаємості $n(z\,|\,\varepsilon(x))$ елемента $z$ у векторі $\varepsilon(x) = b - Ax$ задовольняє рівності

$$n(z\,|\,\varepsilon(x)) = q^{-1}(\hat{g}_z(x) + m),\ x \in R^n, \qquad (4)$$

де

$$g_z(y) = \sum_{\substack{(r\in R\setminus\{0\},\, j\in\overline{1,m}):\\ rA_j = y}} \chi(r(b_j - z)),\ y \in R^n. \qquad (5)$$

**Доведення.** На підставі означення перетворення Фур'є функції (5) та леми 1 справедливі рівності

$$\hat{g}_z(x) = \sum_{y\in R^n} g_z(y)\overline{\chi_y(x)} =$$

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

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

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

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

$$\sum_{j\in\overline{1,m}} (q\delta(z, b_j - A_j x) - 1) = qn(z\,|\,\varepsilon(x)) - m,$$

де передостання рівність випливає зі співвідношення ортогональності для характерів: $\sum_{r\in R} \chi(ru) = q\delta(u, 0)$, $\delta$ є символом Кронекера (див., наприклад, [7]).

Отже, справедлива формула (4). Теорему доведено.

Таким чином, на підставі отриманої теореми при розв'язанні СР (1) над фробеніусовим кільцем $R$ за допомогою ММП достатньо обчислити для кожного $z \in R$ перетворення Фур'є функції (5) та знайти (шляхом повного перебору) точку максимуму функції (2).

Покажемо, як скористатися для обчислення усіх значень (4) швидким алгоритмом, наведеним в [5].

Перш за все, сформулюємо наступну лему, яка доводиться шляхом прямого обчислення.

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

**Теорема 2.** За умови теореми 1 двійкова часова складність обчислення всіх значень (4) не перевищує

$$T_q(n) = 5T_q(1)q^n nl(\log(T_q(1)q^n nm) + 2) + q(q-1)m((n+1)C_\times + C_+ + C_G), \qquad (6)$$

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.** Зрозуміло, що обчислення перетворення Фур'є функції (5) 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 (5) можна обчислити за допомогою швидкого алгоритму зі складністю

$$T'_q(n) = T_q(1)q^{n-1}n \qquad (7)$$

операцій додавання комплексних чисел та їх множення на степені елемента $\omega$, причому число $T_q(1)$ дорівнює складності множення векторів довжини $q$ на матрицю $H_1$ [5].

Далі, елементи матриці $H_n$ як і значення кожної функції (5) є многочленами від $\omega$ 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 $\omega^k$ – 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 (5) як елементів кільця $\mathbf{Z}[\omega]$ не перевищує числа доданків у виразі, який визначає цю функцію, тобто $m(q-1)$. Звідси на підставі леми 2 випливає, що двійкова часова складність обчислення перетворення Фур'є кожної окремої функції (5) 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 (7)). Отже, двійкова складність обчислення перетворень Фур'є усіх $q$ функцій (5) не перевищує

$$T_1 = 5T'_q(n)ql(\log(T'_q(n)mq)+2). \qquad (8)$$

Далі, для визначення кожної функції (5) 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 (5) дорівнює

$$T_2 = q(q-1)l((n+1)C_\times + C_+ + C_G). \qquad (9)$$

Підсумовуючи вирази (8) і (9), отримаємо формулу (6). Теорему доведено.

Зауважимо, при практичній реалізації алгоритму, зазначеного у доведенні теореми 2, в результаті обчислень, виконаних в кільці $\mathbf{Z}[\omega]$, кожне значення $\hat{g}_z(x)$, $x \in R^n$, буде отримано у вигляді многочлена від $\omega$: $\hat{g}_z(x) = \sum_{i=0}^{l-1} c_i(x)\omega^i$, де $c_i(x) \in \mathbf{Z}$, $i \in \overline{0,l-1}$, і на підставі формули (4) 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.

Як приклад, що ілюструє отримані результати, розглянемо задачу LPN над кільцем $R = \mathbf{Z}/(2^N)$. Тоді $q = l = 2^N$, $G(x) = x$ для кожного $x \in R$. Крім того, $C_+ = 5N-2$, $C_\times = 6N^2 - 6N + 2$ [5], $T_q(1) = (2N-1)2^N + 1$ [4] і на підставі теореми 2 двійкова часова складність знаходження істинного розв'язку СР (1) за допомогою швидкого перетворення Фур'є не перевищує

$$T_{2^N}(n) = 5\cdot 2^{(n+2)N+1}Nn\log(2^{N+1}Nnm) + 2^{2N}m((n+1)(6N^2-6N+2)+5N-2).$$

В той же час, згідно з формулою (3), двійкова складність знаходження цього розв'язку за допомогою звичайного алгоритму дорівнює $T = nm2^{Nn}(6N^2-N)$.

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

Як видно з таблиці, значення виграшу практично не залежить від числа $n$ невідомих та швидко зростає з ростом числа $m$ рівнянь у системі (1).

Таблиця 1

Чисельні значення 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) | $1{,}56\cdot10^5$ | $1{,}96\cdot10^7$ | $2{,}53\cdot10^9$ | $3{,}32\cdot10^{11}$ | $4{,}42\cdot10^{13}$ | $5{,}94\cdot10^{15}$ | $8{,}05\cdot10^{17}$ | $1{,}09\cdot10^{20}$ |
| (30, 4) | $1{,}54\cdot10^5$ | $1{,}95\cdot10^7$ | $2{,}51\cdot10^9$ | $3{,}29\cdot10^{11}$ | $4{,}38\cdot10^{13}$ | $5{,}89\cdot10^{15}$ | $7{,}99\cdot10^{17}$ | $1{,}08\cdot10^{20}$ |
| (40, 4) | $1{,}53\cdot10^5$ | $1{,}93\cdot10^7$ | $2{,}49\cdot10^9$ | $3{,}27\cdot10^{11}$ | $4{,}36\cdot10^{13}$ | $5{,}86\cdot10^{15}$ | $7{,}96\cdot10^{17}$ | $1{,}08\cdot10^{20}$ |
| (60, 4) | $1{,}51\cdot10^5$ | $1{,}90\cdot10^7$ | $2{,}46\cdot10^9$ | $3{,}24\cdot10^{11}$ | $4{,}32\cdot10^{13}$ | $5{,}81\cdot10^{15}$ | $7{,}90\cdot10^{17}$ | $1{,}08\cdot10^{20}$ |
| (20, 8) | $1{,}11\cdot10^3$ | $1{,}42\cdot10^5$ | $1{,}85\cdot10^7$ | $2{,}46\cdot10^9$ | $3{,}29\cdot10^{11}$ | $4{,}45\cdot10^{13}$ | $6{,}06\cdot10^{15}$ | $8{,}32\cdot10^{17}$ |
| (30, 8) | $1{,}09\cdot10^3$ | $1{,}41\cdot10^5$ | $1{,}83\cdot10^7$ | $2{,}43\cdot10^9$ | $3{,}26\cdot10^{11}$ | $4{,}42\cdot10^{13}$ | $6{,}02\cdot10^{15}$ | $8{,}27\cdot10^{17}$ |
| (40, 8) | $1{,}08\cdot10^3$ | $1{,}39\cdot10^5$ | $1{,}82\cdot10^7$ | $2{,}42\cdot10^9$ | $3{,}25\cdot10^{11}$ | $4{,}39\cdot10^{13}$ | $5{,}99\cdot10^{15}$ | $8{,}23\cdot10^{17}$ |
| (60, 8) | $1{,}07\cdot10^3$ | $1{,}38\cdot10^5$ | $1{,}81\cdot10^7$ | $2{,}40\cdot10^9$ | $3{,}22\cdot10^{11}$ | $4{,}36\cdot10^{13}$ | $5{,}96\cdot10^{15}$ | $8{,}18\cdot10^{17}$ |
| (80, 8) | $1{,}06\cdot10^3$ | $1{,}37\cdot10^5$ | $1{,}79\cdot10^7$ | $2{,}38\cdot10^9$ | $3{,}20\cdot10^{11}$ | $4{,}34\cdot10^{13}$ | $5{,}93\cdot10^{15}$ | $8{,}15\cdot10^{17}$ |

**Висновки**

При розв'язанні задачі LPN над довільним скінченним фробеніусовим кільцем можна використовувати процедуру швидкого перетворення Фур'є, добре відому для випадку скінченного поля або кільця лишків за модулем $2^N$. Це надає можливість помітно зменшити трудомісткість розв'язання цієї задачі методом максимуму правдоподібності, уникаючи при цьому операцій над комплексними числами. Зокрема, для кільця лишків за модулем $2^N$ виграш в трудомісткості складає від $10^3$ до $10^{20}$ разів в залежності від параметра $N$ та числа рівнянь $m$ у системі (1).

**ЛІТЕРАТУРА**


[1]. А. Алексейчук, С. Игнатенко, "Нижняя граница вероятности восстановления истинного решения системы линейных уравнений с искаженной правой частью над кольцом вычетов по модулю $2^N$", *Захист інформації*, № 4, С. 6-12, 2006.

[2]. А. Алексейчук, С. Игнатенко, "Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю $2^N$", *Збірник наукових праць ІПМЕ НАН України*, Вып. 20, С. 40-48, 2003.

[3]. Г. Балакин, "Введение в теорию случайных систем уравнений", *Труды по дискретной математике*, М.: ТВП, Т. 1, С. 1–18, 1997.

[4]. Р. Блейхут, *Быстрые алгоритмы цифровой обработки сигналов* Пер. с англ. М.: Мир, 1989, 448 с.

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

[6]. А. Левитская, "Системы случайных уравнений над конечными алгебраическими структурами", *Кибернетика и системный анализ*, Т. 41, № 1, С. 82-116, 2005.

[7]. Р. Лидл, Г. Нидеррайтер, *Конечные поля, пер. с англ,* М.: Мир, 1988, 818 с.

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

[9]. M. Albrecht, C. Cid, J. Faugere, R. Fitzpatric, L. Perret, "Algebraic algorithms for LWE problems", *Cryptology ePrint Archive*, Report 2014/1018. [Electronic resource]. Access: http://eprint.iacr.org/2014/1018.

[10]. E. Berlekamp, R. McElice, H. van Tilborg, "On the inherent intractability of certain coding problems", *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 384-386, 1978.

[11]. A. Blum, A. Kalai, H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model", *J. ACM,* vol. 50, no. 3, pp. 506-519, 2003.

[12]. A. Blum, M. Furst, M. Kearns, R. Lipton, "Cryptographic primitives based on hard learning problems", *Crypto'93, LNCS 773,* Springer-Verlag, pp. 278–291.

[13]. H. Gilbert, J. Mattew, M.J. Robshaw, Y. Seurin, "How to Encrypt with the LPN Problem", *ICALP*, Proceedings, Springer Verlag, pp. 679-690, 2008.

[14]. J. Golić, G. Morgari, "Vectorial fast correlation attacks", *Cryptology ePrint Archive*, Report 2004/247. [Electronic resource]. Access: http://eprint.iacr.org/2004/247.

[15]. F. Jönsson, T. Johansson, "Correlation attacks on stream ciphers over $GF(2^n)$", *The 2001 International Symposium on Information Theory. ISIT'2001*, Proceedings. Springer Verlag, pp. 140, 2001.

[16]. A. Juels, S. Weis, "Authenticating pervasive devices with Human protocols", *Crypto'95. LNCS 3126*. Springer-Verlag, pp. 293-308, 1995.

[17]. E. Kiltz, D. Masny, K. Pietrsak, "Simple chosen-ciphertext security from low-noise LPN", *Public Key Cryptography. PKC 2014*. Springer-Verlag, pp. 1-18, 2014.

[18]. A. Maximov, T. Johansson, "Fast computation for large distribution and its cryptographic application" *Advanced in Cryptology. ASIACRYPT 2005*. LNCS 3788. Springer-Verlag, pp. 313- 332.

[19]. O. Regev, "On lattices, learning with errors and random linear codes, and Cryptography", *STOC 2005*, Proceedings, Springer Verlag, pp. 84-93, 2005.

[20]. J. Wood, "Duality for modules over finite rings and application to coding theory", *Amer. J. Math*, vol. 121, pp. 555-575, 1999.

[21]. J. Wood, "A coding-theoretic characterization of finite Frobenius rings", [Electronic resource]. Access: https://www.semanticshol.org/paper/2006.

[22]. B. Zhang, C. Xu, W. Meier, "Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0", *Cryptology ePrint Archive*, Report 2016/311. [Electronic resource]. Access: http://eprint.iacr.org/2016/311.

**REFERENCES**

[1] A. Alekseychuk, S. Ignatenko, "Lover bound of probability of recovering a true solution of a system of linear equations corrupted by noise over residue ring modulo $2^N$", *Zahist informatsii*, no. 4, pp. 6-12, 2006.

[2] A. Alekseychuk, S. Ignatenko, "Evaluations of the effectiveness of universal methods recovering corrupted linear recurrences over residue ring modulo $2^N$", *Zbirnyk naukovyh prac' IPME NAN Ukrainy*, no. 20, pp. 40-48, 2003.

[3] G. Balakin, "Introduction to the theory of random systems of equations", *Trudy po diskretnoy matematike,* vol. 1, pp. 1-18, 1997.

[4] R. Blahut, *Fast algorithms for digital signal processing*, Reading MA: Addicson-Wesley, 1985, 448 p.

[5] S. Ignatenko, "Modification of the maximum likelihood method for solving systems of linear equations corrupted by noise over residue ring modulo $2^N$", *Zahist informatsii*, no. 1, pp. 63-72, 2007.

[6] A. Levitskaya, "Systems of random equations over finite algebraic structures", *Kibernetika I Sistemnyi Analiz,* vol. 41, no. 1, pp. 82-116, 2005.

[7] R. Lidl, G. Niderrayter, *Finite fields*, Cambridge Univ. Press, 1985, 818 p.

[8] S. Chechyota, "Introduction to discrete information and coding theoty: a training edition", M.: MCCME Press, 2011, 224 p.

[9] M. Albrecht, C. Cid, J. Faugere, R. Fitzpatric, L. Perret, "Algebraic algorithms for LWE problems", *Cryptology ePrint Archive*, Report 2014/1018. [Electronic resource]. Access: http://eprint.iacr.org/2014/1018.

[10] E. Berlekamp, R. McElice, H. van Tilborg, "On the inherent intractability of certain coding problems", *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 384-386, 1978.

[11] A. Blum, A. Kalai, H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model", *J. ACM,* vol. 50, no. 3, pp. 506-519, 2003.

[12] A. Blum, M. Furst, M. Kearns, R. Lipton, "Cryptographic primitives based on hard learning problems", *Crypto'93, LNCS 773,* Springer-Verlag, pp. 278–291.

[13] H. Gilbert, J. Mattew, M.J. Robshaw, Y. Seurin, "How to Encrypt with the LPN Problem", *ICALP*, Proceedings, Springer Verlag, pp. 679-690, 2008.

[14] J. Golić, G. Morgari, "Vectorial fast correlation attacks", *Cryptology ePrint Archive*, Report 2004/247. [Electronic resource]. Access: http://eprint.iacr.org/2004/247.

[15] F. Jönsson, T. Johansson, "Correlation attacks on stream ciphers over $GF(2^n)$", *The 2001 International Symposium on Information Theory. ISIT'2001*, Proceedings. Springer Verlag, pp. 140, 2001.

[16] A. Juels, S. Weis, "Authenticating pervasive devices with Human protocols", *Crypto'95. LNCS 3126*. Springer-Verlag, pp. 293-308, 1995.

[17] E. Kiltz, D. Masny, K. Pietrsak, "Simple chosen-ciphertext security from low-noise LPN", *Public Key Cryptography. PKC 2014*. Springer-Verlag, pp. 1-18, 2014.

[18] A. Maximov, T. Johansson, "Fast computation for large distribution and its cryptographic application" *Advanced in Cryptology. ASIACRYPT 2005*. LNCS 3788. Springer-Verlag, pp. 313- 332.

[19] O. Regev, "On lattices, learning with errors and random linear codes, and Cryptography", *STOC 2005*, Proceedings, Springer Verlag, pp. 84-93, 2005.

[20] J. Wood, "Duality for modules over finite rings and application to coding theory", *Amer. J. Math*, vol. 121, pp. 555-575, 1999.

[21] J. Wood, "A coding-theoretic characterization of finite Frobenius rings", [Electronic resource]. Access: https://www.semanticshol.org/paper/2006.

[22] B. Zhang, C. Xu, W. Meier, "Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0", *Cryptology ePrint Archive*, Report 2016/311. [Electronic resource]. Access: http://eprint.iacr.org/2016/311.

## ПРИМЕНЕНИЕ БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ ДЛЯ РЕШЕНИЯ ЗАДАЧИ LPN НАД КОНЕЧНЫМИ ФРОБЕНИУСОВЫМИ КОЛЬЦАМИ

Задача LPN является одной из самых известных вычислительно трудных задач. В наиболее общей постановке она состоит в решении системы линейных уравнений с искаженными правыми частями над произвольным конечным кольцом и включает в себя, в качестве частного случая, задачу декодирования случайного линейного кода над конечным полем. Известны

(как симметричные, так и асимметричные) криптосистемы и протоколы, стойкость которых базируется на сложности решения задачи LPN. Поэтому разработка более эффективных, по сравнению с известными, алгоритмов решения этой задачи является актуальным направлением современной криптологии. Наиболее надежным (и наиболее трудоемким) методом решения задачи LPN является метод максимума правдоподобия. Известно, что для систем линейных уравнений с искаженными правыми частями над конечным полем или кольцом вычетов по модулю степени двойки можно уменьшить трудоемкость этого метода, применяя алгоритмы быстрого преобразования Фурье. Вместе с тем, вопрос о том, насколько широким является класс конечных колец с указанным свойством остается открытым. В данной статье показано, что таким является класс конечных фробениусовых колец. Этот класс очень обширный и включает в себя, в частности, любые кольца главных (левых или правых) идеалов. Полученные результаты свидетельствуют о том, что при решении задачи LPN над произвольным конечным фробениусовым кольцом можно применять алгоритмы быстрого преобразования Фурье, хорошо известные для случая конечного поля или кольца вычетов по модулю степени двойки. Это дает возможность заметно уменьшить трудоемкость решения указанной задачи методом максимума правдоподобия.

**Ключевые слова:** криптология, обоснованная стойкость, задача LPN, система линейных уравнений с искаженными правыми частями, быстрое преобразование Фурье, конечное фробениусово кольцо.

## APPLICATION OF FAST FOURIER TRANSFORM FOR SOLVING OF THE LPN PROBLEM OVER FINITE FROBENIUS RINGS

The LPN problem is one of the most famous hard computational problems. In the most general formulation, it consists in solving a system of linear equations corrupted by noise over an arbitrary finite ring and includes, as a special case, the problem of decoding a random linear code over a finite field. Numerous (both symmetric and asymmetric) cryptosystems and protocols, which resistance relies on the complexity of solving the LPN problem are known. Therefore, the development of more efficient algorithms for solving this problem, in comparison with known algorithms, is an actual direction of modern cryptology. The most reliable (and most time-consuming) method for solving the LPN problem is the maximum likelihood method. It is well known that for systems of linear equations corrupted by noise over a finite field or a residue ring modulo power of two the complexity of this method can be reduced by applying algorithms for the fast Fourier transform. At the same time the question of how wide is the class of finite rings with this property remains open. In this paper we show that this is the class of finite Frobenius rings. This class is very extensive and includes, in particular, any (left or right) principal ideal ring. The obtained results indicate that it is possible to apply algorithms for the fast Fourier transform, well known for the case of a finite field or a residue ring modulo power of two, to the solving the LPN problem over an arbitrary finite Frobenius ring. This makes to significantly reduce the complexity of solving this problem by the maximum likelihood method.

**Keywords:** cryptology, provable security, LPN problem, system of linear equations corrupted by noise, fast Fourier transform, finite Frobenius ring.

**Олексійчук Антон Миколайович**, доктор технічних наук, доцент, професор кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: alex-dtn@ukr.net

**Алексейчук Антон Николаевич,** доктор технических наук, доцент, профессор кафедры Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».

**Alekseychuk Anton,** Doctor of Technical Sciences, Assistant professor, Professor of The Institute of Special Communication and Information Protection of National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».

**Ігнатенко Сергій Михайлович**, аспірант Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
E-mail: mongol_1979@ukr.net.

**Игнатенко Сергей Михайлович**, аспирант Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского».

**Ignatenko Sergiy**, postgraduate of The Institute of Special Communication and Information Protection of National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».