DOI: 10.18372/2410-7840.20.12956
УДК 621.391:519.2

ЗАСТОСУВАННЯ ПОСЛІДОВНОГО МЕТОДУ ДЛЯ ПОБУДОВИ СТАТИСТИЧНОЇ АТАКИ НА ШИФРОСИСТЕМУ LPN-C НАД КІЛЬЦЕМ ЛИШКІВ ЗА МОДУЛЕМ 2^N

Сергій Ігнатенко

Шифросистема LPN-C є однією з перших постквантових симетричних шифросистем, стійкість яких базується на складності розв'язання задачі LPN. Оригінальна версія шифросистеми визначається над полем з двох елементів, проте вона природним чином узагальнюється 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, як показано нижче, шифросистема LPN-C над кільцем за модулем 2^N являє собою виняток з цього правила. В даній статті запропоновано атаку на шифросистему LPN-C над кільцем лишків за модулем 2^N, яка полягає у відновленні ключа шляхом послідовного розв'язання N систем лінійних рівнянь зі спотвореними правими частинами над полем з двох елементів. Показано, що запропонована атака є суттєво більш ефективною в порівнянні з традиційною атакою того ж самого типу, що базується на безпосередньому розв'язанні зазначеної системи рівнянь за допомогою узагальненого алгоритму BKW. Отримані результати свідчать про недоцільність застосування для побудови шифросистем LPN-C кілець лишків за модулем 2^N при $N \geq 2$, оскільки це не призводить до суттєвого підвищення стійкості у порівнянні з випадком $N = 1$.

Ключові слова: *постквантова криптографія, шифросистема LPN-C, система лінійних рівнянь зі спотвореними правими частинами, кільце лишків за модулем 2^N, послідовний метод, узагальнений алгоритм BKW, швидка статистична атака.*

Вступ

Шифросистема LPN-C [10] запропонована у 2008 р. і є однією з перших постквантових симетричних шифросистем, стійкість яких базується на складності розв'язання задачі LPN (Learning Parity with Noise). Остання відноситься до найвідоміших обчислювально складних задач і у загальному формулюванні полягає в розв'язанні системи лінійних рівнянь (СЛР) зі спотвореними правими частинами над довільним скінченним кільцем, включаючи в себе, як окремий випадок, задачу декодування випадкового лінійного коду над скінченним полем (див., наприклад, роботи [5 – 8, 11] та наведені там посилання).

Оригінальна версія шифросистеми визначається над полем з двох елементів, проте вона природним чином узагальнюється на випадок довільного скінченного кільця. В [10] доведено, що за умови належного вибору її параметрів шифросистема LPN-C є стійкою відносно атак з адаптивно вибраним відкритим текстом (IND-P2-C0), тобто супротивник, маючи можливість вибирати відкриті тексти для зашифрування, не зможе (з потрібною високою ймовірністю та за прийнятний час) розрізнити, який відкритий текст відповідає конкретному шифрованому. Поряд з цим, зазначене твердження не знімає з порядку денного дослідження стійкості шифросистеми LPN-C, а також її узагальнень відносно конкретних атак, які базуються на розв'язанні систем лінійних рівнянь зі спотвореними правими частинами над скінченними полями або кільцями.

Мета цієї статті – розробити атаку на шифросистему LPN-C над кільцем $R_N = \mathbf{Z}/(2^N)$ на основі послідовного методу, запропонованого в [1]. На відміну від традиційної атаки, яка базується на безпосередньому розв'язанні СЛР зі спотвореними правими частина над кільцем R_N за допомогою алгоритму BKW [7] або його модифікацій чи узагальнень [4, 9, 12], нова атака полягає у послідовному відновленні істинних розв'язків певних СЛР зі спотвореними правими частинами над полем з двох елементів. Показано, що запропонована атака є суттєво більш ефективною як за трудомісткістю, так і за обсягом матеріалу в порівнянні з традиційною атакою. Зокрема, шифросистема LPN-C над кільцем R_N забезпечує майже таку ж саму стійкість відносно послідовної атаки, що і N "паралельно працюючих" шифросистем LPN-C над полем $R_1 = \mathbf{GF}(2)$, що свідчить про недоцільність використання кілець лишків за модулем 2^N, $N \geq 2$, для побудови шифросистем зазначеного типу.

1. Постановка задачі

Розглянемо узагальнення шифросистеми LPN-C на випадок кільця $R_N = \mathbf{Z}/(2^N)$. Згідно з [10], для побудови шифросистеми вибирається $[L, K, D]$-код C, тобто вільний підмодуль вимірності K лівого модуля $R_N{}^L$ 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, виправ-ляти будь-яку комбінацію з $t \le \left\lfloor \frac{D-1}{2} \right\rfloor$. помилок. В ролі ключа використовується випадкова рівно-ймовірна $n \times L$-матриця M над кільцем R_N, а шифроване повідомлення, що отримується в результаті зашифрування відкритого тексту $x \in {R_N}^K$ 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_N, 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 (див. рис. 1).

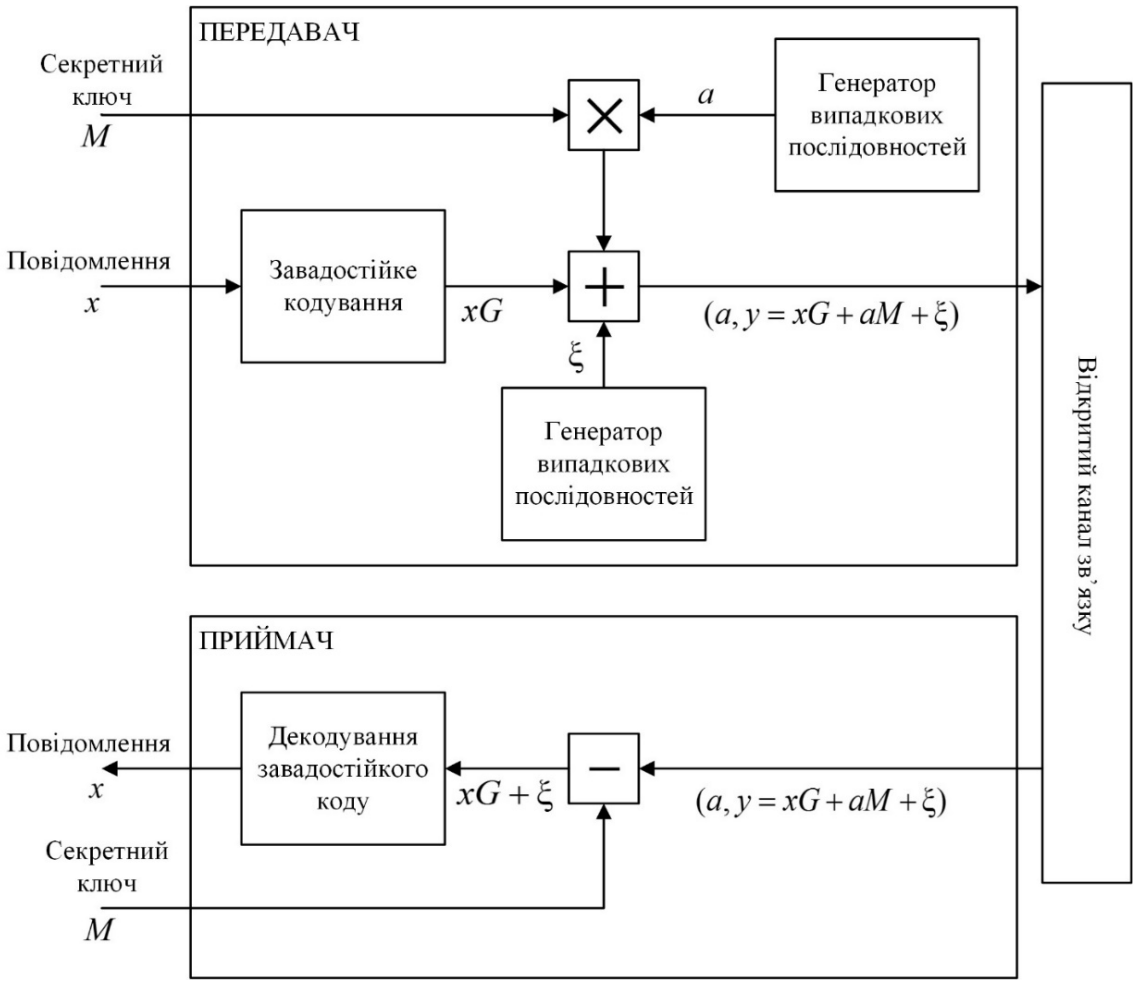

Рис. 1. Схема конфіденційної передачі повідомлень за допомогою шифросистеми LPN-C

При цьому супротивник може реалізувати на шифросистему атаку з вибраним відкритим текстом, зашифровуючи m разів певне фіксоване, наприклад, нульове, повідомлення $x = 0$ та формуючи L СЛР зі спотвореними правими частинами

$$a_i M_j + \xi_{i,j} = y_{i,j},\ i \in \overline{1,m}, \qquad (1)$$

відносно стовпців M_j невідомої матриці M, $j \in \overline{1,L}$, де a_i – незалежні рівноймовірні випадкові вектори довжини n над кільцем R_N, ξ_i – незалежні випадкові вектори довжини L та ваги t над цим кільцем, а $\xi_{i,j}$ та $y_{i,j}$ позначають j-ті координати векторів ξ_i та y_i відповідно, $j \in \overline{1,L}$, $i \in \overline{1,m}$.

Зауважимо, що внаслідок незалежно випадкового вибору векторів a_i, ξ_i при кожному зашифруванні матриця коефіцієнтів СЛР (1), яка складається з рядків $a_1,...,a_m$ над кільцем R_N, є суто випадковою (але відомою супротивнику), а величини $\xi_{1,j},...,\xi_{m,j}$ є незалежними в сукупності та розподілені за законом

$$\mathbf{P}\{\xi_{i,j}=z\}=\frac{\binom{L-1}{t-1}(2^N-1)^{t-1}}{\binom{L}{t}(2^N-1)^t}=\frac{t}{L(2^N-1)},$$

$$z\in R\setminus\{0\},\ \mathbf{P}\{\xi_{i,j}=0\}=1-\frac{t}{L},$$

де $i\in\overline{1,m}$, $j\in\overline{1,L}$. Отже, зазначений закон розподілу має такий вигляд:

$$p_N(0)=2^{-N}(1+(2^N-1)\varepsilon),$$
$$p_N(z)=2^{-N}(1-\varepsilon),\quad z\in R\setminus\{0\}, \tag{2}$$

де

$$\varepsilon=1-\frac{2^N t}{L(2^N-1)}. \tag{3}$$

Традиційна атака на шифросистему LPN-C полягає у складанні та розв'язанні СЛР (1) за допомогою узагальненого алгоритму BKW [4], який є природним узагальненням на випадок довільного скінченного кільця одного з найефективніших на сьогодні алгоритмів розв'язання СЛР зі спотвореними правими частинами над полем з двох елементів [12]. Використовуючи формули для оцінки трудомісткості узагальненого алгоритму BKW (див. [4], теор. 4), можна безпосередньо оцінити стійкість бідь-якої конкретної версії шифросистеми LPN-C над кільцем R_N відносно традиційної атаки. Поряд з тим, специфіка кільця R_N надає принципову можливість застосовувати для розв'язання СРЛ (1) послідовний метод [1], який у певних випадках дозволяє зменшити обчислювальну складність розв'язання цих СЛР. Обґрунтування можливості ефективного застосування послідовного методу для побудови атак на шифросистему LPN-C (шляхом отримання оцінок стійкості шифро-системи відносно таких атак та їх порівняння з традиційною атакою) є основною задачею, що розв'язується далі в статті.

2. Послідовна статистична атака на шифросистему LPN-C

Нагадаємо сутність послідовного методу розв'язання СЛР вигляду (1) за умови, що закон розподілу ймовірностей спотворень у правих частинах рівнянь цієї СЛР визначається за формулами (2), (3). Метод базується на ідеї послідовного вирішення статистичних задач, застосованої до розв'язання булевих систем рівнянь із заважаючими параметрами [2], а також формальному підході до побудови оптимальних за трудомісткістю обчислювальних алгоритмів, який запропоновано в [3].

Ототожнимо елементи кільця R_N з N-вимірними двійковими векторами, вважаючи

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

та задамо відображення $\delta_0,\delta_1: R_N\to R_N$ за формулами $\delta_0(r)=(0,...,0,r_0)$, $\delta_1(r)=(0,r_{N-1},...,r_1)$, де $r=(r_{N-1},...,r_1,r_0)\in R_N$.

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

Розглянемо j-ту СЛР вигляду (1), для розв'язання якої спочатку побудуємо таку систему рівнянь зі спотвореними правими частинами над полем $R_1=\mathbf{GF}(2)$:

$$\delta_0(a_i)\delta_0(M_j)+\delta_0(\xi_{i,j})=\delta_0(y_{i,j}),\ i\in\overline{1,m}. \tag{4}$$

Розв'язуючи отриману СЛР за допомогою будь-якого відомого алгоритму [7, 9, 12], отримаємо оцінку $M^*_{0,j}$ її істинного розв'язку $\delta_0(M_j)$, тобто вектора, який складається з наймолодших розрядів істинного розв'язку СЛР (1). Далі побудуємо систему рівнянь над кільцем R_{N-1}:

$$a_i' z=\delta_1(y_{i,j})-\delta_1(a_i M^*_{0,j}+\xi_i^*),\ i\in\overline{1,m}, \tag{5}$$

де $a_i'=a_i \bmod(2^{N-1})$, $\xi_i^*=\delta_0(y_{i,j}-a_i M^*_{0,j})$ для кожного $i\in\overline{1,m}$.

Зауважимо, що у загальному випадку система рівнянь (5) не є СЛР зі спотвореними правими частинами. Поряд з тим, справедливе таке твердження.

Твердження 1 [1]. Нехай виконується рівність

$$M^*_{0,j}=\delta_0(M_j), \tag{6}$$

тоді система рівнянь (5) є СЛР зі спотвореними правими частинами над кільцем R_{N-1}, яка має істинний розв'язок $\delta_1(M_j)$. При цьому закон розподілу спотворень у правих частинах рівнянь цієї СЛР визначається за формулою

$$p_{N-1}(a_{N-2},...,a_0)=p_N(a_{N-2},...,a_0,0)+$$
$$p_N(a_{N-2},...,a_0,1),\ (a_{N-2},...,a_0)\in R_{N-1},$$

де p_N є розподілом спотворень у правих частинах рівнянь СЛР (1).

З твердження 1 випливає, що за умови (2) розподіл ймовірностей спотворень у правих частинах рівнянь системи (5) має той самий вигляд, що й розподіл спотворень у правих частинах рівнянь СЛР (1) з точністю до заміни N на $N-1$:

$$p_{N-1}(0) = 2^{-(N-1)}(1+(2^{N-1}-1)\varepsilon),$$

$$p_{N-1}(z) = 2^{-(N-1)}(1-\varepsilon),\ z \in R_{N-1} \setminus \{0\}.$$

Крім того, на підставі означення функції δ_0 розподіл спотворень у правих частинах рівнянь булевої СЛР (4) має вигляд

$$p(1) = 1 - p(0) = 1/2 \cdot (1-\varepsilon), \qquad (7)$$

де ε визначається за формулою (3). Це надає можливість використовувати для розв'язання СЛР (5) наведену вище процедуру, яка полягає в побудуванні та розв'язанні для заданої СЛР нових систем рівнянь вигляду (4) та (5) відповідно (із заміною параметра N на $N-1$). Як наслідок, процес знаходження істинного розв'язку СЛР (1) зводиться до

$$T' = NL \cdot \left(T\left(n, 1 - \frac{2^N t}{L(2^N-1)}, \delta N^{-1} L^{-1} \right) + 2(n+1)m'(C_\times(N) + C_+(N)) \right) \qquad (8)$$

двійкових операцій та

$$m' = m\left(n, 1 - \frac{2^N t}{L(2^N-1)}, \delta N^{-1} L^{-1} \right) \qquad (9)$$

зашифровувань, де $C_+ = 5(N-1)$, $C_\times = N(6N-5)$.

Доведення. Атака, зазначена у формулюванні твердження, полягає в побудові для кожного $j \in \overline{1,L}$ системи рівнянь (1) та її розв'язанні з використанням такого *рекурсивного алгоритму* $\mathbf{A}_N$:

1. Якщо $N = 1$, покласти $\mathbf{A}_N = \mathbf{A}$.
2. Якщо $N \geq 2$:

– побудувати за вхідною СЛР (1) систему рівнянь (4) і отримати оцінку $M^*_{0,j}$ її істинного розв'язку $\delta_0(M_j)$ за допомогою алгоритму $\mathbf{A}$;

– побудувати систему рівнянь вигляду (5) над кільцем R_{N-1} та отримати оцінку $M^*_{1,j}$ її істинного розв'язку $\delta_1(M_j)$ за допомогою алгоритму $\mathbf{A}_{N-1}$;

– сформувати оцінку істинного розв'язку СЛР (1) за правилом $M^*_j = M^*_{0,j} + 2M^*_{1,j}$.

З твердження 1 випливає, що наведений алгоритм складається з N кроків, на кожному з яких за допомогою алгоритму $\mathbf{A}$ розв'язується певна булева система з m' лінійних рівнянь зі спотвореннями правими частинами від n невідомих і законом розподілу спотворень (7), причому за означенням параметра m' ймовірність помилки при розв'язанні будь-якої окремої системи рівнянь не перевищує $\delta N^{-1} L^{-1}$. Звідси випливає, що ймовірність помилки алгоритму $\mathbf{A}_N$ при розв'язанні усіх NL зазначених булевих СЛР не перевищує δ.

Далі, при застосуванні алгоритму $\mathbf{A}_N$ до кожної СЛР (1) треба на кожному з N кроків розв'язати деяку булеву СЛР вигляду (4), що потребує

$$T\left(n, \varepsilon, \delta N^{-1} L^{-1}\right) = T\left(n, 1 - \frac{2^N t}{L(2^N-1)}, \delta N^{-1} L^{-1} \right)$$

двійкових операцій, а також побудувати СЛР (5) (за виключенням останнього кроку), що потребує не більше ніж $2(n+1)m'(C_\times(N) + C_+(N))$ двійкових операцій, де $C_\times(N)$ і $C_+(N)$ позначають відповідно двійкові часові складності алгоритмів множення та додавання N-розрядних цілих чисел. Неважко переконатися, що для традиційних алгоритмів додавання та множення справедливі такі оцінки: $C_+ \leq 5(N-1)$ та $C_\times \leq N(6N-5)$. Таким чином, часова складність розв'язання кожної окремої СЛР (1) за допомогою алгоритму $\mathbf{A}_N$ не перевищує

$$N \cdot \left(T\left(n, 1 - \frac{2^N t}{L(2^N-1)}, \delta N^{-1} L^{-1} \right) + 2(n+1)m'(C_\times(N) + C_+(N)) \right)$$

двійкових операцій і, отже, складність розв'язання усіх L зазначених СЛР не перевищує значення (8).

Твердження доведено.

В табл. 1 наведено результати оцінювання часової складності та обсягу матеріалу, потрібного для розв'язання L систем вигляду (1) над кільцем R_N за допомогою узагальненого алгоритму BKW [4] 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. 1 взяті з роботи [10], де їх запропоновано використовувати для побудови шифросистем LPN-C над полем з двох елементів. Параметри $\log T_{\text{BKW}}$ та $\log m$ у табл. 1 позначають двійкові логарифми часової складності та, відповідно, обсягу матеріалу, потрібного для розв'язання усіх СЛР (1) із достовірністю не менше ніж $1-\delta=0{,}99$; для їх обчислення використано формули з теореми 4 роботи [4].

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).

Таблиця 1

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

Зауважимо, що згідно з даними табл. 1, 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 $\mathbf{GF}(2)$. Це свідчить про недоцільність використання кілець лишків за модулем 2^N, $N \geq 2$, для побудови шифросистем зазначеного типу.

Висновки

Запропоновано атаку на шифросистему LPN-C над кільцем $R = \mathbf{Z}/(2^N)$, яка базується на застосуванні послідовного методу розв'язання СЛР зі спотвореними правими частинами над цим кільцем [1]. Показано, що запропонована атака є набагато більш ефективною (як за обчислю-вальною складністю, так і за обсягом матеріалу) у порівнянні з традиційною атакою, яка базується на застосуванні для розв'язання СЛР зі спотвореними правими частинами узагальненого алгоритму BKW.

Отримані результати свідчать про недоцільність застосування для побудови шифросистем LPN-C кілець $R_N = \mathbf{Z}/(2^N)$ при $N \geq 2$, оскільки це не призводить до суттєвого підвищення стійкості у порівнянні з випадком $N = 1$.

ЛІТЕРАТУРА

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

[2]. Г. Балакин, Ю. Никольский, "Последовательное применение метода максимума правдоподобия к решению систем уравнений с мешающими параметрами", *Обозрение прикл. промышл. матем*, Т. 2, Вып. 3, С. 468-476, 1995.

[3]. М. Гаврилкевич, В. Солодовников, "Эффективные алгоритмы решения задач линейной алгебры над полем из двух элементов", *Обозрение прикл. промышл. матем,* Т. 2, Вып. 3, С. 400-437, 1995.

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

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

[6]. 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.

[7]. 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.

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

[9]. S. Bogos, F. Tramer, S. Vaudenay, "On solving LPN using BKW and variants. Implementation and Analysis", *Cryptology ePrint Archive, Report* 2015/049. http://eprint.iacr.org/2015/049.

[10]. H. Gilbert, J.B. Mattew, M.J.B. Robshaw, Y. Seurin, "How to Encrypt with the LPN Problem", *ICALP (2), Proceedings. Springer Verlag*, pp. 679-690, 2008.

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

[12]. 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. http://eprint.iacr.org/2016/311.

APPLICATION OF SEQUENTIAL METHOD FOR CONSTRUCTING A STATISTICAL ATTACK ON THE LPN-C CIPHER SYSTEM OVER RESIDUE RING MODULO 2^N

LPN-C is one of the first post-quantum symmetric cipher systems, which security relies on the complexity of solving the LPN problem. The original version of the cipher system is defined over the field of two elements, nevertheless it is naturally generalized to the case of an arbitrary finite ring. Usually such generalization associated with the complication of the algebraic structure of underlain object used for construction of a cipher system increases its security to known attacks, however, as shown below, the LPN-C cipher system over a residue ring modulo 2^N represents an exception to this rule. In this article, an attack on the LPN-C cipher system over the residue ring modulo 2^N is proposed. The attack is based on recovering the key by sequential solving N systems of linear equations corrupted by noise over the field of order two. It is shown that the proposed attack is significantly more effective in comparison with traditional attacks of the same type based on direct solving these systems using the generalized BKW algorithm. The obtained results indicate that the residue rings modulo 2^N, $N \geq 2$, are not expedient for constructing LPN-C cipher systems, since this does not lead to significant increasing the security in comparison with $N = 1$ case.

Keywords: post-quantum cryptography, LPN-C cipher system, system of linear equations corrupted by noise, residue ring modulo 2^N, sequential method, generalized BKW algorithm, fast statistical attack.

ПРИМЕНЕНИЕ ПОСЛЕДОВАТЕЛЬНОГО МЕТОДА ДЛЯ ПОСТРОЕНИЯ СТАТИСТИЧЕСКОЙ АТАКИ НА ШИФРОСИСТЕМУ LPN-C НАД КОЛЬЦОМ ВЫЧЕТОВ ПО МОДУЛЮ 2^N

Шифросистема LPN-C является одной из первых постквантовых симметричных шифросистем, устойчивость которых базируется на сложности решения задачи LPN. Оригинальная версия шифросистемы определяется над полем из двух элементов, однако она естественным образом обобщается на случай произвольного конечного кольца. Как правило, такое обобщение, связанное с усложнением алгебраической структуры объекта, на основе которого строится та или иная шифросистема, увеличивает ее устойчивость относительно известных атак, однако, как показано ниже, шифросистема LPN-C над кольцом по модулю 2^N представляет собой исключение из этого правила. В данной статье предлагается атаку на шифросистему LPN-C над кольцом вычетов по модулю 2^N, которая заключается в восстановлении ключа путем последовательного решения систем линейных уравнений с исказит ными правыми частями над полем из двух элементов. Показано, что предложенная атака существенно более эффективной по сравнению с традиционной атакой того же типа, основанный на непосредственном решении указанной системы уравнений с помощью обобщенного алгоритма BKW. Полученные результаты свидетельствуют о нецелесообразности применения для построения шифросистем LPN-C колец вычетов по модулю 2^N, при $N \geq 2$, поскольку это не приводит к существенному повышению устойчивости по сравнению со случаем $N = 1$.

Ключевые слова: постквантова криптография, шифросистема LPN-C, система линейных уравнений с искаженными правыми частями, кольцо вычетов по модулю 2^N, последовательный метод, обобщенный алгоритм BKW, быстрая стать-соприкасающаяся атака.

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».