УДК 621.391:519.2

А.М. ОЛЕКСІЙЧУК, д-р техн. наук, С.М. ІГНАТЕНКО

АЛГОРИТМИ ОЦІНЮВАННЯ СТІЙКОСТІ SNOW 2.0-ПОДІБНИХ ПОТОКОВИХ ШИФРІВ НАД КІЛЬЦЯМИ ЛИШКІВ ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК

Вступ

Потоковий шифр SNOW 2.0 [1] запропонований у 2002 році як альтернатива попередньої (більш слабкої) версії – SNOW. На сьогодні цей шифр є стандартизованим [2] та являє собою один з найбільш швидких програмно орієнтованих потокових шифрів.

Найбільш потужними з відомих атак на SNOW 2.0 є кореляційні атаки, сутність яких полягає у складанні та розв'язанні певних систем лінійних рівнянь зі спотвореними правими частинами [3 – 6].

Метою даної статті є відповідь на запитання про те, чи можна підвищити стійкість SNOW 2.0 відносно відомих кореляційних атак шляхом (повної) заміни у схемі генератора гами цього шифру порозрядного булевого додавання арифметичним додаванням за модулем 2^{32}, а також заміни нелінійної підстановки у схемі генератора іншим (швидким) перетворенням.

В п. 1 наведено означення класу SNOW 2.0-подібних потокових шифрів над кільцем лишків за модулем 2^N та описану загальну схему побудови кореляційних атак на них, аналогічних відомим атакам на SNOW 2.0. В п. 2 – 4 на основі аналізу відомих методів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над кільцем лишків за модулем 2^N [7 – 12] наведено алгоритми оцінювання обчислювальної складності зазначених кореляційних атак на шифри, що розглядаються, а п. 5 – відповідні чисельні оцінки їх стійкості відносно цих атак. Наприкінці статті сформульовано стислі висновки.

В цілому отримані результати свідчать про помітну перевагу, з погляду стійкості відносно відомих кореляційних атак, SNOW 2.0-подібних шифрів над кільцями лишків у порівнянні з традиційними SNOW 2.0-подібними шифрами. Поряд з тим, питання про стійкість розглянутих у цій статті шифрів відносно інших (зокрема, алгебраїчних) атак потребує окремого дослідження.

1. Кореляційні атаки на SNOW 2.0-подібні шифри над кільцями лишків за модулем 2^N

Розглянемо генератор гами SNOW 2.0-подібного потокового шифру, який складається з лінійного регістру зсуву (ЛРЗ) над кільцем $R_N = \mathbf{Z}/(2^N)$ та підстановки $\sigma: R_N \to R_N$, поєднаних між собою, як зазначено на рис. 1. Вважатимемо, що многочлен зворотного зв'язку ЛРЗ $g(z) = z^n - (c_{n-1}z^{n-1} + \ldots + c_0)$ над кільцем R_N є многочленом максимального періоду (який дорівнює $2^{N-1}(2^n - 1)$ [13]), а ЛРЗ виробляє лінійну рекурентну послідовність $x_0, x_1, \ldots$, знаки якої пов'язані співвідношенням $x_{i+n} = c_{n-1}x_{i+n-1} + \ldots + c_0 x_i$, $i = 0, 1, \ldots$. Генератор гами являє собою скінченний автономний автомат з множиною внутрішніх станів $R_N{}^n \times R_N{}^2$, функцією переходів

$$h((z_{n-1}, z_{n-2}, \ldots, z_0), u, v) = ((z_n, z_{n-1}, \ldots, z_1), z_\mu + v, \sigma(u)),$$

та функцією виходів

$$f((z_{n-1}, z_{n-2}, \ldots, z_0), u, v) = z_0 + z_{n-1} + u + v,$$

де $z_0, \ldots, z_{n-1}, u, v \in R_N$, $x_n = c_{n-1}x_{n-1} + \ldots + c_0 x_0$. Отже, знак гами в i-му такті визначається за початковим станом $((x_{n-1}, x_{n-2}, \ldots, x_0), u_0, v_0)$ генератора за допомогою таких рекурентних співвідношень:

$$\gamma_i = x_i + x_{i+n-1} + u_i + v_i\,,\ u_{i+1} = x_{i+\mu} + v_i\,,\ v_{i+1} = \sigma(u_i)\,,\ i = 0, 1, \ldots. \qquad (1)$$

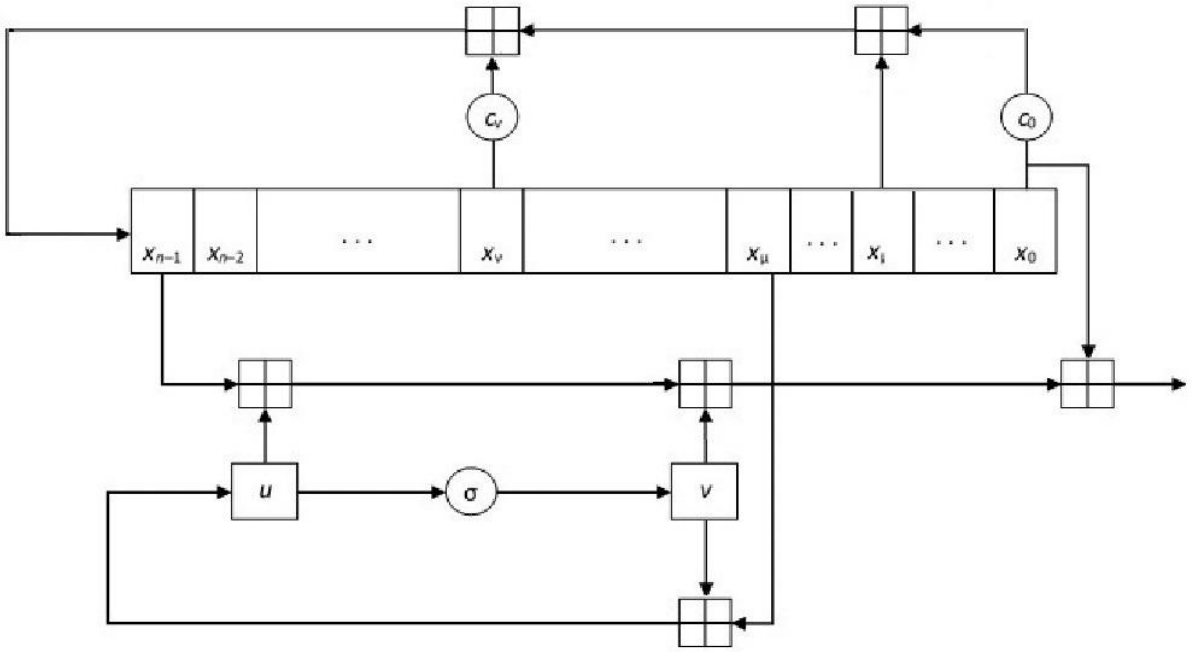

Рис. 1. Схема генератора гами SNOW 2.0-подібного шифру

Зауважимо, що головною відмінністю генератора, що розглядається, від генераторів гами звичайних SNOW 2.0-подібних потокових шифрів [14] є застосування операції + додавання в кільці R_N замість операції $\oplus$ порозрядного додавання двійкових векторів за модулем 2.

Відомі на сьогодні кореляційні атаки на шифр SNOW 2.0 [3 – 6] базуються на тому, що сума (за модулем 2) знаків гами в будь-яких суміжних тактах є результатом спотворення знаку певної лінійної рекуренти з характеристичним многочленом $g(z)$. Для генератора, що розглядається, на підставі співвідношень (1) справедливі такі рівності:

$$\gamma_{i+1} - \gamma_i = x_{i+1} + x_{i+n} - x_i - x_{i+n-1} + x_{i+\mu} + \xi_i\,,\ i = 0, 1, \ldots, \qquad (2)$$

де

$$\xi_i = \sigma(u_i) - u_i\,,\ i = 0, 1, \ldots. \qquad (3)$$

Вважаючи, що змінні $u_0, u_1, \ldots$ є незалежними випадковими величинами з рівномірним розподілом на кільці R_N та виражаючи знаки $x_i, x_{i+1}, x_{i+\mu}, x_{i+n-1}, x_{i+n}$ лінійної рекуренти через початковий стан ЛРЗ на рис. 1, отримаємо систему лінійних рівнянь (2) зі спотвореними правими частинами над кільцем R_N, де спотворення є випадковими величинами (3). Кореляційні атаки, що розглядаються, полягають у розв'язанні цієї системи рівнянь (СР) за допомогою відомих методів [7 – 12].

Позначимо $\sigma'(u) = \sigma(u) - u\,,\ u \in R_N$. Тоді

$$p(z) = \mathbf{P}\{\xi_i = z\} = 2^{-N}\,|\{u \in R_N : \sigma'(u) = z\}|\,,\ z \in R_N\,,\ i = 0, 1, \ldots. \qquad (4)$$

Отже, з погляду спроможності генератора протистояти кореляційним атакам, що базуються на розв'язанні СР (2), найкращим способом вибору підстановки σ є такий, коли розподіл (4) є рівномірним або, що те ж саме, відображення σ' є підстановкою на кільці R_N. Поряд з тим, при $N \geq 2$ таких підстановок σ не існує [15]. Проте існують підстановки σ, для яких розподіл (4) відрізняється від рівномірного розподілу ймовірностей на кільці R_N лише у двох точках:

$$p(0)=0,\ \ p(2^{N-1})=2^{1-N},\ p(z)=2^{-N},\ z\in R_N\setminus\{0,\,2^{N-1}\}. \tag{5}$$

Як приклад, зазначимо підстановку σ, значення якої в точці $z\in R_N$ дорівнює циклічному зсуву двійкового запису числа z в бік старших розрядів [15].

Отже, далі вважатимемо, що підстановка σ вибрана таким чином, що розподіл ймовірностей (4) має вигляд (5). Базуючись на результатах робіт [7 – 12], оцінимо обчислювальну складність розв'язання цієї СР за допомогою відомих методів.

2. Метод максимуму правдоподібності

Запишемо перші m рівнянь системи (2) у вигляді

$$Ax=b, \tag{6}$$

де A є (відомою) $m\times n$-матрицею над кільцем R_N, b є вектором з координатами

$$b_i=A_i a+\xi_i,\ i\in\overline{1,m}, \tag{7}$$

де $A_1,\dots,A_m$ – рядки матриці A, $a=(a_1,\dots,a_n)^{\mathrm{T}}$ – невідомий вектор-стовпець над кільцем R_N, який співпадає з початковим станом ЛРЗ на рис. 1, $\xi_1,\dots,\xi_m$ – незалежні випадкові величини, розподілені за законом (4).

Для будь-якого $x\in {R_N}^n$ позначимо $\varepsilon(x)=b-Ax$. Нагадаємо (див., наприклад, [7, 16]), що розв'язання СР (2) методом максимуму правдоподібності (ММП) полягає в знаходженні "оцінки" a^* вектора a за правилом $\mathbf{P}\{\xi=\varepsilon(a^*)\}=\max\limits_{x\in R^n}\mathbf{P}\{\xi=\varepsilon(x)\}$, де $\xi=(\xi_1,\dots,\xi_m)$. Якщо вектор a є рівномірно розподіленим на множині ${R_N}^n$, то ММП має найменшу середню ймовірність помилки серед усіх методів розв'язання СР (2) (див., наприклад, [16]).

Як випливає з результатів робіт [7, 11], для відновлення вектора a за допомогою ММП з імовірністю не менше $1-\delta$, $\delta\in(0,\,1/2)$, необхідно виконати не менше ніж

$$T=nm_0 2^{Nn}(6N^2-N) \tag{8}$$

двійкових операцій, де

$$m_0=\frac{nN(1-\delta)-h(\delta)}{\Delta(p_\xi)}\ln 2,$$

$$h(\delta)=-\delta\log_2\delta-(1-\delta)\log_2(1-\delta),\ \Delta(p_\xi)=2^{-N}\sum_{z\in R_N}(2^N p(z)-1)^2.$$

3. Послідовний метод

Цей метод запропоновано в [8] і полягає у послідовному відновленні двійкових розрядів координат невідомого вектора a шляхом розв'язання систем лінійних рівнянь зі спотвореними правими частинами, які отримуються з вхідної СР (2) за допомогою канонічних гомоморфізмів кільця R_N в кільця $R_i=\mathbf{Z}/(2^i)$, $i\in\overline{0,N-1}$. Необхідною умовою застосовності методу є відмінність розподілу випадкових величин $\xi_j(\mathrm{mod}2^i)$, $j\in\overline{1,m}$, від рівномірного розподілу ймовірностей на кільці R_i для деякого $i\in\overline{0,N-1}$.

Як випливає з формул (4), (5), для будь-яких $j\in\overline{1,m}$, $z\in R_{N-1}$ справедлива рівність $\mathbf{P}\{\xi_j(\mathrm{mod}2^{N-1})=z\}=2^{-(N-1)}$. Отже, випадкові величини $\xi_j(\mathrm{mod}2^i)$, $j\in\overline{1,m}$, є рівномірно розподіленими на кільці R_i для кожного $i\in\overline{0,N-1}$, і послідовний метод є незастосовним для побудови кореляційних атак на генератор гами, що розглядається.

4. Узагальнений алгоритм BKW та його модифікації

Узагальнений алгоритм BKW [11] є природним узагальненням (на випадок довільного скінченного кільця) одного з найкращих на сьогодні алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами над полем з двох елементів [17, 18]. Цей алгоритм складається з двох етапів, на першому з яких за вхідною СР (2) над кільцем R_N певним чином будується нова система лінійних рівнянь зі спотвореними правими частинами від $n_1 \le n-3$ змінних. Потім, на другому етапі отримана система рівнянь розв'язується за допомогою ММП.

В [10, 12] запропоновано використовувати замість традиційного ММП його модифікації, які базуються, відповідно, на швидкому перетворенні Фур'є та швидкому перетворенні Ферма деяких допоміжних функцій. Показано, що за певних умов це дозволяє помітно зменшити трудомісткість узагальненого алгоритму BKW.

Для оцінювання складності узагальненого алгоритму та його модифікацій введемо низку додаткових позначень. Для будь-якого $n_1 \in \overline{1, n-3}$ позначимо

$$u = \left\lceil \frac{\log(n-n_1)}{2} \right\rceil,\ v = \left\lceil \frac{2(n-n_1)}{\log(n-n_1)} \right\rceil,\ k = 2^{u-1}. \tag{9}$$

Далі, позначимо $p_\xi^{(k)} = (p^{(k)}(z) : z \in R_N)$ розподіл ймовірностей випадкової величини $\xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, де $\xi_1, ..., \xi_k$ є незалежними випадковими величинами, розподіленими за законом (4). Покладемо

$$N_k = \{z \in R_N : p^{(k)}(z) > 0\},\ p_{\max} = \max_{z \in R_N} p^{(k)}(z),\ p_{\min} = \min_{z \in N_k} p^{(k)}(z),$$

$$D(p^{(k)} \| \omega) = \sum_{z \in N_k} p^{(k)}(z) \log(2^N p^{(k)}(z)),\ D(\omega \| p^{(k)}) = -2^{-N} \sum_{z \in N_k} \log(2^N p^{(k)}(z)),$$

$$D_a = \sum_{z \in N_k} p^{(k)}(z) \log^2(2^N p^{(k)}(z)) - D(p^{(k)} \| \omega)^2,\ D = 2^{-N} \sum_{z \in N_k} \log^2(2^N p^{(k)}(z)) - D(\omega \| p^{(k)})^2,$$

$$m_1 = \frac{2n_1 \ln(2^{N+1}\delta^{-1})(\log p_{\max} - \log p_{\min})^2}{(D(p^{(k)} \| \omega) + D(\omega \| p^{(k)}))^2},\ m_2 = \left(\frac{u_\alpha \sqrt{D_a} + u_\beta \sqrt{D_x}}{D(p^{(k)} \| \omega) + D(\omega \| p^{(k)})} \right)^2,$$

де u_α, u_β – квантилі стандартного нормального розподілу, $\alpha, \beta > 0$, $\alpha + (2^{Nn_1} - 1)\beta \le \delta/2$, $\delta \in (0, 1/2)$. Нарешті, покладемо

$$t = \min\{m_1, m_2\},\ l = (u + \left\lceil \ln(2t\delta^{-1}) \right\rceil - 1)q^v, \tag{10}$$

$$m(n_1) = lt. \tag{11}$$

На підставі результатів робіт [9 – 12] трудомісткості узагальненого алгоритму BKW та його модифікацій можна оцінити за допомогою алгоритмів 1, 2, 3.

Алгоритм 1 (обчислення трудомісткості узагальненого алгоритму BKW)

Вхідні дані:

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

– число $\delta \in (0, 1/2)$.

Алгоритм обчислень.

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

1. Обчислити значення (9), (10), (11).

2. Обчислити $T_{\mathrm{BKW}}(n_1) = 2^{Nn_1+1} n_1 t + ult$.

Результат: число n_1 таке, що $T_{\mathrm{BKW}}(n_1) = \min\{T_{\mathrm{BKW}}(s) : s \in \overline{1, n-3}\}$ та відповідні значення $T_{\mathrm{BKW}}(n_1)$, $m(n_1)$.

Алгоритм 2 (обчислення трудомісткості модифікації узагальненого алгоритму BKW, що базується на швидкому перетворенні Фур'є).

Вхідні дані:

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

– число $\delta \in (0, 1/2)$.

Алгоритм обчислень.

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

1. Обчислити значення (9) – (11).
2. Обчислити

$$T'(n_1, t) = \; 5 \cdot 2^{(n_1+2)N+1} N n_1 \log(2^{N+1} N n_1 t) + 2^{2N} t((n_1+1)N(6N-5) + 5(N-1)),$$

$$T'_{\mathrm{BKW}}(n_1) = T'(n_1, t) + ult.$$

Результат: число $n_1{*}$ таке, що $T'_{\mathrm{BKW}}(n_1{*}) = \min\{T'_{\mathrm{BKW}}(n_1) : n_1 \in \overline{1, n-3}\}$ та відповідні значення $T'_{\mathrm{BKW}}(n_1{*})$, $m(n_1{*})$.

Алгоритм 3 (обчислення трудомісткості модифікації узагальненого алгоритму BKW, що базується на швидкому перетворенні Ферма).

Вхідні дані:

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

– число $\delta \in (0, 1/2)$.

Алгоритм обчислень.

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

3. Обчислити значення (9), (10), (11).
4. Обчислити

$$T''(n_1, t) = 26 \cdot 2^{N(n_1+1)} N n_1 + 2^{2N} t((n_1+1)N(6N-5) + 5(N-1) + 7 \cdot 2^{N-1} + 2),$$

$$T''_{\mathrm{BKW}}(n_1) = T''(n_1, t) + ult.$$

Результат: число $\tilde{n}_1{*}$ таке, що $T''_{\mathrm{BKW}}(\tilde{n}_1{*}) = \min\{T''_{\mathrm{BKW}}(n_1) : n_1 \in \overline{1, n-3}\}$ та відповідні значення $T''_{\mathrm{BKW}}(\tilde{n}_1{*})$, $m(\tilde{n}_1{*})$.

Зауважимо, що наведені алгоритми можна застосовувати до оцінювання обчислювальної складності розв'язання будь-яких систем лінійних рівнянь зі спотвореними правими частинами над кільцем лишків за модулем 2^N.

5. Оцінки складності кореляційних атак на SNOW 2.0-подібні потокові шифри

В таблиці наведено оцінки обсягу матеріалу, потрібного для розв'язання СР (2) із заданою достовірністю, а також обчислювальної складності розв'язання цієї СР за допомогою ММП, узагальненого алгоритму BKW та його модифікацій.

Символом T в таблиці позначено нижню межу (8) часової складності ММП; символи $T_{\mathrm{BKW}}(n_1)$, $T'_{\mathrm{BKW}}(n_1{*})$ та $T''_{\mathrm{BKW}}(\tilde{n}_1{*})$ позначають трудомісткості узагальненого алгоритму BKW та його модифікацій із застосуванням швидкого перетворення Фур'є та швидкого перетворення Ферма відповідно, а символи $m(n_1)$, $m(n_1{*})$ і $m(\tilde{n}_1{*})$ позначають обсяг матеріалу (кількість рівнянь в системі (2)), потрібного для успішного застосування узагальненого алгоритму BKW та його модифікацій з використанням швидкого перетворення Фур'є та швидкого перетворення Ферма відповідно.

При проведенні розрахунків використано інформацію про розподіл ймовірностей $p_\xi^{(k)}$, що на підставі формули (5) має такий вигляд:

$$p_\xi^{(k)}(0) = 2^{-N}(1+2^{-(N-1)(k-1)}),\ p_\xi^{(k)}(2^{N-1}) = 2^{-N}(1-2^{-(N-1)(k-1)}),\ p_\xi^{(k)}(z) = 2^{-N},$$
$$z \in R_N \setminus \{0, 2^{N-1}\}.$$

Результати оцінювання стійкості SNOW 2.0-подібних шифрів над кільцями лишків відносно кореляційних атак

Параметр	$n=64,\ N=8$	$n=16,\ N=32$
$\log T$	542,01	568,03
n_1	17	7
n_1*	21	7
$\widetilde{n}_1*$	21	7
$\log T_{\text{BKW}}(n_1)$	200,93	329,26
$\log T'_{\text{BKW}}(n_1*)$	199,20	304,65
$\log T''_{\text{BKW}}(\widetilde{n}_1*)$	192,69	300,72
$\log m(n_1)$	199,04	299,72
$\log m(n_1*)$	191,04	299,72
$\log m(\widetilde{n}_1*)$	191,04	299,72

Як видно з таблиці, за умов (4), (5) для розв'язання СР (2) від $n=64$ невідомих над кільцем $R_N = \mathbf{Z}/(2^8)$ за допомогою ММП необхідно не менше ніж $2^{542,01}$ двійкових операцій. При цьому для відновлення будь-яких $n_1=17$ невідомих з цієї системи рівнянь за допомогою узагальненого алгоритму BKW потрібно лише $2^{200,93}$ операцій та $2^{199,04}$ рівнянь, а при застосуванні швидкого перетворення Ферма – тільки $2^{192,69}$ операцій та $2^{191,04}$ рівнянь. Отже, складність найкращої (з відомих на сьогодні) кореляційних атак на SNOW 2.0-подібний шифр, що розглядається, складає $\left\lceil \frac{64}{21} \right\rceil \cdot 2^{192,69} = 2^{194,69}$ операцій при обсязі матеріалу $\left\lceil \frac{64}{21} \right\rceil \cdot 2^{191,04} = 2^{193,04}$ знаків вихідної послідовності генератора.

При $n=16,\ N=32$ (параметри шифру SNOW 2.0) найкраща з відомих кореляційних атак на шифр потребує $\left\lceil \frac{16}{7} \right\rceil \cdot 2^{300,72} = 2^{302,31}$ операцій та $\left\lceil \frac{16}{7} \right\rceil \cdot 2^{299,72} = 2^{301,31}$ знаків гами (при цьому довжина ЛРЗ генератора складає 512 біт). Зауважимо також, що найкраща з відомих кореляційних атак на оригінальний шифр SNOW 2.0 має обчислювальну складність $2^{164,15}$ операцій та потребує $2^{163,59}$ знаків гами [6].

Висновки

Отримані результати свідчать про можливість безпосереднього застосування методів робіт [7 – 12] до вирішення задачі оцінювання стійкості потокових шифрів над кільцями лишків за модулем 2^N відносно кореляційних атак. Вони надають також можливість цілеспрямовано вибирати компоненти зазначених шифрів для підвищення їх стійкості.

Модифікації узагальненого алгоритму BKW, побудовані на основі швидких перетворень Фур'є або Ферма [10, 12], мають меншу часову складність у порівнянні з традиційною версією цього алгоритму [11]. Зокрема, застосування швидкого перетворення Ферма на другому

етапі узагальненого алгоритму BKW зменшує складність кореляційної атаки на розглянуті версії SNOW 2.0-подібних шифрів у $2^{8,24}$ – $2^{28,54}$ разів в залежності від параметрів n та N.

Заміна в схемі генератора гами шифру SNOW 2.0 порозрядного булевого додавання арифметичним додавання за модулем 2^N приводить (за умови належного вибору підстановки σ) до суттєвого підвищення стійкості шифру відносно відомих кореляційних атак. Зокрема, найкраща з таких атак на розглянуту 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 [6] має обчислювальну складність $2^{164,15}$ та потребує $2^{163,59}$ знаків гами.

Список літератури:

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

2. ISO/IEC 18033-4: 2011(E). Information technology Security techniques Encryption algorithm Part 4: Stream ciphers 2011. 92 p.

3. Nyberg K., Wallen J. Improved linear distinguishers for SNOW 2.0 // Fast Software Encryption FSE 2006. LNCS 4047. Springer-Verlag. P. 144-162.

4. Maximov A., Johansson T. Fast computation for large distribution and its cryptographic application // Advanced in Cryptology ASIACRYPT 2005. LNCS 3788. Springer-Verlag. P. 313-332.

5. Lee J.-K., Lee D.H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks // Advanced in Cryptology ASIACRYPT 2008. LNCS 5350. Springer-Verlag. P. 524-538.

6. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0 // http://eprint.iacr.org/2016/311.

7. Алексейчук А.Н., Игнатенко С.М. Оценки эффективности универсальных методов восстановления искаженных линейных рекуррент над кольцом вычетов по модулю 2^N // Зб. наук. праць ІПМЕ НАН України. 2003. Вип. 20. С. 40–48.

8. 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.

9. 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. С. 5-12.

10. 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. С. 63-72. 11. Олексійчук А.М., Ігнатенко С.М., Поремський М.В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями // Математичне та комп'ютерне моделювання. Сер.: Техн. науки. 2017. Вип. 15. С. 150-155.

12. Олексійчук А.М., Ігнатенко С.М. Застосування швидкого перетворення Фур'є для розв'язання задачі LPN над скінченими фробеніусовими кільцями // Захист інформації. 2017. № 4. С. 271-277.

13. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Псевдослучайные и полилинейные последовательности // Труды по дискретной математике. Москва : ТВП. Т. 1. 1997. С. 139-202.

14. Олексійчук А.М. Достатня умова стійкості SNOW 2.0-подібних потокових шифрів відносно певних атак зі зв'язаними ключами // Захист інформації. 2016. Т. 18. № 3. С. 261-268.

15. Vaudenay S. On the Lai-Massey scheme // Advanced in Cryptology ASIACRYPT'99. Springer-Verlag. 1999. P. 8-19.

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

17. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model // J. ACM. 2003. Vol. 50. № 3. P. 506-519.

18. Bogos S., Tram′er F., Vaudenay S. On solving LPN using BKW and variants. Implementation and analysis // http://eprint.iacr.org/2015/049.

Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Надійшла до редколегії 07.03.2018