УДК 621.391:519.2
DOI: 10.32626/2308-5916.2019-19.114-119

А. М. Олексійчук, д-р техн. наук,
С. М. Конюшок, канд. техн. наук,
М. В. Поремський, аспірант

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

ОБҐРУНТУВАННЯ СТІЙКОСТІ ПОТОКОВОГО ШИФРУ «СТРУМОК» ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК НАД СКІНЧЕННИМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Потоковий шифр SNOW 2.0 запропонований у 2002 р. як альтернатива попередньої (більш слабкої) версії — SNOW. На сьогодні цей шифр є стандартизованим 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 систем лінійних рівнянь із спотвореними правими частинами, зокрема, систем рівнянь над полями порядку більшого ніж 2. Не дивлячись на певний прогрес у цьому напрямі, залишаються не вирішеними задачі, пов'язані з розробкою методів оцінювання та обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак. На сьогодні відсутні методи, які дозволяють обґрунтовувати стійкість зазначених шифрів відносно відомих кореляційних атак безпосередньо за параметрами їх компонент. Крім того, спроба застосувати відомі методи оцінювання стійкості SNOW 2.0 відносно кореляційних атак до інших потокових шифрів (наприклад, шифру «Струмок», який запропоновано в ролі кандидата на національний стандарт шифрування України) наштовхується на труднощі, пов'язані з розміром задач, які треба розв'язувати для отримання оцінок. На відміну від SNOW 2.0, побудованого над полем порядку 2^{32}, шифр «Струмок» задається над полем порядку 2^{64}, що призводить до неможливості практичного застосування відомих певних алгоритмів, часова складність яких збільшується від $2^{32} \div 2^{37}$ до 2^{64} двійкових операцій.

Мета даної роботи — обґрунтування стійкості шифру «Струмок» відносно широкого класу кореляційних атак, який охоплює, зокрема, відомі атаки на SNOW 2.0. Основним результатом є теорема, яка встановлює аналітичну оцінку параметра, що характеризує ефективність кореляційних атак на SNOW 2.0-подібні шифри у термінах їх компонент. Це дозволяє на практи-

ці оцінювати та обґрунтовувати стійкість таких шифрів відносно кореляційних атак над полями характеристики 2.

Ключові слова: *потоковий шифр, кореляційний криптоаналіз, система лінійних рівнянь зі спотвореними правими частинами, обґрунтування стійкості, «Струмок».*

Вступ. Нагадаємо означення класу SNOW 2.0-подібних потокових шифрів [1, 2], до яких відноситься шифр «Струмок» [3].

Позначимо V_r множину двійкових векторів довжини $r \geq 2$. Задамо на цій множині структуру поля порядку 2^r, узгоджену з операцією $\oplus$ покоординатного булевого додавання двійкових векторів. Ототожнимо також звичайним чином елементи множини V_r з r-розрядними цілими числами та позначимо символом $+$ операцію додавання цих чисел за модулем 2^r.

За означенням [2] вхідними даними для побудови генератора гами r-розрядного SNOW 2.0-подібного потокового шифру є примітивний многочлен $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \ldots \oplus c_0$ над полем F_{2^r}, підстановка $\sigma : V_r \to V_r$ та натуральне число $\mu \in \overline{1, n-2}$. Генератор гами являє собою скінченний автономний автомат з множиною станів $V_r{}^n \times V_r{}^2$, функцією переходів

$$h((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = ((x_n, x_{n-1}, \ldots, x_1), x_\mu + v, \sigma(u)),$$

та функцією виходів

$$f((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = x_0 \oplus (x_{n-1} + u) \oplus v,$$

де $x_0, \ldots, x_{n-1}, u, v \in V_r$, $x_n = c_{n-1}x_{n-1} \oplus \ldots \oplus c_0 x_0$. 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 рекурентних співвідношень $\gamma_i = x_i \oplus (x_{i+n-1} + u_i) \oplus v_i$, $u_{i+1} = x_{i+\mu} + v_i$, $v_{i+1} = \sigma(u_i)$, справедливих для усіх $i = 0, 1, \ldots$.

Надалі вважатимемо, що $r = pt$, де $p, t \in \mathbf{N}$, $p, t \geq 2$, і підстановка σ має такий вигляд:

$$\sigma(z_1, \ldots, z_p) = (s_1(z_1), \ldots, s_p(z_p))D, \ (z_1, \ldots, z_p) \in F_{2^t}^p, \qquad (1)$$

де s_i — підстановка (вузол заміни) на множині V_t, яка ототожнюється з адитивною групою поля F_{2^t}, $i \in \overline{1, p}$, D — оборотна матриця порядку p над полем F_{2^t}.

Зауважимо, що у шифрі «Струмок» використовуються такі параметри [3]: $t = 8$, $p = 8$ ($r = 64$), $n = 16$, $\mu = 13$. Підстановка σ

має вигляд (1), де вузли заміни та матриця D задаються так само, як у блоковому шифрі «Калина» [4].

Постановка задачі й отримані результати. Найбільш потужними з відомих сьогодні атак на SNOW 2.0 є кореляційні атаки [5–8], спрямовані на відновлення початкового стану лінійного регістру зсуву (ЛРЗ), що входить до складу генератора, за шифрувальною гамою. В роботі [9] описано загальну схему побудови таких атак на довільні SNOW 2.0-подібні шифри і показано, що усі вони базуються на складанні та розв'язанні певних наслідків системи лінійних рівнянь із спотвореними правими частинами

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

де

$$\xi_i = ((x_{i+n-1} + u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)) \oplus ((x_{i+n} + x_{i+\mu} + v_i) \oplus \\ \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i)), \; i = 0, 1, \ldots, \qquad (3)$$

причому знаки x_i, x_{i+1}, $x_{i+\mu}$, x_{i+n-1}, x_{i+n} лінійної рекуренти у формулі (2) є відомими лінійними функціями початкового стану ЛРЗ, а змінні $x_{i+\mu}$, x_{i+n-1}, x_{i+n}, u_i, v_i у формулі (3) є незалежними випадковими величинами з рівномірним розподілом на множині V_r.

Відповідно до [9] будь-яка кореляційна атака на шифр визначається додатним дільником r' числа r та ненульовим елементом c поля F_{2^r} і полягає у складанні та розв'язанні певної системи рівнянь від $l = nr''$ невідомих, де $r'r'' = r$, із спотвореними правими частинами над полем $F_{2^{r'}}$, причому закон розподілу спотворень η_i у правих частинах рівнянь має такий вигляд:

$$\mathbf{P}\{\eta_i = z\} \;\; = \sum_{x \in F_{2^r}:\; \mathrm{Tr}_{2^{r'}}^{2^r}(cx) = z} \mathbf{P}\{\xi_i = x\}, \; z \in F_{2^{r'}}, \qquad (4)$$

$i = 0, 1, \ldots$, де $\mathrm{Tr}_{2^{r'}}^{2^r}(\cdot)$ позначає функцію сліду поля F_{2^r} в полі $F_{2^{r'}}$.

Для оцінювання середньої трудомісткості атаки і обсягу матеріалу (кількості знаків гами), потрібного для її успішної реалізації, можна використовувати наступний алгоритм [8].

Алгоритм 1.

Вхідні дані:

- натуральні числа n, p, t;
- число $k \geq 2$, що є степенем двійки;
- верхня оцінка $\Delta_{r'}(k)$ параметра

$$\Delta_{c,r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\} - 1)^2, \qquad (5)$$

де $\eta_1,...,\eta_k$ є незалежними випадковими величинами, розподіленими за законом (4).

1. Покласти $r'' = pt(r')^{-1}$, $l = nr''$, $\theta = 1 + \log k$.
2. Для кожного $l' \in \overline{1, l-1}$ обчислити

$$m_{r'}(k) = 2(\Delta_{r'}(k))^{-1} l' r' \ln 2,$$

$$T_{r'}(k,l') = (m_{r'}(k))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{r'}(k) + r' l' 2^{r' l'}) + 2^{r'(l'+1)}.$$

3. Обрати $l^* \in \overline{1, l-1}$ таке, що $T_{r'}(k,l^*) = \min\{T_{r'}(k,l') : l' \in \overline{1, l-1}\}$.

Результат:

- число l^* фрагментів (довжини r' бітів кожний) початкового стану ЛРЗ, які відновлюються за допомогою атаки;
- нижня оцінка середньої часової складності атаки $T_{r'}(k,l^*)$;
- нижня оцінка обсягу матеріалу

$$N_{r'}(k,l^*) = k 2^{\frac{r'(l-l^*)}{\theta}} (2 l^* r' \ln 2)^{\frac{1}{\theta}} (\Delta_{r'}(k))^{-\frac{1}{\theta}},$$

- потрібного для успішної реалізації атаки.

Для того, щоб алгоритм 1 можна було використовувати на практиці, треба вміти оцінювати значення параметра (5) за числом r', елементом $c \in F_{2^{r'}} \setminus \{0\}$ та компонентами шифру (матрицею D і вузлами заміни s_i, $i \in \overline{1, p}$; див. формулу (1)). Отже, постає задача отримання аналітичних верхніх оцінок параметра (5) безпосередньо за компонентами алгоритму шифрування та параметрами кореляційної атаки.

Розв'язок цієї задачі містить наступна теорема (доведення якої виходить за межі статті).

Теорема. За умов, зазначених вище, справедлива нерівність

$$\Delta_{c,r'}(k) \le (2^{r'} - 1)\left(n_{\max}\right)^{2k\left\lceil \frac{B(D^T)}{2} \right\rceil}, \qquad (6)$$

де

$$n_{\max} = \max\{n_{a,b}(s_i) : (a,b) \in V_t \times V_t \setminus \{(0,0)\}, i \in \overline{0, p-1}\}, \qquad (7)$$

$$B(D^T) = \min\{wt(z) + wt(zD^T) : z \in F_{2^t}{}^p \setminus \{0\}\}, \qquad (8)$$

і для будь-яких $a, b \in V_t$, $i \in \overline{0, p-1}$:

$$n_{a,b}(s_i) = \max\{|A^{(i)}_{a,b}(0,0)| + |A^{(i)}_{a,b}(0,1)|, |A^{(i)}_{a,b}(1,0)| + |A^{(i)}_{a,b}(1,1)|\},$$

$$A^{(i)}_{a,b}(u,u') = 2^{-2t} \sum_{\substack{x_i, y_i \in V_t: \\ \mathrm{msb}(x_i + y_i + u) = u'}} (-1)^{(x_i^t + y_i^t + u)a \oplus x_i a \oplus s_i(y_i) b}, \; u, u' \in \{0,1\},$$

де $msb(x_i + y_i + u)$ є найстарший розряд суми цілих чисел, що відповідають зазначеним двійковим векторам довжини t, $\overset{t}{x_i} + \overset{t}{y_i} + u$ позначає суму цих чисел за модулем 2^t.

Використовуючи теорему і алгоритм 1, отримаємо оцінки ефективності кореляційних атак над полем F_{256} на шифр «Струмок» (таблиця). Відзначимо, що в цьому випадку $t = 8$, $p = 8$, $n = 16$, $B(D^T) = p + 1 = 9$, і як показує пряме обчислення, значення параметра (7) дорівнює $n_{\max} = 3 \cdot 2^{-4}$.

Таблиця

Результати виконання алгоритму 1 для шифру «Струмок» ($r' = 8$)

k	l^*	$\log_2 T_{r'}(k, l^*)$	$\log_2 N_{r'}(k, l^*)$
2	44	363,91	361,62
4	34	285,42	285,06
8	29	249,40	249,38
16	1	384,88	283,58

Висновки. Результати обчислень, наведені в таблиці свідчать про те, що будь-яка із зазначених кореляційних атак на «Струмок» має середню часову складність не менше ніж $2^{249,40}$ та потребує не менше ніж $2^{249,38}$ знаків гами. Це свідчить про практичну стійкість зазначеного шифру за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) 2^{80}.

Список використаних джерел:

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. 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.
3. Gorbenko I., Kuznetsov A., Gorbenko Yu., Alekseychuk A., Timchenko V. Strumok Keystream Generator. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies*, DESSERT'2018, 24–27 May, 2018. Kyiv, Ukraine. P. 292–299.
4. Oliynykov R. V., Gorbenko I. D., Kazymyrov O. V. [et. al]. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/ 2015/650.
5. Nyberg K., Wallen J. Improved linear distinguishers for SNOW 2.0. *Fast Software Encryption* — FSE 2006. LNCS 4047. Springer-Verlag. P. 144–162.
6. Maximov A., Johansson Th. Fast computation for large distribution and and its cryptographic application. *Advanced in Cryptology*. ASIACRYPT 2005. — LNCS 3788. Springer-Verlag. P. 313–332.

7. 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.
8. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2016/311.
9. Олексійчук А. М., Поремський М. В. Загальна схема побудови кореляційних атак на SNOW 2.0-подібні потокові шифри. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Вип. 1 (35). 2018. С. 70–79.

SECURITY JUSTIFICATION FOR STRUMOK STREAM CIPHER AGAINST CORRELATION ATTACKS OVER FINITE FIELDS OF CHARACTERISTIC 2

The stream cipher SNOW 2.0 was proposed in 2002 as an alternative to the previous (weaker) version — SNOW. This cipher is standardized today and is one of the fastest program-oriented stream ciphers.

The most powerful known attacks on SNOW 2.0 are correlation attacks, the essence of which is to form and solve systems of noised linear equations, in particular, over finite fields of order greater than 2. Despite some progress in this direction, remain unresolved problems related to the development of methods for evaluation and justification the security of SNOW 2.0-like stream ciphers against correlation attacks. To date, there are no methods that can justify the security of these ciphers against known correlation attacks directly from the parameters of their components. In addition, an attempt to apply known methods for evaluating the security of SNOW 2.0 against correlation attacks to some other stream ciphers (for example, Strumok, which is a candidate for National encryption standard of Ukraine) faces the difficulties associated with the size of tasks that have been solved. Unlike SNOW 2.0, constructed above the field of order 2^{32}, the Strumok cipher is set over a field of order 2^{64}, which leads to the impossibility of practical implementation of some known algorithms, the time complexity of which increases from $2^{32} \div 2^{37}$ to 2^{64} bit operations.

The purpose of this article is to justify the security of Strumok against a wide class of correlation attacks, including known attacks on SNOW 2.0. The main result is a theorem that establishes an analytical bound for parameter characterizing the effectiveness of correlation attacks on SNOW 2.0-like ciphers in terms of their components. This allows in practice to evaluate and justify the security of such ciphers against correlation attacks over finite fields of characteristic 2.

Key words: *stream cipher, correlation cryptanalysis, system of noised linear equations, security justification, Strumok.*

Одержано 15.01.2019