ням. Робота з кожною зоною формує власні події клавіатури (парні та непарні), які аналізуються окремо. Кінцеве рішення про допуск оператора до ресурсів системи приймається на підставі всіх даних з усіх функціональних зон клавіатури. Для парних подій клавіатури використовуються відносини часових параметрів дирафів, що дозволяє врахувати не тільки статичні особливості клавіатурного почерку, а й динамічні. Обробка поодиноких подій клавіатури, де головним обчислюваним параметром є час утримання конкретної клавіші, дозволяє доповнити профіль користувача унікальними ознаками. Такий комплексний підхід дозволяє підвищити точність процедури автентифікації без необхідності збільшення обсягу оброблюваних даних.
Ключові слова: клавіатурний почерк, біометричні алгоритми, метод дирафів, час утримання клавіші, біоеталон користувача.

Алексеев Василий Александрович, аспирант кафедры основ радиотехники харьковского Национального университета радиоэлектроники.
E-mail: vasyl.alieksieiev@nure.ua.
Алексеєв Василь Олександрович, аспірант кафедри основ радіотехніки харківського Національного університету радіоелектроніки.
Alieksieiev Vasyl, postgraduate student of Radio Engineering Fundamentals Academic Dept in Kharkiv National University of Radioelectronics.

Синица Юлия Александровна, магистр технических наук ХНУРЭ, инженер по автоматизации программных продуктов в "Marvell Semiconductor Inc.", Санта Клара, штат Калифорния, США.
E-mail: lm.julia92@gmail.com.
Синиця Юля Олександрівна, магістр технічних наук ХНУРЕ, інженер з автоматизації програмних продуктів в "Marvell Semiconductor Inc.", Санта Клара, штат Каліфорнія, США.
Synytsia Yuliia, M.Eng. KNURE, Ukraine, Software Automation Engineer in Marvell Semiconductor Inc., Santa Clara, CA, USA.

Горелов Денис Юрьевич, кандидат технических наук, доцент кафедры основ радиотехники харьковского Национального университета радиоэлектроники.
E-mail: denis.gorelov@nure.ua
Горелов Денис Юрійович, кандидат технічних наук, доцент кафедри основ радіотехніки харківського Національного університету радіоелектроніки.
Gorelov Denis, PhD in Eng, Associate Professor of Radio Engineering Fundamentals Academic Dept in Kharkiv National University of Radioelectronics.

DOI: 10.18372/2410-7840.18.11087
УДК 621.391:519.7

ДОСТАТНЯ УМОВА СТІЙКОСТІ SNOW 2.0-ПОДІБНИХ ПОТОКОВИХ ШИФРІВ ВІДНОСНО ПЕВНИХ АТАК ЗІ ЗВ'ЯЗАНИМИ КЛЮЧАМИ

Антон Олексійчук

Досліджується клас потокових шифрів, аналогічних відомому шифру SNOW 2.0. Наведено формальне означення шифрів з цього класу та встановлено взаємозв'язок між процесами гамоутворення у схемі SNOW 2.0-подібного потокового шифру і зашифровування повідомлень за допомогою схеми Івена-Мансура. Проаналізовано стійкість SNOW 2.0-подібних потокових шифрів відносно атак, що базуються на існуванні ключів, еквівалентних із затримкою. Зазначені атаки відносяться до класу атак зі зв'язаними ключами та є застосовними до широкого кола потокових шифрів, зокрема, SNOW 2.0. Головним результатом статті є достатня умова стійкості SNOW 2.0-подібних шифрів відносно зазначених атак. Ця умова є зручною для практичного застосування і дозволяє будувати афінні відображення (за допомогою яких здійснюється запис ключа та вектора ініціалізації у накопичувач генератора гами), які гарантують стійкість відповідного шифру відносно зазначених атак. Наведено два приклади таких відображень, які можуть бути використані при побудові нових SNOW 2.0-подібних шифрів.
Ключові слова: *потоковий шифр, схема Івнга-Мансура, еквівалентьність ключів із затримкою, атаки зі зв'язаними ключами, обгрунтована стійкість, SNOW 2.0.*

Вступ. Потоковий шифр SNOW 2.0 [3] запропонований у 2002 році як альтернатива попередньої (більш слабкої) версії – SNOW. На сьогодні цей шифр є стандартизованим [6] та являє собою один з найбільш швидких програмно орієнтованих потокових шифрів. Не відомо атак на повну версію шифру SNOW 2.0, спрямованих на відновлення єдиного ключа (single key recovery attacks), більш ефективних ніж повний перебір ключів. Поряд з тим, відомі ефективні атаки зі зв'язаними ключами (related key attacks), які базуються

на існуванні ключів, еквівалентних із затримкою [5]. Зауважимо, що такі атаки є застосовними також до деяких інших потокових шифрів [1, 5].

Метою даної статті є встановлення умов стійкості SNOW 2.0-подібних потокових шифрів відносно атак, наведених в [5]. В п. 1 дано формальне означення класу SNOW 2.0-подібних потокових шифрів. В п. 2 показано взаємозв'язок між процесами гамоутворення у схемі SNOW 2.0-подібного шифру та зашифровування повідомлень за допомогою схеми Івена-Мансура [4]. На думку автора, зазначений результат може бути використаний в подальшому для зведення задач криптоаналізу SNOW 2.0-подібних шифрів до відповідних задач криптоаналізу схеми Івена-Мансура, яка є добре дослідженим криптографічним об'єктом.

В п. 3 проаналізовано властивість еквівалентності ключів із затримкою у SNOW 2.0-подібних потокових шифрах. Доведено твердження, яке узагальнює окремі результати роботи [5] та встановлює, від яких параметрів залежить стійкість алгоритму шифрування відносно атак, що базуються на існуванні еквівалентних із затримкою ключів. Нарешті, в п. 4 наведено достатню умову стійкості SNOW 2.0-подібних шифрів відносно зазначених атак. Ця умова є зручною для практичного застосування і дозволяє будувати афінні відображення (за допомогою яких здійснюється запис ключа та вектора ініціалізації (ВІ) у накопичувач генератора гами), що гарантують стійкість відповідного шифру відносно зазначених атак. Наведено два приклади таких відображень, які можуть бути використані при побудові нових SNOW 2.0-подібних шифрів.

1. Означення класу SNOW 2.0-подібних потокових шифрів

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

Вхідними даними для побудови *SNOW 2.0-подібного потокового шифру з множиною ключів* V_{l_0} *та множиною векторів ініціалізації* V_{l_1} є такі об'єкти:

– примітивний над полем F_{2^m} поліном $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \ldots \oplus c_0$ степеня $n \geq 3$;

– натуральне число $\mu \in \overline{1, n-2}$;

– ін'єктивне афінне відображення $L : V_{l_0} \times V_{l_1} \to {V_m}^n$;

– підстановка $\sigma : V_m \to V_m$.

Задамо перетворення h та H на множині ${V_m}^n \times {V_m}^2$, вважаючи

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

$$H((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = ((x_n \oplus F, x_{n-1}, \ldots, x_1), u', v')), \quad (2)$$

де

$$x_n = c_{n-1}x_{n-1} \oplus \ldots \oplus c_0 x_0, \quad (3)$$

$$F = (x_{n-1} + u) \oplus v, \quad (4)$$

$$u' = x_\mu + v, \; v' = \sigma(u). \quad (5)$$

Зауважимо, що внаслідок нерівності $c_0 \neq 0$ (яка випливає з умови примітивності полінома $g(z)$) перетворення (1) і (2) є підстановками на множині ${V_m}^n \times {V_m}^2$.

За означенням SNOW 2.0-подібний потоковий шифр є шифром імпульсного гамування, який складається з генератора гами (ГГ) та алгоритму формування початкового стану ГГ за ключем і вектором ініціалізації.

Генератор гами (рис. 1) являє собою скінченний автономний автомат $\Im$ з множиною внутрішніх станів ${V_m}^n \times {V_m}^2$, функцією переходів (1) та функцією виходів

$$f((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = x_0 \oplus F = x_0 \oplus (x_{n-1} + u) \oplus v. \quad (6)$$

Алгоритм формування початкового стану генератора залежить від натурального параметра t і складається з двох етапів:

1) формування за ключем $k \in V_{l_0}$ і ВІ $c \in V_{l_1}$ стану $\iota_0 = (L(k, c), 0, 0)$ автомата $\Im$;

2) обчислення початкового стану ГГ за формулою

$$s_0 = h(H^t(\iota_0)), \quad (7)$$

де H^t позначає t-й степінь відображення H відносно операції композиції.

Отже, на першому етапі за допомогою відображення L обчислюється вектор $L(k,c)$ довжини n над множиною V_m, який записується у накопичувач (рис. 1). Зазначений вектор, поряд з нульовими значеннями змінних u і v, утворює стан ι_0 автомата $\Im$. На другому етапі, згідно з формулою (7), обчислюється початковий стан $s_0 = ((x_{n-1}, x_{n-2}, \dots, x_0), u_0, v_0)$. Далі автомат функціонує за законом $s_{i+1} = h(s_i)$, $\gamma_i = f(s_i)$, $i = 0, 1, \dots$, проходячи послідовність станів $s_i = ((x_{i+n-1}, x_{i+n-2}, \dots, x_i), u_i, v_i)$ та формуючи вихідну послідовність (шифрувальну гаму) γ_i, $i = 0, 1, \dots$. Таким чином, стан генератора в i-му такті визначається за формулою

$$s_i = h^{i+1}(H^t(\iota_0)), i = 0, 1, \dots, \quad (8)$$

а знак вихідної послідовності – за формулою

$$\gamma_i = x_i \oplus (x_{i+n-1} + u_i) \oplus v_i, \; i = 0, 1, \dots . \quad (9)$$

Зауважимо, що змінними параметрами, від яких залежить визначений потоковий шифр, є примітивний над полем F_{2^m} поліном $g(z)$, точка з'єму $\mu \in \overline{1, n-2}$, ін'єктивне афінне відображення L та підстановка σ.

У шифрі SNOW 2.0 [3] використовуються такі параметри: $m = 32$, $n = 16$, $\mu = 5$, $g(z) = z^n \oplus c_{n-1} z^{n-1} \oplus \dots \oplus c_0$, де α є певним примітивним елементом поля $F_{2^{32}}$. При цьому довжина ВІ дорівнює $l_1 = 128$, а довжина ключа може приймати одне з двох значень: $l_0 = 128$ або $l_0 = 256$. Підстановка σ задається аналогічно раундовому перетворенню блокового шифру Rijndael, а відображення L визначається таким чином:

1) якщо $l_0 = 128$, то

$$L(k_3, k_2, k_1, k_0, c_3, c_2, c_1, c_0) = (k_3^{c_0}, k_2, k_1, k_0^{c_1}, \overline{k_3}, \overline{k_2}^{c_2}, \overline{k_1}^{c_3}, \overline{k_0}, k_3, k_2, k_1, k_0, \overline{k_3}, \overline{k_2}, \overline{k_1}, \overline{k_0}),$$

де $k_i, c_i \in V_{32}$, $k^c \stackrel{\text{def}}{=} k \oplus c$, а $\overline{k}$ позначає вектор, який отримується шляхом інвертування усіх координат двійкового вектора k;

2) якщо $l_0 = 256$, то

$$L(k_7, k_6, \dots, k_0, c_3, c_2, c_1, c_0) = (k_7^{c_0}, k_6, k_5, k_4^{c_1}, k_3, k_2^{c_2}, k_1^{c_3}, k_0, \overline{k_7}, \overline{k_6}, \dots, \overline{k_0}),$$

де $k_i, c_i \in V_{32}$, а символи k^c, $\overline{k}$ мають той самий сенс, що і вище.

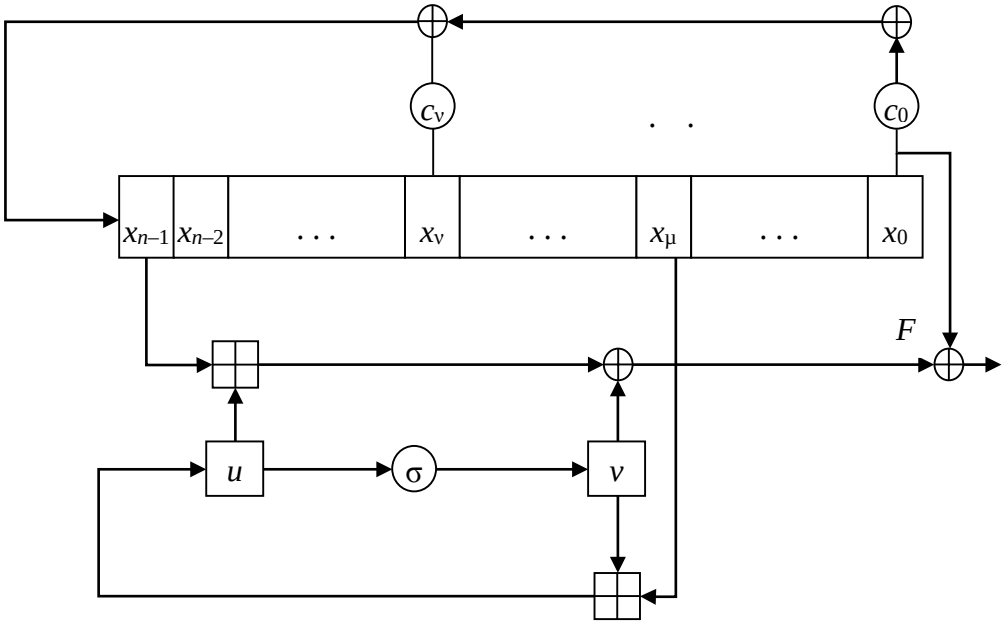

Рис. 1. Схема генератора гами SNOW 2.0-подібного шифру

2. Інтерпретація процесу гамоутворення в термінах схеми Івена-Мансура

Розглянемо означений вище потоковий шифр, побудований за вхідними даними $g(z) = z^n \oplus c_{n-1} z^{n-1} \oplus \dots \oplus c_0$, μ, L, σ. Для будь-яких $x, k \in V_m$ покладемо $\sigma_k(x) = \sigma(x + k)$.

Твердження 1. Система рівнянь гамоутворення шифру, що розглядається, має вигляд

$$(u_0 + x_{n-1}) \oplus v_0 \oplus x_0 = \gamma_0,$$
$$(v_{i-1} + x_{i+\mu-1} + x_{i+n-1}) \oplus v_i \oplus x_i = \gamma_i,$$
$$i = 1, 2, \dots, \quad (10)$$

де $s_0 = ((x_{n-1}, x_{n-2}, \dots, x_0), u_0, v_0)$ є початковим станом ГГ, x_i є i-м знаком лінійної рекурентної

послідовності з початковим вектором $(x_0, x_1, \dots, x_{n-1})$ та характеристичним поліномом $g(z)$,

$$v_{2i} = \sigma_{x'(i-1)}\sigma_{x'(i-2)} \dots \sigma_{x'(0)}(v_0),\ i = 1, 2, \dots$$
$$v_{2i+1} = \sigma_{x''(i-1)}\sigma_{x''(i-2)} \dots \sigma_{x''(0)}(\sigma(u_0)),$$
$$i = 0, 1, \dots, \qquad (11)$$

де $x'(i) = x_{2i+\mu}$, $x''(i) = x_{2i+1+\mu}$, $i = 0, 1, \dots$. При цьому кожна з послідовностей $x'(0), x'(1), \dots$, $x''(0), x''(1), \dots$ є лінійною рекурентою над полем F_{2^m} з примітивним характеристичним поліномом $g^{(2)}(z) = z^n \oplus c_{n-1}^2 z^{n-1} \oplus \dots \oplus c_0^2$.

Доведення. Позначимо $s_i = ((x_{i+n-1}, x_{i+n-2}, \dots, x_i), u_i, v_i)$ стан ГГ в i-му такті, $i = 1, 2, \dots$. З рівностей (5) випливає, що $u_i = v_{i-1} + x_{i+\mu-1}$, $v_{i+2} = \sigma(u_{i+1}) = \sigma(v_i + x_{i+\mu})$. Підставляючи першу з цих рівностей у формулу (9), отримаємо формулу (10). Крім того, згідно з другою рівністю,

$$v_{2(i+1)} = \sigma(v_{2i} + x_{2i+\mu}) = \sigma_{x'(i)}(v_{2i}),$$
$$v_{2(i+1)+1} = \sigma(v_{2i+1} + x_{2i+1+\mu}) = \sigma_{x''(i)}(v_{2i+1}),$$

звідки за допомогою індукції по i отримуються співвідношення (11).

Покажемо, що характеристичний поліном лінійної рекуренти $x'(0), x'(1), \dots$ дорівнює $g^{(2)}(z)$ (для рекуренти $x''(0), x''(1), \dots$ доведення проводиться аналогічно).

Позначимо

$$S = \begin{pmatrix} 0\,0 \dots 0\,c_0 \\ 1\,0 \dots 0\ c_1 \\ 0\,1 \dots 0\,c_2 \\ \dots\ \dots\ \dots \\ 0\,0 \dots 1\,c_{n-1} \end{pmatrix}$$

супровідну матрицю полінома $g(z)$. Ця матриця задовольняє рівності $S^n = c_{n-1}S^{n-1} \oplus c_{n-2}S^{n-2} \oplus \oplus \dots \oplus c_0 I$, де I – одинична матриця порядку n над полем F_{2^m}. Підносячи зазначену рівність до квадрату, отримаємо, що $S^{2n} = c_{n-1}^2 S^{2(n-1)} \oplus \oplus c_{n-2}^2 S^{2(n-2)} \oplus \dots \oplus c_0^2 I$. Звідси, використовуючи відому формулу $x_i = \vec{x}_0 S^i e^{\downarrow}$, $i = 0, 1, \dots$, де $\vec{x}_0 = (x_0, x_1, \dots, x_{n-1})$, $e^{\downarrow} = (1, 0, \dots, 0)^T$, отримаємо такі співвідношення:

$$x'(i+n) = x_{2(i+n)} = \vec{x}_0 S^{2i} S^{2n} e^{\downarrow} = \vec{x}_0 S^{2i}(c_{n-1}^2 S^{2(n-1)} \oplus c_{n-2}^2 S^{2(n-2)} \oplus \dots \oplus c_0^2 I)e^{\downarrow} =$$
$$= c_{n-1}^2\, \vec{x}_0 S^{2i} S^{2(n-1)} e^{\downarrow} \oplus c_{n-2}^2\, \vec{x}_0 S^{2i} S^{2(n-2)} e^{\downarrow} \oplus \dots \oplus c_0^2\, \vec{x}_0 S^{2i} e^{\downarrow} =$$
$$= c_{n-1}^2 x'(i+n-1) \oplus c_{n-2}^2 x'(i+n-2) \oplus \dots \oplus c_0^2 x'(i),\ i = 0, 1, \dots.$$

Отже, $x'(0), x'(1), \dots$ є лінійною рекурентою з характеритистичним поліномом $g^{(2)}(z)$.

Нарешті, згідно з формулами Вієта, коренями полінома $g^{(2)}(z)$ є квадрати коренів полінома $g(z)$ і, оскільки останній є примітивним над полем F_{2^m}, то $g^{(2)}(z)$ також є примітивним над цим полем.

Твердження доведено.

Співвідношення (10), (11) дозволяють наступним чином описати процес формування гами SNOW 2.0-подібного потокового шифру. За початковим станом генератора $s_0 = ((x_{n-1}, x_{n-2}, \dots, x_0), u_0, v_0)$ обчислюються знаки лінійної рекуренти x_i, $i = 0, 1, \dots$, з якої отримуються дві "вибірки", утворені знаками $x'(i) = x_{2i+\mu}$ та $x''(i) = x_{2i+1+\mu}$ (з парними та непарними номерами, з точністю до зсуву на μ) відповідно, $i = 0, 1, \dots$. Далі початкові значення v_0 та $v_1 = \sigma(u_0)$ "зашифровуються" як у схемі Івена-Мансура [4] на «раундових ключах» $x'(i)$ та $x''(i)$ відповідно, в результаті чого отримуються значення (11), за якими, нарешті, обчислюються знаки гами (10).

Зауважимо, що схема Івена-Мансура є добре дослідженим криптографічним об'єктом (див, наприклад, [2]). На думку автора, отримане твердження може бути використано для зведення задач криптоаналізу SNOW 2.0-подібних шифрів до відповідних задач криптоаналізу схеми типу Івена-Мансура, проте конкретні результати в цьому напрямі є предметом подальших досліджень.

3. Еквівалентність ключів із затримкою у SNOW 2.0-подібних потокових шифрах

Розглянемо означений вище потоковий шифр з множиною ключів V_{l_0} та множиною векторів ініціалізації V_{l_1}. Для будь-яких $k, k' \in V_{l_0}$, $c, c' \in V_{l_1}$, $r \in \overline{1,t}$ позначимо $\iota_0 = (L(k,c), 0, 0)$, $\iota_0' = (L(k',c'), 0, 0)$, $\iota_r = H^r(\iota_0)$, $\iota_r' = H^r(\iota_0')$, де підстановка H визначається за формулою (2).

Назвемо *пари* (k,c) та (k',c') *еквівалентними із затримкою* r (r-bits-phase shifting equivalent) [1, 5], якщо виконується рівність $\iota_r = \iota'_0$. *Ключі* k і k' назвемо *еквівалентними із затримкою* r, якщо існують ВІ $c,c' \in V_{l_1}$ такі, що пари (k,c) та (k',c') є еквівалентними із затримкою r.

Поняття еквівалентності із затримкою r має сенс для широкого класу потокових шифрів та означає, що стан генератора гами шифру в r-му такті, сформований за парою (k,c) при виконанні процедури ініціалізації, співпадає з початковим станом цього генератора, сформованим за іншою парою (k',c'). Наявність достатньо великої кількості ключів, еквівалентних із затримкою, дозволяє будувати на шифр атаки зі зв'язаними ключами (див. роботи [1, 5] та наведені в них посилання).

В [5] отримано опис пар (k,c), еквівалентних із затримкою $r \in \{2, 3, 4\}$, для шифру SNOW 2.0. Як приклад, сформулюємо такий результат.

Твердження 2 [5]. Нехай $k = (A_7, k_6, k_5, k_4, k_3, k_2, k_1, A_0)$, де $k_i \in V_{32}$, $i \in \overline{1,6}$, $A_7 = \sigma^{-1}(0) - \sigma(\overline{k_5})$, $A_0 = -(\sigma(\overline{k_6}) + \sigma(0))$ (нагадаємо, що символом $\overline{x}$ позначається вектор, отриманий шляхом інвертування усіх координат довільного двійкового вектора x). Тоді існує єдиний набір $(c_3, c_2, c'_1, c'_0) \in V_{32}{}^4$ такий, що для ключа $k' = (\overline{k_3}, \overline{k_2} \oplus c_2, \overline{k_1} \oplus c_3, \overline{A_0}, A_7, k_6, k_5, k_4)$ та ВІ $c = (c_3, c_2, 0, 0)$, $c' = (0, 0, c'_1, c'_0)$ шифру SNOW 2.0 з довжиною ключа $l_0 = 256$ пари (k,c) та (k',c') є еквівалентними із затримкою 4. При цьому знаки гами γ_4 та γ_9, що виробляються генератором за парою (k,c) у четвертому та дев'ятому тактах відповідно, співпадають зі знаками γ'_0 та γ'_5, які виробляються за парою (k',c') відповідно в нульовому та п'ятому тактах.

Отже, згідно з твердженням 2 для шифру SNOW 2.0 з довжиною ключа 256 біт існує 2^{192} пар ключів, еквівалентних із затримкою 4. При цьому рівності $\gamma'_0 = \gamma_4$, $\gamma'_5 = \gamma_9$, які виконуються для зазначених ключів та векторів ініціалізації, дозволяють побудувати на шифр атаку зі зв'язаними ключами, складність якої є величиною порядку 2^{67} [5].

Дослідимо докладніше властивість еквівалентності із затримкою у довільних SNOW 2.0-подібних потокових шифрах.

Розглянемо зазначений шифр, побудований за вхідними даними $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \ldots \oplus c_0$, μ, L, σ (див. п. 1). Як і вище, позначимо

$$\iota_0 = (L(k,c), 0, 0),\ \iota'_0 = (L(k',c'), 0, 0),$$
$$s_i = h^{i+1}(H^t(\iota_0)),\ s'_i = h^{i+1}(H^t(\iota'_0)),\ \gamma_i = f(s_i),\ \gamma'_i = f(s'_i),\ i = 0, 1, \ldots. \quad (12)$$

Доведемо таке твердження.

Твердження 3. Нехай $\nu = \max\{j \in \overline{0,n-1}: c_j \neq 0\}$, $1 \le r \le n-1-\max\{\mu,\nu\}$, $k,k' \in V_{l_0}$, $c,c' \in V_{l_1}$ і пари (k,c), (k',c') є еквівалентними із затримкою r. Тоді для будь-якого $i \in \overline{0,n-1-\max\{\mu,\nu\}-r}$ виконується рівність $\gamma'_i = \gamma_{i+r}$.

Доведення. З рівності $H^r(\iota_0) = \iota'_0$ випливає, що $s \overset{\text{def}}{=} H^t(\iota_0) = H^{t-r}(\iota'_0)$. При цьому згідно з формулою (12) маємо $s'_i = h^{i+1}(H^r(s))$, $s_{i+r} = h^{i+1}(h^r(s))$, $\gamma'_i = f(s'_i)$, $\gamma_{i+r} = f(s_{i+r})$, $i = 0, 1, \ldots$

Помітимо, що на підставі формул (1), (2) і (5) останні дві координати (u' та v') кожного з векторів $h(s)$, $H(s)$ залежать тільки від u, v-координат вектора s, а також від його координати x_μ. Тому вектори $h^r(s)$ і $H^r(s)$ відрізняються, мабуть, лише першими r координатами, тобто мають такий вигляд:

$$h^r(s) = (y_1, \ldots, y_r,\ x_{n-1}, \ldots, x_r,\ u', v'),$$
$$H^r(s) = (z_1, \ldots, z_r,\ x_{n-1}, \ldots, x_r,\ u', v'),$$

де $y_j, z_j, x_i, u', v' \in V_m$, $j \in \overline{1,r}$, $i \in \overline{r,n-1}$.

Далі, на підставі формули (1) та означення числа ν для кожного $i \in \overline{0,n-1-\max\{\mu,\nu\}-r}$ справедливі рівності

$$s_{i+r} = h^{i+1}(h^r(s)) = (w_1, \ldots, w_{i+1},\ y_1, \ldots, y_r,\ x_{n-1}, \ldots, x_{i+r},\ u'', v''),$$
$$s'_i = h^{i+1}(H^r(s)) = (w_1, \ldots, w_{i+1},\ z_1, \ldots, z_r,\ x_{n-1}, \ldots, x_{i+r},\ u'', v''),$$

де $w_1,...,w_{i+1}, u'', v'' \in V_m$. Звідки в силу формули (9) випливає, що $\gamma'_i = f(s'_i) = f(s_{i+r}) = \gamma_{i+r}$. Твердження доведено.

Зауважимо, що довжина відрізків гами, які збігаються за умови твердження 3, зменшується зі збільшенням параметра $\max\{\mu, \nu\}$. При $r > n-1-\max\{\mu, \nu\}$ тотожний збіг відрізків гами стає неможливим внаслідок відмінностей між перетвореннями (1) і (2).

Застосовуючи твердження 3 до шифру SNOW 2.0 ($n=16$, $\mu=5$, $\nu=11$) отримаємо такий результат.

Наслідок 1. Для шифру SNOW 2.0 еквівалентність пар (k,c) та (k',c') із затримкою $r \le 4$ тягне рівності $\gamma'_i = \gamma_{i+r}$, $i \in \overline{0,4-r}$.

4. Достатня умова стійкості SNOW 2.0-подібних шифрів відносно атак, що базуються на еквівалентних із затримкою ключах

Розглянемо довільний SNOW 2.0-подібний потоковий шифр, побудований за вхідними даними $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus ... \oplus c_0$, μ, L і σ. Позначимо $\mathrm{Im}\, L$ образ афінного відображення L. Назвемо H-*послідовністю* будь-яку послідовність $x_0, x_1, ...$ елементів множини V_m, що задовольняє рекурентному співвідношенню

$$x_{i+n} = c_{n-1}x_{i+n-1} \oplus ... \oplus c_0 x_i \oplus (x_{i+n-1} + u_i) \oplus v_i,\ i = 0, 1, ..., \tag{13}$$

де

$$u_0 = v_0 = 0,\ u_{i+1} = x_{i+\mu} + v_i,\ v_{i+1} = \sigma(u_i),\ i = 0, 1, ... \tag{14}$$

Нагадаємо, що підстановка σ_k визначається за формулою $\sigma_k(x) = \sigma(x+k)$, $x, k \in V_m$.

Доведемо твердження, яке встановлює критерій існування еквівалентних із затримкою ключів у SNOW 2.0-подібних потокових шифрах.

Твердження 4. Нехай $r \in \overline{1,t}$. Тоді еквівалентні із затримкою r ключі SNOW 2.0-подібного шифру існують в тому і тільки тому випадку, коли існує H-послідовність $x_0, x_1, ...$ така, що

$$(x_{n-1}, ..., x_0) \in \mathrm{Im}\, L,\ (x_{n+r-1}, ..., x_r) \in \mathrm{Im}\, L \tag{15}$$

та

$$\sigma_{x_{2(r'-1)+\mu}}\sigma_{x_{2(r'-2)+\mu}} ... \sigma_{x_\mu}(0) = 0,\ \sigma_{x_{2(r'-1)+\mu+1}}\sigma_{x_{2(r'-2)+\mu+1}} ... \sigma_{x_{\mu+1}}(\sigma(0)) = \sigma(0),$$

якщо $r = 2r'$;

$$\sigma_{x_{2(r'-1)+\mu+1}}\sigma_{x_{2(r'-2)+\mu+1}} ... \sigma_{x_{\mu+1}}(\sigma(0)) = 0,\ \sigma_{x_{2r'+\mu}}\sigma_{x_{2(r'-1)+\mu}} ... \sigma_{x_\mu}(0) = \sigma(0),$$

якщо $r = 2r'+1$.

Доведення. Помітимо, що співвідношення (13), (14) рівносильні рівностям

$$((x_{i+n-1}, x_{i+n-2}, ..., x_i), u_i, v_i) = H^i(((x_{n-1}, x_{n-2}, ..., x_0), 0, 0)),\ i = 0, 1, ...,$$

де відображення H визначається за формулою (2). Отже, необхідною і достатньою умовою існування елементів $k, k' \in V_{l_0}$, $c, c' \in V_{l_1}$ таких, що $(L(k',c'), 0, 0) = H^r(L(k,c), 0, 0)$, є існування H-послідовності $x_0, x_1, ...$, яка задовольняє співвідношенням

$$(x_{n-1}, ..., x_0) \in \mathrm{Im}\, L,\ (x_{n+r-1}, ..., x_r) \in \mathrm{Im}\, L,\ u_r = v_r = 0.$$

Для завершення доведення достатньо скористатися формулами

$$v_{2r'} = \sigma_{x_{2(r'-1)+\mu}}\sigma_{x_{2(r'-2)+\mu}} ... \sigma_{x_\mu}(0),\ u_{2r'} = \sigma^{-1}(\sigma_{x_{2(r'-1)+\mu+1}}\sigma_{x_{2(r'-2)+\mu+1}} ... \sigma_{x_{\mu+1}}(\sigma(0))),$$

$$v_{2r'+1} = \sigma_{x_{2(r'-1)+\mu+1}}\sigma_{x_{2(r'-2)+\mu+1}} ... \sigma_{x_{\mu+1}}(\sigma(0)),\ u_{2r'+1} = \sigma^{-1}(\sigma_{x_{2r'+\mu}}\sigma_{x_{2(r'-1)+\mu}} ... \sigma_{x_\mu}(0)),$$

які випливають з рівностей (14).

Твердження доведено.

Зауважимо, що для малих r зазначена у формулюванні твердження 4 умова має достатньо простий вигляд.

Наслідок 2. Для існування еквівалентних із затримкою 2 (відповідно, із затримкою 3) ключів SNOW 2.0-подібного шифру необхідно і достатньо, щоби існувала H-послідовність $x_0, x_1, ...$, яка задовольняє умові (15) та рівностям $x_\mu = \sigma^{-1}(0)$, $x_{\mu+1} = -\sigma(0)$ (відповідно, умові (15) та рівностям $x_{\mu+1} = \sigma^{-1}(0) - \sigma(0)$, $x_{\mu+2} = -\sigma(x_\mu)$).

Сформулюємо зараз достатню умову відсутності ключів, еквівалентних із затримкою r, яка є зручною для практичного застосування.

Для будь-яких $i, j \in \overline{0, n-1-r}$ назвемо пару (i, j) r-*забороненою*, якщо для будь-якого вектора $(x_0, x_1, \dots, x_{n-1}) \in \operatorname{Im} L$ виконується така умова:

$$(x_i = x_j \ \textit{та}\ x_{i+r} \neq x_{j+r}) \ \textit{або}\ (x_i \neq x_j \ \textit{та}\ x_{i+r} = x_{j+r}).$$

Безпосередньо з твердження 4 і даного означення випливає наступний результат.

Твердження 5. Нехай $r \in \overline{1, n-2}$ і для відображення L існує, принаймні, одна r-заборонена пара. Тоді відповідний SNOW 2.0-подібний шифр не має еквівалентних із затримкою r ключів.

Неважко побудувати афінні відображення, які задовольняють умові останнього твердження при малих r.

Приклад 1. Нехай $l_0 = l_1 = 4m$ і

$$L(k_3, k_2, k_1, k_0, c_3, c_2, c_1, c_0) =$$
$$= (\underset{0}{k_3^{c_0}}, \underset{1}{k_2}, \underset{2}{k_1^{c_1}}, \underset{3}{k_0^{c_2}}, \underset{4}{k_3}, \underset{5}{k_2^{c_3}}, \underset{6}{\overline{k_1}}, \underset{7}{\overline{k_0}}, \underset{8}{k_3}, \underset{9}{k_2}, \underset{10}{\overline{k_1}}, \underset{11}{k_0}, \underset{12}{k_3}, \underset{13}{\overline{k_2}}, \underset{14}{k_1}, \underset{15}{\overline{k_0}}),$$

де $k_i, c_i \in V_m$, $k^c \overset{\text{def}}{=} k \oplus c$, а $\overline{k}$ позначає вектор, який отримується шляхом інвертування усіх координат двійкового вектора k. Тоді пари $(6, 14)$, $(8, 12)$, $(4, 8)$ та $(6, 10)$ є r-забороненими при $r = 1, 2, 3, 4$ відповідно. Отже, будь-який SNOW 2.0-подібний шифр, в якому використовується зазначене відображення L, не має еквівалентних із затримкою r ключів при $r \in \{1, 2, 3, 4\}$.

Приклад 2. Нехай $l_0 = 8m$, $l_1 = 4m$ і

$$L(k_7, k_6, k_5, k_4, k_3, k_2, k_1, k_0, c_3, c_2, c_1, c_0) =$$
$$= (\underset{0}{k_7^{c_0}}, \underset{1}{k_6}, \underset{2}{k_5}, \underset{3}{k_4^{c_1}}, \underset{4}{k_3}, \underset{5}{k_2^{c_2}}, \underset{6}{k_1}, \underset{7}{\overline{k_0}}, \underset{8}{k_4^{c_3}}, \underset{9}{\overline{k_6}}, \underset{10}{k_5}, \underset{11}{\overline{k_7}}, \underset{12}{k_3}, \underset{13}{k_2}, \underset{14}{\overline{k_1}}, \underset{15}{k_0}),$$

де $k_i, c_i \in V_m$, а символи k^c, $\overline{k}$ мають той самий сенс, що і вище. Тоді пара $(1, 9)$ є 1-забороненою, пара $(4, 12)$ є 2-забороненою і 3-забороненою, а пара $(2, 10)$ є 4-забороненою. Отже, будь-який SNOW 2.0-подібний шифр, в якому використовується зазначене відображення L, не має еквівалентних із затримкою r ключів при $r \in \{1, 2, 3, 4\}$.

Таким чином, застосування у шифрі SNOW 2.0 відображень, зазначених у прикладах 1 і 2 (при $m = 32$), замість оригінальних відображень гарантує стійкість шифру відносно атак зі зв'язаними ключами, наведених в [5]. Аналогічний висновок є вірним для будь-якого SNOW 2.0-подібного потокового шифру з довжиною накопичувача $n = 16$ (m-розрядних двійкових слів) за умови, що параметр $\max\{\mu, \nu\}$, визначений у формулюванні твердження 3, є не менше 11.

Висновки

Стійкість будь-якого SNOW 2.0-подібного шифру відносно атак, що базуються на існуванні еквівалентних із затримкою r ключів [5], залежить від властивостей афінного відображення L та від параметра $n-1-\max\{\mu, \nu\}$ (див. твердження 3). При $r > n-1-\max\{\mu, \nu\}$ тотожний збіг відрізків гами, отриманих при еквівалентних із затримкою r ключах та векторах ініціалізації, порушується, що виключає можливість проведення на шифр атак, аналогічних описаним в [5].

При $1 \le r \le n-1-\max\{\mu, \nu\}$ відсутність еквівалентних із затримкою r ключів можна забезпечити шляхом вибору відображення L, для якого існують r-заборонені пари (див. твердження 5). Зокрема, при $n = 16$, $\max\{\mu, \nu\} \ge 11$ застосування відображень, зазначених у прикладах 1 і 2, гарантує стійкість відповідного SNOW 2.0-подібного шифру відносно атак, наведених в [5].

ЛІТЕРАТУРА

[1] Berbain C. Understanding phase shifting equivalent keys and exhaustive search /C. Berbain, A. Gouget, H. Sibert // http://eprint.iacr.org/2008/169.

[2] Dunkelman O. Minimalism in cryptography: the Even-Mansour scheme revisited / O. Dunkelman, N. Keller, A. Shamir //http://eprint.iacr.org/2011/541.

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

[4] Even Sh. A construction of a cipher from a single pseudorandom permutation / Sh. Even, Y. Mansour // J. of Cryptology. – 1997. – Vol. 10. – № 3. – pp. 159 – 162.

[5] Kircanski A. On the sliding property of SNOW 3G and SNOW 2.0 / A. Kircansk, A. Youssef // IET Information Security. – 2011. – Vol. 5. – № 4. – pp. 199 – 206.
[6] ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Part 4: Stream ciphers, 2011. – 92 p.

REFERENCES

[1] Berbain C., Gouget A., Sibert H. (2008), "Understanding phase shifting equivalent keys and exhaustive search" , http://eprint.iacr.org/2008/169.
[2] Dunkelman O., Keller N., Shamir A. (2011), "Minimalism in cryptography: the Even-Mansour scheme revisited", http://eprint.iacr.org/2011/541.
[3] Ekdahl P., Johansson T. (2002), "A new version of the stream cipher SNOW". Selected Areas in Cryptography – SAC 2002, LNCS 2295, Springer-Verlag, pp. 47 – 61.
[4] Even Sh., Mansour Y. (1997), "A construction of a cipher from a single pseudorandom permutation", J. of Cryptology, Vol. 10, № 3, pp. 159 – 162.
[5] Kircanski A., Youssef A. (2011), "On the sliding property of SNOW 3G and SNOW 2.0", IET Information Security, Vol. 5, № 4, pp. 199 - 206.
[6] ISO/IEC 18033-4: 2011(E). Information technology – Security techniques – Encryption algorithm – Part 4: Stream ciphers, 2011, 92 p.

ДОСТАТОЧНОЕ УСЛОВИЕ СТОЙКОСТИ SNOW 2.0-ПОДОБНЫХ ПОТОЧНЫХ ШИФРОВ ОТНОСИТЕЛЬНО НЕКОТОРЫХ АТАК СО СВЯЗАННЫМИ КЛЮЧАМИ

Исследуется класс поточных шифров, аналогичных известному шифру SNOW 2.0. Дано формальное определение шифров из этого класса и установлена взаимосвязь между процессами гаммообразованния в схеме SNOW 2.0-подобного поточного шифра и зашифрования сообщений с помощью схемы Івена-Мансура. Проанализирована стойкость SNOW 2.0-подобных поточных шифров относительно атак, основанных на существовании ключей, эквивалентных с задержкой. Указанные атаки относятся к классу атак со связанными ключами и применимы к широкому кругу поточных шифров, в частности, SNOW 2.0. Основным результатом статьи является достаточное условие стойкости SNOW 2.0-подобных шифров относительно указанных атак. Это условие удобно для практического применения и позволяет строить аффинные отображения (с помощью которых осуществляется запись ключа и вектора инициализации в накопитель генератора гаммы), гарантирующие стойкость соответствующего шифра относительно указанных атак. Приведено два примера таких отображений, которые могут быть использованы при построении новых SNOW 2.0-подобних шифров.

Ключові слова: поточный шифр, схема Івена-Мансура, эквивалентность ключей с задержкой, атаки со связанными ключами, обоснованная стойкость, SNOW 2.0.

SUFFICIENT CONDITION FOR SNOW-2.0-LIKE STREAM CIPHERS' TO BE SECURE AGAINST SOME RELATED KEY ATTACKS

A class of stream ciphers similar to the well-known SNOW 2.0 cipher is investigated. The formal description of the ciphers from this class is given and the relation between keysream-generation process of a SNOW 2.0-like cipher and the message encryption with Even-Mansour scheme is determined. The security of SNOW-2.0-like stream ciphers against attacks based on the existence of shifting equivalent keys is analyzed. These attacks are related key attacks and can be applied to many stream ciphers, particularly, to SNOW 2.0. The main result of this paper is a sufficient condition for SNOW 2.0-like ciphers to be secure againt mentioned attacks. This condition is convenient for practical appliances and allows constructing the affine mappings (that proceed keys and initialization vectors inserting into the keystream generator) guarantee the security of corresponding ciphers against mentioned attacks. The two examples of such mappings that can be used for constructing of new SNOW 2.0-like ciphers are proposed.

Index Terms: stream cipher, Even-Mansour scheme, shifting equivalet keys, related key attacks, provable security, SNOW 2.0.

Олексійчук Антон Миколайович, доктор технічних наук, доцент, завідуючий кафедри Кібербезпеки 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, заведующий кафедры Кибербезопасности Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского»
Alekseychuk Anton, Doctor of Technical Sciences, Assistant professor, Head of Cybersecurity Department of The Institute of Special Communication and Information Protection of National technical university of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute».