— для режима гаммирования безопасным является шифрование данных размером 2^{31} блоков, т. е. 16 Гбайт;
— для режима гаммирования с обратной связью безопасным является шифрование данных размером $\sqrt{2^{64}/3}$ блоков, т. е. $\approx 18{,}475$ Гбайт.

Таблица 2

Практические характеристики криптостойкости отечественных режимов шифрования

Название режима шифрования	Практическое значение $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$	Значение σ, обеспечивающее криптостойкость
Простой замены	1	1
Гаммирования	$\leqslant 4\sigma^2/2^{64}$	$\leqslant 2^{31}$
Гаммирования с обратной связью	$\leqslant 3\sigma^2/2^{64}$	$\leqslant \sqrt{2^{64}/3}$

ЛИТЕРАТУРА

1. *Bellare M. and Rogaway P.* Introduction to Modern Cryptography. 2005. `http://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf`
2. *Goldwasser S. and Bellare M.* Lecture Notes on Cryptography. 2001. `http://cseweb.ucsd.edu/~mihir/papers/gb.pdf`
3. *Katz J. and Yehuda L.* Introduction to Modern Cryptography. Boca Raton: Chapman& Hall/CRC, 2008.

УДК 519.7

О ВЫБОРЕ СЛАЙДОВЫХ ПАР В КОРРЕЛЯЦИОННОМ МЕТОДЕ КРИПТОАНАЛИЗА ШИФРА KeeLoq

О. Н. Лебедева

KeeLoq — блочный шифр, широко используемый в системах бесключевого удалённого доступа. Шифр был разработан профессором Г. Каном и запатентован Южно-Африканской компанией «Nanoteq» в середине 80-х. В 1995 г. фирма «MICROCHIP» приобрела KeeLoq у фирмы «Nanoteq» вместе с лицензионными правами.

Алгоритм KeeLoq [1] имеет 64-битный ключ и осуществляет шифрование 32-битных блоков открытого текста. В нём используются два регистра сдвига: один — длины 64 без функции обратной связи (для выработки подключа), другой — регистр сдвига длины 32 с нелинейной функцией обратной связи NLF от пяти переменных (непосредственно для шифрования). Блок открытого текста помещается в текстовый регистр. Шифртекстом является состояние регистра после 528 циклов с использованием регистра ключа. Пусть $V_n = \mathrm{GF}_2^n$ — множество всех n-битных слов; $Y^{(i)} = (y_{31}^{(i)}, \ldots, y_0^{(i)}) \in \in V_{32}$ и $K^{(i)} = (k_{63}^{(i)}, \ldots, y_0^{(i)}) \in V_{63}$ — соответственно состояния текстового регистра и регистра ключа после i тактов. Каждый цикл шифрования может быть описан следующим образом:

— вычисление очередного бита: $\varphi = NLF(y_{31}^{(i)}, y_{26}^{(i)}, y_{20}^{(i)}, y_9^{(i)}, y_1^{(i)}) \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus k_0^{(i)}$;
— сдвиг состояния текстового регистра: $R^{(i+1)} = (\varphi, y_{31}^{(i)}, \ldots, y_1^{(i)})$;
— сдвиг состояния регистра ключа: $K^{(i+1)} = (k_0^{(i)}, k_{63}^{(i)}, \ldots, k_1^{(i)})$.

Первый криптоанализ KeeLoq был опубликован только в феврале 2007 г. А. Богдановым [1]. Эта атака основана на слайдовой технике и линейном приближении нелинейной булевой функции, использующейся в KeeLoq. Криптоанализ имеет временную

сложность 2^{52} и требует 16 Гбайт памяти. Позднее Богданов обновил свой метод, используя алгебраический криптоанализ для нахождения первых 16 битов ключа [2]. Улучшение привело к уменьшению временной сложности до $2^{50,6}$.

В работе [1] Богданов описывает следующие шаги. Для каждого подключа $K' = (k_{15}, \ldots, k_0)$ и случайного 32-битного входа $I_0 \in V_{32}$ с помощью парадокса дней рождения угадывается промежуточный шифртекст $O_0 \in V_{32}$ после 64 циклов шифрования. Такая пара (I_0, O_0) называется *слайдовой парой*. Используя периодическую структуру ключа, в KeeLoq генерируются другие пары $(I_i, O_i) \in (V_{32})^2, i = 1, \ldots, N-1$. Для успешной атаки их число должно быть около 2^8. Для каждого такого набора пар получаются линейные соотношения для неизвестных битов ключа с высокой вероятностью в связи с тем, что нелинейная функция обратной связи, использующаяся в KeeLoq, не является 2-устойчивой. Таким образом, можно определить $(k_{47}, \ldots, k_{16})$ бит за битом. После этого решается треугольная система линейных уравнений для оставшихся битов ключа $(k_{63}, \ldots, k_{48})$.

Отметим, что в методе А. Богданова для каждого подключа $K' = (k_{15}, \ldots, k_0)$ по сути происходит полный перебор всевозможных пар (кандидатов на первую слайдовую пару (I_0, O_0)) из случайного подмножества мощности 2^{16} множества всех двоичных векторов длины 32 и для каждой такой пары (I_0, O_0) выполняется корреляционный криптоанализ.

В данной работе предлагается на каждом шаге корреляционной атаки использовать найденные биты ключа для отсеивания неподходящих пар, а именно можно найти вероятностное соотношение между битами из правильной слайдовой пары и битами ключа, проверка которого позволяет для части неправильных пар остановить выполнение корреляционного криптоанализа уже на этом шаге. В этом соотношении используется линейное приближение нелинейной функции NLF, выполняющееся с вероятностью $5/8$.

Например, связь бита $y_0^{(64)}$ с битами на 16-м раунде выражается так:

$$y_0^{(64)} = y_{31}^{(33)} = NLF(y_{31}^{(32)}, y_{26}^{(32)}, y_{20}^{(32)}, y_9^{(32)}, y_1^{(32)}) \oplus y_{16}^{(32)} \oplus y_0^{(32)} \oplus k_{32} =$$
$$= y_1^{(32)} \oplus y_9^{(32)} \oplus y_{16}^{(32)} \oplus y_0^{(32)} \oplus k_{32} = y_{17}^{(16)} \oplus y_{25}^{(16)} \oplus y_{31}^{(17)} \oplus y_{16}^{(16)} \oplus k_{32} =$$
$$= y_{17}^{(16)} \oplus y_{25}^{(16)} \oplus (NLF(y_{31}^{(16)}, y_{26}^{(16)}, y_{20}^{(16)}, y_9^{(16)}, y_1^{(16)}) \oplus y_{16}^{(16)} \oplus y_0^{(16)} \oplus k_{16}) \oplus y_{16}^{(16)} \oplus k_{32}.$$

Таким образом, после того как будут найдены k_{16} и k_{32} на первом шаге корреляционной атаки, для отсеивания неправильных слайдовых пар используются биты ключа $(k_{16}, k_{15}, \ldots, k_0)$ и k_{32}.

На каждом шаге корреляционной атаки используется дополнительное соотношение для битов входного и выходного текста, что позволяет останавливать криптоанализ с вероятностью $5/8$ для каждой пары, которая не удовлетворяет полученным соотношениям. Следующая таблица иллюстрирует этот процесс.

Шаг	0	1	2	...	15	16
Количество слайдовых пар	2^{32}	2^{31}	2^{30}	...	2^{17}	2^{16}
Найденные биты ключа	$k_{15}, \ldots, k_0$	k_{16}, k_{32}	k_{17}, k_{33}	...	k_{30}, k_{46}	k_{31}, k_{47}

Во второй строке указано количество пар, для которых будет выполняться следующий шаг корреляционного анализа. Например, изначально понадобится перебор 2^{32} пар. Затем находятся биты ключа k_{16} и k_{32} на первом шаге корреляционной атаки, которые используются в соотношении между $y_0^{(64)}$ и битами шифртекста после 16 циклов. Значит, можно не рассматривать пары, не удовлетворяющие этому соотношению.

Следовательно, число пар, для которых будет выполняться следующий шаг криптоанализа, сократится до 2^{31}, и т. д.

При выборе другого приближения нелинейной функции NLF можно добиться повышения вероятности нахождения правильной слайдовой пары.

В дальнейшем необходимо определить параметры улучшенного метода криптоанализа: временную сложность, требуемую память и т. д.

ЛИТЕРАТУРА

1. *Bogdanov A.* Cryptanalysis of the KeeLoq Block cipher // `http://eprint.iarc.org/2007/055`, 2007.
2. *Bogdanov A.* Attack on the KeeLoq Block Cipher and Authentication System // `http://rfidsec07.etsit.uma.es/slides/papers/paper-22.pdf`, 2007.

УДК 519.7

О НЕВОЗМОЖНЫХ УСЕЧЁННЫХ РАЗНОСТЯХ XSL-АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

М. А. Пудовкина

Идея использовать невозможные разности, т. е. разности с нулевой вероятностью, для определения ключа шифрования была предложена Л. Р. Кнудсеном [1] при анализе алгоритма блочного шифрования DEAL. Позже невозможные разности применялись для атак на алгоритмы блочного шифрования Skipjack [2], MISTY1 [3], AES [4], ARIA [5] и др.

Пусть $X^{\times} = X\backslash\mathbf{0}$; $S(X)$ — множество всех подстановок на множестве X; V_t — множество всех t-мерных векторов над $\mathrm{GF}(2)$; $m = d \cdot q$; $\tilde{s}_0, \ldots, \tilde{s}_{q-1} \in S(V_d)$; $H_d \in \in \left\{V_d, \mathrm{GF}(2^d)\right\}$; $\tilde{\alpha} \in V_d$; нелинейное преобразование $s : V_m \to V_m$ есть $s = (\tilde{s}_{q-1}, \ldots, \tilde{s}_0)$, где $\tilde{s}_i \in S(V_d)$; линейное преобразование $a : H_d^q \to H_d^q$ в стандартном базисе задаётся как

$$(\alpha_{q-1,i}, \ldots, \alpha_{0,i})\,\mathbf{a} = \left(\alpha'_{q-1,i}, \ldots, \alpha'_{0,i}\right),$$

где $\mathbf{a} = (a_{ij})$ — обратимая $(q \times q)$-матрица над $\mathrm{GF}(2)$ $(\mathrm{GF}(2^d))$; $\mathbf{a}^{-1} = \mathbf{b} = (b_{ij})$;

$$A^{(j)} = \{i \in \{0, ..., q-1\} : a_{ji} > 0\}, \quad B^{(j)} = \{i \in \{0, ..., q-1\} : b_{ji} > 0\}.$$

В работе рассматриваются алгоритмы блочного шифрования с раундовой функцией $g_\beta : V_m \to V_m$, заданной как $\alpha^{g_\beta} = (\alpha \oplus \beta)^{sa}$ для всех $\beta, \alpha \in V_m$, и $f_{(k_1,\ldots,k_j)} = = g_{k_1} \ldots g_{k_j}$ — j-раундовая функция зашифрования. Предполагается, что раундовые ключи $k_1, \ldots, k_l$ выбираются случайно и равновероятно из V_m.

Зафиксируем номера координат $\{j_1, \ldots, j_c\} \subset \{0, \ldots, q-1\}$, $j_1 < \ldots < j_c$. Положим

$$\Lambda(j_1, \ldots, j_c) = \{\alpha \in H_d^q : \tilde{\alpha}_{j_t} \neq 0,\ t = 1, \ldots, c\}.$$

Множество разностей $(\Lambda(j_1, \ldots, j_c), \Lambda(i_1, \ldots, i_{t'}))$ называется невозможной усечённой разностью для преобразования $v \in S(V_m)$, если для любых векторов $\alpha \in \in \Lambda(j_1, \ldots, j_c)$, $\beta \in \Lambda(i_1, \ldots, i_{t'})$ выполняется равенство $p_{\alpha,\beta}(v) = 0$, где

$$p_{\alpha,\beta}(v) = 2^{-m} \cdot |\{\lambda \in V_m : (\lambda \oplus \alpha)^v \oplus \lambda^v = \beta\}|.$$

В этом случае при $v = f_{(k_1,\ldots,k_j)}$ будем использовать обозначение

$$\Lambda(j_1, \ldots, j_c) \not\twoheadrightarrow_j \Lambda(i_1, \ldots, i_{t'}).$$