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

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

Покажем, что для большого класса XSL-алгоритмов блочного шифрования существуют 3-раундовые невозможные разности.

Утверждение 1. Пусть $\mathbf{a}$ — такая произвольная обратимая $(q \times q)$-матрица над полем GF(2) (GF(2^d)), что по крайней мере один элемент в столбце $a_t^{\downarrow}$ или $b_t^{\downarrow}$ равен нулю для некоторого $t \in \{0, \ldots, q-1\}$. Тогда существует 3-раундовая невозможная усечённая разность $\Lambda(i) \not\twoheadrightarrow_3 \Lambda(j)^a$ для некоторых $i, j \in \{0, \ldots, q-1\}$.

Таким образом, для любой обратимой матрицы $\mathbf{a}$ над полем GF(2) в алгоритме шифрования XSL существует 3-раундовая усечённая невозможная разность, а значит, и просто 3-раундовая невозможная разность. Это следует из того, что если все элементы матрицы $\mathbf{a}$ равны единице, то она является необратимой. Приведём условия, при которых существуют 4-раундовые невозможные усечённые разности.

Утверждение 2. Пусть $i, j \in \{0, \ldots, q-1\}$. Пусть также для всех $\tilde{\alpha}_t'' \in V_d^{\times}$, $t \in A^{(i)}$, $c \in \{0, \ldots, q-1\}$ не выполняются одновременно следующие равенства:

1) $\bigoplus\limits_{t \in A^{(i)}} \tilde{\alpha}_t'' a_{tc} = \tilde{0}$ для всех $c \notin B^{(j)}$;

2) $\bigoplus\limits_{t \in A^{(i)}} \tilde{\alpha}_t'' a_{tc} \neq \tilde{0}$ для всех $c \in B^{(j)}$.

Тогда $\Lambda(i) \not\twoheadrightarrow_4 \Lambda(j)^a$.

Следствие 1. Пусть $i, j \in \{0, ..., q-1\}$. Пусть также для всех $\tilde{\beta}_t'' \in V_d^{\times}$, $t \in B^{(j)}$, $c \in \{0, ..., q-1\}$ не выполняются одновременно следующие равенства:

1) $\bigoplus\limits_{t \in B^{(i)}} \tilde{\beta}_t'' \cdot b_{tc} = \tilde{0}$ для всех $c \notin A^{(i)}$;

2) $\bigoplus\limits_{t \in B^{(i)}} \tilde{\beta}_t'' \cdot b_{tc} \neq \tilde{0}$ для всех $c \in A^{(j)}$.

Тогда $\Lambda(i) \not\twoheadrightarrow_4 \Lambda(j)^a$.

Приведены примеры 4-раундовых усечённых разностей для некоторых алгоритмов блочного шифрования. Отметим, что утверждения 3, 4, 5 работы [6] являются следствием п. 1 утверждения 2.

ЛИТЕРАТУРА

1. *Knudsen L. R.* DEAL — A 128-bit Block Cipher // Technical Report Department of Informatics. University of Bergen, Norway, 1998.
2. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials // LNCS. 1999. V. 2595. P. 12–23.
3. *Dunkelman O. and Keller N.* An Improved Impossible Differential Attack on MISTY1 // LNCS. 2008. V. 5350. P. 441–454.
4. *Lu J., Dunkelman O., Keller N., and Kim J.* New Impossible Differential Attacks on AES // LNCS. 2008. V. 5365. P. 279–293.
5. *Li R., Sun B., Zhang P., and Li C.* New Impossible Differential Cryptanalysis of ARIA // Cryptology ePrint Archive, Report 2008/227. `http://eprint.iacr.org/2008/227`
6. *Li R., Sun B., and Li C.* Impossible Differential Cryptanalysis of SPN Ciphers // Cryptology ePrint Archive, Report 2010/307. `http://iacr.org/2010/307`