

$k, k', k'', k''' \in V_{256}$, удовлетворяющих равенствам

$$\begin{aligned} k \oplus k' &= k'' \oplus k''' = (\varepsilon_{31}, \mathbf{0}, \varepsilon_{31}, \mathbf{0}, \varepsilon_{31}, \mathbf{0}, \varepsilon_{31}, \mathbf{0}, \varepsilon_{31}, \mathbf{0}), \\ k \oplus k'' &= k' \oplus k''' = (\varepsilon_{31}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}). \end{aligned}$$

Для s -боксов из [7] применима только атака с четырьмя связанными ключами. Трудоёмкость алгоритма нахождения ключа шифрования оценивается как $2^{44,8}$ зашифрованных, число открытых текстов равно $2^{26,2}$, вероятность успеха — 0,99.

ЛИТЕРАТУРА

1. Seki H., Kaneko T. Differential cryptanalysis of reduced rounds of gost // Selected Areas in Cryptography. Springer, 2000. No. 2012. P. 315–323.
2. Biham E., Dunkelman O., Keller N. Improved slide attacks // LNCS. 2007. No. 4593. P. 153–166.
3. Kara O. Reflection Cryptanalysis of Some Ciphers // Ibid. 2008. No. 5365. P. 294–307.
4. Ko Y., Hong S., Lee W., et al. Related key differential attacks on 27 rounds of xtea and full-round gost // Ibid. 2004. No. 3017. P. 299–316.
5. Fleischmann E., Gorski M., Huhne J.-H., Lucks S. Key Recovery Attack on full GOST Block Cipher with Zero Time and Memory // WEWoRC. 2009.
6. Rudskoy V. On zero practical significance of “Key recovery attack on full GOST block cipher with zero time and memory” // <http://eprint.iacr.org/2010/>.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.

УДК 519.7

РАЗНОСТНАЯ АТАКА НА 6-РАУНДОВ WHIRLPOOL-ПОДОБНЫХ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ¹

М. А. Пудовкина

В данной работе вводится семейство алгоритмов блочного шифрования, у которых функция зашифрования и алгоритм развёртывания ключа имеют структуру, как у алгоритма блочного шифрования криптосистемы Whirlpool. Криптосистема Whirlpool является одним из финалистов конкурса NESSIE и входит в международный стандарт ISO/IEC 10118-3. Это семейство алгоритмов характеризуется тем, что функция зашифрования и алгоритм развёртывания ключа совпадают.

Обозначения: $\mathbb{N}$ — множество натуральных чисел; $m, d, q \in \mathbb{N}$; $n = m \cdot d \cdot q$; V_d — пространство d -мерных векторов над полем $\text{GF}(2)$; $\oplus$ — операция сложения в векторном пространстве V_n ; $\alpha = (\tilde{\alpha}_0, \dots, \tilde{\alpha}_{dq-1}) = (\hat{\alpha}_0, \dots, \hat{\alpha}_{q-1}) \in V_n$, $\tilde{\alpha} \in V_m$, $\hat{\alpha} \in V_{md}$; $S(X)$ — симметрическая группа на множестве X ; $X_i = \{id, \dots, (i+1)d-1\}$, $i = 0, \dots, q-1$; n_o — число пар открытых текстов; $\hat{r}$ — произвольная подстановка из $S(\{0, \dots, q-1\})$, индуцирующая при координатном действии линейное преобразование r векторов $\alpha = (\tilde{\alpha}_0, \dots, \tilde{\alpha}_{dq-1})$ векторного пространства; $\hat{h}$ — произвольное линейное обратимое преобразование из $S(V_{dm})$; $h : \alpha = (\tilde{\alpha}_0, \dots, \tilde{\alpha}_{qd-1}) \mapsto (\hat{\alpha}_0^{\hat{h}}, \dots, \hat{\alpha}_{q-1}^{\hat{h}})$; $\hat{\alpha}_i^{r^{-1}} = \hat{\alpha}_{i*}$, $i = 0, \dots, q-1$; э.о. — элементарная операция; l — число раундов; произвольные подстановки $\tilde{s}_i \in S(V_m)$ индуцируют покоординатные действия $s \in S(V_n)$, $\hat{s}_j \in S(V_{md})$ и $\hat{s}_i = (\tilde{s}_{id}, \dots, \tilde{s}_{(i+1)d-1})$, т.е. $s : \alpha = (\tilde{\alpha}_0, \dots, \tilde{\alpha}_{qd-1}) \mapsto (\hat{\alpha}_0^{\hat{s}_0}, \dots, \hat{\alpha}_{q-1}^{\hat{s}_{q-1}}) = (\tilde{\alpha}_0^{\tilde{s}_0}, \dots, \tilde{\alpha}_{qd-1}^{\tilde{s}_{qd-1}})$.

¹Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.

В данной работе рассматриваются преобразования r , для которых выполняется соотношение $|X_i^{\hat{r}} \cap X_j| = 1$ для всех $i, j \in \{0, \dots, q-1\}$. Такие подстановки $\hat{r}$ возможны при $q = d$ и используются, например, в алгоритме блочного шифрования криптосистемы Whirlpool. Приведём описание рассматриваемого семейства алгоритмов блочного шифрования.

Алгоритм развёртывания ключа $\varphi : k \mapsto (k^{(1)}, \dots, k^{(l)})$ задаётся следующим образом:

$$k^{(1)} = k, k^{(j)} = (c^{(j-1)} \oplus k^{(j-1)})^{srh} = f_{k^{(j-1)}}(c^{(j-1)}),$$

где $c^{(j)}$ — фиксированные константы, $j = 2, \dots, l$.

Для раундового ключа $k^{(i)} \in V_n$ раундовая функция зашифрования $f_{k^{(i)}} : V_n \rightarrow V_n$ определяется как $f_{k^{(i)}}(\alpha) = (\alpha \oplus k^{(i)})^{srh}$.

Функция зашифрования $g_k : V_n \rightarrow V_n$ определяется как

$$\alpha^{gk} = \alpha^{(l)} = \alpha^{f_{k^{(1)}} \dots f_{k^{(l)}}}.$$

Отметим, что в рассматриваемое семейство алгоритмов при $m = q = d = 8$ и шести раундах попадает алгоритм блочного шифрования криптосистемы Whirlpool.

В данной работе показано, что шесть раундов произвольного алгоритма из рассматриваемого семейства атакуются разностным методом. Для этого построена 3-раундовая разностная характеристика с $2m + 1$ активными s -блоками вероятностью $p_{\text{char}} \geq 2^{-(m-1)(2d+1)}$. Ещё три раунда удаётся «пройти» из-за следующего свойства алгоритма развёртывания ключа.

Утверждение 1. Пусть $\alpha^{(0)}$ — произвольный открытый текст из V_n и $\alpha^{(i)} = (\alpha^{(0)})^{f_{k^{(1)}} \dots f_{k^{(i)}}}$, $i \in \{1, \dots, 6\}$, k — ключ шифрования, $\varphi : k \rightarrow (k^{(1)}, \dots, k^{(l)})$, $l \geq 6$. Тогда справедливо равенство

$$\hat{\alpha}_{j*}^{(3)} = \hat{k}_j^{(5)\hat{h}^{-1}r^{-1}s^{-1}} \oplus \hat{c}_{j*}^{(4)} \oplus \left(\left(\alpha^{(6)\hat{h}^{-1}r^{-1}s^{-1}\hat{h}^{-1}r^{-1}} \oplus \left(\hat{k}_j^{(5)} \oplus c_j^{(5)} \right)^{\hat{s}_j} \right)^{\hat{s}_j^{-1}} \oplus \hat{k}_j^{(5)} \right)_j^{\hat{h}^{-1}r^{-1}s^{-1}}.$$

Таким образом, по известным блоку шифртекста $\alpha^{(6)}$ и подблоку $\hat{k}_j^{(5)}$ раундового ключа находится подблок промежуточного шифртекста $\hat{\alpha}_{j*}^{(3)}$. Затем на основе 3-раундовой характеристики строится атака на 6-раундовый алгоритм.

Пусть $p_{\text{char}} > 2^{-2dm}$ или $m \leq 2d$. Тогда трудоёмкость метода может быть оценена как $2^{2dm+1}n_o + 2^{md+1}n_o(q-2)$ э.о. При $p_{\text{char}} \leq 2^{-2dm}$ трудоёмкость метода оценивается как $3 \cdot 2^{3dm}n_o + 3 \cdot 2^{md}n_o(q-3)$ э.о. Число необходимых пар текстов при заданной надёжности метода находится по формуле (14) работы [1]. Оценка трудоёмкости атаки существенно зависит от выбора соотношений между параметрами m, d, q . При $m = q = d = 8$ и $n = 512$ для алгоритма блочного шифрования криптосистемы Whirlpool оценка сверху трудоёмкости нахождения ключа шифрования равна $2^{236,3}$ э.о., а вероятность успеха — 0,9999999993, число открытых текстов — $2^{107,3}$. Видно, что она меньше, чем корень из трудоёмкости полного перебора. Кроме того, из свойств s -блоков в криптосистеме Whirlpool следует, что $p_{\text{char}} \geq 2^{-(m-2)(2d+1)}$.

ЛИТЕРАТУРА

1. Selcuk A., Bicak A. On Probability of Success in Linear and Differential Cryptanalysis // LNCS. 2002. No. 2365. P. 174–185.