17. *Fleischmann E., Gorski M., Huhne J.-H., Lucks S.* Key Recovery Attack on full GOST Block Cipher with Zero Time and Memory // WEWoRC. 2009.

УДК 519.7

АТАКИ НА АЛГОРИТМ БЛОЧНОГО ШИФРОВАНИЯ ГОСТ 28147-89 С ДВУМЯ И ЧЕТЫРЬМЯ СВЯЗАННЫМИ КЛЮЧАМИ [1]

М. А. Пудовкина, Г. И. Хоруженко

Алгоритм шифрования ГОСТ 28147-89 является обязательным для применения в государственных организациях и ряде коммерческих организаций Российской Федерации. Алгоритм содержит ряд потенциальных слабостей, связанных с алгоритмом развёртывания ключа, в частности, его линейность, использование подблоков ключа в явном виде в раундовых функциях. В последние годы в открытой литературе появилось немало работ [1 – 5], в которых проводился криптоанализ алгоритма ГОСТ 28147-89. В работе [5] приведена атака на алгоритм блочного шифрования ГОСТ 28147-89 на основе методов бумеранга и связанных ключей, которая содержит ряд ошибок и на самом деле не работает. Однако основная идея, лежащая в её основе, позволяет подправить предложенную атаку и, внеся дополнительные модификации, получить работающий алгоритм. Так это было сделано в работе [6]. В предложенной атаке для нахождения всего ключа шифрования при использовании s-боксов из [7] требуется 18 связанных ключей, а её трудоёмкость оценивается как 2^{26} зашифрований. Отметим, что независимо от работы [6] атака на основе 18 связанных ключей была также предложена нами.

Пусть V_n — пространство n-мерных векторов над полем GF(2); $\oplus$ — операция сложения в векторном пространстве V_n; $\varepsilon_i = \left(0, ..., 0, 1, \underbrace{0, ..., 0}_{i}\right) \in V_{32}$, $i = 0, ..., 31$.

Основными нашими результатами являются предложенные атаки на основе двух или четырёх связанных ключей в зависимости от свойств s-боксов алгоритма ГОСТ 28147-89. При атаке на основе двух связанных ключей используются идеи из работы [4] и пара связанных ключей $k, k' \in V_{256}$,

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

На основе разностного метода и метода связанных ключей находятся раундовые ключи $k_{26}, ..., k_{32}$, а раундовый ключ k_{25} определяется с помощью методов бумеранга и связанных ключей. Описан класс s-боксов, для которых данный подход заведомо неприменим. Трудоёмкость метода $T_m^{(1)}$ на основе двух связанных ключей оценивается числом необходимых шифрований. В зависимости от свойств s-бокса она удовлетворяет неравенству $2^{26,6} \leqslant T_m^{(1)} < 2^{40}$, надёжность метода равна 0,98, а число пар открытых текстов $n^{(1)}$ удовлетворяет неравенству $2^{15} \leqslant n^{(1)} < 2^{29}$.

С помощью комбинации идей из работ [4, 6] предложена атака на основе методов связанных ключей, разностного и бумеранга с четырьмя связанными ключами. Показано, что атака из работы [6] и предлагаемая нами неприменимы, если подстановка s_1 s-бокса имеет линейный транслятор ε_3. Отметим, что в работе [6] считалось, что атака применима для всех s-боксов. В нашей атаке используется четверка связанных ключей

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

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

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

Для s-боксов из [7] применима только атака с четырьмя связанными ключами. Трудоёмкость алгоритма нахождения ключа шифрования оценивается как $2^{44,8}$ зашифрований, 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 ШИФРОВАНИЯ[1]

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 $\mathrm{GF}(2)$; $\oplus$ — операция сложения в векторном пространстве V_n; $\alpha = (\tilde{\alpha}_0, ..., \tilde{\alpha}_{dq-1}) = (\hat{\alpha}_0, ..., \hat{\alpha}_{q-1}) \in V_n, \tilde{\alpha} \in V_m, \hat{\alpha} \in V_{md}$; $S(X)$ — симметрическая группа на множестве X; $X_i = \{id, ..., (i+1)d - 1\}$, $i = 0, ..., q-1$; $n_{\text{о}}$ — число пар открытых текстов; $\hat{r}$ — произвольная подстановка из $S(\{0, ..., q-1\})$, индуцирующая при координатном действии линейное преобразование r векторов $\alpha = (\tilde{\alpha}_0, ..., \tilde{\alpha}_{dq-1})$ векторного пространства; $\hat{h}$ — произвольное линейное обратимое преобразование из $S(V_{dm})$; $h : \alpha = (\tilde{\alpha}_0, ..., \tilde{\alpha}_{qd-1}) \mapsto (\hat{\alpha}_0^{\hat{h}}, ..., \hat{\alpha}_{q-1}^{\hat{h}})$; $\hat{\alpha}_i^{r^{-1}} = \hat{\alpha}_{i*}$, $i = 0, ..., q-1$; 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 $\hat{s}_i = (\tilde{s}_{id}, ..., \tilde{s}_{(i+1)d-1})$, т. е. $s : \alpha = (\tilde{\alpha}_0, ..., \tilde{\alpha}_{qd-1}) \mapsto (\hat{\alpha}_0^{\hat{s}_0}, ..., \hat{\alpha}_{q-1}^{\hat{s}_{q-1}}) = (\tilde{\alpha}_0^{\tilde{s}_0}, ..., \tilde{\alpha}_{qd-1}^{\tilde{s}_{qd-1}})$.

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