ЛИТЕРАТУРА

1. *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptol. 1991. V. 4. P. 3–72.
2. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1(1). С. 34–42.
3. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. 2009. № 4(6). С. 56–63.
4. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. 2009. № 4. С. 57–62.

УДК 519.7

О СЛАБОМ КЛАССЕ АЛГОРИТМОВ РАЗВЁРТЫВАНИЯ КЛЮЧА ОТНОСИТЕЛЬНО МЕТОДА СВЯЗАННЫХ КЛЮЧЕЙ[1]

М. А. Пудовкина

В открытой литературе появляется всё больше работ, посвященных атакам на алгоритмы шифрования на основе метода связанных ключей и основанных на слабостях алгоритма развёртывания ключа (см., например, [1 – 8]). Однако имеется небольшое число работ, в которых описываются классы слабых алгоритмов развёртывания ключа или исследуются их свойства. Данную работу можно отнести к их числу.

Обозначим: $\mathbb{N}$ — множество натуральных чисел; $\mathbb{N}_0$ — множество натуральных чисел с нулем; $n, r, d, l \in \mathbb{N}$; V_n — n-мерное векторное пространство над полем $\mathrm{GF}(2)$; l — число раундов шифрования блочного алгоритма; $2 \leqslant r < l$; $g_k : V_n \to V_n$ — раундовая функция; $K = V_d$ — ключевое множество.

В данной работе рассматриваются функция зашифрования и алгоритм развёртывания ключа $\varphi^* = (\delta, \varphi)$, такие, что существуют число $r \in \mathbb{N}$, $r \leqslant l$, и отображения $\lambda : V_n^r \to V_n$, $\delta : K \to V_n^r$, $\varphi : V_n^r \to V_n^l$, удовлетворяющие следующим свойствам:

1) $(r-1) \cdot n < d \leqslant r \cdot n$;
2) $\delta(k) = (k_0, ..., k_{r-1})$;
3) для любого $i \in \mathbb{N}_0$ выполняется равенство

$$(k_i, ..., k_{i+l-1}) = \varphi(k_i, ..., k_{i+r-1}),$$

где $k_{i+l+j} = \lambda(k_{i+j}, ..., k_{i+r-1+j})$, $j = 0, ..., l-r$;
4) раундовая функция на всех раундах не зависит от номера раунда;
5) $g_k \neq g_{k'}$ для любых различных $k, k' \in V_n$;
6) существует такая функция $\psi : V_n \times V_n \to V_n$, что для всех $k \in V_n$, $\alpha \in V_n$ выполняется равенство $k = \psi(\alpha, \beta)$, где $\beta = \alpha^{g_k}$.

Отметим, что условие 5 является естественным и встречается практически во всех алгоритмах блочного шифрования в открытой литературе. Условие 2 означает, что по любой последовательности из r раундовых ключей $k_i, ..., k_{i+r-1}$ для некоторого $i \in \{0, ..., l-r\}$ может быть найден ключ шифрования $k \in K$. Чаще всего ключ шифрования k совпадает с вектором $(k_0, ..., k_{r-1})$, т. е. δ — тождественное отображение. Отметим также, что условие 6 может иногда не выполняться. Кроме того, отображение φ

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

может быть представлено в виде регистрового преобразования. Таким образом, можно говорить об исследовании алгоритмов развёртывания ключа на основе регистров сдвига.

Алгоритмы развёртывания ключа из такого класса имеют, например, следующие алгоритмы шифрования: 25-раундовый ГОСТ 28147-89, полнораундовые LOKI89, LOKI91 [7], MMB [9], TREYFER [10], KeeLoq [11]. Для данного класса предложена атака на основе метода связанных ключей, требующая небольшого числа произвольных открытых текстов, трудоёмкость которой равна трудоёмкости опробования одного раундового ключа. Для построения данной атаки также использовалась идея, применяемая в сдвиговом методе [12]. Отметим, что для атаки на алгоритмы шифрования Фейстеля может потребоваться меньшее число необходимых открытых текстов, чем для атаки на алгоритмы шифрования с произвольный раундовой функцией. Иллюстрируется применение атаки на примере 25-раундового алгоритма шифрования Фейстеля, имеющего функцию развёртывания, как у алгоритма ГОСТ 28147-89. Это даёт ещё один пример атаки на алгоритм ГОСТ 28147-89 в отличие от уже имеющихся открытых работ [13 – 17].

ЛИТЕРАТУРА

1. *Ciet M., Piret G., Quisquater J.-J.* A survey of key schedule cryptanalysis // Universite catholique de Louvain, Crypto Group, `http://www.dice.ucl.ac.be/crypto/techreports.html`. 2002.
2. *Kelsey J., Schneier B., Wagner D.* Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES // LNCS. 1996. No. 1109. P. 237–251.
3. *Kelsey J., Schneier B., Wagner D.* Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA // LNCS. 1997. No. 1334. P. 233–246.
4. *Biryukov A., Khovratovich D., Nikolic I.* Distinguisher and Related-Key Attack on the Full AES-256 // LNCS. 2009. No. 5677. P. 231–249.
5. *Biham E., Dunkelman O., Keller N.* Related-key boomerang and rectangle attacks // LNCS. 2005. No. 3494. P. 507–525.
6. *Biham E.* New Type of Cryptanalytic Attacks Using Related Key // LNCS. 1994. No. 765. P. 229–246.
7. *Knudsen L. R.* Cryptanalysis of LOKI91 // LNCS. 1993. No. 718. P. 196–208.
8. *Ciet M., Piret G., Quisquater J.-J.* Related-Key and Slide Attacks: Analysis, Connections, and Improvements // `http://www.dice.ucl.ac.be/~crypto`.
9. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.
10. *Blunden M., Escott A.* Related Key Attacks on Reduced Round KASUMI // LNCS. 2001. No 2355. P. 277–285.
11. *Courtois N., Bard G.* Algebraic and Slide Attacks on KeeLoq // Cryptology ePrint Archive. 2007. Report 2007/062, 2007.
12. *Biryukov A., Wagner D.* Slide Attacks // LNCS. 1999. No. 1636. P. 245–259.
13. *Seki H., Kaneko T.* Differential cryptanalysis of reduced rounds of gost // Selected Areas in Cryptography. Springer, 2000. No. 2012. P. 315–323.
14. *Biham E., Dunkelman O., Keller N.* Improved slide attacks // LNCS. 2007. No. 4593. P. 153–166.
15. *Kara O.* Reflection Cryptanalysis of Some Ciphers // LNCS. 2008. No. 5365. P. 294–307.
16. *Ko Y., Hong S., Lee W., et al.* Related key differential attacks on 27 rounds of xtea and full-round gost // LNCS. 2004. No. 3017. P. 299–316.

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.