УДК 519.719.2

А.А. МУХОРТОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ СЕМЕЙСТВА 8-РАУНДОВЫХ XSL-АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ МНОГОМЕРНЫМ МЕТОДОМ ВСТРЕЧИ ПОСЕРЕДИНЕ

В работе исследуется семейство XSL-алгоритмов шифрования, основанное на алгоритмах MANTIS и PRINCE, двумерным методом встречи посередине. Предложена атака на 8-раундовые алгоритмы семейства, приведены оценки сложности, необходимый объем памяти и объем материала, включая оценки сложности для оригинальных MANTIS и PRINCE.

Атака двумерным методом встречи посередине является обобщением метода встречи посередине, предложенным в 1977 г. Диффи и Хеллманом [1]. Впервые многомерный метод встречи посередине был предложен применительно к алгоритму KATAN в 2014 г. [2]. Позднее была построена атака методом встречи посередине на алгоритм шифрования PRINCE [3].

PRINCE [4] – низкоресурсный блочный алгоритм шифрования, основанный на XSL-алгоритме шифрования. PRINCE обладает свойством α-отражения, которое определяется как возможность расшифрования шифртекста функцией зашифрования с сопряженным ключом. Раунд шифрования состоит из побитового сложения с раундовым ключом и раундовой константой, подстановки, умножения на матрицу.

MANTIS [5] – низкоресурсный блочный алгоритм шифрования, основанный на алгоритмах PRINCE [4] и MIDORI [6]. От алгоритма шифрования PRINCE MANTIS унаследовал свойство α-отражения и ключевое расписание, а от MIDORI – раундовую функцию.

В работе исследуется обобщенное семейство алгоритмов шифрования, объединяющее алгоритмы MANTIS и PRINCE, а также обобщенное по количеству бит в блоке текста.

В работе проведена модификация атаки, предложенной для алгоритма PRINCE в 2016 г. [3]. Суть атаки состоит в проведении двух атак методом встречи посередине – на первых трех раундах алгоритма и на последних трех. Средние два раунда не используют ключ в соответствии со строением алгоритма шифрования, поэтому в атаке участвуют опосредованно.

Для каждого состояния после трех раундов зашифрования перебираются некоторые биты ключей, после чего происходит встреча после 1.5 раундов зашифрования и 1.5 раундов расшифрования, где и проверяется, удовлетворяют ли ключи условию, что на них был зашифрован данный открытый текст. После отсева ключей, оставшиеся ключи проверяются на второй паре текстов, и остается лишь ключ, на котором было зашифровано сообщение. Таким образом, атака осуществляется с единичной вероятностью.

Временная сложность атаки для алгоритма шифрования выделенного семейства в общем случае при количестве бит в ячейке r и количестве ячеек в блоке текста d варьируется от $2^{r\left(2d-\sqrt{d}\right)}\left(d-\sqrt{d}\right)\cdot d^{-1}\cdot 6^{-1}$ функций зашифрования до $2^{r\left(2d-\sqrt{d}\right)}\left(3d-\sqrt{d}\right)\cdot d^{-1}\cdot 8^{-1}$. Необходимый объем памяти для осуществления атаки варьируется от $2^{r\left(\frac{3}{2}d-2\sqrt{d}\right)}$ до $2^{r\left(\frac{3}{2}d-2\sqrt{d}+3\right)}$ ячеек памяти по $2\cdot \mathrm{r}\left(d-2\sqrt{d}+1\right)$ бит. Необходимый объем материала – 2 пары открытый текст и шифртекст.

Для оригинального 8-раундового MANTIS оценки сложности для атаки многомерным методом встречи посередине предложены в работе впервые, временная сложность алгоритма: $2^{110.8}$ функций зашифрования. Объём памяти: 2^{67} ячеек памяти по 72 бита. Для оригинального PRINCE временная сложность атаки $2^{110.8}$ функций зашифрования. Объем памяти: 2^{65} ячеек памяти по 72 бита, что подтверждает ранее полученные результаты.

Список литературы

1. W. Diffie W. and Hellman M. E., "Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard" // Computer, vol. 10, no. 6, p. 74-84, 1977.
2. Zhu, B., Gong, G. “Multidimensional meet-in-the-middle attack and its applications to KATAN32/48/64” // Cryptography and Communications, 2014.
3. Rasoolzadeh S. and Raddum H., “Cryptanalysis of PRINCE with Minimal Data” // AFRICACRYPT 2016 – vol. 9646, 2016.
4. Borghoff, J. “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications.” // Advances in Cryptology – ASIACRYPT 2012. Lecture Notes in Computer Science, vol. 7658, 2012.
5. Beierle, C. “The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.” // Advances in Cryptology – CRYPTO 2016. Lecture Notes in Computer Science, vol 9815, 2016.
6. Banik, S. “Midori: A Block Cipher for Low Energy.” // Advances in Cryptology – ASIACRYPT 2015. Lecture Notes in Computer Science, vol. 9453, 2015.