Реализация алгебраической атаки на шифры ГОСТ Р 34.12-2015

Е.А. Маро

Южный федеральный университет, Таганрог

Аннотация: В работе приведено описание алгебраического метода анализа стойкости шифров ГОСТ Р 34.12-2015 с размером блоков n=64 и N=128 бит. Рассмотрен метод eXtended Linearization решения системы нелинейных алгебраических уравнений, сформированных для блоков замены размером 4x4 и 8x8 бит. Описан алгоритм параллельного формирования системы уравнений и приведены оценки временной сложности вычисления уравнений.
Ключевые слова: алгоритм шифрования, симметричное блочное шифрование, блок замены, алгебраический метод криптоанализа, eXtended Linearization.

В основе всех алгебраических атак лежит описание преобразований шифрования в виде системы уравнений, связывающей секретный ключ симметричного шифрования и известные криптоаналитику данные. При криптоанализе блочных шифров для генерации системы используются нелинейные преобразования алгоритма шифрования - блоки замены. В зависимости от количества уравнений и переменных в системе, решение может быть найдено с помощью методов линеаризации [1], релинеаризации [2], eXtended Linearization (XL) [3], eXtended Sparse Linearization (XSL)[4]. Важной особенностью алгебраических атак является небольшое количество необходимых криптоаналитику пар открытый текст/шифротекст.

Работа посвящена исследованию криптоанализа алгоритма ГОСТ Р 34.12-2015 [5] с помощью метода eXtended Linearization (XL), предложенного в работе [3] для атаки на алгоритм шифрования Rijndael. В стандарте ГОСТ Р 34.12-2015 приведено описание двух симметричных блочных шифров с длиной блока n: шифр Магма [6] (n=64) и шифр Кузнечик (n=128).

Шифр Магма в каждом раунде использует 8 блоков замены размером 4x4x бита, таблица замены которых задана стандартом. Алгебраическая

иммунность блоков замены шифра Магма равна 2. Для данных блоков замены формируются уравнения заданные формулой (1).

$$\sum \alpha_{i,j} x_i x_j + \sum \beta_{i,j} y_i y_j + \sum \gamma_{i,j} x_i y_j + \sum \delta_i x_i + \sum \varepsilon_i y_i + \eta = 0, \qquad (1)$$

где $x_i x_j$ - комбинация входных битов S-блока;

$y_i y_j$ - комбинация выходных битов S-блока;

$x_i y_j$ – комбинация входных и выходных битов;

x_i и y_i – соответственно входные и выходные биты S-блока;

η – коэффициент, принимающий значения 0 или 1.

Для блока замены шифра Магма можно сформировать 21 линейно независимое уравнение [7]. В системе будут встречаться 37 уникальных одночленов. Написана программа поиска уравнений заданного вида, соответствующих таблице блока замены. Для ускорения поиска реализовано многопроцессорное вычисление при поиске верных уравнений. Каждому потоку передается фиксированный диапазон поиска [8]. Параллельное вычисление уравнений для восьми блоков замены на компьютере с характеристиками Intel Core i5 2.8 ГГц, 8Гбайт потребовало 20 часов (74453 сек.). Структура полученной системы уравнений для одного и двух раундов шифра Магма позволяет найти решение с помощью метода линеаризации [1]. Данный метод заключается в замене каждого нелинейного одночлена ($x_i x_j$) на новое неизвестное u_g и решении получившейся линейной системы уравнений относительно новых переменных, с последующим нахождением решений первоначальной системы путем решения систем специального вида $x_i x_j = u_g$, для каждого полученного решения линейной системы. Для трех раундов шифра Магма система уравнений содержала недостаточное число линейно независимых уравнений для возможности применения метода линеаризации, поэтому использовался метод eXtended Linearization [3].

Разработчиками алгебраического метода анализа сделано допущение, что под сложностью атаки рассматривается решение системы, приведенной к линейному виду (для метода исключения Гаусса сложность $O(n^3)$), не учитывая сложность подготовительных этапов по составлению системы и получению дополнительных уравнений. В этом случае сложность анализа одного раунда шифра Магма составит $80^3 \approx 2^{19}$. Для двух раундов сложность $160^3 \approx 2^{22}$.

Шифр Кузнечик построен на проверенной временем схеме Substitution-Permutation network. По своей структуре шифр близок к Advanced Encryption Standard (AES) [9]. Анализу стойкости шифра Кузнечик посвящены работы [10-12]. Алгоритм формирования таблицы блока замены шифра Кузнечик не описан в стандарте ГОСТ Р34.12-2015, ознакомиться с исследованиями по восстановлению структуры блока замены можно в работе [13]. В отличие от AES (алгебраическая иммунность равна 2) алгебраическая иммунность замены шифра Кузнечик равна 3 [14], поэтому для описания работы блока замены должны быть составлены уравнения вида (2).

$$\sum \alpha_{i,j,k} x_i y_j y_k + \sum \beta_{i,j,k} x_i y_j y_k + \sum \gamma_{i,j} x_i y_j + \sum \delta_i x_i + \sum \varepsilon_i y_i + \eta = 0 \qquad (2)$$

Опираясь на алгоритм, описанный в работе [15], для формирования системы уравнений следует проверить возможные сочетания одночленов на соответствие таблице замены. Для блока замены размером 8x8 бит можно составить 697 одночленов. Формирование системы уравнений для S-блока можно выполнить однократно. Всего следует составить 2^{697} возможных уравнений, не менее 441 уравнения будут линейно независимыми. Для формирования системы уравнений для S-блоков на ПК Intel Corei5 2.8 ГГц, 8Гбайт потребовалось 164 часа (604857 сек.). Для одного раунда шифрования Кузнечик система уравнений после домножения по алгоритму XL содержит 7497 уравнений и 1820 одночленов. Сложность метода приравнивается к сложности решения линейной системы $1820^3 \approx 2^{33}$.

Работа выполнена при поддержке гранта РФФИ № 15-37-20007 мол_а_вед.

Литература

1. Courtois N., Goubin L., Meier W., Tacier J.-D. Solving Underdefined Systems of Multivariate Quadratic Equations. Public Key Cryptography2002: Vol. 2274. Lecture Notes in Computer Science (pp. 211-227). New York: Springer.

2. Kipnis A., Shamir A. Cryptanalysis of the HFE public key cryptosystem by relinearization. Advances in Cryptology–Crypto'99: Vol. 1666. Lecture Notes in Computer Science (pp. 19-30). New York: Springer.

3. Courtois N., Klimov A., Patarin J., Shamir A. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. Advances in Cryptology - EUROCRYPT, 2000: Vol. 1807. Lecture Notes in Computer Science (pp. 392–407). New York: Springer.

4. Courtois N., Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations. Asiacrypt, 2002: Vol. 2501. Lecture Notes in Computer Science (pp. 267-287). New York: Springer.

5. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» // Москва, Стандартинформ, 2015, 26 С.

6. Ищукова Е.А., Калмыков И.А. Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147-89// Инженерный вестник Дона, 2015, №4 URL: ivdon.ru/ru/magazine/archive/n4y2015/3284.

7. Маро Е.А. Алгебраический анализ стойкости криптографических систем защиты информации // Инженерный вестник Дона, 2013, №4 URL: ivdon.ru/ru/magazine/archive/n4y2013/1996.

8. Маро Е.А. Повышение эффективности алгебраических методов оценки стойкости блочных шифров // Материалы VI Международной интернет-

конференции молодых ученых, аспирантов, студентов «Инновационные технологии: теория, инструменты, практика», Изд-во ПНИПУ, Пермь, 2015, С. 129-134.

9. Specification for the ADVANCED ENC RYPTION STANDARD (AES) // Federal Information Processing Standards Publication, URL: csrc.nist.gov/publications/fips/fips197/fips-197.pdf

10. AlTawy R., Duman O., Youssef A.M. Fault analysis of Kuznyechik // URL: eprint.iacr.org/2015/347.pdf

11. AlTawy R., Youssef A.M. A meet in the Middle Attack on Reduced Kuznyechik // URL: https://eprint.iacr.org/2015/096.pdf

12. Fomin D. A timing attack on CUDA implementations of an AES-type block cipher, CTCrypr 2015 Preproceedings, Kazan, 2015.

13. Alex Biryukov, Léo Perrin, Aleksei Udovenko The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob // URL: eprint.iacr.org/2015/812.pdf.

14. Kazymyrov O. Methods and tools for analysis of symmetric cryptographic primitives // Dissertation for the degree of PhD. URL: bora.uib.no/handle/1956/8828.

15. Babenko L.K., Ishchukova E.A., Maro E.A.. Algebraic analysis of GOST encryption algorithm. Proceedings of the 4th International Conference of Security of Information and Networks, 2011 (pp. 57-62). New York: Association for Computing Machinery, Inc.

References

1. Courtois N., Goubin L., Meier W., Tacier J.-D. Solving Underdefined Systems of Multivariate Quadratic Equations. Public Key Cryptography2002: Vol. 2274. Lecture Notes in Computer Science (pp. 211-227). New York: Springer.

2. Kipnis A., Shamir A. Cryptanalysis of the HFE public key cryptosystem by relinearization. Advances in Cryptology–Crypto'99: Vol. 1666. Lecture Notes in Computer Science (pp. 19-30). New York: Springer.

3. Courtois N., Klimov A., Patarin J., Shamir A. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. Advances in Cryptology - EUROCRYPT, 2000: Vol. 1807. Lecture Notes in Computer Science (pp. 392–407). New York: Springer.

4. Courtois N., Pieprzyk J. Cryptanalysis of block ciphers with overdefined systems of equations. Asiacrypt, 2002: Vol. 2501. Lecture Notes in Computer Science (pp. 267-287). New York: Springer.

5. GOST R 34.12-2015 «Informacionnaya tehnologiya. Kriptographicheskaya zashita informacii. Blochnye shifry» [Information technology. Cryptographic protection of information. Block ciphers]. Moscwa, Standartinform, 2015, 26 p.

6. Ishchukova E.A., Kalmyikov I.A. Inženernyj vestnik Dona (Rus), 2015, №4 URL: ivdon.ru/ru/magazine/archive/n4y2015/3284.

7. Mapo E.A. Inženernyj vestnik Dona (Rus), 2013, №4 URL: ivdon.ru/ru/magazine/archive/n4y2013/1996.

8. Maro E.A. Povyishenie effectivnosti algebraicheskih metodov ocenki stoikosti blochnyih shifrov [Improving efficiency of algebraic methods estimate the resistance of block ciphers]. Materialyi VI Mejdynarodnoy internet konferencii molodyih ychenyih, aspirantov, studentov «Innovacionnyie tehnologii: teoriya, instrumentyi, practica», 2015, pp. 129-134.

9. Specification for the ADVANCED ENC RYPTION STANDARD (AES). Federal Information Processing Standards Publication, URL: csrc.nist.gov/publications/fips/fips197/fips-197.pdf

10. AlTawy R., Duman O., Youssef A.M. Fault analysis of Kuznyechik. URL: eprint.iacr.org/2015/347.pdf

11. AlTawy R., Youssef A.M. A meet in the Middle Attack on Reduced Kuznyechik. URL: eprint.iacr.org/2015/096.pdf

12. Fomin D. A timing attack on CUDA implementations of an AES-type block cipher, CTCrypr 2015 Preproceedings, Kazan, 2015.

13. Alex Biryukov, Léo Perrin, Aleksei Udovenko The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob. URL: eprint.iacr.org/2015/812.pdf.

14. Kazymyrov O. Methods and tools for analysis of symmetric cryptographic primitives. Dissertation for the degree of PhD. URL: bora.uib.no/handle/1956/8828.

15. Babenko L.K., Ishchukova E.A., Maro E.A.. Algebraic analysis of GOST encryption algorithm. Proceedings of the 4th International Conference of Security of Information and Networks, 2011 (pp. 57-62). New York: Association for Computing Machinery, Inc.