раскрытия. Трудоемкость механизма отзыва инкапсулируется внутри группы и не делегируется третьей стороне по отношению к группе, а следовательно, и к организации.

ЛИТЕРАТУРА

1. *Васильев П. Н., Артамонов А. В., Маховенко Е. Б.* Классификационная схема групповых подписей для построения распределенных приложений // Научно-технические ведомости СПбГПУ. СПб.: Изд-во Политехнического университета, 2010. С. 71–77.
2. *Shacham H.* New paradigms in signature schemes // `http://hovav.net/dist/thesis.pdf`, 2005.
3. *Delerablee C. and Pointcheval D.* Dynamic fully anonymous short group signatures // LNCS. 2006. V. 4341. P. 193–210.
4. *Bellare M., Shi H., and Zang C.* Foundations of group signatures: the case of dynamic groups // LNCS. 2005. V. 3376. P. 136–153.
5. *Shacham H.* A Cramer — Shoup encryption scheme from the linear assumption and from progressively weaker linear variants // http://eprint.iacr.org/2007/074.pdf.

УДК 519.7

АЛГЕБРАИЧЕСКИЙ КРИПТОАНАЛИЗ ОДНОРАУНДОВОГО S-AES[1]

Р. И. Воронин

Advanced Encryption Standard (AES) — симметричный алгоритм блочного шифрования, принятый в США в качестве стандарта шифрования. AES проектировался как алгоритм, который может эффективно противостоять различным методам криптоанализа. Но в 2002 г. Николя Куртуа и Йозеф Пипджик высказали предположение о возможности алгебраической атаки на шифры с подобной AES структурой [1]. Алгебраическая атака нацелена на анализ уязвимости в математических частях алгоритма и использование его внутренних алгебраических структур. Однако об эффективности такой атаки мало что известно.

В работе исследуется применимость алгебраической атаки к упрощенному варианту S-AES, разработанному в [2]. Длина шифруемого блока и ключа равна 16 битам. Число раундов шифрования равно двум. Для анализа используются соотношения, подобные тем, которые получены в [1] для AES. Точнее, для S-блоков шифра выполнено

$$\forall x \neq 0 \quad 1 = x * y,$$
$$\forall x \quad x = y * x^2,$$
$$z = Ay \oplus b,$$

где x, z — входной и выходной векторы S-блока длины 4; y — обратный вектор к x в поле $\mathrm{GF}(2^4)$ с порождающим многочленом $\lambda^4 + \lambda + 1$; A — некоторая фиксированная матрица и b — фиксированный вектор. С помощью данных уравнений строится система относительно битов открытого текста p, шифртекста c и ключа шифрования k, полностью описывающая процесс шифрования одноразундового S-AES:

$$\sum_{i,j=0}^{15} \alpha_{ijm} p_i c_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm} p_i k_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm} k_i c_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm} k_i k_j \oplus \sum_{i=0}^{15} \beta_{im} p_i \oplus \sum_{i=0}^{15} \beta_{im} k_i \oplus \gamma_m = 0,$$

где $m = 0, \ldots, 31$; $\alpha_{ijm}, \beta_{im}, \gamma_m \in \{0, 1\}$ определяются только структурой шифра и не зависят от выбранных значений p, c, k.

[1]Исследование выполнено при поддержке РФФИ (проект № 11-01-00997).

По сравнению с ранее предложенными в [1, 3, 4] атаками, наш подход отличается использованием двух различных пар открытых текстов/шифртекстов (p, c) и (p', c') при одном и том же ключе k, что позволяет получить систему из небольшого числа уравнений, а именно

$$\sum_{i,j=0}^{15} \alpha_{ijm}(p_i \oplus p'_i)(c_j \oplus c'_j) \oplus \sum_{i,j=0}^{15} \alpha_{ijm}(p_i \oplus p'_i)k_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm}k_i(c_j \oplus c'_j) \oplus \sum_{i=0}^{15} \beta_{im}(p_i \oplus p'_i) = 0, \quad (1)$$

$m = 0, \ldots, 31$, которая является линейной относительно неизвестных битов ключа. Система содержит 32 уравнения с 16 неизвестными.

Будем говорить, что вектор длины 16 обладает дефектом, если при разбиении его на четыре подвектора длины 4 хотя бы один из них является нулевым.

Теорема 1. Пусть ключ k случаен и фиксирован. Тогда верны предложения:

(i) При случайном равновероятном выборе открытых текстов p, p' система уравнений (1) непротиворечива с вероятностью 0,6074.

(ii) При фиксированном p', таком, что $p' \oplus k$ не имеет дефекта, и случайном равновероятном выборе открытого текста p система уравнений (1) непротиворечива с вероятностью 0,7725.

Однако непротиворечивость системы еще не означает существования единственного решения. Использование столь небольшого количества уравнений позволяет в конкретных случаях проанализировать фактическую эффективность алгебраической атаки. Например, для ключа $k = 1010111111001000$ и $p' = 0110010101010101$ найдено 44 747 (68,28 %) открытых текстов p, таких, что система (1) имеет единственное решение — ключ k.

Ранее анализ упрощенного варианта AES проводился в [3, 4]. В [3] для анализа слегка измененного S-AES используются соотношение (15) и соотношения, полученные с помощью таблицы истинности S-блоков. В общей сложности один раунд шифра описывается системой из 150 уравнений с 24 переменными. После преобразования системы к линейному виду она содержит 3600 уравнений с 2324 неизвестными. Для проанализированной в [3] пары открытого текста и шифртекста алгоритм выдаёт в качестве решения 4 ключа, любой из которых является подходящим для данной пары.

В [4] проведён анализ шифра, аналогичного S-AES, с S-блоками по 3 бита. Анализ заключается в переборе всех 4 194 304 возможных квадратичных уравнений относительно переменных S-блока, выборе тех из них, которые выполняются при всех значениях входных битов S-блока и битов выхода. Найдена система из 16 383 линейно зависимых уравнений. Из неё выбрана некоторая более удобная для анализа подсистема. После преобразования подсистемы к линейному виду получена система из 392 уравнений с 164 неизвестными. В [4] приводится её решение.

Система относительно двухраундового S-AES содержит 96 квадратичных уравнений с 32 неизвестными. Использование двух различных пар открытых текстов/шифртекстов сокращает количество мономов с 232 до 160, что позволяет более эффективно применять методы, разработанные для подобных систем.

ЛИТЕРАТУРА

1. *Courtois N. and Pieprzyk J.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // LNCS. 2002. V. 2501. P. 267–287.

2. *Mohammad M., Edward S., and Stephen W.* A simplified AES algorithm and its linear and differential cryptanalyses. // Cryptologia. 2003. No. 27. P. 148–177.

3. *Kleiman E.* The XL and XSL attacks on Baby Rijndael // Ms. Thesis. Iowa SU, USA, 2005.
4. *Бабенко Л. К., Маро Е. А.* Алгебраический анализ упрощенного алгоритма шифрования Rijndael // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». Таганрог: Изд-во ТТИ ЮФУ, 2009. №11 (100). С. 187–199.

УДК 512.62

ДИОФАНТОВОСТЬ ДИСКРЕТНОГО ЛОГАРИФМА

С. Ю. Ерофеев

Дискретный логарифм является важным математическим понятием в криптографии. Существует множество криптографических протоколов, основанных на трудности его нахождения. Достаточно упомянуть протокол разделения секретного ключа Диффи и Хеллмана, протоколы Масси — Омуры и Эль Гамаля. Многие протоколы аутентификации и цифровые подписи также имеют в основе дискретный логарифм.

Цель данной работы — дать представление дискретного логарифма в $\mathbb{Z}_p$ как диофантова множества, а также выписать явное представление соответствующего диофантова многочлена. Тогда проблема нахождения дискретного логарифма будет эквивалентна проблеме нахождения решения диофантова многочлена. Поскольку по знаменитой теореме Ю. В. Матиясевича (решение 10-й проблемы Гильберта) проблема существования решения произвольного диофантова уравнения алгоритмически неразрешима [1 – 3], указанная задача вычислительно трудна.

Определение 1. Множество $S \subseteq Z^n$ является диофантовым, если существует многочлен D с целыми коэффициентами, такой, что

$$\langle a_1, \ldots, a_n \rangle \in S \Longleftrightarrow \exists x_1, \ldots, x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}.$$

Определение 2. Функция $f : \mathbb{Z}^n \to \mathbb{Z}$ является диофантовой, если ее график $\Gamma_f = \{(f(b_1, \ldots, b_n), b_1, \ldots, b_n) : (b_1, \ldots, b_n) \in \operatorname{dom} f\}$ является диофантовым множеством.

Теорема 1. Пусть даны $i, p, n \in \mathbb{N}$, p простое. Тогда если следующая система уравнений имеет решение в натуральных числах в оставшихся аргументах, то $n^k \equiv i \pmod{p}$:

$$\begin{cases} x^2 - (a^2-1)y^2 = 1, \\ u^2 - (a^2-1)v^2 = 1, \\ s^2 - (b^2-1)t^2 = 1, \\ v^2 = ry^2, \\ b = 1 + 4yo = a + qu, \\ s = x + cu, \\ t = k + 4(d-1)y, \\ y = k + e - 1, \\ (x - y(a-n) - m)^2 = (f-1)^2(2an - n^2 - 1)^2, \\ m + g = 2an - n^2 - 1, \\ w = n + h = k + l, \\ a^2 - (w^2-1)(w-1)^2 z^2 = 1, \\ m = i + pj. \end{cases}$$