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 $n^k \equiv i \pmod{p}$:

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

Верно и обратное: если $n^{k'} \equiv i \pmod p$ для некоторого $k' \in \mathbb{N}$, то эта система уравнений имеет решение в натуральных числах, причем $k \equiv k' \pmod{p-1}$.

Следствие 1. Дискретный логарифм в $\mathbb{Z}_p$ является диофантовой функцией.

Заметим, что данное представление может быть основанием протоколов разделения ключа, аутентификации, цифровой подписи и т. п. Кроме того, оно может быть использовано с целью организации атаки на дискретный логарифм.

ЛИТЕРАТУРА

1. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Докл. АН СССР. 1970. Т. 191. № 2. С. 279–282.
2. *Матиясевич Ю. В.* Диофантово представление перечислимых предикатов // Изв. АН СССР. Сер. математ. 1971. № 35. С. 3–30.
3. *Davis M.* Hilbert's Tenth Problem is Unsolvable // Amer. Math. Monthly. 1973. V. 80. No. 3. P. 233–270.

УДК 512.54, 512.62, 519.7

ПОСТРОЕНИЕ ОДНОСТОРОННИХ ФУНКЦИЙ НА ОСНОВЕ НЕРАЗРЕШИМОСТИ ПРОБЛЕМЫ ЭНДОМОРФНОЙ СВОДИМОСТИ В ГРУППАХ

С. Ю. Ерофеев, В. А. Романьков

Односторонние функции — неотъемлемая часть криптографических схем и протоколов. Теоретически их существование до сих пор не установлено. В работах Л. А. Левина [1, 2] представлена универсальная функция, являющаяся односторонней, если существует хотя бы одна односторонняя функция.

Предлагается схема построения односторонней функции в группе с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости, а также протокол аутентификации на ее основе.

Говорят, что в эффективно заданной группе G разрешима проблема эндоморфной сводимости, если существует алгоритм, определяющий по любой паре элементов $g, f \in G$, является ли f эндоморфным образом элемента g.

Существование группы G с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости установлено в работах В. А. Романькова [3, 4]. А именно доказано, что указанным свойством обладают свободные метабелевы группы M_n достаточно большого ранга n и свободные нильпотентные группы N_{rc} достаточно большого ранга r и ступени нильпотентности $c \geqslant 9$.

В общих чертах схема выглядит следующим образом. В группе G выбирается элемент g, эндоморфные значения которого в фиксированной циклической подгруппе $\langle f \rangle$ кодируются наборами целых чисел $\alpha \in \mathbb{Z}^m$. Это позволяет определить функцию $\varphi : \mathbb{Z}^m \to \mathbb{Z}$. Свойства группы G позволяют рассматривать φ как одностороннюю. Для аутентификации фиксируется открытое значение $g \in M_n$ и публикуется значение $\varphi(g)$ для секретного $\varphi \in \operatorname{End} G$, $\varphi \leftrightarrow \alpha \in \mathbb{Z}^m$. Сессионная аутентификация заключается в выборе $\psi \in \operatorname{End} G$ и публикации $h = \psi(\varphi(g))$. При ответе «0» объявляется ψ и проверяется равенство для $\varphi(g)$. При ответе «1» объявляется $\varphi \circ \psi$ и проверяется равенство для g.

Однако в указанной схеме, предложенной в работе Д. Григорьева и В. Шпильрайна [5] и основанной на идее В. А. Романькова, имеется существенная слабость.