С. Ю. Ерофеев, В. А. Романьков, Построение односторонних функций на основе неразрешимости проблемы эндоморфной сводимости в группах, *ПДМ*, 2011,приложение к № 4, 32–33

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.

Для ее надежности требуется неразрешимость проблемы эндоморфизма для образов, в частности для $\varphi(G)$.

Основным результатом настоящей работы является следующая теорема.

Теорема 1. В свободной метабелевой группе M_n достаточно большого ранга неразрешима проблема двукратной эндоморфной сводимости.

Теорема позволяет ликвидировать указанную слабость протокола аутентификации.

ЛИТЕРАТУРА

1. *Levin L. A.* One-way Functions and Pseudorandom Generators // Combinatorica. 1987. V. 7. No. 4. P. 357–363.
2. *Левин Л. А.* Односторонние функции // Проблемы передачи информации. 2003. Т. 39. № 1. С. 103–117.
3. *Романьков В. А.* Об уравнениях в свободных метабелевых группах // Сибирский математический журнал. 1979. Т. 20. № 3. С. 671–673.
4. *Романьков В. А.* О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика. 1977. Т. 16. № 4. С. 457–471.
5. *Grigoriev D. and Shpilrain V.* Zero-knowledge authentication schemes from actions on graphs, groups, or rings // Ann. Pure Appl. Logic. 2010. No. 162. P. 194–200.

УДК 004.056.55

РЕАЛИЗАЦИЯ НА ПЛИС ШИФРА FAPKC[1]

Д. С. Ковалев, В. Н. Тренькаев

Существует немного асимметричных шифров (RSA, El-Gamal, ECC), которые используются на практике. Основным их недостатком является низкое быстродействие. При этом потребность в быстродействующих шифрах с небольшой длиной ключа остается. В частности, это актуально для устройств с ограниченными ресурсами. В работе исследуется автоматный ассиметричный шифр FAPKC (Finite Automata Public Key Cryptosystem) [1 – 3] на пригодность к практическому использованию.

В шифре FAPKC используются обратимые с задержкой автоматы, т. е. автоматы, у которых входное слово восстанавливается по выходному с задержкой на несколько тактов работы, а также автоматы с конечной памятью, значение выходного символа для которых зависит от значений конечного количества входных и выходных символов в предыдущие такты работы. Закрытый ключ состоит из двух обратимых автоматов A и B (нелинейного с задержкой 0 и линейного с задержкой τ соответственно), обратные к которым могут быть построены с полиномиальной сложностью. Открытый ключ есть последовательная композиция автоматов A и B при известном начальном состоянии. При этом по выбранному состоянию композиции вычисляются начальные состояния A и B. При шифровании к открытому тексту добавляются произвольные τ символов. Шифртекст есть реакция автомата открытого ключа в выбранном начальном состоянии на «расширенное» входное слово. Таким образом, длина шифртекста увеличивается на τ символов по сравнению с открытым текстом. При расшифровании сначала находится реакция β автомата, обратного к B, в его начальном состоянии

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).