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).

на зашифрованное слово. Исходный открытый текст получается как реакция автомата, обратного к A, в его начальном состоянии на входное слово β. Стойкость FAPKC основана на сложности решения задачи декомпозиции нелинейного обратимого с задержкой автомата с конечной памятью.

Цель данной работы — изучение вопросов эффективности аппаратной реализации шифра FAPKC на базе программируемых логических интегральных схем (ПЛИС). Проведены исследования по выявлению зависимости количества используемых ресурсов и производительности ПЛИС от параметров шифрсистемы (длины ключа, размерности линейного пространства, задержки шифрующего автомата, стойкости к различным атакам), а также сравнение ПЛИС-реализаций шифров FAPKC и RSA.

В частности, в САПР Xilinx WebPack ISE реализован оценочный вариант шифра FAPKC на ПЛИС Spartan-3 XC3S1500, для которого выявлена зависимость ресурсоемкости и быстродействия от задержки, величина которой изменялась от 32 до 160. Оказалось, что увеличение задержки, а следовательно, длины ключа существенно влияет (в сторону увеличения) только на число используемых ресурсов ПЛИС, в то время как максимальная рабочая частота ПЛИС убывает незначительно. Проведено сравнение шифра RSA-1024 [4] с вариантом FAPKC той же стойкости, результатом которого является утверждение о том, что использование шифра FAPKC предпочтительней как с точки зрения производительности, так и с точки зрения числа используемых ресурсов. При этом коэффициент эффективности ПЛИС-реализации FAPKC (отношение производительности к количеству используемых ресурсов) на порядок лучше этого показателя для RSA. В целом, проведённые исследования показывают, что шифр FAPKC, реализованный на ПЛИС, пригоден для использования на практике и по сравнению с RSA имеет существенно более высокое быстродействие и меньшую ресурсоемкость.

ЛИТЕРАТУРА

1. *Bao F. and Igarashi Y.* Break Finite Automata Public Key Cryptosystem // LNCS. 1995. No. 944. P. 147–158.
2. *Dai Z. D., Ye D. F., and Lam K. Y.* Weak Invertibility of Finite Automata and Cryptanalysis on FAPKC // LNCS. 1998. No. 1514. P. 227–241.
3. *Tao R. J.* Finite Automata and Application to Cryptography. Tsinghua University Press and Springer, 2008.
4. *Wollinger T., Guajardo J., and Paar C.* Cryptography on FPGAs: State of the art implementations and attacks // ACM Trans. Embedded Computing Systems. 2004. V. 3. Iss. 3. P. 534–574.

УДК 003.26

БЕЗОПАСНОСТЬ РЕЖИМОВ ШИФРОВАНИЯ ГОСТ 28147-89

И. А. Кукало

Отечественный алгоритм криптографического преобразования ГОСТ 28147-89 является единственным алгоритмом симметричного шифрования, разрешенным к использованию на территории РФ. Стандарт ГОСТ 28147-89 определяет алгоритм шифрования $E : K \times \{0,1\}^{64} \to \{0,1\}^{64}$, три режима симметричного шифрования $SE = (k, \varepsilon, D)$ с соответствующими уравнениями шифрования ε и расшифрования D, а также режим выработки имитовставки. С момента опубликования и перевода стандарта на английский язык в отечественной и зарубежной литературе появилось боль-