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-

шое количество работ, посвященных анализу криптостойкости *алгоритма* шифрования ГОСТ 28147-89. Однако оценка криптостойкости *режимов* шифрования, определенных в стандарте, до настоящего времени не проводилась, хотя, согласно [1], данная задача является актуальной для современной криптографии.

Согласно [2], основным показателем криптостойкости режимов шифрования является возможность адаптивной атаки по выбранным открытым текстам (IND-CPA). Данный показатель ориентирован на практическую оценку безопасности режима шифрования [3] против злоумышленника с ограниченными ресурсами.

Пусть $SE = (k, \varepsilon, D)$ — произвольный режим шифрования [2] и A — злоумышленник, который передает специальной подпрограмме-оракулу (ППО) множество пар сообщений $(M_{0,1}, M_{1,1}), \ldots, (M_{0,q}, M_{1,q})$ одинаковой длины. ППО возвращает злоумышленнику набор шифртекстов $C_1, \ldots, C_q$ в соответствии с экспериментами:

— для $\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}$ элемент C_i является шифртекстом сообщения $M_{1,i}$, $1 \leqslant i \leqslant q$;
— для $\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}$ элемент C_i является шифртекстом сообщения $M_{0,i}$, $1 \leqslant i \leqslant q$.

Определение 1. Определим возможность адаптивной атаки по выбранным открытым текстам как

$$\mathrm{Adv}_{SE}^{\text{ind-cpa}}(A) = \Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}(A) = 1] - \Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}(A) = 1],$$

где $\Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}(A) = 1]$ — вероятность события, при котором злоумышленник A считает, что ППО зашифровал сообщения $M_{1,i}$ для эксперимента $\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}(A)$; $\Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}(A) = 1]$ — вероятность события, при котором злоумышленник A считает, что ППО зашифровал сообщения $M_{1,i}$ для эксперимента $\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}(A)$.

Режим шифрования является безопасным при $\mathrm{Adv}_{SE}^{\text{ind-cpa}}(A) \to 0$. Определены значения $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$ для всех режимов работы ГОСТ 28147-89, обеспечивающих конфиденциальность обрабатываемой информации. Модель злоумышленника A определяется количеством σ запросов к ППО. Безопасность алгоритма шифрования определяется показателем псевдослучайности функции шифрования $\mathrm{Adv}_{E}^{\text{prf}}(B)$ [2]. Теоретические результаты приведены в табл. 1.

Таблица 1

Теоретические характеристики криптостойкости отечественных режимов шифрования

Название режима шифрования	Теоретическое значение $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$
Простой замены	1
Гаммирования	$\mathrm{Adv}_{\text{GOST}}^{\text{prf}}(B) + 2\sigma^2/2^{64}$
Гаммирования с обратной связью	$\mathrm{Adv}_{\text{GOST}}^{\text{prf}}(B) + \sigma^2/2^{64}$

Практические значения $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$ приведены в табл. 2 и рассчитываются при допущении, что наилучшей атакой на алгоритм шифрования в ГОСТ является атака, основанная на парадоксе дней рождения [1].

Значение σ соответствует количеству блоков данных, зашифрованных ППО, и позволяет определить продолжительность сессии защищенного обмена данными в системах криптографической защиты информации. Таким образом,

— для режима простой замены безопасным является шифрование данных размером в один блок, т. е. 64 бита, или 8 байт;

— для режима гаммирования безопасным является шифрование данных размером 2^{31} блоков, т. е. 16 Гбайт;
— для режима гаммирования с обратной связью безопасным является шифрование данных размером $\sqrt{2^{64}/3}$ блоков, т. е. $\approx 18{,}475$ Гбайт.

Таблица 2

Практические характеристики криптостойкости отечественных режимов шифрования

Название режима шифрования	Практическое значение $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$	Значение σ, обеспечивающее криптостойкость
Простой замены	1	1
Гаммирования	$\leqslant 4\sigma^2/2^{64}$	$\leqslant 2^{31}$
Гаммирования с обратной связью	$\leqslant 3\sigma^2/2^{64}$	$\leqslant \sqrt{2^{64}/3}$

ЛИТЕРАТУРА

1. *Bellare M. and Rogaway P.* Introduction to Modern Cryptography. 2005. `http://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf`
2. *Goldwasser S. and Bellare M.* Lecture Notes on Cryptography. 2001. `http://cseweb.ucsd.edu/~mihir/papers/gb.pdf`
3. *Katz J. and Yehuda L.* Introduction to Modern Cryptography. Boca Raton: Chapman& Hall/CRC, 2008.

УДК 519.7

О ВЫБОРЕ СЛАЙДОВЫХ ПАР В КОРРЕЛЯЦИОННОМ МЕТОДЕ КРИПТОАНАЛИЗА ШИФРА KeeLoq

О. Н. Лебедева

KeeLoq — блочный шифр, широко используемый в системах бесключевого удалённого доступа. Шифр был разработан профессором Г. Каном и запатентован Южно-Африканской компанией «Nanoteq» в середине 80-х. В 1995 г. фирма «MICROCHIP» приобрела KeeLoq у фирмы «Nanoteq» вместе с лицензионными правами.

Алгоритм KeeLoq [1] имеет 64-битный ключ и осуществляет шифрование 32-битных блоков открытого текста. В нём используются два регистра сдвига: один — длины 64 без функции обратной связи (для выработки подключа), другой — регистр сдвига длины 32 с нелинейной функцией обратной связи NLF от пяти переменных (непосредственно для шифрования). Блок открытого текста помещается в текстовый регистр. Шифртекстом является состояние регистра после 528 циклов с использованием регистра ключа. Пусть $V_n = \mathrm{GF}_2^n$ — множество всех n-битных слов; $Y^{(i)} = (y_{31}^{(i)}, \ldots, y_0^{(i)}) \in \in V_{32}$ и $K^{(i)} = (k_{63}^{(i)}, \ldots, y_0^{(i)}) \in V_{63}$ — соответственно состояния текстового регистра и регистра ключа после i тактов. Каждый цикл шифрования может быть описан следующим образом:

— вычисление очередного бита: $\varphi = NLF(y_{31}^{(i)}, y_{26}^{(i)}, y_{20}^{(i)}, y_9^{(i)}, y_1^{(i)}) \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus k_0^{(i)}$;
— сдвиг состояния текстового регистра: $R^{(i+1)} = (\varphi, y_{31}^{(i)}, \ldots, y_1^{(i)})$;
— сдвиг состояния регистра ключа: $K^{(i+1)} = (k_0^{(i)}, k_{63}^{(i)}, \ldots, k_1^{(i)})$.

Первый криптоанализ KeeLoq был опубликован только в феврале 2007 г. А. Богдановым [1]. Эта атака основана на слайдовой технике и линейном приближении нелинейной булевой функции, использующейся в KeeLoq. Криптоанализ имеет временную