ЛИТЕРАТУРА

1. *Wolfram S.* A New Kind of Science. Wolfram Media, 2002. 1192 p.
2. *Seredinski F., Bouvry P., and Zomaya A. Y.* Cellular automata computations and secret key cryptography // Parallel Computing. 2004. V. 30. P. 753–766.
3. *Tomassini M. and Perrenoud M.* Nonuniform cellular automata for cryptography // Complex Systems. 2000. No. 12. P. 71–81.
4. *Nandi S., Kar B., and Chaudhuri P.* Theory and applications of cellular automata in cryptography // IEEE Trans. Comput. 1994. V. 43. No. 12. P. 1346–1357.
5. *Blackburn S. R., Murphy S., and Paterson K. G.* Comments on "Theory and Applications of Cellular Automata in Cryptography" // IEEE Trans. Comput. 1997. V. 46. No. 5. P. 637–638.
6. *Guan S. U. and Tan S. K.* Pseudorandom number generation with self-programmable cellular automata // IEEE Trans. Computer Aided Design of Integrated Circuits and Systems. 2004. V. 23. No. 7. P. 1095–1101.
7. *Ефремова А. А., Гамова А. Н.* Генератор псевдослучайных чисел на основе клеточных автоматов // Материалы Междунар. науч. конф. «Компьютерные науки и информационные технологии». Саратов: СГУ, 2016. С. 131–134.
8. *Marsaglia G.* Diehard: A Battery of Tests of Randomness. 1995. `http://stat.fsu.edu/pub/diehard/`

УДК 517.19 DOI 10.17223/2226308X/10/33

ПОСТРОЕНИЕ $(4, 8)$-СХЕМЫ ВИЗУАЛЬНОЙ КРИПТОГРАФИИ НА ОСНОВЕ КЛАССА ЛИНЕЙНЫХ ХЭШ-ФУНКЦИЙ

Н. А. Зорина, Ю. В. Косолапов

С использованием визуальной криптографии строится $(4, 8)$-схема разделения секрета, представляющего собой чёрно-белое изображение. Для её построения применяется $(4, 4)$-схема визуальной криптографии и класс линейных хэш-функций. Показано, что использование этого класса позволяет построить стойкую схему с приемлемой относительной контрастностью восстанавливаемого секретного чёрно-белого изображения.

Ключевые слова: *визуальная криптография, линейные хэш-функции.*

В [1] М. Наором и А. Шамиром предложена (k, n)-схема разделения секрета, представляющего собой чёрно-белое изображение. В основе этой схемы лежит построение на основе исходного изображения n таких чёрно-белых («теневых») изображений, что при совмещении любых k из них (и более) можно восстановить исходное секретное изображение. При этом «совмещение» теневых изображений следует представлять как наложение этих изображений, нанесённых на прозрачную пленку, а «восстановление» — просмотр совмещённых теневых изображений на свет. Свою схему М. Наор и А. Шамир назвали схемой визуальной криптографии. В [1] сначала строятся (k, k)-схемы, а затем на их основе — (k, n)-схема $(n > k)$, в частности, с использованием k-универсальных хэш-функций. В настоящей работе ставится задача построения $(4, 8)$-схемы на основе класса линейных хэш-функций [2].

Для построения схемы возьмём $(4,4)$-схему визуальной криптографии из [1]. Рассмотрим матрицы

$$S^0 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \; S^1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

и соответствующие им коллекции матриц $\mathcal{C}_0$ и $\mathcal{C}_1$, $\mathcal{C}_i = \{\gamma(S^i) : \gamma \in \mathcal{S}_8\}$, $i = 0, 1$, где $\mathcal{S}_8$ — симметрическая группа подстановок; $\gamma(S^i)$ — перестановка столбцов матрицы S^i в соответствии с перестановкой γ. Для построения четырёх теневых изображений секретное чёрно-белое изображение представляется в виде последовательности нулей (белый пиксель изображения) и единиц (чёрный пиксель). Теневые изображения формируются следующим образом: для очередного пикселя (бита) $b \in \{0, 1\}$ секретного изображения случайным образом выбирается матрица $\hat{S}^b$ из коллекции $\mathcal{C}_b$ и в j-е теневое изображение записывается j-я строка матрицы $\hat{S}^b$, $j \in \{1, 2, 3, 4\}$. Таким образом, один бит секретного изображения кодируется восемью битами теневого изображения (размер каждого теневого изображения в 8 раз больше секретного изображения). Как следует из [1], четыре теневых изображения позволяют восстановить секретное изображение, так как в коллекции $\mathcal{C}_0$ все матрицы имеют один нулевой столбец, в то время как в коллекции $\mathcal{C}_1$ таких матриц нет. Относительная контрастность секретного изображения, получаемого при совмещении теневых изображений, пропорциональна доле α нулевых столбцов в матрице S^0: $\alpha = 1/8$. Стойкость этой $(4,4)$-схемы характеризуется тем, что совмещение трёх и менее теневых изображений не даёт какой-либо информации о секретном изображении (кроме его размера), так как удаление из матриц S^0 и S^1 любых l ($l \in \{1, 2, 3\}$) строк даёт матрицы S^0_l и S^1_l, одинаковые с точностью до перестановки столбцов:

$$\{\gamma(S^0_l) : \gamma \in \mathcal{S}_8\} = \{\gamma(S^1_l) : \gamma \in \mathcal{S}_8\}.$$

Для построения $(4,8)$-схемы воспользуемся правилом построения из [1] на основе хэш-функций. Однако вместо класса k-универсальных хэш-функций применим класс линейных хэш-функций. Рассмотрим множество $\mathcal{H}$ всех $(0,1)$-матриц размера 3×2, $|\mathcal{H}| = 2^6 = 64$. Для $H \in \mathcal{H}$ определим функцию

$$f_H : \{0,1\}^3 \to \{0,1\}^2, \tag{1}$$

действующую на элемент $\mathbf{x} \in \{0,1\}^3$ по правилу $f_H(\mathbf{x}) = H \cdot \mathbf{x}^{\mathrm{T}}$, где $\mathbf{x}^{\mathrm{T}}$ — транспонирование $\mathbf{x}$. Класс функций

$$\mathcal{F}_{\mathcal{H}} = \{f_H : H \in \mathcal{H}\}$$

является 2-универсальным классом линейных хэш-функций [2]. Пусть $b_l : \{0,1\}^l \to \to \{1, \ldots, 2^l\}$ — функция, ставящая однозначно в соответствие вектору из $\{0,1\}^l$ число из множества $\{1, \ldots, 2^l\}$, $b_l^{-1} : \{1, \ldots, 2^l\} \to \{0,1\}^l$ — обратная к b_l функция; рассмотрим также функцию $h : \{1, \ldots, 64\} \to \mathcal{H}$, однозначно сопоставляющую десятичным числам из множества $\{1, \ldots, 64\}$ матрицы из $\mathcal{H}$.

Для построения $(4,8)$-схемы необходимо построить коллекции матриц $\hat{\mathcal{C}}_0$ и $\hat{\mathcal{C}}_1$, с помощью строк которых будут кодироваться белые пиксели (нулевые биты) и черные пиксели (единичные биты) соответственно. Представляется удобным описать формирование матрицы $\hat{S}^b \in \hat{\mathcal{C}}_b$ для кодирования бита b, а не вводить громоздкое определение коллекции $\hat{\mathcal{C}}_b$. Для построения матрицы $\hat{S}^b$ случайным образом выбираются (возможно, с повторениями) 64 матрицы $T^b_1, \ldots, T^b_{64}$ из коллекции $\mathcal{C}_b$, построенной для $(4,4)$-

схемы. Тогда элемент i-й строки ($1 \leqslant i \leqslant 8$) и $(j \cdot l)$-го столбца ($1 \leqslant j \leqslant 8$, $1 \leqslant l \leqslant 64$) матрицы $\hat{S}^b$ формируется следующим образом:

$$\hat{S}^b[i, j \cdot l] = T_l^b[b_2(f_{h(l)}(b_3^{-1}(i))), j], \tag{2}$$

где $f_{h(l)}$ — функция вида (1). Отметим, что построенная таким образом матрица $\hat{S}^b$ имеет 8 строк и 512 столбцов. Правило (2) предложено в [1], за исключением того, что в [1] используемый класс $\mathcal{F}$ хэш-функций должен быть применительно к $(4, 8)$-схеме 4-универсальным, а именно: для всех подмножеств $B \subset \{1, \ldots, 8\}$, $|B| = 4$, и всех q, $1 \leqslant$ $\leqslant q \leqslant 4$, вероятность того, что случайно выбранная функция $f \in \mathcal{F}$ имеет q различных значений на множестве B, одна и та же. В настоящей работе доказано утверждение, из которого следует, что класс функций вида (1) не является 4-универсальным классом.

Утверждение 1. Пусть $\mathcal{B}$ — множество двоичных (4×3)-матриц, состоящих из попарно различных строк; $C(B, H)$ — число различных значений, которые функция $f_H \in \mathcal{F}_\mathcal{H}$ принимает на множестве строк матрицы $B \in \mathcal{B}$,

$$\mathcal{C}_B(l) = |\{H \in \mathcal{H} : C(B, H) = l\}|, \;\; l = 1, \ldots, 4.$$

Тогда $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$, $|\mathcal{B}_1| = 56$, $|\mathcal{B}_2| = |\mathcal{B}_3| = 7$, причём $\mathcal{B}_i \cap \mathcal{B}_j = \varnothing$ для всех $i \neq j$ и

1) $\mathcal{C}_B(1) = 1$, $\mathcal{C}_B(2) = 21$, $\mathcal{C}_B(3) = 36$, $\mathcal{C}_B(4) = 6$ для всех $B \in \mathcal{B}_1$;
2) $\mathcal{C}_B(1) = 4$, $\mathcal{C}_B(2) = 36$, $\mathcal{C}_B(3) = 0$, $\mathcal{C}_B(4) = 24$ для всех $B \in \mathcal{B}_2$;
3) $\mathcal{C}_B(1) = 4$, $\mathcal{C}_B(2) = 36$, $\mathcal{C}_B(3) = 0$, $\mathcal{C}_B(4) = 24$ для всех $B \in \mathcal{B}_3$.

Утверждение 2. Пусть $(4, 8)$-схема визуальной криптографии построена с применением класса линейных хэш-функций по правилу (2) на основе $(4, 4)$-схемы. Тогда построенная $(4, 8)$-схема характеризуется относительной контрастностью, пропорциональной числу $\hat{\alpha} = 0{,}01875$.

Отметим, что стойкость $(4, 8)$-схемы следует из стойкости $(4, 4)$-схемы [1].

Полученные результаты показывают, что возможно построение схем визуальной криптографии на основе 2-универсальных классов хэш-функций, при этом обеспечивается приемлемая для схем визуальной криптографии относительная контрастность восстанавливаемых изображений [3]. Недостатком предложенной схемы является большое увеличение размеров теневых изображений. В частности, размер каждого теневого изображения увеличивается в 512 раз. Представляется, что сокращения размера теневых изображений можно добиться путем использования не всего класса $\mathcal{F}_\mathcal{H}$, а случайно выбранного подмножества из этого класса.

ЛИТЕРАТУРА

1. *Naor M. and Shamir A.* Visual cryptography // LNCS. 1994. V. 950. P. 1–12.
2. *Carter J. L. and Wegman M. N.* Universal classes of hash functions // J. Computer System Sciences. 1979. V. 18. P. 143–154.
3. *Lakshmanan R. and Arumugam S.* Construction of a (k, n)-visual cryptography scheme // Designs, Codes and Cryptography. 2017. V. 82. No. 3. P. 629–645.