ИНФОРМАТИКА

УДК 517.9

О ПОСТРОЕНИИ (n, k)-СХЕМЫ ВИЗУАЛЬНОЙ КРИПТОГРАФИИ С ПРИМЕНЕНИЕМ КЛАССА ЛИНЕЙНЫХ ХЭШ-ФУНКЦИЙ НАД БИНАРНЫМ ПОЛЕМ

Ю. В. Косолапов

Косолапов Юрий Владимирович, кандидат технических наук, доцент кафедры алгебры и дискретной математики, Южный федеральный университет, Россия, 344006, Ростов-на-Дону, Большая Садовая, 105/42, itaim@mail.ru

В статье исследуется вопрос построения (n, k)-схемы визуальной криптографии, в которой черно-белое секретное изображение распределяется среди n участников и только коалиции мощности k и более участников могут восстановить секретное изображение. Именно исследуется вопрос применения набора $\mathscr{F}$ хэш-функций для построения (n, k)-схемы на основе (k, k)-схемы визуальной криптографии М. Наора и А. Шамира. Получены условия на $\mathscr{F}$, при выполнении которых возможно построение (n, k)-схемы. В работе, в частности, исследуется применение класса линейных хэш-функций, который в общем случае не позволяет построить (n, k)-схему, однако с помощью него возможно построение (n, K, k)-схемы, для которой любые $k-1$ и менее участников восстановить секрет не могут, а любые K и более могут. Для класса линейных хэш-функций получены достаточные условия на K, при выполнении которых коалиция мощности K и более может восстановить секрет. В частном случае исследована схема разделения секрета среди восьми участников, построенная на основе $(4, 4)$-схемы Наора – Шамира с применением класса линейных хэш-функций. Показано, что такая схема является $(8, 4)$-схемой и характеризуется меньшей длиной долей секретов и большей контрастностью, чем $(8, 4)$-схема, построенная с помощью класса хэш-функций, предложенного М. Наором и А. Шамиром.

Ключевые слова: визуальная криптография, линейные хэш-функции.

DOI: 10.18500/1816-9791-2018-18-2-227-239

НАУЧНЫЙ ОТДЕЛ

ВВЕДЕНИЕ И ПОСТАНОВКА ЗАДАЧИ

В [1,2] предложена схема разделения секрета (СРС), в которой некоторый секрет $\mathbf{s}$ разделяется среди конечного множества участников $\underline{n} = \{0, \ldots, n-1\}$, занумерованных числами от 0 до $n-1$, и только подмножество участников с мощностью не менее определенного заранее числа k может восстановить исходный секрет.

Схемы разделения секрета, в которых любые k и более участников образуют *правомочную коалицию*, то есть могут восстановить секрет, а меньшее число участников секрет восстановить не может, называются *пороговыми* (n,k)-схемами [3]. В настоящее время СРС применяются как самостоятельно, так и в качестве примитива при синтезе других криптографических протоколов, например, протоколов многосторонних конфиденциальных вычислений [4]. Здесь и далее под СРС будем понимать следующую схему. Пусть секретом является вектор $\mathbf{s} = (s_1, \ldots, s_M)$ длины $M(\geqslant 1)$ из множества $\{0,1\}^M$ $(M \geqslant 1)$, $\underline{n}$ — упорядоченное множество из n участников, среди которых *дилер* разделяет секрет. Для l-го бита $s_l = b(\in \{0,1\})$ секрета $\mathbf{s}$ независимо от других битов этого секрета дилером применяется *протокол разделения одного бита*. Именно для бита b протокол разделения бита состоит в нахождении дилером для каждого $i \in \underline{n}$ значения соответствующего (несекретного) отображения

$$f_i : \{0,1\} \times \mathscr{R} \to \{0,1\}^m, \tag{1}$$

где $\mathscr{R}$ — подходящее для конкретной СРС множество, значения из которого принимает случайный аргумент, $m \in \mathbb{N}$, $m > 1$. Таким образом, по биту $s_l = b$ формируется набор из n *долей*, который представим в виде набора n векторов, каждый из которых принадлежит $\{0,1\}^m$:

$$s_l \to (\mathbf{s}_0^l, \mathbf{s}_1^l, \ldots, \mathbf{s}_{n-1}^l), \qquad \mathbf{s}_i^l = f_i(s_l, r_l), i = 0, \ldots, n-1, \tag{2}$$

где r_l — значение случайного аргумента, выбранное дилером из $\mathscr{R}$ случайно и равновероятно для l-го бита. Для секрета $\mathbf{s} = (s_1, \ldots, s_M)$ *протокол разделения секрета* состоит в нахождении для каждого участника $i \in \underline{n}$ соответствующей доли $\mathbf{s}_i$ длины $M \cdot m$ и вида $\mathbf{s}_i = \mathbf{s}_i^1 \parallel \ldots \parallel \mathbf{s}_i^M$, где $\mathbf{a} \parallel \mathbf{b}$ — конкатенация векторов $\mathbf{a}$ и $\mathbf{b}$.

Пусть $\underline{n}(K) = \{i_1, \ldots, i_K\}$ — подмножество участников мощности K, $\underline{n}(K) \subseteq \underline{n}$, а $S_K = [\mathbf{s}_{i_1}, \ldots, \mathbf{s}_{i_K}]$ — набор долей секрета $\mathbf{s}$. Символом $g^{\underline{n}(K)}$ обозначим такое отображение вида

$$g^{\underline{n}(K)} : \underbrace{\{0,1\}^m \times \ldots \times \{0,1\}^m}_{K} \to \{0,1\}, \tag{3}$$

что $g^{\underline{n}(K)}(\mathbf{s}_{i_1}^l, \ldots, \mathbf{s}_{i_K}^l) = s_l$ для $K \geqslant k$, а при $K < k$ вероятность события $g^{\underline{n}(K)}(\mathbf{s}_{i_1}^l, \ldots, \mathbf{s}_{i_K}^l) = 1$ равна $1/2$. Другими словами, отображение $g^{\underline{n}(K)}$ однозначно восстанавливает каждый бит секрета $\mathbf{s}$ при $K \geqslant k$, а при $K < k$ вероятность восстановления каждого бита равна вероятности угадывания значения соответствующего бита. *Протокол восстановления l-го бита* коалицией $\underline{n}(K)$ состоит в нахождении значения $g^{\underline{n}(K)}(\mathbf{s}_{i_1}^l, \ldots, \mathbf{s}_{i_K}^l)$, а *протокол восстановления секрета* коалицией $\underline{n}(K)$ по совокупности долей S_K состоит в нахождении вектора вида

$$g^{\underline{n}(K)}(\mathbf{s}_{i_1}^1, \ldots, \mathbf{s}_{i_K}^1) \parallel g^{\underline{n}(K)}(\mathbf{s}_{i_1}^2, \ldots, \mathbf{s}_{i_K}^2) \parallel \ldots \parallel g^{\underline{n}(K)}(\mathbf{s}_{i_1}^M, \ldots, \mathbf{s}_{i_K}^M).$$

Отметим, что любое черно-белое изображение может быть представлено в виде вектора из нулей и единиц, где «0» соответствует, например, белому пикселю изображения, а «1» — черному. В [5] М. Наором (Naor) и А. Шамиром (Shamir) предложена (n,k)-схема разделения секрета, представляющего собой черно-белое изображение. В основе этой схемы лежит построение на основе исходного изображения n таких черно-белых изображений («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, нанесенных на прозрачную пленку, а «восстановление» —

как просмотр совмещенных теневых изображений на свет. Свою схему М. Наор и А. Шамир назвали схемой визуальной криптографии, так как при совмещении k и более «теневых» изображений имеется возможность визуально отличить области, соответствующие черным пикселям, от областей, соответствующих белым пикселям. Другими словами, имеется ненулевая относительная контрастность (различие) между черными и белыми областями. Заметим, что порог контрастной чувствительности глаза человека составляет порядка 0.01 [6], поэтому представляют интерес (n,k)-схемы с относительной контрастностью не менее 0.01. В [5] сначала строятся (k,k)-схемы, а затем на основе этих схем строится (n,k)-схема ($n>k$), в частности, с использованием k-универсальных хэш-функций.

В настоящей работе ставится задача исследования (n,k)-схемы, построенной на основе класса линейных хэш-функций [7], который, с одной стороны, не является k-универсальным классом хэш-функций при $k>2$, а с другой стороны, для рассматриваемой (n,k)-схемы содержит меньше функций, чем класс, предложенный в [5], что позволяет уменьшить размеры (длины) долей участников.

Работа имеет следующую структуру. В парагр. 1 приводятся необходимые сведения о схемах визуальной криптографии из [5] и предварительные результаты относительно применения хэш-функций для построения (n,k)-схем. В парагр. 2 исследуется схема визуальной криптографии на основе класса линейных хэш-функций и доказывается утверждение о контрастности восстанавливаемого секретного изображения. Там же приводятся результаты анализа $(8,4)$-схемы. Доказательство основного результата для $(8,4)$-схемы вынесено в приложение.

1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ И РЕЗУЛЬТАТЫ

Пусть $\mathbf{s}=(s_1,\ldots,s_M)(\in\{0,1\}^M$ — секрет, соответствующий черно-белому изображению. Опишем протокол восстановления l-го бита s_l секрета $\mathbf{s}$ в соответствии с [5]. Секретному биту s_l соответствует набор долей секретов (2). Для двух векторов $\mathbf{a}=(a_1,\ldots,a_m)(\in\{0,1\}^m)$ и $\mathbf{b}=(b_1,\ldots,b_m)(\in\{0,1\}^m)$ определим операцию $\vee$ покоординатного логического «или»: $\mathbf{a}\vee\mathbf{b}=(a_1\vee b_1,\ldots,a_m\vee b_m)$, где операция «$a\vee b$» — это логическое «или» двоичных величин a и b. Для восстановления значения бита $s_l=b$ коалицией участников $\underline{n}(K)=\{i_1,\ldots,i_K\}$ необходимо найти вектор

$$\mathbf{p}_l^{s_l}=\mathbf{s}_{i_1}^l\vee\mathbf{s}_{i_2}^l\vee\ldots\vee\mathbf{s}_{i_K}^l \tag{4}$$

и вычислить для этого вектора вес Хэмминга $w(\mathbf{p}_l^{s_l})$ — количество ненулевых координат вектора. Согласно [5] при $K\geqslant k$ отображение (3) должно иметь вид

$$g^{\underline{n}(K)}(\mathbf{s}_{i_1}^l,\mathbf{s}_{i_2}^l,\ldots,\mathbf{s}_{i_K}^l)=\begin{cases}1, & \text{если } w(\mathbf{p}_l^{s_l})\geqslant d(\underline{n}(K)),\\ 0, & \text{если } w(\mathbf{p}_l^{s_l})\leqslant d(\underline{n}(K))-\alpha(\underline{n}(K))\cdot m,\end{cases}$$

где $d(\underline{n}(K))(\leqslant m)$ — пороговое значение для веса Хэмминга, при котором вектор $\mathbf{p}_l^{s_l}$ соответствует биту $s_l=1$, а величина $\alpha(\underline{n}(K))(0<\alpha(\underline{n}(K))<1)$ характеризует *относительную контрастность* между вектором вида (4), соответствующим $s_l=1$, и вектором того же вида, соответствующим $s_l=0$:

$$\alpha(\underline{n}(K))=\frac{w(\mathbf{p}_l^1)-w(\mathbf{p}_l^0)}{m}. \tag{5}$$

Заметим, что пороговое значение $d(\underline{n}(K))$ и относительная контрастность $\alpha(\underline{n}(K))$ в общем случае могут зависеть также и от l (так как значение r_l при выполнении

протокола разделения секрета (2) выбирается случайно и равновероятно), однако здесь рассматриваются только (n,k)-схемы, где эти величины не зависят от значения случайного аргумента. При $K<k$ в (n,k)-схеме веса «черного» и «белого» пикселей должны быть неразличимы, т.е. $\alpha(\underline{n}(K))=0$.

В [5] построена (k,k)-схема (далее — схема Наора – Шамира), для которой $m=2^{k-1}$ и величины $d(\underline{n}(K))$ и $\alpha(\underline{n}(K))$ зависят только от мощности K коалиции $\underline{n}(K)$. В удобном виде приведем описание (k,k)-схемы из [5].

Рассмотрим множество $W=\{e_0;e_1;\ldots;e_{k-1}\}$. Пусть $\Sigma^0=\{\sigma_1^0,\sigma_2^0,\ldots,\sigma_{2^{k-1}}^0\}$ и $\Sigma^1=\{\sigma_1^1,\sigma_2^1,\ldots,\sigma_{2^{k-1}}^1\}$ — наборы подмножеств множества W четной и нечетной мощности соответственно. Набору Σ^b сопоставляется $(k\times m)$-матрица $S^b=(\mathbf{S}_i^b)_{i=0}^{k-1}$, $\mathbf{S}_i^b=(S_{i,1}^b,\ldots,S_{i,m}^b)$, $b\in\{0,1\}$, где

$$S_{i,j}^b=\begin{cases}1, & \text{если } e_i\in\sigma_j^b,\\ 0, & \text{иначе,}\end{cases}\qquad b\in\{0,1\}. \tag{6}$$

При $k=4$ имеем:

$$\Sigma^0=\{\{e_0,e_1\},\{e_0,e_2\},\{e_0,e_3\},\{e_1,e_2\},\{e_1,e_3\},\{e_2,e_3\},\varnothing,\{e_0,e_1,e_2,e_3\}\},$$
$$\Sigma^1=\{\{e_0\},\{e_1\},\{e_2\},\{e_3\},\{e_0,e_1,e_2\},\{e_0,e_1,e_3\},\{e_0,e_2,e_3\},\{e_1,e_2,e_3\}\},$$

а соответствующие матрицы имеют вид

$$S^0=\begin{pmatrix}1&1&1&0&0&0&0&1\\1&0&0&1&1&0&0&1\\0&1&0&1&0&1&0&1\\0&0&1&0&1&1&0&1\end{pmatrix},\qquad S^1=\begin{pmatrix}1&0&0&0&1&1&1&0\\0&1&0&0&1&1&0&1\\0&0&1&0&1&0&1&1\\0&0&0&1&0&1&1&1\end{pmatrix}. \tag{7}$$

Согласно [5] далее по матрицам (6) строятся соответствующие им коллекции матриц $\mathscr{C}_0$ и $\mathscr{C}_1$, $\mathscr{C}_b=\{\gamma(S^b):\gamma\in\mathscr{S}_{2^{k-1}}\}$, $b\in\{0,1\}$, где $\mathscr{S}_{2^{k-1}}$ симметрическая группа перестановок множества $\{1,\ldots,2^{k-1}\}$, $|\mathscr{S}_{2^{k-1}}|=2^{k-1}!$, $\gamma(S^b)$ — перестановка столбцов матрицы S^b в соответствии с перестановкой γ. Для построения k долей, соответствующих одному биту $b(\in\{0;1\})$ секретного вектора $\mathbf{s}$, случайным образом выбирается матрица $\widetilde{S}^b$ из $\mathscr{C}_b$; доля участника i представляет собой i-ю строку матрицы $\widetilde{S}^b$, $i\in\{0,\ldots,k-1\}$ (нумерация с нуля). Поэтому отображение (1) в данном случае — это выбор i-й строки в случайно выбранной из коллекции $\mathscr{C}_b$ матрице $\widetilde{S}^b=\gamma(S^b)$, $\gamma\in\mathscr{R}=\mathscr{S}_{2^{k-1}}$.

Пусть $\tau\subset\{0,\ldots,k-1\}$, $1\leqslant|\tau|\leqslant k-1$, $\gamma(S^b)_\tau$ — матрица, полученная из матрицы $\gamma(S^b)$ выбрасыванием строк с номерами из множества $\{0,\ldots,k-1\}\setminus\tau$, w_b^τ — вес вектора, получающегося выполнением операции $\vee$ над строками матрицы S^b с номерами из множества τ, $b\in\{0,1\}$. Матрицы S^0 и S^1 обладают следующими свойствами [5]:

1) *матрица S^0 имеет один нулевой столбец, а в матрице S^1 таких столбцов нет;*

2) *наборы $(\gamma(S^1)_\tau)_{\gamma\in\mathscr{S}_{2^{k-1}}}$ и $(\gamma(S^0)_\tau)_{\gamma\in\mathscr{S}_{2^{k-1}}}$ совпадают с точностью до перестановки матриц внутри наборов*;

3) $w_0^{\tau_1}=w_1^{\tau_2}$ *и* $w_b^{\tau_1}=w_b^{\tau_2}$ *для любых таких* τ_1 *и* τ_2, *что* $|\tau_1|=|\tau_2|<k$, где $b\in\{0,1\}$.

Из свойства 3) следует, что $w_b^{\tau_1}$ зависит только от мощности K множества τ, поэтому положим $w_b^{\tau_1}=w_K$. В силу свойства 3) и способа построения коллекций $\mathscr{C}_0$

и $\mathscr{C}_1$ для (k,k)-схемы Наора – Шамира величины $d(\underline{n}(K))$ и $\alpha(\underline{n}(K))$ зависят только от мощности K коалиции $\underline{n}(K)$. Соответствующие величины обозначим $d(K)$ и $\alpha(K)$. В частности, из свойств 2) и 1) следует, что для (k,k)-схемы Наора – Шамира

$$\alpha(K)=\begin{cases}0, & \text{если } K<k,\\ \frac{1}{2^{k-1}}, & \text{если } K=k,\end{cases}\qquad d(K)=\begin{cases}w_K, & \text{если } K<k,\\ 2^{k-1}, & \text{если } K=k.\end{cases} \tag{8}$$

В [5] предложен способ построения (n,k)-схемы на основе (k,k)-схемы. При построении коллекций матриц $\hat{\mathscr{C}_0}$ и $\hat{\mathscr{C}_1}$ для (n,k)-схемы М. Наором и А. Шамиром предлагается использовать класс $\mathscr{F}=\{f_i\}_{i=1}^{L}$ хэш-функции вида $f_i:\{0,\ldots,n-1\}\to\{0,\ldots,k-1\}$. Здесь представляется удобным описать формирование случайной матрицы $\hat{S}^b(\in\hat{\mathscr{C}_b})$ для бита b, а не вводить громоздкое определение коллекции $\hat{\mathscr{C}_b}$. Для построения матрицы $\hat{S}^b$ случайным образом выбираются (возможно, с повторениями) L матриц $T^{b,1},\ldots,T^{b,L}$ ($T^{b,i}\in\mathscr{C}_b$) из коллекции $\mathscr{C}_b$, построенной для (k,k)-схемы Наора – Шамира. Элемент на пересечении i-й строки ($0\leqslant i\leqslant n-1$) и $(j+(l-1)\cdot(2^{k-1}))$-го столбца ($1\leqslant j\leqslant 2^{k-1}$, $1\leqslant l\leqslant L$) матрицы $\hat{S}^b=(\hat{\mathbf{S}}_i^b)_{i=0}^{n-1}$ определяется следующим образом:

$$\hat{S}^b_{i,j+(l-1)\cdot(2^{k-1})}=T^{b,l}_{f_l(i),j},\ f_l\in\mathscr{F}. \tag{9}$$

Построенная таким образом матрица $\hat{S}^b$ состоит из n строк и $2^{k-1}\cdot L$ столбцов и представима в виде конкатенации L матриц размера $(n\times n)$: $\hat{S}^b=[\widetilde{T}^{b,1}\parallel\ldots\parallel\widetilde{T}^{b,L}]$, где $(n\times n)$-матрица $\widetilde{T}^{b,l}$ имеет вид $\widetilde{T}^{b,l}=[\mathbf{T}^{b,l}_{f_l(i)}]_{i=0}^{n-1}$, где $\mathbf{T}^{b,l}_j$ — j-я строка матрицы $T^{b,l}(\in\mathscr{C}_b)$.

Утверждение 1. *Пусть* $\underline{n}(K)=\{i_1,\ldots,i_K\}$ *— коалиция,* $B=\{i_1,\ldots,i_K\}$, $\hat{\mathbf{p}}^b=\vee_{j=1}^{K}\hat{\mathbf{S}}^b_{i_j}$, *Пусть* $\mathscr{A}\subseteq\mathscr{F}$,

$$C(B,f)=|\{f(b):b\in B\}|,\ f\in\mathscr{A}, \tag{10}$$

$\mathscr{C}^{\mathscr{A}}_B(l)=|\{f\in\mathscr{A}:C(B,f)=l\}|$. *Тогда относительная контрастность* $\alpha(\underline{n}(K))$ *для* (k,n)*-схемы, построенной с применением хэш-функций из* $\mathscr{A}$*, вычисляется по формуле*

$$\alpha(\underline{n}(K))=\frac{\mathscr{C}^{\mathscr{A}}_B(k)}{|\mathscr{A}|(2^{k-1})}. \tag{11}$$

Доказательство. Несложно проверить, что величина $w(\hat{\mathbf{p}}^b)$ может быть представлена в виде $w(\hat{\mathbf{p}}^1)=\mathscr{C}^{\mathscr{A}}_B(k)\cdot d(k)+\sum\limits_{l=1}^{k-1}\mathscr{C}^{\mathscr{A}}_B(l)\cdot w_l$ и $w(\hat{\mathbf{p}}^0)=w(\hat{\mathbf{p}}^1)-\mathscr{C}^{\mathscr{A}}_B(k)(\alpha(k)2^{k-1})$, где $\alpha(K)$ — относительная контрастность для (k,k)-схемы Наора – Шамира. Подставляя в (5) значения $w(\hat{\mathbf{p}}^b)$ вместо $w(\mathbf{p}^b)$, $b\in\{0,1\}$, и учитывая равенство $\alpha(k)=\frac{1}{2^{k-1}}$ (см. (8)), получим (11), так как в этом случае $m=|\mathscr{A}|\cdot(2^{k-1})$. □

Учитывая, что $\mathscr{C}^{\mathscr{A}}_B(k)=0$ при $K<k$ для любого B мощности K и менее, то любая коалиция мощности менее k не сможет восстановить секрет (черные и белые пиксели неразличимы). Следующее утверждение устанавливает ограничение на класс функций $\mathscr{F}$, который может применяться для построения (n,k)-схемы по (k,k)-схеме.

Утверждение 2. *Пусть $\mathscr{B}$ — набор всех подмножеств множества $\{0,\dots,n-1\}$ мощности k. Для того чтобы (n,k)-схема, построенная на основе (k,k)-схемы и набора хэш-функций $\mathscr{A}(\subseteq \mathscr{F})$, обеспечивала ненулевую относительную контрастность, необходимо и достаточно, чтобы для всех $B \in \mathscr{B}$ выполнялось неравенство $\mathscr{C}_B^{\mathscr{A}}(k) > 0$.*

Доказательство. Достаточность условия следует из (11).

Докажем необходимость. Предположим, что (n,k)-схема обеспечивает ненулевую контрастность, но существует такое B', $|B'| = k$, что $\mathscr{C}_{B'}^{\mathscr{A}}(k) = 0$. Отсюда получаем, что коалиция участников с номерами из B' не сможет восстановить секретное изображение, так как контрастность нулевая (следует из (11)). Но это противоречит тому, что контрастность ненулевая. □

В общем случае для заданного подмножества $\mathscr{A}(\subseteq \mathscr{F})$ набор $\mathscr{B}$ можно представить в виде объединения непересекающихся подмножеств: $\mathscr{B} = \mathscr{B}_0^{\mathscr{A}} \cup \mathscr{B}_1^{\mathscr{A}} \cup \ldots \cup \mathscr{B}_{L_A}^{\mathscr{A}}$, $L_A = |\mathscr{A}|$, где $\mathscr{B}_i^{\mathscr{A}} = \{B \in \mathscr{B} : \mathscr{C}_B^{\mathscr{A}}(k) = i\}$. Если $\mathscr{B}_0^{\mathscr{A}} = \varnothing$, то набор $\mathscr{A}$ удовлетворяет условиям утверждения 2, при этом если в разбиении множества $\mathscr{B}$ имеется более одного непустого подмножества, то для каждого из этих подмножеств обеспечивается своя относительная контрастность. Таким образом, наборы функций $\mathscr{A}$ (в частности, $\mathscr{A} = \mathscr{F}$), удовлетворяющие условиям утверждения 2, в общем случае позволяют строить схемы визуальной криптографии, названные в [8] *несбалансированными*. В [5] ко множеству $\mathscr{A}$ (в частном случае, к классу $\mathscr{F}$) предъявляются более строгие требования, чем в утверждении 2, для обеспечения одинаковой (сбалансированной) контрастности: для всех $B \in \mathscr{B}$ и всех $1 \leqslant q \leqslant k$ вероятность того, что случайно выбранная функция $f \in \mathscr{A}$ имеет q различных значений на множестве B, должна быть одной и той же. В частности, как указано в [5], этому условию удовлетворяет класс $\mathscr{F}'$, являющийся классом k-универсальных (k-независимых) хэш-функций [9], так как для любых разных $x_1,\dots,x_k$ из $\{0,\dots,n-1\}$ случайные величины $F(x_1),\dots,F(x_k)$ полностью независимы, если F — случайно и равновероятно выбранная функция из $\mathscr{F}'$. Согласно теореме 5.2 из [5] относительная контрастность в этом случае равна $\frac{(2e)^{-k}}{\sqrt{2\pi k}}$, а длина каждой доли, соответствующей одному секретному биту, равна $n^k 2^{k-1}$. Например, при построении $(8,4)$-схемы на основе $(4,4)$-схемы с использованием предложенного в [5] класса 4-универсальных хэш-функций каждый бит будет представлен 32768-ю битами в «теневом» изображении, при этом контрастность будет приблизительно 0.00024. Далее будет показано, что существует такой класс хэш-функций, для которого $(8,4)$-схема обеспечивает контрастность не менее 0.011, при этом каждый бит кодируется не более чем 512-ю битами.

2. (n,k)-СХЕМА НА ОСНОВЕ КЛАССА ЛИНЕЙНЫХ ХЭШ-ФУНКЦИЙ

Рассмотрим множество $\mathscr{H}^{p,t}$ всех $(0,1)$-матриц размера $(p \times t)$, $t \leqslant p$. Пусть

$$b_l : \{0,1\}^l \to \{0,1,\dots,2^l-1\} \tag{12}$$

— функция, ставящая однозначно в соответствие вектору из $\{0,1\}^l$ число из множества $\{0,\dots,2^l-1\}$, а $b_l^{-1} : \{0,\dots,2^l-1\} \to \{0,1\}^l$ — обратная к b_l функция. (Удобным представляется полагать, что $b_l^{-1}(i)$ — двоичная запись числа i.) Зафиксируем отображение

$$h : \mathscr{H}^{p,t} \to \{1,\dots,2^{p\cdot t}\}, \tag{13}$$

однозначно ставящее матрицам из $\mathscr{H}^{p,t}$ десятичное число из диапазона $\{1,\dots,2^{p\cdot t}\}$. Для $H\in\mathscr{H}^{p,t}$ определим функцию $f_{h(H)}:\{0,\dots,2^p-1\}\to\{0,\dots,2^t-1\}$, действующую на элемент $x\in\{0,\dots,2^p-1\}$ по правилу: $f_{h(H)}(x)=b_t(b_p^{-1}(x)\cdot H)$. Класс функций $\mathscr{F}_{\mathscr{H}^{p,t}}=\{f_{h(H)}:H\in\mathscr{H}^{p,t}\}$ называется классом линейных хэш-функций [7], $|\mathscr{F}_{\mathscr{H}^{p,t}}|=2^{p\cdot t}$.

Пусть $k=2^t$, $n=2^p$. Применим правило (9) для построения СРС, где $\mathscr{F}=\mathscr{F}_{\mathscr{H}^{p,t}}$. Отметим, что такая СРС в общем случае может не являться (n,k)-схемой в том смысле, что не для любой коалиции мощности k относительная контрастность будет ненулевая. Однако она при определенных условиях на K является (n,K,k)-схемой, где менее k участников секрет восстановить не могут, а не менее K могут (ramp-схема [4]).

Утверждение 3. *Пусть СРС с n участниками построена на основе (k,k)-схемы Наора – Шамира с применением правила* (9) *и класса $\mathscr{F}_{\mathscr{H}^{p,t}}$. Тогда для любой коалиции $\underline{n}(K)$ мощности K не менее $2^p-(2^{p-t}-1)$ выполняются равенства:*

$$\alpha(\underline{n}(K))=\frac{\prod_{j=0}^{t-1}(2^p-2^j)}{2^{p\cdot t}\cdot(2^{k-1})},\qquad m=2^{p\cdot t}\cdot(2^{k-1}). \tag{14}$$

Доказательство. Пусть $\mathscr{B}_{K,p}$ — множество двоичных $(K\times p)$-матриц, состоящих из попарно различных строк, причем двум двоичным матрицам B_1 и B_2, в каждой из которых нет повторяющихся строк и отличающихся только порядком строк, соответствует одна матрица из $\mathscr{B}_{K,p}$. Отметим, что каждая матрица $B=(\mathbf{b}_i)_{i=1}^K$, $\mathbf{b}_i\in\{0,1\}^p$, принадлежащая $\mathscr{B}_{K,p}$, однозначно соответствует коалиции $\{b_p(\mathbf{b}_1),\dots,b_p(\mathbf{b}_K)\}$ из K участников набора $\underline{n}$. Пусть H — $(p\times t)$-матрица из множества $\mathscr{H}^{p,t}$, $\operatorname{rank}(H)=t$, тогда матрица H может быть рассмотрена как проверочная матрица некоторого бинарного $[p,p-t]$-кода $\mathscr{D}$ длины p и размерности $p-t$. Для заданного $\mathbf{y}\in\mathbb{F}_2^t$ множеством решений уравнения $\mathbf{y}=\mathbf{x}H$ относительно вектора неизвестных $\mathbf{x}=(x_1,\dots,x_p)$ является некоторый смежный класс кода $\mathscr{D}$. Так как мощность смежного класса равна $|\mathscr{D}|=2^{p-t}$, то для того, чтобы при умножении на матрицу H бинарных векторов длины p, представляющих собой строки матрицы B, получалось 2^t различных значений, достаточно, чтобы в матрице B было не менее $2^{p-t}\cdot(2^t-1)+1$ различных строк. Таким образом, для каждой матрицы H ранга t в матрице $B\cdot H$ найдутся 2^t различных строк. Так как над полем $\mathbb{F}_2$ имеется $\prod_{j=0}^{t-1}(2^p-2^j)$ матриц размера $p\times t$ и ранга t, то для $B\in\mathscr{B}_{K,p}$ имеем: $|\mathscr{F}_{B,k}|\geqslant\prod_{j=0}^{t-1}(2^p-2^j)$. Имеется $2^{\operatorname{rank}(H)}$ возможных значений линейных комбинаций строк матрицы H, поэтому при $\operatorname{rank}(H)<t$ любая линейная комбинация строк этой матрицы дает менее k значений. Поэтому на основании (11) получаем (14). □

Таким образом, при $K\geqslant 2^p-(2^{p-t}-1)$ построенная схема является (n,K,k)-схемой. Из доказательства утверждения 3 получаем

Следствие 1. *Пусть $\mathscr{F}=\mathscr{F}_{\mathscr{H}_t^{p,t}}=\{f_{h(H)}\in\mathscr{F}_{\mathscr{H}^{p,t}}:\operatorname{rank}(H)=t\}$, $k=2^t$, $n=2^p$. Тогда для (n,K,k)-схемы при $K\geqslant 2^p-(2^{p-t}-1)$ имеем: $\alpha(\underline{n}(K))=\frac{1}{2^{k-1}}$, $m=\prod_{j=0}^{t-1}(2^p-2^j)\cdot(2^{k-1})$.*

Далее рассматривается случай, когда $k=4$ и $n=8$ ($p=3$, $t=2$), для которого показано, что построенная СРС является $(8,4)$-схемой. Напомним, что для $(4,4)$-схемы Наора – Шамира матрицы S^0 и S^1 имеют вид (7), $d(4)=8$, $\alpha=\frac{1}{8}$. Пусть $\underline{8}=\{0,\dots,7\}$ — участники схемы. Участнику с номером i сопоставим в соответствие

вектор $b_3^{-1}(i)$ длины три. Рассмотрим множества $\mathscr{H} = \mathscr{H}^{3,2}$ и $\widetilde{\mathscr{B}} = \mathscr{B}_{4,3}$, $|\mathscr{H}| = 64$, $|\widetilde{\mathscr{B}}| = 70$. Для (4×3)-матрицы $B = (\mathbf{b}_i)_{i=1}^4$ символом $b_3(B)$ обозначим множество $\{b_3(\mathbf{b}_1), \ldots, b_3(\mathbf{b}_4)\}$ (см. (12)).

Утверждение 4. *Для множества $\widetilde{\mathscr{B}}$ имеет место разбиение $\widetilde{\mathscr{B}} = \widetilde{\mathscr{B}}'_1 \cup \widetilde{\mathscr{B}}'_2$, $|\widetilde{\mathscr{B}}'_1| = 56$, $|\widetilde{\mathscr{B}}'_2| = 14$, причем $\widetilde{\mathscr{B}}'_1 \cap \widetilde{\mathscr{B}}'_2 = \varnothing$ и для любых $B \in \widetilde{\mathscr{B}}'_1$ справедливы равенства $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(1) = 1$, $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(2) = 21$, $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(3) = 36$, $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(4) = 6$, для любых $B \in \widetilde{\mathscr{B}}'_2$ — равенства $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(1) = 4$, $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(2) = 36$, $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(3) = 0$, $\mathscr{C}^{\mathscr{F}_{\mathscr{H}}}_{b_3(B)}(4) = 24$.*

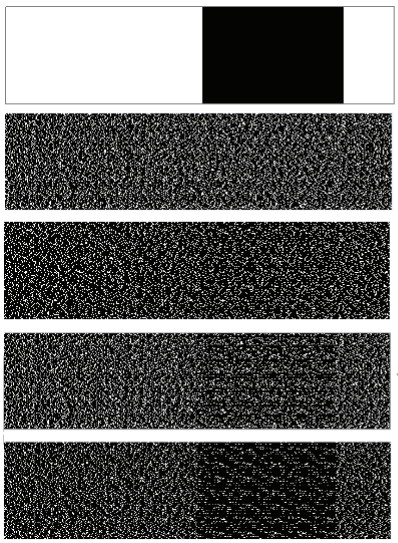
Доказательство утверждения 4 приведено в приложении. Пусть χ — отображение, ставящее в соответствие любой коалиции $\underline{8}(4) = \{i_1, i_2, i_3, i_4\}$ матрицу из $\widetilde{\mathscr{B}}$ по правилу: $\chi(\underline{8}(4)) = \left(b_3^{-1}(i_j)\right)_{j=1}^4$, где $b_3^{-1}(i_j)$ — j-я строка матрицы $\chi(\underline{8}(4))$.

Утверждение 5. *Схема, построенная с применением класса $\mathscr{F}_{\mathscr{H}}$ по правилу* (9) *на основе $(4,4)$-схемы Наора – Шамира, является $(8,4)$-схемой, при этом $m = 512$ и множество $\widetilde{\mathscr{B}}$ распадается на два множества $\widetilde{\mathscr{B}}'_1$, $|\widetilde{\mathscr{B}}'_1| = 56$ и $\widetilde{\mathscr{B}}'_2$, $|\widetilde{\mathscr{B}}'_2| = 14$, так, что*

$$\alpha(\underline{8}(4)) = \begin{cases} 6/512 \approx 0.0117 & \text{для } \chi(\underline{8}(4)) \in \widetilde{\mathscr{B}}'_1, \\ 24/512 \approx 0.0468 & \text{для } \chi(\underline{8}(4)) \in \widetilde{\mathscr{B}}'_2. \end{cases} \tag{15}$$

Доказательство. Доказательство вытекает из утверждений 1, 2 и 4. □

Из утверждения 4 получаем, что если некоторой коалиции мощности 4 соответствует матрица из $\widetilde{\mathscr{B}}'_1$, то $w(\mathbf{p}^1) = 430$ и $w(\mathbf{p}^0) = 424$, где $\mathbf{p}^b$ — вектор вида (4) при $K = 4$. В случае, когда такой коалиции соответствует матрица из $\widetilde{\mathscr{B}}'_2$, то $w(\mathbf{p}^1) = 424$ и $w(\mathbf{p}^0) = 400$. Вычисления в соответствии с (14) показывают, что для семи и восьми долей относительная контрастность равна $42/512 \approx 0.082$. Из результатов работы [10] и утверждения 5 следует, что построенная $(8,4)$-схема обеспечивает приемлемую для схем визуальной криптографии относительную контрастность восстанавливаемых изображений. Также отметим, что построенная схема лучше (как по контрастности, так и по длине долей секрета) соответствующей $(8,4)$-схемы, построенной с применением класса k-универсальных хэш-функций ($k = 4$), предложенного в [5]. Пример применения $(8,4)$-схемы показан на рисунке.



Применения $(8,4)$-схемы
Applications of $(8,4)$-scheme

Из утверждения 2 и доказательства утверждения 4 следует, что построенная $(8,4)$-схема может быть модифицирована путем рассмотрения класса $\mathscr{F}_{\mathscr{H}_2} = \{f_{h(H)} : H \in \mathscr{H}, \operatorname{rank}(H) = 2\}$, так как для каждой матрицы из $\widetilde{\mathscr{B}}$ в $\mathscr{F}_{\mathscr{H}_2}$ найдется хотя бы одна функция, для которой выполняется условие из утверждения 2. В этом случае длина доли каждого участника равна 336 (а не 512), при этом $\alpha(\underline{8}(4)) = 6/336 \approx 0.0178$ для $\chi(\underline{8}(4))$ из $\widetilde{\mathscr{B}}'_1$ и $\alpha(\underline{8}(4)) = 24/336 \approx 0.0714$ для $\chi(\underline{8}(4))$ из $\widetilde{\mathscr{B}}'_2$ (сравните с (15)). Из следствия 1 получаем, что при использовании класса $\mathscr{F}_{\mathscr{H}_2}$ для семи и восьми долей относительная контрастность равна 0.125.

Заметим, что в [10] построена (n,k)-схема, для которой при $n=8$ и $k=4$ относительная контрастность равна $0.0208(3)$, а каждый пиксель кодируется 48-ю битами. Таким образом, построенная в настоящей работе с применением $\mathscr{F}_{\mathscr{H}_2}$ $(8,4)$-схема лучше по контрастности $(8,4)$-схемы из [10], когда $\chi(\underline{8}(4)) \in \widetilde{\mathscr{B}}'_2$, и незначительно хуже, когда $\chi(\underline{8}(4)) \in \widetilde{\mathscr{B}}'_1$, однако при этом длина пикселя в построенной схеме больше в 7 раз.

Библиографический список

1. *Shamir A.* How to share a secret // Communications of the ACM. 1979. Vol. 22, № 11. P. 612–613.
2. *Blakley G. R.* Safeguarding cryptographic keys // Proc. of the National Computer Conference. 1979. Vol. 48. P. 313–317.
3. *Погорелов Б. А., Сачков В. Н.* Словарь криптографических терминов. М. : МЦНМО, 2006. 91 с.
4. *Chen H., Cramer R., Goldwasser S., Haan R., Vaikuntanathan V.* Secure Computation from Random Error Correcting Codes // Advances in Cryptology – EUROCRYPT 2007. EUROCRYPT 2007. Lecture Notes in Computer Science. Berlin ; Heidelberg : Springer, 2007. Vol. 4515. P. 291–310. DOI: 10.1007/978-3-540-72540-4_17
5. *Naor M., Shamir A.* Visual cryptography // Advances in Cryptology – EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science. Berlin, Heidelberg : Springer, 1994. Vol. 950. P. 1–12. DOI: 10.1007/BFb0053419
6. *Pelli D.G., Bex P.* Measuring contrast sensitivity // Vision Res. 2013. Vol. 90. P. 10–14. DOI: 10.1016/j.visres.2013.04.015
7. *Carter J. L., Wegman M. N.* Universal classes of hash functions // Journal of Computer and System Sciences. 1979. Vol. 18, iss. 2. P. 143–154. DOI: 10.1016/0022-0000(79)90044-8
8. *Bose M., Mukerjee R.* Optimal (k,n) visual cryptographic schemes for general k // Des. Codes Cryptogr. 2010. Vol. 55, iss. 1. P. 19–35. DOI: 10.1007/s10623-009-9327-6
9. *Cormen T.H., Leiserson C.E., Rivest R.L., Stein C.* Introduction to Algorithms. Cambridge, Massachusetts; London, England : MIT Press, 2009. 1312 p.
10. *Lakshmanan R., Arumugam S.* Construction of a (k,n)-visual cryptography scheme // Des. Codes Cryptogr. 2017. Vol. 82, iss. 3. P. 629–645. DOI: 10.1007/s10623-016-0181-z

ПРИЛОЖЕНИЕ. ДОКАЗАТЕЛЬСТВО УТВЕРЖДЕНИЯ 4

Рассмотрим разбиение $\widetilde{\mathscr{B}} = \widetilde{\mathscr{B}}_0 \cup \widetilde{\mathscr{B}}_1 \cup \widetilde{\mathscr{B}}_2 \cup \widetilde{\mathscr{B}}_3$, где $\widetilde{\mathscr{B}}_i = \{B \in \widetilde{\mathscr{B}} : \operatorname{rank}(B) = i\}$. Очевидно, что $\widetilde{\mathscr{B}}_0 = \widetilde{\mathscr{B}}_1 = \varnothing$, $|\widetilde{\mathscr{B}}_2| = 7$, $|\widetilde{\mathscr{B}}_3| = 63$, поэтому $\widetilde{\mathscr{B}} = \widetilde{\mathscr{B}}_2 \cup \widetilde{\mathscr{B}}_3$. Выпишем все матрицы множества $\widetilde{\mathscr{B}}_2$:

$$\widehat{B}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \widehat{B}_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad \widehat{B}_3 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \widehat{B}_4 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

$$\widehat{B}_5 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \widehat{B}_6 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \widehat{B}_7 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Множество $\widetilde{\mathscr{B}}_3$ представим в виде $\widetilde{\mathscr{B}}_3 = \widetilde{\mathscr{B}}_{3,1} \cup \widetilde{\mathscr{B}}_{3,2} \cup \widetilde{\mathscr{B}}_{3,3}$, где $\widetilde{\mathscr{B}}_{3,1}$ — матрицы из $\widetilde{\mathscr{B}}_3$, у которых первая строка нулевая (напомним, строки не упорядочены, поэтому можем полагать, что нулевой является первая строка), $\widetilde{\mathscr{B}}_{3,2}$ — матрицы из $\widetilde{\mathscr{B}}_3$, содержащие четыре

ненулевые строки, каждая из которых равна сумме трех других строк, $\widetilde{\mathscr{B}}_{3,3}$ — матрицы из $\widetilde{\mathscr{B}}_3$, содержащие ненулевые строки и одна из строк является суммой двух каких-либо других строк. Покажем, что $|\widetilde{\mathscr{B}}_{3,1}| = 28$, $|\widetilde{\mathscr{B}}_{3,2}| = 7$, $|\widetilde{\mathscr{B}}_{3,3}| = 28$. Заметим, что имеется $(2^3-1)(2^3-2)(2^3-2^2) = 168$ матриц над $\mathbb{F}_2$ размера (3×3) и ранга 3. При этом множество всех этих матриц разбивается на классы, где в каждом классе матрицы отличаются только перестановкой строк. Так как в каждом таком классе 6 матриц, то $|\widetilde{\mathscr{B}}_{3,1}| = 168/6 = 28$. Отсюда также следует $|\widetilde{\mathscr{B}}_{3,2}| = |\widetilde{\mathscr{B}}_{3,1}|/4 = 7$ и $|\widetilde{\mathscr{B}}_{3,3}| = |\widetilde{\mathscr{B}}_3| - (28+7)$. Выпишем все матрицы множества $\widetilde{\mathscr{B}}_{3,2}$:

$$B_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$B_5 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, \quad B_6 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad B_7 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Множество матриц $\mathscr{H} = \mathscr{H}^{3,2}$ также представим в виде разбиения $\mathscr{H} = \mathscr{H}_0 \cup \mathscr{H}_1 \cup \mathscr{H}_2$, где $\mathscr{H}_i = \{H \in \mathscr{H} : \operatorname{rank}(H) = i\}$. Легко проверить, что $|\mathscr{H}_0| = 1$, $|\mathscr{H}_2| = C_7^2 \cdot 2 = 42$ и $|\mathscr{H}_1| = 64 - (42+1) = 21$. Из (10) следует, что $C(b_3(B), f_{h(H)}) = 1$ для всех $B \in \widetilde{\mathscr{B}}$ и всех $H \in \mathscr{H}_0$, где $h(\cdot)$ — отображение вида (13). Для удобства множество $\mathscr{H}_2$ представим в виде: $\mathscr{H}_2 = \mathscr{H}_{2,1} \cup \mathscr{H}_{2,2} \cup \mathscr{H}_{2,3}$, где $\mathscr{H}_{2,1}$ — множество матриц из $\mathscr{H}_2$, содержащих одну нулевую строку, $\mathscr{H}_{2,2}$ — множество матриц из $\mathscr{H}_2$, не содержащих нулевых строк, но при этом какие-либо две строки совпадают, $\mathscr{H}_{2,3}$ — множество матриц из $\mathscr{H}_2$, в которых нет нулевых строк, а сумма всех строк над $\mathbb{F}_2$ равна нулевой строке. Непосредственно проверяется, что $|\mathscr{H}_{2,1}| = |\mathscr{H}_{2,2}| = 18$, $|\mathscr{H}_{2,3}| = 6$.

Вычислим $C(b_3(B), f_{h(H)})$ для случая $B \in \widetilde{\mathscr{B}}_3$ и $H \in \mathscr{H}_2$. Пусть $B \in \widetilde{\mathscr{B}}_{3,1}$, тогда имеет место представление: $B = \begin{pmatrix} \mathbf{0} \\ B' \end{pmatrix}$, где $\mathbf{0} = (0,0,0) \in \mathbb{F}_2^3$, B' — (3×3)-матрица ранга 3. Отметим, что $B' \cdot \mathscr{H}_2 := \{B' \times H : H \in \mathscr{H}_2\} = \mathscr{H}_2$. Отсюда получаем количество значений, которое принимает функция $f_{h(H)}$ на строках матриц из множества $\widetilde{\mathscr{B}}_{3,1}$, когда $H \in \mathscr{H}_2$. Так как матрицы из $\mathscr{H}_2$ имеют ранг 2, то $C(b_3(B), f_{h(H)})$ равно либо трем, либо четырем. На каких функциях $C(b_3(B), f_{h(H)}) = 3$, а на каких $C(b_3(B), f_{h(H)}) = 4$, показано в табл. 1. В частности, все функции $f_{h(H)}$ для $H \in \mathscr{H}_{2,1} \cup \mathscr{H}_{2,2}$ принимают три значения, а для $H \in \mathscr{H}_{2,3}$ — четыре значения.

Таблица 1 / Table 1

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_{3,1}$ и $\mathscr{H}_2$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_{3,1}$ and $\mathscr{H}_2$

Матрица / Matrix	$\mathscr{H}_{2,1}$		$\mathscr{H}_{2,2}$		$\mathscr{H}_{2,3}$	
$C(b_3(B), f_{h(H)})$	*3*	*4*	*3*	*4*	*3*	*4*
$B \in \widetilde{\mathscr{B}}_{3,1}$	18	0	18	0	0	6

Отметим, что так как $\operatorname{rank}(H) = 2$ для всех $H \in \mathscr{H}_2$, то $\mathscr{C}_B^{h(\mathscr{H}_2)}(1) = 0$ для всех $B \in \widetilde{\mathscr{B}}$, где $h(\mathscr{H}_2) = \{f_{h(H)} : H \in \mathscr{H}_2\}$. Действительно, H можно рассматривать как проверочную матрицу некоторого бинарного $[3,1]$-кода длины 3 и размерности 2, мощность которого равна 2. Так как в матрице B четыре разные строки, то в этом случае $C(b_3(B), f_{h(H)}) > 1$. Отметим, что вектор $\mathbf{a} = \mathbf{b}H$ в теории кодирования называется синдромом вектора $\mathbf{b}$.

Рассмотрим случай, когда $B \in \widetilde{\mathscr{B}}_{3,2}$. Если $\mathbf{b}$ — строка матрицы B такая, что $\mathbf{b}H = \mathbf{0}$, то $C(b_3(B), f_{h(H)}) = 4$. Действительно, предположим, что имеются две разные строки $\mathbf{b}'$ и $\mathbf{b}''$ такие, что $\mathbf{b}'H = \mathbf{b}''H$. Отсюда следует, что $(\mathbf{b}' \oplus \mathbf{b}'')H = \mathbf{0}$. Так как в матрице B нет нулевых

строк, то $\mathbf{b}' \oplus \mathbf{b}'' = \mathbf{b}$. Но это противоречит тому, что в матрице нет строк, которые бы являлись суммой *двух* других строк этой матрицы (следует из определения множества $B \in \widetilde{\mathscr{B}}_{3,2}$). Если в матрице B нет таких строк $\mathbf{b}$, что $\mathbf{b}H = \mathbf{0}$, то $C(b_3(B), f_{h(H)}) = 2$. Покажем это. Заметим, что $C(b_3(B), f_{h(H)}) < 4$, так как всего для матрицы H может быть 4 разных синдрома, а по предположению нулевого синдрома при умножении строк матрицы B на матрицу H нет. Выше также отмечалось, что $C(b_3(B), f_{h(H)}) > 1$. Покажем, что $C(b_3(B), f_{h(H)}) \neq 3$. Предположим, что первым строкам $\mathbf{b}_1$, $\mathbf{b}_2$ и $\mathbf{b}_3$ матрицы B соответствуют три разных синдрома: $\mathbf{s}_1$, $\mathbf{s}_2$ и $\mathbf{s}_3$ соответственно. Но так как четвертая строка $\mathbf{b}_4$ матрицы B является суммой первых трех строк, то $\mathbf{s}_4 = \mathbf{s}_1 \oplus \mathbf{s}_2 \oplus \mathbf{s}_3$. В силу того что $C(b_3(B), f_{h(H)}) < 4$, получаем, что какие-то два вектора из набора $\mathbf{s}_1$, $\mathbf{s}_2$, $\mathbf{s}_3$ совпадают, что противоречит предположению. Отсюда $C(b_3(B), f_{h(H)}) = 2$.

Для каждого вектора $\mathbf{b}$ из $\mathbb{F}_2^3$ четного веса во множестве $\mathscr{H}_{2,2}$ найдется набор из 6 матриц, при умножении вектора $\mathbf{b}$ на которые получается нулевой синдром. Причем для двух разных ненулевых векторов четного веса такие наборы матриц не пересекаются (иначе получили бы, что эти векторы линейно зависимые). Для векторов нечетного веса синдромы на матрицах из $\mathscr{H}_{2,2}$ ненулевые. Заметим, что в наборе $\widetilde{\mathscr{B}}_{3,2}$ только одна матрица содержит все векторы нечетного веса — матрица B_1, а остальные содержат по два вектора четного веса. Следовательно, в $\widetilde{\mathscr{B}}_{3,2}$ имеется одна матрица (матрица B_1), при умножении которой на любую матрицу из $\mathscr{H}_{2,2}$ получаются два различных вектора (для разных матриц из $\mathscr{H}_{2,2}$ векторы могут быть разными). И имеется 6 матриц в $\widetilde{\mathscr{B}}_{3,2}$, которые на 12 матрицах из $\mathscr{H}_{2,2}$ принимают четыре разных значения, а на 6 матрицах — два значения. Для матриц из $\mathscr{H}_{2,1}$ только векторы единичного веса могут давать нулевой синдром. Поэтому в $\widetilde{\mathscr{B}}_{3,2}$ имеется одна матрица, которая на всех матрицах из $\mathscr{H}_{2,1}$ дает четыре разных значения; три матрицы, которые на 12 матрицах из $\mathscr{H}_{2,1}$ дают четыре значения и на 6 матрицах дают два значения; три матрицы, которые на 12 матрицах из $\mathscr{H}_{2,1}$ дают два значения и на 6 матрицах дают четыре значения.

Для матриц из $\mathscr{H}_{2,3}$ только векторы веса три могут давать нулевой синдром, так как все столбцы матриц из $\mathscr{H}_{2,3}$ имеют четный вес. Следовательно, четыре матрицы из $\widetilde{\mathscr{B}}_{3,2}$ на всех матрицах $\mathscr{H}_{2,3}$ дают четыре разных значения и три матрицы из $\widetilde{\mathscr{B}}_{3,2}$ на всех матрицах из $\mathscr{H}_{2,3}$ дают два разных значения (табл. 2).

Таблица 2 / Table 2

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_{3,2}$ и $\mathscr{H}_2$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_{3,2}$ and $\mathscr{H}_2$

Матрица / Matrix	$\mathscr{H}_{2,1}$		$\mathscr{H}_{2,2}$		$\mathscr{H}_{2,3}$	
$C(b_3(B), f_{h(H)})$	*2*	*4*	*2*	*4*	*2*	*4*
B_2, B_3, B_4	6	12	6	12	6	0
B_5, B_6, B_7	12	6			0	6
B_1	0	18	18	0		

Рассмотрим множество $\widetilde{\mathscr{B}}_{3,3}$. Без нарушения общности можно полагать, что для каждой матрицы $B = (\mathbf{b}_i)_{i=1}^4$ из $\widetilde{\mathscr{B}}_{3,3}$ выполняется условие: $\mathbf{b}_1 = \mathbf{b}_2 \oplus \mathbf{b}_3$ и $\operatorname{rank}(B)' = 3$, где $B' = (\mathbf{b}_i)_{i=2}^4$. Рассмотрим множество $B \cdot \mathscr{H}_2 = \{BH : H \in \mathscr{H}_2\}$. Из вида матриц множества $\widetilde{\mathscr{B}}_{3,3}$ следует, что $B \cdot \mathscr{H}_2 = \{\left((\mathbf{h}_1 \oplus \mathbf{h}_2)^\top \parallel H^\top\right)^\top : H = (\mathbf{h}_i)_{i=1}^3 \in \mathscr{H}_2\}$. Отсюда следует распределение для $C(b_3(B), f_{h(H)})$, показанное в табл. 3.

Таблица 3 / Table 3

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_{3,3}$ и $\mathscr{H}_2$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_{3,3}$ and $\mathscr{H}_2$

Матрица / Matrix	$\mathscr{H}_{2,1}$		$\mathscr{H}_{2,2}$		$\mathscr{H}_{2,3}$	
$C(b_3(B), f_{h(H)})$	*3*	*4*	*3*	*4*	*3*	*4*
$B \in \widetilde{\mathscr{B}}_{3,3}$	12	6	18	0	6	0

Теперь рассмотрим множество $\mathscr{H}_1$. Представим его в виде $\mathscr{H}_1 = \mathscr{H}_{1,1} \cup \mathscr{H}_{1,2} \cup \mathscr{H}_{1,3}$, где $\mathscr{H}_{1,1}$ — матрицы, состоящие из трех одинаковых ненулевых строк, $\mathscr{H}_{1,2}$ — множество матриц, состоящих из двух одинаковых ненулевых строк и одной нулевой строки, $\mathscr{H}_{1,3}$ — множество матриц, состоящих из одной ненулевой и двух нулевых строк; $|\mathscr{H}_{1,1}| = 3$, $|\mathscr{H}_{1,2}| = 9$, $|\mathscr{H}_{1,3}| = 9$.

Матрицы множества $\widetilde{\mathscr{B}}_{3,1}$ при умножении на любую матрицу H из $\mathscr{H}_1$ не дадут нулевую

матрицу (иначе бы получили, что матрицы из множества $\widetilde{\mathscr{B}}_{3,1}$ имеют ранг 2). Поэтому $C(b_3(B), f_{h(H)}) = 2$ для всех $H \in \mathscr{H}_1$ и всех $B \in \widetilde{\mathscr{B}}_{3,1}$.

Рассмотрим множество $\widetilde{\mathscr{B}}_{3,2}$. Отметим, что в $\widetilde{\mathscr{B}}_{3,2}$ только матрица B_1 не имеет строк четного веса, поэтому только матрица B_1 на множестве $\mathscr{H}_{1,1}$ даст одно значение, а все остальные матрицы из $\widetilde{\mathscr{B}}_{3,2}$ на матрицах из $\mathscr{H}_{1,1}$ будут давать два значения. В общем случае, для любой матрицы H из $\mathscr{H}_1$ найдется матрица B (только одна), строки которой представляют собой смежный класс кода с проверочной матрицей H. При этом для матрицы B имеется ровно три матрицы из $\mathscr{H}_1$, дающие одинаковый синдром (если учитывать линейные комбинации столбцов матриц H). На остальных матрицах из $\mathscr{H}_1$ матрица B дает два значения. Поэтому $\mathscr{C}_B^{h(\mathscr{H}_1)}(1) = 3$ и $\mathscr{C}_B^{h(\mathscr{H}_1)}(2) = 18$ для всех $B \in \widetilde{\mathscr{B}}_{3,2}$.

Все матрицы из $\widetilde{\mathscr{B}}_{3,3}$ на матрицах из $\mathscr{H}_1$ дают два значения, так как произведение таких матриц не может дать нулевую матрицу, и в матрицах из $\widetilde{\mathscr{B}}_{3,3}$ первая строка является суммой каких-то двух других строк. Поэтому синдром, соответствующий первой строке, равен сумме синдромов и $\mathscr{C}_B^{h(\mathscr{H}_1)}(2) = 21$ для всех $B \in \widetilde{\mathscr{B}}_{3,3}$.

Рассмотрим теперь множество $\widetilde{\mathscr{B}}_2$. Так как $\operatorname{rank}(B) = 2$ для любой $B \in \widetilde{\mathscr{B}}_2$, то B может быть представлена в виде: $B = \left(\mathbf{0}^\top \parallel \mathbf{b}_1^\top \parallel \mathbf{b}_2^\top \parallel (\mathbf{b}_1 \oplus \mathbf{b}_2)^\top\right)^\top$, где $\mathbf{a}^\top$ — транспонированный вектор $\mathbf{a}$. Тогда во множестве $\mathscr{H}_2$ найдутся 18 матриц (по 6 штук на каждую ненулевую строку матрицы B), что при умножении на них матрица B будет давать два разных значения (так как любую ненулевую строку матрицы B вместе с нулевой строкой можно рассматривать как одномерный код, а оставшиеся две ненулевые строки – как смежный класс этого кода; для кода размерности один также существует 6 различных проверочных матриц). Также отметим, что если для двух ненулевых строк матрицы синдромы одинаковые, то для других двух строк синдромы будут нулевые. Если же для двух ненулевых строк матрицы B синдромы ненулевые и разные, то синдром для третьей ненулевой строки будет отличен от этих двух. Таким образом, для оставшихся 24 матриц из $\mathscr{H}_2$ при умножении на B будет четыре разных значения.

Рассмотрим множество $\mathscr{H}_1$. Непосредственно проверяется, что матрица $\widehat{B}_4$ принимает на всех матрицах набора $\mathscr{H}_{1,1}$ одно (нулевое) значение, так как все строки матрицы $\widehat{B}_4$ имеют четный вес. Все остальные матрицы на всех матрицах набора $\mathscr{H}_{1,1}$ принимают 2 значения. Также любая из матриц $\widehat{B}_1, \widehat{B}_2, \widehat{B}_3$ дает на матрицах из $\mathscr{H}_{1,2}$ два разных значения (так как есть две разные строки единичного веса). На матрицах из $\mathscr{H}_{1,3}$ эти матрицы $(\widehat{B}_1, \widehat{B}_2, \widehat{B}_3)$ дают одно значение на трех матрицах и два значения на 6 матрицах. Матрица $\widehat{B}_4$ дает два значения на всех матрицах наборов $\mathscr{H}_{1,2}$ и $\mathscr{H}_{1,3}$. Для каждой матрицы $\widehat{B}_5, \widehat{B}_6, \widehat{B}_7$ в $\mathscr{H}_{1,2}$ найдутся три матрицы, на которых будет приниматься одно значение, а для остальных 6 матриц — два значения. На всех матрицах из $\mathscr{H}_{1,3}$ матрицы $\widehat{B}_5, \widehat{B}_6, \widehat{B}_7$ принимают два разных значения (так как в матрицах $\widehat{B}_5, \widehat{B}_6, \widehat{B}_7$ имеется строка из единиц и в матрицах из $\mathscr{H}_{1,3}$ вес каждого столбца не выше 1). Результаты для этого случая обобщены в табл. 4. Полагая $\widetilde{\mathscr{B}}_1' = \widetilde{\mathscr{B}}_{3,1} \cup \widetilde{\mathscr{B}}_{3,3}$ и $\widetilde{\mathscr{B}}_2' = \widetilde{\mathscr{B}}_{3,2} \cup \widetilde{\mathscr{B}}_2$ и учитывая, что нулевая матрица из $\mathscr{H}$ дает одно значение, получим доказываемое утверждение.

Таблица 4 / Table 4

Распределение $C(b_3(B), f_{h(H)})$ для $\widetilde{\mathscr{B}}_2$ и $\mathscr{H}_1$

The distribution of $C(b_3(B), f_{h(H)})$ for $\mathscr{B}_2$ and $\mathscr{H}_1$

Матрица / Matrix	$\mathscr{H}_{1,1}$		$\mathscr{H}_{1,2}$		$\mathscr{H}_{1,3}$	
$C(b_3(B), f_{h(H)})$	*1*	*2*	*1*	*2*	*1*	*2*
$\widehat{B}_4$	3	0	0	9	0	9
$\widehat{B}_1, \widehat{B}_2, \widehat{B}_3$	0	3	0	9	3	6
$\widehat{B}_5, \widehat{B}_6, \widehat{B}_7$	0	3	3	6	0	9

Образец для цитирования:

Косолапов Ю. В. О построении (k, n)-схемы визуальной криптографии с применением класса линейных хэш-функций над бинарным полем // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2018. Т. 18, вып. 2. С. 227–239. DOI: 10.18500/1816-9791-2018-18-2-227-239

On the Construction of (n, k)-schemes of Visual Cryptography Using a Class of Linear Hash Functions Over a Binary Field

Yu. V. Kosolapov

Yury V. Kosolapov, https://orcid.org/0000-0002-1491-524X, Southern Federal University, 105/42, Bol'shaya Sadovaya Str., Rostov-on-Don, 344006, Russia, itaim@mail.ru

The paper explores the use of a set of hash functions for constructing a secret sharing scheme among n participants based on the (k, k)-scheme M. Nahor and A. Shamir. Conditions are obtained for a set of hash functions, in which it is possible to construct (k, n)-schemes where any coalition of power k or more can restore a secret, and a coalition of lower power cannot restore the secret. In particular, the application of the class of linear hash functions is investigated. In general, this class does not allow us to construct a (k, n)-scheme, but it is possible to construct a (k, K, n)-scheme for which any $k - 1$ and less participants cannot restore the secret, and any K and more can. For a class of linear hash functions, sufficient conditions are obtained for K, in which the coalition of power K and more can restore the secret. In a particular case, a secret sharing scheme for eight participants was developed, based on the $(4, 4)$-scheme of M. Naor and A. Shamir using a class of linear hash functions. It is shown that for any 4-power coalition the secret can be restored, that is, the constructed scheme is a $(8, 4)$-scheme. The $(8, 4)$-scheme constructed in particular is characterized by a shorter length of shares than the $(8, 4)$-scheme constructed in accordance with the algorithm proposed by M. Naor and A. Shamir.

Key words: secret sharing scheme, visual cryptography, linear hash functions.

References

1. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22, № 11, pp. 612–613.
2. Blakley G. R. Safeguarding cryptographic keys. *Proc. of the National Computer Conference*, 1979, vol. 48, pp. 313–317.
3. Pogorelov B. A., Sachkov V. N. *Slovar' kriptograficheskih terminov* [Dictionary of cryptographic terms]. Moscow, MTsNMO, 2006. 91 p.(in Russian).
4. Chen H., Cramer R., Goldwasser S., Haan R., Vaikuntanathan V. Secure Computation from Random Error Correcting Codes. *Advances in Cryptology – EUROCRYPT 2007. EUROCRYPT 2007. Lecture Notes in Computer Science*. Berlin, Heidelberg, Springer, 2007, vol. 4515, pp. 291–310. DOI: 10.1007/978-3-540-72540-4_17
5. Naor M., Shamir A. Visual cryptography. *Advances in Cryptology — EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science*. Berlin, Heidelberg, Springer, 1994, vol. 950, pp. 1–12. DOI: 10.1007/BFb0053419
6. Pelli D.G., Bex P. Measuring contrast sensitivity. *Vision Res.*, 2013, vol. 90, pp. 10–14. DOI: 10.1016/j.visres.2013.04.015
7. Carter J. L., Wegman M. N. Universal classes of hash functions. *Journal of Computer and System Sciences*, 1979, vol. 18, iss. 2, pp. 143–154. DOI: 10.1016/0022-0000(79)90044-8
8. Bose M., Mukerjee R. Optimal (k, n) visual cryptographic schemes for general k. *Des. Codes Cryptogr.*, 2010, vol. 55, iss. 1, pp. 19–35. DOI: 10.1007/s10623-009-9327-6
9. Cormen T. H., Leiserson C. E., Rivest R. L., Stein C. *Introduction to Algorithms*. Cambridge, Massachusetts; London, England, MIT Press, 2009. 1312 p.
10. Lakshmanan R., Arumugam S. Construction of a (k, n)-visual cryptography scheme. *Des. Codes Cryptogr.*, 2017, vol. 82, iss. 3, pp. 629–645. DOI: 10.1007/s10623-016-0181-z

Cite this article as:
Kosolapov Yu. V. On the Construction of (k, n)-Schemes of Visual Cryptography Using a Class of Linear Hash Functions Over a Binary Field. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2018, vol. 18, iss. 2, pp. 227–239 (in Russian). DOI: 10.18500/1816-9791-2018-18-2-227-239