УДК 519.7

О применении конечных полей в некоторых совершенных криптосистемах

С. М. Рацеев, Е. Е. Беспалова, П. В. Буранкина, М. А. Гусарова

В работе приводятся конструкции совершенных имитостойких шифров и оптимальных кодов аутентификации на основе конечных полей и ортогональных таблиц.

Ключевые слова: шифр, совершенный шифр, имитация сообщения, код аутентификации.

1. Введение

Конечные поля активно используются в криптографии. Например, на основе конечных полей $GF(2^8)$ построены симметричные блочные шифры AES [1] и «Кузнечик» [2], где AES — международный стандарт блочного шифрования ISO/IEC 18033-3:2010, «Кузнечик» — шифр из российского стандарта ГОСТ Р 34.12-2015 [2]. Асимметричная криптосистема Шора–Ривеста [3] строится на основе дискретных логарифмов в мультипликативной группе конечного поля $GF(p^n)$, до сих пор пользуется доверием и не поддается вскрытию. В данной работе показано, как на основе конечных полей можно строить совершенные криптосистемы.

Пусть X, K, Y — конечные множества открытых текстов, ключей и шифрованных текстов соответственно. Обозначим через

$$\Sigma_B = (X, K, Y, E, D, P_X, P_K)$$

вероятностную модель шифра (см. [4]). Распределения вероятностей P_X и P_K естественным образом индуцируют распределение вероятностей P_Y следующим образом:

$$P_Y(y) = \sum_{\substack{(x,k)\in X\times K \\ E_k(x)=y}} P_X(x)\cdot P_K(k), \quad y \in Y.$$

Пусть $x \in X$, $y \in Y$. Обозначим через $K(x,y)$ множество всех таких ключей $k \in K$, для которых $E_k(x) = y$. Условная вероятность $P_{Y|X}(y|x)$ определяется естественным образом:

$$P_{Y|X}(y|x) = \sum_{k\in K(x,y)} P_K(k).$$

На основе теоремы умножения вероятностей определяется условная вероятность $P_{X|Y}(x|y)$:

$$P_{X|Y}(x|y) = \frac{P_X(x)\cdot P_{Y|X}(y|x)}{P_Y(y)}.$$

2. Совершенные и имитостойкие шифры

Напомним, что шифр Σ_B называется совершенным (по Шеннону), если для любых $x \in X$, $y \in Y$ выполнено равенство $P_{X|Y}(x|y) = P_X(x)$. Другими словами, перехваченное шифрованное сообщение y не дает никакой дополнительной информации об открытом тексте x.

В работе [5] приводится критерий, позволяющий однозначно определить, существует ли для заданных X, K, P_K совершенный шифр.

Теорема 1 ([5]). Для заданных X, $|X| = n$, K, $|K| = m$, P_K существует совершенный шифр $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$ тогда и только тогда, когда найдется такое натуральное число s и n разбиений множества K

$$\begin{aligned} K &= K_{11} \cup K_{12} \cup \ldots \cup K_{1s}, \quad K_{1i} \cap K_{1j} = \emptyset, \quad 1 \le i < j \le s, \\ K &= K_{21} \cup K_{22} \cup \ldots \cup K_{2s}, \quad K_{2i} \cap K_{2j} = \emptyset, \quad 1 \le i < j \le s, \\ &\ldots \\ K &= K_{n1} \cup K_{n2} \cup \ldots \cup K_{ns}, \quad K_{ni} \cap K_{nj} = \emptyset, \quad 1 \le i < j \le s, \end{aligned}$$

для которых выполнены следующие условия:

1) $K_{it} \cap K_{jt} = \emptyset$, $1 \le i < j \le n$, $t = 1, \ldots, s$;

2) для любых $1 \le i < j \le n$, $t = 1, \ldots, s$ выполнено равенство

$$\sum_{k \in K_{it}} P_K(k) = \sum_{k \in K_{jt}} P_K(k).$$

Рассмотрим вероятностное пространство $(\Omega = K, F_K, P_K)$. Зафиксируем $y \in Y$. Обозначим через $K(y)$ следующее множество: $K(y) = \{k \in K \mid y \in E_k(X)\}$. Под обозначением $K(y)$ будем также понимать событие ($K(y) \in F_K$), заключающееся в том, что при случайном выборе ключа $k \in K$ шифрованный текст y можно расшифровать на ключе k, то есть $y \in E_k(X)$. Тогда событию $K(y)$ будут благоприятствовать все элементы из множества $K(y)$, и только они. Поэтому

$$P(K(y)) = \sum_{k \in K(y)} P_K(k).$$

Если канал связи готов к работе и на приеме установлены действующие ключи, но в данный момент времени никакого сообщения не передается, то в этом случае противником может быть предпринята попытка имитации сообщения. Тогда вероятность успеха имитации определяется следующим образом:

$$P_{im} = \max_{y \in Y} P(K(y)).$$

Если же в данный момент передается некоторое сообщение $y \in Y$ (которое получено из открытого текста $x \in X$ на ключе $k \in K$), то противник может заменить его на $\widetilde{y} \in Y$, отличный от y. При этом он будет рассчитывать на то, что на действующем ключе k криптограмма $\widetilde{y}$ при расшифровании будет воспринята как некий осмысленный открытый текст $\widetilde{x}$, отличный от x. Пусть «$K(\widetilde{y}) \mid K(y)$» — событие, заключающееся в попытке подмены сообщения y сообщением $\widetilde{y}$. Применяя теорему о произведении вероятностей, получаем, что

$$P(K(\widetilde{y}) \mid K(y)) = \frac{P(K(y) \cap K(\widetilde{y}))}{P(K(y))} = \frac{\sum_{k \in K(y,\widetilde{y})} P_K(k)}{\sum_{k \in K(y)} P_K(k)},$$

где $K(y, \widetilde{y}) = K(y) \cap K(\widetilde{y})$. Тогда вероятность успеха подмены сообщения будет вычисляться по следующей формуле:

$$P_{podm} = \max_{\substack{y, \widetilde{y} \in Y \\ y \ne \widetilde{y}}} P(K(\widetilde{y}) \mid K(y)).$$

Теорема 2 ([4]). Для любого шифра Σ_B справедливы неравенства

$$P_{im} \ge \frac{|X|}{|Y|}, \quad P_{podm} \ge \frac{|X| - 1}{|Y| - 1}.$$

При этом $P_{im} = |X|/|Y|$ тогда и только тогда, когда для любого $y \in Y$ выполнено равенство $P(K(y)) = |X|/|Y|$. Также $P_{podm} = (|X| - 1)/(|Y| - 1)$ тогда и только тогда, когда для любых $y, \widetilde{y} \in Y$, $y \ne \widetilde{y}$ выполнено равенство $P(K(\widetilde{y}) \mid K(y)) = (|X| - 1)/(|Y| - 1)$.

Назовем шифр Σ_B имитостойким, если для него одновременно выполнены нижние границы (меньшие единицы) для вероятностей успехов имитации и подмены шифрованных сообщений.

Сделаем некоторые пояснения. В рассматриваемых моделях шифров нет привязки к естественным языкам и распределение вероятностей P_X не играет никакой роли для построения совершенных имитостойких шифров (можно сказать, совсем не учитывается), т.е. шифровать можно любую информацию с любым распределением вероятностей. При этом заметим, что шифр Вернама хоть и является совершенным (при равновероятном распределении ключевых последовательностей), но максимально уязвим к попыткам имитации и подмены шифрованных сообщений, особенно если в качестве открытых текстов выступают тексты не на естественных языках. Тогда после факта подмены или имитации шифрованного сообщения принимающая сторона после расшифрования может этот факт не обнаружить, так как получила какое-то двоичное сообщение, которое предполагалось использовать в качестве ключа.

Если же мощность множества Y будет больше, чем мощность множества X (в отличие от шифра Вернама), то вероятность обнаружить факт имитации или подмены может увеличиться. Приведем пример.

Пример 1. Пусть Σ_B — шифр, определенный множествами

$$X = \{x_1, x_2\}, \quad K = \{k_1, k_2, k_3\}, \quad Y = \{y_1, y_2, y_3\}$$

и матрицей зашифрования

$K \diagdown X$	x_1	x_2
k_1	y_1	y_2
k_2	y_2	y_3
k_3	y_3	y_1

Предположим, что у абонентов A и B установлены ключи k_2. В данный момент времени сообщение от A к B не передается, но злоумышленник отправил от имени абонента A сообщение y_1. Так как на ключе k_2 нельзя получить этого шифрованного текста, то абонент B поймет, что произошло что-то не то.

В этом случае, если P_K равномерно, то данный шифр обладает свойством совершенности, плюс к этому вероятности имитации и подмены меньше единицы (в отличие от шифра Вернама), а именно, $P_{im} = 2/3$, $P_{podm} = 1/2$.

3. Построение совершенных имитостойких шифров на основе конечных полей

Рассмотрим некоторые конструкции из работы [6]. Напомним несколько важных определений. *Латинским квадратом* s-го порядка над множеством $Y = \{y_1, \ldots, y_s\}$ называется таблица размера $s \times s$, заполненная элементами множества Y таким образом, что в каждой строке и в каждом столбце каждый элемент встречается ровно один раз. Две матрицы $A = (a_{ij})$ и $B = (b_{ij})$ над множеством $Y = \{y_1, \ldots, y_s\}$ называются *ортогональными*, если все упорядоченные пары (a_{ij}, b_{ij}) различны. *Ортогональной таблицей* $OA(s, n)$ над множеством $Y = \{y_1, \ldots, y_s\}$ называется матрица порядка $s^2 \times n$ над множеством Y с тем условием, что для любых двух столбцов данной матрицы каждая из пар $(y_i, y_j) \in Y \times Y$ встречается ровно один раз. Существование ортогональной таблицы $OA(s, n)$ над множеством Y эквивалентно существованию n попарно ортогональных квадратных матриц порядка s над множеством Y.

Теорема 3 (Bose [7]). Для любого простого p и натурального d существуют $p^d - 1$ ортогональных латинских квадратов.

Пример 2. Пусть в теореме 3 $p = 2$, $d = 2$. Построим три ортогональных латинских квадрата порядка 4. Пусть α — алгебраический элемент поля $GF(2^2)$ степени два над полем $\mathbb{Z}_2$ с неприводимым многочленом $x^2 - x - 1$. Все элементы поля $GF(2^2)$ можно представить в виде двоичных наборов длины два со следующим соответствием:

$$0 \to 00, \;\; 1 \to 01, \;\; \alpha \to 10, \;\; \alpha + 1 \to 11.$$

Матрицы A_{01}, A_{10}, A_{11} из теоремы 3 будут соответственно иметь такой вид:

$$\begin{pmatrix} 00 & 01 & 10 & 11 \\ 01 & 00 & 11 & 10 \\ 10 & 11 & 00 & 01 \\ 11 & 10 & 01 & 00 \end{pmatrix}, \begin{pmatrix} 00 & 01 & 10 & 11 \\ 10 & 11 & 00 & 01 \\ 11 & 10 & 01 & 00 \\ 01 & 00 & 11 & 10 \end{pmatrix}, \begin{pmatrix} 00 & 01 & 10 & 11 \\ 11 & 10 & 01 & 00 \\ 01 & 00 & 11 & 10 \\ 10 & 11 & 00 & 01 \end{pmatrix}.$$

Ортогональная таблица легко получается из ортогональных латинских квадратов и наоборот.

Пример 3. Построим ортогональную таблицу $OA(4, 3)$ над множеством $GF(4)$ на основе ортогональных латинских квадратов из примера 2. Сначала все строки матрицы A_{01} выпишем построчно. Под полученной строкой построчно выпишем все строки матрицы A_{10}. То же самое проделаем и с матрицей A_{11}. Транспонировав полученную матрицу, получим ортогональную таблицу $OA(4, 3)$ над полем $GF(4)$:

$$\begin{pmatrix} 00 & 01 & 10 & 11 & 01 & 00 & 11 & 10 & 10 & 11 & 00 & 01 & 11 & 10 & 01 & 00 \\ 00 & 01 & 10 & 11 & 10 & 11 & 00 & 01 & 11 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\ 00 & 01 & 10 & 11 & 11 & 10 & 01 & 00 & 01 & 00 & 11 & 10 & 10 & 11 & 00 & 01 \end{pmatrix}^T.$$

Используем теорему 3 для построения совершенных шифров. Так как вся информация на электронных устройствах хранится в основном в двоичном виде, то для практических целей в теореме 3 удобно использовать $p = 2$ и шифровать/расшифровывать двоичные блоки, получая при этом двоичные блоки длины d.

Определенная вероятностная модель шифра Σ_B позволяет рассматривать в качестве множества открытых текстов X лишь последовательности в некотором конечном алфавите A, длины которых ограничены некоторой заранее определенной константой. В работе [4] приводятся модели шифров замены с ограниченным и неограниченным ключом, для которых, в частности, на множество X такое ограничение не накладывается. Поскольку в общем случае шифр замены с ограниченным ключом совершенным не является (см. [4]), нас будет интересовать шифр замены с неограниченным ключом. Приведем модель данного шифра.

Пусть U — конечное множество возможных шифрвеличин, а V — конечное множество возможных шифробозначений. Пусть также имеются r ($r > 1$) инъективных отображений из U в V. Пронумеруем данные отображения: E_1, E_2,..., E_r. Данные отображения называются простыми заменами. Обозначим $\mathbb{N}_r = \{1, 2, ..., r\}$. Опорным шифром шифра замены назовем совокупность $\Sigma = (U, \mathbb{N}_r, V, E, D)$, для которой выполнены следующие свойства:

1) для любых $u \in U$ и $j \in \mathbb{N}_r$ выполнено равенство $D_j(E_j(u)) = u$;

2) $V = \bigcup_{j \in \mathbb{N}_r} E_j(U)$.

При этом $E = \{E_1, ..., E_r\}$, $D = \{D_1, ..., D_r\}$, $D_j : E_j(U) \to U$, $j \in \mathbb{N}_r$.

l-ой степенью опорного шифра Σ назовем совокупность

$$\Sigma^l = (U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)}),$$

где $U^l, \mathbb{N}_r^l, V^l$ — декартовы степени соответствующих множеств U, $\mathbb{N}_r$, V. Множество $E^{(l)}$ состоит из отображений $E_{\overline{j}} : U^l \to V^l$, $\overline{j} \in \mathbb{N}_r^l$, таких, что для любых $\overline{u} = u_1...u_l \in U^l$, $\overline{j} = j_1...j_l \in \mathbb{N}_r^l$ выполнено равенство

$$E_{\overline{j}}(\overline{u}) = E_{j_1}(u_1)...E_{j_l}(u_l) = v_1...v_l \in V^l,$$

а множество $D^{(l)}$ состоит из отображений $D_{\overline{j}} : E_{\overline{j}}(U^l) \to U^l$, $\overline{j} \in \mathbb{N}_r^l$, таких, что для любых $\overline{v} = v_1...v_l \in V^l$, $\overline{j} = j_1...j_l \in \mathbb{N}_r^l$ выполнено равенство

$$D_{\overline{j}}(\overline{v}) = D_{j_1}(v_1)...D_{j_l}(v_l) = u_1...u_l \in U^l.$$

Пусть ψ_c — случайный генератор ключевого потока, который для любого натурального числа l вырабатывает случайный ключевой поток $j_1...j_l$, где все $j_i \in \mathbb{N}_r$.

Обозначим через Σ_H^l следующую совокупность величин:

$$\Sigma_H^l = (U^l, \mathbb{N}_r^l, V^l, E^{(l)}, D^{(l)}, P(U^l), P(\mathbb{N}_r^l)).$$

Шифром замены с неограниченным ключом назовем семейство

$$\Sigma_H = (\Sigma_H^l,\ l \in \mathbb{N};\ \psi_c).$$

Для шифра замены с неограниченным ключом Σ_H обозначим через P_{im}^l вероятность успеха имитации сообщения для шифра Σ_H^l, а через $P_{podm}^l(t)$ — вероятность успеха подмены в сообщении длины l ровно t символов для шифра Σ_H^l, где $t \leq l$.

Следующий пример показывает важность рассмотрения модели шифра Σ_H.

Пример 4. В классической модели шифра Σ_B множества X, Y и K конечны. Поэтому вероятности имитации и подмены ограничены снизу константой (в зависимости от шифра). Шифр Σ_H строится, в частности, для того, чтобы эти вероятности устремить к нулю. На основе примера 1 построим шифр Σ_H.

Пусть Σ_H — шифр, определенный множествами

$$U = \{u_1, u_2\},\ \ \mathbb{N}_r = \{1, 2, 3\},\ \ V = \{v_1, v_2, v_3\}$$

и матрицей зашифрования

$\mathbb{N}_r \diagdown U$	u_1	u_2
1	v_1	v_2
2	v_2	v_3
3	v_3	v_1

В этой модели шифра символы открытого текста шифруются (расшифровываются) независимо. Например, нужно зашифровать сообщение $\overline{u} = u_2u_1u_2$. Случайный генератор вырабатывает номера простых замен, к примеру, 213. Тогда шифртекст равен $\overline{v} = E_2(u_2)E_1(u_1)E_3(u_2) = v_3v_1v_1$.

Для имитации сообщения длины l злоумышленник должен сгенерировать l элементов множества V. Имитация каждого символа имеет вероятность, меньшую единицы. Поэтому вероятность имитации сообщения длины l стремится к нулю с ростом l.

Пусть $OA(s, n)$ — ортогональная таблица над множеством $V = \{v_1, \ldots, v_s\}$, где s — степень простого числа, $1 < n < s$, в которой i-я строка содержит только элемент v_i, $i = 1, \ldots, s$ (теорема 3). Вычеркнем из таблицы $OA(s, n)$ первые s строк и обозначим полученную таблицу через $A(s, n)$. Понятно, что таблица $A(s, n)$ имеет размерность $(s^2 - s) \times n$, в каждой строке нет повторяющихся элементов, а каждый столбец содержит ровно $s - 1$ экземпляров элемента v_i, $i = 1, \ldots, s$.

Теорема 4 ([8]). Пусть для шифра Σ_H выполнены следующие условия:

(i) $|U| = n$, $|V| = s$, $1 < n < s$, $r = s^2 - s$;

(ii) матрица зашифрования опорного шифра представляет собой таблицу вида $A(s, n)$;

(iii) распределение вероятностей $P(\mathbb{N}_r)$ является равномерным.

Тогда шифр Σ_H является совершенным и имитостойким и для любого l выполнены следующие равенства:

$$P_{im}^{l} = \left(\frac{n}{s}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{n-1}{s-1}\right)^{t},$$

т.е. $P_{im}^{l} \to 0$ при $l \to \infty$, $P_{podm}^{l}(t) \to 0$ при $t \to \infty$.

Пример 5. На основе примера 3 построим совершенный имитостойкий шифр Σ_H со следующими характеристиками: $|U| = 3$, $|V| = 4$, $r = 12$ и следующей матрицей зашифрования:

$\mathbb{N}_r \backslash U$	u_1	u_2	u_3
1	01	10	11
2	00	11	10
3	11	00	01
4	10	01	00
5	10	11	01
6	11	10	00
7	00	01	11
8	01	00	10
9	11	01	10
10	10	00	11
11	01	11	00
12	00	10	01

Например, пусть требуется зашифровать сообщение $\overline{u} = u_2u_3u_1$. Для этого необходима ключевая последовательность длины 3. Предположим, что случайный генератор ψ_c сгенерировал последовательность $\overline{j} = 378$. Тогда шифрованное сообщение получается следующим образом: $\overline{v} = E_3(u_2)E_7(u_3)E_8(u_1) = 001101$.

Если распределение вероятностей $P(\mathbb{N}_r)$ является равномерным (генератор ключевых последовательностей вырабатывает равновероятные гаммы), то шифр Σ_H будет являться совершенным и имитостойким, причем

$$P_{im}^{l} = \left(\frac{3}{4}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{2}{3}\right)^{t},$$

причем $P_{im}^{l} \to 0$ при $l \to \infty$, $P_{podm}^{l}(t) \to 0$ при $t \to \infty$.

4. Построение оптимальных кодов аутентификации на основе конечных полей

Пусть $h : K \times X \to Y$ — ключевая криптографическая хеш-функция, где X — конечное множество сообщений, K — конечное множество ключей, Y — конечное множество сверток. Напомним, что *кодом аутентификации* (без сокрытия) называется четверка (X, K, Y, h), для которой выполнено равенство $Y = \bigcup_{k \in K} h_k(X)$.

Как и для случая шифров, рассмотрим понятия имитации и подмены сообщений для кодов аутентификации.

Пусть канал связи готов к работе и на приеме установлены действующие ключи $k \in K$, но в данный момент времени никакого сообщения вида (x, y), где $y = h_k(x)$, не передается. Тогда в этом случае противником может быть предпринята попытка имитации сообщения некоторой парой $(x, y) \in X \times Y$.

Рассмотрим вероятностное пространство $(\Omega = K, F_K, P_K)$. Зафиксируем $(x, y) \in X \times Y$. Обозначим через $K(x, y)$ следующее множество:

$$K(x, y) = \{k \in K \mid h_k(x) = y\}.$$

Под обозначением $K(x, y)$ будем также понимать событие из алгебры событий F_K, заключающееся в том, что при случайном выборе ключа $k \in K$ будет выполнено равенство $h_k(x) = y$. Тогда событию $K(x, y)$ будут благоприятствовать все элементы из множества $K(x, y)$, и только они. Поэтому

$$P(K(x, y)) = \sum_{k \in K(x,y)} P_K(k).$$

Поскольку противник имеет возможность выбора $(x, y) \in X \times Y$, его шансы на успех имитации сообщения выражаются такой величиной:

$$P_{im} = \max_{(x,y) \in X \times Y} P(K(x, y)).$$

Если же в данный момент передается некоторое сообщение вместе со своей сверткой $(x, y) \in X \times Y,\ y = h_k(x)$, то противник может заменить его на $(\widetilde{x}, \widetilde{y}) \in X \times Y,\ \widetilde{x} \neq x$. При этом он будет рассчитывать на то, что на действующем ключе k при проверке будет выполнено равенство $\widetilde{y} = h_k(\widetilde{x})$. Чем больше вероятность этого события, тем успешнее будет попытка подмены. Пусть «$K(\widetilde{x}, \widetilde{y}) \mid K(x, y)$» — событие, заключающееся в попытке подмены сообщения (x, y) сообщением $(\widetilde{x}, \widetilde{y})$. Применяя теорему о произведении вероятностей, получаем, что

$$P(K(\widetilde{x}, \widetilde{y}) \mid K(x, y)) = \frac{P(K(x, y) \cap K(\widetilde{x}, \widetilde{y}))}{P(K(x, y))}.$$

Тогда вероятность успеха подмены сообщения будет вычисляться по следующей формуле:

$$P_{podm} = \max_{\substack{x, \widetilde{x} \in X,\ y, \widetilde{y} \in Y \\ x \neq \widetilde{x}}} P(K(\widetilde{x}, \widetilde{y}) \mid K(x, y)).$$

Теорема 5 ([9]). Для любого кода аутентификации (X, K, Y, h) справедливы следующие утверждения:

(i) $P_{im} \geq \frac{1}{|Y|}$, причем нижняя граница достигается тогда и только тогда, когда для любой пары $(x, y) \in X \times Y$ выполнено равенство $P(K(x, y)) = \frac{1}{|Y|}$.

(ii) $P_{podm} \geq \frac{1}{|Y|}$, причем нижняя граница достигается тогда и только тогда, когда для любых $x, \widetilde{x} \in X,\ x \neq \widetilde{x},\ y, \widetilde{y} \in Y$ выполнено равенство $P(K(\widetilde{x}, \widetilde{y}) \mid K(x, y)) = \frac{1}{|Y|}$.

(iii) P_{im} и P_{podm} одновременно достигают нижней границы тогда и только тогда, когда для любых $x, \widetilde{x} \in X,\ x \neq \widetilde{x},\ y, \widetilde{y} \in Y$ выполнено равенство

$$P(K(x, y) \cap K(\widetilde{x}, \widetilde{y})) = \frac{1}{|Y|^2}.$$

Большой интерес представляют коды аутентификации со свойством $P_{im} = P_{podm} = \frac{1}{|Y|}$. Такие коды называются *оптимальными.* Для описания таких кодов используется понятие ортогональной таблицы.

Теорема 6 ([9]). Пусть код аутентификации (X, K, Y, h) является оптимальным. Тогда верны следующие утверждения:

(i) $|K| \geq |Y|^2$;

(ii) $|K| = |Y|^2$ тогда и только тогда, когда табличное задание хеш-функции h представляет собой ортогональную таблицу $OA(|Y|, |X|)$ над Y и распределение вероятностей P_K является равномерным.

Следствие. *Пусть для кода аутентификации (X, K, Y, h) выполнено равенство $|K| = |Y|^2$. Код аутентификации (X, K, Y, h) является оптимальным тогда и только тогда, когда выполнены следующие условия:*

(i) *табличное задание хеш-функции h представляет собой ортогональную таблицу $OA(|Y|, |X|)$;*

(ii) *распределение вероятностей на множестве K равномерно.*

Пример 6. Пусть $|X| = 5$, $Y = \{00, 01, 10, 11\}$, $|K| = 16$, табличное задание хеш-функции h размера 16×5 над множеством Y представляет собой ортогональную таблицу $OA(4, 5)$ (на основе таблицы $OA(4, 3)$ из примера 3 с добавлением двух строк):

$$\begin{pmatrix} 00 & 00 & 00 & 00 & 01 & 01 & 01 & 01 & 10 & 10 & 10 & 10 & 11 & 11 & 11 & 11 \\ 00 & 01 & 10 & 11 & 00 & 01 & 10 & 11 & 00 & 01 & 10 & 11 & 00 & 01 & 10 & 11 \\ 00 & 01 & 10 & 11 & 01 & 00 & 11 & 10 & 10 & 11 & 00 & 01 & 11 & 10 & 01 & 00 \\ 00 & 01 & 10 & 11 & 10 & 11 & 00 & 01 & 11 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\ 00 & 01 & 10 & 11 & 11 & 10 & 01 & 00 & 01 & 00 & 11 & 10 & 10 & 11 & 00 & 01 \end{pmatrix}^T.$$

При этом строки полученной матрицы пронумерованы элементами множества K, а столбцы — элементами множества X. Тогда если распределение P_K равномерно, то полученный код аутентификации (X, K, Y, h) является оптимальным (см. следствие).

Заметим, что недостатком данной математической модели кода аутентификации являются ограничения, накладываемые на мощности множеств X и K. Рассмотрим математическую модель кода аутентификации без этих ограничений, введенную в работе [10], которая является аналогом математической модели шифров замены с ограниченным и неограниченным ключом, введенной А. Ю. Зубовым в работе [4].

Пусть U, V — соответственно конечные множества возможных кодвеличин и кодобозначений (как аналог шифрвеличин и шифробозначений в модели шифра замены с неограниченным ключом [4]). Перед выработкой кода аутентификации сообщение $x \in X$ предварительно представляется в виде последовательности кодвеличин, которые в процессе выработки кода аутентификации заменяются на кодобозначения. Пусть также имеется конечное множество ключей K и ключевая хеш-функция $h : K \times U \to V$. Процесс выработки кода аутентификации для сообщения $x = u_1...u_l$ на ключе $k_1...k_l$ заключается в замене каждой кодвеличины u_i на кодобозначение v_i в соответствии с ключом k_i, $i = 1, ..., l$. *Опорным кодом* кода аутентификации назовем совокупность $\Delta_H = (U, K, V, h)$, для которой выполнено равенство $V = \bigcup_{k \in K} h_k(U)$.

l-й степенью опорного кода Δ_H назовем совокупность

$$\Delta_H^l = (U^l, K^l, V^l, h^{(l)}),$$

где U^l, K^l, V^l — декартовы степени соответствующих множеств U, K, V; множество $h^{(l)}$ состоит из отображений

$$h_{\overline{k}} : U^l \to V^l, \ \ \overline{k} \in K^l,$$

таких, что для любых $\overline{u} = u_1...u_l \in U^l$, $\overline{k} = k_1...k_l \in K^l$ выполнено равенство

$$h_{\overline{k}}(\overline{u}) = h_{k_1}(u_1)...h_{k_l}(u_l) = v_1...v_l \in V^l.$$

Кодом аутентификации с неограниченным ключом назовем семейство

$$\Delta_H = (\Delta_H^l,\ l \in \mathbb{N};\ \psi_c),$$

где ψ_c — случайный генератор ключевого потока.

Будем говорить, что код аутентификации с неограниченным ключом Δ_H является *оптимальным*, если оптимальным является код Δ_H^l для любого $l \in \mathbb{N}$.

Пример 7. Пусть $U = \{u_1, u_2, u_3, u_4, u_5\}$, $V = \{00, 01, 10, 11\}$, $K = \{k_1, \ldots, k_{16}\}$, табличное задание хеш-функции h размера 16×5 над множеством V представляет собой ортогональную таблицу $OA(4, 5)$ из примера 6. Предположим, что требуется получить свертку для сообщения $\overline{u} = u_4u_2u_5$. В этом случае генератором ключевых последовательностей ψ_c вырабатывается последовательность длины 3, например, $\overline{k} = k_5k_3k_8$. Тогда свертка сообщения $\overline{u}$ будет иметь вид $\overline{v} = h_{k_5}(u_4)h_{k_3}(u_2)h_{k_8}(u_5) = 001001$. В этом случае сообщение $\overline{u}$ вместе со сверткой будет иметь вид $(u_4u_2u_5, 001001)$.

При этом для данного примера

$$P_{im}^l = \frac{1}{4^l},\ \ P_{podm}^l(s) = \frac{1}{4^s},$$

то есть $P_{im}^l \to 0$ при $l \to \infty$, $P_{podm}^l(s) \to 0$ при $s \to \infty$.

При практической реализации для удобства работы с двоичными данными можно в приведенной выше таблице $OA(4, 5)$ вычеркнуть любой столбец и работать с данными $U = V$.

5. Заключение

Шеннон в 40-х годах XX века ввел понятие совершенного шифра, обеспечивающего наилучшую защиту открытых текстов. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте на основе перехваченной криптограммы. При этом хорошо известный шифр гаммирования с равновероятной гаммой является совершенным, но максимально уязвимым к попыткам имитации и подмены. Это происходит потому, что в шифре гаммирования алфавиты для записи открытых и шифрованных текстов равномощны. Для построения совершенных имитостойких шифров и оптимальных кодов аутентификации можно использовать конструкции на основе конечных полей и ортогональных таблиц.

Так как длины ключевых последовательностей рассмотренных выше криптографических объектов не меньше длин передаваемых сообщений, то их целесообразно использовать в исключительно важных случаях.

Литература

1. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.
2. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.
3. *Rivest R. L., Chor B.* A knapsack-type public key cryptosystem based on arithmetic in finite fields // IEEE Transactions on Information Theory. 1988. Vol. 34, № 5. P. 901–909.
4. *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.
5. *Рацеев С. М.* Некоторые обобщения теории Шеннона о совершенных шифрах // Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование. 2015. Т. 8, № 1. С.111–127.

6. *Рацеев С. М., Черепатенко О. И.* Построение совершенных имитостойких шифров на основе полей Галуа // Образование и информационная культура: теория и практика. Выпуск «Кибербезопасность». Материалы межрегионального форума (3 декабря 2015 г.). Ульяновск, 2016. С. 99–101.
7. *Bose R. S.* On the applications of the properties of Galois fields to the problems of construction of Hyper-Graeco-Latin squares // Indian J. Stat. 1938. № 3, Part 4. P. 323–338.
8. *Рацеев С. М., Черепатенко О .И.* О совершенных шифрах на основе ортогональных таблиц // Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование. 2014. Т. 7, № 2. С. 66–73.
9. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009. 272 с.
10. *Рацеев С. М.* Об оптимальных кодах аутентификации // Системы и средства информатики. 2013. Т. 23, № 1. С. 53–57.

Статья поступила в редакцию 18.04.2017;
переработанный вариант – 25.06.2017.

Рацеев Сергей Михайлович
д.ф.-м.н., профессор кафедры информационной безопасности и теории управления Ульяновского государственного университета (432017, Ульяновск, ул. Льва Толстого, 42), e-mail: ratseevsm@mail.ru.

Беспалова Елизавета Евгеньевна
студентка кафедры информационной безопасности и теории управления Ульяновского государственного университета.

Буранкина Полина Вячеславовна
студентка кафедры информационной безопасности и теории управления Ульяновского государственного университета.

Гусарова Мария Андреевна
студентка кафедры информационной безопасности и теории управления Ульяновского государственного университета.

On application of finite fields in some perfect cryptosystems

S. M. Ratseev, E. E. Bespalova, P. V. Burankina, M. A. Gusarova

Constructions of perfect imitation resistant ciphers and authentication codes resistant to imitation and substitution messages are considered in this paper. Finite fields and orthogonal tables are applied in these constructions.

Keywords: cipher, perfect cipher, imitation of the message, authentication code.