Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. 2023, № 2, с. 53-60.

Поступила: 28.11.2023
Окончательный вариант: 28.11.2023

УДК 519.7

Применение конечных полей в криптографии

Макаев А.И., Чернявская В.А. *

*otvet.article@gmail.com
УлГУ, Ульяновск, Россия

В работе приводятся конструкции совершенных шифров и оптимальных кодов аутентификации на основе конечных полей. Также рассматриваются примеры шифрования сообщений и получение свертки для сообщений.

***Ключевые слова**: шифр, конечное поле, совершенный шифр, имитация сообщения, оптимальный код аутентификации.*

Введение

Совершенный шифр обеспечивает наилучшую защиту открытых текстов. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте на основе перехваченной криптограммы. Проблема состоит в том, что такие шифры максимально уязвимы к попыткам имитации и подмены. В данной работе приводится пример реализации построения ортогональных латинских таблиц на основе конечных полей. Данная схема актуальна тем, что на основе полученной таблицы можно строить конструкции совершенных имитостойких шифров.

Коды аутентификации применяются для обеспечения целостности данных и аутентификации источника данных. В данной работе исследуются коды аутентификации, стойкие к имитации и подмене сообщений. Особо выделен случай, когда вероятности имитации и подмены достигают нижних границ. Такие коды аутентификации называются оптимальными. В данной работе приводится пример построения оптимального кода аутентификации на основе ортогональных таблиц в конечном поле. Данная работа основана на работе [3].

1. Латинские квадраты

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.

Теорема 1 (Боуз [2]). Для любого простого p и натурального d существуют $p^d - 1$ ортогональных латинских квадратов.

Известно, что если число s является степенью некоторого простого числа, то в этом случае существуют s − 1 попарно ортогональных латинских квадрата, или, что то же самое, s + 1 ортогональных матриц: для этого достаточно рассмотреть многочлены $f_\alpha(x, y) = \alpha x + y$ над полем GF(s) при ненулевых α [6].

Ортогональной таблицей OA(s, n) над s-элементным 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 [4]. Более подробную информацию можно найти в [1].

Знание понятия ортогональных таблиц поможет нам описать, что же такое оптимальные коды аутентификации и совершенные шифры.

2. Построение конечных полей

Из теории конечных полей известно, что конечное поле из p^n элементов можно построить для любого простого p и натурального n. Чтобы построить поле $GF(p^n)$ нужен неприводимый многочлен степени n с коэффициентами из поля $GF(p)$, где поле $GF(p)$ — привычное кольцо вычетов по модулю p (с точностью до изоморфизма). Неприводимый многочлен является аналогом простого числа, неприводимый многочлен $f(x)$ нельзя представить в виде $f(x) = g(x)h(x)$, где степени многочленов $g(x)$ и $h(x)$ больше нуля (т. е. таких $g(x)$ и $h(x)$ не существует) [3, 5].

3. Оптимальные коды аутентификации

3.1. Коды аутентификации

Кодом аутентификации (без сокрытия) называется четверка (X, K, Y, h), где X — конечное множество сообщений, K — конечное множество ключей, Y — конечное множество сверток, h — ключевая хеш-функция и выполнено равенство

$$Y = \bigcup_{k \in K} h_k(X).$$

Протокол аутентификации, решающий задачи обеспечения целостности сообщения при передаче/хранении, а также аутентификации источника данных для случая доверяющих друг другу сторон, основанный на использовании кода аутентификации (называемый

также схемой имитозащиты), предполагает наличие общего секретного ключа и заключается в передаче одного сообщения (x, a), где $a = h_k(x)$:

$$A \rightarrow B : (x, a).$$

Протокол аутентификации состоит в следующем: участник A для передачи сообщения x вычисляет проверочное значение - код аутентичности сообщения $a = h_k(x)$, дописывает его к x и отправляет полученную пару (x, a) участнику B. Получив такое сообщение, участник B проверяет равенство $a = h_k(x)$: если оно выполнено, то принимает его; если — нет, то отвергает.

Поскольку противник имеет возможность выбора $(x, y) \in X \times Y$, его шансы на успех при 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

$(x, y) \in X \times Y, y = h_k(x)$,

то противник может заменить его на $(\tilde{x}, \tilde{y}) \in X \times Y, \tilde{x} \neq x$. При этом он будет рассчитывать на то, что на действующем ключе k при проверке будет выполнено равенство $\tilde{y} = h_k(\tilde{x})$. Чем больше вероятность этого события, тем успешнее будет попытка подмены. Пусть "$K(\tilde{x}, \tilde{y}) \mid K(x, y)$" — событие, заключающееся в попытке подмены сообщения (x, y) сообщением $(\tilde{x}, \tilde{y})$. Применяя теорему о произведении вероятностей, получаем, что:

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

Тогда вероятность подмены сообщения будет вычисляться по следующей формуле:

$$P_{podm} = \max_{x,\tilde{x}\in X,\ y,\tilde{y}\in Y,\tilde{x}\neq x} P(K(\tilde{x}, \tilde{y}) \mid K(x, y)) \text{ [2].}$$

Теорема 2 ([2]). Для любого кода аутентификации (X, K, Y, h) справедливы следующие утверждения:

1. $P_{im} \geq \frac{1}{|Y|}$, (1)

причем равенство в (1) достигается тогда и только тогда, когда для всех $(x, y) \in X \times Y$ выполнено равенство $P(K(x, y)) = \frac{1}{|Y|}$.

2. $P_{podm} \geq \frac{1}{|Y|}$, (2)

причем равенство в (2) имеет место тогда и только тогда, когда для любых $x, \tilde{x} \in X,\ y, \tilde{y} \in Y,\ \tilde{x} \neq x$ выполнено равенство $P(K(\tilde{x}, \tilde{y}) \mid K(x, y)) = \frac{1}{|Y|}$.

3. P_{im} и P_{podm} одновременно достигают нижней границы ($P_{im} = P_{podm} = \frac{1}{|Y|}$) тогда и только тогда, когда для любых $x, \tilde{x} \in X,\ y, \tilde{y} \in Y,\ \tilde{x} \neq x$ выполнено равенство $P(K(x, y) \cap K(\tilde{x}, \tilde{y})) = \frac{1}{|Y|^2}$.

3.2. Оптимальные коды аутентификации

Коды аутентификации со свойством $P_{im} = P_{podm} = \frac{1}{|Y|}$ называются оптимальными.

Теорема 3 ([2]) (О достаточных условиях оптимального кода аутентификации). Пусть (X, Y, K, h) — некоторый код аутентификации, для которого выполнены следующие условия:

1. $|K| = |Y|^2|K|$;
2. табличное представление порядка |K| × |X| над множеством Y хеш-функции h, в которой строки пронумерованы элементами множества K, а столбцы — элементами множества X, является ортогональной таблицей;
3. распределение вероятностей на множестве K равномерно.

Тогда данный код аутентификации является оптимальным и распределение вероятностей на множестве Y равномерно [4, 6]. Для описания оптимальных кодов аутентификации используется понятие ортогональной таблицы.

Теорема 4 ([2]). Пусть код аутентификации (X, Y, K, h) является оптимальным. Тогда:

1. $|K| \geq |Y|^2$;
2. $|K| = |Y|^2$ тогда и только тогда, когда табличное задание хеш-функции h представляет собой ортогональную таблицу $OA(|Y|, |X|)$ и распределение вероятностей P(K) является равномерным.

Теорема 5 ([2]). Пусть для некоторого 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:

1. табличное представление порядка $|K| \times |X|$ над множеством Y хеш-функции h, в которой строки пронумерованы элементами множества K, а столбцы элементами множества X, является ортогональной таблицей;
2. распределение вероятностей на множестве K равномерно.

Предложение 1 ([6]). Вероятности успехов имитации и успехов подмены для кодов аутентификации (X, K, Y, h) и (X, $\widetilde{K}$, Y,$\tilde{h}$) соответственно равны, в частности, из оптимальности одного кода аутентификации следует оптимальность другого.

3.3. Пример построения оптимальных кодов аутентификации

Пусть X = $\{x_1, x_2, x_3\}$, Y = {00, 01, 10, 11}, K = $\{k_1, \dots, k_{16}\}$, табличное задание хеш-функции h размера 16 × 3 представляет собой ортогональную таблицу OA(4, 3), таблица приведена ниже (таблица 1). Предположим, что требуется получить свертку для сообщения $\bar{x} = x_2x_3x_1$. В этом случае генератором ключевых последовательностей вырабатывается последовательность длины 3, например, $\bar{k} = k_7k_3k_9$. Тогда свертка сообщения $\bar{x}$ будет иметь вид $\bar{v} = h_{k_7}(x_2)h_{k_3}(x_3)h_{k_9}(x_1) = 001010$. В этом случае сообщение будет иметь вид $(x_2x_3x_1, 001010)$.

При этом для данного примера $P_{im} = P_{podm} = \frac{1}{|4|^n}$, то есть с ростом длины сообщения, вероятность имитации и подмены стремится к нулю.

Таблица 1. Ортогональная таблица $OA(4, 3)$ над полем $GF(4)$

K\X	x_1	x_2	x_3
k_1	00	00	00
k_2	01	01	01
k_3	10	10	10
k_4	11	11	11
k_5	01	10	11
k_6	00	11	10
k_7	11	00	01
k_8	10	01	00
k_9	10	11	01
k_{10}	11	10	00
k_{11}	00	01	11
k_{12}	01	00	10
k_{13}	11	01	10
k_{14}	10	00	11
k_{15}	01	11	00
k_{16}	00	10	01

4. Совершенные шифры

Шифр $\sum_B$ называется совершенным (по Шеннону), если для любых $x \in X$ и $y \in Y$ выполняется следующее равенство: $P(x|y) = P(x)$.

Лемма 1 ([2]) (эквивалентные условия совершенных шифров). Для произвольного шифра $\sum_B$ следующие условия эквивалентны:

1. Для любых $x \in X$ и $y \in Y$ выполнено равенство

$P(x|y) = P(x)$;

2. Для любых $x \in X$ и $y \in Y$ выполнено равенство

$P(y|x) = P(y)$;

3. Для любых $x_1, x_2 \in X$ и $y \in Y$ выполнено равенство

$P(y|x_1) = P(y|x_2)$.

Лемма 2 ([2]) (необходимое условие совершенных шифров). Пусть $\sum_B$ — совершенный шифр. Тогда для шифра $\sum_B$ будут выполнены следующие свойства:

1. для любых $x \in X$ и $y \in Y$ найдется такой ключ $k \in K$, что E_k(x) = y (иными словами, для любых $x \in X$ и $y \in Y$ подмножество ключей $K(x,y)$ в K не является пустым);
2. для множеств X, Y и K справедливы следующие неравенства |X| ≤ |Y | ≤ |K|.

Условие 1 леммы 2 эквивалентно тому, что каждый элемент множества Y должен присутствовать во всех столбцах матрицы зашифрования совершенного шифра $\sum_B$.

Теорема 6 (К. Шеннон [2]). Пусть $\sum_B$ — некоторый шифр, для которого выполнено равенство $|X| \leq |Y| \leq |K|$. Шифр $\sum_B$ является совершенным тогда и только тогда, когда выполнены следующие условия:

1. $|K(x,y)| = 1$ для любых $x \in X$ и $y \in Y$;
2. распределение вероятностей $P(K)$ является равномерным, т.е. $P(k) = \frac{1}{|K|}$, для любого $k \in K$.

Пример 1. Рассмотрим пример шифра с равномерным распределение ключей и докажем, что он совершенный. Пусть $\sum_B$ — шифр, определенный множествами:

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

И матрицей зашифрования:

Таблица 2. Матрица зашифрования

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

Для начала докажем, что шифр удовлетворяет необходимым условиям совершенного шифра. Применим лемму 2 и рассмотрим первое условие, из него следует, что каждый элемент множества Y должен присутствовать во всех столбцах матрицы зашифрования совершенного шифра $\sum_B$.

1. $K(x_1, y_1) \neq \emptyset, K(x_1, y_2) \neq \emptyset, K(x_1, y_3) \neq \emptyset, K(x_2, y_1) \neq \emptyset, K(x_2, y_2) \neq \emptyset, K(x_2, y_3) \neq \emptyset$;
2. $|X| \leq |Y| \leq |K| \Rightarrow |2| \leq |3| \leq |3|$.

Получаем, что данный шифр удовлетворяет необходимым условиям совершенного шифра. Перейдем к проверки достаточных условий. Применяя теорему 6 получаем: $|K(x,y)| = 1$ для любых $x \in X$ и $y \in Y$. Иными словами, это условие теоремы обозначает, что в каждом столбце матрицы зашифрования все элементы из Y присутствуют по одному разу.

В пункте втором теоремы сказано о необходимости соблюдения условия равномерного распределения вероятностей. Исходя из формулировки задания P(K) — равномерно.

Таким образом, рассмотренный шифр является совершенным.

5. Пример шифрования на основе совершенных имитостойких шифров

Пусть U = {а, м, й}, Y = {00, 01, 10, 11}, $r = 12$. На основе ортогональной таблицы, приведенной ниже (таблица 3), зашифруем сообщение «май». Для этого необходима ключевая последовательность длины 3. Предположим, что случайный генератор сгенерировал последовательность $\bar{j} = 491$. Тогда шифрованное сообщение получается следующим образом: $y = E_4(\text{м})E_9(\text{а})E_1(\text{й}) = 011111$.

Если распределение вероятностей является равномерным, то шифр будет являться совершенным и имитостойким, причем

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

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

Таблица 3. Ортогональная таблица $OA(4, 3)$ над полем $GF(4)$

$\mathbb{N}_r$\U	а	м	й
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

Заключение

В работе приведено применение оптимальных кодов аутентификации и совершенных шифров на основе конечных полей. Использование конечных полей в криптографии позволяет строить совершенные криптосистемы, вероятность имитации и подмены которых уменьшается с увеличением длины сообщения.

Список литературы

1. *Основы криптографии:* учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2005. 480 с.
2. Рацеев С. М. *Математические методы защиты информации*: учеб. пособие для вузов, 2-е изд., стер. СПб.: Лань, 2023. 544 с.
3. Рацеев С. М., Беспалова Е. Е., Буранкина П. В., Гусарова М. А. О применении конечных полей в некоторых совершенных криптосистемах // *Вестник СибГУТИ*. 2017. № 4, с. 35-44.
4. Рацеев С. М. Об оптимальных кодах аутентификации // *Системы и средства информ*., 2013. Т. 23, № 1 («Проблемы информационной безопасности и надежности систем информатики»), с. 53–57
5. Рацеев С. М. *Элементы высшей алгебры и теории кодирования*: учебное пособие для вузов. Спб.: Лань, 2022. 656 с.
6. Рацеев С.М., Череватенко О.И. О кодах аутентификации на основе ортогональных таблиц // *Вестник Самарского государственного технического университета. Серия Физ.-мат. науки.* 2014. № 4 (37), с. 178-186.

Application of finite fields in cryptography

Makaev, A.I., Chernyavskaya, V.A. *

*otvet.article@gmail.com

Ulyanovsk State University, Russia

The paper presents constructions for constructing perfect ciphers and optimal authentication codes based on finite fields. Examples of message encryption and receiving convolution for messages are also considered.

Keywords*: cipher, finite field, perfect cipher, message imitation, optimal authentication code.*