УДК 519.7

ОБ ОПТИМАЛЬНЫХ КОДАХ АУТЕНТИФИКАЦИИ НА ОСНОВЕ КОНЕЧНЫХ ПОЛЕЙ

ON AUTHENTICATION CODES BASED ON FINITE FIELDS

[1]С.М. Рацеев, [2]О.И. Череватенко
S.M. Ratseev, O.I. Cherevatenko

[1]Ульяновский государственный университет, 432017, г. Ульяновск, ул. Льва Толстого, 42.
Ulyanovsk State University, 432017, Ulyanovsk, Lev Tolstoy 42

E-mail: ratseevsm@mail.ru

[2]Ульяновский государственный педагогический университет имени И.Н.Ульянова, 432063, г. Ульяновск, пл. 100-летия со дня рождения В.И. Ленина, 4.
Ulyanovsk State I.N.Ulyanov Pedagogical University, Ploshchad' 100-letiya so dnya rozhdeniya V.I. Lenina, 4

E-mail: chai@pisem.net

Аннотация
В 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. Приводятся конструкции оптимальных кодов аутентификации на основе ортогональных таблиц.

Abstract
In the work authentication codes resistant to imitation and substitution messages are investigated. The case when the probability of imitation and substitution reach the lower limits has been highlighted. Such authentication codes are called optimal. We study constructions of optimal authentication codes based on orthogonal tables.

Ключевые слова: код аутентификации, имитация сообщения, хеш-функция.
Keywords: authentication code, hash function.

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

Заметим, что потенциальный противник может осуществлять не только пассивные действия относительно передаваемых по каналу связи сообщений, которые заключаются, например в подслушивании или перехвате сообщений, но также и активные атаки, заключающиеся в *имитации* или *подмене* сообщения.

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 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 $(x, y) \in X \times Y$, $y = h_k(x)$, то противник может заменить его на $(x', y') \in X \times Y$, $x' \neq x$. При этом он будет рассчитывать на то, что

на действующем ключе k при проверке будет выполнено равенство $y' = h_k(x')$. Чем больше вероятность этого события, тем успешнее будет попытка подмены. Пусть "$K(x',y')|K(x,y)$" — событие, заключающееся в попытке подмены сообщения (x,y) сообщением (x',y'). Применяя теорему о произведении вероятностей, получаем

$$P(K(x',y')|K(x,y)) = \frac{P(K(x,y) \cap K(x',y'))}{P(K(x,y))}.$$

Тогда вероятность успеха подмены сообщения будет вычисляться по следующей формуле:

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

Теорема 1 [1]. Для любого кода аутентификации (X,K,Y,h), $|Y| = s$, справедливы следующие утверждения:

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

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

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

Напомним, что ортогональной таблицей $OA(s,n,\lambda)$ над множеством $Y = \{y_1,\ldots,y_s\}$ называется матрица порядка $\lambda s^2 \times n$ 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 в λ строках.

Большой интерес представляют коды аутентификации со свойством $P_{im} = P_{podm} = 1/|Y|$. Такие коды аутентификации называются оптимальными. Для описания оптимальных кодов аутентификации используется понятие ортогональной таблицы [2].

Теорема 2 [1]. Пусть код аутентификации (X,K,Y,h) является оптимальным, $|X| = n$, $|Y| = s$. Тогда верны следующие утверждения:

(i) $|K| \geq n(s-1)+1$;

(ii) $|K| = n(s-1)+1$ тогда и только тогда, когда табличное задание хеш-функции h представляет собой ортогональную таблицу $OA(s,n,\lambda)$ при $\lambda = \frac{n(s-1)+1}{s^2}$ и распределение вероятностей P_K является равномерным.

Следствие 1. Пусть для некоторого кода аутентификации (X,K,Y,h), $|X| = n$, $|Y| = s$, *выполнено равенство* $|K| = n(s-1)+1$. 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 $OA\left(s,n,\frac{n(s-1)+1}{s^2}\right)$;

(ii) распределение вероятностей на множестве K равномерно.

Обобщим алгоритм создания ортогональной таблицы из работы [1].

Пусть $F = GF(q)$ — конечное поле из q элементов, $q = p^n$ — степень простого числа p, F^d — векторное пространство размерности d, $d \geq 2$, над полем F. Пусть M — подмножество в F^d, состоящее из попарно линейно независимых векторов над F. Например, множество M можно построить следующим образом.

Рассмотрим следующие подмножества в F^d:

$$M_i = \{(0,\ldots,0,1,x_{i+1},\ldots,x_d) | x_j \in F, j = i+1,\ldots,d\}, .$$

Тогда в качестве M возьмем такое множество: $M = \bigcup_{i=1}^{d} M_i$. Заметим, что

$$|M| = 1 + q + \ldots + q^{d-1} = \frac{q^d - 1}{q-1}.$$

Пусть A — матрица порядка $|F^d|\times|M|$ над F. Пронумеруем строки матрицы A элементами множества F^d, а столбцы — элементами множества M. В матрице A на пересечении строки с номером $x=(x_1,\ldots,x_d)\in F^d$ и столбца с номером $y=(y_1,\ldots,y_d)\in M$ поставим элемент $(x,y)=\sum_{i=1}^{d}x_iy_i\in F$.

Предложение 1. Полученная матрица A является ортогональной таблицей $OA(q,|M|,q^{d-2})$ над F.

Доказательство. Так как любая пара различных элементов множества M является линейно независимой, то для любых $a,b\in F$, $y,z\in M$, $y\neq z$, найдутся ровно q^{d-2} элементов x пространства F^d, для которых система

$$\begin{cases}(x,y)=a,\\(x,z)=b\end{cases}$$

разрешима относительно $x\in F^d$. Это означает, что в любых двух столбцах матрицы A каждая из пар $(a,b)\in F\times F$ встречается ровно $\lambda=q^{d-2}$ раз.

Осталось заметить, что число строк матрицы A равно $q^d=\lambda q^2$. Предложение доказано.

Предложение 2. Пусть табличное задание хеш-функции $h:K\times X\to Y$ представляет собой построенную выше матрицу A и распределение вероятностей на множестве ключей K равномерно. Тогда код аутентификации (X,K,Y,h) является оптимальным.

Доказательство следует из предложения 1 и следствия 1.

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 [3], которая является аналогом математической модели шифров замены с ограниченным и неограниченным ключом, введенную А.Ю. Зубовым в работе [4] и позволяющая строить совершенные имитостойкие шифры [5].

Пусть U, V — соответственно конечные множества возможных кодвеличин и кодобозначений (как аналогия шифрвеличинам и шифробозначениям 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 аутентичности заменяются на кодобозначения. Пусть также имеются конечное множество ключей K и ключевая хеш-функция $h:K\times U\to V$. Процесс выработки кода аутентификации для сообщения $x=u_1\ldots u_l$ на ключе $k_1\ldots k_l$ заключается в замене каждой кодвеличины u_i на кодобозначение v_i в соответствии с ключом k_i, $i=1,\ldots,l$. Опорным кодом кода аутентификации назовем совокупность $\Delta=(U,K,V,h)$, для которой выполнено равенство $V=\bigcup_{k\in K}h_k(U)$.

l-й степенью опорного кода Δ назовем совокупность

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

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

$$h_k:U^l\to V^l,\ k\in K^l,$$

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

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

Кодом аутентификации с неограниченным ключом назовем семейство

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

где ψ_c — случайный генератор ключевого потока.

Для кода аутентификации Δ^l, $l\in\mathbb{N}$, обозначим через $P_{им}^l$ вероятность успеха имитации, а через $P_{подм}^l(t)$ — вероятность успеха подмены в сообщении длины l ровно t элементов множества U элементами множества V.

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

$$P_{im}^{l}=\frac{1}{|V|^{l}},\ P_{podm}^{l}(t)=\frac{1}{|V|^{t}}.$$

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

Так как случайный генератор ψ_c вырабатывает ключевые элементы k_i, $i=1,\ldots,l$, ключа $k_1\ldots k_l$ независимо, то

$$P_{im}^{l}=\left(P_{im}\right)^{l},\ P_{podm}^{l}(t)=\left(P_{podm}\right)^{t},$$

где P_{im} и P_{podm} — соответственно вероятности успехов имитации и подмены опорного кода Δ. Исходя из этого, верна следующая теорема.

Теорема 3. Код аутентификации Δ_H является оптимальным тогда и только тогда, когда опорный код Δ является оптимальным.

Следствие 2. Пусть для кода аутентификации Δ_H, $|U|=n$, $|V|=s$, выполнено равенство $|K|=n(s-1)+1$. Код аутентификации Δ_H является оптимальным тогда и только тогда, когда выполнены следующие условия:

(i) табличное задание хеш-функции h представляет собой ортогональную таблицу $OA\left(s,n,\frac{n(s-1)+1}{s^2}\right)$;

(ii) распределение вероятностей на множестве K равномерно.

Доказательство следует из теоремы 3 и следствия 1.

Теорема 3 дает удобный способ построения оптимальных кодов аутентификации Δ_H. Примером тому служит следующий пример.

Предложение 3. Пусть табличное задание хеш-функции $h: K\times U\to V$ опорного кода Δ представляет собой построенную выше матрицу A и распределение вероятностей на множестве ключей K равномерно. Тогда код аутентификации Δ_H является оптимальным.

Доказательство следует из предложения 2 и теоремы 3.

Список литературы
References

1. Черемушкин А.В. 2009. Криптографические протоколы. Основные свойства и уязвимости. М.: Издательский центр "Академия": 272 .

Cheremushkin A.V. 2009. Cryptographic Protocols: Basic Properties and Vulnerability. Moscow, Akademiia: 272.

2. Рацеев С.М., Череватенко О.И. 2014. О кодах аутентификации на основе ортогональных таблиц // Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки. Т. 37, № 4: 178–186.

Ratseev S.M., Cherevatenko O.I. 2014. On authentication codes based on orthogonal tables. Journal of Samara State Technical University, Ser. Physical and Mathematical Sciences, Vol. 37, № 4: 178–186.

3. Рацеев С.М. 2013. Об оптимальных кодах аутентификации. Системы и средства информатики. Т. 23, № 1: 53–57.

Ratseev S. M. 2013. On optimal authentication codes, Systems and Means of Informatics, vol. 23, № 1.: 53–57.

4. Зубов А.Ю. 2005. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ: 192.

Zubov A. Iy. 2005. Cryptographic Methods of Information Security. Perfect Ciphers. Moscow, Gelios ARV:192.

5. Рацеев С.М. 2015. Некоторые обобщения теории Шеннона о совершенных шифрах. Вестн. ЮУрГУ. Сер. Матем. моделирование и программирование. Т. 8. № 1: 111–127.

Ratseev S.M. 2015. Some generalizations of Shannon's theory of perfect ciphers. Vestnik YuUrGU. Ser. Mat. Model. Progr.. Vol. 8. № 1: 111–127.