УДК 681.3.06

СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ

Г.З. ХАЛИМОВ

Представлены результаты строго универсального хеширования на основе методов ортогональных массивов, независимых массивов и слабосмещенных массивов. Получены оценки параметров семейства хеш-функций строго универсального хеширования. Наилучшие результаты универсального хеширования достигаются на слабо смещенных массивах Вейля-Карлитца-Ушиямы.

Ключевые слова: универсальное хеширование.

Задача построения доказуемо секретной аутентификации впервые сформулирована в работе [1]. Решение было предложено в классе универсальных хеш-функции, как аутентификации с максимальной теоретически достижимой секретностью. В методе универсального хеширования на основе скалярного произведения достигается $P_{\text{кол}} = 1/|B|$, при условии что $|K| = |D|$, а в методе полиномиального хеширования $P_{\text{кол}} \sim \log|D|$, $|K| = |B|$, где $|K|, |D|, |B|$ – мощности пространств ключей, сообщений и хеш-кодов. Идеи универсальной аутентификации получили развитие в теории безусловной аутентификации с использованием строго универсального хеширования [2]. Теория построение массивов строго универсальных аутентификаторов определяется ортогональными массивами. Основной результат строго универсального хеширования состоит в том, что вероятность коллизии $P_{\cdot\geq} = 1/|B|$ достигается при условии $|K| \geq |D||B|$. Применение слабосмещенных массивов для построения почти строго универсальных хеш-функций снимает ограничение на размер ключевого пространства $|K| \geq |B|^2$, но увеличивает при этом вероятность коллизии $P_{\text{кол}} > 1/|B|$. Основное противоречие доказуемо стойкой аутентификации состоит в том, что для обеспечения гарантированной вероятности обмана на уровне нижней границы, размер ключа должен быть не меньше размера сообщения, а фиксирование размера ключа на нижней границе определяемой мощностью пространства хешей приводит к пропорциональному росту вероятности коллизии от длины данных.

Целью статьи является решение задачи построения строго универсального хеширования на основе методов ортогональных массивов, независимых массивов и слабосмещенных массивов. В разделе 1 рассмотрены коллизионные свойства MAC кодов универсального хеширования. В разделе 2 получены оценки параметров строго универсального хеширования на основе ортогональных массивов. В разделе 3 представлено строго универсальное хеширование на основе почти независимых массивов. В разделе 4 приводятся свойства универсального хеширования на основе слабосмещенных массивов.

1. КОЛЛИЗИОННЫЕ СВОЙСТВА MAC КОДОВ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ

MAC коды универсального хеширования определяются массивами с известными статистическими и комбинаторными свойствами, что позволяет, как правило, получить точные коллизионные границы. Основные положения универсального хеширование приведены в работах [1, 2, 3], уточнения и дополнения в [4].

Определение 1 [1]. $(N;n,m)$ хеш-семейство является ε-универсальным, если для любых двух различных элементов $x_1, x_2 \in A$, существует самое большее εN функций $h \in H$ таких, что $h(x_1) = h(x_2)$. Аббревиатура $\varepsilon - U$ используется для обозначения ε-универсальных хеш-функций.

Утверждение 1 [4]. Пусть h выбирается случайно из заданного $\varepsilon - U(N;n,m)$ хеш-семейства, тогда вероятность коллизии хеш-значений для двух разных входных сообщений $x_1, x_2 \in A$ не превышает ε.

Замечание 1.

1. Первоначальное определение универсальных хеш-функций Картера и Вегмана было предложено для $\varepsilon = 1/m$ [1].

2. Вероятность коллизии для универсальных хеш-функций Картера и Вегмана является наименьшей и определяется мощностью пространства хеш-значений $P_{\text{кол}} = 1/|B|$.

Определение 2 [1]. H является ε – почти универсальным семейством хеш-функций ($\varepsilon - AU(N;n,m)$),если $P_{\text{кол}} = \Pr_{h \in H}\left[h(x_1) = h(x_2)\right] \leq \varepsilon$ для $x_1, x_2 \in A$, $x_1 \neq x_2$, $1/m < \varepsilon \leq 1$.

Замечание 2.

1. Для почти универсальных семейств несколько ослабляются требования к вероятности коллизии.

2. Свойство универсальности (почти универсальности) не связанно с распределением MAC значений по ключевому пространству и, следовательно, не определяет вероятностные характеристики имитационной атаки.

3. Универсальное хеширование определяет доказуемо стойкую аутентификацию со счетчиком в представлении Картера – Вегмана [1].

Дальнейшим развитием универсальных схем являются строго универсальные.

Определение 3 [2]. $(N;n,m)$ хеш-семейство является ε-строго универсальным ($\varepsilon - SU(N;n,m)$),

если для каждого $x \in A$ и $y \in B$ число функций $h \in H$, таких, что $h(x) = y$ равно N / m, а для любых двух различных элементов $x_1, x_2 \in A$, и не обязательно различных $y_1, y_2 \in B$ число функций $h \in H$ таких, что $h(x_1) = y_1$, $h(x_2) = y_2$ не превышает $\nu \le \varepsilon \cdot N / m$. Аббревиатура $\varepsilon - SU$ используется для обозначения ε-строго универсальных хеш-функций.

Замечание 3.

1. Строгая универсальность определена для $\varepsilon = 1/m$.

2. При смягчении требования $\varepsilon > 1/m$ класс функций определяется как почти строго универсальный $\varepsilon - ASU$.

3. Строго (почти строго) универсальное хеширование определяет безусловную аутентификацию и было представлено Стинсоном [2,3].

Коллизионные свойства почти строго универсальных MAC кодов представлены следующими утверждениями.

Утверждение 2. Пусть $(N;n,m)$ семейство хеш-функций является $\varepsilon-$ строго универсальным ($\varepsilon - SU(N;n,m)$). Тогда $N \ge m^2$, $P_{8<} = 1/m$ и $P_{?\searrow 4} = 1/m$.

Доказательство. По определению строгой универсальности число функций $h \in H$ таких, что $h(x_1) = y_1$, $h(x_2) = y_2$ не превышает $\varepsilon \cdot N / m$. Возьмём нижнюю границу $\nu = 1$ и, т. к. $\varepsilon = 1/m$, имеем $N \ge m^2$. Прямое вычисление вероятности имитационной атаки по ключу дает $N \ge m^2$ $P_{\text{им.кл}} = (N/m)/M = 1/m$, что соответствует нижней границе для вероятности имитации по MAC коду, следовательно $P_{\text{им}} = 1/m$. Вероятность подмены определяется условной вероятностью. Так как число h для которых $h(x) = y$ равно N/m, а число h для которых $h(x) = y$, $h(x') = y'$ равно $\nu \le \varepsilon \cdot N/m = N/m^2$, получим $P_{\text{под}} = 1/m$.◊

Утверждение 3. Пусть $\varepsilon - ASU(N;n,m)$ семейство почти строго универсальных хеш-функций. При равновероятном выборе хеш-функции вероятность успеха имитационной атаки равна $P_{\text{им}} = 1/m$ и вероятность подмены $P_{\text{под}} \le \varepsilon$.

Доказательство аналогично предыдущему.

2. СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ НА ОСНОВЕ ОРТОГОНАЛЬНЫХ МАССИВОВ

Определение 4 [5]. Пусть X, Y являются множествами из k и v элементов, соответственно, и H есть множество функций осуществляющих отображение $f: X \to Y$. *Ортогональным массивом* $OA_\lambda(t,k,v)$ называется массив элементов $y_i \in Y$, со столбцами, соответствующими элементам множества X и строками, определяемыми элементами множества m, в котором для любой выборки из t элементов $y_1, y_2, ..., y_t$ из Y существует только λ функций $f \in m$, для которых справедливо $f(x_i) = y_i$, $i = 1,2,...,t$.

Основная конструкция OA массивов определена теоремой 1.

Теорема 1 [6]. Пусть q простое число, m,n,t — целые числа, $n \ge m$, $2 \le t \le q^n$. Зафиксируем сьюрективное F_q — линейное отображение $\varphi: F_q^n \to F_q^m$. Для каждого t набора $(z, a_1, a_2, ..., a_{t-1})$, где $z \in F_{q^m}$, $a_j \in F_{q^n}$, $i = 1,2,...,t-1$, определим отображение $f = f(z, a_1, a_2, ..., a_{t-1}): F_q^n \to F_q^m$, вида

$$f(x) = \varphi\left(\sum_{j=1}^{t-1} a_j x^j\right) + z. \qquad (1)$$

Тогда массив, составленный из отображений вида (1) является ортогональным с параметрами $OA_{q^{(t-1)(n-m)}}(t, q^n, q^m)$.

Следствие 1. Пусть q — простое число, $n = m$, $t = 2$. Тогда $OA_{\lambda=1}(2, q^m, q^m)$ называется простым, каждая строка повторяется только (точно) один раз и определяется линейным отображением $\varphi: F_q^m \to F_q^m$ с функцией $f(x) = \varphi(ax) + z$, где $a, z \in F_{q^m}$.

Метод ортогональных массивов можно применить для построения строго универсальных хеш-функций. Основной результат представлен в теореме 2.

Теорема 2 [4]. Пусть q — простое число, a, b, k — целые числа, $a > b$. Тогда существует $\frac{k}{q^b} - SU(q^{a+b}, q^{ka}, q^b)$ семейство хеш-функций.

Замечание 4.

1. Если $k = 1$ имеем строго универсальный класс хеш-функций $\frac{1}{q^b} - SU(q^{a+b}, q^a, q^b)$. Размер ключевых данных N определяется произведением пространства аутентификаторов и пространства сообщений, что уточняет ранее полученную границу утверждения 2.

2. Для почти строго универсального хеширования снижаются требования к размеру ключевых данных, которое ограничивается размерами поля вычислений F_{q^a} и F_{q^b}.

Пример 1 [4]. Пусть $q = 2$, $a = 4$, $b = 2$. Построить строго универсальный класс хеш-функций.

Построим простой ортогональный массив $OA_{q^{(a-b)}}(2, q^a, q^b)$ с помощью линейного отображения $\varphi: F_2^4 \to F_2^2$ с функцией $f(x) = \varphi(ax) + z$. Ортогональный массив будет иметь вид матрицы, в которой строки определяются функциями f_j с параметрами $a_i \in F_{2^4}$, $z_i \in F_{2^2}$, столбцы — значениями $x_i \in F_{2^4}$, а элементы — значениями $y_i \in F_{2^2}$. Существует самое большее $\lambda = 4$ функций, для которых справедливо $f(x_1) = y_1$ и $f(x_2) = y_2$. Данный ортогональный массив является семейством строго универсальных хеш-функций. По определению 3 имеем следующие параметры. Общее число функций $N = 64$. Число записей со значением у в каждом столбце матрицы отображения $X \to Y$ встречается $\frac{N}{2^m} = 16$ раз. Число функций $f \in H$ таких, что $f(x_1) = y_1$, $f(x_2) = y_2$ не превышает $v \le 4$, т. к. $\lambda = 4$. Вероятность коллизии ε будет равна

$\varepsilon \cdot \frac{N}{2^b} = \lambda$, $\varepsilon = \frac{1}{4}$ и имеем $\frac{1}{4} - SU(64,16,4)$ семейство хеш-функций.

Утверждение 5. Линейное отображение $\varphi: F_{q_1} \to F_{q_2}$ с функцией $f(x) = \varphi(ax) + z$, где q_1 и q_2 — простые числа, $q_1 > q_2$, $a \in F_{q_1}$, $z \in F_{q_2}$ приводит к почти строго универсальному хешированию $\frac{2}{q_2} - ASU(q_1 q_2, q_1, q_2)$.

Действительно, пусть q_1 и q_2 — простые числа, $q_1 > q_2$, $t = 2$. Тогда $OA_{\lambda=\lceil q_1/q_2 \rceil}(2, q_1, q_2)$ — массив, каждая строка которого повторяется самое большее $\lambda = \lceil q_1 / q_2 \rceil$ раза, где $\lceil q_1 / q_2 \rceil$ определяет округление к большему целому. Вероятность коллизии ε по определению строгой универсальности будет равна $\varepsilon \cdot \frac{N}{q_2} = \lambda$, $N = q_1 q_2$, $\varepsilon = \lambda / q_1 = \lceil q_1 / q_2 \rceil / q_1 \le 2 / q_2$ и получим почти строго универсальное хеширование $\frac{2}{q_2} - ASU(q_1 q_2, q_1, q_2)$. ◊

Замечание 5.

1. Теорема 2 определяет строго универсальное хеширование $\frac{1}{q^m} - SU(q^{n+m}, q^n, q^m)$ над расширенным полем (см. утверждение 3 [4]).

2. Линейное отображение $\varphi: F_q^n \to F_q^m$ определяет умножение элементов в F_{q^n}, проектирование m координат $F_{q^n} \to F_{q^m}$ и сложение в F_{q^m} (см. пример 1).

3. Линейное отображение $\varphi: F_{q_1} \to F_{q_2}$, где q_1 и q_2 — простые числа, определяет отображение простого конечного поля на простое поле меньшей размерности.

3. СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ НА ОСНОВЕ ПОЧТИ НЕЗАВИСИМЫХ МАССИВОВ

Обобщением ортогональных массивов являются почти независимые массивы (almost independent arrays). Теория почти независимых массивов снимает ограничение на равновероятное распределение наборов хешей по столбцам массива. Почти независимые массивы были рассмотрены Стинсоном [2,3] и в рамках этой теории были определены многократные или t связные коды аутентификации.

Определение 5 [7]. Пусть $0 \le \varepsilon \le 1$. Массив $(n,k)_p$ является t — связным, ε — зависимым (ε — dependent), если для любого набора U из $s \le t$ столбцов и каждого вектора $a \in F_p^s$ частота $v_U(a)$ появления в столбцах значения a удовлетворяет условию $\left| \frac{v_U(a)}{n} - \frac{1}{p^s} \right| \le \varepsilon$.

Замечание 6. Если массив $(n,k)_p$ является t-связным, независимым (0-зависимым), тогда по определению имеем $v_U(a)/n = 1/p^t$. В этом случае $(n,k)_p$ является ортогональным массивом силы t и образует t-строго универсальное семейство хеш-функций [7, 8].

Утверждение 6 [8]. Пусть $(n,k)_p$ — массив, содержащий n строк, k столбцов и записи из набора p элементов. Для $\forall a \in F_p$ частота $v_a(u)$ появления значения a в столбцах массива $u = (u_1, u_2, ..., u_n) \in F_p^n$ удовлетворяет условию $\left| v_a(u)/n - 1/p \right| \le \varepsilon_1$ и для любых пар столбцов u, u' частота $v_{a,a'}(u,u')$ появления в столбцах значений a и a' удовлетворяет условию $\left| v_{a,a'}(u,u')/n - 1/p^2 \right| \le \varepsilon_2$. Тогда $(n,k)_p$-массив есть семейство $\varepsilon - ASU(n,k,p)$ хеш-функций и $\varepsilon = (p^{-2} + \varepsilon_2)/(p^{-1} - \varepsilon_1)$.

Доказательство. Параметр ε определяется условной вероятностью появления любых записей a, a' для различных столбцов u, u' при равновероятном выборе i строки $\varepsilon = \Pr(u'_i = a' / u_i = a)$. По формуле полной вероятности имеем

$$\Pr(u'_i = a' / u_i = a) = \Pr(u_i = a, u'_i = a') / \Pr(u_i = a).$$

Вероятность появления в произвольно выбранном столбце значения a определяется, как $\Pr(u_i = a) = v_a(u)/n$ и с условием ограничения $\left| v_a(u)/n - 1/p \right| \le \varepsilon_1$ удовлетворяет неравенству

$$p^{-1} - \varepsilon_1 \le \Pr(u_i = a) \le p^{-1} + \varepsilon_1.$$

Аналогично для вероятности

$$\Pr(u_i = a, u'_i = a') = v_{(a,a')}(u,u')/n$$

имеем $p^{-2} - \varepsilon_2 \le \Pr(u_i = a, u'_i = a') \le p^{-2} + \varepsilon_2$.

Максимальное значение условной вероятности $\Pr(u'_i = a' / u_i = a) = (p^{-2} + \varepsilon_2)/(p^{-1} - \varepsilon_1)$ получим, подставляя выражение для полной вероятности

$$\Pr(u_i = a) = p^{-1} - \varepsilon_1 \text{ и } \Pr(u_i = a, u'_i = a') = p^{-2} + \varepsilon_2. \text{ ◊}$$

Замечание 7.

1. Параметр ε-зависимость характеризует отклонение от равномерного распределения совместных вероятностей появления кодовых комбинаций в t произвольных столбцах случайно выбранной строки $(n,k)_p$ массива. В теории безусловной аутентификации Стинсона $t = 2$ и рассматривается ASU_2 аутентификация.

2. Как следует из утверждения 6, значение параметра зависимости ε определяет вероятность коллизии MAC кодов и в общем случае, как показано в [9], коллизионные свойства t-кратных кодов аутентификации. Практическое построение почти независимых массивов является проблематичным, т. к. нужны методы, которые позволяют формировать массивы хешей с заданными распределениями по столбцам. В этом отношении для построения строго универсальных хеш-функций более продуктивным является применение слабо смещенных массивов.

4. СТРОГО УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ НА ОСНОВЕ СЛАБОСМЕЩЕННЫХ МАССИВОВ

Слабо смещённые массивы впервые были введены в работах [10, 11] для массивов дискретных значений большой размерности с распределением незначительно отличающимся от равномерного.

Слабо смещённые массивы определяют свойства распределений хешей в столбцах массива [8].

Определение 6. Пусть p - — простое число, $u=(u_1,u_2,...,u_n)\in F_p^n$. Для $\forall i\in F_p$, $v_i(u)$ есть частота появления элемента i в последовательности u $v_i(u)=\frac{n}{p}+\delta_i(u)$, где $\delta_i(u)$ — отклонение частоты $v_i(u)$ от среднего значения и $\sum_{i\in F_p}\delta_i(u)=0$.

Пусть ξ — комплексный корень p-степени из единицы, тогда смещение вектора u определяется как

$$bias(u)=\frac{1}{n}\left|\sum_{i\in F_p}\delta_i(u)\xi^i\right|=\frac{1}{n}\left|\sum_{i\in F_p}v_i(u)\xi^i\right|.$$

Смещение $bias(u)$ имеет следующие свойства.

Утверждение 7 [8]. Для произвольного вектора u $0\le bias(u)\le 1$ и $bias(u)=1$ только тогда, когда $u=const$.

Определение 7. Пусть $(n,k)_p$ — массив, содержащий n строк, k столбцов и записи из набора p элементов и $0\le\varepsilon\le 1$. Массив $(n,k)_p$ является ε-смещённым (ε-biased), если любая нетривиальная линейная комбинация столбцов имеет смещение $bias\le\varepsilon$.

Замечание 7.

1. Смещение массива является свойством F_p — линейного кода, построенного с помощью столбцов порождающей матрицы.

2. Для двоичных массивов параметр ε смещения прямо связывается с вероятностями появления 0 и 1 в столбцах массива.

3. Для строго универсального класса, массив хеш-значений определяется $(n,k)_p$ массивом со смещением равным нулю [8].

Утверждение 1.11 [8]. Пусть (n,k) двоичный ε-смещённый массив, содержащий n строк, k столбцов, тогда вес Хемминга ω любой нетривиальной линейной комбинации столбцов удовлетворяет неравенству

$$\frac{1-\varepsilon}{2}\le\frac{\omega}{n}\le\frac{1+\varepsilon}{2}.$$

Пусть ω_i вес Хемминга нетривиальной линейной комбинации u_i столбцов двоичной матрицы (n,k). Тогда $v_1(u)=\omega_i$, $v_0(u)=n-\omega_i$ и по определению 6 получим

$$\frac{1}{n}\left|\sum_{i\in F_p}v_i(u)\xi^i\right|=\frac{1}{n}\left|v_0\xi^0+v_1\xi^1\right|=$$

$$=\frac{1}{n}\left|n-2\omega_i\right|\le\varepsilon \text{ или } \frac{1-\varepsilon}{2}\le\frac{\omega_i}{n}\le\frac{1+\varepsilon}{2}. \qquad \Diamond$$

В общем случае, когда $p\ne 2$ прямого соответствия между смещением и вероятностью появления символов в столбцах массива нет.

Практическим методом построения слабосмещенных массивов является метод сумм экспонент Вейля- Карлитца- Ушиямы (ВКУ).

Определение 8 [12]. Метод сумм экспонент ВКУ определяет массив $(p^f,f\cdot(n-n/p))_p$ со смещением $bias\le(n-1)p^{-f/2}$, с записями вида $Tr(a_j\alpha^i)$, где a_j — базис поля $F_{p^f}\left|F_p\right.$, $i\le n$ и i не кратно p, $Tr;F_{p^f}\to F_p$ — след элемента $a_j\alpha^i$.

Пример 2 [8]. Построить массив ВКУ $(p^f,f\cdot(n-n/p))_p$ со смещением $bias\le(n-1)p^{-f/2}$ при $p=2,f=4,n=1$. Базисные элементы поля имеют вид $a_j:1,\alpha,\alpha^2,\alpha^3$. Так как $n=1$, следует взять только одну экспоненту $\varphi:X$. Строки массива индексируются элементами $\alpha\in F_{2^4}$, столбцы — функциями: $X,\alpha X,\alpha^2X,\alpha^3X$, а записи — $Tr(\beta)=\beta+\beta^2+\beta^4+\beta^8$. Получим $(2^4,4)$ массив со смещением $bias=(1-1)2^{-2}=0$.

Пример 3. Построить массив ВКУ $(p^f,f\cdot(n-n/p))_p$ со смещением $bias\le(n-1)p^{-f/2}$ при $p=3,f=2,n=2$. Тогда $a_j:1,\alpha$, $\varphi:X,X^2$ и $Tr(\beta)=\beta+\beta^3$. Строки массива индексируются элементами $\alpha\in F_{3^2}$ (порождающий многочлен поля z^2+z+2), столбцы — функциями: $X,\alpha X,\alpha X^2,X^2=\alpha^4X+1 \pmod{X^2+X+2}$. Массив $(3^2,4)_3$ имеет вид, представленный в табл. 1.

Таблица 1

Слабосмещенный массив ВКУ $(3^2,4)_3$

α^i	X	αX	X^2	αX^2
0	0	0	0	0
α^0	α^4	α^4	α^4	α^4
α^1	α^4	0	0	α^4
α^2	0	α^4	α^0	α^0
α^3	α^4	α^0	0	α^0
α^4	α^0	α^0	α^4	α^4
α^5	α^0	0	0	α^4
α^6	0	α^0	α^0	α^0
α^7	α^0	α^4	0	α^0

Зададим произвольную линейную комбинацию столбцов $Y=\sum_{j=1}^{4}\gamma^jY_j$, $\gamma^j\in F_3$, например, $Y=Y_1+\alpha^4Y_2+\alpha^4Y_4$. Получим результирующий вектор

$$Y_p=(0,\alpha^0,0,0,0,\alpha^0,\alpha^4,\alpha^0,\alpha^0).$$

Значения частот элементов $0,\alpha^0,\alpha^4$ равны: $v_0=4$, $\delta_0=+1$, $v_{\alpha^0}=4$, $\delta_{\alpha^0}=+1$, $v_{\alpha^4}=1$, $\delta_{\alpha^4}=-2$, а смещение

$$bias(v_Y)=\frac{1}{9}\left|1\cdot e^{j\frac{2\pi}{3}\cdot 0}+1\cdot e^{j\frac{2\pi}{3}\cdot 1}+(-2)\cdot e^{j\frac{2\pi}{3}\cdot 2}\right|=$$

$$=\frac{1}{9}\left|1-\frac{1}{2}+\frac{\sqrt{3}}{2}j+1+\sqrt{3}j\right|=\frac{1}{3}.$$

Для всех нетривиальных линейных комбинаций столбцов значение $bias\le\frac{1}{3}$ и $bias\le p^{-1}$.

Замечание 9.

1. Пусть $f=2$, $n=1$, тогда имеем $(p^2,2)_p$. Строки массива индексируются элементами $\alpha\in F_{p^2}$, столбцы — функциями: $X,\alpha X$, записи — $Tr(\beta)=\beta+\beta^p$. Значение смещения столбца $bias\le(n-1)p^{-f/2}$ будет равно 0. Можно показать,

что если $f\cdot(n-n/p)$ чуть меньше 2, верхняя граница смещения массива $(p^2,2)_p$ $bias\le p^{-1}$.

2. Линейная комбинация столбцов массива $(p^2,2)_p$ $Y=\sum_{j=1}^{2}\gamma^j Y_j$, $\gamma^j\in F_p$ имеет смещение $bias=0$ и значение $Y+\eta$ в строке индексированной α, η, $\alpha\in F_{p^2}$, $\eta\in F_p$ определяет строго универсальный класс $\frac{1}{p}-SU(p^3,p^2,p)$. Это совпадает с результатами теоремы 2.

3. Пусть $f=2$, $n=2$, тогда имеем $(p^2,4)_p$. Строки массива индексируются элементами $\alpha\in F_{p^2}$, столбцы – функциями: $X,\alpha X,X^2,\alpha X^2$, записи – $Tr(\beta)=\beta+\beta^p$. Если $f\cdot(n-n/p)$ строго равняется 4, значение смещения будет точно равно $bias=p^{-1}$. Можно показать, что если $f\cdot(n-n/p)$ чуть меньше 4, верхняя граница смещения массива $(p^2,4)_p$ $bias\le 2/p$. Линейная комбинация столбцов массива $(p^2,4)_p$ $Y=\sum_{j=1}^{4}\gamma^j Y_j$, $\gamma^j\in F_p$, имеет смещение $bias\le 1/p$ и значение $Y+\eta$ в строке индексированной α, η, $\alpha\in F_{p^2}$, $\eta\in F_p$ определяет почти строго универсальный класс $\frac{1}{p}-ASU(p^3,p^4,p)$.

4. В случае $f=1$, $n=1$, имеем простой ортогональный массив $(q,1)_q$ с линейным отображением $\varphi: F_q\to F_q$ и функцией $f(x)=\varphi(ax)+z$, где $a,z\in F_q$.

Теорема 3 [9]. Если массив является t-связным и ε-смещенным, он является также и t-связным и ε'-зависимым, причём, $\varepsilon'<\varepsilon$.

Фундаментальное значение этой теоремы заключается в том, что она определяет возможность применения слабо смещённых массивов в схемах аутентификации.

Теорема 4 [7]. Пусть $(n,k)_p$ – массив со смещением ε_0 и $t\le k$. Тогда существует $\varepsilon-ASU_2(p^t n,p^k,p^t)$ универсальное хеширование, где $\varepsilon=p^{-t}+\varepsilon_0$.

Отличие схемы ASU_2 по теореме 4 состоит в том, что используется специальное индексирование строк массива аутентификаторов и записей, что увеличивает пространство ключей и записей, и приводит к лучшим оценкам параметров аутентификации.

ВЫВОДЫ

1. Практическим методом построения строго универсального семейства хеш-функция на основе слабосмещенных массивов является метод сумм экспонент Вейля — Карлитца — Ушиямы.

2. Универсальное хеширование по теореме 4 определяется через слабосмещённые массивы, является обобщением конструкций линейных кодов, ВКУ массивов.

Литература

[1] Carter J. L. Universal classes of hash functions /J. L.Carter, M.N.Wegman // Journal of Computer and Systems Science. – 1979. – V.18. – P. 143-154.

[2] Stinson D.R. Combinatorial techniques for universal hashing / D.R.Stinson //Journal of Computer and Systems Science. – 1994. – V.48. – P.337-346.

[3] Stinson D.R. Universal hashing and authentication codes. / D.R.Stinson // Designs, Codes and Cryptography. –1994. – N. 4. – P.369–380.

[4] Халимов Г.З. Аутентификация и универсальное хеширование / Г.З.Халимов, А.А.Кузнецов // Радиотехника. Всеукр. межвед. науч.-техн. сб. – 2001. – Вып. 119. – С. 88-94.

[5] Mukhopadhyay A.L. Construction of some series of ortogonal array / A.L. Mukhopadhyay //Sankya B43. – 1981. – P. 81-92.

[6] Bierbrauer J. Bounds on orthogonal arrays and resilient functions / J.Bierbrauer //Journal of Combinatorial Designs. – 1995. – N. 3. –P. 179–183.

[7] Bierbrauer J. Weakly biased arrays, almost independent arrays and error-correcting codes / J.Bierbrauer, H.Schellwat //Publication in Proceedings of AMS-DIMACS. – 2000. – P.33.

[8] Халимов Г.З. Безусловная аутентификация с использованием слабосмещенных массивов / Г.З. Халимов // Радиотехника. Всеукр. межвед. науч.-техн. сб. Тем. выпуск «Информационная безопасность». – 2003. – № 134. – С. 165–171 .

[9] Kurosawa K. Almost k-wise independent sample spaces and their cryptologic applications / K.Kurosawa, T.Johansson, D.Stinson // Lecture Notes in Computer Science. – 1997. – N. 1233. – P. 409–421.

[10] Alon N. Simple constructions of almost k-wise independent random variables / N.Alon, O.Goldreich, J.Hastad, R.Peralta //Random Structures and Algorithms. – 1992. – N. 3. – P. 289–304.

[11] Naor J. Small-bias probability spaces: efficient constructions and applications / J.Naor, M.Naor //SIAM Journal on Computing. – 1993. – N. 22. – P. 838–856.

[12] Carlitz L. Bounds for exponential sums / L.Carlitz, S.Uchiyama // Duke Mathematical Journal. – 1957. – N. 24. – P. 37–41.

Поступила в редколлегию 15.03.2013

Халимов Геннадий Зайдулович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Научные интересы: методы и средства аутентификации данных.

УДК 681.3.06

Суворо універсальне гешування / Г.З. Халімов// Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 220–224.

Наведено результати суворо універсального гешування на основі методів ортогональних масивів, незалежних масивів і слабко зміщених масивів. Отримано оцінки параметрів сімейства геш-функцій суворо універсального гешування. Найкращі результати універсального гешування досягаються на слабко зміщених масивах Вейля-Карлітца-Ушіями.

Ключові слова: універсальне гешування.

Табл.: 01. Бібліогр.: 12 найм.

UDC 681.3.06

Strongly universal hashing / G.Z. Khalimov // Applied Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 220–224.

This paper presents the results of strongly universal hashing based on the methods of orthogonal arrays, independent arrays and weakly biased arrays. Estimates of parameters of a hash functions family of strongly universal hashing are obtained. The best results of universal hashing are achieved on Weil-Carlitz-Uchiyama weakly biased arrays.

Keywords: universal hashing.

Tab.: 01. Ref.: 12 items.