УДК 681.3.06

Г.З. Халимов

Харьковский национальный университет радиоэлектроники, Харьков

БЕЗУСЛОВНАЯ АУТЕНТИФИКАЦИЯ С УНИВЕРСАЛЬНЫМ ХЕШИРОВАНИЕМ ПО МАКСИМАЛЬНЫМ КРИВЫМ

Представлено решение задачи построения безусловной аутентификации с универсальным хешированием по максимальным кривым в композиционной схеме с ортогональными и слабо смещенными массивам.

Ключевые слова: *максимальные кривые, универсальное хеширование, ортогональные массивы, слабо смещенные массивы.*

Введение

Безусловная аутентификация впервые представлена Стинсоном [1] и определяется семейством хеш функций в классе почти строго универсального хеширования связности 2. Наилучший результат достигается в композиционном хешировании [2]. Применение в первом каскаде эффективной функции сжатия с универсальным хешированием по алгебраическим кривым и во втором каскаде строго универсального хеширования на основе больших массивов с почти равновероятным распределением значений обеспечивает компромисс между ключевыми затратами на аутентификацию и верхним значением вероятности коллизии. Основные результаты по схемам композиционного хеширования представлены в работах [3, 4]. В работах [3, 4] рассмотрены оценки параметров схем строго универсального хеширования на основе ортогональных и слабо смещенных массивов. Граничные оценки параметров для композиционных схем со слабо смещенными массивами представлены в [3]. Универсальное хеширование по алгебраическим кривым представлено в [5], результаты хеширования по максимальным кривым в [6-8]. Актуальным является построение безусловной аутентификации по максимальным кривым в композиционной конструкции со строго универсальным хешированием.

Целью статьи является построение и оценка параметров строго универсального хеширования по максимальным кривым. В разделе 1 рассмотрены граничные оценки универсальной аутентификации. В разделе 2 представлены результаты строго универсального хеширования по максимальным кривым в композиционной схеме с ортогональными и слабо смещенными массивами.

1. Граничные оценки универсальной аутентификации

Определение 1 [3]. Массив аутентификаторов $(n,k)_p$ является ε почти строго универсальным ASU_2 если каждый столбец имеет смещение 0 и для двух записей e,e' одной строки в любых столбцах c,c' условная вероятность $Pr(c_i = e \mid c_i' = e') \le \varepsilon$ и равномерном распределении номера строка i.

Замечание 1.

1. Строка массива $(n,k)_p$ определяется значением ключа, столбец - сообщением источника и значение записи является аутентификационным тегом.

2. Определение ASU_2 аутентификации вводится в теории безусловной аутентификации (замечание 9), свойства следуют из утверждения 1.

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

Оценки для параметров схем универсальной аутентификации представлены в работах [3, 9]. Основные результаты следующие.

Теорема 1 [9]. Пусть q - простое число, a, b, k целые числа, $a > b$. Тогда существует $k/q^b - SU(q^{a+b}, q^{ka}, q^b)$ семейство хеш-функций.

Замечание 2.

1. Результат теоремы определяется сьюрективным F_q - линейным отображением $\varphi : F_q^n \to F_q^m$, таким, что для каждого t набора $(z, a_1, a_2, ..., a_{t-1})$, где $z \in F_{q^m}$, $a_j \in F_{q^n}$, $i = 1,2,...,t-1$, существует отображение $f = f(z, a_1, a_2, ..., a_{t-1}) : F_q^n \to F_q^m$, вида

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

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

2. Если $k = 1$ имеем строго универсальный класс хеш-функций $1/q^b - SU(q^{a+b}, q^a, q^b)$. Размер ключевых данных N определяется произведением

пространства аутентификаторов и пространства сообщений, что уточняет ранее полученную границу из утверждения 1. Построение схем строго универсального хеширования описывается теорией ортогональных массивов [9].

3. 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 [9]. Пусть $q=2$, $a=4$, $b=2$. Построим простой ортогональный массив $OA_{q^{a-b}}(2,q^a,q^b)$ с помощью линейного отображения $\phi: F_2^4 \to F_2^2$ с функцией $f(x)=\phi(ax)+z$. Ортогональный массив будет иметь вид матрицы, в которой строки определяются функциями f_i 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 $y_i \in F_{2^2}$. Ортогональный массив $OA_{2^2}(2,2^4,2^2)$ определяет $\frac{1}{4}-SU(64,16,4)$ строго универсальное семейство хеш-функций. Анализ приведенной матрицы показывает, что существует самое большее $\lambda=4$ функций, для которых справедливо $f(x_1)=y_1$ и $f(x_2)=y_2$, так как $z_0=0$, $z_1=1$, $z_2=\beta$, $z_3=\beta^2$. Общее число функций $N=64$. Число записей со значением y в каждом столбце матрицы отображения $X \to Y$ встречается $N/2^m=16$ раз. Число функций $f \in H$ таких, что $f(x_1)=y_1$, $f(x_2)=y_2$ не превышает $v \le 4$, так как $\lambda=4$. Вероятность коллизии ε будет равна $\varepsilon \cdot \frac{N}{2^b}=\lambda$, $\varepsilon=\frac{1}{4}$.

Слабо смещённые массивы для массивов дискретных значений большой размерности с распределением незначительно отличающимся от равномерного впервые были представлены в работах [12,13]. Слабо смещённые массивы определяют свойства распределений хешей в столбцах массива.

Определение 2 [4]. 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 $\delta_i(u)$ - есть 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

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

Определение 3 [4]**.** 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 3. Для строго универсального класса, массив хеш значений определяется $(n,k)_p$ массивом со смещением равным нулю.

Применение слабо смещенных массивов для универсальной аутентификации приводит к следующим оценкам.

Теорема 2. [3] Пусть $f_p(b,e)$ есть минимальное значение a. Тогда существует эффективная конструкция массива $(p^a,p^b)_p$ со смещением $\varepsilon=p^{-e}$ для которого $f_p(b,e) \le 2(b+e)$.

Замечание 4.

1. Строго универсальный класс хеш-функций $1/q^b-SU(q^{a+b},q^a,q^b)$, $a \ge b$ определяется массивом $(p^{a/b+1},a/b)_{p=q^b}$ со смещением $\varepsilon=p^{-1}$. Значение $f_p(b,e)=a/b+1$ и $f_p(b,e)>2(\log_p a/b+1)$, что превышает границу теоремы 2.

2. Граница теоремы 2 реализуется в методе сумм экспонент Вейля- Карлитца- Ушиямы (ВКУ).

Определение 4 [10]. 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 $F_{p^f}|F_p$, $i \le n$ и i не кратно p, $Tr; F_{p^f} \to F_p$ - след элемента $a_j\alpha^i$.

Замечание 5. Строки массива $\left(p^f, f\cdot(n-n/p)\right)_p$ индексируются элементами $\alpha \in F_{p^f}$, а столбцы - функциями a_jX^i, $(n-n/p)$ определяет возможное число экспонент a_jX^i при $i \le n$ и i не кратно p.

Пример 2. 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: $X, \alpha X, \alpha^2 X, \alpha^3 X$, а записи - $Tr(\beta)=\beta+\beta^2+\beta^4+\beta^8$. Получим $(2^4,4)$ массив со смещением $bias=(1-1)2^{-2}=0$.

Пусть $p=3, f=2, n=2$. Тогда $a_j: 1,\alpha$, $\phi: X, X^2$

и $\mathrm{Tr}(\beta)=\beta+\beta^3$. Строки массива индексируются элементами $\alpha\in F_{3^2}$ (порождающий многочлен поля z^2+z+2), столбцы – функциями : $X,\alpha X,\alpha X^2,X^2=\alpha^4X+1 \pmod{X^2+X+2}$. Для всех нетривиальных линейных комбинаций столбцов значение $\mathrm{bias}\le 1/3$ и $\mathrm{bias}\le p^{-1}$.

Замечание 6. Для простого p существует массив ВКУ с параметрами $\left(p^2,2\right)_p$ со смещением $\mathrm{bias}=0$ и массив $\left(p^2,4\right)_p$ со смещением $\mathrm{bias}=1/p$. Это следует из обобщения результатов примера 2.

Теорема 3 [2]. Композиция из универсального класса хеш-функций $\varepsilon_1-U(N_1,n,u)$ и строго универсального класса хеш-функций $\varepsilon_2-SU(N_2,n,m)$ является строго универсальным классом с параметрами $\varepsilon-SU(N_1N_2,n,m)$, где $\varepsilon=\varepsilon_1+\varepsilon_2-\varepsilon_1\varepsilon_2$.

Граничные оценки параметров для композиционных схем со слабо смещенными массивами определяются теоремой 4.

Теорема 4 [3]. Пусть C линейный код определенный над $F_{q=p^m}$ и $\left(p^m,m\right)_p$ -несмещенный массив (включает все m наборы). Тогда справедливы следующее оценки

a) $f_p(b,e)=2(b+e-\log_p m)$ - для кодов РС;

b) $f_p(b,e)\le\frac{5}{3}(b+e)$, $b\ge 2e$ - для кодов Эрмита;

c) $f_p(b,e)\le\frac{3}{2}(b+e)+2$, $b>3e$ - для кодов Сузуки.

Замечание 7.

1. Результат для кодов РС является новым.

Пусть над $F_{q=p^m}$ задан РС код с параметрами $\left(p^m,\varepsilon p^m,p^m-\varepsilon p^m+1\right)_{q=p^m}$, $0<\varepsilon<1$ и пусть $\varepsilon=p^{-e}$. Массив $\left(p^m,m\right)_p$ является несмещенным и $\varepsilon_0=0$. По теореме 3 имеем массив $\left(p^{2m},m\varepsilon p^m\right)_p=\left(p^{2m},mp^{m-e}\right)_p$ со смещением $\varepsilon=1-\delta+\delta\varepsilon_0=1-(1-p^{-e})-p^{-m}<p^{-e}$ и получим

$$f_p(b,e)=2(b+e-\log_p m)=2m,$$

где $b=\log_p(m\cdot p^{m-e})$. ◊

2. Результаты для кодов Эрмита и Сузуки впервые представлены в [3].

3. Применение длинных алгебраических кодов дает лучшие результаты для параметров слабосмещенных массивов по сравнению с ВКУ методом.

Пример 3. Построить слабо смещенный массив с РС кодом в $F_{q=p}4$. Определим РС код с параметрами $\left(p^4,p^3,p^4-p^3+1\right)$ и внутренний массив $\left(p^2,4\right)_p$ (пример 2). Тогда по теореме 3 имеем массив $\left(p^6,4p^3\right)_p$ со смещением

$$\varepsilon=1-\frac{p^4-p^3+1}{p^4}+\frac{p^4-p^3+1}{p^4}*\frac{1}{p}\le\frac{2}{p}.$$

Теорема 4 [3]. Пусть $(n,k)_p$ массив со смещением ε_0 и $t\le k$. Тогда существует $\varepsilon-ASU_2(p^tn,p^k,p^t)$ универсальная аутентификация, где $\varepsilon=p^{-t}+\varepsilon_0$.

Замечание 8.

1. Универсальная аутентификация по теореме 4 устанавливается через слабо смещённые массивы, является обобщением конструкций линейных кодов, ВКУ массивов.

2. Отличие схемы ASU_2 теоремы 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.

2. Оценки параметров композиционной конструкции строго универсального хеширования в квадратичном поле

Замечание 9.

1. Композиционная конструкция для строго универсального хеширования определяется теоремой 3.

2. Наилучший результат универсального хеширования достигается на максимальных кривых в квадратичном поле.

3. Строго универсальное хеширование определяется конструкциями ортогональных и слабо смещенных массивов.

Кривая Эрмита является кривой наибольшего рода, с наибольшим числом точек. Основной результат универсального хеширования по кривой Эрмита определяется утверждением 2.

Определение 5 [11]. Хеш функция $h_{x,y}(m)\in F_{q^2}$ для сообщения m по рациональным функциям в точке x, y кривой Эрмита определяется выражением

$$h_{x,y}(m)=\sum_{i\ge 0,0\le j\le q-1,iq+j(q+1)\le\rho_k} m_{i,j}\cdot x^i\cdot y^j, \quad (2)$$

где ρ_k полюс подгруппы Вейерштрасса $H(P_\infty)$, $m_{i,j}\in F_{q^2}$ -слова сообщения m.

Утверждение 2 [6]. Хеширование по рациональным функциям кривой Эрмита над полем F_{q^2} определяет универсальный хеш класс

$\varepsilon - U(q^3, q^{2k}, q^2)$, где q^3 - число хеш функций (объём ключевого пространства), q^{2k} - объём пространства сообщений, q^2 - объём пространства хеш кодов. Вероятность коллизии ε определяется соотношениями

$$\varepsilon = k/q^3 + s/q^2 - s(s-1)/(2q^3),$$

если $$k < q(q-1)/2, \quad (3)$$

$$\varepsilon = k/q^3 + 1/(2q) - 1/(2q^2),$$

если $$k \geq q(q-1)/2, \quad (4)$$

где $s = \left\lceil (2k+1/4)^{1/2} - 1/2 \right\rceil$ есть округление значения до наибольшего целого.

Следствие 1. Асимптотика вероятности коллизии универсального хеширования по кривым Эрмита, для случая $k < q(q-1)/2$ при больших значениях размерности поля $q \to \infty$ имеет вид

$$\varepsilon < k/q^3 + \sqrt{2k}/q^2 \quad (5)$$

Замечание 10.

1. Результат (5) следует из оценки поведения выражения для вероятности коллизии (3) при большом значении q, с учетом подстановки

$$s = \left\lceil (2k+1/4)^{1/2} - 1/2 \right\rceil.$$

2. Основные результаты строго универсального хеширования ортогональными и слабо смещенными массивами следуют из примеров 1,2 и замечания 6 и представлены в табл. 1.

Оценки параметров композиционной конструкции хеширования по кривым Эрмита следуют из теоремы 3 и представлены в табл. 2

Таблица 1

Свойства хеш классов построенных на ортогональных и ВКУ массивах

Входные параметры	Определение отображения	Свойства массива	Вычисление хеша	Свойства хеш класса
$OA_q(2, q^2, q)$	$f(x) = \phi(ax) + z$, $\phi: F_q^2 \to F_q^1$	$bias = 0$	$f(x) = \phi(ax) + z$, строка индексируется a, z, $a \in F_{q^2}$, $z \in F_q$	$1/q - SU(q^3, q^2, q)$
$\left(q^2, 2\right)_q$, $f = 2$, $n = 1$	$Y = \sum_{j=1}^{2} \gamma_j Y_j$, $\gamma_j \in F_q$	$bias = 0$	$Y + \eta$, строка индексируется $\alpha, \eta, \alpha \in F_{q^2}, \eta \in F_q$	$1/q - SU(q^3, q^2, q)$
$\left(q^2, 4\right)_q$, $f = 2$, $n = 2$	$Y = \sum_{j=1}^{4} \gamma_j Y_j$, $\gamma_j \in F_q$	$bias \leq 1/q$	$Y + \eta$, строка индексируется $\alpha, \eta, \alpha \in F_{q^2}, \eta \in F_q$	$1/q - ASU(q^3, q^4, q)$

Таблица 2

Оценки параметров композиционной конструкции хеширования по кривой Эрмита

Класс отображения	Универсальный класс $\varepsilon_1 - U(N_1, N, q)$	Строго (почти строго) универсальный класс	Композиционная конструкция
$f(x) = \phi(ax) + z$, $\phi: F_{q^2} \to F_q$, $a \in F_{q^2}$, $z \in F_q$	$\varepsilon_1 - U(q^3, q^{2k}, q^2)$, $\varepsilon_1 < k/q^3 + \sqrt{2k}/q^2$	$\frac{1}{q} - SU(q^3, q^2, q)$	$\varepsilon - SU(q^6, q^{2k}, q)$, $\varepsilon = \sqrt{2k}/q^2 + 1/q$
$\left(q^2, 2\right)_q, \phi: F_{q^2} \to F_q$	$\varepsilon_1 - U(q^3, q^{2k}, q^2)$, $\varepsilon_1 < k/q^3 + \sqrt{2k}/q^2$	$\frac{1}{q} - SU(q^3, q^2, q)$	$\varepsilon - SU(q^6, q^{2k}, q)$, $\varepsilon = \sqrt{2k}/q^2 + 1/q$
$\left(q^2, 4\right)_q$, $\phi: F_{q^2} \to F_q$	$\varepsilon_1 - U(q^3, q^{2k}, q^2)$, $\varepsilon_1 < k/(2q^3) + \sqrt{k}/q^2$	$\frac{1}{q} - ASU(q^3, q^4, q)$	$\varepsilon - ASU(q^6, q^{2k}, q)$, $\varepsilon = \sqrt{k}/q^2 + 1/q$

Выводы

1. Для фиксированного поля вычислений и числа хешируемых слов данных композиционная конструкция с кривыми Эрмита имеет меньшую вероятность коллизии по сравнению с хешированием по проективной прямой. Для фиксированной вероятности коллизии и числа хешируемых слов данных композиционная конструкция с кривыми Эрмита является более эффективной по затратам ключа по сравнению с хешированием по проективной прямой.

Пусть $F_{q_1^2}$ определяет хеширование по кривой Эрмита и $F_{q_2^2}$ - хеширование по проективной кривой. Фиксируем вероятность коллизии

$$\varepsilon = k/q_2^2 = \sqrt{2k}/q_1^2.$$

Отсюда имеем

$$q_2 = q_1 (k/2)^{1/4} \approx q_1 k^{1/4}.$$

Пусть $k = q_1$ и $q_2 = q_1^{1,25}$. Рассмотрим строго универсальное хеширование по кривой Эрмита $\varepsilon - SU(q_1^6, q_1^{2k}, q_1)$, $\varepsilon = \sqrt{2k}/q_1^2 + 1/q_1$ с отображе-

нием $f(x) = \phi(ax) + z$, $\phi : F_{q_1^2} \to F_{q_1}$. Эквивалентное по вероятности коллизии строго универсальное хеширование по проективной прямой $\varepsilon - SU(q_2^5, q_2^{2k}, q_2)$ имеет параметры $\varepsilon - SU(q_1^{6,25}, q_1^{2,5k}, q_1^{1,25})$. Если $k = q_1^2$ и $q_2 = q_1^{1,5}$, тогда $\varepsilon - SU(q_1^{7,5}, q_1^{3k}, q_1^{1,5})$. Чем больше размер хешируемых данных, тем больше выигрыш по ключевому пространству.

2. Вычисления для композиционных конструкций по максимальным кривым второго и третьего рода являются близкими к оценкам хеширования по кривой Эрмита, имеют небольшой проигрыш в 2÷3 раза по вероятности коллизии и соответствующий выигрыш по затратам ключей.

3. Строгое (почти строгое) универсальное хеширование допускает отображение на подполе $\phi : F_{q^2} \to F_q$. Данное отображение является эффективным, когда вероятность коллизии на первом каскаде за счет длины хешируемых данных приближается к значению q^{-1}. С помощью отображения $\phi : F_{q^2} \to F_q$ размер хеш кода приводится к энтропийному значению.

Список литературы

1. Stinson D. Universal hashing and authentication codes. // Stinson D. // Design, Codes and Cryptography, – 1994. – V. 4. –P.369 – 380.

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. 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.

4. Халимов Г.З. Безусловная аутентификация с использованием слабо смещенных массивов / Г.З.Халимов // Радиотехника. Всеукр. межвед. науч. – техн. сб. Тем. выпуск «Информационная безопасность». – 2003. – №134. –С. 165 – 171.

5. Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования / Г.З.Халимов // Материалы XI Международной научно – практической конференции «Информационная безопасность» (Таганрог, Россия, 23 – 25 июня 2010), ТТИ ЮФУ. – 2010. – Ч. 3. – С. 144 – 146.

6. Халимов Г.З. Универсальное хеширование по рациональным функциям кривой Эрмита / Г.З.Халимов, А.Ю.Иохов // Международная научно – практическая конференция «Застосування інформаційніх технологій у підготовці та діяльності сил охорони правопорядку» Академія внутрішніх військ МВС України 17 – 18.03.2011. Зб. тези доповідей. – 2011. – С.48 – 51.

7. Халимов Г.З. Универсальное хеширование по максимальным кривым второго рода / Г.З.Халимов //Тезисы докладов международной конференции, посвященной 50 – летию механико – математического факультета «Современные проблемы математики и её приложения в естественных науках и информационных технологиях» 17 – 22.04.2011. – С. 191 – 192.

8. Халимов Г.З. Универсальное хеширование по рациональным функциям максимальных плоских кривых / Г.З.Халимов, Ю.И.Горбенко // Праці Міжнародної молодіжної математичної школи «Питання оптимізації обчислень (ПОО – XXXVII)», Національна академія наук України, Інститут кібернетики імені В.М. Глушкова, Україна, Крим, Велика Ялта, смт. Кацивелі, 22–29.09.2011. –С. 149 – 151.

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

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

11. Халимов Г.З. Аутентификация с применением эрмитовых кодов / Г.З.Халимов, А.Ю.Иохов // Вестник ХПИ. – Х., НТУ „ХПИ". – 2005. –Вып. 9. –С. 26 – 32.

12. 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.

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

Поступила в редакцию 2.04.2013

Рецензент: д-р техн. наук проф. В.И. Долгов, Харьковский национальный университет радиоэлектроники, Харьков.

БЕЗУМОВНА АВТЕНТИФІКАЦІЯ З УНІВЕРСАЛЬНИМ ГЕШУВАННЯМ ЗА МАКСИМАЛЬНИМИ КРИВИМИ

Г.З. Халімов

Представлено рішення задачі побудови безумовної автентифікації з універсальним гешуванням за максимальними кривими в композиційній схемі з ортогональними і слабо зміщеними масивам

***Ключові слова**: максимальні криві, універсальне хешування, ортогональні масиви, слабо зміщені масиви.*

UNCONDITIONAL AUTHENTICATION WITH UNIVERSAL HASHING ON THE MAXIMAL CURVES

G.Z. Khalimov

The solution of the problem of constructing unconditional authentication with universal hashing on the maximal curves in the composite scheme with orthogonal and weakly biased arrays.

***Keywords:** maximal curves, universal hashing, orthogonal arrays, weakly biased arrays.*