УДК 681.3.06

Г.З. Халимов

Харьковский национальный университет радиоэлектроники, Украина

МНОГОКРАТНОЕ УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО МАКСИМАЛЬНЫМ КРИВЫМ

Представлены оценки вероятности коллизии, и сложности вычислений для многократного хеширования по алгебраическим кривым над конечным полем.

Ключевые слова: *алгебраические кривые, универсальное хеширование.*

Введение

Универсальное хеширование в концепции проективного многообразия по алгебраическим кривым, на основе скалярного произведения по рациональным функциям функционального поля алгебраических кривых представлено в работах [1, 2]. Практическим аспектом универсального хеширования по рациональным функциям алгебраических кривых является увеличение вероятности коллизии с ростом объема хешируемых данных. Стинсон рассмотрел композиционную конструкцию аутентификации на основе универсального и строго универсального классов хеш функций и показал, что такая схема аутентификации является строго универсальным классом [3]. Композиционная конструкция снимает ограничение на размер ключевых данных в малом поле вычислений. Многократное хеширование эффективно снижает вероятность коллизии, но приводит к росту объёма ключевых данных и размера хеш кода.

Построение универсальных хеш функций по алгебраическим кривым с большим числом точек широко представлено в [4 – 9] и позволяет обеспечить большой коэффициент сжатия для входных сообщений большого объёма. Многократное универсальное хеширование по алгебраическим кривым лежит в плоскости выбора хороших алгебраических кривых с большим отношением числа точек к роду кривой, оценки вероятности коллизии, вычислительных затрат на хеширование при фиксированном поле вычислений и размере хеш кода.

Целью статьи является исследование многократного универсального хеширования по алгебраическим кривым над малыми конечными полями с гибким

диапазоном значений длин хешируемых данных. В разделе 1 представлено определение и свойства многократного универсального хеширования. В разделе 2 рассмотрены оценки коллизионной стойкости и вычислительной сложности многократного универсального хеширования по максимальным кривым и кривым с большим числом точек над конечным полем.

1. Определение и свойства многократного универсального хеширования

Хеширование сообщения по нескольким независимо выбранным хеш функциям приводит к уменьшению вероятности коллизии.

Определение 1 [10]. Пусть $H_1 = h:\left\{\{0,1\}^a \to \{0,1\}^b\right\}$ и $H_2 = h:\left\{\{0,1\}^a \to \{0,1\}^c\right\}$ есть классы хеш функций. Класс хеш функций по нескольким независимо выбранным хеш функциям $H_1 \bigcap H_2 = h:\left\{\{0,1\}^a \to \{0,1\}^{b+c}\right\}$ имеет вид

$$(h_1, h_2)(x) = h_1(x) \| h_2(x). \qquad (1)$$

Утверждение 1 [10]. Если H_1 есть $\varepsilon_1 - U$ универсальный класс и H_2 есть $\varepsilon_2 - U$, тогда $H_1 \bigcap H_2$ есть $\varepsilon_1\varepsilon_2 - U$.

Замечание 1.

1. Распространение конструкции (1) на t кратное хеширование приводит к схеме с вероятностью коллизии пропорциональной степени ε^t. Значения хеш кода увеличивается в t раз и сложность вычислений увеличивается в t раз.

2. Особенность вычисления хеш кода по выражению (1) заключается в использовании разных ключей для хеш функций $h_1(x)$ и $h_2(x)$.

Универсальное хеширование определяется проективным многообразием алгебраических кривых имеющим определение над полем F_q.

Определение 2 [1]. Пусть задана абсолютно неразложимая, несингулярная проективная кривая χ над полем F_q с точками $P = \{P_1, P_2, ..., P_n\} \in \chi(F_q)$. Для каждой алгебраической кривой можно определить поле рациональных функций $F_q(\chi)$. В каждой точке P_j кривой χ можно вычислить оценку ϑ_P для рациональных функций $f_i \in F_q(\chi)$, которая определяет порядок нуля или полюса функции f_i в этой точке. Хеш значение $h_{P_j}(m) \in F_q$ для сообщения $m = (m_1, ..., m_k)$, $m_i \in F_q$ в точке $P_j \in F_q$ определяется выражением

$$h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i,$$

где $f_i \in F_q(\chi)$ с упорядоченными порядками полюсов $0 < \rho_1 < ... < \rho_k$. Хеш функция $h_{P_j}(m)$ определяет универсальный хеш класс $\varepsilon - U(N, q^k, q)$, где вероятность коллизии $\varepsilon \le \rho_k / N$, N - число точек алгебраической кривой.

Замечание 2.

1. Ключевой параметр хеш функции $h_{P_j}(m)$ определяется вычислением в точке алгебраической кривой.

2. Наилучший результат универсального хеширования, как следует из оценки вероятности коллизии $\varepsilon \le \rho_k / N$, достигается на максимальных кривых. Для максимальных кривых C над конечным полем достигается максимальное отношение числа точек кривой к роду g. Теорема Хассе-Вейля определяет число F_q рациональных точек кривой $N_q(g) \le 1 + q + 2\sqrt{q}g(C)$.

3. Существуют три замечательных семейства максимальных кривых, которые связываются с Дэлигнэ-Лустига (Deligne-Lusztig) многообразием размерности $\dim = 1$. Кривая Дэлигнэ-Лустига ассоциируется с проективной специальной линейной группой (кривые Эрмита), с группой Сузуки (Suzuki) Sz(q) (кривые Сузуки) и Ри (Ree) группой $R(q)$ [11]. Не существует максимальных кривых над полем F_q рода больше, чем $g > \sqrt{q}(\sqrt{q} - 1)/2$. Важный результат для плоских кривых, который позволяет расширить поиск семейств максимальных кривых, утверждает, что если кривая покрывается максимальной кривой, то она также является максимальной.

4. Наилучшие результаты универсального хеширования по максимальным кривым Эрмита, Судзуки и кривым Ферма представлены в табл. 1.

Замечание 3.

1. Таблица 1 представлена по результатам работ [4-9]. Кривая Эрмита имеет наилучшее отношение числа точек к роду кривой $N_q(g)/g$. Кривые $y^q + y = x^d$ покрываются кривой Эрмита и определяет максимальные кривые второго и третьего рода.

2. Универсальное хеширование по рациональным функциям максимальных плоских алгебраических кривых имеет наилучшие оценки вероятности коллизии. Верхняя граница вероятности коллизии для универсального хеширования $h_{P_j}(m)$ определена в области малых значений $k \le 2g$, g -род кривой и для максимальных кривых является прямо пропорциональной корню квадратному из k.

3. Абсолютно наилучший результат универсального хеширования достигается на кривой Судзуки.

Таблица 1.

Оценки вероятности коллизии и сложности хеш вычислений
по максимальным кривым и кривым с большим числом точек

Уравнение кривой	Определение универсального класса $\varepsilon - U(N,n,m)$ и оценки вероятности коллизии ε, $k < g$	Оценки сложности хеш вычислений
Проективная прямая $X+Y+Z=0$, F_q	$\varepsilon - U(q,q^k,q)$, $\varepsilon = k/q$	k
Кривая Эрмита $y^q + y = x^{q+1}$, F_{q^2}	$\varepsilon - U(q^3,q^{2k},q^2)$, $\varepsilon = k/q^3 + s/q^2 - s(s-1)/(2q^3)$	$k+s$
Максимальные кривые $y^q + y = x^d$, $d \mid q+1$, F_{q^2} $U(q^2+(d-1)(q-1)q, q^{2k}, q^2)$	$\varepsilon - U(q^2+(d-1)(q-1)q, q^{2k}, q^2)$, $\varepsilon = (iq+jd)/(q^2+(d-1)(q-1)q)$	$k+s_1$
Кривая Судзуки $y^q - y = x^{q_0}(x^q - x)$, F_q, $q = 2q_0^2$, $q_0 = 2^s$,	$\varepsilon - U(q^2,q^k,q)$, $\varepsilon = (i(q+2q_0)+j(q+2q_0+1)+t(q+q_0)+rq)/q^2$	$2k+$ $+(3k)^{2/3}/2-1$
Кривая Ферма $X^{(q-1)/3}+Y^{(q-1)/3}+Z^{(q-1)/3}=0$ F_q, $q \equiv 1 \pmod 3$	$\varepsilon - U(2(q-1)^2/9, q^k, q)$, $\varepsilon = 3\left\lceil (2k+1/4)^{1/2} - 1/2 \right\rceil / (2(q-1))$	$k+s$

$s = \left\lceil (2k+1/4)^{1/2} - 1/2 \right\rceil$, $s_1 = \left\lceil (2kd/(q+1)+1/4)^{1/2} - 1/2 \right\rceil$, $\lceil \cdot \rceil$ - *округление к большему целому числу.*

2. Оценки параметров многократного универсального хеширования по алгебраическим кривым

Многократное хеширование H_t которое определяется выражением (1), распространяется на универсальное хеширование по рациональным функциям алгебраических кривых. Рассмотрим универсальное хеширование по алгебраической кривой Ah_{qt}.

Определение 3. Пусть F_q - конечное поле, M – сообщение. Алгоритм вычисления хеш кода с t - кратным универсальное хеширование по алгебраической кривой Ah_q определяется выражением

$$(Ah_{q1}, Ah_{q2}, ..., Ah_{qt})(M) = Ah_{q1}(M) \| Ah_{q2}(M) \| .. \| Ah_{qt}(M). \quad (2)$$

Оценки вероятности коллизии для многократного хеширования определяются свойствами универсального класса $(Ah_{q1}, Ah_{q2}, ..., Ah_{qt})(M)$ в конструкции t связных кодов аутентификации.

Определение 4 [12]. 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 $\nu_U(a)$ появления в столбцах значения a удовлетворяет условию $\left|\nu_U(a)/n - p^{-s}\right| \le \varepsilon$.

Замечание 4.

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 почти строго универсальная аутентификация ASU_2.

2. Значение параметра зависимости ε определяет вероятность коллизии MAC кодов и в общем случае, коллизионные свойства *t* - кратных кодов аутентификации.

Справедливо следующее утверждение.

Утверждение 2. Класс хеш функций $(Ah_{q1}, Ah_{q2}, ..., Ah_{qt})(M)$ является $t - \varepsilon - U$ универсальным.

Доказательство. Пусть M и M' разные сообщения произвольной длины. Для M и M' имеем хеш коды $Ah_{q1}(M) \| Ah_{q2}(M) \| .. \| Ah_{qt}(M)$ и $Ah_{q1}(M') \| Ah_{q2}(M') \| .. \| Ah_{qt}(M')$, соответственно. Рассмотрим один хеш код из общего ряда. По свойству универсальности Ah_{qt} имеем

$$\Pr\left(Ah_{qi}(M) = Ah_{qi}(M')\right) \le \varepsilon. \quad (3)$$

С другой стороны

$$\Pr\left(Ah_{qi}(M) = Ah_{qi}(M')\right) \le \varepsilon = \left|\nu_U(a)/n\right|, \quad (4)$$

где $\nu_U(a)/n$ - частота появления значения a в столбцах массива хеш кодов U, n - число строк массива U или размер ключевых данных. По определению 4, массив хеш кодов U является t - связанным, если для любого набора из $s \le t$ столбцов и каждого вектора a, что определяет хеш код, частота появления в столбцах значения a удовлетворяют условию

$$\left|\nu_U(a)/n - 1/p^s\right| \le \varepsilon, \quad (5)$$

p - размер хеш кода. $\Pr\left(Ah_{qi}(M) = Ah_{qi}(M')\right)$ со-

ответствует случаю $s=1$ и подставляя (3) в (5) имеем неравенство (4). ◊

Оценка вероятности коллизии при многократном Ah_q определяется следующим утверждением.

Утверждение 3. Для t-связанного $\varepsilon-U$ универсального класса по алгебраической кривой при равновероятном выборе хеш функций вероятность коллизии

$$\Pr\begin{bmatrix}(Ah_{q1},Ah_{q2},...,Ah_{qt})(M)=\\(Ah_{q1},Ah_{q2},...,Ah_{qt})(M')\end{bmatrix}\le\varepsilon^t.$$

Доказательство. Действительно, хеш код $Ah_{q1}(M)||Ah_{q2}(M)||..||Ah_{qt}(M)$ представляет конкатенацию хеш результатов Ah_{qt}, $i=1,...,t$. Для каждого из них существует самое большее εn функций $h_i\in Ah_{qi}$ таких, что $Ah_{qi}(M)=Ah_{qi}(M')$ при $M\neq M'$. Так как h_i выбираются независимо и равновероятно из множества Ah_{qt}, тогда для полного хеш кода $Ah_{q1}(M)||Ah_{q2}(M)||..||Ah_{qt}(M)$ существует самое большее $(\varepsilon n)^t$ хеш функций таких, что хеш коды для сообщений M и M' принимают фиксированную пару значений $Ah_{q1}(M)||Ah_{q2}(M)||..||Ah_{qt}(M)$ и $Ah_{q1}(M')||Ah_{q2}(M')||..||Ah_{qt}(M')$. Так как полное значение хеш функций n^t, по соотношению 4 получим оценку для t – связанного $\varepsilon-U$ универсального хеш класса. ◊

Определение 3 и утверждение 3 определяют свойства многократного универсального хеширования по алгебраическим кривым. Применение универсального хеширования по максимальным кривым, Ферма и Сузуки с оценками вероятности коллизий из табл. 1 приводит к коллизионным оценкам многократного хеширования представленными в табл. 2.

Таблица 2

Оценки вероятности коллизии и сложности вычислений
для многократного хеширования по алгебраическим кривым над полем F_q

Уравнение кривой над F_q	t	Вероятность коллизии для данных размером L /сложность вычислений			Размер ключей (бит)	Размер хеш кода (бит)
		1Кбт	1Мбт	1Гбт		
Проективная прямая $X+Y+Z=0$, $q=2^{32}-99$	1	$2^{-24}/2^8$	$2^{-14}/2^{18}$	$2^{-4}/2^{28}$	32	32
	2	$2^{-48}/2^9$	$2^{-28}/2^{19}$	$2^{-8}/2^{29}$	64	64
	3	$2^{-72}/2^{9,58}$	$2^{-42}/2^{19,58}$	$2^{-12}/2^{29,58}$	96	96
	4	$2^{-96}/2^{10}$	$2^{-56}/2^{20}$	$2^{-16}/2^{30}$	128	128
$q=2^{64}-189$	1	$2^{-57}/2^7$	$2^{-47}/2^{17}$	$2^{-37}/2^{17}$	64	64
	2	$2^{-114}/2^8$	$2^{-94}/2^{18}$	$2^{-74}/2^{28}$	128	128
Кривая Эрмита $y^{\sqrt{q}}+y=x^{\sqrt{q}+1}$ $\sqrt{q}=2^{16}+1$	1	$2^{-27,5}/2^8+2^{4,5}$	$2^{-22,5}/2^{18}+2^{9,5}$	$2^{-17,5}/2^{28}+2^{14,5}$	48	32
	2	$2^{-55}/2^9+2^{5,5}$	$2^{-45}/2^{19}+2^{10,5}$	$2^{-35}/2^{29}+2^{15,5}$	96	64
	3	$2^{-82,5}/2^{9,6}+2^{6,1}$	$2^{-67,5}/2^{19,6}+2^{11,1}$	$2^{-52,5}/2^{29,6}+2^{16,1}$	144	96
	4	$2^{-110}/2^{10}+2^{6,5}$	$2^{-90}/2^{20}+2^{11,5}$	$2^{-70}/2^{30}+2^{16,5}$	192	128
$\sqrt{q}=2^{32}-5$	1	$2^{-60}/2^7+2^4$	$2^{-55}/2^{17}+2^9$	$2^{-50}/2^{27}+2^{14}$	96	64
	2	$2^{-120}/2^8+2^5$	$2^{-110}/2^{18}+2^{10}$	$2^{-100}/2^{28}+2^{15}$	192	128
Кривая Ферма $X^{(q-1)/3}+Y^{(q-1)/3}+Z^{(q-1)/3}=0$ $q=2^{32}-99$	1	$2^{-26,89}/2^8+2^{4,5}$	$2^{-21,91}/2^{18}+2^{9,5}$	$2^{-16,9}/2^{28}+2^{14,5}$	62	32
	2	$2^{-53,78}/2^9+2^{5,5}$	$2^{-43,82}/2^{19}+2^{10,5}$	$2^{-33,8}/2^{29}+2^{15,5}$	124	64
	3	$2^{-80,67}/2^{9,6}+2^{6,1}$	$2^{-65,73}/2^{19,6}+2^{11,1}$	$2^{-50,7}/2^{29,6}+2^{16,1}$	186	96
	4	$2^{-107,56}/2^{10}+2^{6,5}$	$2^{-87,64}/2^{20}+2^{11,5}$	$2^{-67,6}/2^{30}+2^{16,5}$	248	128
$q=2^{64}-189$	1	$2^{-59,41}/2^7+2^4$	$2^{-54,41}/2^{17}+2^9$	$2^{-49,41}/2^{27}+2^{14}$	126	64
	2	$2^{-118,82}/2^8+2^5$	$2^{-108,82}/2^{18}+2^{10}$	$2^{-98,82}/2^{28}+2^{15}$	252	128
Кривая Сузуки $y^q-y=x^{q_0}(x^q-x)$ $q=2^{31}$	1	$2^{-27,79}/2^9+2^{5,4}+2^{4,19}$	$2^{-24,46}/2^{19}+2^{12,05}+2^{7,5}$	$2^{-21,13}/2^{29}+2^{18,7}+2^{10,86}$	62	31
	2	$2^{-55,58}/2^{10}+2^{6,4}+2^{5,19}$	$2^{-48,92}/2^{20}+2^{13,05}+2^{8,5}$	$2^{-42,26}/2^{30}+2^{19,7}+2^{11,86}$	124	62
	3	$2^{-83,37}/2^{10,6}+2^7+2^{5,8}$	$2^{-73,38}/2^{20,6}+2^{13,65}+2^{9,1}$	$2^{-63,39}/2^{30,6}+2^{20,3}+2^{12,46}$	186	93
	4	$2^{-111,16}/2^{11}+2^{7,4}+2^{6,19}$	$2^{-97,84}/2^{21}+2^{14,05}+2^{9,5}$	$2^{-84,52}/2^{31}+2^{20,7}+2^{12,86}$	248	124
$q=2^{63}$	1	$2^{-60,13}/2^8+2^{4,72}+2^{3,86}$	$2^{-56,8}/2^{18}+2^{11,39}+2^{7,19}$	$2^{-53,47}/2^{28}+2^{18,05}+2^{10,53}$	126	63
	2	$2^{-120,26}/2^9+2^{5,72}+2^{4,86}$	$2^{-113,6}/2^{19}+2^{12,39}+2^{8,19}$	$2^{-106,94}/2^{29}+2^{19,05}+2^{11,53}$	252	126

Замечание 5. Кратность хеширования t определяется в двух случаях конечного поля 32 и 64 бит. В графах таблицы, где оценивается сложность вычислений, показаны добавки, которые определяют второй проход за схемой вычисления Горнера, в соответствии с ускоренным алгоритмом хеширования по максимальным кривым.

Выводы

1. Многократное хеширование эффективно уменьшает вероятность коллизии, а увеличение размерности поля q увеличивает длину данных хеширования и фиксирует на заданном уровне вероятность коллизии.

2. Применение многократного хеширования приводит к t-кратному увеличению сложности вычислений $N_t = tN_1$, где N_1 – сложность вычисления универсального хеширования по алгебраической кривой.

3. Хеш вычисления по проективной прямой в 32 бит конечном поле является эффективным для малых длин данных. Трёхкратное хеширование обеспечивает $P_{кол} < 2^{-64}$ для данных длиной порядка нескольких Кбт и четырёхкратное хеширование для данных порядка нескольких сотен Кбт. Вычисления в 64 бит конечном поле обеспечивают $P_{кол} < 2^{-64}$ при двухкратном хешировании для всех практических длин данных. Для $P_{кол} < 2^{-128}$ следует использовать трёхкратное хеширование.

4. Хеширование по максимальным плоским кривым в 32 бит конечном поле является эффективным для больших длин данных. Трёхкратное хеширование обеспечивает $P_{кол} < 2^{-64}$ для данных длиной порядка нескольких Мбт и четырёхкратное хеширование для данных порядка нескольких Гбт. Вычисления в 64 бит конечном поле обеспечивают $P_{кол} < 2^{-50}$ при однократном хешировании для практических длин данных и $P_{кол} < 2^{-64}$ реализуется при двухкратном хешировании. Оценки сложности не сильно отличаются от оценок для проективной прямой, а затраты бит по ключу в 1,5 раза больше.

5. Многократное хеширование по кривым Ферма с большим числом точек имеет те же коллизионные оценки, что для максимальных кривых. Затраты бит по ключу в 2 раза превышают затраты при хешировании по проективной прямой.

6. Хеширование по кривой Сузуки в 31 бит конечном поле является наилучшим. Трёхкратное хеширование обеспечивает $P_{кол} < 2^{-64}$ для данных длиной до Гбт. Вычисления в 63 бит конечном поле обеспечивают $P_{кол} < 2^{-53}$ при однократном хешировании для практических длин данных и $P_{кол} < 2^{-107}$ реализуется при двухкратном хешировании. По сложности уступает в 2 раза хешированию по максимальным кривым и по проективной прямой. По затратам бит ключа в 2 раза проигрывает хешированию по проективной прямой.

Список литературы

1. Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования / Г.З.Халимов // Материалы XI Межд. НПК «Информационная безопасность» (Таганрог, Россия, 23-25 июня 2010), ТТИ ЮФУ. – 2010. – Ч. 3. – С. 144-146.

2. Халимов Г.З. Оценка параметров кривых Ферма для универсального хеширования в простом поле / Г.З.Халимов // НТК Компьютерное моделирование в наукоемких технологиях (часть 2). КМНТ Харьков, 18-21 мая 2010. – С.266.

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

4. Халимов Г.З. Универсальное хеширование по рациональным функциям кривой Эрмита / Г.З.Халимов, А.Ю.Иохов // Межд. НПК «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.

5. Халимов Г.З. Универсальное хеширование по максимальной кривой второго рода / Г.З.Халимов // Журнал «Радиоэлектронные и компьютерные системы». – Харьков, НАУ ХАИ, 2011. - № 1(49). – С.70-76.

6. Халимов Г.З. Универсальное хеширование по максимальной кривой третьего рода / Г.З. Халимов // Научные ведомости Белгородского государственного университета. – 2011. – №1 (96), – Вып. 17/1. – С. 137–145.

7. Халимов Г.З. Универсальное хеширование по алгебраическим кривым в простом поле / Г.З.Халимов // Журнал «Системи управління, навігації та зв'язку» Міністерство промислової політики України, ДП «Центральний науково-дослідний інститут навігації і управління» Київ. – 2011. – Вип. 1(17). – С. 156-161.

8. Халимов Г.З. Универсальное хеширование по рациональным функциям алгебраических кривых в кубическом поле / Г.З.Халимов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник Київ. - 2010. – Вип.2(21) – С. 59-65.

9. Халимов Г.З. Алгоритм универсального хеширования по кривой Сузуки / Г.З.Халимов, Е.В.Котух // Восточно-Европейский журнал передовых технологий. – 2011. - № 3/9 (51). – С. 10-16.

10. Wegman. M. N. New hash functions and their use in authentication and set equality / M.N.Wegman, J.L.Carter // Journal of Computer and Systems Science.– 1981. – V. 22. – P. 265–279.

11. Deligne P. Representations of reductive groups over finite fields / P.Deligne, Lusztig// Annatatsiya of Mathematics. – 1976. –N.103. –P. 103–161.

12. 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.

Поступила в редакцию 7.05.2013

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

БАГАТОКРАТНЕ УНІВЕРСАЛЬНЕ ГЕШУВАННЯ ЗА МАКСИМАЛЬНИМИ КРИВИМИ

Г.З. Халімов

Представлені оцінки ймовірності колізії, та складності обчислень для багаторазового гешування за алгебричними кривими у кінцевому полі.

***Ключові слова**: алгебричні криві, універсальне гешування.*

MULTIPLE UNIVERSAL HASHING ON THE MAXIMAL CURVES

G.Z. Khalimov

Estimates of the probability of collision, and the computational complexity for multiple hashing on the algebraic curves over finite fields.

***Keywords:** algebraic curves, universal hashing.*