

УДК 681.3.06

Г.З. Халимов

Харьковский национальный университет радиоэлектроники, Украина

ОЦЕНКИ КОЛЛИЗИОННОЙ СТОЙКОСТИ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ ПО АЛГЕБРАИЧЕСКИМ КРИВЫМ

Представлены оценки коллизийной стойкости универсального хеширования по наилучшим алгебраическим кривым с большим числом точек и максимальным кривым.

Ключевые слова: алгебраические кривые, универсальное хеширование.

Введение

Универсальное хеширование в конструкции алгеброгеометрических кодов предложено Биэрбрауэром в [1] и развито в концепции проективных многообразий по алгебраическим кривым на основе скалярного произведения по рациональным функциям функционального поля алгебраических кривых в работах [2 –

4]. Хеширование по алгебраическим кривым широко представлено в [5 – 10] и лежит в плоскости выбора хороших алгебраических кривых с большим отношением числа точек к роду кривой. Практическим аспектом универсального хеширования по рациональным функциям линейного векторного пространства алгебраических кривых является построение алгоритма хеширования, оценка параметров хеширования: вероят-

ности коллизии, оценки вычислительных затрат на хеширование при фиксированном поле вычислений и размере хеш кода, сложности вычисления точек кривой по ключевым данным.

Целью статьи является оценка коллизионной стойкости универсального хеширования по наилучшим алгебраическим кривым.

В разделе 1 представлено определение универсального хеширования по алгебраическим кривым.

В разделе 2 рассмотрены оценки коллизионной стойкости универсального хеширования по максимальным кривым и кривым с большим числом точек над конечным полем.

Основной раздел

1. Определение универсального хеширования по алгебраическим кривым

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

Определение 1 [4]. Пусть задана абсолютно неразложимая, несингулярная проективная кривая χ над полем F_q с точками $P = \{P_1, P_2, \dots, P_n\} \in \chi(F_q)$. Для каждой алгебраической кривой можно определить поле рациональных функций $F_q(\chi)$. В каждой точке P_j кривой χ можно вычислить оценку \mathfrak{P}_j 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 $m = (m_1, \dots, m_k)$, $m_i \in F_q$ в точке $P_j \in F_q$ определяется выражением

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

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

Замечание 1.

1. Параметры универсального хеш класса $\varepsilon - U(N, q^k, q)$ на основе хеширования по рациональным функциям определяются свойствами алгебраической кривой. Подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < \dots\}$ определяется полюсами рациональных функций в особой точке кривой и рациональные функции упорядоченные по значениям полюсов образуют векторное линейное пространство размерности

$$\dim(L(G)) = v_\ell := \{(i, j) \in N^2 : \rho_i + \rho_j = \rho_{\ell+1}\}.$$

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

3. Наилучший результат универсального хеширования, как следует из оценки вероятности коллизии $\varepsilon \leq \rho_k / N$, 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 $N_q(g) \leq 1 + q + 2\sqrt{qg(C)}$.

Известные результаты по алгебраическим кривым над полем F_q , $q = l^2$.

1. Кривая Эрмита $y^l + y = x^{l+1}$ является наилучшей максимальной плоской кривой наибольшего первого рода $g = l(l-1)/2$ и функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

2. Алгебраические кривые:

$$- y^l + y = x^{(l+1)/2};$$

$$- \sum_{i=1}^t y^{l/2^i} = x^{l+1}, \quad l = 2^t;$$

$$- y^l + y = x^{(l+1)/3}, \quad l \equiv 2 \pmod{3};$$

$$- \sum_{i=0}^{t-1} y^{3^i} = \omega x^{l+1}, \quad l = 3^t, \quad \omega \in F_{l^2}, \quad \omega^{l-1} = -1$$

являются максимальными кривыми второго и третьего рода, имеют подгруппу Вейерштрасса $H(P_\infty) = \langle \rho_1, \rho_2 \rangle$ размерности $\dim = 2$ и функциональное поле $\{x^i \cdot y^j\}$.

3. Максимальные кривые вида:

$$- x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0, \quad l \equiv 2 \pmod{3};$$

$$- \omega x^{(l-1)/3} - \omega x^{2(l-1)/3} + y^l = 0, \quad l \equiv 1 \pmod{3},$$

$$\omega \in F_{l^2}, \quad \omega^{l-1} = -1;$$

$$- y^l + y = \left(\sum_{i=1}^t x^{l/3^i} \right)^2, \quad l = 3^t$$

имеют подгруппу Вейерштрасса $H(P_\infty)$ размерности $\dim = 3$ и функциональное поле определяется рациональными функциями вида $\{x^i \cdot y^j \cdot v^t\}$.

4. Кривая Судзуки $y^q - y = x^{q_0}(x^q - x)$ определена над полем F_q , $q = 2q_0^2$, $q_0 = 2^s$ рода $g = q_0(q-1)$ и имеет число точек $N = q^2 + 1$. Базис пространства $L(\rho_\ell P_0)$, задается функциями вида

$$\{w^j \cdot v^i \cdot y^t \cdot x^r : i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + r \cdot q \leq \rho_\ell\}.$$

5. Кривая Ферма

$$x^{(q-1)/3} + y^{(q-1)/3} + z^{(q-1)/3} = 0$$

над F_q , $q \equiv 1 \pmod{3}$ является кривой с большим числом точек $N = 2(q-1)^2 / 9$.

Замечание 2.

1. Кривая Эрмита имеет наилучшее отношение числа точек к роду кривой $N_q(g)/g$.

2. Максимальные кривые второго и третьего рода покрываются кривой Эрмита.

3. Абсолютно наилучший результат $N_q(g)/g$ достигается на кривой Судзуки.

Определения универсальных хеш классов по максимальным кривым Эрмита, Судзуки и кривым с большим числом точек Ферма и оценки вероятности коллизии представлены в табл. 1.

Таблица 1

Определения универсальных хеш классов

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

$s = \lceil (2k + 1/4)^{1/2} - 1/2 \rceil$ – округление к большему целому числу.

Замечание 3.

1. Табл. 1 представлена по результатам [5 – 10].
 2. Универсальное хеширование по рациональным функциям максимальных плоских алгебраических кривых имеет наилучшие асимптотические результаты. Верхняя граница вероятности коллизии для универсального хеширования $h_{P_j}(m)$ определена в области малых значений $k \leq 2g$, g -род кривой, является прямо пропорциональной корню квадратному из k .

2. Оценки коллизионной стойкости универсального хеширования

Асимптотические оценки вероятности коллизии универсального хеширования по рациональным функциям алгебраических кривых для фиксированного поле вычислений представлены в табл. 2.

Замечание 4.

1. Результаты табл. 2 определяются подстановкой значений k в оценки вероятности коллизии универсального хеширования табл. 1.

2. Хеширование по максимальным кривым имеет наилучшие результаты среди плоских кривых, чуть ухудшаются с уменьшением рода. Такие же оценки достигаются на кривой с большим числом точек Ферма $X^{(q-1)/3} + Y^{(q-1)/3} + Z^{(q-1)/3} = 0$.

3. Абсолютный результат реализуется для хеширования на кривой Сузуки. Вычисления по кривым Ферма и Сузуки является результативным для значений длины данных k , больших размерность поля.

Результаты вычисления параметров универсального хеширования для случая простого поля представлены в табл. 3.

Таблица 2

Оценки вероятности коллизии универсального хеширования по алгебраическим кривым над полем F_q

Тип кривой	Оценки вероятности коллизий $\varepsilon_{q \rightarrow \infty}(k)$ для k слов данных			
	$k = 1$	$k = \sqrt{q}$	$k = q$	$k = q^{3/2}$
Проективная прямая	$1/q$	$1/q^{1/2}$	1	1
Кривая Эрмита	$1/q$	$\sqrt{2}/q^{3/4}$	$\sqrt{2}/q^{1/2}$	1
Максимальные кривые второго рода	$1/q$	$2/q^{3/4}$	$2/q^{1/2}$	1
Максимальные кривые третьего рода	$1/q$	$\sqrt{6}/q^{3/4}$	$\sqrt{6}/q^{1/2}$	1
Кривые Ферма с большим числом точек	$1/q$	$3/(\sqrt{2}q^{3/4})$	$3/(\sqrt{2}q^{1/2})$	$3/(\sqrt{2}q^{1/4})$
Кривая Сузуки	$1/q$	$\sqrt[3]{3}/q^{5/6}$	$\sqrt[3]{3}/q^{2/3}$	$\sqrt[3]{3}/q^{1/2}$

Таблица 3

Оценки параметров универсального хеширования для простого поля

Параметры конечного поля F_q	Уравнение кривой	Размер пространства ключей (бит)	Вероятность коллизии для данных размером L бит			Размер хеш кода (бит)
			1Кбт	1Мбт	1Гбт	
$q = 2^{32} - 99$	$X + Y + Z = 0$	32	2^{-24}	2^{-14}	2^{-4}	32
$q = 2^{32} - 99$	$X^{(q-1)/3} + Y^{(q-1)/3} + Z^{(q-1)/3} = 0$	62	$2^{-26,89}$	$2^{-21,91}$	$2^{-17,5}$	32
$q = 2^{64} - 189$	$X + Y + Z = 0$	64	2^{-57}	2^{-47}	2^{-37}	64
$q = 2^{64} - 189$	$X^{(q-1)/3} + Y^{(q-1)/3} + Z^{(q-1)/3} = 0$	126	$2^{-59,41}$	$2^{-54,41}$	$2^{-49,41}$	64
$q = 2^{96} - 87$	$X + Y + Z = 0$	96	$2^{-89,57}$	$2^{-79,57}$	$2^{-69,57}$	96
$q = 2^{96} - 87$	$X^{(q-1)/3} + Y^{(q-1)/3} + Z^{(q-1)/3} = 0$	190	$2^{-91,7}$	$2^{-86,7}$	$2^{-81,7}$	96
$q = 2^{128} - 159$	$X + Y + Z = 0$	128	2^{-122}	2^{-112}	2^{-102}	128
$q = 2^{128} - 159$	$X^{(q-1)/3} + Y^{(q-1)/3} + Z^{(q-1)/3} = 0$	254	$2^{-123,96}$	$2^{-118,96}$	$2^{-113,96}$	128

Замечание 5.

1. Универсальное хеширование в простом поле определяется на проективной прямой и кривой Ферма. Для эффективных вычислений в конечном поле значения размерности поля q определяются как простые числа ближайшие к 2^{32} , 2^{64} , 2^{96} , 2^{128} и $q \equiv 1 \pmod{3}$.

2. Наилучший результат хеширования достигается на кривой Ферма. Практические вычисления для вероятности коллизии $\varepsilon \approx 2^{-50} \div 2^{-100}$ реализуются на модулях 64÷128 бит для размеров данных до нескольких Гбт.

3. Ключевые затраты на хеширование по кри-

вым Ферма в два раза превышают по числу бит при хешировании по проективной прямой.

Оценки параметров хеширования в квадратичном поле представлены в табл. 4.

Замечание 6.

1. Универсальное хеширование в квадратичном поле определяется на проективной прямой, максимальных кривых и кривой с большим числом точек Ферма. Значения размерности квадратичного поля F_{q^2} определяются как простые числа q ближайшие к значениям 2^{32} , 2^{48} , 2^{64} и $q \equiv 1 \pmod{6}$. Соответственно мощность поля вычислений будет равна 64, 96 и 128 бит.

Таблица 4

Оценки параметров универсального хеширования для квадратичного поля

Параметры конечного поля F_{q^2}	Уравнение кривой	Размер пространства ключей (бит)	Вероятность коллизии для данных размером L бит			Размер хеш кода (бит)
			1Кбт	1Мбт	1Гбт	
$q = 2^{32} - 5$	$X + Y + Z = 0$	64	2^{-57}	2^{-47}	2^{-37}	64
$q = 2^{32} - 5$	$y^q + y = x^{q+1}$	96	2^{-60}	2^{-55}	2^{-50}	64
$q = 2^{32} - 5$	$y^q + y = x^{(q+1)/2}$	95	$2^{-59,5}$	$2^{-54,5}$	$2^{-49,5}$	64
$q = 2^{32} - 5$	$y^q + y = x^{(q+1)/3}$	95	$2^{-59,2}$	$2^{-54,2}$	$2^{-49,2}$	64
$q = 2^{32} - 5$	$x^{(q^2-1)/3} + x^{(q^2-1)/3} + 1 = 0$	126	$2^{-59,41}$	$2^{-54,41}$	$2^{-49,41}$	64
$q = 2^{48} - 59$	$X + Y + Z = 0$	96	$2^{-89,57}$	$2^{-79,57}$	$2^{-69,57}$	96
$q = 2^{48} - 59$	$y^q + y = x^{q+1}$	144	$2^{-92,28}$	$2^{-87,28}$	$2^{-82,28}$	96
$q = 2^{48} - 59$	$y^q + y = x^{(q+1)/2}$	143	$2^{-91,78}$	$2^{-86,78}$	$2^{-81,78}$	96
$q = 2^{48} - 59$	$y^q + y = x^{(q+1)/3}$	143	$2^{-91,49}$	$2^{-86,49}$	$2^{-81,49}$	96
$q = 2^{48} - 59$	$x^{(q^2-1)/3} + x^{(q^2-1)/3} + 1 = 0$	190	$2^{-91,7}$	$2^{-86,7}$	$2^{-81,7}$	96
$q = 2^{64} - 59$	$X + Y + Z = 0$	128	2^{-122}	2^{-112}	2^{-102}	128
$q = 2^{64} - 59$	$y^q + y = x^{q+1}$	192	$2^{-124,5}$	$2^{-119,5}$	$2^{-114,5}$	128
$q = 2^{64} - 59$	$y^q + y = x^{(q+1)/2}$	191	2^{-124}	2^{-119}	2^{-114}	128
$q = 2^{64} - 59$	$y^q + y = x^{(q+1)/3}$	191	$2^{-123,7}$	$2^{-118,7}$	$2^{-113,7}$	128
$q = 2^{64} - 59$	$x^{(q^2-1)/3} + x^{(q^2-1)/3} + 1 = 0$	254	$2^{-123,96}$	$2^{-118,96}$	$2^{-113,96}$	128

2. Найлучшие результаты хеширования достигаются на максимальных кривых и кривой Ферма. Практические вычисления для вероятности коллизии $\varepsilon \approx 2^{-50} \div 2^{-100}$ реализуются на модулях $64 \div 128$ бит для размеров данных до нескольких Гбт.

3. Ключевые затраты на хеширование по максимальным кривым в полтора раза и по кривым Ферма в два раза превышают по числу бит на хеширование по проективной прямой.

Параметры универсального хеширования для кубического поля представлены в табл. 5.

Замечание 7.

1. Универсальное хеширование в кубическом поле определяется на проективной прямой и кривой с большим числом точек Ферма. Значения размерности кубического F_{q^3} определяются как простые числа q ближайšie к 2^{16} , 2^{32} , 2^{48} . Мощность поля вычислений определяется в 48, 96 и 144 бит.

2. Найлучшие результаты хеширования достигаются на кривой Ферма.

Практические вычисления для вероятности к

оллизии $\varepsilon \approx 2^{-70} \div 2^{-130}$ реализуются на модулях $96 \div 144$ бит для размеров данных до нескольких Гбт.

3. Ключевые затраты на хеширование по кривым Ферма в 5/3 раз превышают по числу бит на хеширование по проективной прямой. Параметры универсального хеширования для расширенного поля характеристики 2 представлены в табл. 6.

Замечание 8.

1. Универсальное хеширование в расширенном поле характеристики 2 определяется на проективной прямой, кривой Сузуки и кривой Ферма с большим числом точек.

2. Найлучшие результаты хеширования достигаются на кривой Сузуки. Несколько уступает по вероятности коллизии хеширование по кривой Ферма. Практические вычисления для вероятности коллизии $\varepsilon \sim 2^{-50}$ и меньше реализуются на модулях в 64 бит и больше для данных до нескольких Гбт.

3. Ключевые затраты на хеширование по кривым Сузуки и Ферма в 2 раза превышают по числу бит на хеширование по проективной прямой.

Таблица 5

Оценки параметров универсального хеширования для кубического поля

Параметры конечного поля F_{q^3}	Уравнение кривой	Размер пространства ключей (бит)	Вероятность коллизии для данных размером L бит			Размер хеш-кода (бит)
			1Кбт	1Мбт	1Гбт	
$q = 2^{16} - 15$	$X + Y + Z = 0$	48	$2^{-40,58}$	$2^{-30,58}$	$2^{-20,58}$	48
$q = 2^{16} - 15$	$x^{q^2+q+1} + y^{q^2+q+1} + 1 = 0$	80	$2^{-43,79}$	$2^{-38,79}$	$2^{-33,79}$	48
$q = 2^{32} - 5$	$X + Y + Z = 0$	96	$2^{-88,58}$	$2^{-78,58}$	$2^{-68,58}$	96
$q = 2^{32} - 5$	$x^{q^2+q+1} + y^{q^2+q+1} + 1 = 0$	160	$2^{-91,79}$	$2^{-86,79}$	$2^{-81,79}$	96
$q = 2^{48} - 59$	$X + Y + Z = 0$	144	$2^{-136,58}$	$2^{-126,58}$	$2^{-116,58}$	144
$q = 2^{48} - 59$	$x^{q^2+q+1} + y^{q^2+q+1} + 1 = 0$	250	$2^{-139,79}$	$2^{-134,79}$	$2^{-129,79}$	144

Таблица 6

Оценки параметров универсального хеширования для расширенного поля

			1Кбт	1Мбт	1Гбт	
$q = 2^{32}$	$X + Y + Z = 0$	32	2^{-24}	2^{-14}	2^{-4}	32
$q = 2^{31}$	$y^q - y = x^{q^0}(x^q - x)$	62	$2^{-27,79}$	$2^{-24,46}$	$2^{-21,13}$	31
$q = 2^{32}$	$x^{(q-1)/3} + x^{(q-1)/3} + 1 = 0$	64	$2^{-26,89}$	$2^{-21,91}$	$2^{-17,5}$	32
$q = 2^{64}$	$X + Y + Z = 0$	63	2^{-57}	2^{-47}	2^{-37}	64
$q = 2^{63}$	$y^q - y = x^{q^0}(x^q - x)$	126	$2^{-60,13}$	$2^{-56,8}$	$2^{-53,47}$	63
$q = 2^{64}$	$x^{(q-1)/3} + x^{(q-1)/3} + 1 = 0$	128	$2^{-59,41}$	$2^{-54,41}$	$2^{-49,41}$	64

Выводы

1. Оценки вероятности коллизии универсального хеширования по алгебраическим кривым представленные в таблицах 3÷6 являются верхними и определяют коллизионную границу для хеширования k слов данных.

2. Найлучшее применение универсального хеширования по алгебраическим кривым определяется

выбором конечного поля и аспектами реализации вычислений в полях. Вычисления в простом поле являются быстрыми. Универсальное хеширование по кривой Ферма с большим числом точек имеет преимущество. Вероятность коллизии обратно пропорционально зависит от размерности поля вычислений.

Для обеспечения вероятности коллизии $\varepsilon < 2^{-50}$ над практическими данными до нескольких Гбт поле вычислений должно быть не меньше 64 бит.

Список литературы

14. Bierbrauer J. On families of hash functions via geometric codes and concatenation. / J. Bierbrauer, T. Johansson, G. Kabatianskii, B. Smeets // *Advances in Cryptology-CRYPTO '93 Proceedings*, Springer-Verlag-1994. – P. 331-342.
15. Халимов Г.З. Аутентификация с применением алгеброгеометрических кодов / Г.З. Халимов, А.А. Кузнецов // *Радиотехника: всеукр. межвед. науч.-техн. сб.* – 2001. – Вып. 119. – С. 103-109.
16. 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.
17. Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования / Г.З. Халимов // *Матлы XI Международн. научн.-пр. конф. «Информационная безопасность»* (Таганрог, Россия, 23-25 июня 2010), ТТИ ЮФУ. – 2010. – Ч. 3. – С. 144-146.
18. Халимов Г.З. Универсальное хеширование по рациональным функциям кривой Эрмита / Г.З. Халимов, А.Ю. Иохов // *Междунар. научн.-пр. конф. «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» Академія внутрішніх військ МВС України 17-18.03.2011.* Зб. тези доповідей. – 2011. – С. 48-51.
19. Халимов Г.З. Универсальное хеширование по максимальной кривой второго рода / Г.З. Халимов // *Журнал «Радиоэлектронные и компьютерные системы».* – Х.: НАУ ХАИ, 2011. – № 1(49). – С. 70-76.
20. 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.
21. 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».* – К. – 2011. – Вип. 1(17). – С. 156-161.
22. 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: наук.-техн. зб.* – К. – 2010. – Вип. 2(21) – С. 59-65.
23. 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.

Поступила в редколлегию 4.02.2013

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

**ОЦІНКИ КОЛІЗІЙНОЇ СТІЙКОСТІ УНІВЕРСАЛЬНОГО ГЕШУВАННЯ
ЗА АЛГЕБРИЧНИМИ КРИВИМИ**

Г.З. Халімов

Представлені оцінки колізійної стійкості універсального гешування за найкращими алгебричними кривими з великим числом точок і максимальними кривими.

Ключові слова: алгебричні криві, універсальне гешування.

**COLLISION RESISTANCE EVALUATION OF UNIVERSAL HASHING
ON THE ALGEBRAIC CURVES**

G.Z. Khalimov

Estimates of collision resistance of the universal hashing on the best algebraic curves with a large number of points and the maximal curves.

Keywords: algebraic curves, universal hashing.