МЕТОДЫ, МЕХАНИЗМЫ И ПРОТОКОЛЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3.06

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО МАКСИМАЛЬНЫМ КРИВЫМ ГУРВИЦА

Г. З. ХАЛИМОВ

Представлены результаты исследований по максимальным кривым Гурвица для целей универсального хеширования, условия максимальности обобщенных кривых, максимальная кривая Гурвица с третьим значением рода.

Ключевые слова: универсальное хеширование, кривые Гурвица.

ВВЕДЕНИЕ

Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе-Вейля. Основные результаты по кривым Гурвица представлены в работах F.Torres [1,2], также в работах[3,4]. Связь между кривыми Гурвица и Ферма представлена P. Carbonne, T.Henocq в [3]. В работе [1] введено определение обобщенных кривых Гурвица и установлен морфизм между обобщенными кривыми Гурвица и Ферма. Здесь же определены условия максимальности для обычных кривых Гурвица и обобщенных кривых при ограничении на выбор показателей степени кривой. Оценки числа решений кривой Гурвица для произвольного конечного поля и частные результаты по оценкам представлены в [4]. Теорема о существования нетривиальных кривых Гурвица и правила построения нетривиальных кривых также получены в [4].

Целью статьи является определение условий максимальности кривых Гурвица без ограничений на показатели степени кривой. В разделе 1 приводятся определение и свойства универсального хеширования в поле рациональных функций по точкам алгебраической кривой. В разделе 2 представлены определение и свойства кривых Гурвица, в разделе 3 – результаты по построению максимальных кривых Гурвица и оценке параметров.

1. УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ В ПОЛЕ РАЦИОНАЛЬНЫХ ФУНКЦИЙ

Универсальное хеширование в поле рациональных функций по точкам алгебраической кривой впервые введено Биербрауэром [5]. Интерпретация алгеброгеометрического подхода излагается в работах [4, 6].

Определение 1 [6]. 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 $m=(m_1, m_2, ..., m_k)$, $m_i\in F_q$ в точке $P_j\in F_q$ определяется выражением

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

где $f_i\in F_q(\chi)$ с упорядоченными порядками полюсов $0<u_1<u_2< ...<u_k$. Хеш функция $h_{P_j}(m)$ определяет универсальный хеш класс $\varepsilon-U(N,q^k,q)$, где вероятность коллизии $\varepsilon\le u_k/N$, N – число точек алгебраической кривой.

Проблематика построения схем универсального хеширования на основе алгеброгеометрического представления заключается в выборе алгебраических кривых с требуемыми параметрами. Интерес представляют алгебраические кривые с как можно большим отношением числа точек кривой к её роду, определенные над конечным полем F_q. Наилучший результат универсального хеширования достигается на максимальных кривых [2]. Классическими максимальными кривыми являются кривые Эрмита, Сузуки, Делигнэ-Лустига. Lachaud G в [7] показал, что если кривая покрывается максимальной кривой, то она также является максимальной.

Предложение 1. [7] Пусть X_1 и X_2 неприводимые алгебраические кривые, определенные в проективном пространстве над полем F_q. Предположим, что существует морфизм $f: X_1\to X_2$ над полем F_q. Тогда если X_1 является максимальной кривой, тогда максимальной кривой является X_2.

Этот замечательный результат позволяет расширить поиск максимальных кривых Гурвица.

2. ОПРЕДЕЛЕНИЕ И СВОЙСТВА КРИВЫХ ГУРВИЦА

Кривые Гурвица H_n определяются выражением

$$X^nY+Y^nZ+XZ^n=0 \qquad (2)$$

и имеют частные производные вида $F_X=nX^{n-1}Y+Z^n$, $F_Y=nY^{n-1}Z+X^n$, $F_Z=nZ^{n-1}X+Y^n$.

Существует обобщение кривых Гурвица $H_{n,l}$, которое имеет вид

$$X^nY^l + Y^nZ^l + X^lZ^n = 0, \quad (3)$$

где $n \geq l \geq 2$ и $\Delta(n, l) = n^2 - nl + l^2 \geq 2$.

Между кривыми Гурвица и Ферма существует морфизм, установленный P. Carbonne, T.Henocq в [3] и определенный в лемме 1.

Лемма 1. Кривая Гурвица H_n является F_q покрытой кривой Ферма

$$U^{n^2-n+1} + V^{n^2-n+1} + W^{n^2-n+1} = 0.$$

Известно обобщение леммы 1 для кривых Гурвица общего вида F.Torres в [1].

Лемма 2. Кривая Гурвица $H_{n,1}$ является F_q покрытой кривой Ферма

$$U^{n^2-nl+l^2} + V^{n^2-nl+l^2} + W^{n^2-nl+l^2} = 0.$$

Следующее утверждение является новым и определяет семейства нетривиальных кривых Гурвица, число точек которых не равно размерности поля.

Утверждение 1. Пусть F_q конечное поле и $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $e_i \geq 1$. Нетривиальные кривые Гурвица $\mathcal{H}_{n,l}$ принадлежат одному из семейств:

a) $X^nY + Y^nZ + XZ^n = 0$,

если $\Delta(n,l=1) = n^2 - n + 1 = p_i \cdot \ldots \cdot p_j$, где делители $p_i, \ldots, p_j$ тождественны 1 по *mod 6* кроме делителя, равного 3, и взяты из набора делителей порядка поля $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$;

b) $X^nY^l + Y^nZ^l + X^lZ^n = 0$,

если $\Delta(n,l) = n^2 - nl + l^2 = p_i \cdot \ldots \cdot p_j$, где делители $p_i, \ldots, p_j$ тождественны 1 по *mod 6* кроме равного 3, и взяты из набора делителей порядка поля $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $\gcd(n,l) = 1$;

c) $X^{cn}Y^{cl} + Y^{cn}Z^{cl} + X^{cl}Z^{cn} = 0$,

если $\Delta(cn,cl) == c^2 \cdot p_i \cdot \ldots \cdot p_j$, где делители $p_i, \ldots, p_j$ тождественны 1 по *mod 6* кроме делителя, равного 3, и все $c, p_i, \ldots, p_j$ взяты из набора делителей порядка поля $q-1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, $\gcd(n,l) > 1$;

d) $X^cY^c + Y^cZ^c + X^cZ^c = 0$,

если $\Delta(c,c) = c^2$, где c есть делитель порядка поля $q-1$.

Доказательство выходит за рамки статьи и требует привлечения техники доказательств по оценкам числа точек [4]

Замечание 1.

1. Многообразие нетривиальных кривых Гурвица определяется значениями делителей порядка поля, как следует из утверждения 1.

2. Важной задачей является определение условий построения максимальных кривых Гурвица и оценка их параметров.

3. УСЛОВИЕ МАКСИМАЛЬНОСТИ КРИВЫХ ГУРВИЦА

Квадратичное поле замечательно тем, что в F_{q^2} существуют максимальные кривые, например, кривые Эрмита. Как следует из предложения 1, каждая кривая над полем F_{q^2}, которая покрывается кривой Эрмита, является F_{q^2} максимальной [3]. Основные результаты по максимальным кривым Гурвица представлены в работах F.Torres [1, 2].

Теорема 1. [1] Кривая Гурвица H_n над полем F_{q^2} является максимальной, если и только если $q+1 \equiv 0 \bmod (n^2 - n + 1)$.

Доказательство теоремы является важным, вытекает из предложения 1 и результата леммы 1. Действительно по лемме морфизм

$$(u:v:1) \to (x:y:1) = \left(u^n v^{-1} : uv^{n-1} : 1\right)$$

отображает кривую $u^{n^2-n+1} + v^{n^2-n+1} + 1 = 0$ на кривую $x^n y + y^n + x = 0$.

По условию теоремы $q+1 \equiv 0 \bmod (n^2 - n + 1)$ и кривая $u^{n^2-n+1} + v^{n^2-n+1} + 1 = 0$ принадлежит семейству кривых Эрмита. Тогда и $x^n y + y^n + x = 0$ по предложению 1 является максимальной.

Условие «только если» доказывается следующим образом. Обозначим точки кривой Гурвица на бесконечности как $P_0 := (1:0:0)$, $P_1 := (0:1:0)$ и $P_2 := (0:0:1)$. В работе Carbonne P. и др. [5] показано, что подгруппа Вейерштрасса для кривой Гурвица в точке $P_1 := (0:1:0)$ образуется набором $S := \{s(n-1)+1 : s = 1, \ldots, n\}$. Пусть λ есть линия с уравнением $X = 0$. Тогда λ пересекает кривую Гурвица χ в точках P_1 и P_2. Вычислим кратность пересечения λ с кривой χ в точке P_2 $I(P_2, \chi, \lambda)$. В точке P_2 имеем $x^n y + y^n + x = 0$ и после преобразований $x = y^n / \left(1 + x^{n-1} y\right) = 0$. Отсюда следует, что $I(P_2, \chi, \lambda) = n$. По теореме Безу кратность пересечения λ с кривой χ равна $I(\chi, \lambda) = n+1$, что определяет значение $I(P_1, \chi, \lambda) = 1$. Таким образом $\chi'' \lambda = nP_2 + P_1$. Аналогично для $\mu : Y = 0$ получим $\chi'' \mu = P_2 + nP_0$ и для $\gamma : Z = 0$ имеем $\chi \bullet \gamma = P_0 + nP_1$. Значение дивизоров рациональных функций будут равны $(x/z) = nP_2 - (n-1)P_1 - P_0$ и

$$(y/z) = (n-1)P_0 - P_2 - nP_1,$$

и

$$\left(x^{s-1} y\right) = \left(n(s-1)+1\right)P_2 + (n-s)P_0 - \left(s(n-1)+1\right)P_1.$$

Это доказывает, что набор S содержится в подгруппе Вейерштрасса $H(P_1)$ для точки P_1. Практически это означает, что $H(P_1)$ включает счетное множество чисел набора S.

Пусть кривая Гурвица является F_{q^2} максимальной. В работе [8] показано, что при характеризации Эрмитовых функциональных полей выполняется условие эквивалентности порядков рациональных функций в точках бесконечности $(q+1)P_1 \sim (q+1)P_2$. В случае $s = n$, имеем следующее представление дивизора $\left(x^{n-1} y\right) = \left(n(n-1)+1\right)P_{20} - \left(n(n-1)+1\right)P_1$. Известно, что степень дивизора рациональной функции равна 0 и имеем условие эквивалентности для порядков дивизора рациональных функций

на кривой Гурвица $\left(n^2-n+1\right)P_1 \sim \left(n^2-n+1\right)P_2$. Пусть $d=\gcd\left(n^2-n+1,q+1\right)$ и значение d в силу F_{q^2} максимальности кривой содержится в подгруппе Вейерштрасса $H(P_1)$. В соответствии с представлением Carbonne P. и др. [5] для S значение d должно иметь вид $d=A(n-1)+B$ при $A\geq B\geq 1$. Нужно показать, что $d=n^2-n+1$. Предположим, это не так и существует разложение $n^2-n+1=C\left(A(n-1)+B\right)$. После ряда преобразований имеем $BC=D(n-1)+1$ и $AD(n-1)+A+BD=Bn$ для $D\geq 0$. Левая часть последнего уравнения будет равна правой только при условии $B=C=1$ и $D=0$. Тогда $A=n$ и $d=n^2-n+1$, что завершает доказательство. ◊

Замечание 2.

1. Теорема 1 указывает на существование максимальных кривых Гурвица малого рода. Легко показать, что род кривых равен $g=\left(n^2-n-1\right)/2$ и не может быть большим, т.к. n^2-n+1 есть делитель $q+1$. Условия теоремы являются не только необходимыми, но и достаточными.

2. Эта теорема исчерпывает все максимальные кривые обычных кривых Гурвица H_n.

Условия F_{q^2} максимальности обобщенных кривых Гурвица были рассмотрены F.Torres в работах [1,2]. Основной результат представлен теоремой 2.

Теорема 2. Пусть $H_{n,l}$ есть несингулярная кривая Гурвица над полем F_{q^2}, $\gcd(n,l)=1$ и $Q=n^2-nl+l^2$ простое число. Тогда $H_{n,l}$ является максимальной, если и только если $n^2-nl+l^2\equiv 0\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$, где $\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$ определяет операцию по модулю делителя $q+1$.

Доказательство аналогично доказательству теоремы 1. Так как Q по условию простое, условие $n^2-nl+l^2\equiv 0\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$ фактически определяет, что n^2-nl+l^2 является простым делителем $q+1$. Из результата леммы 2 следует морфизм кривой $u^{n^2-nl+l^2}+v^{n^2-nl+l^2}+1=0$ на кривую $x^n y^l+y^n+x^l=0$. По условию теоремы $n^2-nl+l^2\equiv 0\left\langle \mathrm{mod}\left|(q+1)\right.\right\rangle$ и кривая $u^{n^2-nl+l^2}+v^{n^2-nl+l^2}+1=0$ принадлежит семейству кривых Эрмита. Тогда и $x^n y^l+y^n+x^l=0$ по предложению 1 является максимальной.

Условие «только если» доказывается следующим образом. Пусть $P_0:=(1:0:0)$, $P_1:=(0:1:0)$ и $P_2:=(0:0:1)$ есть точки кривой Гурвица на бесконечности. Подгруппа Вейерштрасса для кривой Гурвица в точке $P_1:=(0:1:0)$ образуется набором

$$H:=\left\{\begin{matrix}(n-l)s+nt:s,y\in Z;t\geq 0,\\ -lt/n\leq s\leq (n-l)t/l\end{matrix}\right\}.$$

Пусть λ есть линия с уравнением $X=0$. Тогда λ пересекает кривую Гурвица χ в точках P_1 и P_2. Вычислим кратность пересечения λ с кривой χ в точке P_2 $I(P_2,\chi,\lambda)$. В точке P_2 имеем $x^n y^l+y^n+x^l=0$ и после преобразований $x^l=y^n/\left(1+x^{n-l}y^l\right)=0$. Так как $\gcd(n,l)=1$, следует $I(P_2,\chi,\lambda)=n$. По теореме Безу кратность пересечения λ с кривой χ равна $I(\chi,\lambda)=n+l$, что определяет значение $I(P_1,\chi,\lambda)=l$. Таким образом $\chi\bullet\lambda=nP_2+lP_1$. Аналогично для $\mu: Y=0$ получим $\chi\bullet\mu=lP_2+nP_0$ и для $\gamma: Z=0$ имеем $\chi\bullet\gamma=lP_0+nP_1$. Значение дивизоров рациональных функций будут равны

$$(x/z)=nP_2-(n-l)P_1-lP_0$$

$$\text{и } (y/z)=(n-l)P_0+lP_2-nP_1,$$

$$\text{и } \left(x^s y^l\right)=(ns+lt)P_2+\left(-ls+(n-l)t\right)P_0-$$
$$-\left((n-l)s+nt\right)P_1.$$

Так как степень дивизора рациональной функции равна 0 и $(n-l)s+nt\in H(P_1)$, что предусматривает $ns+lt\geq 0$ и $-ls+(n-l)t\geq 0$ и тогда $H\subseteq H(P_1)$.

В случае $s=n-l$ и $t=l$ имеем следующее представление дивизора $\left(x^{n-l}y^l\right)=\left(n^2-nl+l^2\right)P_2-\left(n^2-nl+l^2\right)P_1$. Имеем условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица $QP_1\sim QP_2$. Следовательно, $d=\gcd(Q,q+1)\in H(P_1)$, так как условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых определяется $(q+1)P_1\sim(q+1)P_2$. Так как $1\notin H(P_1)$ и Q простое число следует искомый результат. ◊

Рассмотрим примеры, поясняющие действие теорем 1 и 2.

Пример 1. В поле F_{q^2}, $q=2^7$ построить максимальные кривые Гурвица. По утверждению 1 п. a,b существуют нетривиальные кривые Гурвица $\mathcal{H}_{n,l}$ вида $X^nY+Y^nZ+XZ^n=0$ и $X^nY^l+Y^nZ^l+X^lZ^n=0$, если $n^2-n+1=p_i\cdot\ldots\cdot p_j$, и соответственно $n^2-nl+l^2=p_i\cdot\ldots\cdot p_j$, где делители $p_i,\ldots,p_j$ тождественны 1 по *mod 6* кроме, делителя равного 3, и взяты из набора делителей порядка поля. Имеем разложение порядка поля $q^2-1=2^{14}-1=3*43*127$ и $q+1=129=3*43$. Под условия утверждения 1 попадают делители $p_1=3$ и $p_2=43$. По теореме 1 кривая $X^nY+Y^nZ+XZ^n=0$ является максимальной, если n^2-n+1 является делителем $q+1$. Имеем три случая: $n^2-n+1=3$, $n^2-n+1=43$ и $n^2-n+1=3*43=129$. Первые два случая дают решения: $n=2$ и $n=7$. Таким образом существует тривиальная кривая $X^2Y+Y^2Z+XZ^2=0$ рода $g=1$ и числом точек $N_{2,1}=16641$ и нетривиальная $X^7Y+Y^7Z+XZ^7=0$ рода $g=21$ и числом точек $N_{7,1}=21761$. Других максимальных кривых, которые удовлетворяют условиям теоремы 1 и 2, нет.

Пример 2. В поле F_{q^2}, $q=2^9$ построить максимальные кривые Гурвица. Имеем разложение порядка поля $q^2-1=2^{18}-1=262143=3^3*7*19*73$ и $q+1=513=3^3*19$. Под условия утверждения 1 и теорем 1,2 попадают делители $p_1=3$

и $p_2 = 19$. По теореме 1 имеем три случая: $n^2 - n + 1 = 3$, $n^2 - n + 1 = 19$ и $n^2 - n + 1 = 3*19 = 57$. Первые и третий случаи дают решения: $n = 2$ и $n = 8$. Таким образом, существует тривиальная кривая $X^2Y + Y^2Z + XZ^2 = 0$ рода $g = 1$ и числом точек $N_{2,1} = 263169$ и нетривиальная $X^8Y + Y^8Z + XZ^8 = 0$ рода $g = 28$ и числом точек $N_{8,1} = 290817$. Второй случай, с делителем 19, соответствует условию теоремы 2 для $n^2 - nl + l^2 = 19$ и дает обобщенную максимальную кривую вида $X^5Y^2 + Y^5Z^2 + X^2Z^5 = 0$, рода $g = 9$ и числом точек $N_{5,2} = 271361$.

Замечание 3.

1. Теорема 1 исчерпывает все максимальные обычные кривые Гурвица H_n.

2. Теорема 2 рассматривает максимальные обобщенные кривые Гурвица $H_{n,l}$ при ограничении $\gcd(n,l) = 1$, $Q = n^2 - nl + l^2$ — простое число и $n^2 - nl + l^2 \equiv 0 \langle \bmod |(q+1)\rangle$, в то время как утверждение 4 указывает на существование четырёх разнообразий кривых Гурвица.

Следующие теоремы являются новыми и снимают ограничение на показатель $Q = n^2 - nl + l^2$.

Теорема 3. Пусть $H_{n,l}$ есть несингулярная кривая Гурвица над полем F_{q^2}, $\gcd(n,l) = 1$. Тогда $H_{n,l}$ является максимальной, если и только если $q + 1 \equiv 0 \bmod \left(n^2 - nl + l^2\right)$.

Доказательство аналогично доказательству теорем 1 и 2. Действительно, так как $n^2 - nl + l^2$ является делителем $q+1$, из результата леммы 2 следует морфизм кривой $u^{n^2-nl+l^2} + v^{n^2-nl+l^2} + 1 = 0$ на кривую $x^n y^l + y^n + x^l = 0$. Кривая $u^{n^2-nl+l^2} + v^{n^2-nl+l^2} + 1 = 0$ принадлежит семейству кривых Эрмита и $x^n y^l + y^n + x^l = 0$ по предложению 1 является максимальной.

Условие «только если» доказывается подобным образом. Имеем условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица $\left(n^2 - nl + l^2\right)P_1 \sim \left(n^2 - nl + l^2\right)P_2$. Так как условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых определяется $(q+1)P_1 \sim (q+1)P_2$, следовательно, $d = \gcd\left(n^2 - nl + l^2, q+1\right) \in H(P_1)$. Так как $1 \notin H(P_1)$ и $n^2 - nl + l^2$ есть делитель $q+1$, следует искомый результат. ◊

Теорема 3 определяет условия максимальности для обобщенных кривых п. b) из утверждения 4.

Пример 3. Рассмотрим, как в примере 3, поле F_{q^2}, $q = 2^7$. По утверждению 1 п. b) существует нетривиальная кривая Гурвица для случая $n^2 - nl + l^2 = 3*43 = 129$. Это попадает под условия максимальности теоремы 3 и дает обобщенную максимальную кривую вида $X^{13}Y^5 + Y^{13}Z^5 + X^5Z^{13} = 0$, рода $g = 64$ и числом точек $N_{13,5} = 32769$.

Следующая теорема определяет условия максимальности кривых Гурвица из п. d) утверждения 1.

Теорема 4. Пусть $H_{n,l}$ есть кривая Гурвица над полем F_{q^2}, $n = l$. Тогда $H_{n,l}$ является максимальной, если и только если $q + 1 \equiv 0 \bmod n$.

Действительно отображение морфизма $(x:y:1) \to (u:v:1) = (y:\frac{y}{x}:1)$ кривой Гурвица $x^n y^n + y^n z^n + x^n z^n = 0$ есть кривая Ферма $u^n + v^n + 1 = 0$. Если $q + 1 \equiv 0 \bmod n$ кривая $u^n + v^n + 1 = 0$ принадлежит семейству кривых Эрмита и по предложению 1 следует максимальность $x^n y^n + y^n z^n + x^n z^n = 0$. Условие «только если» доказывается, как в теореме 3. Заметим, что точки на бесконечности кривой Гурвица $P_0 := (1:0:0)$, $P_1 := (0:1:0)$ и $P_2 := (0:0:1)$ имеют кратность n. Имеем условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица $n^2 P_1 \sim n^2 P_2$. Условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых с учетом кратности точек на бесконечности определяется, как $n(q+1)P_1 \sim n(q+1)P_2$. Значение $d = \gcd\left(n^2, n(q+1)\right)$ должно содержаться в подгруппе Вейерштрасса $H(P_1)$ для точки P_1. Так как $1 \notin H(P_1)$ и n есть делитель $q+1$, следует искомый результат. ◊

Пример 4. Рассмотрим поле F_{q^2}, $q = 2^7$. По утверждению 1 п. d) существуют нетривиальные кривые Гурвица для $n = l = 3,43,127,129$. Значения $n = 3,43,129$ являются условиями максимальности по теореме 4. Например, кривая вида $X^{43}Y^{43} + Y^{43}Z^{43} + X^{43}Z^{43} = 0$ имеет род $g = 861$ и число точек $N_{43,43} = 236675$, из которых F_{q^2} рациональных 236672 и 3 точки на бесконечности с кратностью 43. Сумма точек с учетом кратности дает значение на границе Хассе-Вейля $N = 236801$.

Замечание 4. Максимальная кривая Гурвица $X^{q+1}Y^{q+1} + Y^{q+1}Z^{q+1} + X^{q+1}Z^{q+1} = 0$, тождественна кривой Эрмита $X^{q+1} + Y^{q+1} + Z^{q+1} = 0$ наибольшего рода $g = q(q-1)/2$.

Общий результат максимальности обобщенных кривых Гурвица вида c) из утверждения 1 представлен следующей теоремой.

Теорема 5. Пусть кривая Гурвица $H_{n,l}$ вида $X^{cn}Y^{cl} + Y^{cn}Z^{cl} + X^{cl}Z^{cn} = 0$, $\gcd(n,l) = 1$, $c \geq 1$ определена над полем F_{q^2}. Тогда $H_{n,l}$ является максимальной, если и только если $q + 1 \equiv 0 \bmod \left(c\left(n^2 - nl + l^2\right)\right)$.

Случаи $c = 1$ и $n = l > 1$ определяются теоремами 3 и 4. Точки на бесконечности кривой Гурвица $P_0 := (1:0:0)$, $P_1 := (0:1:0)$ и $P_2 := (0:0:1)$ имеют кратность c. Условие эквивалентности для порядков дивизора рациональных функций на кривой Гурвица имеет $c^2\left(n^2 - nl + l^2\right)P_1 \sim c^2\left(n^2 - nl + l^2\right)P_2$. Условие эквивалентности порядков рациональных функций F_{q^2} максимальных кривых с учетом кратности точек на бесконечности определяется, как $c(q+1)P_1 \sim c(q+1)P_2$. Значение $d = \gcd\left(c^2\left(n^2 - nl + l^2\right), c(q+1)\right)$ должно содержать-

ся в подгруппе Вейерштрасса $H(P_1)$ для точки P_1. Так как $1 \notin H(P_1)$ и $c\left(n^2 - nl + l^2\right)$ есть делитель $q+1$, следует искомый результат. ◊

Пример 5. Рассмотрим поле F_{q^2}, $q = 2^7$. По утверждению 1 п. c) существуют нетривиальные кривые Гурвица вида $X^{cn}Y^{cl} + Y^{cn}Z^{cl} + X^{cl}Z^{cn} = 0$, если $\Delta(cn,cl) == c^2 \cdot p_i \cdot \ldots \cdot p_j$, где делители $p_i,\ldots,p_j$ тождественны 1 по *mod 6,* кроме делителя равного 3, и все $c, p_i,\ldots,p_j$ взяты из набора делителей порядка поля $q^2 - 1 = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. По условию теоремы 5, если $c\left(n^2 - nl + l^2\right)$ является делителем $q+1$, кривая $H_{cn,cl}$ является максимальной. Делителями разложения $q+1$ есть числа 3,43,129. В примерах 3,5,6 построены максимальные кривые вида a,b,d) утверждения 1. По теореме 5 определим следующие максимальные кривые:

1. $X^{21}Y^3 + Y^{21}Z^3 + X^{21}Z^3 = 0$, род $g = 160$ и число точек $N_{21,3} = 65025$, с учетом кратности 3 точек на бесконечности;

2. $X^{86}Y^{43} + Y^{86}Z^{43} + X^{86}Z^{43} = 0$, род $g = 2710$ и число точек $N_{86,43} = 710145$, с учетом кратности 43 точек на бесконечности.

Теорема 5 является обобщением теорем 1-4, так как определяет условия F_{q^2} максимальности всех видов кривых Гурвица.

Важной задачей является построение наилучшей максимальной кривой Гурвица. Следующая теорема определяет максимальную кривую Гурвица наибольшего рода и соответственно с наибольшим числом точек.

Теорема 6. Пусть F_{q^2} конечное поле и $q+1 \equiv 0 \bmod 3$. Тогда обобщенная кривая Гурвица в F_{q^2} вида

$$X^{2(q+1)/3}Y^{(q+1)/3} + Y^{2(q+1)/3}Z^{(q+1)/3} + X^{(q+1)/3}Z^{2(q+1)/3} = 0 \quad (4)$$

является максимальной кривой наибольшего рода $g = g_3 = \left(q^2 - q + 4\right)/6$.

Действительно, отображение морфизма $(x:y:1) \to (u/v:v:1) = (x:y:1)$ кривой

$$x^{2(q+1)/3}y^{(q+1)/3} + y^{2(q+1)/3}z^{(q+1)/3} + x^{(q+1)/3}z^{2(q+1)/3} = 0$$

есть кривая $u^{2(q+1)/3} + u^{(q+1)/3} + v^{q+1} = 0$, которая является максимальной [1]. По предложению 1 следует максимальность кривой Гурвица. Условие «только если» доказывается, по теореме 5. Следует проверить, что $q+1 \equiv 0 \bmod \left(c\left(n^2 - nl + l^2\right)\right)$. Действительно, $c = (q+1)/3$ и $n^2 - nl + l^2 = 3$ тождество следует. Значение рода равно

$$g = \left(c^2\left(n^2 - nl + l^2\right) + 2 - (q+1)\right)/2 = \left((q+1)^2/3 + 2 - (q+1)\right)/2 = \left(q^2 - q + 4\right)/6 = g_3. \quad (5)$$

По классификации максимальных кривых это третье значение рода и наилучшая максимальная кривая Гурвица. ◊

ВЫВОДЫ

Впервые описаны семейства нетривиальных кривых Гурвица и представлены условия максимальности для кривых Гурвица общего вида со снятием ограничения на показатели степени кривой, впервые получена максимальная кривая Гурвица с третьим значением рода для максимальных кривых.

Литература.

[1] *Torres F.* Plan maximal curves, Acta Arith. 98(2) (2001), 165-179.

[2] *Cossidente A., Korchm'aros G. and Torres F.,* Curves of large genus covered by the Hermitian curve. Comm. Algebra 28(10), 4707–4728 (2000).

[3] *Carbonne P., Henocq T.,* Decomposition de la Jacobienne sur les corps finis. Bull. Polish Acad. Sci. Math. 42(3) (1994), 207-215.

[4] *Халимов Г.З.* Оценка параметров кривых Гурвица для целей универсального хеширования. Сб. трудов Первой международной научно-технической конференции "Компьютерные науки и технологии". Белгород, Россия. 8-10 октября 2009 г., ч. 2, с 118-121.

[5] *Jurgen Bierbrauer.* Authentication via algebraic-geometric codes. URL http://www.math.mtu.edu/~jbierbra/potpap.ps.

[6] *Халимов Г.З.* Максимальные кривые Гурвица для целей универсального хеширования. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. с.144-146

[7] *Lachaud G.* Sommes d'Eisenstein et nombre de points de certaines courbes algebriques sur les corps finis, C.R. Acad.Sci. Paris 305,Serie 1 (1987), 729-732.

[8] *Ruck H.G. and Stichtenoth,* A characterization of Hermition function fields over finite, J. Reine Angew. Math. 457, 185-188 (1994).

Поступила в редколлегию 2.06.2010.

Халимов Геннадий Зайдулович, канд. техн. наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: методы и средства высокоскоростной аутентификации данных.

УДК 681.3.06

Універсальне хешування за максимальними кривими Гурвіца / Г.З. Халімов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 365-369.

Представлені результати досліджень по максимальних кривих Гурвіця для цілей універсального хешування, умови максимальності узагальнених кривих, максимальна крива Гурвіця з третім значенням роду.

Ключові слова: універсальне хешування, криві Гурвіця.

Бібліогр.: 08 найм.

UDC 681.3.06

Universal hashing by the maximum of Hurwitz curves / G.Z. Halimov// Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 365-369.

The results of studies on the maximum Hurwitz curves for universal hashing and conditions for maximum generalized curves, the maximum Hurwitz curves with the third genus value are provided.

Key words: universal hashing, Hurwitz curves.

Ref.: 08 items.