дослучайных чисел, которые должны быть получены Проверяющим в неизменном виде.

СПИСОК ЛИТЕРАТУРЫ

1. *Brickell, E.* Direct Anonymous Attestation[Электронный ресурс] / Brickell E., Camenisch J. and Chen L. // Cryptology ePrint Archive. – Report 2004/205. – Режим доступа: http://eprint.iacr.org/2004/205/.
2. Trusted Computing Group [Электронный ресурс]. – Режим доступа: http://www.trustedcomputinggroup.org/.
3. *Chaum, D.* Blind Signatures for Untraceable Payments / Chaum D., Rivest R. L. and Sherman A. T. (Eds.) // Advances in Cryptology : proceedings of CRYPTO'82. – Plemum, New York, 1983. – P. 89–105.
4. *Brickell, E.* Simplified security notions of direct anonymous attestation and a concrete scheme from pairings / Brickell E., Chen L. and Li J. // International Journal of Information Security. – 2009. – Vol. 8. – P. 315–330.
5. *Stallman, R.* Can You Trust Your Computer? [Электронный ресурс] / Richard Stallman // Free Software Free Society: selected essays of Richard M. Stallman. – Режим доступа: http://www.gnu.org/philosophy/can-you-trust.html.
6. *Anderson, R.* 'Trusted Computing' Frequently Asked Questions [Электронный ресурс] / Anderson R. – Режим доступа: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.
7. Trusted Computing: Promise and Risk [Электронный ресурс] // Electronic Frontier Foundation whitepaper. – Режим доступа: http://www.eff.org/wp/trusted-computing-promise-and-risk.
8. *Fiat, A.* How to Prove Yourself: Practical Solutions to Identification and Signature Problems / Fiat A. and Shamir A. // Lecture Notes in Computer Science. – 1987. – Vol. 263. – P.186–194.
9. *Camenisch, J.* A Signature Scheme with Efficient Protocols / Camenisch J. and Lysyanskaya A. // Lecture Notes in Computer Science. – 2003. – Vol. 2576. – P.268–289.
10. *Fedyukovych, V.* A strategy for any DAA Issuer and an additional verification by a Host [Электронный ресурс] / V. Fedyukovych // Cryptology ePrint Archive. – Report 2008/277. – Режим доступа: http://eprint.iacr.org/2008/277/.
11. *Федюкович, Е.* Восстановление анонимности при использовании протоколов DAA [Электронный ресурс] / В. Е. Федюкович // Рускрипто 2009. – Режим доступа: http://ruscrypto.ru/sources/conference/rc2009/.
12. *Brickell, E.* Enhanced Privacy ID from Bilinear Pairing [Электронный ресурс] / Brickell E. and Li J. // Cryptology ePrint Archive. – Report 2009/095. – Режим доступа: http://eprint.iacr.org/2009/095/.
13. *Chaum, D.* Wallet Databases with Observers / Chaum D. and Pedersen T. P. // Lecture Notes in Computer Science. – 1993. – Vol. 740/1993. – P. 89–105.

Надійшла 1.11.2010

Федюкович В. Є.

ПРО ДОДАТКОВУ ПЕРЕВІРКУ СЕРТІФІКАТА СХЕМИ DAA

Було виконано аналіз схеми DAA. Було знайдено, що схема не є анонімною: Емітент може випустити сертифікат, який завжди може впізнати Перевіряючий. Також було запропоновано додаткове рівняння перевірки, щоб уникнути такої атаки.

Ключові слова: DAA, анонімність, атрибуція, протокол доказу знання, TPM.

Fedyukovych V.

ON ADDITIONAL VERIFICATION OF DDA CERTIFICATE

A strategy for colluding Issuer and Verifier with DAA scheme was found to let such an adversary always distinguish honest Users that were issued 'tagged' certificates voiding anonymity property of DAA. Additional verification equation was introduced to detect such an attack.

Key words: DAA, anonimity, authentication, proof of knowledge, TPM.

УДК 681.3.06

Халимов Г. З.

Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники

ОЦЕНКА ПАРАМЕТРОВ КРИВЫХ ФЕРМА ДЛЯ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ

Получены точные решения для числа точек кривых Ферма, когда порядок поля имеет делители 2, 3 и 6, также оценки числа точек на основе вероятностного подхода. Приводятся асимптотические границы отношения максимального числа точек кривой Ферма в простом поле к ее роду и к границе Хассе – Вейля.

Ключевые слова: универсальное хеширование, кривые Ферма.

ОБЩАЯ ПОСТАНОВКА ЗАДАЧИ И ЕЕ АКТУАЛЬНОСТЬ

Универсальное хеширование на основе алгеброгеометрического подхода впервые было предложено Биербрауэром и Кабатинским [1]. Пусть задана абсолютно неразложимая, несингулярная проективная кривая χ над полем F_q с точками $P = \{P_1, P_2, \ldots, P_n\} \in \chi(F_q)$. 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 $m = (m_1, m_2, \ldots, m_k)$, $m_i \in F_q$ 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 $0 < u_1 < u_2 < \ldots < u_k$. Хеш-функция $h_{P_j}(m)$ опреде-

ляет универсальный хеш-класс $\varepsilon - U(N, q^k, q)$, где вероятность коллизии $\varepsilon \le u_k/N$, N – число точек алгебраической кривой, q^k – объем пространства сообщений, q – объем пространства хеш-кодов. Хеш-функция $h_{P_j}(m)$ является ключевой, ее значение зависит от точки P_j кривой χ. Оценка для вероятности коллизии зависит от алгеброгеометрических параметров кривой.

Утверждение 1. [2] Вероятность коллизии при универсальном хешировании (1) при $k > 2g - 1$, где g – род алгебраической кривой и N – число точек кривой, определяется границей

$$\varepsilon \le (k + g - 1)/N. \qquad (2)$$

Проблематика построения схем универсального хеширования на основе алгеброгеометрического представления заключается в выборе алгебраических кривых с требуемыми параметрами, прежде всего с как можно большим отношением числа точек кривой к ее роду, а также с реализацией вычислений в конечном поле F_q, простотой вычислений и согласованностью с представлением информационных данных. Интерес представляют конструкции простых полей с модулями $2^m \pm 1$ или близких к ним простых чисел. В представленных материалах отображены основные результаты исследований по кривым Ферма в простом поле для целей универсального хеширования.

Целью статьи является нахождение оценок для числа решений кривой Ферма в простом поле. В разделе 1 рассмотрены основные свойства кривых Ферма и точные значения числа точек для кривых Ферма в простом поле. В разделе 2 на основе вероятностного подхода получены оценки числа решений уравнения Ферма в конечном поле. В разделе 3 приводятся асимптотические результаты по кривым Ферма над простым полем.

1. ТОЧНЫЕ ЗНАЧЕНИЯ ЧИСЛА ТОЧЕК ДЛЯ КРИВЫХ ФЕРМА В ПРОСТОМ ПОЛЕ

Кривые Ферма Fr_m определяются выражением

$$X^m + Y^m + Z^m = 0, \qquad (3)$$

имеют частные производные вида $F_X = mX^{m-1}$, $F_Y = mY^{m-1}$, $F_Z = mZ^{m-1}$. Рассмотрим основные свойства кривых Ферма для случая простого поля F_q.

Утверждение 1. Пусть кривая Ферма Fr_m определена над простым полем F_q. Справедливо следующее:

1) кривая Fr_m является неприводимой, несингулярной кривой степени m без особенностей, рода $g = \dfrac{(m-1)(m-2)}{2}$;

2) если m взаимно просто с $q - 1$, тогда $X^m + Y^m + Z^m = 0$ изоморфна $X + Y + Z = 0$ и имеет число точек $N = q + 1$;

3) кривая вида $X^{(q-1)/3} + Y^{(q-1)/3} + Z^{(q-1)/3} = 0$ имеет $N = 2(q-1)^2/9$ и $g = (q-4)(q-7)/18$;

4) кривая вида $X^{(q-1)/2} + Y^{(q-1)/2} + Z^{(q-1)/2} = 0$ имеет $N = 3(q-1)/2$ и $g = (q-3)(q-5)/8$;

5) кривая вида $X^{(q-1)/6} + Y^{(q-1)/6} + Z^{(q-1)/6} = 0$ имеет число точек $N = (q-1)/2 + (q-1)^2/18$ и род $g = (q-7)(q-13)/72$;

6) кривая $X^{(q-1)/2^m} + Y^{(q-1)/2^m} + Z^{(q-1)/2^m} = 0$ имеет род $g = (q - 2^m - 1)(q - 2^m - 2)/2^{2m+1}$ и число точек $N = 3(q-1)/2^m$, если $\left|2^{2^{m-1}}\right| \ne 1 (\mathrm{mod} q)$ и $N = 3(q-1)/2^m + 3(q-1)^2/2^{2m}$, если $2^{2^{m-1}} = -1 (\mathrm{mod} q)$.

Результаты 1 и 2 являются очевидными и известными. Результаты 3–6 получаются методом подсчета числа решений для уравнений Ферма на основе свойства суммы элементов мультипликативной подгруппы второго, третьего и шестого порядка. Значение рода кривой определяется формулой Римана – Роха.

Результат 3 следует из того, что решениями уравнения кривой в проективном пространстве P^2 над F_q являются точки $(\gamma : \xi : 1)$, для которых справедливо $\gamma^{(q-1)/3} + \xi^{(q-1)/3} + 1 = 0$. Так как $\gamma, \xi \in F_q$ и $\gamma = \alpha^i$, $\xi = \alpha^j$, α – образующий элемент поля, имеем $\alpha^{i(q-1)/3} + \alpha^{j(q-1)/3} + 1 = 0$ или $\beta^i + \beta^j + 1 = 0$, где $\beta = \alpha^{(q-1)/3}$ – образующий элемент мультипликативной подгруппы третьего порядка. В силу свойства $\sum_{k=0}^{n-1} \beta^k = 0$ для элементов мультипликативной группы порядка n получим, что уравнение Ферма имеет решение, если и только если $\beta^{(i)} = \beta^1$ и $\beta^{(j)} = \beta^2$, где $(\cdot)$ обозначает вычисление значения степени по модулю порядка β, а так же если $\beta^{(i)} = \beta^2$ и $\beta^{(j)} = \beta^1$. Число решений по каждому набору условий равно $(q-1)^2/9$ и $N = 2(q-1)^2/9$.

Результат 4 является очевидным. Элементы поля $\alpha^{i(q-1)/2}$ принадлежат мультипликативной подгруппе второго порядка: $1, \beta = \alpha^{(q-1)/2}$ и $1 + \beta = 0$. Кривая Ферма имеет решения, если одна из координат P^2, например $z = 0$, а две другие удовлетворяют равенствам $Y^{(q-1)/2} = 1$ и $X^{(q-1)/2} = \beta$. Искомыми решениями являются $y = 1$ и $x = \alpha^{2i+1}$, $i = \overline{0, (q-1)/2 - 1}$. Общее число решений с учетом перестановок координат будет $N = 3(q-1)/2$.

Аналогично получим результат 5. Элементы поля $\alpha^{i(q-1)/6}$ принадлежат мультипликативной группе шестого порядка: $1, \beta^1, \beta^2, \beta^3, \beta^4, \beta^5$, где $\beta = \alpha^{(q-1)/6}$. Мультипликативная группа шестого порядка включает мультипликативные подгруппы вто-

рого порядка $1, \beta^3$ и третьего $1, \beta^2, \beta^4$. По свойству суммы элементов мультипликативной группы имеем $1 + \beta^3 = 0$ и $1 + \beta^2 + \beta^4 = 0$. Первое условие дает $(q-1)/6$ решений для уравнения кривой в виде $z = 0$, $y = 1$ и $x = \alpha^{3(2i+1)}$, $i = \overline{0, (q-1)/6 - 1}$, а с учетом перестановки координат – $3(q-1)/6$ решений. Второе условие – $2(q-1)^2/6$ решений по аналогии с доказательством результата 3. Так как элементы подгрупп не пересекаются и нет других подгрупп порядка 2 или 3, общее число решений $N = (q-1)/2 + (q-1)^2/18$.

Для вывода результата 6 заметим, что элементы поля $\alpha^{i(q-1)/2^m}$ принадлежат мультипликативной группе порядка 2^m: $1, \beta, \beta^2, \ldots, \beta^{2^m-1}$, где $\beta = \alpha^{(q-1)/2^m}$.

Мультипликативная группа содержит мультипликативные подгруппы только четных порядков 2^e, $e = \overline{1, m}$. Если $\left|2^{2^{m-1}}\right| \neq 1 (\mathrm{mod} q)$, уравнение Ферма имеет только решения, когда одна из координат, например $z = 0$, а две другие удовлетворяют равенствам $Y^{(q-1)/2^m} = 1$ и $X^{(q-1)/2^m} = \gamma$, где γ есть элемент подгруппы второго порядка. Решением по координате y является значение $y = 1$, а по координате x являются точки $x = \alpha^{2^m i + 2^{m-1}}$, $i = \overline{0, (q-1)/2^m - 1}$. Общее число решений с учетом перестановок координат будет $N = 3(q-1)/2^m$.

Если $2^{2^{m-1}} = -1 (\mathrm{mod} q)$, в подгруппе порядка 2^m: $1, \beta, \beta^2, \ldots, \beta^{2^m-1}$, существует элемент $\alpha = 2$, в силу $(2^{2^{m-1}})^2 = 1 (\mathrm{mod} q)$. Все степени α порождают подгруппу 2^m порядка, которая является перестановкой элементов подгруппы $1, \beta, \beta^2, \ldots, \beta^{2^m-1}$. Очевидно, что среди элементов подгруппы $1, \alpha, \alpha^2, \ldots, \alpha^{2^m-1}$ будет элемент $\lambda = -2$, так как $\alpha \bullet \alpha^{2^{m-1}} = 2 \bullet 2^{2^{m-1}} = -2 (\mathrm{mod} q)$ и элемент $\gamma = (q-1)/2$, в силу $\alpha^{2^{m-1}}/\alpha = 2^{2^{m-1}}/2 = (q-1)/2 (\mathrm{mod} q)$. В этом случае кривая Ферма имеет решения, которые определяются условиями: 1) $z = 0$, $Y^{(q-1)/2^m} = 1$, $X^{(q-1)/2^m} = \gamma$; 2) $Z^{(q-1)/2^m} = 1$, $Y^{(q-1)/2^m} = 1$, $X^{(q-1)/2^m} = \lambda$; 3) $Z^{(q-1)/2^m} = 1$, $Y^{(q-1)/2^m} = \gamma$, $X^{(q-1)/2^m} = \gamma$. Число решений по условию 1), как и в предыдущем случае, равно $N_1 = 3(q-1)/2^m$. По условию 2) число корней по каждой координате y и x равно $(q-1)/2^m$, и с учетом перестановок координат общее число решений равно $N_2 = 2(q-1)^2/2^{2m}$. Аналогично для условия 3) с учетом, что перестановок по координатам нет, $N_3 = (q-1)^2/2^{2m}$. Общее число решений определяется суммой $N_1 + N_2 + N_3$, что дает искомое N.

Пример 1. Уравнения $X^m + Y^m + Z^m = 0$ над F_q при $q = 257$ соответствуют случаю, когда делителями порядка поля $q - 1 = 256$ являются степени двойки. Прямое вычисление решений при $m = 128, 64, 32, 16$ дает значения $N = 384, 192, 96, 816$. При $m = 128, 64, 32$ выполняется первое условие для результата 6, т. е. $\left|2^{(q-1)/(2m)}\right| \neq 1 (\mathrm{mod} q)$, и число точек кривой равно $N = 3(q-1)/((q-1)/m) = 3m$, что совпадает с прямыми вычислениями. Для $m = 16$ справедливо $2^{(q-1)/(2m)} = -1 (\mathrm{mod} q)$ и $N = 3m + 3m^2$, что также совпадает с точным значением.

Точные вычисления числа решений для уравнений Ферма, когда степень уравнения является произвольным делителем порядка конечного поля F_q, является трудоемкой задачей. Ниже рассматриваются оценочные значения для числа точек.

2. ОЦЕНКИ ДЛЯ ЧИСЛА ТОЧЕК КРИВЫХ ФЕРМА В КОНЕЧНОМ ПОЛЕ

Оценки числа решений уравнения Ферма в конечном поле F_q получим на основе вероятностного подхода.

Теорема 1. Пусть кривая $X^m + Y^m + Z^m = 0$ определена над простым полем F_q, где m есть делитель $q - 1$. Оценка для числа точек кривой Ферма при $m > 2$ равна

$$N \approx 2\left\lceil \frac{(q-1)}{2m^2} \right\rceil m^2, \qquad (4)$$

где $\lceil x \rceil$ – округление числа до большего целого.

Доказательство. Решениями уравнения кривой в проективном пространстве P^2 над F_q являются точки $(\gamma : \xi : 1)$, для которых справедливо $\gamma^m + \zeta^m + 1 = 0$ или $\delta + \eta + 1 = 0$, с учетом подстановки $\gamma^m = \delta$, $\zeta^m = \eta$. Пусть $\delta = \beta^i$, $\eta = \beta^j$, где β – образующий элемент поля F_q. Первое условие $\gamma^m + \zeta^m + 1 = 0$ определяет, что степени i и j должны иметь делитель m и β^i, β^j должны удовлетворять второму условию $\delta + \eta + 1 = 0$. Число пар δ, η, удовлетворяющих условию $\delta + \eta + 1 = 0$, равно $(q-1)/2$, а число элементов поля β^i, которые имеют делитель степени m, равно $(q-1)/m$. Образующий элемент $\beta = a$ выбирается из множества чисел $\overline{0, q-1}$, и элементы числового поля вычисляются по правилу $a^i \mathrm{mod} q$. Последнее выражение определяет рандомизатор, для которого соответствие между числовым значением элемента мультипликативной группы и его индексом является псевдослучайным. Таким образом, среднее число пар δ, η, удовлетворяющих условиям 1 и 2, будет равно $n = \frac{(q-1)}{2} \cdot P(i = 0 \mathrm{mod} m, j = 0 \mathrm{mod} m)$, где сомножитель $(q-1)/2$ определяет общее число δ, η, удовлетворяющих условию $\delta + \eta + 1 = 0$, а $P(i = 0 \mathrm{mod} m, j = 0 \mathrm{mod} m)$ – вероятность того, что индексы элементов δ, η имеют делитель m. Предполагая равновероятность распределения индексов элементов поля в парах δ, η, полу-

чим $P(i = 0 \bmod m,\ j = 0 \bmod m) = 1/m^2$ и оценку для n в виде $n = (q-1)/2m^2$. Так как число пар есть целое число, выполним округление n до большего целого. Округление к ближайшему целому для случаев, когда $m > \sqrt{(q-1)}$, привело бы к нулевой оценке числа решений, что не является верным (см. утв. 1). Наконец, учтем перестановку пар по координатам x, y и то, что по каждой координате число корней равно m, получим искомое выражение N. ◊

Рассмотрим следствия данной теоремы, но сначала отметим следующую полезную лемму.

Лемма 1. Пусть кривая $X^m + Y^m + Z^m = 0$ определена над простым полем F_q, где m есть делитель $q-1$. Справедливо следующее:

1) если $(q-1)/m$ содержит делитель 2, в число решений входит $3m$;

2) если $(q-1)/m$ содержит делитель 3, в число решений входит $2m^2$;

3) если $(q-1)/m$ содержит делители 2 и 3, в число решений входит $3m+2m^2$;

4) если $(-2)^{(q-1)/m} = 1 (\bmod q)$, в число решений входит $3m^2$.

Доказательство прямо следует из результатов утверждения 1.

Следствия теоремы 1 с уточнением по результатам леммы 1 представлены в предложении 1.

Предложение 1. Пусть кривая $X^m + Y^m + Z^m = 0$ определена над простым полем F_q, где $m > 2$ есть делитель $q-1$. Оценки числа точек N для кривой Ферма имеют следующий вид.

A) Если $(-2)^{(q-1)/m} \neq 1 (\bmod q)$,

1) $(q-1)/m = 0 (\bmod 2)$, $(q-1)/m \neq 0 (\bmod 3)$, тогда $N \approx 3m + 2\langle (q-1)/(2m^2) \rangle_3 m^2$;

2) $(q-1)/m \neq 0 \bmod 2$, $(q-1)/m = 0 \bmod 3$, тогда $N \approx 2(1 + \langle (q-1)/(2m^2) - 1 \rangle_3) m^2$;

3) $(q-1)/m = 0 \bmod 6$, тогда $N \approx 3m + 2(1 + \langle (q-1)/(2m^2) - 1 \rangle_3) m^2$;

4) $(q-1)/m \neq 0 \bmod 2$, $(q-1)/m \neq 0 \bmod 3$, тогда $N \approx 2\langle (q-1)/(2m^2) \rangle_3 m^2$.

B) Если $(-2)^{(q-1)/m} = 1 (\bmod q)$,

1) $(q-1)/m = 0 (\bmod 2)$, $(q-1)/m \neq 0 (\bmod 3)$, тогда $N \approx 3m + 2\langle (q-1)/(2m^2) - 1 \rangle_3 m^2 + 3m^2$;

2) $(q-1)/m \neq 0 \bmod 2$, $(q-1)/m = 0 \bmod 3$, тогда $N \approx 2(1 + \langle (q-1)/(2m^2) - 2 \rangle_3) m^2 + 3m^2$;

3) $(q-1)/m = 0 \bmod 6$, тогда $N \approx 3m + 2(1 + \langle (q-1)/(2m^2) - 2 \rangle_3) m^2 + 3m^2$;

4) $(q-1)/m \neq 0 \bmod 2$, $(q-1)/m \neq 0 \bmod 3$, $N \approx 2\langle (q-1)/(2m^2) - 1 \rangle_3 m^2 + 3m^2$.

Здесь $\langle x \rangle_3$ – округление x до ближайшего целого, кратного 3.

Доказательство следует из результатов теоремы 1 и леммы 1. Вычисления оценочных значений числа точек и точные вычисления дают хорошее совпадение. Так, для $q = 1021$ имеем совпадение результатов при $m = 510,340,255,204,170,102,85,68,60,51,34,30,20,17,12,5,3,2$ и число точек $N = 1530,231200,765,0,58310,306,14705,9248,0,153,2414,90,800,629,864,965,1008,1022$. Для значений $m = 15,10,6,4$ точные $N = 45,1430,882,1088$, а приближенные $N' = 1335,830,1098,992$. Расхождения проявляются и могут быть существенными, когда степень уравнения становится меньше $\sqrt{q}$. Относительная погрешность вероятностной оценки уменьшается с ростом q.

3. АСИМПОТИЧЕСКИЕ РЕЗУЛЬТАТЫ ПО КРИВЫМ ФЕРМА НАД ПРОСТЫМ ПОЛЕМ

Асимптотические результаты по кривым Ферма над простым полем определяются теоремами 2, 3.

Теорема 2. Асимптотическая граница для отношения максимального числа точек $N_g(q)$ к ее роду g для кривой Ферма в простом поле определяется выражением

$$\limsup_{g \to \infty} \frac{N_g(q)}{g} = 10. \qquad (5)$$

Доказательство. Предел отношения $N_g(q)/g$ определяется максимальной оценкой для числа точек кривых Ферма. Род кривой Ферма равен $g = (m-1)(m-2)/2$, где m – степень уравнения. Движение $g \to \infty$ возможно, когда $q \to \infty$ и $m \to q$. Подставляя в предел отношения $N_g(q)/g$ максимальное значение для числа точек на кривой в простом поле $N \approx 3m + 2(1 + \langle (q-1)/(2m^2) - 2 \rangle_3) m^2 + 3m^2$, что соответствует условию $(-2)^{(q-1)/m} = 1 (\bmod q)$ и $(q-1)/m = 0 (\bmod 6)$ предложения 1, получим искомую оценку (5). ◊

Теорема 3. Асимптотическая граница отношения максимального числа точек $N_g(q)$ для кривой Ферма в простом поле к максимальному числу точек по границе Хассе – Вейля определяется выражением

$$\limsup_{g \to \infty} \frac{N_g(q)}{N_g(q)_{HV}} = \frac{5}{\sqrt{q}}. \qquad (6)$$

Доказательство. Из теоремы 2 следует, что максимальная оценка для числа точек кривых Ферма в простом поле имеет вид $N \approx 3m + 2(1 + \langle (q-1)/(2m^2) - 2 \rangle_3) m^2 + 3m^2$. Выразим m из выражения для рода кривой. Для больших g справед-

ливо $g \approx m^2/2$ и $m \approx \sqrt{2g}$. Подставляя последний результат m в выражение для числа точек, получим

$$N_g(q) = 2\sqrt{2g} + 4(1 + \langle (q-1)/(4g^2) - 2 \rangle_3)g + 6g.$$

Граница Хассе – Вейля для максимальных кривых равна $N_g(q)_{HV} = q + 1 + 2g\sqrt{q}$. Вычисление $\limsup_{g \to \infty} N_g(q)/N_g(q)_{HV}$ даст (6). ◊

Точные вычисления $N_g(q)/g$ согласуются с результатами (5) и (6). Так, для $q = 257$ и $m = 16$ имеем $N = 816$ и $N_g(q)/g = 7{,}76$, а для $q = 2^{16} + 1 = 65537$ и $m = 2048$ имеем $N = 12589056$ и $N_g(q)/g = 6{,}01$.

ВЫВОДЫ

1. В простом поле не существует максимальных кривых Ферма. При большом роде проигрыш границе Хассе – Вейля пропорционален $1/(\sqrt{q})$. С уменьшением рода кривой значение числа точек приближается к границе Хассе – Вейля, и при $g = 0{,}1$ имеем тривиальный случай $N = q + 1$.

2. Универсальное хеширование по кривым Ферма в простом поле не обеспечивает требования по вероятности коллизии. В соответствии с выражением (2) для є алгебраическая кривая должна быть большого рода, с большим числом точек и значительным отношением $N_g(q)/g$. Асимптотика $N_g(q)/g$ для кривых Ферма равна 10. Кривые малого рода проигрывают по параметру N, что не обеспечивает требования по вероятности коллизии для практических значений q.

3. Результаты для кривых Ферма представлены для простого поля и частично могут быть отнесены к свойствам кривых в расширениях конечного поля. Расширенные конечные поля имеют большее многообразие по комбинаторным свойствам, что влияет на оценки параметров кривых.

СПИСОК ЛИТЕРАТУРЫ

1. *Bierbrauer, J.* On families of hash functions via geometric codes and concatenation. / Bierbrauer J., Johansson T., Kabatianskii G., Smeets B. // Advances in Cryptology-CRYPTO'93 Proceedings. – Springer-Verlag, 1994. – P. 331–342.
2. *Халимов, Г. З.* Коллизионные оценки универсального хеширования на основе схем с алгебраическими кодами / Халимов Г. З. // Прикладная радиоэлектроника. – 2009. – Т. 8, Вып. 3. – С. 338–342.

Надійшла 25.10.2010

Халімов Г. З.

ОЦІНКА ПАРАМЕТРІВ КРИВИХ ФЕРМА ДЛЯ УНІВЕРСАЛЬНОГО ГЕШУВАННЯ

Отримано точні рішення для числа точок кривих Ферма, коли порядок поля має дільники 2, 3 та 6, також оцінки числа точок на основі ймовірнісного підходу. Приводяться асимптотичні границі відношення максимального числа точок кривої Ферма в простому полі до її роду та до границі Хассе – Вейля.

Ключові слова: універсальне гешування, криві Ферма.

Khalimov G. Z.

ESTIMATION OF FERMA CURVES PARAMETERS FOR UNIVERSAL HASHING OF NUMBER SOLUTION FOR HURVITZ EQUATION IN THE FINITE FIELD

Exact solutions for a number of Ferma curves points when the field order has dividers 2, 3 and 6 as well as estimates of points number have been obtained using probabilistic approach. Asymptotic boundaries of the ratio of maximum number of Ferma curve points in a simple field to its genus and to Hasse–Weil boundary are given.

Key words: universal hashing, Ferma curves.

УДК 004

Овсяк О. В.

Канд. техн. наук, доцент Львівської філії Київського національного унів ерситету культури і мистецтв

МОДЕЛЬ РОЗШИРЕНОЇ НОТАЦІЇ ТЕКСТОВОГО ОПИСУ ФОРМУЛ АЛГОРИТМІВ

З метою запису у пам'ять комп'ютера графічно-текстових формул алгоритмів, які утворені фукційними унітермами з впорядкованими змінними і параметрами, створено розширену **xml**-подібну нотацію опису формул алгоритмів. Модель розширеної нотації описана засобами алгебри алгоритмів з використанням операції секвентування. Наведено приклад використання розширеної нотації для опису формули алгоритму Евкліда.

Ключові слова: модель, нотація, синтаксис, семантика, унітерм, секвенція, елімінування, паралелення.

ВСТУП

Для опису алгоритмів інформаційних технологій і систем найчастіше використовуються вербальний і блок-схемний методи. Відомо, що ці методи, як і методи машин Тюрінга [1], Поста [2], Колмогорова [3], Ахо – Ульмана – Хопкрофта [4], Шонхаге [5] і рекур-