Таблиця 3 – Результати тестування послідовностей, утворених шляхом випадкового чергування лінійних рекурент та якісного генератора псевдовипадкових чисел, з шумом, $p = 0.01$

Довжина блоку	Тест LP			Тест NIST		
	Номер послідовності					
	1	2	3	1	2	3
500	-	-	-	-	-	+
1000	-	-	-	+	+	+
2000	-	-	-	+	+	+
3000	-	-	-	+	+	+
4000	-	-	-	+	+	+
5000	-	-	-	+	+	+

Таблиця 4 – Результати тестування послідовностей, утворених шляхом випадкового чергування лінійних рекурент та гарного генератора псевдовипадкових чисел, з шумом, $p = 0.02$

Довжина блоку	Тест LP			Тест NIST		
	Номер послідовності					
	1	2	3	1	2	3
500	-	-	-	+	+	+
1000	-	-	-	+	+	+
2000	+	+	-	+	+	+
3000	+	+	+	+	+	+
4000	+	+	+	+	+	+
5000	+	+	+	+	+	+

IV Висновки

Запропоновано новий тест оцінки випадковості, що базується на властивостях профілю лінійної складності випадкової послідовності. Статистика тесту LP заснована на кількості стрибків лінійної складності на відрізках вхідної послідовності певної довжини. На деяких типах неякісних послідовностей новий тест показує кращі результати, ніж тест на лінійну складність з набору NIST; крім того, тест LP має більш просту реалізацію через нормально розподілену статистику, на відміну від специфічного розподілу у тесті NIST. Швидкість роботи обох тестів приблизно однакова, адже обидва використовують для розрахунків алгоритм Берлекемпа-Мессі.

Література: ***1.*** *NIST Special Publications 800-22, A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. – 2000.* ***2.*** *J. L. Massey. Shift-register synthesis and BCH decoding // IEEE Trans. Information Theory , 1969. – IT-15 (1). – pp. 122–127.* ***3.*** *A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. – CRC Press, 1996. – 816 p.* ***4.*** *K. Hamano, F. Sato, H. Yamamoto. A new randomness test based on linear complexity profile // IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science, E92.A(2009). – No1. – pp.166-172.* ***5.*** *R. A. Rueppel. Analysis and Design of Stream Ciphers. – N.Y.: Springer-Verlag, 1986. – 236 p.* ***6.*** *В. Феллер. Введение в теорию вероятностей и ее приложения. В 2-х томах. Т1. – М.: МИР, 1967 – 498 с.*

УДК 681.3.06

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО РАЦИОНАЛЬНЫМ ФУНКЦИЯМ АЛГЕБРАИЧЕСКИХ КРИВЫХ В КУБИЧЕСКОМ ПОЛЕ

Геннадий Халимов
Харьковский национальный университет радиоэлектроники

Аннотация: **Представлено универсальное хеширование по рациональным функциям алгебраических кривых с большим числом точек в кубическом поле.**
Summary: **Present the universal hashing of rational functions of algebraic curves with many points in a cubic field.**

Ключевые слова: **Универсальное хеширование, алгебраические кривые.**

I Введение

Универсальное хеширование на функциональном поле проективных многообразий по точкам алгебраических кривых определяет построение доказуемой безусловной аутентификации [1 – 4]. В работе [1] определено универсальное хеширование по линейному базисному пространству алгебраических кодов. В работах [2 – 4] определено хеширование по функциональному полю максимальных кривых Эрмита, Гурвица и представлены их свойства. Наилучший результат достигается на максимальных кривых, число точек которых лежит на границе Хассе-Вейля. Проблематика построения универсального хеширования на основе алгеброгеометрических методов заключается в выборе алгебраических кривых и связанных с ними функциональных полей. Вероятность коллизии универсального хеширования по рациональным функциям алгебраических кривых определяется отношением значения полюса базисных функций к числу точек кривой над конечным полем. Интерес представляют кривые с как можно большим числом точек кривой. В представленных материалах отображены исследования по универсальному хешированию в кубическом поле.

Целью статьи является определение универсального хеширования по рациональным функциям алгебраических кривых Ферма и Гурвица с большим числом точек в кубическом поле. В разделе 1 приводятся основные результаты по алгебраическим кривым в кубическом поле, в разделе 2 – определение и свойства универсального хеширования на функциональном поле алгебраических кривых в кубическом поле.

II Основные результаты по алгебраическим кривым в кубическом поле

Известные результаты.

1. В кубическом поле не существует максимальных кривых. Наилучший результат по асимптотическому отношению максимального числа точек $N_g\left(q^3\right)$ к её роду g достигается $\limsup_{g\to\infty} N_g\left(q^3\right)/g = 2q-4$ для кривой Ферма [5]

$$X^{q^2+q+1}+Y^{q^2+q+1}+Z^{q^2+q+1} \tag{1}$$

и кривой Гурвица (кривая представлена в [6], свойства определяются теоремой 1)

$$X^{q^2-1}Y^{q-1}+Y^{q^2-1}+X^{q-1}=0. \tag{2}$$

2. При большом роде проигрыш границе Хассе-Вейля в кубическом поле для кривых Ферма и Гурвица пропорционален $1/\sqrt{q}$. С уменьшением рода кривой значение числа точек приближается к границе Хассе-Вейля.

3. Кривая $X^{q^2+q+1}+Y^{q^2+q+1}+Z^{q^2+q+1}$ имеет $N=(q-2)\left(q^2+q+1\right)^2+3\left(q^2+q+1\right)$, F_{q^3} рациональных точек, род $g=\left(q^2+q\right)\left(q^2+q-1\right)/2$.

- Точками кривой являются q^2+q+1 точек $P_{a,b}=(a:b:0)$ и точки $P_{a,b}=(a:b:1)$, где $a,b\in F_q$ и $a^{q^2+q+1}+b^{q^2+q+1}+1=0$.
- Базис пространства $L(mP_\infty)$ задается функциями вида $\{x^i\cdot y^j:(i+j)(q^2+q+1)\le m\}$ (лемма 1).

4. Кривая $X^{q^2-1}Y^{q-1}+Y^{q^2-1}+X^{q-1}=0$ имеет $N=\left(q^3-1\right)\left(q^2-1\right)$, F_{q^3} рациональных точек вида $P_{a,b}=(a:b:1)$, $a,b\in F_q$, $a\neq 0$, $b\neq 0$, $a^{q^2-1}b^{q-1}+b^{q^2-1}+a^{q-1}=0$ и три точки $P_0=(1:0:0)$, $P_1=(0:1:0)$, $P_2=(0:1:0)$. Род кривой $g=1+1/2\left\{(q-1)^2\left(q^2+q+1\right)-3(q-1)\right\}$.

- Функциональное поле кривой определяется рациональными функциями $x=X/Z$, $y=Y/Z$. Базис пространства $L(mP_\infty)$ задается полиномами $x^i\cdot y^j$.

Теорема 1. Кривая $X^{q^2-1}Y^{q-1}+Y^{q^2-1}+X^{q-1}=0$ имеет число F_{q^3} рациональных точек, $N=\left(q^3-1\right)\left(q^2-1\right)$ и род $g=1+1/2\left\{(q-1)^2\left(q^2+q+1\right)-3(q-1)\right\}$.

Кривую $X^{q^2-1}Y^{q-1}+Y^{q^2-1}+X^{q-1}=0$ получим из полинома $r(T)=T^{q^2-1}+T^{q-1}+1$ с использованием преобразования $X^t f_q\left(X^s Y\right)$. Действительно, если $s=q$ и $t=q-1$, получим искомую кривую $X^{q-1}f_q\left(X^q Y\right)=X^{q^3-1}Y^{q^2-1}+X^{q^2-1}Y^{q-1}+X^{q-1}=Y^{q^2-1}+X^{q^2-1}Y^{q-1}+X^{q-1}$, так как $X^{q^3-1}=1$. Полином $r(T)=T^{q^2-1}+T^{q-1}+1$ имеет q^2-1 нулей в F_{q^3}. С учетом подстановки $T=X^qY$ и порядка q^3-1 для элемента поля по координате X, общее число решений без точек на бесконечности будет равно $\left(q^3-1\right)\left(q^2-1\right)$. Кривая $X^{q^2-1}Y^{q-1}+Y^{q^2-1}+X^{q-1}=0$ имеет три сингулярные точки на бесконечности с ветвлением $q-1$. При нечетной характеристике поля точки на бесконечности являются не рациональными. Род кривой следует из соотношения $g=(n^2-nl+l^2+2-3\gcd(n,l))/2$ для рода кривых Гурвица общего вида.

Пример 1. Пусть задано F_{3^3} и кривая Ферма $x^{13}+y^{13}+z^{13}=0$. Число точек кривой $N=208$. Первые 76 точек кривой представлены в табл. 1.

Таблица 1 – Точки кривой $x^{13}+y^{13}+z^{13}=0$

	***P*0**	***P*1**	***P*2**	***P*3**	***P*4**	***P*5**	***P*6**	***P*7**	***P*8**	***P*9**	***P*10**	***P*11**	***P*12**	***P*13**	***P*14**	***P*15**	***P*16**	***P*17**	***P*18**
z	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1
y	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
x	α^1	α^3	α^5	α^7	α^9	α^{11}	α^{13}	α^{15}	α^{17}	α^{19}	α^{21}	α^{23}	α^{25}	α^1	α^3	α^5	α^7	α^9	α^{11}
	***P*19**	***P*20**	***P*21**	***P*22**	***P*23**	***P*24**	***P*25**	***P*26**	***P*27**	***P*28**	***P*29**	***P*30**	***P*31**	***P*32**	***P*33**	***P*34**	***P*35**	***P*36**	***P*37**
z	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
x	α^{13}	α^{15}	α^{17}	α^{19}	α^{21}	α^{23}	α^{25}	1	α^2	α^4	α^6	α^8	α^{10}	α^{12}	α^{14}	α^{16}	α^{18}	α^{20}	α^{22}
	***P*38**	***P*39**	***P*40**	***P*41**	***P*42**	***P*43**	***P*44**	***P*45**	***P*46**	***P*47**	***P*48**	***P*49**	***P*50**	***P*51**	***P*52**	***P*53**	***P*54**	***P*55**	***P*56**
z	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	1	α^1	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^3	α^4	α^4	α^4
x	α^{24}	0	1	α^2	α^4	α^6	α^8	α^{10}	α^{12}	α^{14}	α^{16}	α^{18}	α^{20}	α^{22}	α^{24}	0	1	α^2	α^4
	***P*57**	***P*58**	***P*59**	***P*60**	***P*61**	***P*62**	***P*63**	***P*64**	***P*65**	***P*66**	***P*67**	***P*68**	***P*69**	***P*70**	***P*71**	***P*72**	***P*73**	***P*74**	***P*75**
z	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^5	α^6	α^6	α^6	α^6	α^6	α^6	α^6	α^6
x	α^6	α^8	α^{10}	α^{12}	α^{14}	α^{16}	α^{18}	α^{20}	α^{22}	α^{24}	0	1	α^2	α^4	α^6	α^8	α^{10}	α^{12}	α^{14}

Распределения кратностей пересечения полиномов базисного пространства $L(mP_\infty)$ и кривой без точек $P_{a,b}=(a:b:0)$ представлены в табл. 2. Хеш вычисления в конечном поле F_{3^3} по полиномиальному базису $L(39P_\infty)$ на кривой $x^{13}+y^{13}+z^{13}=0$ дает оценку вероятности коллизии $\varepsilon=m/N=39/195=0.2$.

Таблица 2 – Распределение кратности пересечения полиномов базисного пространства и кривой $x^{13}+y^{13}+z^{13}=0$

Базисное пространство	Число испытаний	Распределение кратности пресечения (значение числа точек пересечения =число опытов)			
1,x,y	10^5	9:=46581 13:=53254 195:=162			
1,x,y,x^2,xy,y^2	10^5	8:=56 9:=129 10:=2386 11:=10902 12:=22522	13:=24626 14:=15885 15:=8206 16:=7653	17:=1016 18:=1975 19:=1881 20:=1376	21:=675 22:=557 25:=119 26:=36

1,x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3	10^5	9:=15 10:=1334 11:=12163 12:=26593 13:=26731	14:=17674 15:=8805 16:=4010 17:=1593 18:=598	19:=259 20:=105 21:=67 22:=21 23:=17	24:=9 25:=3 26:=1 27:=1 30:=1
1,x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3, x^4,x^3y,x^2y^2,xy^3,y^4	10^6	9:=111 10:=13872 11:=118766 12:=260654 13:=265583	14:=176860 15:=93342 16:=42963 17:=17540	18:=6666 19:=2396 20:=793 21:=309	22:=106 23:=28 24:=9 25:=2

Действительно число точек кривой без точек $P_{a,b}=(a:b:0)$ равно $N=195$ и число совпадающих хешей при вычислении по полиномиальному базису $L(39P_\infty)$ не превышает значения 39. Число слов данных равно 10.

Пример 2. Пусть задано F_{3^3} и кривая Гурвица $x^8y^2+y^8+x^2=0$. Число точек кривой равно $N=211$. Первые 48 точек кривой представлены в табл. 3. Точки $P_0=(1:0:0)$ и $P_1=(0:1:0)$ определяются как точки на бесконечности.

Таблица 3 – Точки кривой $x^{12}y^6+y^{12}+x^6=0$

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}
z	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	0	1	0	1	1	1	1	1	1	1	1	α^1	α^1	α^1	α^1	α^1	α^1	α^1
x	1	0	0	1	α^1	α^3	α^9	α^{13}	α^{14}	α^{16}	α^{22}	1	α^4	α^5	α^7	α^{13}	α^{17}	α^{18}
	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}	P_{25}	P_{26}	P_{27}	P_{28}	P_{29}	P_{30}	P_{31}	P_{32}	P_{33}	P_{34}	P_{35}
z	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	α^1	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^3	α^3	α^3	α^3	α^3	α^3	α^3	α^3	α^4
x	α^{20}	α^4	α^8	α^9	α^{11}	α^{17}	α^{21}	α^{22}	α^{24}	1	α^2	α^8	α^{12}	α^{13}	α^{15}	α^{21}	α^{25}	α^3
	P_{36}	P_{37}	P_{38}	P_{39}	P_{40}	P_{41}	P_{42}	P_{43}	P_{44}	P_{45}	P_{46}	P_{47}	P_{48}	P_{49}	P_{50}	P_{51}	P_{52}	P_{53}
z	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
y	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^5	α^5	α^5	α^5	α^5	α^5	α^5	α^5	α^6	α^6	α^6
x	α^4	α^6	α^{12}	α^{16}	α^{17}	α^{19}	α^{25}	α^3	α^7	α^8	α^{10}	α^{16}	α^{20}	α^{21}	α^{23}	α^1	α^7	α^{11}

Распределения кратностей пересечения полиномов базисного пространства $L(mP_\infty)$ и кривой Гурвица без точек P_0 и P_1 представлены в табл. 4.

Хеш вычисления в конечном поле F_{3^3} для 10 слов данных по полиномиальному базису $L(30P_\infty)$ на кривой $x^8y^2+y^8+x^2=0$ дают оценку вероятности коллизии $\varepsilon=m/N=30/209=0.143$. Действительно число точек кривой $N=209$ и число совпадающих хешей при вычислении по полиномиальному базису $L(30P_\infty)$ не превышает значения 30. Это лучше чем по кривой $x^{13}+y^{13}+z^{13}=0$.

Таблица 4 – Распределение кратности пересечения полиномов базисного пространства и кривой $x^8y^2+y^8+x^2=0$

Базисное пространство	Число испытаний	Распределение кратности пресечения (значение числа точек пересечения =число опытов)			
1,x,y	10^5	8:=7258 10:=92588			
1,x,y,x^2,xy,y^2	10^6	8:=6 10:=2346 11:=62212	12:=192173 13:=199986 14:=209502	15:=58239 16:=62590 17:=93339	18:=24238 19:=49139 20:=46230

1,x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3	10^6	9:=2 10:=1116 11:=36886 12:=172491 13:=275473 14:=238725	15:=145317 16:=72649 17:=32772 18:=13759 19:=5924 20:=2730	21:=1212 22:=521 23:=243 24:=91 25:=30	26:=24 27:=12 28:=9 29:=12 30:=2
1,x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3, x^4,x^3y,x^2y^2,xy^3,y^4	10^6	10:=1258 11:=36520 12:=169706 13:=270302 14:=237785	15:=149127 16:=76857 17:=35013 18:=14578 19:=5642	20:=2073 21:=760 22:=250 23:=87 24:=30	25:=5 26:=4 27:=2 30:=1

Пример 3. Пусть задано F_{3^3} и проективная прямая $x+y+z=0$. Число точек кривой равно $N=28$. Точка $P_0=(1:0:0)$ является точкой на бесконечности. Хеш вычисления в конечном поле F_{3^3} для 10 слов данных по полиномиальному базису $L(9P_\infty)$ на проективной прямой $x+y+z=0$ дает оценку вероятности коллизии $\varepsilon = m/N = 9/27 = 0.33$.

Замечание 1. Чуть лучший результат для хеширования в кубическом поле дают кривые Гурвица (2). Этот выигрыш не существенный, так как степень кривой Гурвица q^2+q-2, а кривой Ферма - q^2+q+1 и по теореме Безу число точек пересечения гиперповерхностей функционального базиса с точками кривой отличается на значение, равное 3. Хеширование по проективной прямой сильно проигрывает по вероятности коллизии кривым Ферма и Гурвица. Сравнительные оценки представлены в выводах к п. 2.

III Определение универсального хеширования по алгебраическим кривым в кубическом поле

Определение 1. Хеш функция $h_{x,y}(m) \in F_{q^3}$ для сообщения m по рациональным функциям базисного пространства $L(\rho_k P_\infty)$ в точке x, y кривой $X^{q^2+q+1}+Y^{q^2+q+1}+Z^{q^2+q+1}$ определяется выражением

$$h_{x,y}(m) = \sum_{i\ge 0, j\ge 0, (i+j)(q^2+q+1)\le \rho_k} m_{i,j}\cdot x^i \cdot y^j , \qquad (5)$$

где $m_{i,j} \in F_{q^3}$ - слова сообщения m, параметр k определяет число слов данных.

Замечание 2. Выражение (5) можно применить для хеширования по кривой Гурвица $X^{q^2-1}Y^{q-1}+Y^{q^2-1}+X^{q-1}=0$ при соответствующей индексации степеней i и j, так как функциональное поле кривой определяется рациональными функциями $x = X/Z$, $y = Y/Z$.

Для теоретической оценки вероятности коллизии определим соответствие значения k показателям i, j степеней рациональных функций $x^i \cdot y^j$.

Лемма 1. Пусть $k < g$, g – род кривой, тогда $j = k - s(s-1)/2$, $i = s - j$ и $s = \left\lfloor (2k+1/4)^{1/2} - 1/2 \right\rfloor$, где $\lceil\cdot\rceil$ округление к большему целому числу.

Доказательство. Базис пространства $L(\rho_k P_\infty)$ задается функциями вида $\{x^i \cdot y^j : (i+j)(q^2+q+1) \le \rho_k\}$ и по теореме Безу ρ_k кратно q^2+q+1. Действительно степень кривой равна q^2+q+1 и число точек пересечения алгебраической кривой с однородными полиномами степени $i+j=s$ с учетом их кратностей равно $(i+j)(q^2+q+1)$. Значение k определяется числом всех комбинаций степеней i и j таких, что $i+j \le s$ и

$$k = s(s-1)/2 + j . \qquad (6)$$

Имеем оценку

$$s(s-1)/2 < k \le (s+1)s/2 . \quad (7)$$

Верхняя граница определяется значением $j = s$. Определим k по верхней границе. Рассмотрим неравенство $s^2 + s - 2k \ge 0$. При фиксированном k положительное решение для равенства имеет вид

$$s = \sqrt{2k + 1/4} - 1/2 .$$

Округление $s = \left\lfloor (2k+1/4)^{1/2} - 1/2 \right\rfloor$ к большому целому значению дает решение для неравенства (7) относительно ближайшего целого s. Решение относительно j следует из (6) и определяется $j = k - s(s-1)/2$. Решение относительно i есть $i = s - j$.

Утверждение 1. Хеширование по рациональным функциям кривой $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1}$ над полем F_{q^3} определяет универсальный хеш класс $\varepsilon - U((q-2)(q^2+q+1)^2 + 2(q^2+q+1), q^{3k}, q^3)$, где $(q-2)(q^2+q+1)^2 + 2(q^2+q+1)$ - число хеш функций (объём ключевого пространства), q^{3k} - объём пространства сообщений, q^3 - объём пространства хеш кодов. Вероятность коллизии ε определяется выражением

$$\varepsilon = \left\lceil (2k+1/4)^{1/2} - 1/2 \right\rceil / ((q-2)(q^2+q+1)+2) , \text{ если } k < g , \quad (8)$$

где g - род кривой, $\lceil \cdot \rceil$ есть округление значения до наибольшего целого.

Доказательство. Параметры универсального класса $\varepsilon - U((q-2)(q^2+q+1)^2 + 2(q^2+q+1), q^{3k}, q^3)$ следуют из определения кривой Ферма и числа её точек за вычетом q^2+q+1 точек вида $P_{a,b} = (a:b:0)$ над F_{q^3}. Вероятность коллизии ε определяется отношением $\varepsilon = \rho_k / N$, где ρ_k - значение полюса рациональной функций $f_k = x^i \cdot y^j$, i, j определяются по лемме 1, $N = (q-2)(q^2+q+1)^2 + 2(q^2+q+1)$ - число точек кривой. По определению базиса пространства $L(\rho_k P_\infty)$ значение полюса рациональной функций $x^i \cdot y^j$ равно $\rho_k = (i+j)(q^2+q+1) = s(q^2+q+1)$. Пусть $k < g$. По лемме 1 имеем $s = \left\lfloor (2k+1/4)^{1/2} - 1/2 \right\rfloor$ и подстановка в выражение для ρ_k даёт соотношение (8)

Следствие 1. Асимптотика вероятности коллизии универсального хеширования по кривой $X^{q^2+q+1} + Y^{q^2+q+1} + Z^{q^2+q+1}$, при больших значениях размерности поля $q^3 \to \infty$ имеет вид

$$\varepsilon_{q^3 \to \infty} = \sqrt{2} k^{1/2} / q^3 , \; k < g . \quad (9)$$

Доказательство. Результат (9) следует из оценки поведения вероятности коллизии (8) при большом значении q. Раскрывая выражение (8) путем подстановки $s = \left\lfloor (2k+1/4)^{1/2} - 1/2 \right\rfloor$ получим (9). ◊

Следствие 2. Универсальное хеширование по кривой Гурвица $X^{q^2-1} Y^{q-1} + Y^{q^2-1} + X^{q-1} = 0$ при $k < g$ имеет оценки вероятности коллизии

$$\varepsilon \approx \left\lfloor (2k+1/4)^{1/2} - 1/2 \right\rfloor / (q^3 - q^2 + 2q - 4) , \quad (10)$$

$$\varepsilon_{q^3 \to \infty} = \sqrt{2} k^{1/2} / q^3 . \quad (11)$$

Доказательство. Результат (10) следует из выражения $\varepsilon = \rho_k / N$, где ρ_k - значение полюса рациональной функций $f_k = x^i \cdot y^j$, по теореме Безу $\rho_k = (i+j)(q^2+q-2)$, i, j определяются по

лемме 1, $N=\left(q^3-1\right)\left(q^2-1\right)$. Раскрывая выражение (10) путем подстановки $s=\left|(2k+1/4)^{1/2}-1/2\right|$ при большом значении q получим (11).

IV Выводы

1. Кривая Ферма $X^{q^2+q+1}+Y^{q^2+q+1}+Z^{q^2+q+1}$ имеет большой род $g=\left(q^2+q\right)\left(q^2+q-1\right)/2$ и оценка (8) для ε определена для широкого диапазона практических значений k. Для $k\geq g$ справедливо выражение $\varepsilon=(k+g)/N$ для вероятности коллизии. Оценки вероятности коллизии для кривой Гурвица являются подобными. Асимптотика вероятности коллизии универсального хеширования по кривой Ферма при малых значениях k определяется отношением корня квадратного длины данных к размерности поля, в $\sqrt{k}$ лучше, по сравнению с хешированием по проективной прямой $X+Y+Z=0$ и равняется асимптотике хеширования по кривой Эрмита в квадратичном поле той же размерности F_{p^2}, $p^2=q^3$.

2. Практический алгоритм вычисления хеш кода по рациональными функциями $x=X/Z$, $y=Y/Z$ кривой Ферма определяется схемой вычисления Горнера по двум переменным $h_{x,y}(m)=\sum_{j=0}^{s}y^j\cdot\sum_{i=0}^{s-j}m_{i,j}\cdot x^i$. Сложность универсального хеширования равна $N_{опер}=k+s$, $s=\left|(2k+1/4)^{1/2}-1/2\right|$, что соответствует сложности по кривой Эрмита в квадратичном поле [3].

3. Асимптотическая оценка сложности универсального хеширования по кривой $X^{q^2+q+1}+Y^{q^2+q+1}+Z^{q^2+q+1}$ определяется $N_{опер}(FC)=k+\sqrt{2}k^{1/2}$, так как $s=\left|(2k+1/4)^{1/2}-1/2\right|$. Хеширование по кривой Ферма по сравнению с хешированием по проективной прямой сложнее на $N_{опер}(FC)-N_{опер}(PC)=\sqrt{2}k^{1/2}$ операций. Относительное увеличение сложности вычислений является несущественным $N_{опер}(FC)/N_{опер}(PC)=1+\sqrt{2}k^{-1/2}$.

Література: ***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. Аутентификация с применением алгеброгеометрических кодов. / Халимов Г. З., Кузнецов А. А. //Радиотехника. Всеукр. межвед. науч.-техн. сб.- 2001.- Вып. 120.- С. 103-109.* ***3.*** *Халимов Г. З. Аутентификация с применением Эрмитовых кодов. /Халимов Г. З., Иохов А. Ю. // Вестник ХПИ. – Х., -2005. НТУ „ХПИ". –Вып. 9. –С. 26-32.* ***4.*** *Халимов Г. З. Универсальное хеширование по максимальным кривым Гурвица. / Халимов Г. З. // Журнал "Прикладная радиоэлектроника". Харьков: ХНУРЭ. 2010. - Том. 9 № 3, - С.365-370* ***5****. Pellikan R. The Klein quartic, the Fano plan and curves representing design / Pellikan R.// In Codes, Curves and Signals: Common Threads in Communications, (A. Vardy Ed.), Kluwer Acad. Publ., Dordrecht. -1998. - P.9-20,* ***6.*** *Beelen P. The Newton polygon of plane curves with many rational points./ Beelen P., Pellikan R. //, Designs, Codes and Cryptography.- 2000. -V.21.- P. 41–67.*

УДК 004.7

ВИРІШЕННЯ ПРОБЛЕМИ ДОСТУПНОСТІ ОДНОТИПНИХ ОБ'ЄКТІВ МЕРЕЖІ ЗА ДОМЕННИМ ІМ'ЯМ В ПРОТОКОЛІ ТРАНСЛЯЦІЇ МЕРЕЖЕВИХ АДРЕС

Юрій Яремчук, Дмитро Кец, Євгеній Ніколаєв, Дар'я Іванішина
Вінницький національний технічний університет

Анотація: **Проведено аналіз проблеми доступності однотипних локальних сервісів до глобальної мережі, зокрема, доступності однотипних об'єктів до мережі за доменним ім'ям. Для вирішення даної проблеми було запропоновано метод, який шляхом додавання нових і розширення існуючих таблиць протоколу NAT та інтеграції з ними модифікованих таблиць протоколу DNS, забезпечує доступність сервісів за глобальним доменним ім'ям. Запропонований метод дозволив значно**