УДК 681.3.07

МЕТОД УНІВЕРСАЛЬНОГО ГЕШУВАННЯ ПО РАЦІОНАЛЬНИМ ФУНКЦІЯМ АЛГЕБРАЇЧНИХ КРИВИХ НАД КІЛЬЦЯМИ

А.О. БОЙКО, Г.З. ХАЛІМОВ

Запропоновано метод універсального гешування по раціональним функціям алгебраїчних кривих над кільцями векторів, що на відміну від існуючих методів універсального гешування в полях забезпечує вищу швидкодію і не вразливий до атак спостереження за часом виконання.

Ключові слова: універсальна функція гешування, перетворення над кільцями.

ОГЛЯД СТАНУ

Універсальні геш-функції — це родина геш-функцій, що виконують наступне відображення: $KxM \to H$, де K – множина ключів, M – множина вхідних повідомлень, H – множина геш-значень, для якої виконується для будь-яких $x, y \in M$ наступне .

$$Pr_{h\in H}\{h(x)=h(y)\}=\frac{1}{|H|}. \qquad (1)$$

Алгоритм UMAC [1] є алгоритмом універсального гешування, що виконує гешування по проективним прямим.

UMAC в якості основного кроку використовує функцію поліноміального гешування PolyCW, яка обчислюється за формулою

$$h_x(m)=\sum_{i=0}^{k} m_i x^i \bmod p, \qquad (2)$$

де p – просте число і k – ціле число, $k>0$.

Поліноміальна родина геш-функций PolyCW є універсальною, і імовірність колізії [1]

$$Pr_{h\in H}\{h_x(a)=h_x(b)\bmod p\}=k/p. \qquad (3)$$

Це визначається основною теоремою алгебри, що стверджує, що у полінома степені k може бути не більше k коренів.

У роботах [2-4] було запропоновано методи універсального гешування по проективним кривим, визначеним над полями Галуа.

Недоліком методів гешування, що використовують обчислення над простим полем, є вразливість до атак спостереження за часом виконання. Зазвичай, вхідні блоки повідомлення представляються числами $0 \le m_i \le 2^n - 1$. Однак модуль перетворень P має вигляд $2^n - k$. При обчисленні геш-значення блок $m_i < k$ можна замінити на $m_i + P$ так, що геш-значення не зміниться. Для уникнення такої можливості блок повідомлення, такий що $m_i \ge P - 2$, заміняється парою $\{P-2, P-m_i\}$. Однак для обробки такої пари необхідно витратити в 2 рази більше часу, ніж для обробки "дозволеного" блоку, що і дає інформацію зловмиснику щодо вмісту блоків, які обробляються. Крім того, кожне таке розширення повідомлення приводить до зростання імовірності колізії у відповідності до формули (3).

Можливі шляхи вирішення проблеми:

1) використання проективних кривих, визначених над розширеним двійковим полем;

2) використання проективних кривих, визначених над кільцем, що містить 2^n елементів.

ВИКОРИСТАННЯ ПРОЕКТИВНИХ КРИВИХ, ВИЗНАЧЕНИХ НАД РОЗШИРЕНИМ ДВІЙКОВИМ ПОЛЕМ

Сучасні процесори загального призначення не мають інструкцій, орієнтованих на реалізацію операцій у $GF(2^n)$. Тому при реалізації операцій було використано методи оптимізації, запропоновані у роботі [5]. Однак ці методи вимагають чисельних вибірок з пам'яті по невирівненим адресам, що суттєво знижує швидкодію.

Внаслідок того, що набори інструкцій сучасних процесорів загального призначення не підтримують обчислення у розширеному двійковому полі, то швидкодія методів гешування, що використовують проективні криві, визначені над розширеним двійковим полем, значно гірша за методи, що використовують обчислення у простому полі або в кільці, незважаючи на оптимізації.

Використання проективних кривих, визначених над кільцем з 2^n елементів

Переваги використання кривих над кільцем для гешування:

– висока швидкодія, оскільки всі обчислення виконуються по модулю 2^n, тобто окремої операції приведення по модулю не потрібно, лише складання і множення, що потребує мінімум інструкцій процесора;

– невразливість до атак спостереження за часом виконання.

МЕТОД ПОБУДУВАННЯ УНІВЕРСАЛЬНИХ ГЕШ-ФУНКЦІЙ, ЩО ВИКОРИСТОВУЮТЬ ОБЧИСЛЕННЯ ПО ПРОЕКТИВНИХ КРИВИМ НАД КІЛЬЦЕМ ВЕКТОРІВ

Побудування і властивості кільця векторів

В ході досліджень проективних кривих над кільцем цілих чисел по модулю 2^n виявлено, що такі криві мають дуже мало точок і є ізоморфними проективним прямим, визначеним над тим же кільцем. Тобто, геш-функції, побудовані на основі таких кривих не мають переваг у імовірності колізії над геш-функціями, побудованими на основі обчислень над проективними прямими.

Вперше використання обчислень векторів для побудування груп для криптографічних застосувань (електронного цифрового підпису) було запропоновано у роботі [6]. У роботі [6] запропоновані наступні положення:

1) вектори виду $ae+bi+...+cj$, де $e,i,...j$ – базисні вектори, які також можуть бути представлені у вигляді набору координат $(a,b,...c)$, які є елементами скінченого поля $GF(p)$;

2) операція складання векторів визначається як складання одноіменних координат;

3) операція множення векторів визначається по правилу множення поліномів із урахуванням того, що множення базисних векторів виконується за правилами, заданими таблично;

4) результатом множення базисних векторів є базисний вектор або базисний вектор, помножений на коефіцієнт розтягнення, що обраний спеціальним чином з числа елементів поля $GF(p)$;

5) множина векторів виду $ae+bi+...+cj$ за умови того, що таблиця множення базових векторів має спеціальний вигляд, утворює поле.

Однак обчислення у полі векторів, визначених над простим полем, мають той же недолік, що і самі обчислення у простому полі — можливість атак спостереження за часом виконання. Тому запропоновано для побудування геш-функцій використовувати обчислення у кільці векторів, визначених над кільцем цілих чисел по модулю 2^n (далі позначається як $Z/Z2^n$).

У якості вектора приймається кортеж $\{a,b\}$ з двох елементів $a,b\in Z/Z2^n$. Також цей вектор може бути представлений у вигляді полінома $a+bi$, де $a,b\in Z/Z2^n$, а i — базисний вектор, для якого вірно $i^2=-1 \bmod 2^n$.

Додавання векторів визначено у відповідності до [6] як

$$\begin{gathered}(a+bi)+(c+di)= \\ \left((a+c)\bmod 2^n+\left((b+d)\bmod 2^n\right)i\right).\end{gathered} \quad (4)$$

Множення векторів визначено як

$$\begin{gathered}(a+bi)(c+di)= \\ \left((ac-bd)\bmod 2^n\right)+\left((ad+bc)\bmod 2^n\right)i.\end{gathered} \quad (5)$$

Операції додавання і множення векторів формально співпадають з відповідними операціями над комплексними числами з тією лише різницею, що у випадку векторів всі обчислення здійснюються по модулю 2^n (координати вектора належать $Z/Z2^n$).

Твердження. Множина векторів, що мають 2 координати з $Z/Z2^n$ і $i^2=-1\bmod 2^n$, над якою визначені операції додавання і множення векторів, є комутативним кільцем.

Доведення.

Комутативним кільцем називається множина R, над якою задані бінарні операції додавання "+" і множення "*" такі, що:

$r_1+(r_2+r_3)=(r_1+r_2)+r_3$ для всіх $r_1,r_2,r_3\in R$;

$r_1*(r_2*r_3)=(r_1*r_2)*r_3$ для всіх $r_1,r_2,r_3\in R$;

$r_1*r_2=r_2*r_1$ і $r_1+r_2=r_2+r_1$ для всіх; $r_1,r_2\in R$

існує такий елемент $O\in R$, що для усіх $r\in R$ виконується $r+O=O+r=r$;

існує такий елемент $e\in R$, що для усіх $r\in R$ виконується $r*e=e*r=r$;

для усіх $r\in R$ існує $r'\in R$ таке, що $r+r'=O$.

Асоціативність операції додавання доводиться як

$$\begin{gathered}\big((a+bi)+(c+di)\big)+(e+fi)= \\ \big(((a+c)+e)+((b+d)+f)i\big)= \\ \big((a+(c+e))+(b+(d+f))i\big)= \\ (a+bi)+\big((c+di)+(e+fi)\big)\end{gathered}.$$

Асоціативність операції множення доводиться як

$$\begin{gathered}\big((a+bi)*(c+di)\big)*(e+fi)= \\ \big((ac-bd)+(bc+ad)i\big)(e+fi)= \\ \big((ac-bd)e-(bc+ad)f\big)+ \\ +\big((ac-bd)f+(bc+ad)e\big)i= \\ (ace-bde-bcf-adf)+ \\ +(acf-bdf+bce+ade)i \\ (a+bi)*\big((c+di)*(e+fi)\big)= \\ (a+bi)*\big((ce-df)+(cf+de)i\big)= \\ \big(a(ce-df)-b(cf+de)\big)+ \\ +\big(b(ce-df)+a(cf+de)\big)i= \\ (ace-adf-bcf-bde)+ \\ +(bce-bdf+acf+ade)i\end{gathered}$$

Результат однаковий з точністю до порядка членів. Оскільки у $Z/Z2^n$ додавання комутативне, то можна прийняти, що результати однакові.

Комутативність додавання доводиться як

$$(a+bi)+(c+di)=(a+c)+(b+d)i.$$

Оскільки у $Z/Z2^n$ додавання комутативне, то

$$\begin{gathered}(a+c)+(b+d)i=(c+a)+(d+b)i= \\ (c+di)+(a+bi)\end{gathered}.$$

Комутативність множення доводиться як

$$(a+bi)(c+di)=(ac-bd)+(bc+ad)i,$$

$$(c+di)(a+bi)=(ca-db)+(cb+da)i.$$

Оскільки у $Z/Z2^n$ додавання комутативне, то $(ca-db)+(cb+da)i=(ac-bd)+(bc+ad)i$, звідки $(a+bi)(c+di)=(c+di)(a+bi)$.

Нульовим елементом у кільці векторів є {0, 0} (або $0+0i$ у поліноміальному представленні):

$$(a+bi)+(0+0i)=(0+0i)+(a+bi)=$$
$$(a+0)+(b+0)i=a+bi.$$

Одиничним елементом у кільці векторів є {1, 0} (або $1+0i$ у поліноміальному представленні):

$$(a+bi)(1+0i)=(1a-b0)+(1b+a0)i=$$
$$(a-0)+(b+0)i=a+bi.$$

Для вектора $a+bi$ аддитивно оберненим буде вектор $(2^n-a)+(2^n-b)i$, оскільки

$$(a+bi)+((2^n-a)+(2^n-b)i)=$$
$$=(a+2^n-a)+(b+2^n-b)i=2^n+2^n i=0+0i.$$

Твердження доведено.

Тут і далі, коли згадується кільце векторів, то мається на увазі саме кільце векторів, визначених над кільцем цілих чисел по модулю 2^n.

Твердження. Вектори, у яких одна з координат парна, а інша — непарна, утворюють циклічну мультиплікативну групу, у якій відсутні дільники нуля (оскільки сам нульовий вектор {0, 0} не належить до цієї групи).

Доведення. Як було раніше вказано, операції над векторами з 2-ма координатами з $Z/Z2^n$ і $i^2=-1 \bmod 2^n$ відповідають операціям над комплексними числами. Розглянемо матричне представлення комплексного числа. Комплексне число $a+bi$ може бути представлене у вигляді $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Детермінант такої матриці визначається як $\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix}=a^2+b^2$. Отже, якщо координата a або b непарна, а інша число координата парна, то детермінант такої матриці зажди непарний:

$$(2k_1+1)^2+(2k_2)^2=4k_1^2+4k_1+1+4k_2^2=$$
$$2(2k_1^2+2k_1+2k_2^2)+1.$$

Непарні числа по модулю 2^n утворюють циклічну мультиплікативну групу. Наприклад:

$$3^0 \bmod 16=1$$
$$3^1 \bmod 16=3$$
$$3^2 \bmod 16=9$$
$$3^3 \bmod 16=11$$
$$3^4 \bmod 16=1$$

Оскільки

$$\det\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)=\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix}*\det\begin{pmatrix} c & d \\ -d & c \end{pmatrix},$$

то обчислення детермінанту можна розглядати як гомоморфізм, що відображає мультиплікативну групу матриць виду $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ у мультиплікативну групу непарних чисел по модулю 2^n. З цього, а також з того, що мультиплікативна група непарних чисел по модулю 2^n є циклічною, слідує, що мультиплікативна група матриць виду $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ також є циклічною. Отже і вектори, у яких одна координата є парною, а інша — непарною, утворюють циклічну мультиплікативну групу. Твердження доведено.

Використання мультиплікативної групи, що має дільники нуля, може погіршити властивості геш-функцій, тому запропоновано використовувати в якості ключів саме вектори, у яких одна з координат парна, а інша — непарна.

Однак сумма двох векторів, що належать циклічній мультиплікативній групі, не належить цій групі, оскільки обидві її координати або парні, або непарні.

Однак можливо при перетворенні блоку повідомлення у вектор можливо робити це таким чином, щоб обидві координати вектора були або парними, або непарними. Тоді усі обчислення повертатимуть результат, що належатиме циклічній мультиплікативній групі.

Однак вектори, що належать групі, не можуть утворити точку на кривій Ферма виду $X^m+Y^m+1=0$, тому що сумма X^m+Y^m+1 належатиме циклічній мультиплікативній групі, тоді як $0+0i$ до неї не належатиме.

Тому запропоновано використовувати криву виду $X^m+Y^m+2=0$, або в узагальненому вигляді $X^m+Y^m+\{2s,2t\}=0$.

ВЛАСТИВОСТІ ГЕШ-ФУНКЦІЙ, ЩО ВИКОРИСТОВУЮТЬ ОБЧИСЛЕННЯ ПО ПРОЕКТИВНИМ КРИВИМ НАД КІЛЬЦЕМ ВЕКТОРІВ

У зв'язку з тим, що теорія проективних кривих над кільцями ще не розроблена, усі дослідження проводилися шляхом виконання обчислювальних експериментів з кривими над невеликими кільцями.

Розглядалась можливість використання кривих Ферма виду $X^m+Y^m+const=0$ над кільцем векторів виду $x+yi$, де $0\le x,y<2^n$, а $i^2=-1 \bmod 2^n$.

Під час досліджень актуальними питаннями були:

1) яку кількість точок має крива Ферма над кільцем векторів і як ця кількість змінюється в залежності від розміру кільця;

2) які колізійні властивості мають геш-функції, побудовані на кривих Ферма над кільцем векторів.

При дослідженні кривих Ферма над кільцем векторів з обмеженням, заданим у твердженні (1), найкращі результати показали криві виду $X^m+Y^m+\{2^{n-1},2^{n-1}\}=0$, де $m=4k+2$ з цілим $k>0$, 2^n — модуль перетворень у кільці, якому належать координати вектора. У всіх проведених

експериментах такі криві завжди мали 2^{n+2} точок. Дослідження виконувалося шляхом побудування всіх можливих точок на кривій перебором.

Дослідження колізійних властивостей геш-функції проводилось наступним чином:

1) було побудовано матрицю значень усіх раціональних функцій степені не вище k від координат точок кривої x і y, розмір матриці $k(k+1)/2-1\,x\,N$, де k — максимальна степінь раціональної функції, а N — кількість точок на кривій;

2) випадковим чином було згенеровано $k(k+1)/2-1$ блоків повідомлення від a_1 до $a_{k(k+1)/2-1}$;

3) за формулою (6) було обчислено N значень від s_1 до s_N, що за фізичним змістом представлять собою множину усіх значень геш-функції при фіксованому повідомленні $\{a_1 \| ... \| a_{k(k+1)/2-1}\}$ і всіх можливих значеннях ключів від (x_1, y_1) до (x_N, y_N);

$$\begin{pmatrix} x_1 & y_1 & x_1^2 & x_1y_1 & y_1^2 & \dots & x_1^k y_1^k \\ x_2 & y_2 & x_2^2 & x_2y_2 & y_2^2 & \dots & x_2^k y_2^k \\ x_3 & y_3 & x_3^2 & x_3y_3 & y_3^2 & \dots & x_3^k y_3^k \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ x_N & y_N & x_N^2 & x_Ny_N & y_N^2 & \dots & x_N^k y_N^k \end{pmatrix} * \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_{k(k+1)/2-1} \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ \dots \\ s_N \end{pmatrix}; \quad (6)$$

4) у множині значень від s_1 до s_N було знайдено значення, що зустрічається найчастіше і підраховано кількість появ цього значення;

5) отримане на попередньому кроці число було занесене до відповідного списку;

6) кроки 2-5 було повторено 10^6 разів;

7) значення k змінювалося від 2 до 6, N приймало значення $2^8, 2^{10}, 2^{12}, 2^{14}, 2^{16}$.

Отримані результати внесені у табл. 1.

Таблиця 1

n	Макс степінь раціональної функції, k	Модуль 2^n	Розмір кільця векторів	$N_т$ кількість точок на кривій 2^{2n+2}	$N_{макс}$ максимальна кількість однакових значень	Імовірність коллізії $N_{макс}/N_т$	Примітка
3	2	8	32	$256=2^8$	64	0,25	1/4
3	3	8	32	$256=2^8$	64	0,25	1/4
3	4	8	32	$256=2^8$	64	0,25	1/4
3	5	8	32	$256=2^8$	32	0,125	1/8
3	6	8	32	$256=2^8$	192	0,75	3/4
4	2	16	128	$1024=2^{10}$	96	0,09375	3/32
4	3	16	128	$1024=2^{10}$	96	0,09375	3/32
4	4	16	128	$1024=2^{10}$	96	0,09375	3/32
4	5	16	128	$1024=2^{10}$	64	0,0625	1/16
4	6	16	128	$1024=2^{10}$	768	0,75	3/4
5	2	32	512	$4096=2^{12}$	160	0,03906	
5	3	32	512	$4096=2^{12}$	160	0,03906	
5	4	32	512	$4096=2^{12}$	160	0,03906	
5	5	32	512	$4096=2^{12}$	128	0,03125	1/32
5	6	32	512	$4096=2^{12}$	1568	0,38281	
6	2	64	2048	$16384=2^{14}$	288	0,01758	
6	3	64	2048	$16384=2^{14}$	288	0,01758	
6	4	64	2048	$16384=2^{14}$	288	0,01758	
6	5	64	2048	$16384=2^{14}$	256	0,01562	1/64
6	6	64	2048	$16384=2^{14}$	4224	0,25781	
7	2	128	8192	$65536=2^{16}$	544	0,00830	
7	3	128	8192	$65536=2^{16}$	544	0,00830	
7	4	128	8192	$65536=2^{16}$	544	0,00830	
7	5	128	8192	$65536=2^{16}$	512	0,00781	1/128
7	6	128	8192	$65536=2^{16}$	8352	0,12744	

З табл. 1 видно, що найкращі результати з імовірності колізії досягаються, коли максимальна степінь раціональних функцій дорівнює 5 (повідомлення з 14 блоків) і досягає $\frac{1}{2^n}$, де 2^n – модуль перетворень (розмір кільця, над яким визначено кільце векторів), і одразу різко погіршуються, коли максимальна степінь раціональних функцій досягає 6. Таким чином на повідомленні з 14 блоків геш-функція веде себе як універсальна геш-функція. Із збільшенням розміру кільця векторів колізійна стійкість геш-функцій зростає.

Практичні результати вимірювання швидкодії різних методів універсального гешування наведені у табл. 2. Висока швидкодія методу гешування по проективним кривим над кільцями пояснюється тим, що алгоритми складання і множення векторів є простими і повністю використовують можливості по одночасному виконанню кількох команд у сучасних суперскалярних процесорах.

З таблиці видно, що програш у швидкодії при використанні операцій у $GF\left(2^n\right)$ складає 5-10 раз, що у більшості застосувань є неприпустимим.

В той же час швидкодія алгоритму гешування над кільцями в майже в 4 рази більша ніж гешування по кривим Ферма над квадратичним полем.

Нерозв'язані питання для наступних досліджень:

1) побудова теорії проективних кривих над кільцями, що дозволила б обчислювати число точок на кривій і шукати криві з більшим числом точок, а також уникнути погіршення колізійних властивостей при збільшенні довжини повідомлення;

2) побудова методу оцінки колізійної стійкості геш-функцій, що використовують криві Ферма над кільцями;

3) розробка алгоритму генерації ключів для таких геш-функцій.

ВИСНОВКИ

1. Основним недоліком алгоритмів гешування, що використовують перетворення у простому полі по модулю $2^n - k$ є вразливість до атаки спостереження за часом виконання.

2. Алгоритми гешування, що використовують перетворення у розширеному двійковому полі, не вразливі до атаки спостереження за часом виконання, однак мають значно нижчу швидкодію.

3. Для того, щоб уникнути вразливості до атаки спостереження за часом виконання і зберегти високу швидкодію вперше запропоновано метод універсального гешування, по раціональним функціями проективних кривих над кільцями векторів, які в свою чергу також визначені над кільцями цілих чисел по модулю 2^n.

4. Для практичної перевірки було розглянуто метод гешування по кривим Ферма над кільцями векторів. Найкращі результати з імовірності колізії досягаються, коли максимальна степінь раціональних функцій дорівнює 5 (повідомлення з $5*(5+1)/2-1=14$, блоків), таким чином на повідомленні з 14 блоків геш-функція веде себе як універсальна геш-функція.

Таблиця 2

Метод гешування	Швидкодія (тактів на байт)	Розмір поля (кільця)	Довжина ключа (біт)	Довжина геш-значення	Імовірність колізії
Гешування по проективній прямій $GF(q)$ $q=2^{64}-59$	8,7	$2^{64}-59$	64	64	$\approx 2^{64}$
Гешування по проективній прямій $GF(q)$ $q=2^{32}-5$ $f(t)=t^2-2$	4,8	$(2^{32}-5)^2$	64	64	$\approx 2^{64}$
Гешування по кривій Ферма $GF(q)$ $q=2^{32}-5$	3,7	$2^{32}-5$	64	32	$\approx 2^{64}$
Гешування по проективній прямій $GF\left(\left(\left(2^8\right)^4\right)^2\right)$	41	2^{64}	64	64	$\approx 2^{64}$
Гешування по кривій Ерміта $GF\left(\left(2^8\right)^4\right)$	18	2^{32}	64	32	$\approx 2^{64}$
Гешування по кривим Ферма над кільцем векторів	1,0	2^{128}	256	128	$\approx 2^{64}$

5. Завдяки простим алгоритмам додавання і множення векторів і можливості використання паралельних обчислень всередині цих алгоритмів геш-функції по проективним кривим над кільцями векторів мають дуже високу швидкодію.

6. Нерозв'язаними питаннями залишаються побудова теорії проективних кривих над кільцями і побудова алгоритму генерування ключів для такої геш-функції.

Література

[1] *J. Black, S. Halevi, H. Krawczyk, T. Krovetz, P. Rogaway.* UMAC: Fast and Secure Message Authentication [Електронний ресурс] http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=B1DBCEDF9D4955AF4E565C921F9B38C8?doi=10.1.1.114.7878&rep=rep1&type=pdf.

2] *Халимов Г.З., Котух Е.В.* Универсальное хеширование по кривой Сузуки. Прикладная радиоэлектроника, Том 10, 2011, №2, с.164 – 170.

3] *Халимов Г.З.* Каскадное универсальное хеширование по рациональным функциям алгебраических кривых. Радиотехника, 2011, вып. 166 с. 26-31.

4] *Халимов Г.З.* Универсальное хеширование по максимальным кривым 2-го рода. Тезисы докладов международной конференции "Современные проблемы математики и ее приложения в естественных науках и информационных технологиях", Харьков 2011, с. 191-193.

5] *K Greenan, E. Miller, T. Schwarz.* Optimizing Galois Field Arithmetic for Diverse Processor Architectures and Applications [Електронний ресурс] http://dicc.ucu.edu.uy/publicaciones/mascots08GF.pdf.

6] *Молдовян Н.А.* Группы векторов для алгоритмов электронной цифровой подписи Вестник Санкт-Петербургского университета, серия 10 вып. 1, 2009, с. 96-102.

Надійшла до редколегії 3.04.2012

Бойко Артем Олександрович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: функції гешування, побудування високошвидкісних систем захисту інформації.

Халімов Геннадій Зайдулович, кандидат технічних наук, доцент кафедри БІТ ХНУРЕ. Область наукових інтересів: методи та засоби автентифікації даних.

УДК 004.056

Метод универсального хеширования по рациональным функциям алгебраических кривых над кольцами / А.А. Бойко, Г.З. Халимов // Прикладная радиоэлектроника: науч.-техн. журнал. – Том 11. № 2. – С. 165–170.

Рассмотрены известные методы универсального хеширования. Описаны их недостатки, в частности наличие уязвимости к наблюдению за временем исполнения. Для решения данной проблемы предложено заменить вычисления в полях на вычисления в кольцах. Предложен метод универсального хеширования по рациональным функциям алгебраических кривых над кольцами векторов, который в отличие от существующих методов универсального хеширования в полях обеспечивает более высокое быстродействие и не является уязвимым к наблюдению времени исполнения.

Ключевые слова: универсальная функция хеширования, переобразования с кольцами.

Табл. 2. Библиогр.: 6 назв.

UDC 004.056

Technique of universal hashing by rational functions of algebraic curves over rings / A.A. Boiko, G.Z. Halimov // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 165–170.

The paper considers the known techniques of universal hashing and describes their shortcomings, in particular, vulnerabilities to observation of implementation time. It is suggested that calculations over fields be replaced with calculations over rings to solve the problem. A technique of universal hashing by rational functions of algebraic curves over vector rings is suggested which unlike the existing ones over fields is faster and invulnerable to the observation of implementation time.

Keywords: universal hashing, transformations over rings.

Tab. 2. Ref.: 6 items.