УДК 681.3.06

Є. В. Котух, молодший науковий співробітник
Харківський національний університет радіоелектроніки, м. Харків

АСИМПТОТИЧНІ ОЦІНКИ УНІВЕРСАЛЬНОГО ХЕШУВАННЯ ЗА АЛГЕБРИЧНИМИ КРИВИМИ

У роботі представлені результати універсального хешування за кривими, які асоційовані з кривими Делігне-Лустіга над розширеннями кінцевого поля. Отримано порівняльні асимптотичні оцінки ймовірності колізії універсального хешування. З оцінки випливає, що найкращий результат досягається на кривій Рі над полем характеристики 3 з параметрами $q = 3q_0^2$ і $q_0 = 3^m$.

Ключові слова: *універсальне хешування, група Судзукі, криві Судзукі, криві Рі, криві Ерміта.*

Вступ. Універсальне хешування за раціональними функціями алгебричних кривих на основі скалярного множення за раціональними функціями лінійного базисного простору ґрунтується на фундаментальній теоремі Рімана-Роха, яка визначає параметри лінійного базисного простору функціонального поля алгебричних кривих. Ймовірність колізії універсального хешування визначається найбільшим значенням полюса в підгрупі Вейєрштрасса для раціональних функцій лінійного базисного простору, що дозволяє отримати колізійні оцінки. Проблематика побудови універсального хешуванняя за раціональними функціями алгебричних кривих полягає у виборі алгебричних кривих з необхідними параметрами. Важливою науковою задачею є оцінка ймовірності колізії універсального хешування за раціональними функціями максимальних алгебричних кривих, що лежать на кордоні Хассе-Вейля або кривих, які близькі кордону Дрінфельда-Владуца.

У роботі отримані асимптотичні оцінки для ймовірності колізії універсального хешування за кривими, що відносяться до кривих Делігне-Лустіга.

Визначення універсального хешування за раціональними функціями алгебричних кривих. Нехай χ — абсолютно нерозкладна, несингулярна проективна крива над полем F_q, $P_1, P_2, ..., P_n$ — точки кривої χ, P_∞ — точка на нескінченності або особлива точка кривої χ, $f_i \in F_q(\chi) \setminus \{0\}$ — раціональні функції функціонального поля кривої χ, $div_\infty(f_i) = \rho_i$ — значення дивізора або порядок полюса раціональної функції f_i у точці P_∞, $f_i(P_j)$ — значення раціональної функції у точці P_j.

Хеш-функція $h_{P_j}(m) \in F_q$ для повідомлення $m = (m_1, ..., m_k)$, $m_i \in F_q$ у точці P_j визначається виразом

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

де $f_i \in F_q(\chi)$ із впорядкованими порядками полюсів $0 < \rho_1 < \rho_2 < ... < \rho_k$ [1].

Хеш-функція $h_{P_j}(m)$ визначає універсальний хеш-клас $\varepsilon - U(N, q^k, q)$, де N — кількість точок алгебричної кривої, q^k — обсяг простору повідомлень, q — обсяг простору хеш-кодів та ймовірність колізії визначається виразом

$$\varepsilon = \rho_k / N , \qquad (1)$$

де ρ_k — значення полюса раціональної функції f_k.

Оцінки асимптотичних границь ймовірності колізії. Криві Делігне-Лустіга асоціюються з проективною спеціальною лінійною групою (криві Ерміта), з групою Сузукі (Suzuki) $Sz(q)$ (криві Сузукі) та Рі (Ree) групою $R(q)$ [2].

Крива Ерміта над квадратичним полем F_q визначається рівнянням

$$y^{\sqrt{q}} + y = x^{\sqrt{q}+1}$$

і є кривою Делігне-Лустіга першого типу. Крива Ерміта є максимальною кривою найбільшого роду $g = \sqrt{q}(\sqrt{q} - 1)/2$ серед максимальних кривих над F_q, має підгрупу Вейєрштрасса $H(P) = \left\langle \sqrt{q}, \sqrt{q} + 1 \right\rangle$ і визначається лінійною серією розмірності $\dim = 2$.

Хешування за раціональними функціями кривої Ерміта над полем F_q визначає універсальний хеш-клас $\varepsilon - U(q\sqrt{q}, q^k, q)$, де $q\sqrt{q}$ — кількість хеш-функцій (обсяг ключового простору), q^k — обсяг простору повідомлень, q — обсяг простору хеш-кодів. Ймовірність колізії ε визначається співвідношеннями

$$\varepsilon = k / q\sqrt{q} + s / \sqrt{q} - s(s-1) / (2q\sqrt{q}) , \text{ якщо } k < \sqrt{q}(\sqrt{q} - 1)/2 , \quad (2)$$

$$\varepsilon = k / q\sqrt{q} + 1 / (2\sqrt{q}) - 1 / (2q) , \text{ якщо } k \geq \sqrt{q}(\sqrt{q} - 1)/2 , \quad (3)$$

де $s = \left\lceil (2k + 1/4)^{1/2} - 1/2 \right\rceil$ є округленням значення до найбільшого цілого.

Розкриваючи вираз (2) шляхом підстановки s, отримаємо асимптотику ймовірності колізії універсального хешування за кривими Ерміта при великих значеннях розмірності поля $q \to \infty$

$$\varepsilon_{q\to\infty} = k / q\sqrt{q} + \sqrt{2}k^{1/2} / q \approx \sqrt{2}k^{1/2} / q$$

Нехай $k \approx \sqrt{q}(\sqrt{q}-1)/2$, маємо $\varepsilon_{q\to\infty} \approx 1/\sqrt{q}$.

Криві Сузукі S є F_q ізоморфними плоскій кривій

$$y^q - y = x^{q_0}(x^q - x),$$

де $q = 2q_0^2$ і $q_0 = 2^s$ — крива Делігне-Лустіга другого типу. Рід кривої $g = q_0(q-1)$ і кількість F_q раціональних точок дорівнює q^2+1.

Крива Делігне-Лустіга, асоційована з групою Сузукі, визначається повною лінійною серією $D = \left|\left(q+2q_0+1\right)P_0\right|$ розмірності $\dim = 4$ і ступеню $q+2q_0+1$, яка виводиться з енумератора Зета-функції [3]. Відображення кривої Сузукі на проективний простір P^4 і підгрупа Вейєрштрасса $H(P)$, $P \in X\left(F_q\right)$ розглянуті у роботах [4].

F_q раціональний морфізм кривої Сузукі в P^4 є відображенням

$$\pi := (1 : x : y : v : w),$$

де x, y, v, w визначаються рівняннями: $y^q - y = x^{q_0}(x^q - x)$, $v := x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$ і порядки полюсів дорівнюють $div_\infty(x) = qP_0$, $div_\infty(y) = \left(q+q_0\right)P_0$, $div_\infty(v) = \left(q+2q_0\right)P_0$, $div_\infty(w) = \left(q+2q_0+1\right)P_0$.

Крива Сузукі може бути представлена в P^4 множиною точок вигляду

$$P_{(a,b)} := (1 : a : b : f\left(a,b\right) : af\left(a,b\right)+b^2) \cup \pi(P_0) = \left(0:0:0:0:1\right),$$

де $a,b \in F_q$ і $f\left(a,b\right) := a^{2q_0+1} + b^{2q_0}$.

Підгрупа Вейєрштрасса $H(P)$, $P \in C\left(F_q\right)$ функціонального поля кривої містить підгрупу

$$H(P) = \left\langle q, q+q_0, q+2q_0, q+2q_0+1 \right\rangle.$$

Хешування за раціональними функціями кривої Сузукі визначає універсальний хеш-клас $\varepsilon - U(q^2, q^k, q)$, де q^2 — кількість хеш-функцій (обсяг ключового простору), q^k — обсяг простору повідом-

лень, q — обсяг простору хеш-кодів. Ймовірність колізії ε визначається співвідношеннями

$$\varepsilon = (i(q+2q_0)+j(q+2q_0+1)+t(q+q_0)+rq)/q^2, \text{ якщо } k < q_0(q-1),$$

$$\varepsilon = (k+q_0(q-1))/q^2, \text{ якщо } k \geq q_0(q-1),$$

де $0 \leq i \leq q_0-1, 0 \leq j \leq q_0-1, 0 \leq t \leq 1, 0 \leq r \leq q-1$.

Нехай $k \approx \sqrt{q}(\sqrt{q}-1)/2$, маємо значення параметрів $i \approx s$, $j=0$, $t=0$, $r=0$, $s \approx \left[(3k)^{1/3}\right] \approx (q)^{1/3}$ та оцінку ймовірності колізії

$$\varepsilon \approx q^{1/3}(q+q_0)/q^2 \approx q^{-1/6}\varepsilon_{EK},$$

де $\varepsilon_{EK} = 1/\sqrt{q}+1/q$ — значення ймовірності колізії універсального хешування за кривою Ерміта у квадратичному полі F_q при $k = \sqrt{q}(\sqrt{q}-1)/2$. Із оцінки $\varepsilon \approx q^{-1/6}\varepsilon_{EK}$ слідує виграш у $q^{1/6}$ разів за ймовірністю колізії відносно хешування за кривою Ерміта. Розмір ключових даних порівняно з хешуванням за кривою Ерміта більше у $\sqrt{q}$ разів.

Для $k = q_0(q-1)$ маємо ймовірність колізії хешування за кривими Сузукі

$$\varepsilon = 2q_0(q-1)/q^2 \approx \sqrt{2}q^{-1/2}.$$

Підстановка $k = q_0(q-1)$ у вираз для ймовірності колізії хешування за кривими Ерміта дає

$$\varepsilon = k/q^3 + 1/(2q) - 1/(2q^2) \approx 1/\sqrt{2}.$$

Криві Рі визначені над полем F_q, характеристики $p=3$, $q_0 = 3^m$, $q = 3q_0^2$ мають q^3+1 точок $F_R := F_q(x, y_1, y_2)$, які пов'язані рівняннями

$$y_1^q - y_1 = x^{q_0}\left(x^q - x\right);$$

$$y_2^q - y_2 = x^{q_0}\left(y_1^q - y_1\right).$$

Рід кривої $g = 3q_0(q-1)(q+q_0+1)$, кількість F_q раціональних точок дорівнює q^3+1 [5]. Криві Рі є оптимальними в тому сенсі, що мають кількість F_q раціональних точок відносно роду достатньо близьким до кордону Хассе-Вейля. Існує морфізм

$$\pi = \left(1 : x : y_1 : y_2 : w_1 : w_2 : w_3 : w_4 : w_5 : w_6 : w_7 : w_8 : w_9 : w_{10}\right),$$

асоційований з лінійною серією $D = \left| mP_\infty \right|$, який визначає відображення кривої Рі на проективний простір P^{13}. Рівняння, що визначають координати w_i, мають вигляд:

$$w_1 := z^{3q_0+1} - y_1^{2q_0},\ w_2 := zy_1^{3q_0} - y_2^{3q_0},\ w_3 := zy_2^{3q_0} - w_1^{3q_0},$$

$$w_4 := zw_2^{q_0} - y_1 w_2^{q_0},\ v := xw_3^{q_0} - y_2 w_1^{q_0},\ w_5 := y_1 w3_{q_0} - y_2 w_1^{q_0},$$

$$w_6 := v^{3q_0} - w_2^{3q_0} + xw_4^{3q_0},\ w_7 := y_1 w_3^{q_0} - xw_3^{q_0} - w_6^{q_0} = w_2 + v,$$

$$w_8 := w_6^{3q_0} + xw_7^{3q_0},\ w_9 := w_4 w_2^{q_0} - y_1 w_6^{q_0},\ w_{10} := y_2 w_6^{q_0} - w_3^{q_0} w_4.$$

Підгрупа Вейєрштрасса $H(P)$, $P \in C(F_q)$ функціонального поля кривої містить підгрупу

$$H(P) = \left\langle \begin{array}{l} q^2, q^2 + q_0 q, q^2 + 2q_0 q, q^2 + 3q_0 q, q^2 + 3q_0 q + q, q^2 + 3q_0 q + 2q, \\ q^2 + 2q_0 q + q, q^2 + 3q_0 q + q + q_0, q^2 + 3q_0 q + q, \\ q^2 + 2q_0 q + q + q_0, q^2 + 3q_0 q + 2q + 3q_0 + 1, q^2 + 3q_0 q + 2q + q_0, \\ q^2 + 3q_0 q + 2q + 2q_0, q^2 + 3q_0 q + 2q + 3q_0, \end{array} \right\rangle.$$

Хешування за раціональними функціями кривої Рі визначає універсальний хеш-клас $\varepsilon - U(q^3, q^k, q)$, де q^3 — кількість хеш-функцій (обсяг ключового простору), q^k — обсяг простору повідомлень, q — обсяг простору хеш-кодів. Ймовірність колізії ε визначається співвідношенням

$\varepsilon = (k + 3q_0(q-1)(q+q_0+1))/q^3$, якщо $k \geq 3q_0(q-1)(q+q_0+1)$.

Для $k = 3q_0(q-1)(q+q_0+1)$ маємо ймовірність колізії хешування за кривими Рі $\varepsilon = 6q_0(q-1)(q+q_0+1)/q\sqrt{3} \approx 2\sqrt{3}q^{-1/2}$.

Висновки. Абсолютно найкращий результат універсального хешування за оцінками ймовірності колізії досягається за кривими Рі. Тому, що рід кривої Рі є найбільшим, це призводить до затягнення характеристики ймовірності колізії порівняно з іншими кривими на більші обсяги даних, що хешуються. Практична побудова алгоритму хешування за кривими Рі потребує розв'язку в силу великої розмірності базису функціонального поля, асоційованого з кривою.

Список використаних джерел:

1. Халимов Г. З. Универсальное хеширование по максимальным кривым. XIII Международная научно-практическая конференция «*Безопасность информации в информационно-телекомуникационных системах*», Киев, 18–21 мая 2010г. тезисы докладов. С. 53.
2. Hansen J. P. Deligne-Lusztig varieties and group codes. *Lecture Notes of Mathematics.* 1992. Vol. 1518. P. 63–81.

3. Hansen J. P., Stichtenoth H. Group codes on certain algebraic curves with many rational points. AAECC. 1990. N 1. P. 67–77.
4. Халимов Г. З., Котух Е. В. Универсальное хеширование по кривым Сузуки. Журнал *«Прикладная радиоэлектроника»*. Харьков: ХНУРЭ. 2011. Том. 10. № 2. С. 164–170.
5. Pedersen J. P. A function field related to the Ree group. Lecture Notes Mathematics. 1992. Vol. 1518. P. 122–131.

This paper presents the results of universal hashing for curves that are associated with curves Delihne Lustig on extensions of the finite field. An asymptotic comparative estimates of the collision probability of universal hashing are obtained. Evaluation shows that the best result is achieved on the Ri curve over a field of characteristic 3 with parameters $q = 3q_0^2$ and $q_0 = 3^m$.

Key words: *universal hashing, group Suzuki, Suzuki curves, Ri curves, Hermite curves.*

Одержано 15.02.2017

УДК 681.32

Б. Б. Круліковський*, канд. техн. наук, доцент,
Н. Я. Возна,** канд. техн. наук, доцент,
В. М. Грига*,** канд. техн. наук,
А. Я. Давлетова,** аспірантка

*Національний університет водного господарства
та природокористування, м. Рівне,
**Тернопільський національний економічний університет, м. Тернопіль,
***Прикарпатський національний університет
імені Василя Стефаника, м. Івано-Франківськ

ОПТИМІЗАЦІЯ СТРУКТУРНИХ РІШЕНЬ КОМБІНАЦІЙНИХ СУМАТОРІВ ЗГІДНО КРИТЕРІЇВ МІНІМАЛЬНОЇ ЧАСОВОЇ, АПАРАТНОЇ ТА СТРУКТУРНОЇ СКЛАДНОСТІ

Запропонована структура суматора з прискореним переносом для виконання операції додавання двійкових чисел у базисі Радемахера. Виконано мікроелектронну реалізацію запропонованого суматора з прискореним переносом на ПЛІС. В результаті синтезу на ПЛІС відомого та запропонованого суматорів з прискореним переносом отримано характеристики складності, які співпадають з теоретичними розрахунками.

Ключові слова: *суматор з прискореним переносом, базис Радемахера, ПЛІС, САПР, інкрементний суматор.*

Вступ. Традиційно, при розробці компонентів процесорів обчислювальної техніки критерієм оптимальності вважалися мінімальна апаратна та часова складність [1]. Для успішного розвитку цього на-

