УДК 004.056.55

Семикрас А.О.
Кирилащук Т.Г.

ДВОРІВНЕВА ГЕШ-ФУНКЦІЯ З ЄДИНИМ КЛЮЧЕМ НА ОСНОВІ BRW-ПОЛІНОМІВ

Вінницький національний технічний університет

Анотація

У тезах розглядається конструкція дворівневої геш-функції Hash2L, яка поєднує поліноми Бернштейна–Рабіна–Віноґрада (BRW) на нижньому рівні та правило Горнера на верхньому. Досліджується можливість усунення практичних труднощів реалізації BRW для повідомлень змінної довжини шляхом фіксації розміру суперблоку. Показано, що конструкцію можна будувати з єдиним елементом скінченного поля як ключем, зберігаючи при цьому доведену майже-XOR-універсальність геш-сімейства. Реалізація над двійковим полем $F_{2^{128}}$ з використанням апаратної інструкції pclmulqdq продемонструвала перевищення швидкодії GHASH та POLYVAL на 23–53% на процесорах Intel Haswell та Skylake.

Ключові слова: геш-функція, BRW-поліноми, правило Горнера, дворівневе гешування, код автентифікації повідомлень, бінарне поле, pclmulqdq.

Abstract

The theses consider the construction of a two-level hash function Hash2L that combines Bernstein–Rabin–Winograd (BRW) polynomials at the lower level with Horner's rule at the upper level. The study examines how fixing the super-block size eliminates the practical difficulties of implementing BRW for variable-length messages. It is shown that the construction can be built using a single finite field element as the hash key while preserving the provably almost-XOR-universal property of the hash family. An implementation over the binary field $F_{2^{128}}$ using the pclmulqdq hardware instruction demonstrated 23–53% speed improvements over GHASH and POLYVAL on Intel Haswell and Skylake processors.

Keywords: hash function, BRW polynomials, Horner's rule, two-level hashing, message authentication code, binary field, pclmulqdq.

Вступ

Геш-функції з доведено низькою імовірністю колізій є фундаментальним примітивом у сучасній криптографії. Вони застосовуються для побудови схем автентифікації повідомлень (MAC), автентифікованого шифрування та захисту дискової пам'яті. Серед підходів до побудови таких функцій виділяють два основні класи: гешування на основі правила Горнера (Horner), яке реалізоване зокрема у GHASH, POLYVAL та Poly1305, та гешування на основі поліномів BRW. Правило Горнера потребує $\ell-1$ множень у скінченному полі для повідомлення з ℓ блоків, тоді як BRW-поліноми вимагають лише $\frac{\ell}{2}$ множень і $lg\ \ell$ піднесень до квадрату — значно менше. Однак рекурсивна природа BRW ускладнює реалізацію для повідомлень змінної довжини: увесь текст потрібно буферизувати до початку обчислень, а визначення операндів множень потребує значних додаткових зусиль [1]. Саме ця суперечність між теоретичною перевагою BRW та труднощами практичного застосування визначає актуальність дослідженої конструкції.

Результати дослідження

Основна ідея конструкції Hash2L полягає у розподілі вхідного повідомлення на суперблоки фіксованого розміру η блоків. BRW-поліном застосовується до кожного суперблоку незалежно, а отримані значення об'єднуються за правилом Горнера. Оскільки розмір суперблоку фіксовано, реалізація BRW виконується без рекурсії і без попередньої буферизації повідомлення, що усуває головну практичну перешкоду [1].

Суттєвою властивістю конструкції є єдиний ключ: якщо ключем рівня BRW є τ, а d(η) — степінь BRW-полінома суперблоку, то ключем для рівня Горнера обирається $\tau^{d(\eta)}+1$). Такий вибір гарантує, що коефіцієнти поліномів різних суперблоків асоційовані з різними степенями τ, — ін'єктивність

конструкції та доведена майже-XOR-універсальність (AXU) геш-сімейства слідують безпосередньо з ін'єктивності BRW [1]. Для $\eta = 2^{(r+1)} - 1$ потрібно всього r+1 піднесень до квадрату для обчислення всіх необхідних степенів τ.

При η = 31 загальна кількість множень становить приблизно $16\ell - 1$ для ℓ суперблоків, що відповідає ≈ 52% від кількості множень при суто горнерівському підході. Кількість множень BRW-підходу складає ≈ 97–100% від кількості множень Hash2L, тобто дворівнева конструкція майже не поступається «чистому» BRW за обчислювальною складністю [1].

Для практичної реалізації над $F_{2^{128}}$ та $F_{2^{256}}$ використано апаратну інструкцію pclmulqdq процесорів Intel. Застосовано техніку відкладеного зведення (delayed reduction): кілька послідовних множень виконуються без проміжних зведень, після чого одне зведення виконується для їх суми. Також реалізовано пакетне множення (batch multiplication) з розміром пакету 3 та 3-decimated Horner для ефективного паралелізму на рівні інструкцій [1].

Вимірювання швидкодії проводились на процесорах Intel Core i7-4790 Haswell (3,60 ГГц) та Intel Core i7-6500U Skylake (2,5 ГГц) під керуванням Ubuntu 14.04 LTS з компілятором GCC 4.8.4. На Haswell реалізація Hash2L над $F_{2^{128}}$ для повідомлень 512–8192 байт є швидшою за GHASH на 23,5–49,1% та за POLYVAL на 15,2–19,3%. На Skylake ці показники становлять відповідно 25,1–53,7% та 10,6–15,6% [1]. Для $F_{2^{256}}$ без інструкції pclmulqdq показано, що при використанні FFT-алгоритму множення вартість обчислення Hash2L складає не більше 46,4 бітових операцій на біт дайджесту без прихованих витрат на генерацію ключа. Це вигідно відрізняє Hash2L від конструкції Auth256, де ключ такий самий довгий, як і повідомлення [1].

Висновки

У роботі розглянуто дворівневу геш-функцію Hash2L, яка поєднує BRW-поліноми на нижньому рівні з правилом Горнера на верхньому при збереженні єдиного ключа скінченного поля. Фіксація розміру суперблоку дозволяє використовувати ефективну нерекурсивну реалізацію BRW, усуваючи головні практичні труднощі. Доведено властивості ін'єктивності та майже-XOR-універсальності конструкції. Практична реалізація над $F_{2^{128}}$ демонструє суттєву перевагу у швидкодії над GHASH та POLYVAL на сучасних процесорах Intel. Результати підтверджують перспективність використання дворівневих геш-конструкцій для побудови MAC-схем і систем автентифікованого шифрування, а загальна ідея конструкції застосовна до довільних скінченних полів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Chakraborty D., Ghosh S., Sarkar P. A Fast Single-Key Two-Level Universal Hash Function // IACR Transactions on Symmetric Cryptology. – 2017. – Vol. 1. – P. 106–128. DOI: 10.13154/tosc.v2017.i1.106-128.
2. Bernstein D. J. Polynomial evaluation and message authentication. – 2007. URL: http://cr.yp.to/papers.html#pema (дата звернення: 10.05.2026).
3. Gueron S., Kounavis M. E. Efficient implementation of the Galois counter mode using a carry-less multiplier and a fast reduction algorithm // Information Processing Letters. – 2010. – Vol. 110, No. 14–15. – P. 549–553.
4. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Boston : Pearson Education, 2019. – 768 p.

Семикрас Анжеліка Олександрівна – студентка групи 2БС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: lisemykras@gmail.com

Науковий керівник: ***Кирилащук Тетяна Геннадіївна*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kgt0998@gmail.com

Semykras Anzhelika – student of group 2BS-24B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: lisemykras@gmail.com

Scientific Supervisor: ***Kyrylashchuk Tatyana*** – assistant of the Information Security Department, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com