слення Хеммінгової віддалі в унітарному базисі та базисі Радемахера. Запропонована структура високопродуктивного спецпроцесора визначення Хеммінгової віддалі у ТЧБ Радемахера та оцінена його часова складність, яка зменшена у 16 разів у порівнянні з відомими пристроями.

Список використаних джерел:

1. Николайчук Я. М. Коди поля Галуа. Тернопіль: ТзОВ «Терно граф». 2012. 576 с.
2. Николайчук Я. М., Заведюк Т. О. Структура та функції рекурентного біонейрона для розпізнання образів у Хеммінговому просторі. *Збірник наукових праць Бучацького інституту менеджменту і аудиту*. Бучач. 2010. № 6. С. 37–40.
3. Николайчук Я. М., Кімак В. Л., Волинський О. І., Круліковський Б. Б. Пристрій визначення залишку по модулю багаторозрядного числа. Патент України на корисну модель № 90144, Бюл. № 9, 2014.
4. Устройство для суммирования. [Електронний ресурс]. Режим доступу: http//www.findpatent.ru/patent/254/2546569.html.).

In this paper the structure and components of multi-system characteristics special processors. Developed special processor scans and definition Hemmingi distance between codes presented in unitary theoretical and numerical basis conversion to binary code Rademacher.

Key words: *special processor, theoretical and numerical basis, Hemming distance.*

Одержано 16.02.2017

УДК 681.3.06

Г. З. Халімов, д-р техн. наук

Харківський національний університет радіоелектроніки, м. Харків

АНАЛІЗ СКЛАДНОСТІ РЕАЛІЗАЦІЙ КРИПТОСИСТЕМ НА ГРУПАХ

Представлений порівняльний аналіз реалізацій криптосистем на групах. Показано, що побудова криптосистем на групах вимагає ефективного алгоритму для відображень числа на групу і зворотного відображення з обчислювально простою груповою операцією. До теперішнього часу відома тільки одна реалізація криптосистеми MST_3, побудованої за Абелевим центром групи Судзукі.

Ключові слова: *логарифмічний підпис, криптосистеми PGM, MST_1, MST_2, MST_3.*

Вступ. Криптографія з відкритим ключем будується на складності розв'язання математичних проблем, які дуже часто, але не виключно, виникають з теорії чисел. На початку 80-х років, було запропоновано

застосування групових теоретичних проблем для криптографії (Wagner і Magyarik [1], Wagner [2], Magliveras [3]). Зокрема в роботах Magliveras та ін., були зроблені пропозиції для криптографічних схем на основі спеціальних розкладів кінцевих груп (так звані логарифмічні сигнатури) [3]. Крім того, відомі інші криптографічні дослідження Gonzarlez Vasco, Steinwandt, Birget, Bohliet і ін. Ці розкладання, як математичні об'єкти цікаві самі по собі. Наприклад, робота Hajors про гіпотезу Маньківського показує, що для абелевих груп, цей вид розкладання виникає при вивченні багатовимірних покриттів.

Прикладами криптосистем з відкритим ключем є MST_1, MST_2, MST_3. Актуальним завданням їх реалізації є побудова коротких логарифмічних сигнатур. Логарифмічні підписи, особливий тип групових розкладів, представляється як основні компоненти деяких криптографічних ключів. Науковий інтерес зв'язується з пошуком логарифмічних підписів у кінцевих групах (такі розкладання існують для вирішуваних, симетричних і знакозмінних груп), оцінкою їх практичної можливості бути реалізованим та секретності.

У роботі розглянуті основні реалізації криптосистем на групах і аналіз оцінки складності обчислень.

Логарифмічний підпис. Нехай $\alpha = [A_1, A_2, ...A_s]$ — накриття класу $(r_1, r_2, ..., r_s)$ для ς з $A_i = [\mathrm{a}_{i,1}, \mathrm{a}_{i,2}, ..., \mathrm{a}_{i,r_i}]$ і нехай $m = \prod_{i-1}^{s} r_i$. Нехай $m_1 = 1$ і $m_i = \prod_{j=1}^{i-1} r_j$ для $i = 2, ..., s$. Позначимо τ як канонічну бієкцію від $\mathbb{Z}_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \cdots \oplus \mathbb{Z}_{r_s}$ на $\mathbb{Z}_m$, тобто

$$\mathbb{Z}_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \cdots \oplus \mathbb{Z}_{r_s} \to \mathbb{Z}_m,$$

$$\tau(j_1, j_2, ..., j_s) := \sum_{i=1}^{s} j_i m_i .$$

Використовуючи τ, можемо визначити сюр'єктивне відображення $\breve{\alpha}$ породжене α:

$$\breve{\alpha} : \mathbb{Z}_m \to \varsigma,$$

$$\breve{\alpha}(x) := a_{1,j_1} \cdot a_{2,j_2} \cdots a_{\mathrm{s},j_s},$$

де $(j_1, j_2, ..., j_s) = \tau^{-1}(x)$. Оскільки τ й τ^{-1} ефективно обчислювані, то відображення $\breve{\alpha}(x)$ також ефективно обчислюване.

З іншого боку, з даним накриттям α і елементом $y \in \varsigma$, щоб визначити будь-який елемент $x \in \breve{\alpha}^{-1}(y)$, необхідно отримати кожне з можливих розкладень для y і визначити показники $j_1, j_2, ..., j_s$ такі, що $y = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{\mathrm{s},j_s}$. Це можливо тільки якщо α — просте. Оскі-

льки вектор $(j_1, j_2, ..., j_s)$ визначено, то $\breve{\alpha}^{-1}(y) = \tau(j_1, j_2, ..., j_s)$ може бути ефективно обчислено.

Криптосистема PGM (відображення груп перестановок) була запропонована С. Магліверасом заснована на логарифмічних підписах для кінцевих груп перестановок визначається як ендоморфічна криптосистема з закритим ключем.

Нехай $[\alpha, \beta]$ буде парою поперечних логарифмічних підписах для групи перестановок ς. Процедура шифрування $E_{\alpha,\beta} : \mathbb{Z}|\varsigma| \to \mathbb{Z}|\varsigma|$ визначена за допомогою:

$$E_{\alpha,\beta} \coloneqq \breve{\alpha} \circ \breve{\beta}^{-1}.$$

Відповідне перетворення з дешифрування представлено як:

$$D_{\alpha,\beta} \coloneqq E^{-1}{}_{\alpha,\beta} = E_{\beta,\alpha} = \breve{\beta} \circ \breve{\alpha}^{-1}.$$

Обидві логарифмічні підписи α і β — прості, вони мають зберігатися в секреті. Операції з логарифмічними підписами виконуються обчислювальне ефективно, отже, шифрування і дешифрування також виконується обчислювальне ефективно.

Криптосистема $\mathbf{MST_1}$. Нехай α — випадкова і β — простий логарифмічний підпис для кінцевої групи перестановок ς. Тоді відображення $\breve{\alpha} \circ \breve{\beta}^{-1} : \mathbb{Z}_{|\varsigma|} \to \mathbb{Z}_{|\varsigma|}$ — одностороння перестановка в $\sigma_{|\varsigma|}$. Однак, якщо $\breve{\alpha} \circ \breve{\beta}^{-1}$ записана як добуток кінцевої (сподіваємося малого) кількості поперечних логарифмічних підписів, то воно може бути ефективно інвертовано. Нехай $\theta_1, ..., \theta_k$ буде набором простих логарифмічних підписів, таких як: $\breve{\alpha} \circ \breve{\beta}^{-1} = \breve{\alpha} \circ \breve{\beta}^{-1} = \breve{\theta}_1 \circ ... \circ \breve{\theta}_k$. Еліс публікує $[\alpha, \beta]$ і ς, як відкритий ключ, але тримає в секреті $[\theta_1, ..., \theta_k]$. Перетворення шифрування $E_{\alpha,\beta} : \mathbb{Z}_{|\varsigma|} \to \mathbb{Z}_{|\varsigma|}$ визначено як:

$$E_{\alpha,\beta} \coloneqq \breve{\alpha} \circ \breve{\beta}^{-1}.$$

Шифрування є ефективно обчислювальним, так як β — проста. Функція дешифрування для даної системи визначається як:

$$D_{\alpha,\beta} \coloneqq \breve{\theta}_k^{-1} \circ ... \circ \breve{\theta}_1^{-1}.$$

Дешифрування є обчислюваним тільки якщо відомо розкладання $\breve{\alpha} \circ \breve{\beta}^{-1} = \breve{\theta}_1 \circ ... \circ \breve{\theta}_k$. Оскільки всі логарифмічні підписи θ_i — прості, то воно також є ефективним.

Хоча на практиці, не існує відомого ефективного алгоритму побудови даних розкладів, попередній результат показує, що вони дійс-

но існують. Припускаємо, що розкладання $\breve{\alpha} \circ \breve{\beta}^{-1}$ є обчислювальне неможливим.

Відомі потенційні проблеми, що пов'язані з генерацією ключів. До сьогодні залишається неясним, як отримати конкретні екземпляри MST_1.

Криптосистема MST_2. Нехай $\alpha = (a_{i,j})$ буде $[s,r]$ — сіткою чимала групи перестановок ς. Нехай H буде другою групою і $f : \varsigma \to \mathrm{H}$ — епіморфізмом. Тоді $\beta = (b_{i,j})$, де $b_{i,j} = f(a_{i,j})$ є $[s,r]$– сіткою для H. $[\alpha, \beta]$ — відкритий ключ, а відображення f зберігається в секреті.

Для шифрування повідомлення $h \in \mathrm{H}$ виконуємо наступну послідовність дій:

1) вибираємо випадкове ціле $R \in \mathbb{Z}_{r^s}$;
2) обчислюємо наступні значення: $y_1 = \breve{\alpha}(R), y_2 = h \bullet \breve{\beta}(R)$.

Пара $y = (y_1, y_2)$ є шифр текстом для повідомлення h.

Для дешифрування повідомлення виконуємо:

1) знаючи f обчислюємо $g = \breve{\beta}(R) = f(\breve{\alpha}(R)) = f(y_1)$;
2) отримуємо повідомлення $h = y_2 \bullet g^{-1}$.

Існує два відомих типу можливих атак на MST_2. Перша атака заснована на спробі визначення випадкового R, такого щоб $y_1 = \breve{\alpha}(R)$. В загальному випадку, R — не унікальне, але знаходження будь-якого R' з $y_1 = \breve{\alpha}(R')$ є злом системи. Ефективно обчислити R з $y_1 = \breve{\alpha}(R)$ означає розкласти y_1 щодо α, тобто знайти $(j_1, ..., j_s)$ такі, щоб $y_1 = a_{1,j_1} ... a_{s,j_2}$. Безпека системи проти такого роду атак заснована на припущенні, що для даної $[s,r]$-сітки α групи ς та елемента $g \in \varsigma$ знаходження розкладу $g = a_{1,j_1} ... a_{s,j_2}$ є не вирішена проблема.

У деяких класах груп, знання мережі та її образу від g розкриває деяку інформацію про g. Це може використовуватися для атаки на криптосистему MST_2 для цих класів групи [4].

Криптосистема MST_3 [4]. Аліса обирає велику групу ς й генерує:

1) простий логарифмічний підпис $\beta = [B_1, B_2, ..., B_s] := (b_{ij})$ класу $(r_1, r_2, ..., r_s)$ для $\mathbb{Z}$;

2) випадкове накриття $\alpha = [A_1, A_2, ..., A_s] := (a_{i,j})$ такого самого класу, як і β для деякої підмножини J від ς такого, що $A_1, ..., A_s \subseteq \varsigma \setminus \mathbb{Z}$.

Потім, обирає $t_0, t_1 ..., t_s \in \varsigma \setminus \mathbb{Z}$ й обчислює:

3) $\breve{\alpha} = [\tilde{A}_1, \tilde{A}_2, ..., \tilde{A}_s]$, де $\tilde{A}_i = t_{i-1}^{-1} A_i t_i$ для $i = 1, ..., s$;

4) $\gamma := (h_{ij}) = (b_{ij} \tilde{a}_{ij})$.

Аліса публікує свій відкритий ключ $(\alpha = (a_{ij}), \gamma = (h_{ij}))$, а $(\beta = (b_{ij}), (t_0, ..., t_s))$ — зберігає як свій закритий ключ.

Шифрування. Якщо Боб хоче відіслати повідомлення $x \in \mathbb{Z}_{|Z|}$ для Аліси, то

1) обчислює $y_1 = \breve{\alpha}(x)$ і $y_2 = \breve{\gamma}(x)$;

2) посилає $y = (y_1 y_2)$ Алісі.

Дешифрування. Аліса знає y_2 і обчислює

$$y_2 = \breve{\gamma}(x) = b_{1j_1} \tilde{a}_{1j_1} \cdot b_{2j_2} \tilde{a}_{2j_2} \cdots b_{sj_s} \tilde{a}_{sj_s} = b_{1j_1} t_0^{-1} a_{1j_1} t_1 \cdots b_{sj_s} t_{s-1}^{-1} a_{sj_s} t_s =$$

$$= b_{1j_1} b_{2j_2} \cdots b_{sj_s} t_0^{-1} a_{1j_1} a_{2j_2} \cdots a_{sj_s} t_s = \breve{\beta}(x) . t_0^{-1} \breve{\alpha}(x) t_s = \breve{\beta}(x) . t_0^{-1} y_1 t_s .$$

Далі обчислюється $\breve{\beta}(x) = y_2 t_s^{-1} y_1^{-1} t_0$.

Аліса відновлює x з $\breve{\beta}(x)$ використовуючи $\breve{\beta}^{-1}$, який ефективно обчислюємо, оскільки β — проста.

Перша реалізація MST_3 криптосистеми була створена на Судзукі 2-й групі порядку q^2, доказовою стійкістю яка визначається розміром кінцевого поля q. Імовірність реалізації зловмисником успішної атаки дорівнює $1/q(q-1)$.

Висновки. Стійкість криптосистем на групах ґрунтується на припущенні важко вирішуваної задачі розкладання елемента групи по набору елементів логарифмічною підпису. До теперішнього часу відома тільки одна реалізація криптосистеми MST_3, побудованої за Абелевим центром групи Судзукі. Практична побудова криптосистем на групах вимагає ефективного алгоритму для відображень числа на групу і зворотного відображення з обчислювально простою груповою операцією.

Список використаних джерел:

1. Wagner N. R. and Magyarik M. R. «A Public Key Cryptosystem Based on the Word Problem». In Advances in Cryptology. Proceedings of CRYPTO 1984, P. 19–36, edited by G. R. Blakley and D. Chaum, Lecture Notes in Computer Science 196. Berlin: Springer, 1985.

2. Wagner N. R. «Searching for Public-Key Cryptosystems». In Proceedings of the 1984 Symposium on Security and Privacy (SSP ’84), P. 91–98. Los Alamitos, CA: IEEE Computer Society Press, 1990.
3. Magliveras S. S. «A Cryptosystem from Logarithmic Signatures of Finite Groups». In Proceedings of the 29th Midwest Symposium on Circuits and Systems, P. 972–975. Amsterdam: Elsevier Publishing Company, 1986.
4. Lempken W., Magliveras S. S., Tran van Trung and Wei W. Apublic key cryptosystem based on non-abelian finite groups. J. of Cryptology. 2009. 22. P. 62–74.

This paper presents comparative analysis of cryptographic realyzations on groups. It is shown that the construction of cryptosystems in groups requires efficient algorithm for the mapping of number to the group and feedback mapping with computationally simple operation group. To date, there is only one known implementation of a cryptosystem MST_3, built on the base of the abelian center of Suzuki group.

Key words: *logarithmic signature, cryptosystems PGM, MST_1, MST_2, MST_3.*

Одержано 16.02.2017

УДК 681.31

Б. М. Шевчук, канд. техн. наук

Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ

ЗАВАДОСТІЙКА ПЕРЕДАЧА ЗАХИЩЕНИХ ПАКЕТІВ ДАНИХ В ІНФОРМАЦІЙНО-ЕФЕКТИВНИХ РАДІОМЕРЕЖАХ

З урахуванням оптимізації обчислень в процесі стиску та захисту сигналів, кадрів відеоданих та масивів даних запропонований комплексний підхід до реалізації швидкодіючого завадостійкого кодування і декодування захищених масивів даних, які передаються кодово-сигнальними послідовностями пакетів інформації з мінімально допустимою базою.

Ключові слова: *інформаційно-ефективні радіомережі, криптостійкі та завадостійкі пакети інформації, кодово-сигнальні послідовності пакетів, оптимізація обчислень в процесі кодування.*

Вступ. Широке застосування радіомереж, включаючи сенсорних, локально-регіональних, мікросупутникових, базується на побудові абонентських систем (АС), процесорні засоби яких здійснюють комплекс алгоритмів стиску, захисту вхідних масивів даних (сигналів, кадрів відеоданих), завадостійкого кодування стислих та захищених масивів даних, формування кодово-сигнальних послідовностей (КСП) інформаційних пакетів (ІП) з підвищеною інформаційною єм-