CURRENT ISSUES OF COMPUTER SCIENCE AND CYBERNETICS

DOI https://doi.org/10.30525/978-9934-26-373-6-1

CONSTRUCTION OF HIGH ORDER ELEMENTS FOR CRYPTOSYSTEMS WHICH USE NON-COMMUTATIVE GROUPS

ПОБУДОВА ЕЛЕМЕНТІВ ВЕЛИКОГО ПОРЯДКУ ДЛЯ КРИПТОСИСТЕМ, ЯКІ ВИКОРИСТОВУЮТЬ НЕКОМУТАТИВНІ ГРУПИ

Popovych B. R.
Assistant at the Department of Specialized Computer Systems Lviv Polytechnic National University Lviv, Ukraine

Попович Б. Р.
асистент кафедри спеціалізованих комп'ютерних систем Національний університет «Львівська політехніка» м. Львів, Україна

Popovych R. B.
Doctor of Physics and Mathematics, Professor, Professor at the Department of Specialized Computer Systems Lviv Polytechnic National University Lviv, Ukraine

Попович Р. Б.
доктор фізико-математичних наук, професор, професор кафедри спеціалізованих комп'ютерних систем Національний університет «Львівська політехніка» м. Львів, Україна

Безпека низки відомих криптографічних примітивів (протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля) ґрунтується на складності проблеми дискретного логарифму в скінченній циклічній групі [5, p. 103]. Нагадаємо, що проблема дискретного логарифму полягає в такому: для заданих елементів g і h групи знайти натуральне число x таке, що $g^x = h$. Своєрідним узагальненням цієї проблеми можна вважати проблему спряженості: для заданих елементів g і h групи знайти елемент x групи такий, що $g^x = xgx^{-1}$. Хоча проблему дискретного логарифму формулюють для будь якої скінченої групи, але в

застосуваннях до криптології добре вивчені лише кілька груп: мультиплікативні групи простого та розширеного скінченних полів (алгоритм Діффі-Хелмана), група взаємно простих з числом pq (p, q – прості) і менших за нього натуральних чисел (криптосистема RSA), група точок еліптичної кривої над скінченним полем. Усі наведені групи є абелевими. Для більшості інших груп, зокрема неабелевих, складність проблеми дискретного логарифму є недостатньо дослідженою. У всіх випадках (як абелевих, так і неабелевих груп) складність проблеми дискретного логарифма забезпечується наявністю в групі елемента великого порядку (в ідеалі твірного елемента групи) [5, p. 160]. Тому питання дослідження складності задачі дискретного логарифма, а також пов'язане з ним питання побудови елементів великого порядку в неабелевих групах, залишається актуальним.

Однією з широко відомих неабелевих груп є загальна лінійна група $GL(m, F_q)$ – матриці розміру $m \times m$, заповнені елементами скінченого поля F_q та з ненульовим визначником відносно операції множення матриць (або в іншій формі лінійні перетворення в першому варіанті з $(F_q)^m$ в $(F_q)^m$, а в другому – з F_{q^m} в F_{q^m} відносно операції композиції відображень) [3, p. 1276; 7, p. 22]. Елемент, який називають циклом Зінгера, має максимальний можливий для цієї групи порядок $q^m - 1$. Проте, невідомо як явно збудувати такий елемент. Є лише результати про його існування.

В [3, p. 1275] збудовано криптосистему з відкритим ключем, складність зламування якої ґрунтується на комбінації двох обчислювально складних задач: дискретного логарифму та спряженості. Суттєвою рисою цієї криптосистеми є те, що її розглядають в некомутативній групі $GL(m, F_q)$. Для реалізації системи потрібно мати в загальній лінійній групі два елементи великого порядку, які не комутують. Проте, як отримати такі елементи в роботі не описано. У наведеному в ній прикладі елементи вибирають випадком чином, а потім програмним шляхом обчислюють їх порядки. У випадку, коли загальна лінійна група має досить багато елементів, це неможливо зробити за прийнятний час.

У роботах [6, p. 115; 7, p. 27] запропоновано криптосистеми з використанням низки бієктивних перетворень (як лінійних, так і нелінійних) векторного простору $(F_q)^m$. Такі перетворення з операцією їх композиції утворюють неабелеву групу. Маючи в цій групі елемент великого порядку, можна реалізувати протокол Діффі-Хелмана, схему Ель-Гамаля чи цифровий підпис. Для отримання такого елемента

потрібен елемент великого порядку в загальній лінійній групі. Як його можна отримати в роботах не сказано. Є лише згадка про використання циклу Зінгера.

У роботі [4, p. 4] для протоколу узгодження таємного ключа через відкритий канал зв'язку використовують два елементи великого порядку із загальної лінійної групи над простим скінченним полем. Попередниками цього протоколу є протокол Діффі-Хелмана для комутативної групи та протокол Стікеля для некомутативної групи. Яким чином отримати потрібні елементи в роботі не пояснено.

Таким чином, проблема стійкості до зламування трьох згаданих постквантових криптосистем залежить від наявності елементів великого порядку із загальної лінійної групи. Тому актуальним є питання отримання елементів великого порядку в цій групі.

Для отримання елемента великого порядку є два відомих підходи: 1) побудова елемента з отриманням нижньої межі для порядку цього елемента [2, p. 73–76]; 2) використання теореми Лагранжа для скінченних груп [5, p. 76, 162]. Згідно з теоремою Лагранжа для скінченних груп, порядок елемента скінченої групи є дільником кількості елементів групи. Цей підхід можна застосувати лише якщо порядок групи розкладений в добуток простих чисел.

Далі описано, як можна втілити перший підхід у загальній лінійній групі [1, с. 278–285]. При цьому спираємося на результати з [2, p. 73–76] стосовно отримання елементів великого порядку в довільних скінченних полях.

Основна думка полягає в тому, щоб утворити матрицю A, визначник якої дорівнює $\det A = \theta$, де θ – елемент великого порядку, рівного $ord(\theta)$ в скінченному полі F_q. Оскільки визначник добутку матриць над полем дорівнює добутку визначників цих матриць, тобто $\det \prod_{i=1}^{r} M_i = \prod_{i=1}^{r} \det M_i$, то порядок матриці A є принаймні $ord(\theta)$. Дійсно, $\det A^i = \theta^i$, $\theta^i \neq 1$ при $1 \le i < ord(\theta)$ та $\theta^{ord(\theta)} = 1$. Порядок матриці A може бути й більшим від $ord(\theta)$, бо те, що визначник матриці $A^{ord(\theta)}$ дорівнює одиниці, не обов'язково означає співпадіння цієї матриці з одиничною матрицею.

Пропонуємо утворювати матрицю з визначником рівним α як добуток нижньої трикутної та верхньої трикутної матриць. Перевага – визначник нижньої або верхньої трикутної матриці дорівнює добутку її діагональних елементів. Тому просто утворити бажану трикутну матрицю, а тоді й довільну матрицю з потрібним визначником.

Зауважимо, що кожна матриця із загальної лінійної групи має *LU*-розклад, тобто може бути записана у вигляді добутку нижньої трикутної та верхньої трикутної матриць.

Більш точно, беремо нижню трикутну матрицю

$$\begin{pmatrix} \theta & 0 & ... & 0 \\ a_{21} & 1 & ... & 0 \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & 1 \end{pmatrix},$$

де θ – елемент великого порядку в F_q. Її визначник дорівнює θ. Вона має порядок принаймні $ord(\theta)$ і є елементом великого порядку в групі $GL(m, F_q)$. Верхня трикутна матриця має вигляд

$$\begin{pmatrix} 1 & b_{12} & ... & b_{1m} \\ 0 & 1 & ... & b_{2m} \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{pmatrix}.$$

Добуток таких нижньої трикутної і верхньої трикутної матриць є матрицею з визначником θ, яка загалом вже не є ні верхньою, ні нижньою трикутною матрицею. Вона має порядок принаймні $ord(\theta)$. Елементи в матрицях під (відповідно над) головною діагоналлю можемо довільно вибирати, виходячи з певних додаткових міркувань.

Література:

1. Попович Б. Р., Попович Р. Б. Елементи великого порядку для криптосистем з неабелевими базовими групами. *Вісник Хмельницького національного університету: серія «Технічні науки»*. 2023. № 4. С. 278–285.

2. Dunets R., Popovych B., Popovych R. On construction of high order elements in arbitrary finite fields. *JP Journal of Algebra, Number Theory and Applications*. 2019. Vol. 42 (1). P. 71–76.

3. Kanwal S., Ali R. A cryptosystem with noncommutative platform groups. *Neural Computing and Applications*. 2018. Vol. 29. P. 1273–1278.

4. Lizama-Pérez L., Romero J. Non-Commutative Key Exchange Protocol. Preprints 2021, 2021030716. https://doi.org/10.20944/preprints 202103.0716.v2.

5. Menezes A., Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, Boca Raton. 2001. 816 p.

6. Ustimenko V. On the families of stable transformations of large order and their cryptographical applications. *Tatra Mountains Mathematical Publications*. 2017. Vol. 70 (1). P. 107–117.

7. Ustimenko V. On Computations with Double Schubert Automaton and Stable Maps of Multivariate Cryptography. *Interdisciplinary Studies of Complex Systems.* 2021. № 19. P. 18–32.