DOI 10.31891/2307-5732-2024-339-4-22
УДК 621.397

ПОПОВИЧ БОГДАН
Львівський національний медичний університет імені Данила Галицького,
Національний університет "Львівська політехніка"
https://orcid.org/0000-0001-6259-2361
e-mail: bogdan.popovych@gmail.com
ПОПОВИЧ РОМАН
Національний університет "Львівська політехніка"
https://orcid.org/0009-0006-0992-0825
e-mail: rombp07@gmail.com

УЗАГАЛЬНЕННЯ НЕКОМУТАТИВНОГО ПРОТОКОЛУ УЗГОДЖЕННЯ КЛЮЧА

Наведено порівняльний аналіз відомих протоколів узгодження таємного ключа через відкритий канал зв'язку. Запропоновано узагальнення відомого протоколу з використанням некомутативного множення матриць над простим скінченним полем на випадок довільного скінченного поля.

Ключові слова: протокол узгодження ключа, скінченне поле, загальна лінійна група, порядок елемента.

POPOVYCH BOGDAN
Lviv National Medical University named after Danylo Halytskyi,
Lviv Polytechnic National University
POPOVYCH ROMAN
Lviv Polytechnic National University

GENERALIZATION OF NON-COMMUTATIVE KEY EXCHANGE PROTOCOL

A symmetric cryptosystem requires a secret key agreed by both parties. The Diffie-Hellman protocol was originally proposed for its exchange via an open communication channel. It is based on the computational complexity of the discrete logarithm problem in certain finite groups (the multiplicative group of a finite field, the group of points of an elliptic curve over a finite field). The availability of a powerful quantum computer will allow solving the discrete logarithm problem in these groups. Therefore, the issue of construction of secret key exchange protocols that will be resistant to attacks using a quantum computer has become urgent.

The paper provides a comparative analysis of known protocols for a secret key exchange via an open communication channel. A generalization of the known protocol using non-commutative matrix multiplication over a prime finite field for the case of an arbitrary finite field is proposed. In this protocol, two high order elements from the general linear group over a finite field should be used, which satisfy an additional condition. It consists in the fact that each of the matrices cannot be reduced to a diagonal form by conjugation transformation. This condition follows from the considerations of avoiding an attack on the protocol. It is shown how to construct such elements.

For the proposed generalization of the protocol, the sizes of public and private keys, secret key, the size of the finite field, which ensure the appropriate level of security, are calculated. The dimensions of matrices (elements of the general linear group) that we use are also given. The generalization of the protocol to the case of an arbitrary finite field increases the flexibility of choosing protocol parameters to ensure the desired level of security.

Keywords: key exchange protocol, finite field, general linear group, order of element.

Постановка проблеми

Для того, щоб можна було користуватись симетричною криптосистемою, потрібен узгоджений двома сторонами таємний ключ для шифрування (дешифрування). Для його узгодження через відкритий канал зв'язку початково був запропонований протокол Діфі-Хелмана [1]. Цей протокол ґрунтується на обчислювальній складності задачі дискретного логарифму [2] в певних скінченних групах (мультиплікативна група скінченного поля, група точок еліптичної кривої над скінченним полем). Наявність потужного квантового комп'ютера дозволить розв'язувати задачу дискретного логарифму в цих групах за поліноміальний час [3]. Тому актуальним є питання побудови протоколів узгодження таємного ключа, які будуть стійкими до атак з використанням квантового комп'ютера.

Аналіз останніх джерел

Через F_q, де $q = p^n$ для деякого простого числа p та натурального числа n, позначаємо скінченне поле з q елементів. Мультиплікативна група скінченного поля дорівнює $F_q^* = F_q \backslash \{0\}$. Загальна лінійна група $GL(m, F_q)$ – це матриці розміру $m \times m$ заповнені елементами поля F_q та з ненульовим визначником відносно операції множення матриць. Операція множення в цій групі є некомутативною. Такі групи прийнято називати неабелевими. Кількість елементів у згаданій групі дорівнює $\prod_{i=0}^{m-1}(q^m - q^i)$, а максимально можливий порядок елемента $q^m - 1$ [4].

Послідовність дій при реалізації протоколу Діфі-Хелмана [1] описана далі. Спочатку користувачі Аліса та Боб погоджують скінченну групу G та елемент g великого порядку в цій групі. Аліса та Боб обмінюються утвореними ними елементами g^a та g^b і тоді обчислюють однаковий елемент $(g^b)^a = (g^a)^b = g^{ab}$, який не проходить через відкритий канал зв'язку й може слугувати, скажімо, як таємний ключ при симетричному шифруванні. Реалізацію цього протоколу в абелевій групі (мультиплікативна група скінченного поля, еліптична крива) можна зламати з використанням квантового комп'ютера.

Тому запропоновано протокол узгодження таємних даних через відкритий канал зв'язку з використанням неабелевих груп та двох різних елементів у них [5]. Цей протокол можна розглядати як перенесення ідеї протоколу Діфі-Хелмана для комутативних груп на некомутативний випадок. У комутативному випадку використовують степінь g^u одного елемента g групи. У протоколі Стікеля використовують некомутативну поведінку добутку степенів a^v, b^w двох елементів a,b групи.

Послідовність дій у протоколі Стікеля описано далі. Спочатку користувачі погоджують скінченну неабелеву групу G з q елементами та елементи a, b великого порядку в цій групі, для яких $ab \neq ba$. Група G та елементи a, b є публічними даними. Аліса вибирає два випадкових натуральних числа $1<m,n\leq q-1$, обчислює $u = a^m b^n$ та пересилає значення u Бобу. Він вибирає два числа $1 < r,s \leq q-1$, обчислює $v = a^r b^s$ та надсилає значення v Алісі. Аліса формує величину $a^m v b^n = a^{m+r} b^{n+s}$. Боб аналогічно формує $a^r u b^s = a^{r+m} b^{s+n}$. У результаті цих дій як Аліса, так і Боб мають той самий елемент $a^{m+r} b^{n+s}$. Він може слугувати як узгоджений таємний ключ. Для зламування цього протоколу (якщо він реалізований в загальній лінійній групі) запропонована атака на основі розв'язування системи лінійних рівнянь.

В роботі [6] наведено низку аналогів протоколу Діфі-Хелмана у загальній лінійній групі. Зокрема, використано перетворення подібності (спряженості). Проте для їх реалізації розглянуто отримання матриць максимально можливого порядку лише для часткового випадку $q = 2$. Виписано (без доведення в загальному) приклади таких матриць для непарних m та для $m = 32,\ 64,\ 128,\ 256$. Також досліджувалось питання отримання матриць максимально можливого порядку в групі $GL(m, F_2)$ при умові, що маємо примітивний елемент поля F_{2^m}. Останню побудову не можна вважати явною побудовою елемента максимального порядку. Ще одним недоліком є те, що матриці, які отримуємо таким способом, комутують.

У роботі [7] для протоколу узгодження таємного ключа через відкритий канал зв'язку використовують алгебру квадратних матриць фіксованого розміру, заповнених елементами простого скінченного поля, відносно операції множення. Стійкість цього протоколу до зламування ґрунтується на обчислювальній складності проблеми спряженості у вказаній алгебрі. Проте цей протокол задано лише над простим скінченним полем. Можливість його застосування над довільним (тобто розширеним) скінченним полем залишається невирішеною. Також для цього протоколу потрібні дві матриці великого порядку та недіагоналізовні. Виникає питання, як їх отримати.

В роботі [8] розглянуто побудову елементів (матриць) великого порядку в загальній лінійній групі над скінченним полем. Проте, вимога одночасної не діагоналізовності матриць не розглядалася.

Тому актуальною задачею є узагальнення протоколу та отримання в загальній лінійній групі елементів великого порядку, які не діагоналізуються.

Метою роботи є узагальнити протокол узгодження таємного ключа з роботи [7] на випадок загальної лінійної групи над довільним скінченним полем та запропонувати деякі вдосконалення цього протоколу.

Виклад основного матеріалу

Побудова протоколу з роботи [7] починається з вибору двох елементів u та v загальної лінійної групи. У праці [7] для реалізації протоколу брали просте скінченне поле F_p. Наше пропозиція полягає в тому, що можна узагальнити згадану побудову на випадок матриць над довільним (як простим, так і розширеним) скінченним полем. Узагальнення протоколу на випадок довільного скінченного поля збільшує гнучкість вибору параметрів протоколу для забезпечення потрібного рівня безпеки. Також на відміну від згаданої роботи беремо лише матриці, для яких існують обернені (матриці з ненульовим визначником). Дійсно, в роботі [7] зауважено, що при отриманні таємного ключа, який не є оборотною матрицею, слід повторити роботу протоколу. Тому логічно виконувати обчислення лише з оборотними матрицями. Таким чином вважаємо, що матриці u, v є елементами загальної лінійної групи $GL(m, F_q)$ над будь-яким скінченним полем F_q.

Приватні ключі обидвох сторін включають матрицю із загальної лінійної групи та пари натуральних чисел, які менші від максимально можливого порядку $q^m - 1$. Більш точно, приватний ключ Аліси це трійка (K_A, x_A, y_A), де K_A – випадково вибраний елемент загальної лінійної групи, x_A та y_A – випадково вибрані натуральні числа, які менші від $q^m - 1$. Аналогічно, приватний ключ Боба – це трійка (K_B, x_B, y_B), де K_B – випадково вибраний елемент загальної лінійної групи, x_B та y_B – випадково вибрані натуральні числа, які менші від $q^m - 1$.

Обидві сторони обчислюють свої публічні ключі згідно з аналогічними виразами. Кожен публічний ключ є парою елементів із загальної лінійної групи. Публічний ключ Аліси отримують згідно з виразами

$$P_A = K_A u^{x_A} K_A^{-1},\ Q_A = K_A v^{y_A} K_A^{-1},$$

а публічний ключ Боба – згідно з виразами

$$P_B = K_B u^{x_B} K_B^{-1},\ Q_B = K_B v^{y_B} K_B^{-1}.$$

Сторони обмінюються своїми публічними ключами через відкритий канал зв'язку. Тоді обчислюють свої так звані канальні ключі C_A (обчислює Аліса) та C_B (обчислює Боб) згідно з такими виразами:

$$C_A = (P_B)^{x_A} (Q_B)^{y_A} = K_B (u)^{x_A x_B} (v)^{y_A y_B} K_B^{-1},$$

$$C_B = (P_A)^{x_B}(Q_A)^{y_B} = K_A(u)^{x_A x_B}(v)^{y_A y_B}K_A^{-1}.$$

Сторони відсилають свої канальні ключі один одному та виконують над ними обчислення з використанням своїх приватних матриць. Власне Аліса обчислює

$$K_{SA} = K_A^{-1}C_B K_A = (u)^{x_A x_B}(v)^{y_A y_B},$$

а Боб обчислює

$$K_{SB} = K_B^{-1}C_B K_B = (u)^{x_A x_B}(v)^{y_A y_B}.$$

У результаті виконання протоколу, Аліса та Боб узгодили таємний ключ

$$K = K_{SA} = K_{SB} = (u)^{x_A x_B}(v)^{y_A y_B}.$$

Послідовність дій в описаному протоколі схематично відображена на рис. 1.

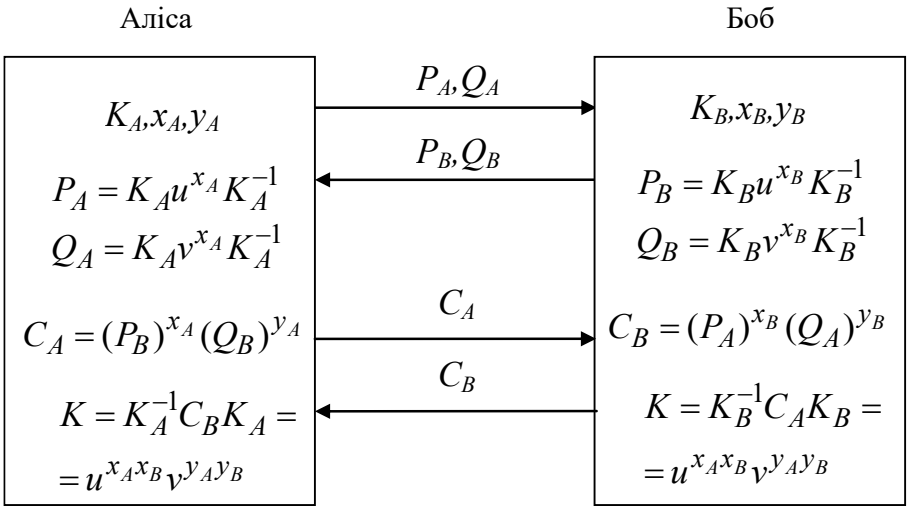

Рис. 1. Послідовність дій в узагальненому протоколі

Узгоджений таємний ключ K можна використати по-різному. Загальноприйнятий варіант: перетворити K в послідовність бітів і застосовувати як таємний ключ для симетричного шифрування (а потім розшифровування). Інший варіант запропоновано в [7]. Він залишається вірним і для запропонованого нами узагальнення цього протоколу. Для матриці K існує обернена матриця K^{-1}. Матрицю K та обернену до неї матрицю K^{-1} можна використовувати для зашифровування повідомлення $C = K^{-1}MK$, а потім відповідно для розшифровування $M = KCK^{-1}$, де M є початковим повідомленням (не мусить бути оборотною матрицею), а C – криптограмою, отриманою в результаті зашифровування цього повідомлення.

Щоб забезпечити стійкість цього протоколу до зламування, матриці u та v повинні мати великий мультиплікативний порядок [8] і, крім того, бути не діагоналізовними. Пропонуємо як не діагоналізовну матрицю брати матрицю вигляду

$$A = \begin{pmatrix} \alpha & b_{12} & \dots & b_{1m} \\ 0 & \alpha & \dots & b_{2m} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha \end{pmatrix},$$

де щонайменше один елемент над головною діагоналлю наведеної матриці не дорівнює нулю, а α є елементом великого порядку в F_q. Дійсно, характеристичний многочлен $p(\lambda) = det(A - \lambda E) = (\lambda - \alpha)^m$ наведеної матриці має лише один корінь α кратності m та відповідно лише один власний вектор. Очевидно, що визначник такої матриці дорівнює α^m. Якщо число m взаємно просте з $q - 1$, то порядок елемента α^m співпадає з порядком елемента α. Тоді запропонована матриця є елементом великого порядку, а саме порядку принаймні $ord(\alpha)$. Таким чином, отримали матрицю, яка є елементом великого порядку в загальній лінійній групі та одночасно не є діагоналізованою.

Зрозуміло, що коли матриця A не є діагоналізовною, то спряжена з нею матриця PAP^{-1} також не діагоналізована. Тобто, взявши замість матриці A спряжену з нею матрицю PAP^{-1}, отримаємо не діагоналізовану матрицю, яка вже не є верхньою трикутною матрицею. Разом з тим, порядок останньої матриці співпадає з порядком початкової матриці A.

Зловмисник може пробувати отримати таємний ключ, використовуючи один з канальних ключів C_A або C_B. Для цього йому треба розв'язати обчислювально складну задачу спряженості в загальній лінійній групі: відтворити K за канальним ключем $C_A = K_B K K_B^{-1}$ або за канальним ключем $C_B = K_A K K_A^{-1}$.

Для запропонованого узагальнення протоколу підраховано розміри публічних та приватних ключів, секретного ключа, розмір скінченого поля, які забезпечують відповідний рівень безпеки. Також наведено розміри матриць (елементів загальної лінійної групи), якими користуємося. Під розміром скінченого поля розуміємо логарифм за основою два від кількості елементів скінченного поля. Результати обчислень наведені в табл. 1. Усі величини в ній даються в бітах.

Таблиця 1

Розміри скінченного поля/публічних/приватних ключів (біт) залежно від рівня безпеки та розміру матриць *m*

Рівень безпеки, біт	Розмір скінченного поля/публічного/приватного ключа, біт			
	m=2	*m*=3	*m*=4	*m*=5
80	20/160/160	9/162/135	5/160/120	4/200/140
96	24/192/192	11/198/165	6/192/144	4/200/140
112	28/224/224	13/234/195	7/224/168	5/250/175
128	32/256/256	15/270/225	8/256/192	6/300/210
160	40/320/320	18/324/270	10/320/240	7/350/245
192	48/384/384	22/396/330	12/384/288	8/400/280
224	56/448/448	25/450/375	14/448/336	9/450/315
256	64/512/512	29/522/435	16/512/384	11/550/385
512	128/1024/1024	57/1026/855	32/1024/768	21/1050/735

Оскільки секретний ключ – це одна матриця із загальної лінійної групи, то розмір секретного ключа дорівнює $m^2\ log_2\ q$. Вважаємо, що рівень безпеки співпадає з розміром секретного ключа. Виходячи з цього, якщо маємо задані рівень безпеки s і розмір матриць, то розмір поля дорівнює $log_2\ q = \frac{s}{m^2}$. Так як публічний ключ – це дві матриці із загальної лінійної групи, то розмір публічного ключа дорівнює $2m^2\ log_2\ q$. Оскільки приватний ключ – це два числа, які не перевищують $q^m - 1$, та одна матриця із загальної лінійної групи, то розмір приватного ключа – $m^2\ log_2\ q + 2\ log_2(\ q^m - 1)$.

Як бачимо з табл. 1, зокрема, для рівня безпеки $s = 512$ та розміру матриць $m = 4$ маємо розмір скінченого поля 32 біт, розмір публічного ключа дорівнює 1024 біт, а розмір приватного ключа – 768 біт.

Висновки

Узагальнено на випадок довільного скінченного поля відомий некомутативний протокол узгодження ключа. Попередниками цього протоколу є протокол Діфі-Хелмана для комутативної групи та протокол Стікеля для некомутативної групи. У цьому протоколі слід використовувати два елементи великого порядку із загальної лінійної групи з додатковою умовою. Умова полягає в тому, що ці дві матриці повинні бути не діагоналізованими. Вона випливає з міркувань уникнення атаки на протокол. Показано, як збудувати такі елементи.

Для запропонованого узагальнення протоколу оцінено кількість елементів скінченного поля та розміри публічних і приватних ключів залежно від заданого рівня безпеки протоколу та розміру матриць, які використовуємо в протоколі.

Література

1. Diffie W. New directions in cryptography / W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory. – 1976. – Vol. 22, No. 6. – P. 644–654. DOI: https://doi.org/10.1109/TIT.1976.1055638

2. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton: CRC Press, 2001. – 816 p.

3. Galbraith S. D. Mathematics of Public Key Cryptography / S. D. Galbraith. – New York: Cambridge University Press, 2012. – 630 p.

4. Ghorpade S. R. Primitive polynomials, singer cycles and word-oriented linear feedback shift registers / S. R. Ghorpade, S. U. Hasan, M. Kumari // Designs, Codes and Cryptography. – 2011. – Vol. 58, No. 2. – P. 123–134. DOI: https://doi.org/10.1007/s10623-010-9387-7

5. Stickel E. A new method for exchanging secret keys / E. Stickel // Proc. of 3-rd Int. Conf. on Information Technology and Applications, July 4–7, 2005, Sydney, Australia. – Vol. 2, P. 426-430. DOI: https://doi.org/10.1109/ICITA.2005.33

6. Білецький А. Я. Матричні аналоги протоколу Діффі-Хеллмана / А. Я. Білецький, А. А. Білецький, Р. Ю. Кандиба // Вісник нац. ун-ту "Львівська політехніка" Автоматика, вимірювання та керування. – 2012. – № 741. – С. 128–133.

7. Lizama-Pérez L. A. Non-Commutative Key Exchange Protocol / L. A. Lizama-Pérez, J. M. L. Romero // Preprints 2021, 2021030716. DOI: https://doi.org/10.20944/preprints202103.0716.v2

8. Попович Б. Р. Елементи великого порядку для криптосистем з неабелевими базовими групами / Б. Р. Попович, Р. Б. Попович // Вісник Хмельницького нац. ун-ту: серія "Технічні науки". – 2023. – № 4. – S. 278–285. DOI: https://www.doi.org/10.31891/2307-5732-2023-323-4-278-285

References

1. Diffie W. New directions in cryptography / W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory. – 1976. – Vol. 22, No. 6. – P. 644–654. DOI: https://doi.org/10.1109/TIT.1976.1055638

2. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton: CRC Press, 2001. – 816 p.

3. Galbraith S. D. Mathematics of Public Key Cryptography / S. D. Galbraith. – New York: Cambridge University Press, 2012. – 630 p.

4. Ghorpade S. R. Primitive polynomials, singer cycles and word-oriented linear feedback shift registers / S. R. Ghorpade, S. U. Hasan, M. Kumari // Designs, Codes and Cryptography. – 2011. – Vol. 58, No. 2. – P. 123–134. DOI: https://doi.org/10.1007/s10623-010-9387-7

5. Stickel E. A new method for exchanging secret keys / E. Stickel // Proc. of 3-rd Int. Conf. on Information Technology and Applications, July 4–7, 2005, Sydney, Australia. – Vol. 2, P. 426-430. DOI: https://doi.org/10.1109/ICITA.2005.33

6. Biletskyi A. Ya. Matrychni analohy protokolu Diffi-Khellmana / A. Ya. Biletskyi, A. A. Biletskyi, R. Yu. Kandyba // Visnyk nats. un-tu “Lvivska politekhnika” Avtomatyka, vymiriuvannia ta keruvannia. – 2012. – № 741. – S. 128–133.

7. Lizama-Pérez L. A. Non-Commutative Key Exchange Protocol / L. A. Lizama-Pérez, J. M. L. Romero // Preprints 2021, 2021030716. DOI: https://doi.org/10.20944/preprints202103.0716.v2

8. Popovych B. R. Elementy velykoho poriadku dlia kryptosystem z neabelevymy bazovymy hrupamy / B. R. Popovych, R. B. Popovych // Visnyk Khmelnytskoho nats. un-tu: seriia “Tekhnichni nauky”. – 2023. – № 4. – S. 278–285. DOI: https://www.doi.org/10.31891/2307-5732-2023-323-4-278-285