МОДИФІКОВАНИЙ КВАНТОВИЙ АЛГОРИТМ ШОРА ДЛЯ ПОШУКУ ДИСКРЕТНОГО ЛОГАРИФМУ

Максутов Д.С
Науковий керівник – к.т.н., проф. Качко О.Г.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф. Системотехніки,
тел. (057) 702-13-06)
e-mail: dmytro.maksutov@nure.ua, факс (057) 702-11-13

The given work is devoted to the modern developments in the field of quantum computer algorithms related to cryptanalysis. The major topic of the work is a modification of the Shor quantum algorithm that is designed to solve a discrete logarithm problem. The work also contains information about the current state of quantum computing technologies and known non-quantum solutions to the discrete logarithm problem. The aim of the work is to demonstrate that nowadays-cryptographic systems based on Elliptic-curve cryptography (ECC) are vulnerable to quantum algorithms or will be vulnerable in the near future.

З розвитком технології виробництва та емуляції квантових комп'ютерів, а також стрімкого розвитку технологій що покладаються на засоби асиметричної криптографії з використанням еліптичних кривих, таких як шифрування даних у пристроях компанії Blackberry та деякі імплементації Blockchain, нагальним стає питання крипто аналізу криптографії на еліптичних кривих та пошук і вдосконалення алгоритмів пошуку дискретного логарифму, який лежить в її основі.

На сьогодні існує декілька не квантових алгоритмів для пошуку дискретного логарифму, які досягають теоретичного максимуму швидкодії можливого на звичайних ЕВМ. Це таки алгоритми, як модифікація загального методу решета числового поля (GNFS) [1] з асимптотичною оцінкою $O(e^{(\frac{64}{9})^{\frac{1}{3}}(\ln p)^{\frac{1}{3}}(\ln\ln p)^{\frac{2}{3}}})$ та p-алгоритм Поларда [2] з асимптотичною оцінкою $O(\sqrt{q})$, де q – це порядок підгрупи F_p і p – порядок поля Галуа F_p.

З появою теорії квантових комп'ютерів почалася активна розробка квантових алгоритмів для ефективного вирішення проблем факторизації та пошуку дискретного логарифму. В 1994 році Пітер Шор опублікував перший варіант квантового алгоритму для вирішення вищеозначених проблем. Через три роки був опублікований докладний опис алгоритму [3]. Шор описав алгоритм поліноміальної складності для пошуку дискретного логарифму лише для певного випадку, а саме, пошук дискретного логарифму у мультиплікативній групі F_p^* поля F_p.

Це залишило простір для вдосконалення алгоритму з метою покращення асимптотичної оцінки складності, кількості задіяних кубітів і

застосування його в інших групах поля F_p. Одним з таких вдосконалень є адаптація алгоритму Шора для пошуку дискретного логарифму в групі G з відомим простим порядком q, і груповою операцією $\odot$ [4]. Вдосконалений алгоритм складається з двох кроків:

1. Власне квантовий алгоритм, який приймає на вхід генератор групи g і елемент $x = [d]g$ і повертає, як результат пару (k, j) і $[e]g$, що ігнорується.
2. Класичний алгоритм, що приймає на вхід пару (k, j) і повертає, як результат шуканий дискретний логарифм d, якщо пара «хороша», тобто відповідає певним вимогам.

Описаний алгоритм потребує $2[\log_2 q]$ регістрів для індексу і обчислення двох квантових перетворень Фур'є розміру $2^{[\log_2 q]}$. Теоретична нижня границя вірогідності отримання шуканого дискретного логарифму з першого запуску дорівнює 2^{-10}. Практична вірогідність має бути вищою, але це ще необхідно перевірити.

Алгоритм теоретично обґрунтовано, тому подальше дослідження буде стосуватися вивчення поведінки алгоритму на практиці, а саме його реалізацію і запуск на емуляторі або одному з доступних квантових комп'ютерів (IBM), з подальшим відстеженням його роботи під впливом можливої декогеренції та квантового шуму.

Список джерел:

1. O. Schirokauer, "Discrete Logarithms and Local Units", in Philosophical Transactions of the Royal Society of London, volume A 345, 1993, pp. 409-423.
2. S. C. Pohlig, M. E. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance", in IEEE Transactions on Information Theory, volume IT-24, no 1, 1978, pp. 106-110.
3. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", in SIAM Journal of Computing, volume 26, no 5, 1997, pp. 1484-1509.
4. Martin Ekerå, "Modifying Shor's algorithm to compute short discrete logarithms", in IACR Cryptology ePrint Archive, 2016