ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ СИМЕТРИЧНИХ ШИФРІВ ДЛЯ ПОБУДОВИ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Михайло Савчук[1] , Андрій Фесенко[2]

Національний технічний університет України "КПІ"
пр. Перемоги, 37, Київ, 03056, Україна, тел.: (+38044) 241-68-76
E-mail: [1] msavchuk@ukrpost.net, [2] yustas92@ukr.net

Анотація

Навіть у випадку створення потужного квантового комп'ютера деякі задачі так і залишаться для нас важкими з точки зору відсутності ефективних квантових алгоритмів. Для криптографії цей факт означає те, що вже зараз можна перейти до нових систем, які дозволять їх використовувати без остраху можливості створення потужних екземплярів квантового комп'ютера.

В даній роботі запропоновано викоростовувати перетворення блочних шифрів, які є стійкими до атак на основі відкритого тексту, в якості односторонніх перетворень для багатьох криптографічних протоколів. Від блочного шифру додатково вимагається бути частково комутативним, або локально комутативним. Такі перетворення будуть у багатьох випадках односторонніми і важкооборотними навіть за моделі квантових обчислень. Досліджено існування таких шифрів і проаналізовано стійкість новоутворених криптопротоколів та схем за стандартної моделі квантових обчислень.

Вступ

Після достатньої кількості досліджень, які були проведені останнім часом, виявилося, що квантові комп'ютери не стануть панацеєю від усіх проблем. Зокрема, досі не відомий жоден ефективний квантовий алгоритм для будь-якої *NP*-повної задачі. Навіть не доведено, що такого алгоритму немає, оскільки ця задача є надзвичайно важкою й нерозв'язаною також і у класичному випадку (проблема *P* vs *NP*). Ми не можемо довести існування такого квантового алгоритму й за припущення, що $P \neq NP$, що є більш ймовірним. Але більшість дослідників вважають, що стандартна модель квантових обчислень з оракулом не зможе розв'язати *NP*-повну задачу, більш того на даний момент існує думка, що й деякі задачі з класу *NPI*, який належить *NP*, але не перетинається з класом *NP*-повних задач, не знайдуть швидкого вирішення на квантовому комп'ютері [1]. Зрозуміло, що вирішення цих питань є важливим для перспектив сучасної криптографії. У випадку створення досить потужного квантового комп'ютера будуть зламані багато існуючих криптоситем, що базуються, наприклад, на складності задач факторизації та дискретного логарифму, завдяки алгоритму Шора [2]. З іншого боку, доведені, або загально узгоджені обмеження квантової моделі обчислень можна використовувати для побудови нових криптопримітивів, стійких у більш широкому сенсі.

Постановка задачі

Абсолютна більшість дослідників вважає, що відомі стійкі алгоритми блочного шифрування не матимуть ефективних алгоритмів взламування і за квантової моделі обчислень. Хіба що буде необхідним збільшити розмір ключів, оскільки в будь-якому випадку, навіть якщо і не знайдеться швидкий алгоритм розв'язку, алгоритм Гровера поліпшить швидкість пошуку з $O(N)$ до $O(\sqrt{N})$ [3]. Це один з результатів, які ми використаємо для побудови нових криптографічних протоколів.

Припустимо, що $E_k : X \to X$, де $k \in K$ - деякий ключ з ключового простору, а X - множина відкритих текстів, буде алгоритмом блочного шифрування, який є стійким до атак на основі відкритого тексту і для якого в нас є підстави вважати його стійким навіть у випадку застосування квантового комп'ютера. Для подальшого використання нам необхідно також вимагати від E_k додаткової властивості. А саме, припустимо, що E_k буде частково комутативним відображенням, тобто $\forall x \in X$, $\forall k_1, k_2 \in K$ буде справедливим наступне співвідношення $E_{k_2}(E_{k_1}(x)) = E_{k_1}(E_{k_2}(x))$ (або, що E_k буде локально комутативним відображенням, тобто $\exists X_0 \subset X$ $\forall x_0 \in X_0$, $\forall k_1, k_2 \in K$ $E_{k_2}(E_{k_1}(x_0)) = E_{k_1}(E_{k_2}(x_0))$, при чому потужність множини X_0 або дорівнює одиниці, або суттєво менша за потужність множини X). Такої властивості буде достатньо для заміни односторонньої функції в багатьох криптографічних протоколах, таких як протокол Діффі-Хелмана, криптосистема Ель-Гамаля, схема Мессі-Омури та ін. [4].

Наприклад, аналог схеми Діффі-Хелмана з використанням блочного шифру матиме наступний вигляд. Нехай E_k - локально комутативний шифр і x_0 - одна з його точок комутативності.

1. Абонент А генерує випадкове значення k_A для ключа, обчислює $y_A = E_{k_A}(x_0)$ та відсилає це значення абоненту В.
2. Абонент В генерує випадкове значення k_B для ключа, обчислює $y_B = E_{k_B}(x_0)$ та відсилає це значення абоненту А.
3. Абонент А обчислює значення $s_A = E_{k_A}(y_B) = E_{k_A}(E_{k_B}(x_0))$.
4. Абонент В обчислює значення $s_B = E_{k_B}(y_A) = E_{k_B}(E_{k_A}(x_0))$.

Завдяки властивості локальної комутативності буде справедливою тотожність $s_A = s_B$.

Аналіз

Одним з перших питань, що постають у разі використання таких односторонніх функцій є питання існування блочних шифрів з заданою властивістю. Ми можемо ствердно відповісти на це питання, але в цій частині залишається відкритим питання щодо можливості викорастання деякою схеми, яка могла б наділяти бажаною властивістю вже відомі блочні шифри. Другим, питанням, що досліджувалося було питання про зменшення стійкості блочного шифру завдяки властивості комутативності. І, нарешті, головне питання дослідження – це питання стійкості запропонованої схеми побудови криптографічних протоколів в рамках квантової моделі обчислень з оракулом і складністю відносно кількості запитів. Саме ці питання й досліджуються в даній роботі.

Література:

[1] S. Aaronson, "NP-complete problems and physical reality", ACM SIGACT News, 36(1) :30–52
[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comp., 26, No. 5, pp 1484–1509, 1997
[3] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack", Phys. Rev. Lett. 79, 325-328 , 1997
[4] B. Schneier, "Applied Cryptography : Protocols, Algorithms, and Source Code in C", Wiley, 2nd Edition, 1995