КРАТКИЕ СООБЩЕНИЯ

А.В. ФЕСЕНКО

УДК 512.54.05

УЯЗВИМОСТЬ В КВАНТОВОЙ МОДЕЛИ ВЫЧИСЛЕНИЙ КРИПТОПРИМИТИВОВ, ОСНОВАННЫХ НА ЗАДАЧЕ ПОИСКА СОПРЯГАЮЩЕГО ЭЛЕМЕНТА И СТЕПЕНИ

Аннотация. Разработан эффективный алгоритм решения в квантовой модели вычислений обобщенной задачи дискретного логарифмирования с использованием сведения к абелевой задаче о скрытой подгруппе. Предложенный метод позволяет в квантовой модели вычислений эффективно решить частную задачу поиска сопрягающего элемента и степени, на сложности решения которой в отдельных группах основывается стойкость нескольких криптографических систем и протоколов.

Ключевые слова: квантовая модель вычислений, задача поиска сопрягающего элемента и степени, криптография, основанная на группах.

ВВЕДЕНИЕ

Одним из современных направлений криптографии является криптография, основанная на группах [1]. В основе стойкости подобных систем лежат труднорешаемые алгоритмические проблемы теории групп. Это направление считается одним из перспективных для построения стойких постквантовых криптосистем. Однако в последнее время в качестве выбранной группы для построения криптографической системы, так называемой группы-платформы, используются конечные некоммутативные группы. При этом также ожидается постквантовая стойкость таких систем.

В данной статье рассмотрена задача поиска сопрягающего элемента и степени, на труднорешаемости которой основывается, например, стойкость криптосистемы в [2]. Получен ряд результатов, которые показывают, что во многих случаях эта задача может быть эффективно решена в квантовой модели вычислений для конечных некоммутативных групп. В частности, существует эффективный квантовый алгоритм решения этой задачи для группы-платформы из [2].

ЭФФЕКТИВНЫЕ АЛГОРИТМЫ В КВАНТОВОЙ МОДЕЛИ ВЫЧИСЛЕНИЙ

Квантовая модель вычислений не предоставляет приниципиально новых вычислимых функций, но некоторые задачи в ней можно решить быстрее, чем в классической модели. На данный момент практически все известные качественно более эффективные квантовые алгоритмы можно описать с помощью задачи о скрытой подгруппе.

Задача 1 (задача о скрытой подгруппе). Пусть заданы множество образующих элементов группы G, некоторое конечное множество S и функция $f : G \to S$ с дополнительным условием: существует такая подгруппа $H \subseteq G$, что для

$\forall g_1, g_2 \in G$ выполняется равенство $f(g_1) = f(g_2)$ тогда и только тогда, когда $g_1 H = g_2 H$. Необходимо найти множество образующих элементов подгруппы H, используя вычисления функции f.

Главным заданием квантовой модели вычислений при решении задачи о скрытой подгруппе является уменьшение сложности до некоторого полинома от величины $O(\log |G|)$, которую принято считать размером входных данных для этой задачи, с учетом количества вычислений функции и любой классической обработки результатов измерения квантового состояния. Такой полиномиально ограниченный по ресурсам квантовый алгоритм будем называть эффективным.

Утверждение 1 [3]. Если функция f эффективно вычислима в классической модели вычислений, а группа G — абелева, то в квантовой модели вычислений существует эффективный алгоритм получения образующих элементов скрытой подгруппы H.

В данной работе доказано существование эффективного алгоритма в квантовой модели вычислений решения некоторой задачи исключительно методом ее сведения к абелевому случаю задачи о скрытой подгруппе.

ЧАСТНЫЕ РЕШЕНИЯ ЗАДАЧИ ПОИСКА СОПРЯГАЮЩЕГО ЭЛЕМЕНТА И СТЕПЕНИ

Для анализа задачи поиска сопрягающего элемента и степени воспользуемся ее описанием из [2]. Пусть заданы конечная некоммутативная группа G, а также элементы $R, Q \in G$ с известными достаточно большими простыми порядками r и q соответственно. Дополнительным требованием является условие, что $RQR^{-1}Q \neq QRQR^{-1}$, и известен элемент $Y = R^w Q^x R^{-w}$ для некоторых значений $0 \le w < r$ и $1 < x < q$. Искомым значением является пара значений (w, x). Именно такая постановка задачи поиска сопрягающего элемента и степени будет предметом исследования данной работы.

Сначала покажем, что в квантовой модели вычислений имеет эффективное решение обобщенная в некотором смысле задача дискретного логарифмирования.

Теорема 1. Пусть задан элемент $A \in G$ с известным порядком a и известен такой элемент $B \in G$, что $A^n B \neq BA^n$ для любого значения $n \in Z_a$, $n \neq 0$. Тогда существует эффективный квантовый алгоритм, который по заданному значению $K = A^x Z$, где $x \in Z_a$ — неизвестное значение, а Z — неизвестный элемент из пересечения $Z_G(A) \cap Z_G(B)$, может восстановить значение x и элемент Z.

Используя теорему 1, несложно доказать справедливость следующего утверждения.

Утверждение 2. Дополнительно известный элемент Q^x или R^w позволяет эффективно вычислить искомую пару значений (w, x) в квантовой модели вычислений.

Рассмотрим дополнительное условие, которое позволяет эффективно решить задачу поиска сопрягающего элемента и степени.

Теорема 2. Пусть для любого элемента $W \in Z_G(R)$ из соотношения $[WQW^{-1}, Q] = 1$ следует, что $W \in Z_G(Q)$. Любое решение системы $[XY, R] = 1$ $[X^{-1}YX, Q] = 1$ позволяет эффективно найти искомую пару значений (w, x) в квантовой модели вычислений.

Группа-платформа из [2] — группа обратимых элементов обобщенной алгебры кватернионов над полем $GF(p)$, удовлетворяет условию теоремы 2. Соответствующая система соотношений эквивалентна системе квадратичных сравнений по модулю p. Таким образом, согласно теореме 2 криптопримитив из [2] не может быть стойким в квантовой модели вычислений. Этот же вывод получен в [4], но с помощью дополнительных особенностей выбранной группы-платфор-

мы. Используя групповую операцию, несложно вычислить элемент $Y^k = R^w Q^{xk} R^{-w}$ для любого $k \in Z_q$. Но если существует метод получения, например, значения $Y^x = R^w Q^{x^2} R^{-w}$, не зная самого значения x, то это тоже позволяет эффективно решить задачу поиска сопрягающего элемента и степени.

Теорема 3. Существует эффективный квантовый алгоритм, который по известным элементам $Y_k = R^w Q^{x^k} R^{-w}$, $Y_l = R^w Q^{x^l} R^{-w}$ и известному значению $l-k$ ($k, l \in Z_q^*$ — неизвестные значения) вычисляет неизвестные значения $w \in Z_r$ и $x \in Z_q^*$ при условии, что $Y_k \neq Y_l$ и $GCD(l-k, q-1) = 1$.

Следствие. Для эффективного алгоритма вычисления значений $w \in Z_r$ и $x \in Z_q^*$ в квантовой модели вычислений по известным элементам R, Q и $Y = R^w Q^x R^{-w}$ достаточно знать элемент $Y = R^w Q^{x^2} R^{-w}$.

ЗАКЛЮЧЕНИЕ

В настоящей работе показаны эффективные частные решения задачи поиска сопрягающего элемента и степени, а также эффективное решение обобщенной задачи дискретного логарифмирования в квантовой модели вычислений путем сведения к абелевому случаю задачи о скрытой подгруппе. Полученные решения подтверждают отсутствие постквантовой стойкости у некоторых криптопримитивов на основе задачи поиска сопрягающего элемента и степени, таких как в [2 и 5].

СПИСОК ЛИТЕРАТУРЫ

1. Myasnikov A., Shpilrain V., Ushakov A. Group-based cryptography. — Advances courses in Math. — CRM, Barselona. — Basel; Berlin; New York: Birkhauser Verlag, 2008. — 183 p.
2. Moldovyan D.N., Moldovyan N.A. A new hard problem over non-commutative finite groups for cryptographic protocols // Lecture Notes in Comput. Sci. — 2010. — **6258**. — P. 183–194.
3. Kitaev A. Quantum computations: algorithms and error correction // Rus. Mathemat. Surveys. — 1997. — **52**, N 6. — P. 53–112.
4. Фесенко А.В. Оценка стойкости коммутативного криптопримитива, построенного на некоммутативной группе обратимых многомерных векторов // Кибернетика и вычисл. техника. — 2011. — Вып. 165. — С. 47–62.
5. Kahrobaei D., Khan B. A non-commutative generalization of ElGamal key exchange using polycyclic groups // Global Telecom. Conf. — 2006, GLOBECOM'06, IEEE. — P. 1–5.

Поступила 06.05.2014