Ерохин А.Г. Разработка симулятора квантового алгоритма Шора для демонстрации этапов криптоанализа криптосистем с открытым ключом // Международный журнал информационных технологий и энергоэффективности.– 2024. –Т. 9 № 8(46) с. 25–30

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

РАЗРАБОТКА СИМУЛЯТОРА КВАНТОВОГО АЛГОРИТМА ШОРА ДЛЯ ДЕМОНСТРАЦИИ ЭТАПОВ КРИПТОАНАЛИЗА КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ

Ерохин А.Г.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: erokhin_anton@lenta.ru

В статье рассматривается квантовый алгоритм дискретного логарифмирования Шора и программа, моделирующая его работу. Алгоритм разделён на этапы, каждый из которых подробно описан. Симулятор выполняет эти этапы и отображает состояния квантовых регистров, что обеспечивает понятное и наглядное изучение алгоритма Шора. Сделан вывод о перспективах разработанного симулятора для криптоанализа систем с открытым ключом.

Ключевые слова: Квантовые вычисления, алгоритм Шора, дискретное логарифмирование, криптосистема с открытым ключом, криптоанализ.

DEVELOPMENT OF A SIMULATOR OF THE QUANTUM SHORE ALGORITHM TO DEMONSTRATE THE STAGES OF CRYPTANALYSIS PUBLIC KEY CRYPTOSYSTEMS

Erokhin A.G.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: erokhin_anton@lenta.ru

The article discusses the quantum algorithm of discrete logarithm of Shore and the program that simulates its operation. The algorithm is divided into stages, each of which is described in detail. The simulator performs these steps and displays the states of the quantum registers, which provides a clear and visual study of the Shore algorithm. The conclusion is made about the prospects of the developed simulator for cryptanalysis of public key systems.

Keywords: Quantum computing, Shor's algorithm, discrete logarithm, public key cryptosystem, cryptanalysis.

В современном мире обеспечение конфиденциальности и целостности информации имеет ключевое значение, поэтому криптографические алгоритмы должна обеспечивать достаточный уровень защищённости данных. [1] На сегодняшний день наиболее перспективными являются криптосистемы с открытым ключом, вычислительная стойкость которых основана на использовании односторонних функций. Однако дальнейшее развитие квантовых технологий может привести к практической непригодности некоторых криптосистем для долговременной защиты информации.

Дискретное логарифмирование в криптографии

Задача дискретного логарифмирования представляет собой одну из основных задач, на которых строятся криптосистемы с открытым ключом. В общем виде, дискретное логарифмирование – это обращение функции g^t в мультипликативной группе конечного поля. Пусть задано уравнение:

$$x = g^t \ mod \ p, \tag{1}$$

где g и x – целое неотрицательно число, p – простое число.

Решением задачи дискретного логарифмирования является нахождение целого числа t, в соответствии с формулой (1).

Известны алгоритмы решения этой задачи, однако для достаточно больших значений p они все являются непригодны, так как имеют экспоненциальную (субэкспоненциальную) сложность. В связи с этим можно считать показательную функцию односторонней. Проблема вычисления дискретного логарифмирования используется в качестве основы криптосистем с открытым ключом Диффи-Хеллмана, Эль-Гамаля, Мэсси-Омуры.

Квантовый алгоритм Шора

На данный момент наиболее перспективным алгоритмом нахождения дискретного логарифма является алгоритм [2] Шора, использующий квантовые вычисления. Теоретически доказано, что с его помощью можно вычислить дискретный логарифм за полиномиальное время. Для реализации алгоритма необходимо использовать три квантовых регистра, два из которых содержат значения аргументов, а третий – значения функции. Схема алгоритма представлена на Рисунке 1.

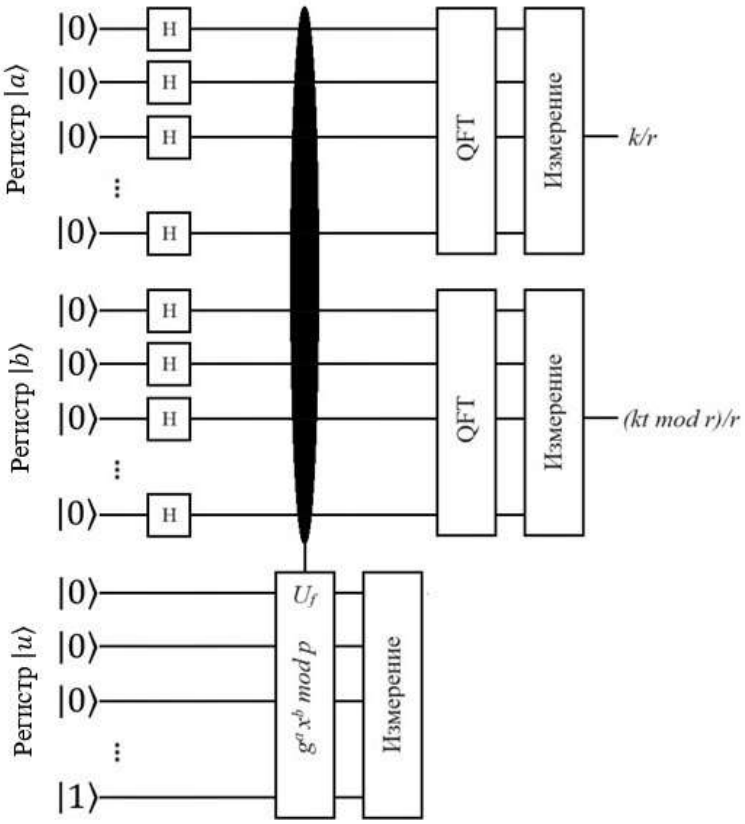

Рисунок 1. - Схема алгоритма Шора

Реализацию алгоритма можно разделить на следующие этапы:

1. Инициализация квантовых регистров;
2. Установка равновероятной суперпозиции возможных состояний регистров $|a\rangle$ и $|b\rangle$;
3. Квантовое возведение в степень;
4. Измерение значения функции в регистре $|u\rangle$;
5. Обратное квантовое преобразование Фурье;
6. Измерение состояния регистров;
7. Постквантовая обработка.

В результате выполнения алгоритма будет получено значение дискретного логарифма. Более подробно рассмотрим каждый этап квантовой части алгоритма.[3]

Два n-кубитовых регистра $|a\rangle$ и $|b\rangle$ установить в состояние $|0\rangle = |000 \dots 0\rangle$. Регистр $|u\rangle$ (такой же размерности) установить в состояние $|1\rangle = |000 \dots 1\rangle$. В результате состояние регистров примет вид:

$$|0\rangle|0\rangle|1\rangle. \tag{2}$$

К кубитам регистров $|a\rangle$ и $|b\rangle$ применяется преобразование Адамара. В результате получаем равновероятные суперпозиции всех возможных состояний. Состояние, описанное формулой (2), переход в состояние:

$$|0\rangle|0\rangle|1\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} \sum_{b=0}^{2^n-1} |a\rangle|b\rangle|1\rangle\,. \tag{3}$$

Полученные суперпозиции управляют оператором U_f, где вычисляются значения функции $g^a x^b \bmod p$ сразу для всех a и b. [4] Результаты вычислений записываются в регистр $|u\rangle$. В результате состояние регистров, описанное формулой (3), примет вид:

$$\frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} \sum_{b=0}^{2^n-1} |a\rangle|b\rangle|1\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} \sum_{b=0}^{2^n-1} |a\rangle|b\rangle|g^a x^b \bmod p\rangle\,. \tag{4}$$

Измеряется $|u\rangle$. Ввиду того что функция $g^a x^b \bmod p$ – периодическая и имеет два независимых периода, получаем периодическую суперпозицию состояний регистров a и b, удовлетворяющих измеренному значению u. Состояние, описанное формулой (4), переход в состояние вида:

$$\frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} \sum_{b=0}^{2^n-1} |a\rangle|b\rangle|g^a x^b \bmod p\rangle \xrightarrow{measure\ |u\rangle} \frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} \sum_{b=0}^{2^n-1} |a\rangle|b\rangle|u\rangle. \tag{5}$$

Применяется обратное квантовое преобразование Фурье к последовательностям значений a и b одноимённых регистров, которые соответствуют фиксированному значению u (формула (5)). QFT^{-1} переводит состояние $|a\rangle|b\rangle$ в состояние:

$$|a\rangle|b\rangle \xrightarrow{QFT^{-1}} \frac{1}{\sqrt{2^n}} \sum_{c=0}^{2^n-1} \sum_{d=0}^{2^n-1} e^{\frac{-2\pi i(ac+bd)}{2^n}} |c\rangle|d\rangle . \quad (6)$$

Значения состояний c и d, сохраняются после преобразования, в соответствии с формулой (6), в регистрах a и b. Проводится измерение состояний регистров $|a\rangle$ и $|b\rangle$. В результате измерения регистров, полученные значения передаются на постквантовую обработку. [5] На этом выполнение квантового алгоритма Шора завершено.

Описание симулятора

Симулятор разработан с использованием языка программирования C++ и фреймворка для кроссплатформенной разработки Qt. На данный момент симулятор поддерживает работу на операционных системах семейства Windows и Astra Linux.

При запуске симулятора пользователь должен ввести исходные данные, для того чтобы начать выполнение алгоритма дискретного логарифмирования Шора. Здесь так же отображены параметры системы, процесс выполнения алгоритма и краткие теоретические сведения об алгоритме Шора.

После выполнения расчётов предусмотрена возможность переключения между окнами, каждое из которых представляет собой один этап выполнения. В случае, если введены некорректные данные, по которым невозможно вычислить дискретный логарифм, программа сообщит об этом.

На каждом этапе отображается краткий теоретический материал и представлены таблицы, показывающие возможные состояния квантовых регистров от 0 до 2^n-1, где n – число кубит. Пример такого окна приведён на Рисунке 2. Каждый квадрат соответствует одном из состояний регистра. Светлый квадрат свидетельствует, что это состояние активно.

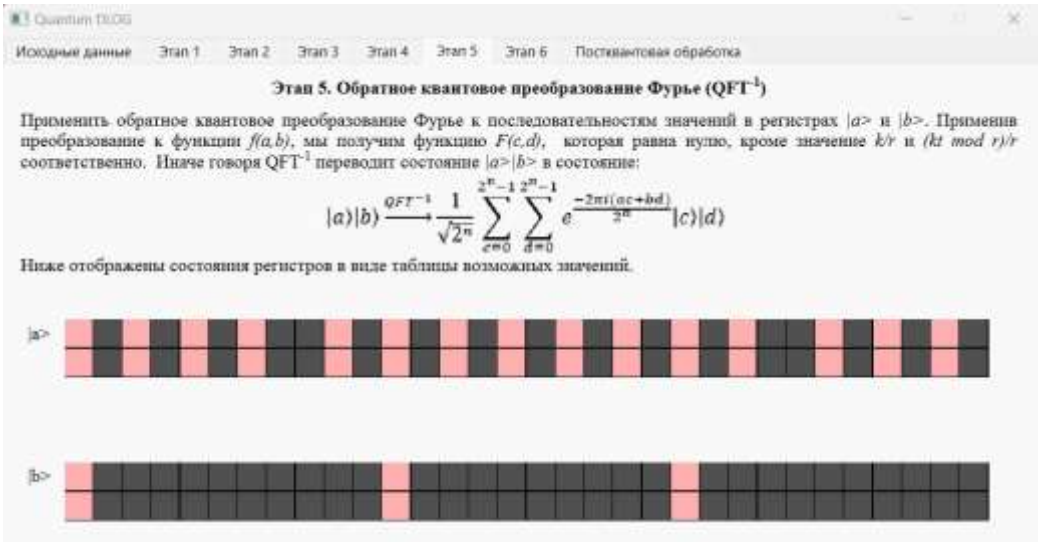

Рисунок 2. - Пример работы симулятора

После выполнения алгоритма должен быть получен результат вычисления дискретного логарифма вместе с проверкой правильности вычисления. Пример результата работы симулятора приведён на Рисунке 3. В случае если результат не был получен, не обходимо повторить выполнение алгоритма. Это связано с тем, что алгоритм имеет вероятностный характер.

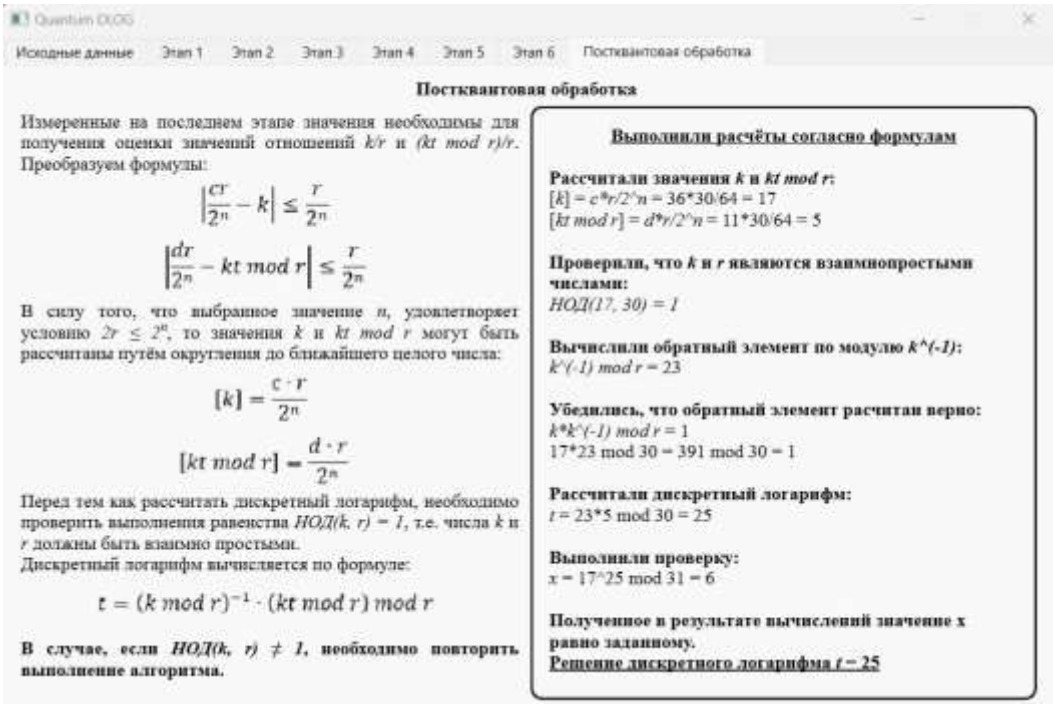

Рисунок 3. - Результат работы

Заключение

В статье проведено исследование квантового алгоритма дискретного логарифмирования Шора, с помощью которого можно показать, что криптосистемы, основанные на задаче дискретного логарифмирования, утратят свои функции к долговременной защите информации при дальнейшем развитии квантовых компьютеров.

Разработана программа-симулятор, демонстрирующая работу данного алгоритма. Данный симулятор предназначен для наглядного изучения алгоритма Шора в рамках криптоанализа криптосистем с открытым ключом, в основе которых лежит задача дискретного логарифмирования.

Список литературы

1. Кайе Ф., Лафламм Р., Моска М. Введение в квантовые вычисления – М. – Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований, 2009. – 360 с. ISBN 978-5-93972-766-2.
2. Коржик В. И., Яковлев В. А., Основы криптографии: учебное пособие – СПб., ИЦ Интермедия, 2016. – 296 с. ISBN 978-5-89160-097-3.
3. Нильсен М., Чанг И. квантовые вычисления и квантовая информация : Пер. с англ. – М. : Мир, 2006. – 824 с. ISBN 5-03-003524-9.
4. Сысоев С.С. Введение в квантовые вычисления. Квантовые алгоритмы : учебное пособие. СПб: Изд-во С.-Петерб. ун-та, 2019. – 144 с. ISBN 978- 5-288-05933-9.
5. *Shor P. W.* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a

Quantum Computer // Foundations of Computer Science : Conference Publications. 1997. С. 1484–1509.

References

1. Kaye F., Laflamme R., Mosca M. Introduction to quantum Computing – Moscow – Izhevsk: SIC "Regular and Chaotic Dynamics", Institute of Computer Research, 2009. – 360 p. ISBN 978-5-93972-766-2.
2. Korzhik V. I., Yakovlev V. A., Fundamentals of cryptography: textbook – St. Petersburg, IC Intermedia, 2016. – 296 p. ISBN 978-5-89160-097-3.
3. Nielsen M., Chang I. quantum computing and quantum information : Translated from English – M. : Mir, 2006. – 824 p. ISBN 5-03-003524-9.
4. Sysoev S.S. Introduction to quantum computing. Quantum algorithms : a textbook. St. Petersburg: Publishing House of St. Petersburg University, 2019. – 144 p. ISBN 978- 5-288-05933-9.
5. Shop P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithm on a Quantum Computer // Foundations of Computer Science : Conference Publications. 1997. pp. 1484-1509.