УДК 003.26

Неласая А.В., Сидоренко Т.С.
Запорожский национальный технический университет

Моделирование квантового алгоритма Шора факторизации натуральных чисел

Квантовая криптография является новым этапом в эволюции информационной защиты, основанным на законах квантовой физики. Каждый бит кода передается с помощью квантового состояния элементарной частицы света-фотона. Как известно, аксиома квантовой физики свидетельствует, что квантовое состояние невозможно измерить, не нарушив его. Таким образом, исключается попытка злоумышленника завладеть информацией, что выводит криптографию как науку на принципиально новый уровень.

Однако квантовая технология имеет и определенные недостатки: неустойчивость поляризации одиночного фотона (основное количество ошибок в сыром ключе наблюдается из-за потери поляризации фотонов после прохождения по информационному каналу); из-за неустойчивости поляризации системы данного типа ограничены длиной линии передачи; процесс исправления ошибок детектирования поляризации делает систему громоздкой и уменьшает ее скорость; низкая скорость существующей элементной базы лавинных фотодиодов и их низкая квантовая эффективность; сложные методики контроля поляризации, которые обычно не оправдывают себя, что приводит к увеличению ошибок в ключе.

Несмотря на трудности аппаратного воплощения квантовых технологий, корпорация IBM совсем недавно уже открыла тестовый доступ к своему облачного квантового компьютера, по их мнению, поможет исследователям всего мира работать над инновационными технологиями [1].

Авторами выполнено моделирование квантового алгоритма Шора факторизации натуральных чисел[2] с помощью специализированного математического пакета. Квантовый алгоритм Шора сводит задачу разложения на множители к нахождению периода некоторой функции. Алгоритм Шора, при выполнении на квантовом компьютере, способен был бы произвести факторизацию числа за полиномиальное время, не намного превосходящее время умножения целых чисел.

Привлекательность исследований в области квантовых компьютеров обеспечивается естественным параллелизмом таких вычислений, который можно смоделировать на современных массивно - параллельных устройствах еще до использования реального квантового компьютера. Направления дальнейших исследований заключается в моделировании квантовых алгоритмов с использованием технологии CUDA в рамках парадигмы GPGPU.

Поскольку задача создания масштабируемого квантового компьютера еще не решена, актуальной является задача разработки программных моделей протоколов квантовой криптографии, что позволит исключить недостатки протоколов на этапе моделирования.

Список использованных источников

1. *IBM открыла доступ к своему облачному квантовому компьютеру [Електроний ресурс]: / Ольга Карпенко / Новости от 05.05.2016 — Название с титул. экрана, Режим доступа: http://ain.ua/2016/05/05/646763.*
2. *Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Text] / P.W. Shor // SIAM J.Sci.Statist.Comput. - 1997. - 26(5). – P. 1484 – 1509. Режим доступа: http://arxiv.org/pdf/quant-ph/9508027v2.*