УДК 004.056.55

Разработка алгоритма на основе одноразовой подписи Лэмпорта для защиты от квантовых атак

Бакшина С.А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – Таранов С.В. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. В настоящее время создание квантовых компьютеров становится все более реальным. Они способны решать задачи, которые не решают классическими компьютерами, что делает их потенциально мощными инструментами в различных областях. Однако, создание квантовых компьютеров также подвергает сомнению безопасность многих современных методов шифрования, так как они способны взламывать некоторые из них значительно быстрее. Поэтому существует необходимость в разработке новых методов шифрования, которые будут устойчивы к квантовым вычислениям. Одним из таких методов является использование одноразовой подписи Лэмпорта. Создание алгоритма на основе данной подписи представляется перспективным направлением для защиты информации от квантовых атак.

Основная часть. В работе был представлен анализ одноразовых подписей Лэмпорта, Винтерница и Меркла. Был проведен сравнительный анализ устойчивости данных подписей к таким атакам, как алгоритмов Шора и алгоритм Гровера. Далее был разработан алгоритм для защиты от квантовых атак. Данный алгоритм основывается на одноразовой подпись Лэмпорта, которая позволяет гарантировать целостность и подлинность данных при передаче, используя специальный ключ подписи, который может быть использован только один раз. Затем была реализована программа по данному алгоритму на языке программирования Python. Эффективность полученной программы была проверена с помощью различных тестов и сравнительного анализа результатов теста с аналогами.

Вывод. В работе был разработан алгоритм и его программная реализация, которая помогает решать проблему безопасности данных в условиях создания квантовых компьютеров. Были выделены преимущества и недостатки полученного алгоритма.

Список литературы

1. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on — IEEE, 1994. — P. 124–134.
2. L. Lamport. Constructing digital signatures from a one-way function. Technical Report CSL98, SRI International, Palo Alto, 1979.
3. S. Alboaie, Doina Cosovan, L. Chiorean, M. Vaida Lamport n-time signature scheme // IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), 2018.

Бакшина С.А. (автор)

Таранов С.В. (научный руководитель)