УДК 004.056.55

ЦИФРОВАЯ ПОДПИСЬ НА КВАНТОВОЗАЩИЩЕННЫХ КЛЮЧАХ

Грабовой М.Н.[1], Торопова Д. И.[1], Кузьмин С. В.[1]
Научный руководитель – канд. физико-математических. наук Егоров В. И.[1]
[1]Университет ИТМО
m.grab@inbox.ru

Введение

В последнее десятилетие КЦП находятся в стадии активных исследований раннего внедрения. Она представляет собой симбиоз традиционных механизмов цифровой подписи и методов квантовой криптографии, а именно квантового распределения ключей [1-2]. В связи с относительно недолгим сроком службы токенов цифровой подписи, риском появления квантового компьютера, способного взломать все наиболее распространенные методы шифрования, а также с проблемой распространения всех ныне существующих КЦП на большие расстояния, существует проблема, решение которой необходимо найти незамедлительно [3-4].

Основная часть

В работе предлагается масштабируемая архитектура квантовой цифровой подписи на квантово-защищенных ключах, преодолевающая ограничения по дальности за счет введения цепочки доверенных промежуточных опорных узлов. Ключевой особенностью подхода является вынос дорогостоящего оборудования квантового распределения ключей из клиентской инфраструктуры. Конечные пользователи оснащаются лишь модулями управления ключами, что существенно снижает порог внедрения технологии.

Протокол реализует трехстороннюю схему взаимодействия между подписантом, адресатом и доверенным проверяющим. Генерация ключевой информации осуществляется на опорных узлах сети, после чего ключи адресата и проверяющего доставляются подписанту в защищенном виде с применением квантово-распределенных ключей. Ключ подписанта формируется как сумма полученных ключей и используется для хеширования документа. Верификация выполняется проверяющим путем сверки хеш-кода при наличии обеих составляющих ключа.

Для демонстрации предложенного решения разработана программная модель, имитирующая полный цикл работы протокола: от распределения ключей до попытки компрометации канала связи нарушителем.

Предложенная схема обеспечивает информационно-теоретическую стойкость подписи, не требует от пользователей квантовых каналов связи и допускает наращивание географии обслуживания за счет увеличения числа промежуточных узлов без потери уровня безопасности.

Выводы

В работе предложена и детально описана новая схема реализации квантовой цифровой подписи на основе квантово-защищенных ключей.

Литература

1. Gostassistent.ru [Электронный ресурс] : ПНСТ 830-2023. Квантовые коммуникации. Термины и определения. URL: https://gostassistent.ru/doc/e1fcd84f-f26c-4d4a-b496-4d915da12288 (дата обращения: 20.03.2025)
2. Gostassistent.ru [Электронный ресурс] : ПНСТ 829-2023. Квантовые коммуникации. Общие положения. URL: https://gostassistent.ru/doc/373118a0-bc9a-4878-807c-c241ab432361 (дата обращения: 30.03.2025)

3. Gostassistent.ru [Электронный ресурс] : ПНСТ 832-2023. Квантовый интернет вещей. Термины и определения. URL: https://gostassistent.ru/doc/522ea051-19a7-459b-9e07-8a8b2ec621ae (дата обращения: 05.04.2025)
4. Gostassistent.ru [Электронный ресурс] : ПНСТ 831-2023. Квантовый интернет вещей. Общие положения. URL: https://gostassistent.ru/doc/e19bfb65-6254-47ed-9e21-a2f0c4b4e7a9 (дата обращения: 10.04.2025)