Квантовое шифрование. Квантовая передача информации

Основы информационной безопастности

Астраханцева А. А.

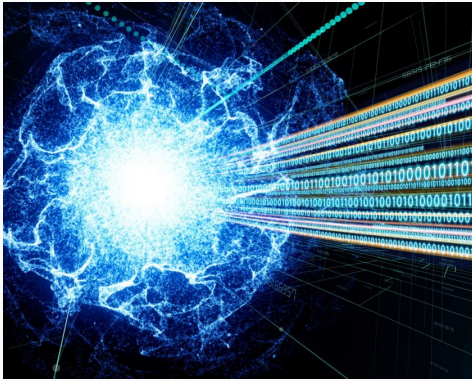
10 мая 2024

Российский университет дружбы народов, Москва, Россия

НКАбд-01-22

Введение

- Большое значение в цифровом мире
- Надежные методы защиты данных
- Перспективы в криптографии и безопасности
- Использование квантовых свойств частиц для криптографических протоколов
- Квантовая передача информации обеспечивает конфиденциальность



Основы квантового шифрования

Квантовая криптография - это метод обеспечения безопасности коммуникаций, использующий принципы квантовой физики. Идея защиты информации с помощью квантовых объектов впервые была предложена в 1970 году Стивеном Визнером, а затем развита Чарльзом Беннетом и Жилем Брассардом, которые создали первый протокол квантовой криптографии (BB84) в 1984 году.

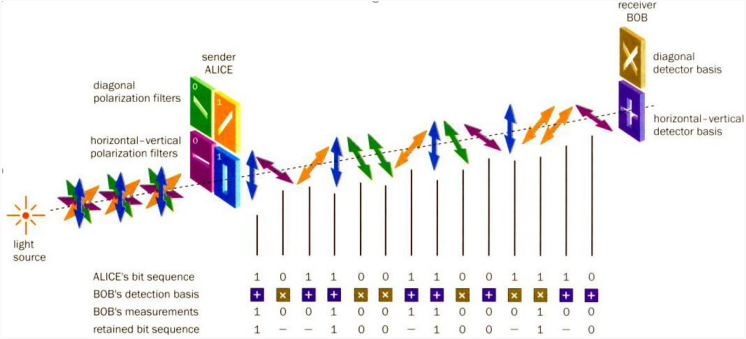
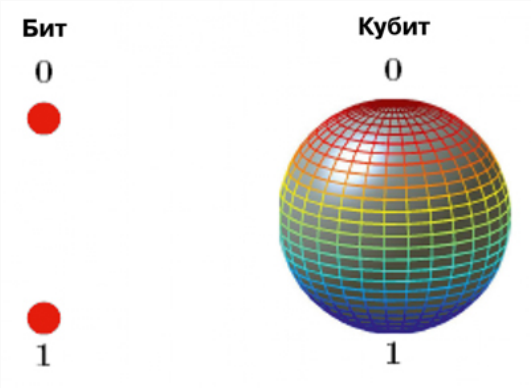


Схема реализации квантовой криптографии

Слева находится передающая сторона, а справа - принимающая. Свет из светоизлучающего диода направляется на коллиматорю. После коллиматора идут Ячейки Покеля, которые изменяют поляризацию фотонов в системе передачи данных. На принимающей стороне системы устанавливается кальцитовая призма, которая разделяет пучок на два фотодетектора для измерения ортогональных составляющих поляризации. Проблема с интенсивностью импульсов квантов возникает при их формировании, где оптимальное количество квантов в импульсе составляет около единицы для предотвращения перехвата информации.

Квантовая передача информации

- Квантовая телепортация - это процесс передачи состояния, а не конкретных объектов или энергии, основанный на квантовых свойствах частиц. Квантовая телепортация использует кубиты, базовые элементы передаваемого состояния, находящиеся в суперпозиции двух состояний. Эффект запутанности позволяет передать уникальные состояния с минимальным количеством информации.



Практические применения квантового шифрования

- Рынок квантовых технологий остается относительно небольшим, где одним из первых игроков стала компания ID Quantique. Тем не менее, компании как ID Quantique, так и российские учреждения, включая Российский Квантовый Центр (РКЦ), активно продвигают квантовые технологии, разрабатывая инновационные системы и проводя успешные эксперименты для обеспечения безопасности данных.

Заключение

- Квантовая передача информации позволяет создавать сети связи, устойчивые к взлому и помехам, обеспечивая безопасную коммуникацию на глобальном уровне.
- Квантовое шифрование имеет широкие перспективы применения в финансах, государственной безопасности и медицине.
- Дальнейшее развитие квантового шифрования и передачи информации является ключевой задачей для научного и технологического сообщества.
- Новые исследования и инновации в этой области позволят расширить возможности цифровой безопасности и коммуникаций.

Спасибо за внимание