Квантовая криптография

Выполнил студент магистратуры
Сёмов М.Н.
Научный руководитель,
д.ф.-м.н. профессор
Килин С.Я

Цели и задачи

- Демонстрация ненадежности классических криптографических систем, основанных на сложности.
- Создание криптосистем на новых базовых принципах, обеспечивающих абсолютную защищенность информации.
- Рассмотрение конкретных примеров передачи данных с использованием квантовых носителей.
- Внедрение новых технологий в современную практику.

Что же такое криптография?

Квантовая криптография – это раздел квантовой информатики, изучающий методы защиты информации путем использования квантовых носителей

Проблема защиты информации остро стоит в условиях приближения к информационному типу общества.

Свойства квантовых объектов, используемые в криптографии.

- Смешенные (суперпозиционные состояния)

$$|\psi\rangle = \sum_i \alpha_i |e_i\rangle$$

- Перепутанные состояния

$$|\psi\rangle \neq |\phi\rangle \otimes |\varphi\rangle$$

Протокол квантового распределения ключа Беннетта и Брасарда (BB84)

Случайные биты (Алиса)	0	1	1	0	1	1	0	0
Случайные базисы (А)	D	D	D	P	P	D	D	P
Поляризация фотонов	45	135	135	0	90	135	45	0
Случайные базисы (Б)	P	P	D	D	P	P	P	P
Полученные Бобом биты	0	0	1	1	1	0	0	0
Б сообщает базисы А	P	P	D	D	P	P	P	P
Алиса дает ответ	N	N	Y	N	Y	N	N	Y
Общий ключ А и Б	--	--	1	--	1	--	--	0

Протокол квантового распределения ключа Беннетта (B92)

- Тот же метод приготовления состояний, что и в BB84
- Используются два неортогональных состояния, например фотоны с поляризацией 45 и 90 соответствующие логическим 0 и 1
- Измерения проводятся с помощью POVM
- Велика вероятность нерезультативного измерения

Безусловная защищенность протоколов КРП

- Оценка уровня шума
- Маскировка перехвата под шум
- Различные типы перехватов
- Вторичная обработка ключа
- Усиление секретности
- Защита классического канала связи

Индивидуальный перехват

Метод промежуточного базиса

$$|\bar{0}\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$

$$|\bar{1}\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$$

Промежуточный базис

$$|\alpha\rangle = (|0\rangle + |\bar{0}\rangle)/\sqrt{2+\sqrt{2}}$$

$$|\beta\rangle = (|1\rangle + |\bar{1}\rangle)/\sqrt{2+\sqrt{2}}$$

Вероятности получения значений при использовании описанного метода

$$P(\beta \mid 0) = \left|\langle \beta \mid 0 \rangle\right|^2 = \left|1 / \sqrt{4+2\sqrt{2}}\right|^2 \equiv p \approx 0{,}1416$$

$$P(\alpha \mid 0) = \left|\langle \alpha \mid 0 \rangle\right|^2 = \left|(\sqrt{2}+1) / \sqrt{4+2\sqrt{2}}\right|^2 \equiv 1-p$$

$$P(\alpha \mid 1) = \left|\langle \alpha \mid 1 \rangle\right|^2 = \left|1 / \sqrt{4+2\sqrt{2}}\right|^2 \equiv p$$

$$P(\beta \mid 1) = \left|\langle \beta \mid 1 \rangle\right|^2 = \left|(\sqrt{2}+1) / \sqrt{4+2\sqrt{2}}\right|^2 \equiv 1-p$$

Другие методы индивидуальной атаки. Другие типы атак

- Метод случайного базиса
- Метод косвенной индивидуальной атаки

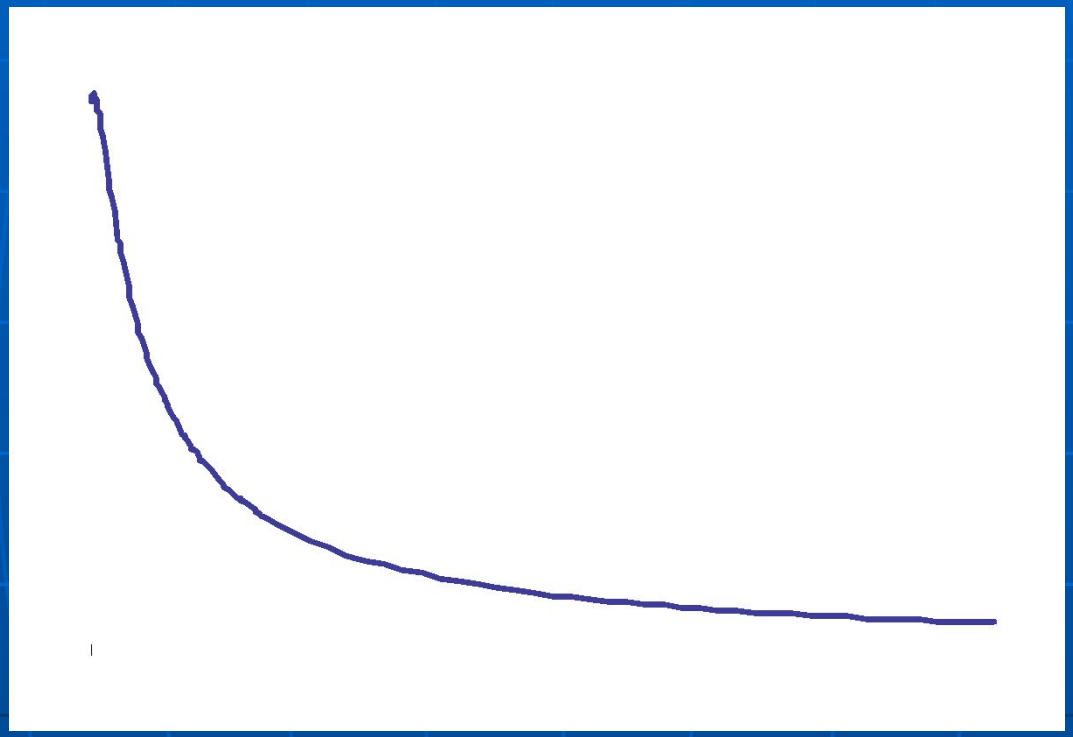
- Коллективный перехват
- Когерентный перехват

Минимизация взаимной информации нелегитимного пользователя

$$i_{CK} = 1 + \log_2 \frac{(1-p)^4 + p^4}{((1-p)^2 + p^2)^2} = 1 + \log_2 \frac{17}{18} \approx 0.9175$$

$$I_E(Q) = \frac{Q}{1-Q} \frac{1-p_{err}}{p_{err}} i_{CK}$$

График зависимости взаимной информации от уровня шума



Результаты:

- Изучены протоколы квантового распределения ключа и вопрос их защищенности от прослушивания
- На примере протокола BB84 показана безусловная защищенность протоколов КРК
- Рассчитана взаимная информация между легитимными пользователями и взломщиком для различных типов атак
- Получена функциональная зависимость взаимной информации от уровня шума, создаваемого перехватом
- Минимизирована взаимная информация

Литература:

- http://msiomau.narod.ru
- http://prola.aps.org

- Килин, С.Я. Квантовая криптография / С.Я.Килин, Д.Б. Хорошко, А.П.Низовцев // Минск: «Белорусская наука», 2007.
- Килин С.Я. Квантовая информация / С.Я.Килин // УФН. – 1999. – Т.169. – с.507.

Спасибо за внимание!