СМАРТС
КВАНТТЕЛЕКОМ

Исследование уязвимостей систем квантового распределения ключа

Козубов Антон Владимирович,
Начальник отдела перспективных исследований и разработок

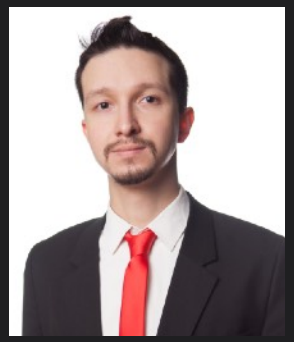
«Самые смертельные ошибки проистекают из устаревших допущений»
Ф. Герберт, Дети Дюны

Команда

СМАРТС КВАНТТЕЛЕКОМ

Козубов А.В.

Гайдаш А.А.



Нурыев Р.К.

ИТМО

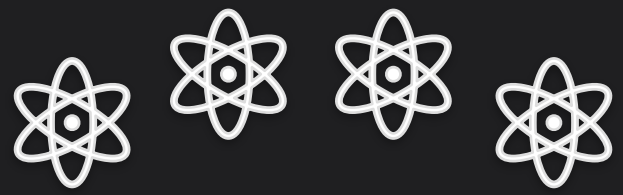
Смирнов С.В.

Халтуринский А.К

МИАН

Атаки на системы КРК

СМАРТС КВАНТТЕЛЕКОМ



Атаки на квантовые состояния

Атаки на техническую реализацию

Комбинированные атаки

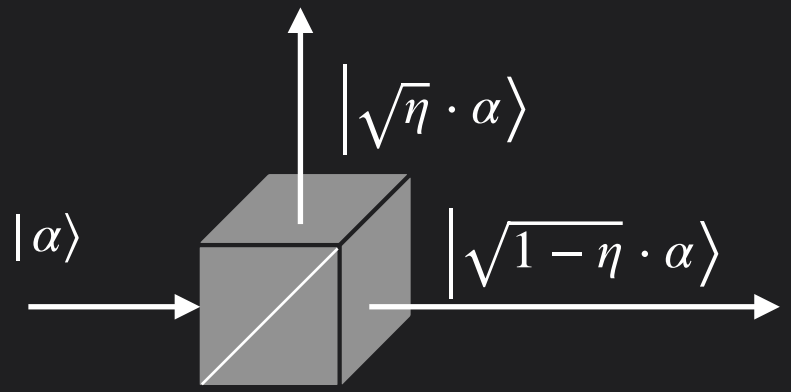
Типы атак

СМАРТС КВАНТТЕЛЕКОМ

Пассивные атаки

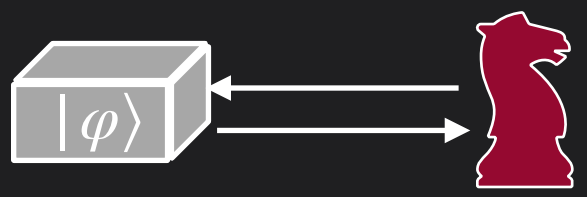
Атака на протокол КРК

Атака со светоделителем

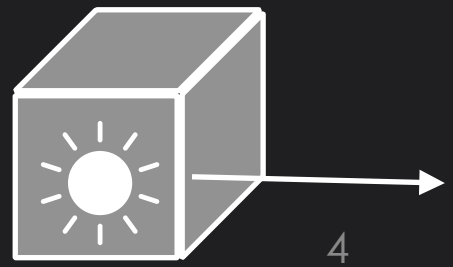


Атака на техническую реализацию

Троянский конь



Переизлучение детектора



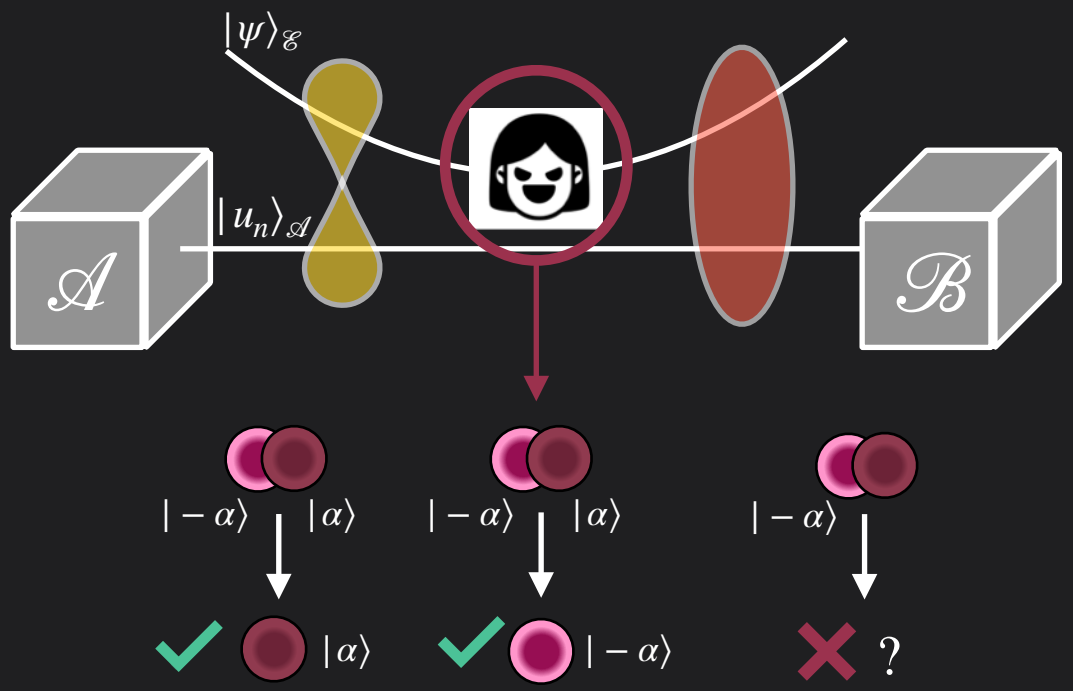
Типы атак

СМАРТС КВАНТТЕЛЕКОМ

Активные атаки

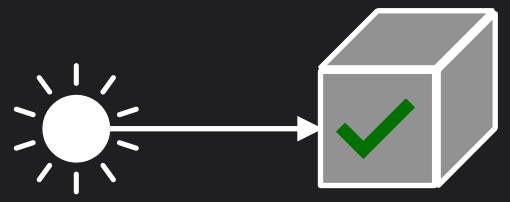
Атака на протокол КРК

Атаки с постселекцией

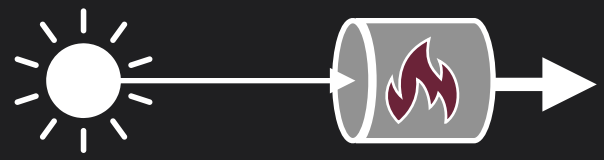


Атака на техническую реализацию

Управление детектором



Лазерное повреждение



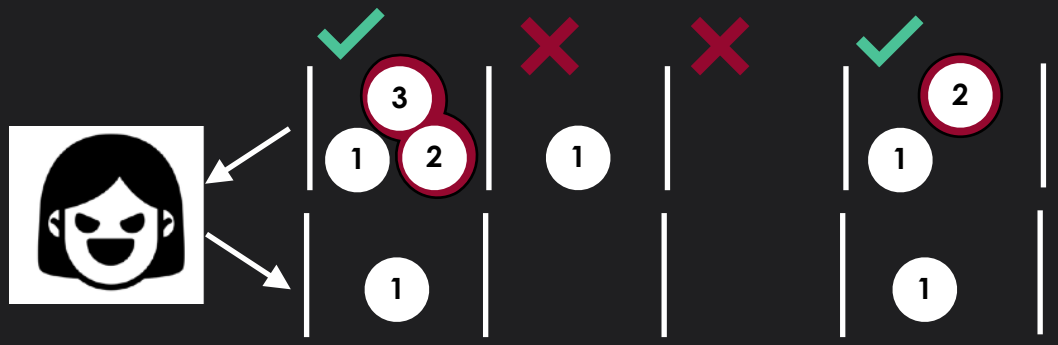
Типы атак

СМАРТС КВАНТТЕЛЕКОМ

Смешанные атаки

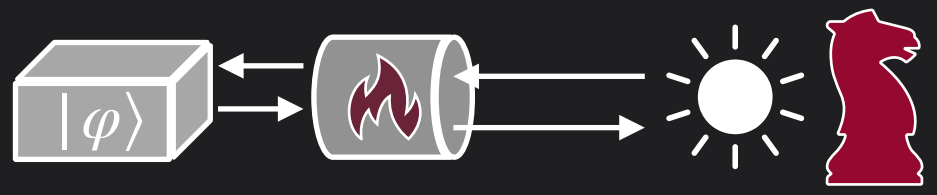
Атака на протокол КРК

Атака с разделением числа фотонов



Атака на техническую реализацию

Лазерное повреждение +
Троянский конь



Критерии успешной атаки

СМАРТС КВАНТТЕЛЕКОМ

Успешная стратегия нарушителя

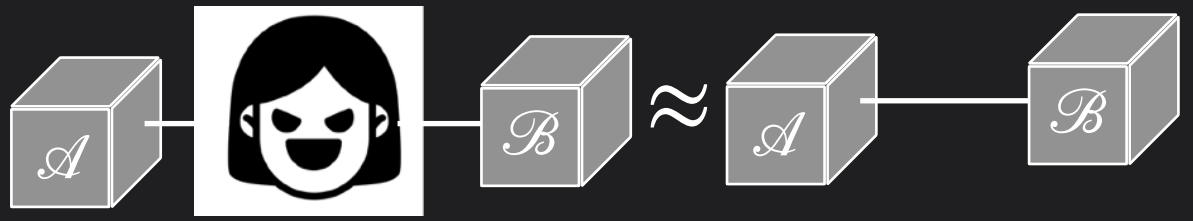
Информационное превосходство

$$A \to E \to B,$$

$$I(A;E) \geq I(A;B),$$

$$I(X;Y) = H(X) - H(X|Y)\,.$$

Сохранение статистики



$$\sum_{b\neq 0} \mathscr{P}(b|a) \leq \sum_{b\neq 0} \tilde{\mathscr{P}}^{\mathscr{E}}(b|a),$$

$$\sum_{b\neq a,0} \mathscr{P}(b|a) \geq \sum_{b\neq a,0} \tilde{\mathscr{P}}^{\mathscr{E}}(b|a),$$

Пример реализации атаки с постселекцией

СМАРТС КВАНТТЕЛЕКОМ

Вероятность успешного различения без ошибок

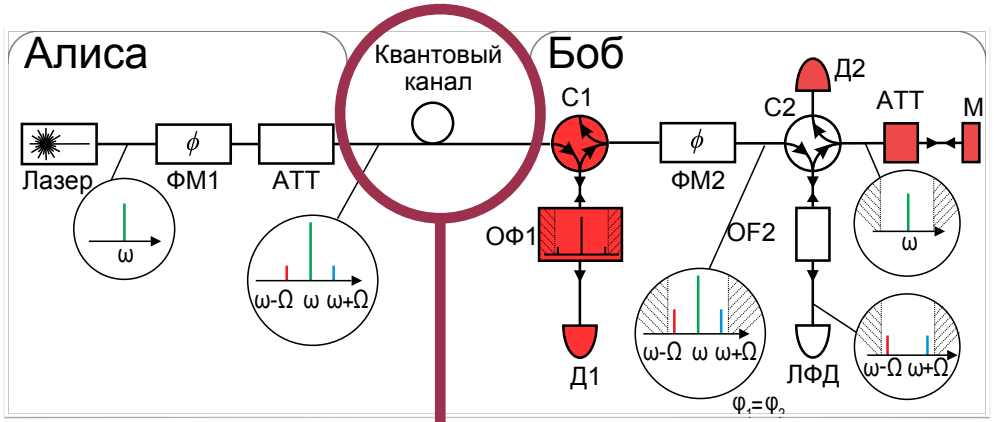
$$P_U \approx \frac{2N}{(2N-1)!}(|\alpha|^2)^{2N-1}.$$

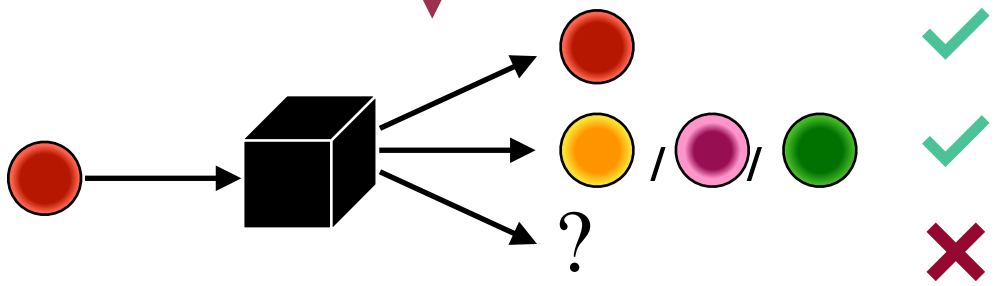
Вероятность определенного результата

$$P = \sum_n \tilde{P}^{\mathscr{E}}(n|n) + \sum_{m \neq n,0} \tilde{P}^{\mathscr{E}}(m|n)$$

Режими навязывания

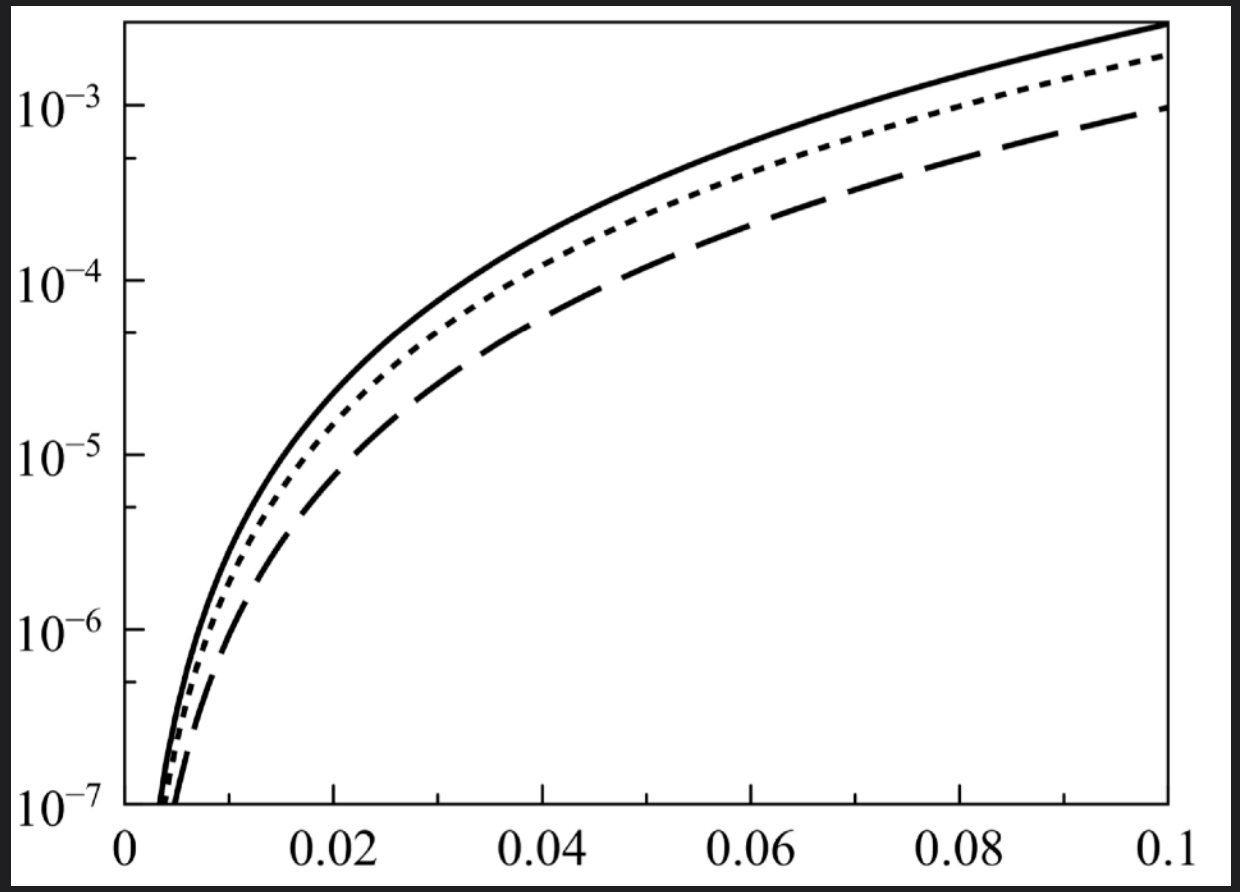
- Срабатывает всегда, кроме $\Delta\varphi = \pm\pi$
- Вероятность срабатывания соотносится с разностью фаз
- Срабатывает только в случае $\Delta\varphi = 0$





Пример реализации атаки с постселекцией

СМАРТС КВАНТТЕЛЕКОМ



Зависимость вероятности срабатывания детектора от режима навязывания

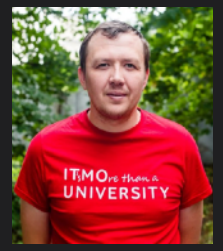
- Сплошная линия соответсвует срабатывания всегда, кроме $\Delta\varphi = \pm\pi$
- Точечная линия соответсвует срабатываниям, соотносящимся с разностью фаз
- Пунктирная линия соответсвует срабатываниям только в случае $\Delta\varphi = 0$

Троянский конь + Атака общего вида

СМАРТС КВАНТТЕЛЕКОМ

QPM Lab ITMO UNIVERSITY





Наседкин Б.А. Исмагилов А.О. Цыпкин А.Н.

$$\tilde{\chi} = \chi(\mu) + (1 - \chi(\mu)) \cdot \chi(\mu_{THA}) + \\ + (1 - \chi(\mu)) \cdot \chi(\mu_{THB}) .$$

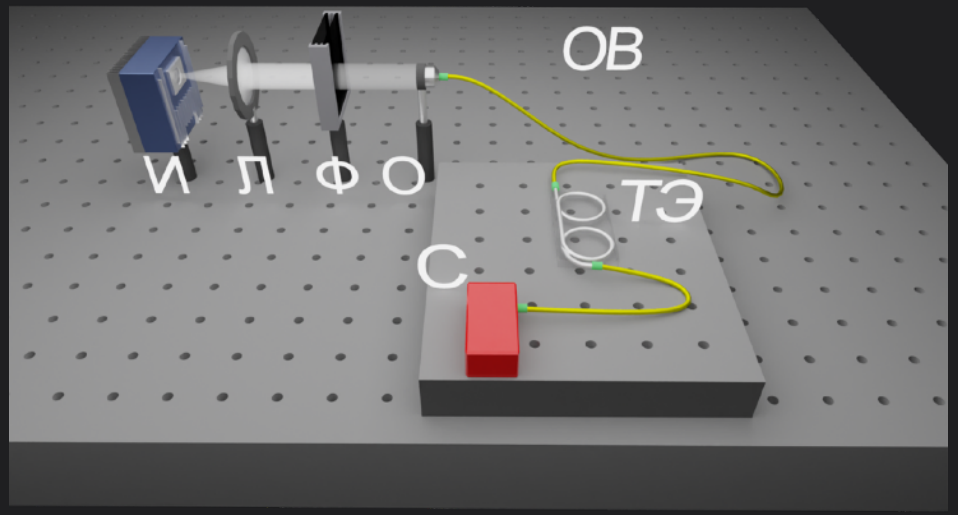
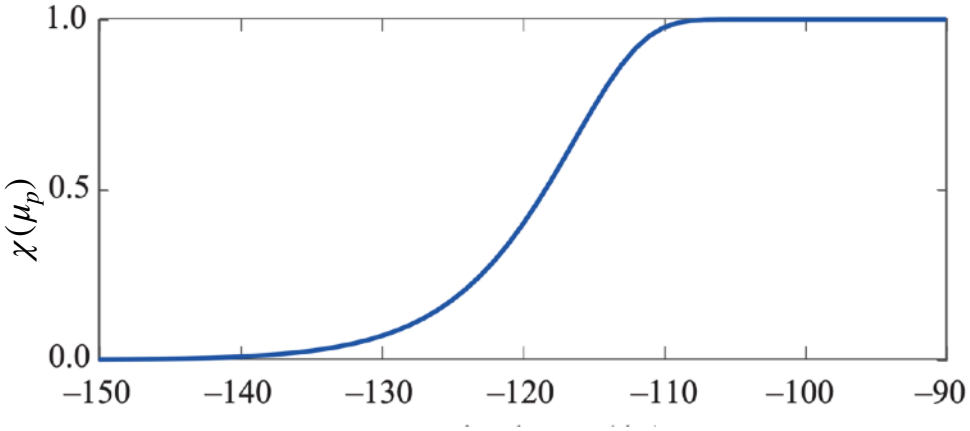


Схема экспериментальной установки для измерения пропускания волоконно-оптических элементов.

И – широкополосный источник оптического излучения, Л – линза, Ф – светофильтры, О – микрообъектив, установленный на трёхкоординатную подвижку, ОВ – одномодовое оптическое волокно, ТЭ - исследуемый волоконно-оптический элемент, С – спектрометр



Вносимые потери, дБ

Характеристики классов атак

СМАРТС КВАНТТЕЛЕКОМ

Пассивные атаки

Плюсы

- Сохраняют статистику
- Используют общее унитарное преобразование

Минусы

- При правильных контрмерах не дают информационного преимущество

Активные атаки

Плюсы

- Дают информационное преимущество
- Позволяют управлять характеристиками приборов

Минусы

- При правильных контрмерах не дают возможности сохранять статистику

Смешанные атаки

Плюсы

- Дают информационное преимущество
- Позволяют управлять характеристиками приборов
- Дают потенциальную возможность сохранять статистику

Подходы к организации контрмер

СМАРТС КВАНТТЕЛЕКОМ

Пассивные атаки

- Учет атак с квантовой памятью и общих унитарных атак
- Пассивные контрмеры при конструировании прибора
- Активные контрмеры (фотодиоды, датчики температуры)

Активные атаки

- Учет атак с постселекцией
- Активные контрмеры (фотодиоды, датчики температуры)
- Алгоритмические способы оценки статистики детектирования

Смешанные атаки

- Учет атак с постселекцией
- Учет атак с квантовой памятью и общих унитарных атак
- Активные контрмеры (фотодиоды, датчики температуры)
- Пассивные контрмеры при конструировании прибора
- Алгоритмические способы оценки статистики детектирования

СМАРТС
КВАНТТЕЛЕКОМ

Спасибо за внимание!

квanттелеком.рф