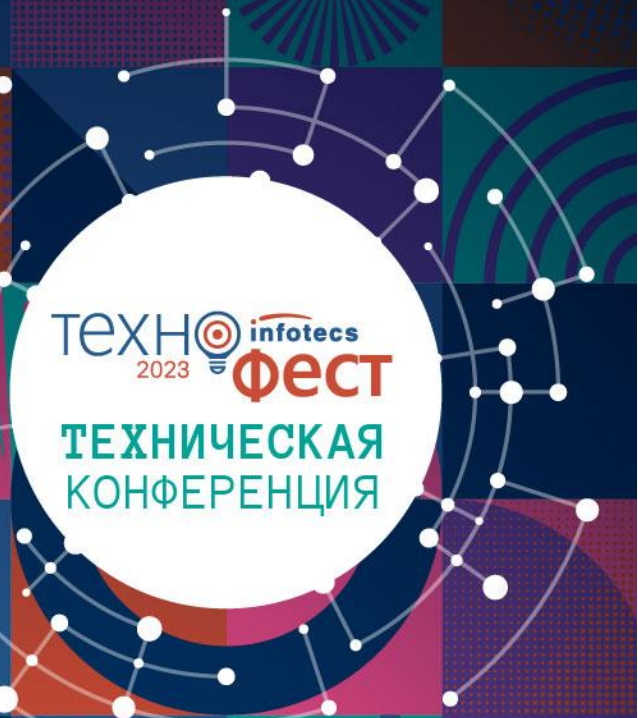
Границы утечки информации при атаке «Trojan Horse» на системы квантового распределения ключей



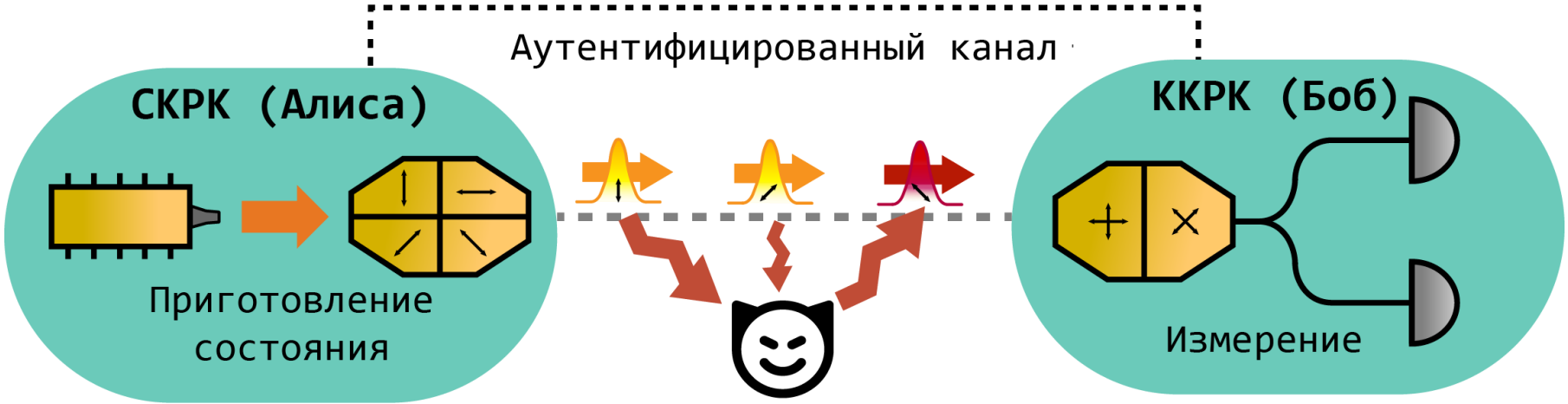
Сущев Иван Сергеевич
Ведущий специалист

Инженерно-квантовая лаборатория ООО «СФБ Лаб»

Квантовое распределение ключей

Безопасность протокола обеспечивается законами квантовой физики

Квантовое распределение ключей



Атака на квантовые состояния приводит к их возмущению. Наблюдается рост ошибочных срабатываний

Квантовое распределение ключей

Атаки на техническую реализацию

Из-за неидеальной реализации система КРК может быть подвержена атакам

Побочные каналы

- Trojan Horse
- Backflash
- Радиоизлучение

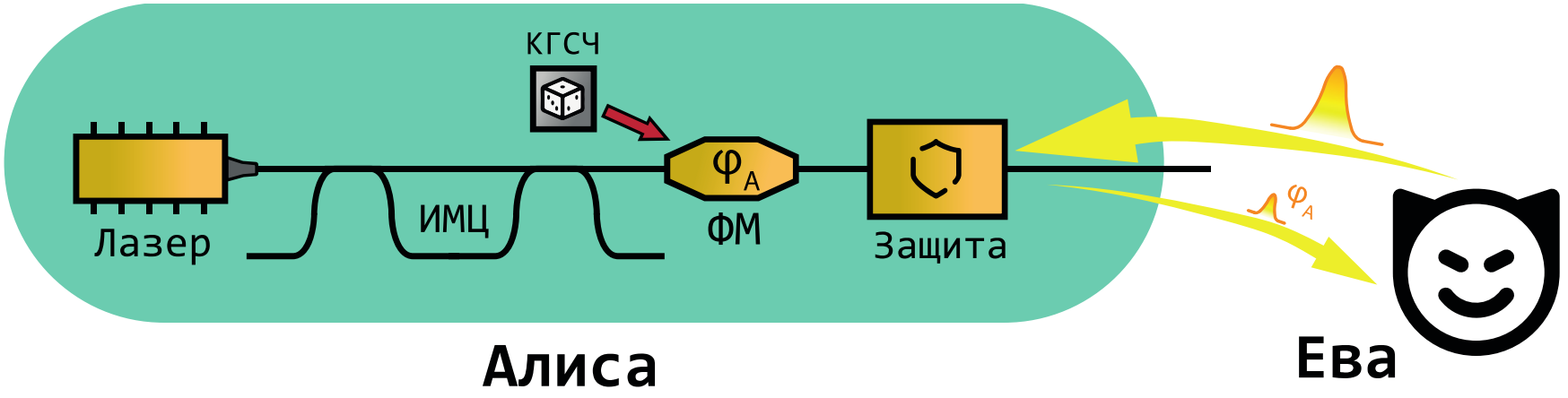
Навязывание

- Detector Blinding
- After-Gate
- Detector Efficiency Mismatch

Изменение свойств системы

- Laser Damage
- Laser Seeding

Атака «Trojan Horse»



Ева вводит мощное излучение внутрь системы и проводит измерения над отраженным сигналом

История

1999-2002

- Идея атаки
- Первые попытки анализа

[Makarov, 2001]

2006

- Вероятность успеха атаки зависит от μ основной инструмент

[Gisin, 2006]

2015

- Максимальная мощность зондирования)
- Аппарат теории информации
- Оптимальная стратегия атаки

[Shields, 2015]

2014-2017

- Проведение атаки на систему IDQ Clavis2 на 1550 нм и 1924 нм
- Необходимость спектральных измерений

[Makarov, 2014/17]

2020

- Спектры пропускания в ограниченном динамическом и спектральном диапазоне

[Borisova, 2020]

История

- Строгое доказательство секретности при наличии побочных каналов

2020

[Molotkov, 2020]

- Полный экспериментальный анализ атаки
- Применение к реальной системе КРК
- Измерения в максимально широком спектральном и динамическом диапазоне

2021

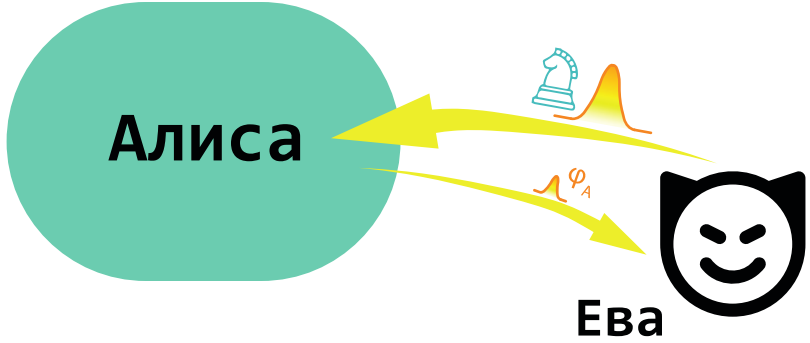
[Sushchev, 2021]

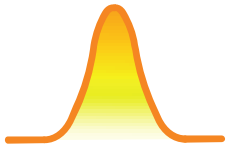
- Абсолютная граница утечки информации при атаке «Trojan Horse»

2023

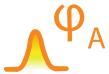
Атака «Trojan Horse»

- Ева генерирует световой импульс мощностью P_{Eve}
- Импульс претерпевает потери отражается
- Среднее число фотонов в отраженном импульсе: μ_{Eve}



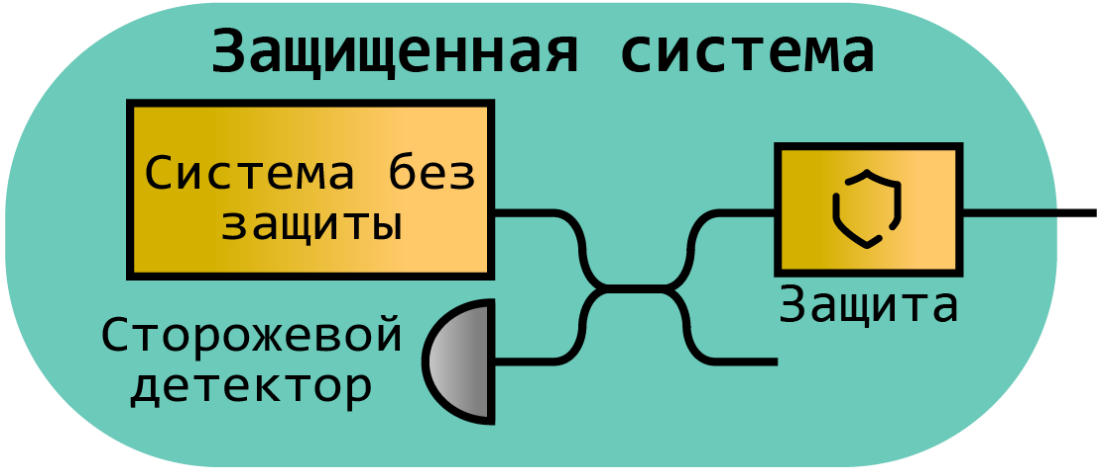


входной импульс



отраженный импульс с наложенной фазой

Защита от «Trojan Horse»



Алиса

Защита понижает уровень отраженного сигнала

Элементы защиты

Утечка информации

- Мощность отраженного сигнала можно **измерить** и оценить μ_{Eve}
- Величину утечки информации можно **вычислить,** зная μ_{Eve}
- Долю доступной Еве информации можно **свести к нулю** при **усилении секретности**

Длина секретного ключа:

$$\ell = 1 - \chi(\epsilon\eta) - h(Q)$$

$$\eta = \eta(\mu_{Eve})$$

Анализ защищенности

Необходимо измерить 3 физических параметра
Их достаточно для оценки μ_{Eve}

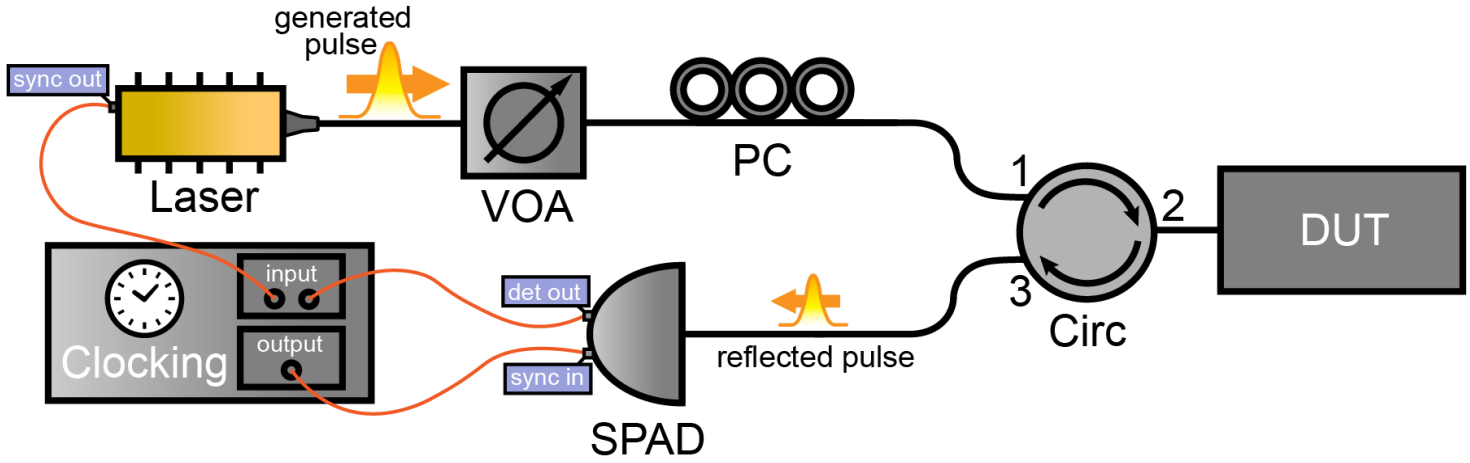
P_{max} – мощность при атаке с лазерным повреждением (Laser Damage attack)

R – величина максимального пика отражения внутри системы

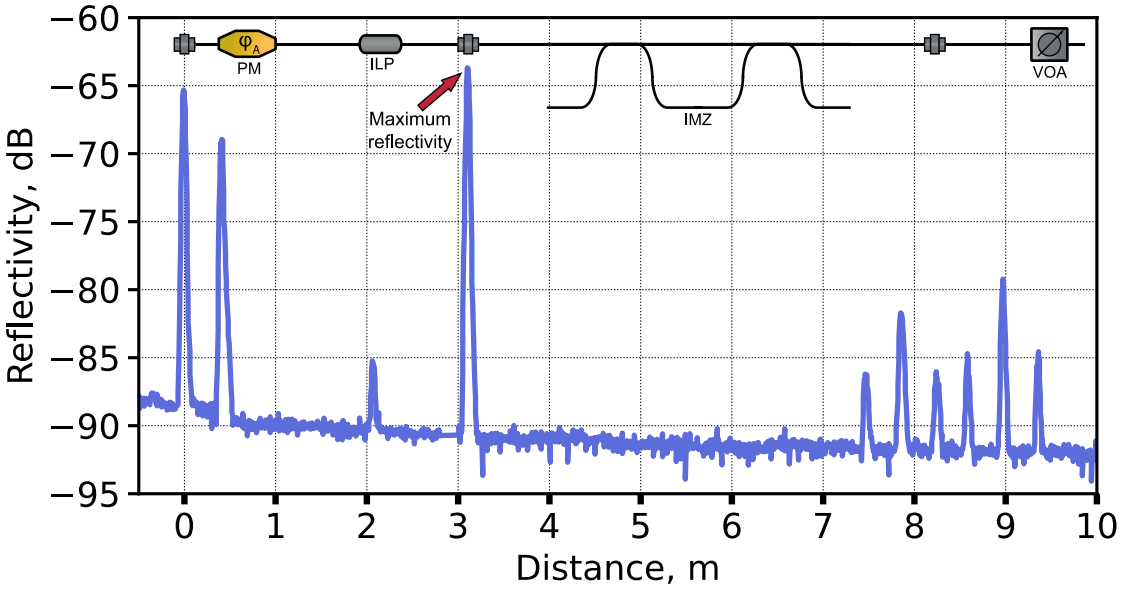
T – спектр пропускания элементов защиты

Рефлектометрия

- Для определения максимального пика отражения проводится **рефлектометрия** системы КРК
- **Рефлектометр** вводит в систему лазерный импульс, засекает время его возврата и измеряет мощность



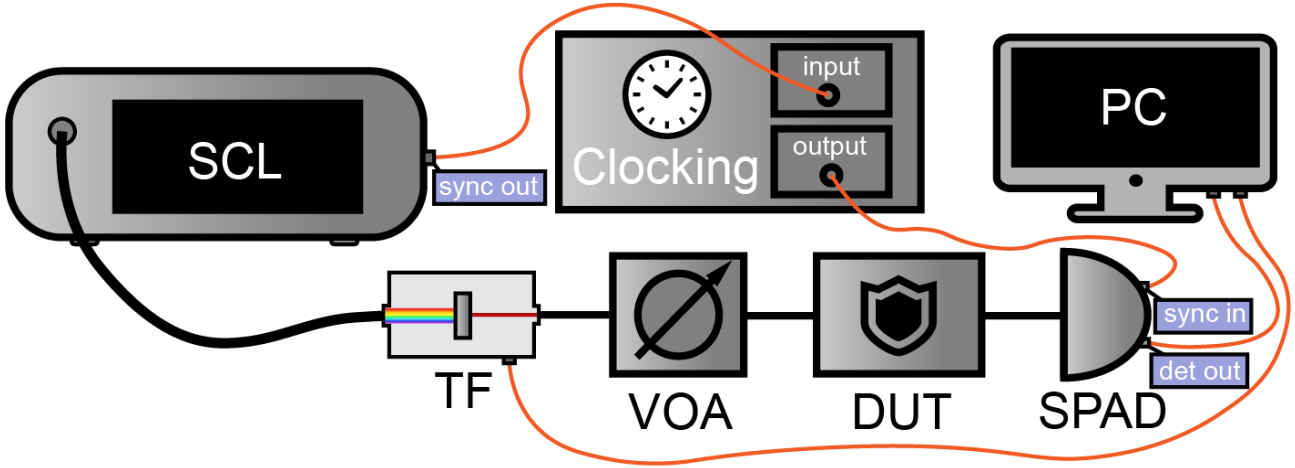
Анализ рефлектограммы



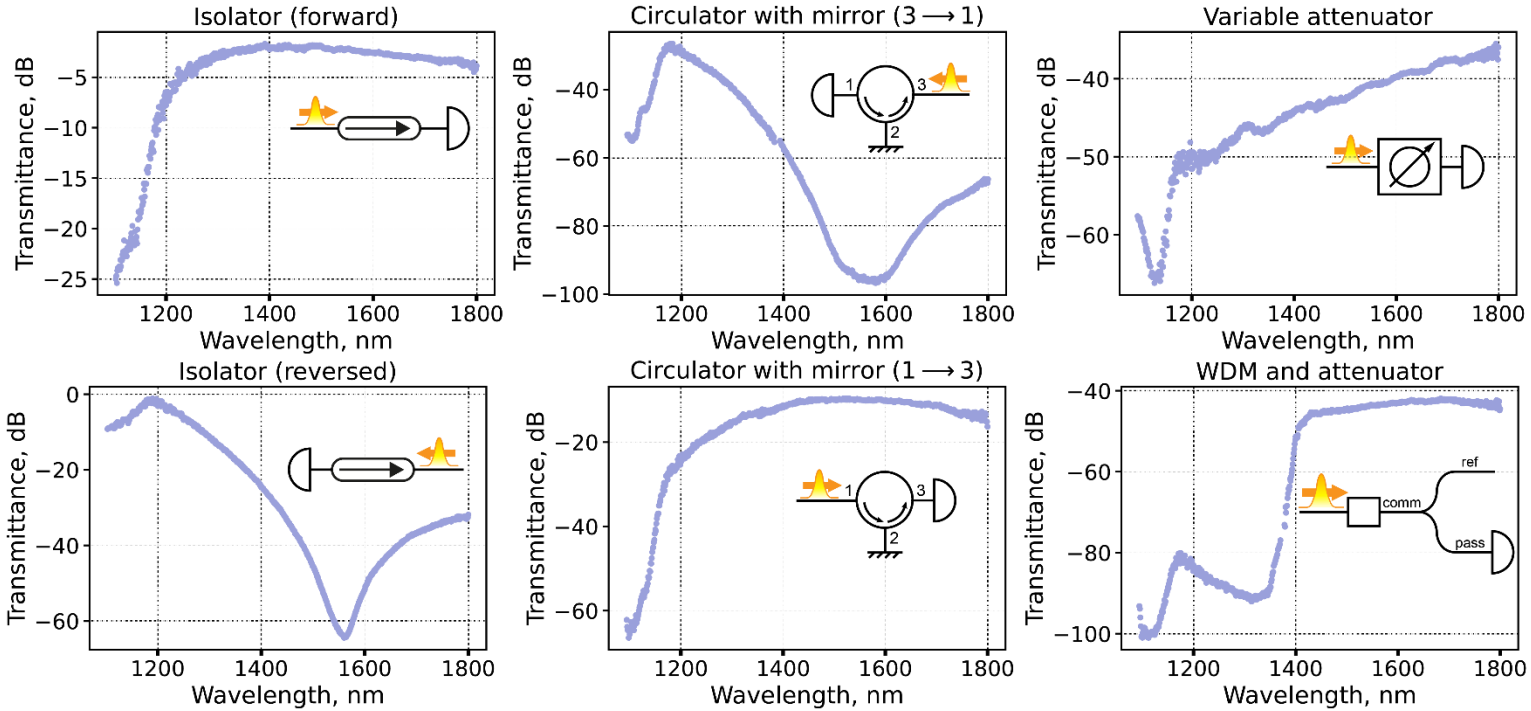
Рефлектограмма – результат рефлектометрии

Измерение спектра пропускания

- Через элементы защиты пропускается излучение **широкополосного лазера** и измеряется его мощность
- **Однофотонный детектор** обеспечивает большой динамический диапазон



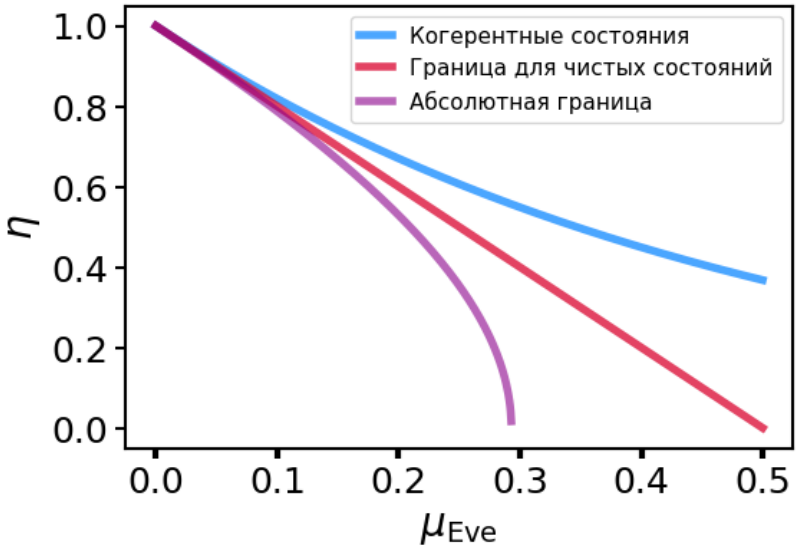
Спектры пропускания



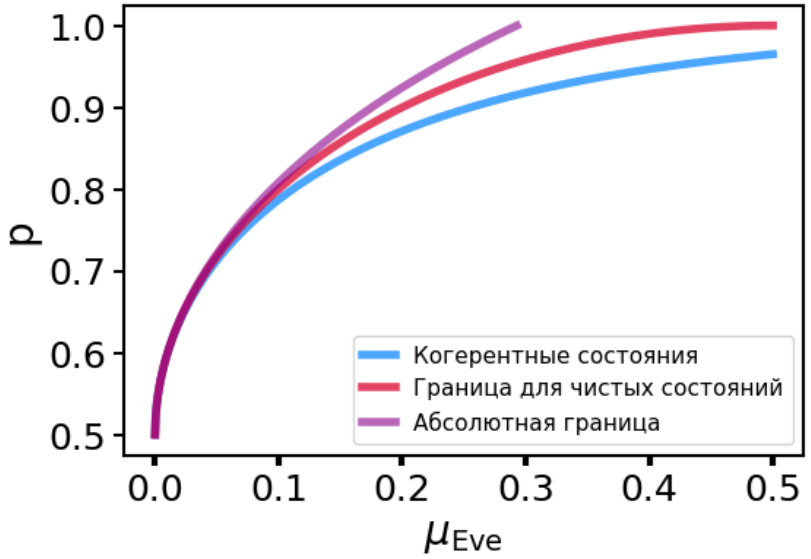
Спектры пропускания элементов защиты

Границы утечки информации

Оценка уровня утечки позволяет свести ее к нулю!



Зависимость корня из фиделити от μ_{Eve}



Зависимость вероятности успеха Евы от μ_{Eve}

Выводы

Системы КРК могут гарантировать безопасное распределение ключей даже при наличии побочных каналов утечки

Необходимо **измерять** физические параметры (среднее число фотонов), характеризующие уровень утечки

Зная уровень утечки, можно **вычислить** долю информации, доступной злоумышленнику

Сокращение длины секретного ключа при **усилении секретности** позволит свести долю раскрытой информации к **нулю**

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363