конференция РусКрипто

СФБ ЛАБ

Практический анализ защищенности системы КРК от атаки «Trojan Horse»

Вахрушева Вероника Михайловна, специалист, ООО «СФБ Лаб»

Квантовое распределение ключей

- Безопасность протокола обеспечивается законами квантовой физики
- Атака на квантовые состояния приводит к их возмущению. Наблюдается рост ошибочных срабатываний

Атаки на техническую реализацию

СФБ ЛАБ

Побочные каналы

- Trojan Horse
- Backflash
- Радиоизлучение

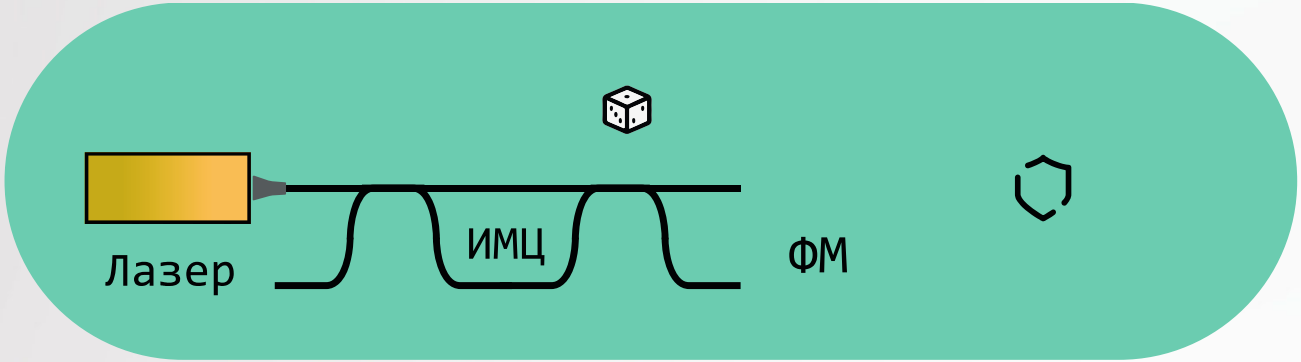
Навязывание

- Detector Blinding
- After-Gate
- Detector Efficiency Mismatch

Изменение свойств системы

- Laser Damage
- Laser Seeding

Атака «Trojan Horse»



- Ева посылает световой импульс высокой мощности внутрь системы КРК
- Импульс претерпевает потери и отражается
- Ева проводит измерения над сигналом в отраженном импульсе со средним числом фотонов μ_{Eve}

История

[Makarov, 2001]

1999-2002

- Идея атаки
- Первые попытки анализа

[Gisin, 2006]

2006

- Рефлектометрия основной инструмент
- Вероятность успеха атаки зависит от μ

[Shields, 2015]

2015

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

[Makarov, 2014/17]

2014-2017

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

- Спектры пропускания в спектральном диапазоне 1260 – 1650 нм (динамический диапазон 60 дБ)

2020

[Borisova, 2020]

- Строгое доказательство секретности при наличии побочных каналов

2020

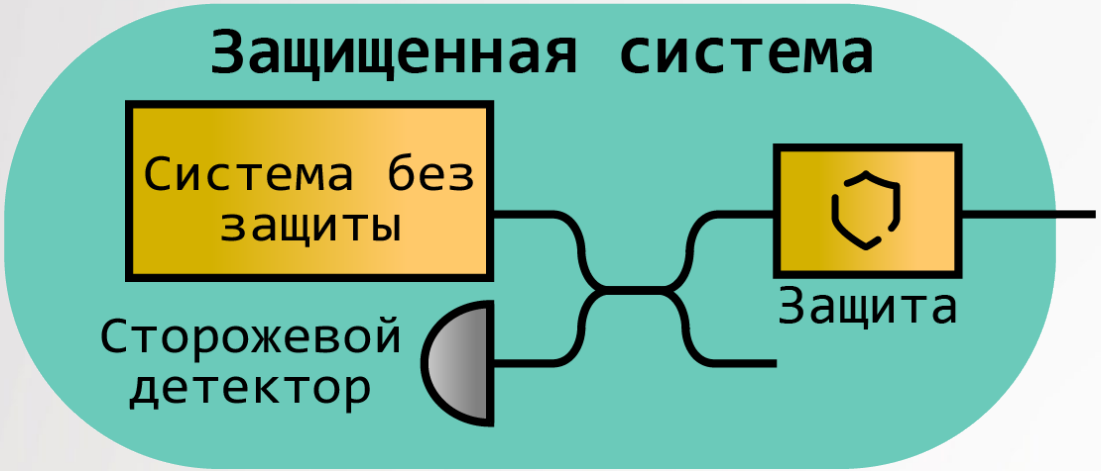
[Molotkov, 2020]

- Спектры пропускания в диапазоне 700 – 850 нм и 1500 – 2100 нм (динамический диапазон 50 дБ)

2022-2023

[Nasedkin, 2022/2023]

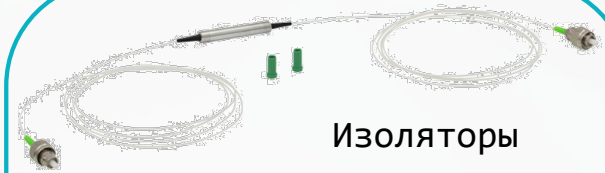
Защита от «Trojan Horse»



Алиса

Защита понижает уровень отраженного сигнала

Элементы защиты


Изоляторы


Циркуляторы


Фильтры


Аттенюаторы


Детекторы

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**

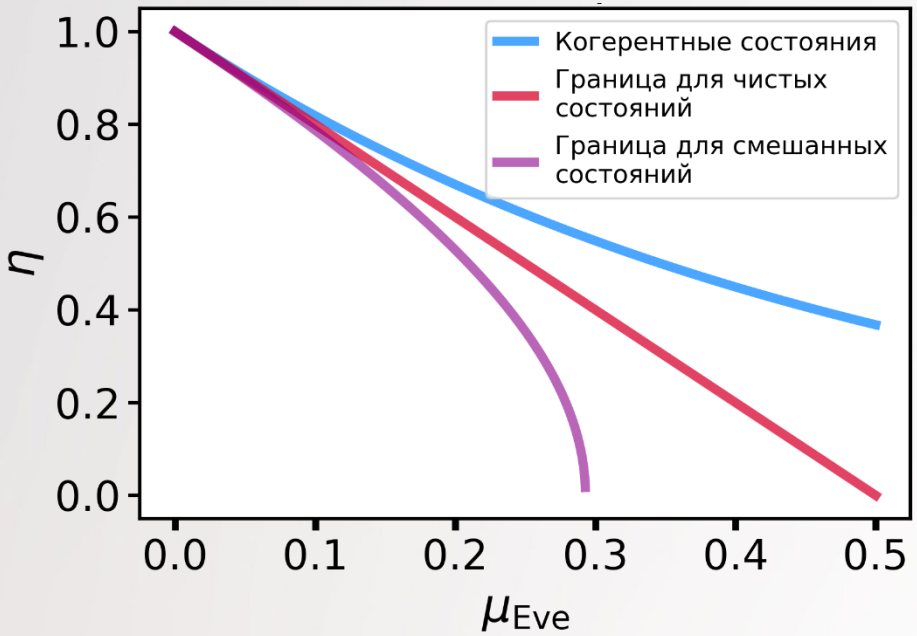
Длина секретного ключа

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

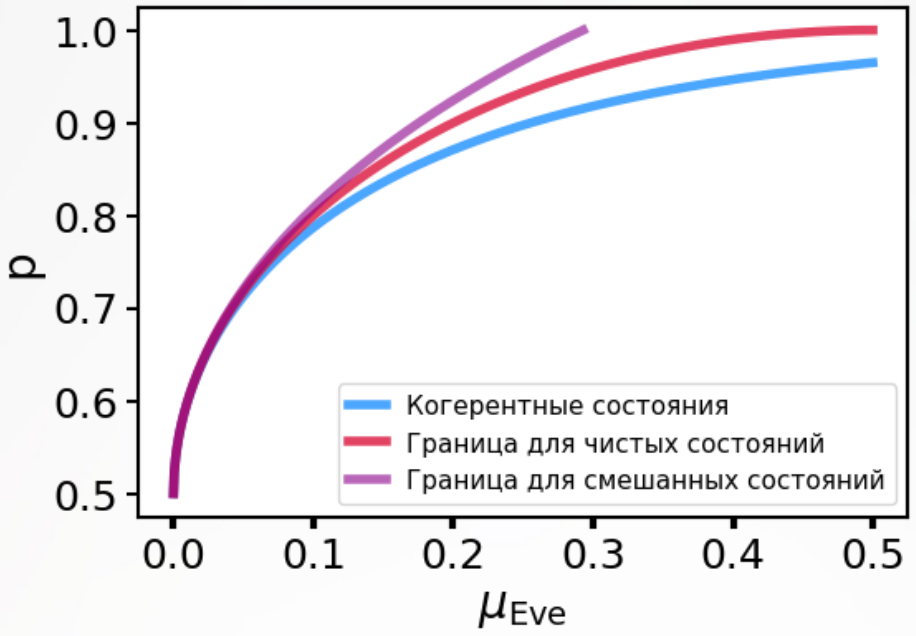
$$\eta = \eta(\mu_{Eve})$$

Границы утечки информации

Фазовое кодирование



Зависимость корня из фиделити от μ_{Eve}



Зависимость вероятности успеха Евы от μ_{Eve}

Анализ защищенности

Для оценки μ_{Eve} достаточно измерить **3 физических параметра**

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

$\boldsymbol{R}$ – величина максимального пика отражения внутри системы

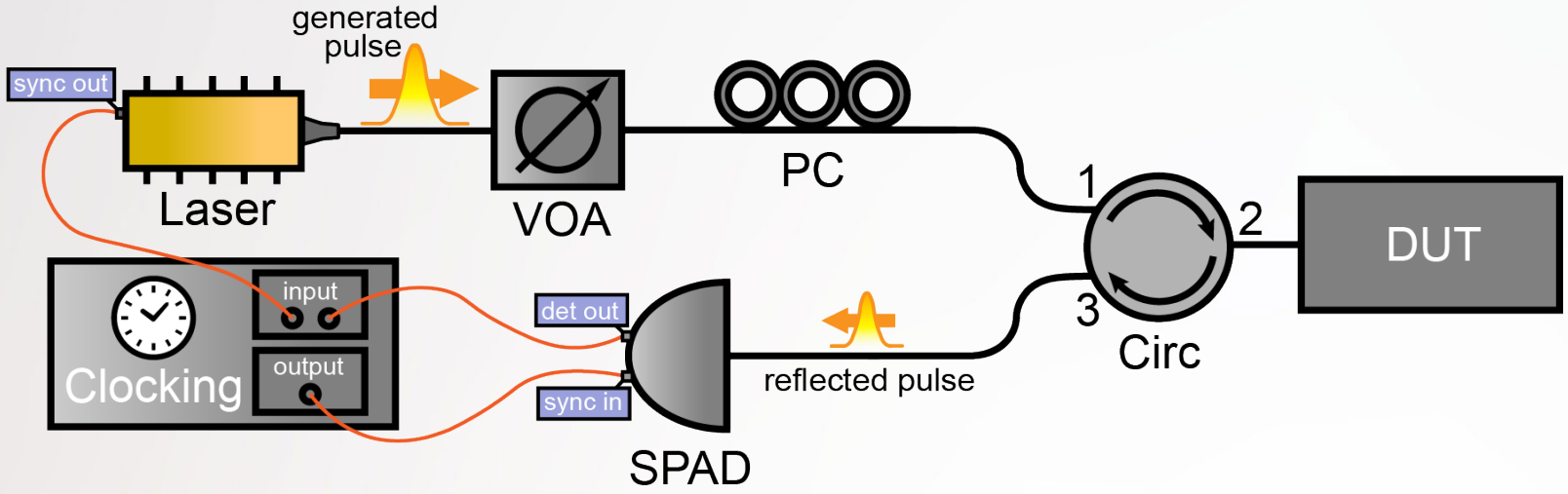
$\boldsymbol{T}$ – спектр пропускания элементов защиты

$$\mu_{Eve}(\lambda) = \frac{P_{Eve}(\lambda) \cdot \lambda}{fhc}$$

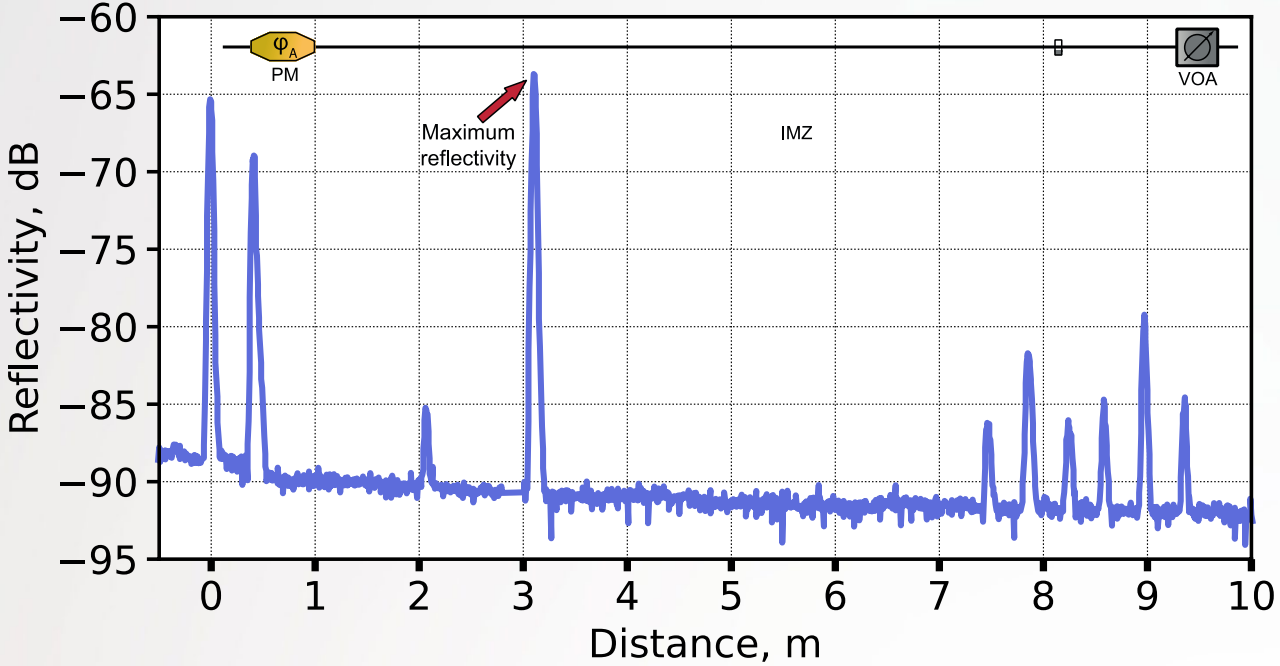
$$P_{Eve}[dBm] = P_{max}[dBm] + T[dB] + R[dB]$$

Рефлектометрия

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



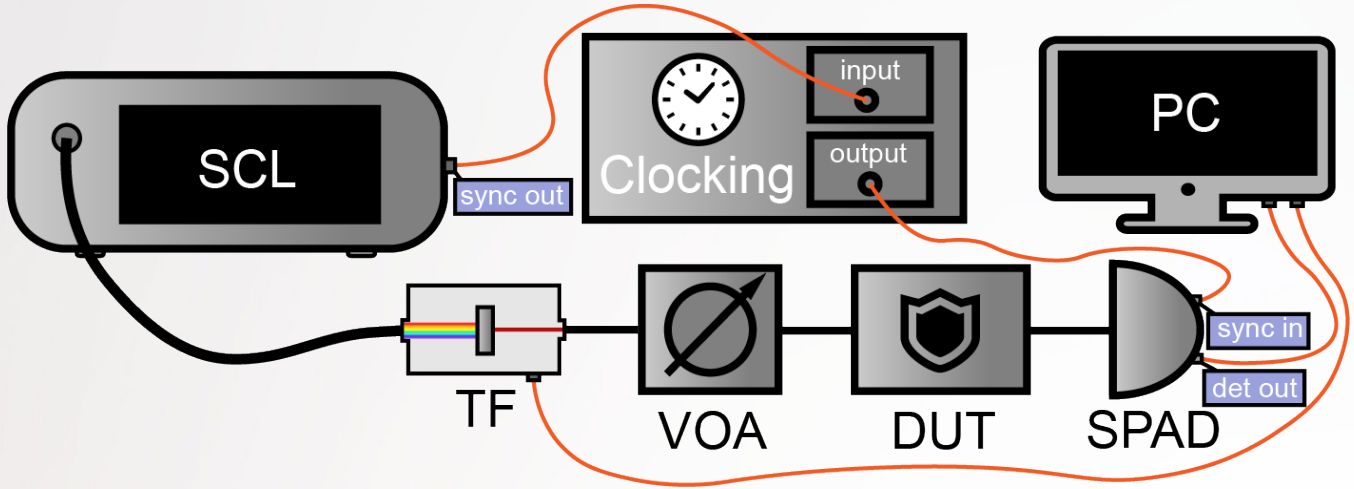
Анализ рефлектограммы



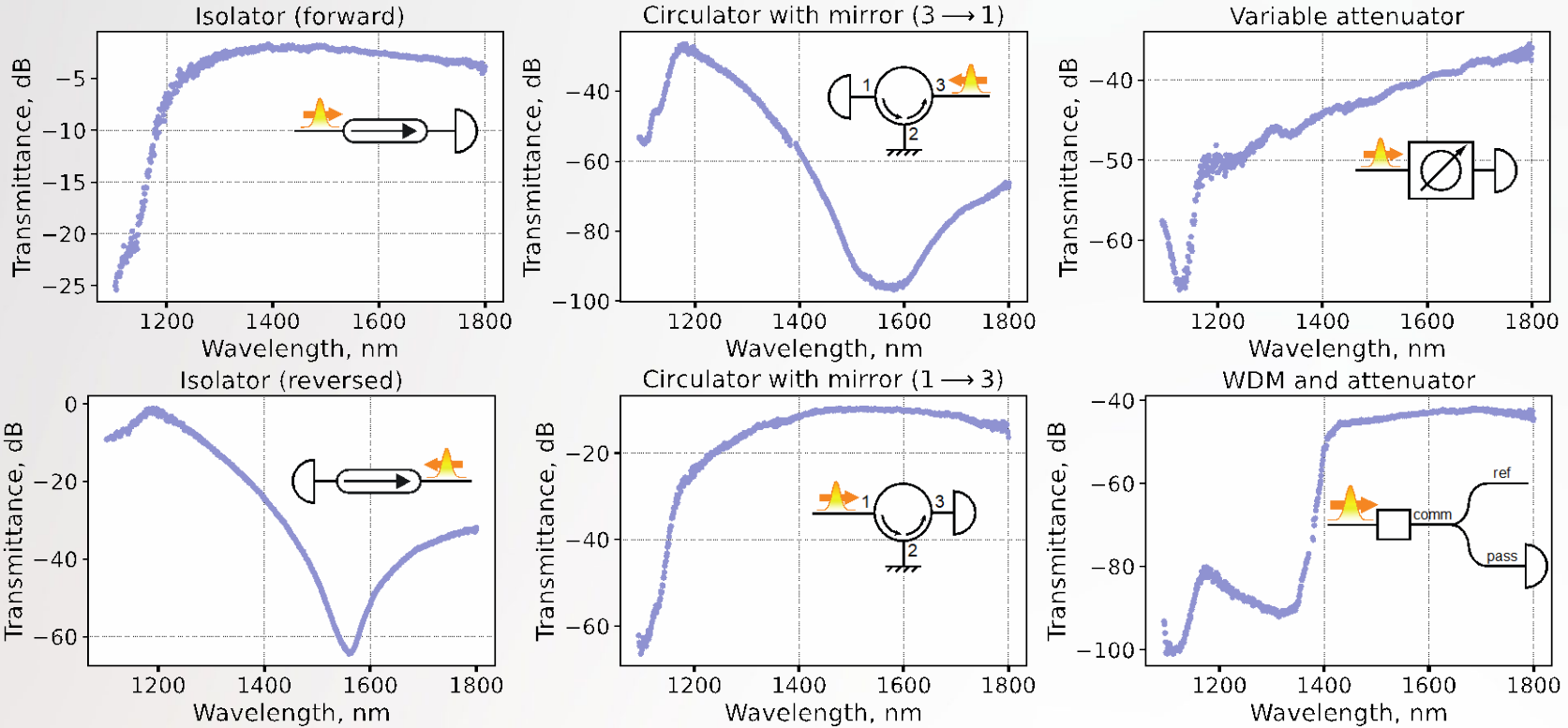
Рефлектограмма – результат рефлектометрии

Измерение спектров пропускания

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



Спектры пропускания элементов защиты



Выводы

СФБ ЛАБ

- 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**

Спасибо за внимание!