Атака "Trojan Horse" на реальные системы квантового распределения ключей: теоретический и экспериментальный анализ

И.С.Сущев, Д.С.Булавин, К.Е.Бугай, А.С.Сидельникова, Д.А.Дворецкий

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

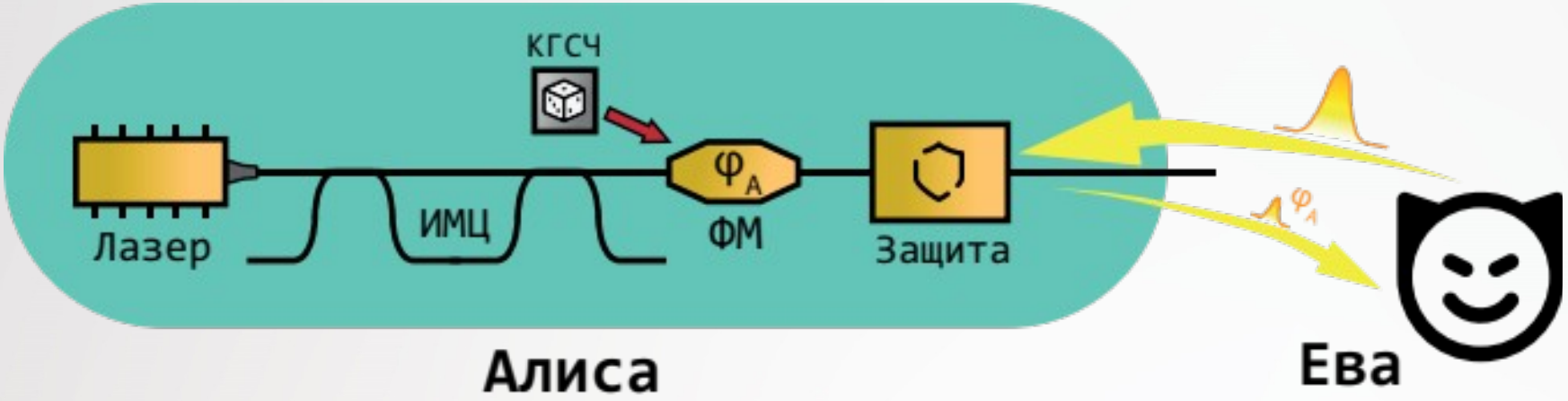
Навязывание

- 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

История

Список источников

1999-2002

- Идея атаки
- Первые попытки анализа

[Makarov, 2001]

2006

- Рефлектометр как основной инструмент
- Вероятность успеха атаки зависит от

[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

Список источников

- Строгое доказательство секретности при наличии побочных каналов

2020

[Molotkov, 2020]

- Полный экспериментальный анализ атаки
- Применение к реальной системе КРК
- Проведены измерения в области 1100 – 1800 нм (динамический диапазон 120 дБ)
- Предложен способ измерения в области 400 – 2000 нм

2021

[Sushchev, 2021]

- Проведены измерения в областях 700 – 850 нм и 1500 – 2100 нм (динамический диапазон 50 дБ)

2022-2023

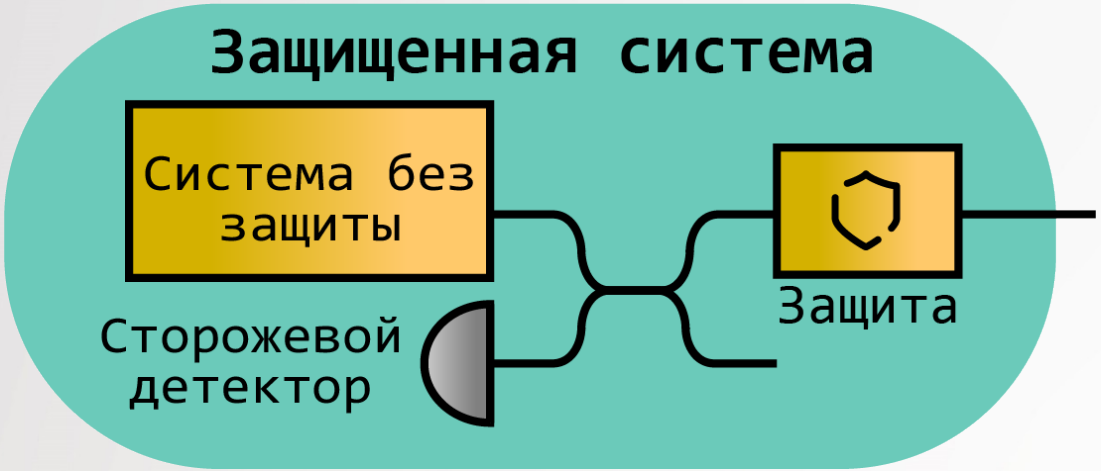
[Nasedkin, 2022/23]

- Граница утечки информации при атаке «Trojan Horse» для состояний общего вида

2024

[Sushchev, 2024]

Защита от «Trojan Horse»



Алиса

Защита понижает уровень отраженного сигнала

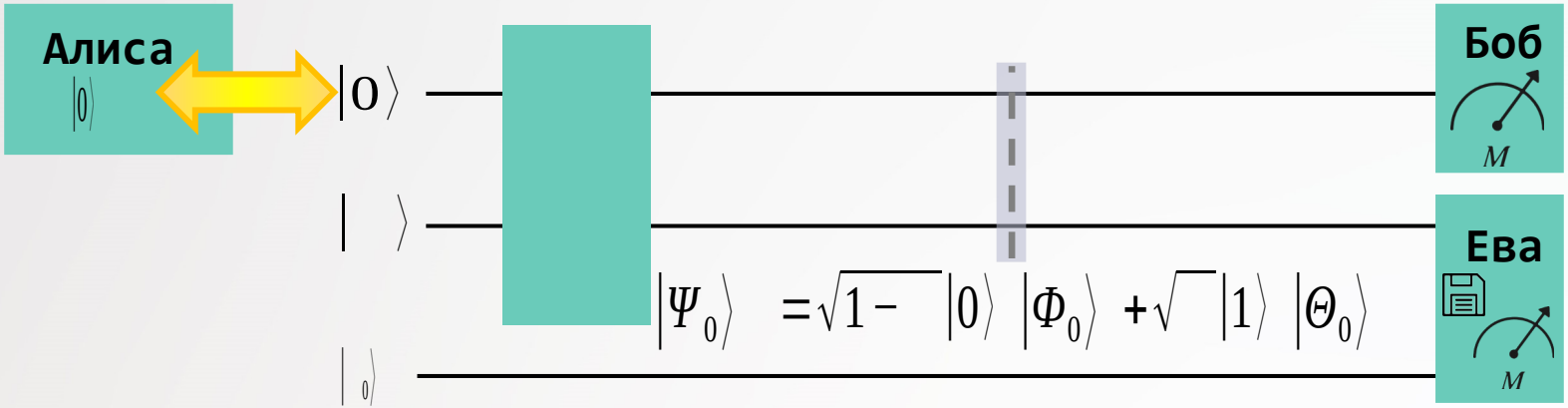
Элементы защиты

Утечка информации

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

Длина секретного ключа

Квантовая схема атаки



- В общем случае Ева комбинирует атаку «Trojan Horse» с коллективной атакой

Секретность в условиях атаки (BB84)

- Длина секретного ключа

$$= \quad _{0} \quad ^{0} \quad + \quad _{1} \quad ^{1}$$

Величина Холево

$$= \left(\right) - \sum \left(\right)$$

Энтропия фон Неймана

$$\left(\right) = - \left(\log \right)$$

Информация Евы при атаке

- Известный результат:

Бинарная энтропийная функция Шеннона

$$h(\quad)=-\quad\log\quad-(1-\quad)\log(1-\quad)$$

Для оптимальной атаки:

QBER вычисляется при постобработке

Перекрытие (корень из фиделити) между состояниями Евы:

Выражается через ?

Когерентные состояния

- Модельные соображения – Ева использует когерентные состояния (ослабленные лазерные импульсы)

Когерентное состояние

$$|\rangle = \sum_{=0}^{\infty} \frac{}{\sqrt{\quad !}} \vee \quad \rangle$$

$$= | \quad |^2$$

Поляризационное кодирование

$$= |\langle \quad |0\rangle|^2 = \quad -$$

Фазовое кодирование

$$= \quad - \quad \sum_{=0}^{\infty} \frac{\left(- \quad \right)}{\quad !} = ¿ \quad ^{-2} \quad ¿$$

Связь с вероятностью вакуумной компоненты

СФБ ЛАБ

- Можно ли отказаться от модельных соображений и найти абсолютную границу (зависящую только от)?
- Идея: любые состояния с содержат тождественную вакуумную компоненту с вероятностью

$$= \sum_{=0}^{\infty} \qquad = \sum_{=1}^{\infty} \qquad \geq \sum_{=1}^{\infty} \qquad = 1 - \quad _0$$

- Отсюда получаем:

$$_0 \geq 1 -$$

Произвольные чистые состояния

Поляризационное кодирование

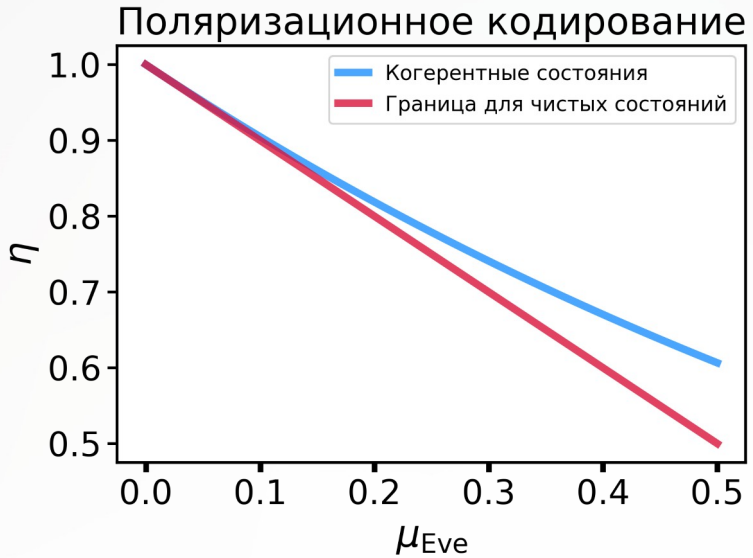
$$= \langle \quad | \quad \rangle = | \quad _{o}|^{2} = \quad _{o}$$

Связь перекрытия состояний с

$$\geq 1 -$$

Граница достигается, например, на состояниях:

$$\left| \quad \right\rangle = \sqrt{1 - \quad} \left| \quad \right\rangle + \sqrt{\quad} \left| 10 \right\rangle$$
$$\left. \quad \right\rangle = \sqrt{1 - \quad} \left. \quad \right\rangle + \sqrt{\quad} \left| 01 \right\rangle$$



Произвольные чистые состояния

Фазовое кодирование

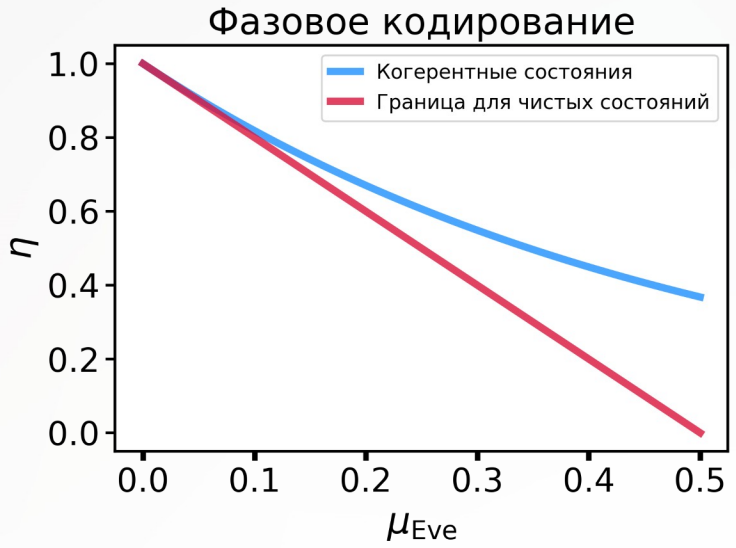
$$= \langle \quad _0 \quad _1 \rangle = \quad _0 ^2 + \quad _1 ^2 \quad ^1 + \quad _2 ^2 \quad ^2 + \ldots$$

Связь перекрытия состояний с

$$\geq 1 - 2$$

Граница достигается, например, на состояниях:

$$\quad _0 \rangle = \sqrt{1 - \quad} \quad \rangle + \sqrt{\quad} \, |1\rangle$$
$$\quad _1 \rangle = \sqrt{1 - \quad} \quad \rangle - \sqrt{\quad} \, |1\rangle$$



Смешанные состояния Евы

- В общем случае Ева использует **смешанные** состояния

$$= \quad _{o} \quad ^{o} \quad + \quad _{1} \quad ^{1}$$

Неравенство для величины Холево

$$\leq \_\_ = h\left(\frac{1-\sqrt{\mathcal{F}}}{2}\right)$$

Roga, Fannes, Życzkowski
Ph Rev letters 2010, 105, 4

Фиделити смешанных состояний

$$\mathcal{F} = \quad ^{2}\sqrt{\sqrt{\quad}\sqrt{\quad}} = \quad ^{2}\sqrt{\quad} \geq \quad \left(\quad\right)$$

Произвольные смешанные состояния

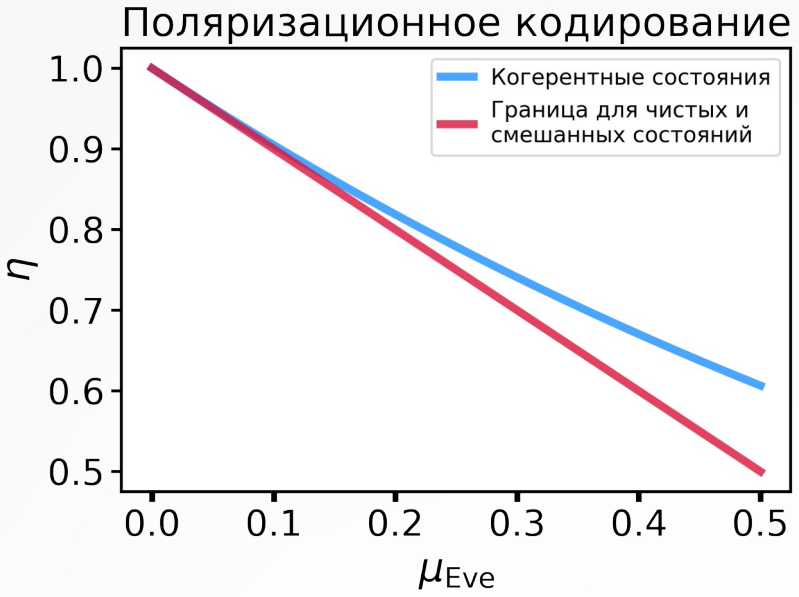
Поляризационное кодирование

$$\mathcal{F} \geq \quad \left(\quad \right) = \quad _{00} \quad _{00} = \quad \frac{2}{0}$$

Результат аналогичен случаю чистых состояний!

Связь перекрытия состояний с

$$\geq 1 -$$



Произвольные смешанные состояния

Фазовое кодирование

Величина «Purity»

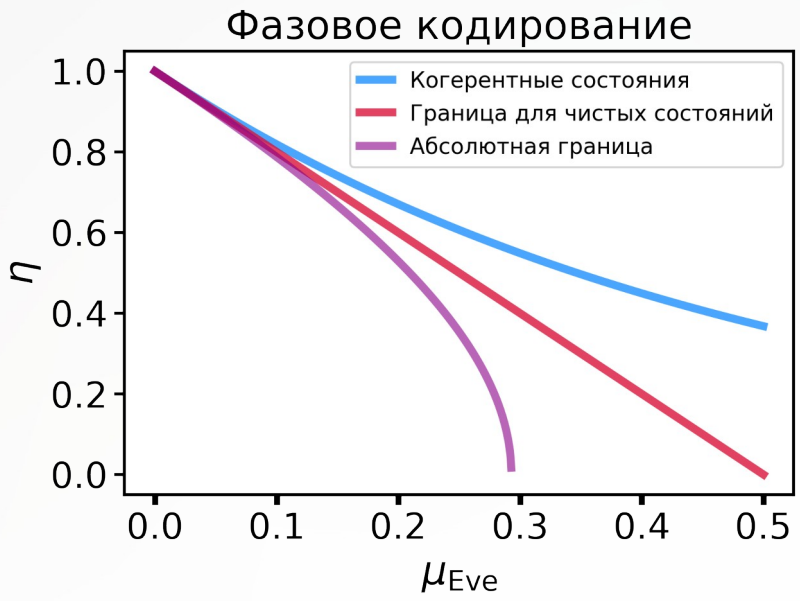
$$\equiv \quad ^2 = \sum_{,\ =0}^{\infty} \left| \quad \right|^2 = \sum_{=0}^{\infty} \left| \quad \right|^2 + \sum_{\neq}^{\infty} \left| \quad \right|^2 \leq 1$$

$$\mathscr{F} \geq \quad \left(\quad ^0 \quad ^1 \right) \geq \sum_{=0}^{\infty} \left| \quad \right|^2 - \sum_{\neq}^{\infty} \left| \quad \right|^2 \geq 2 \quad ^2 -$$

Результат не совпадает со случаем чистых состояний! При граница недостижима

Связь перекрытия состояний с

$$\geq \sqrt{2\left(1 - \quad \right)^2 - 1}$$



Анализ защищенности

Для оценки достаточно измерить **3 физических параметра**

– мощность при атаке с лазерным повреждением (Laser Damage attack)

– величина максимального пика отражения внутри системы

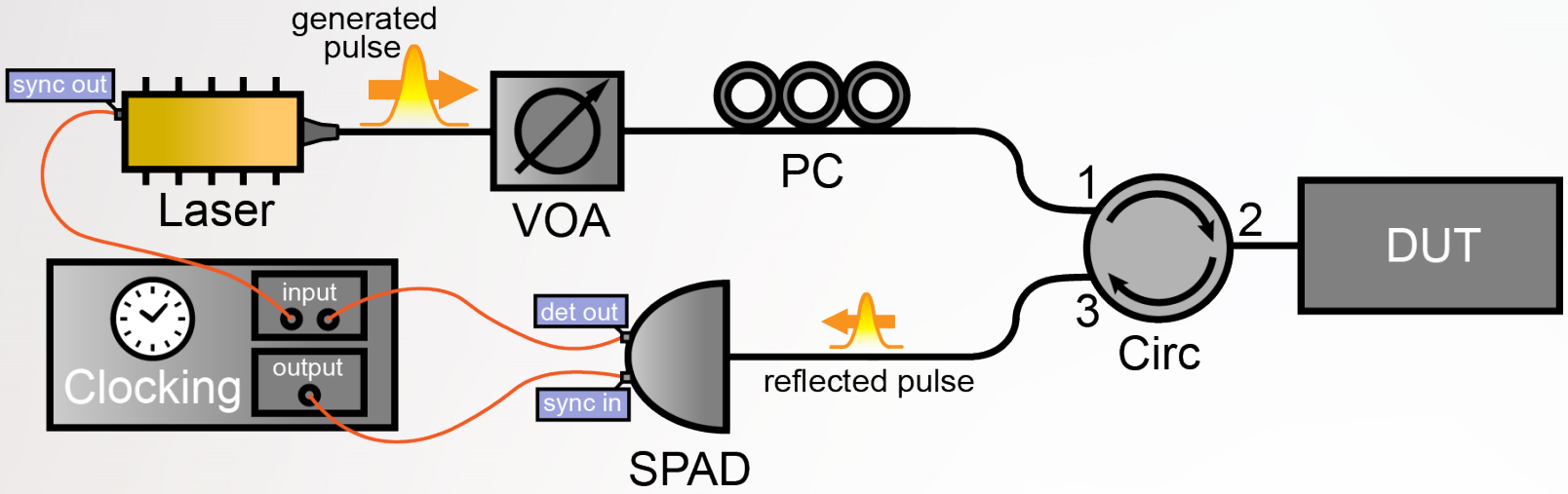
– спектр пропускания элементов защиты

$$(\quad) = \frac{(\quad) \cdot}{h}$$

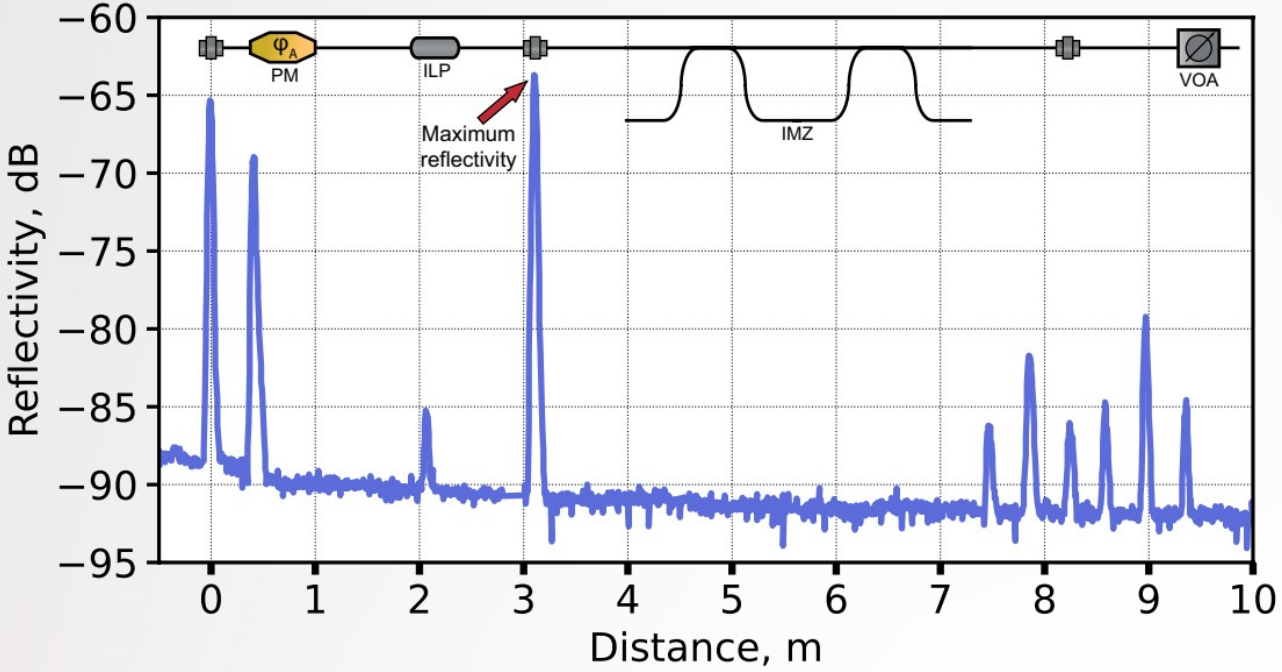
$$[\quad] = [\quad] + [\quad] + [\quad]$$

Рефлектометрия

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



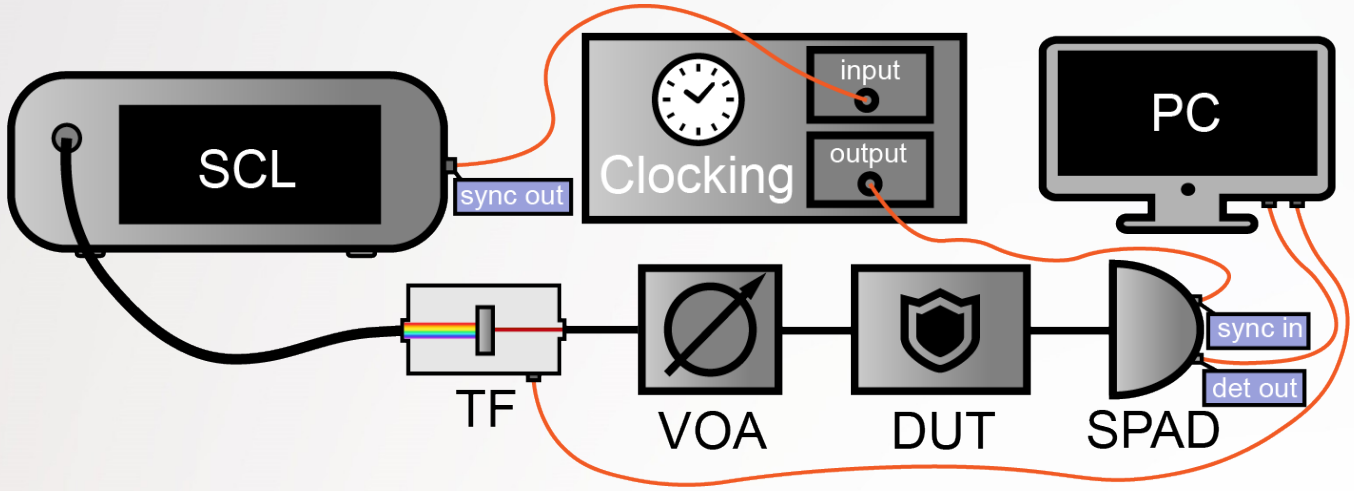
Анализ рефлектограммы



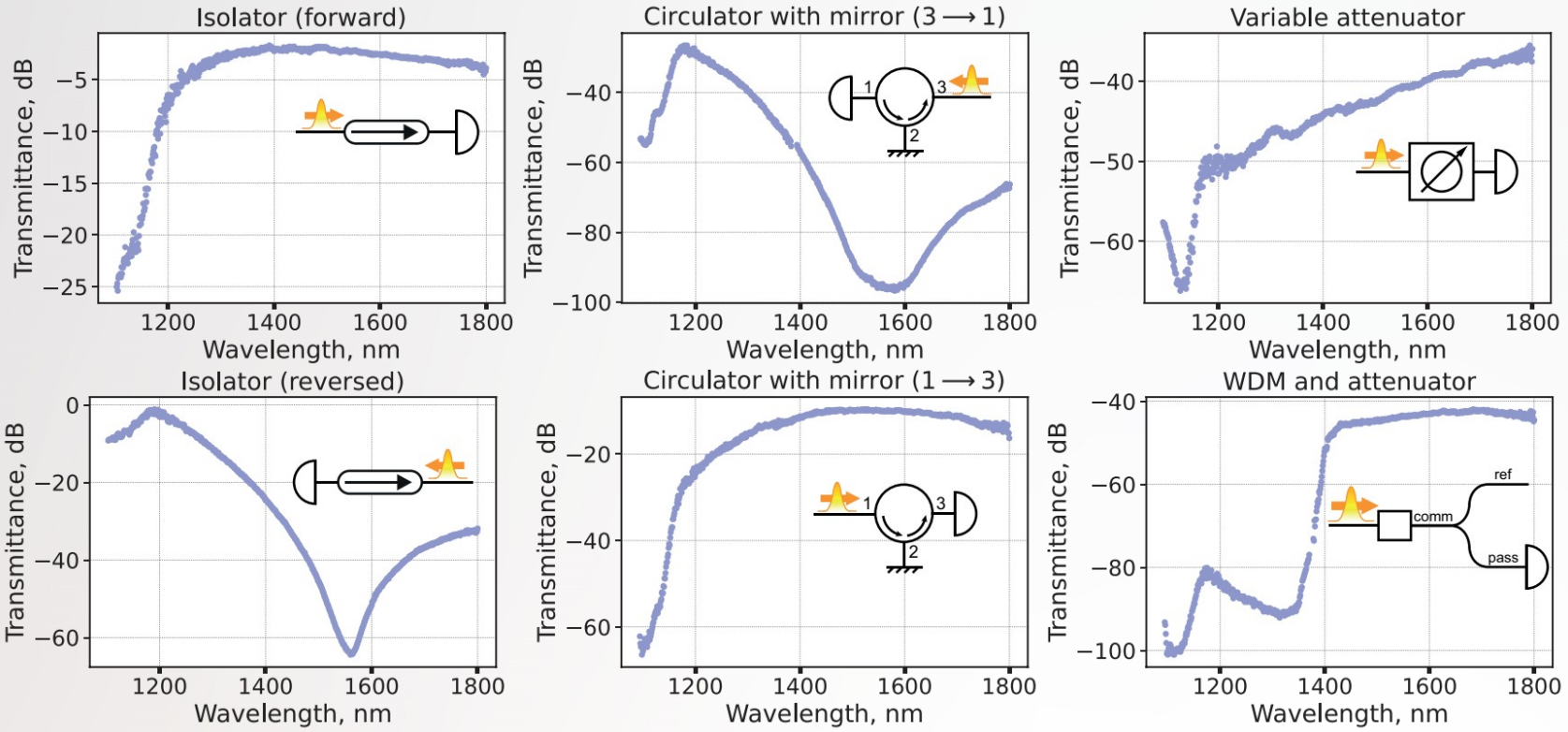
Рефлектограмма – результат рефлектометрии

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!

Инженерно-квантовая лаборатория ООО
«СФБ Лаб»
Ведущий специалист
Иван Сергеевич Сущев

ivan.sushchev@sfblaboratory.ru

СФБ ЛАБ