Широкополосная рефлектометрия для анализа уязвимостей систем КРК в ближнем инфракрасном диапазоне

К.Д. Бондарь

СФБ ЛАБ

1755

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

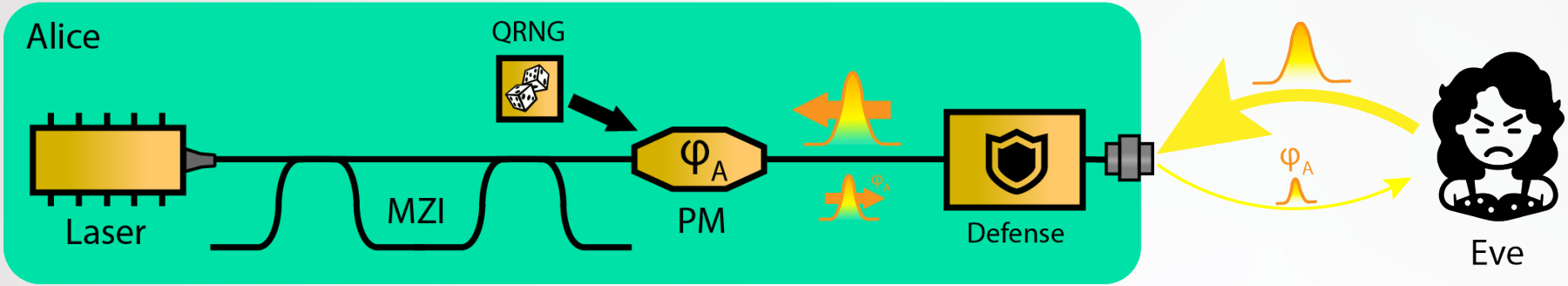
Навязывание

- Detector Blinding
- After-Gate
- Detector Efficiency Mismatch

Изменение свойств системы

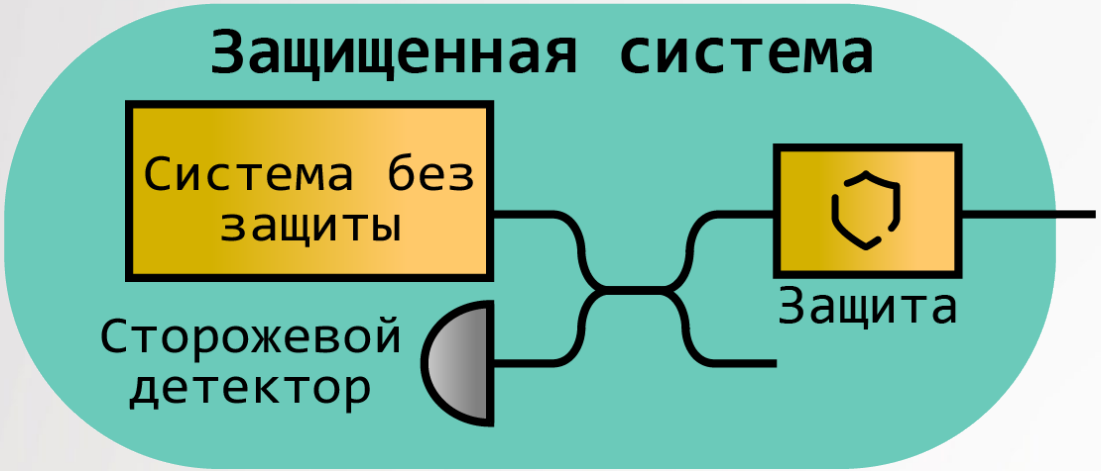
- Laser Damage
- Laser Seeding

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}

Защита от «Trojan Horse»



Алиса

- Защита понижает мощность зондирующего излучения
- Демонстрируется нестабильная эффективность в широком спектре

Элементы защиты

Утечка информации при атаке в широком спектре

СФБ ЛАБ

- Мощность отраженного сигнала P_{Eve} можно **измерить** и оценить μ_{Eve}:

- $\boldsymbol{P_{max}}$ – 40 dBm-порог повреждения системы внешним излучением (или чувствительность сторожевого детектора)

- $\boldsymbol{T}$ – спектр пропускания пассивных компонентов защиты

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

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

$$\mu_{\text{Eve}}(\lambda) = \frac{P_{\text{Eve}}(\lambda)[W] \cdot \lambda}{f_{\text{Eve}} \cdot h \cdot c}$$

- Величину утечки информации можно **вычислить,** зная μ_{Eve}

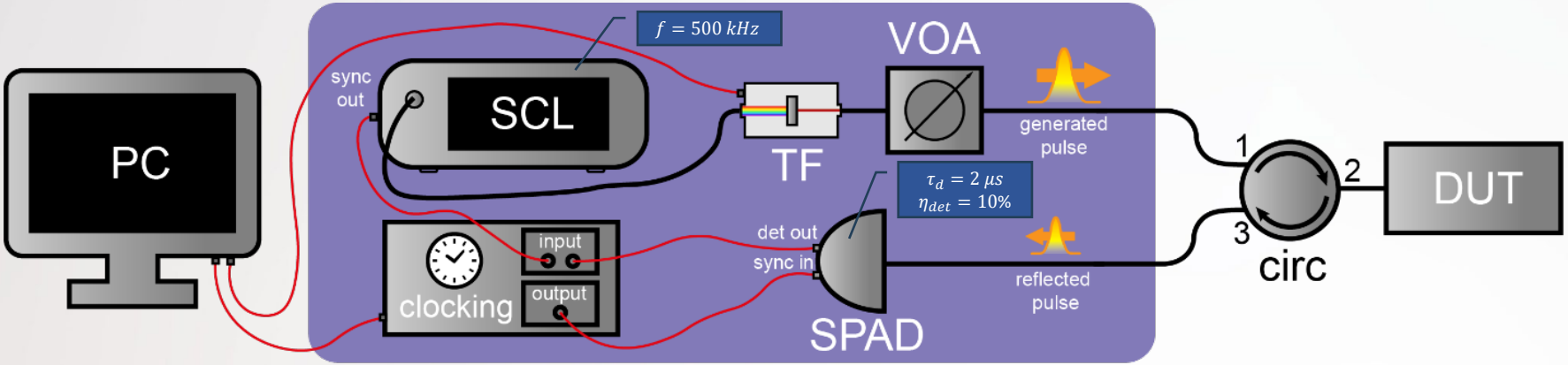
Информация Евы (QBER = 0)

$$\eta = \eta(\mu_{Eve}) \approx 1 - 2\mu_{Eve}$$

$$\bar{\chi}_{Eve} = h\left(\frac{1-\eta}{2}\right) \approx h(\mu_{Eve})$$

Широкополосный рефлектометр (ν - OTDR)

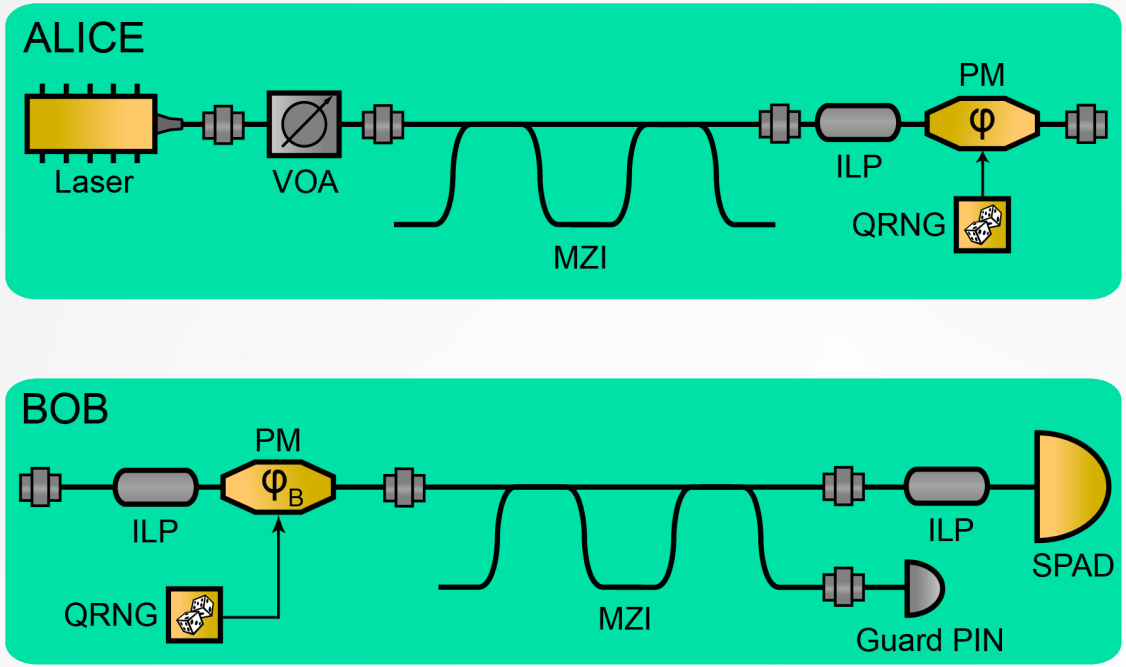
- Для определения максимального пика отражения в широком спектральном диапазоне ($\lambda = 1100 - 1800$ нм) проводится широкополосная **рефлектометрия** системы КРК
- **Рефлектометр** вводит в систему лазерный импульс на каждой длине волны, засекает время возврата его отраженных частей и измеряет их мощность. Динамический диапазон измерений ≈ 80 dB (рэлеевское рассеяние), пространственное разрешение до 10 см в широком спектре.



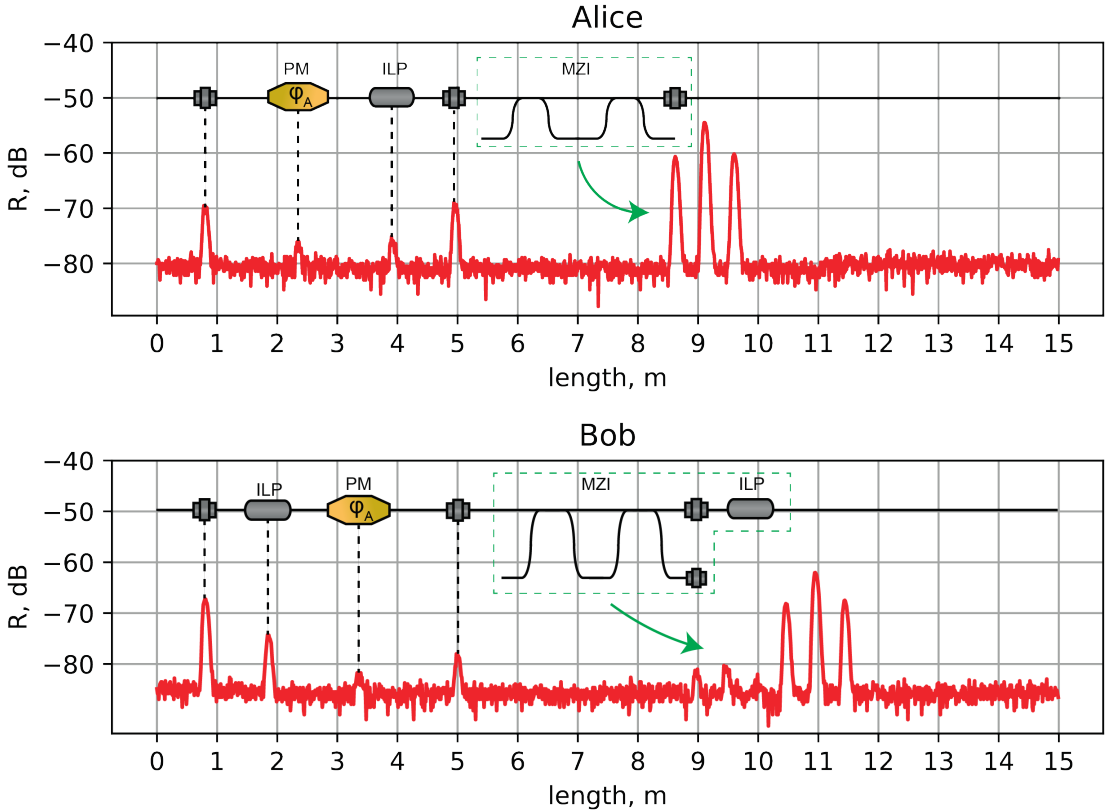
SCL - суперконтинуумный пикосекундный лазер, TF - перестраиваемый фильтр, VOA - перестраиваемый аттенюатор, SPAD - лавинный фотодиод на базе InGaAs, CIRC – волоконный циркулятор

Исследуемая система

- Оптические установки намеренно исследуются без пассивных компонентов защиты для максимизации динамического диапазона
- В системе реализован фазово-временной протокол КРК

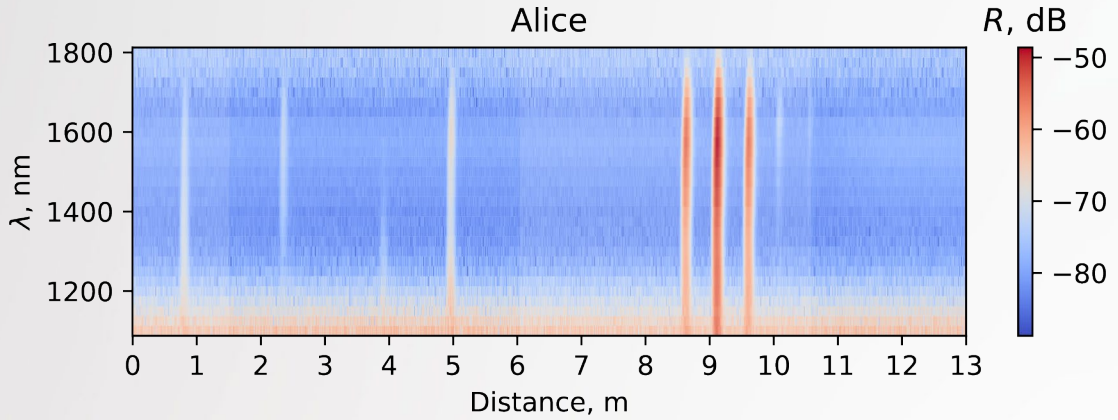


Анализ рефлектограммы на длине волны $\lambda = 1325$ nm

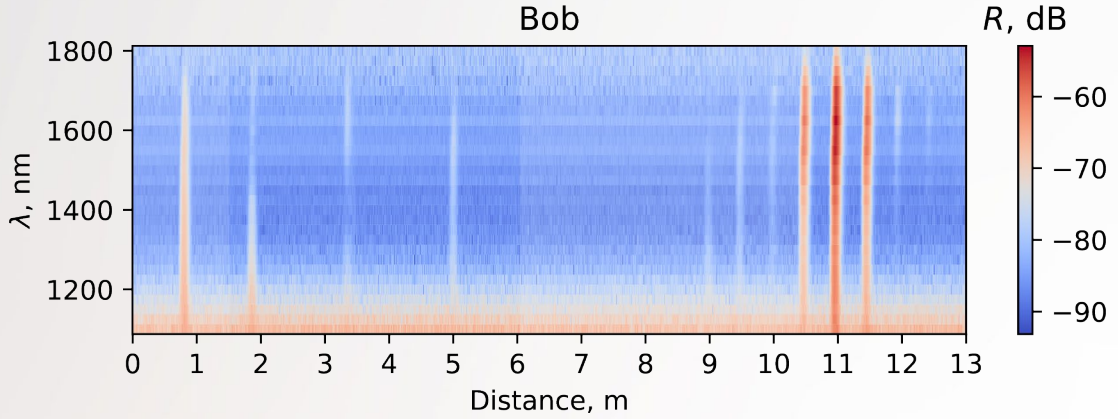


- На длине волны 1325 нм прослеживаются все пики отражений
- Проведено соответствие между пиками на рефлектограмме и волоконными компонентами СКРК
- Максимальные по величине отражения происходят на коннекторах после MZI

Тепловые карты отражений

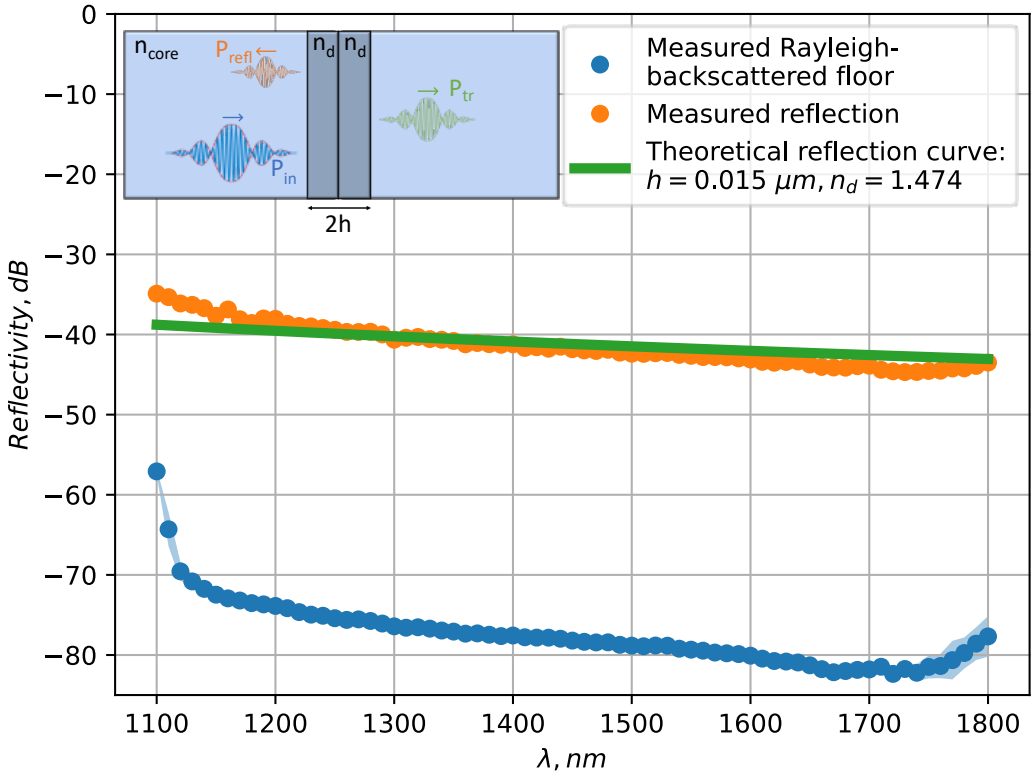


- Максимальное отражение в оптической установке Алисы $R^{\mathrm{A}}_{\max} \approx -49\,\mathrm{dB}$ принадлежит коннектору в схеме MZI ($\lambda_{\mathrm{A}} = 1575\,\mathrm{нм}$)



- Максимальное отражение в оптической установке Боба $R^{\mathrm{B}}_{\max} \approx -53\,\mathrm{dB}$ также принадлежит коннектору в схеме MZI ($\lambda_{\mathrm{B}} = 1625\,\mathrm{нм}$)

Величина отражений волоконного коннектора FC/PC

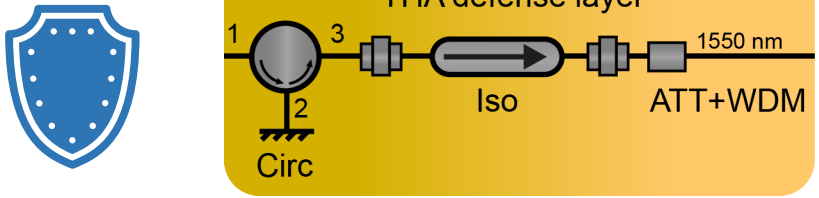


- Измерения проведены в стробируемом режиме работы SPAD
- Динамический диапазон определяется рэлеевским рассеянием
- Теоретическая зависимость описывается моделью резонатора Фабри – Перо [M. Kihara 1996]:

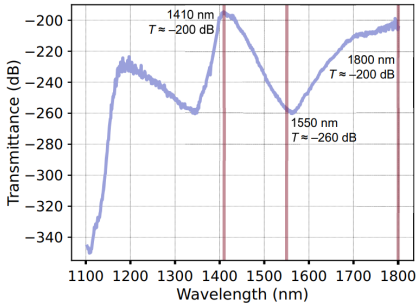
$$R_0 = \left(\frac{n_d - n_{core}}{n_d + n_{core}}\right)^2$$

$$R \approx 10 \cdot \log_{10}\left(R_0 \cdot \left(\frac{4\pi \cdot n_d \cdot 2h}{\lambda}\right)^2\right)$$

Анализ защищенности системы от атаки Trojan-Horse ($\lambda = 1100 - 1800$ nm)



Circ – циркулятор, Iso – изолятор, ATT+WDM – сваренные аттенюатор и WDM-фильтр



Пропускание системы из пассивных компонентов защиты

[Sushchev 2024]

$T^{\mathrm{A}}_{\mathrm{def}}(\lambda_{\mathrm{A}}) \approx -250$ dB

Рефлектометрия:

$R^{A}_{\max} \approx -49$ dB

Информация Евы при полном внутреннем отражении (R = 0 dB):

$$\mu^{A}_{\mathrm{refl}} \approx 2 \cdot 10^{-11}, \quad \bar{\chi}^{\mathrm{A}}_{\mathrm{Eve}} \approx 10^{-9}$$

Информация Евы при фактическом отражении (рефлектометрия):

$$\mu^{A}_{\mathrm{refl}} \approx 2 \cdot 10^{-16}, \quad \bar{\chi}^{\mathrm{A}}_{\mathrm{Eve}} \approx 10^{-14}$$

Выводы

- Представленный широкополосный рефлектометр с **сантиметровым пространственным разрешением** и **динамическим диапазоном до -80 dB** позволил напрямую исследовать возможность и эффективность атаки Trojan Horse в спектральном диапазоне $\lambda = 1100 - 1800$ нм
- Показано, что наибольшие по величине отражения около -50 dB в исследуемой системе КРК принадлежат **оптическим коннекторам**
- Информацию Евы можно свести к 0 со сколь угодно заданной точностью, рассчитав требуемый уровень изоляции системы по утечке в ходе атаки на оптимальной длине волны. Это позволяет сэкономить до 50 dB оптической изоляции и упростить компонентную базу защиты от атаки
- Полноценный анализ уязвимости систем КРК к атаке Trojan Horse подразумевает снятие **рефлектограмм** и **спектров пропускания** защитных компонентов в широком спектральном диапазоне

Спасибо за внимание!

Инженерно-квантовая лаборатория
ООО «СФБ Лаб»
Специалист
Клим Дмитриевич Бондарь

Klim.Bondar@infotecs.ru

СФБ ЛАБ