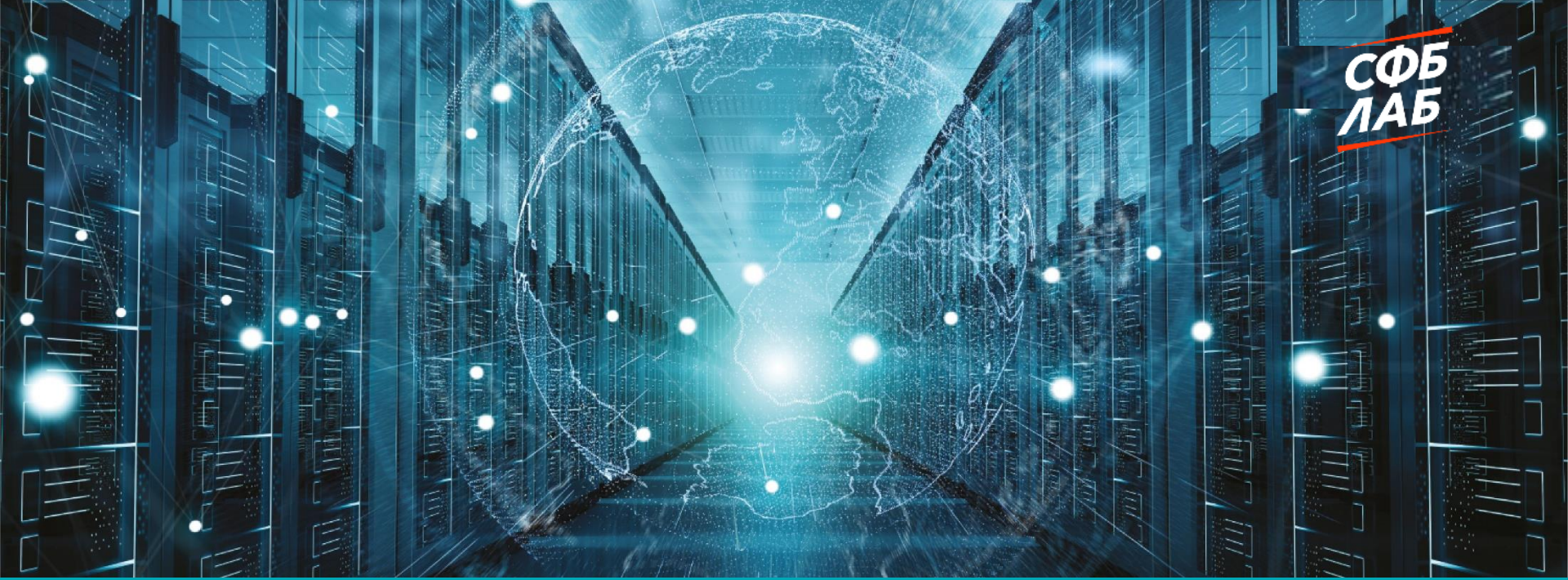
Об оценке эффективности защиты от оптических атак на волоконные квантовые криптографические системы выработки и распределения ключей

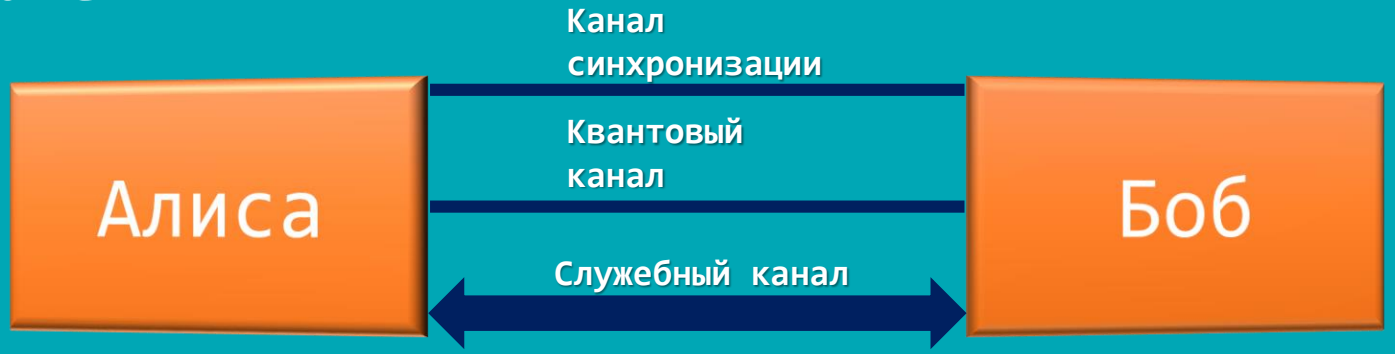
Дворецкий Д.А., к.т.н., ведущий специалист, СФБ Лаб
Зызыкин А.П., ведущий специалист, СФБ Лаб
Сущев И.С., специалист, СФБ Лаб
Бугай К.Е., специалист, СФБ Лаб
Богданов С.А., специалист, СФБ Лаб
Булавкин Д.С., специалист, СФБ Лаб

Содержание



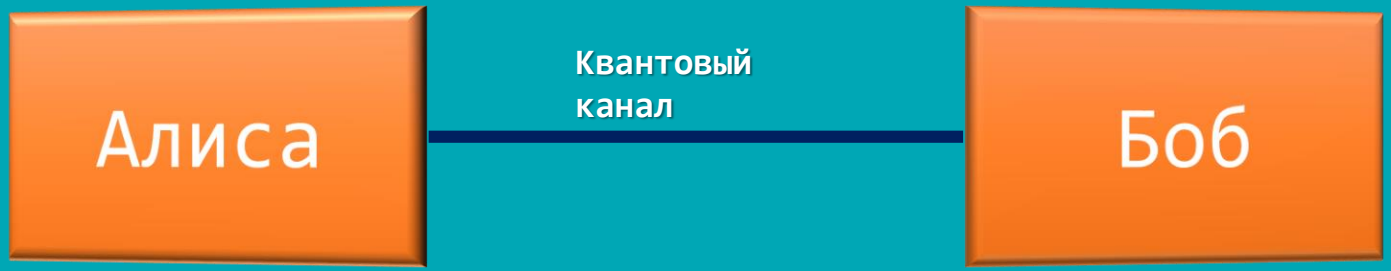
Введение

- Квантовое распределение ключей



Безопасность распределения ключей гарантируется законами квантовой физики

- Квантовое распределение ключей



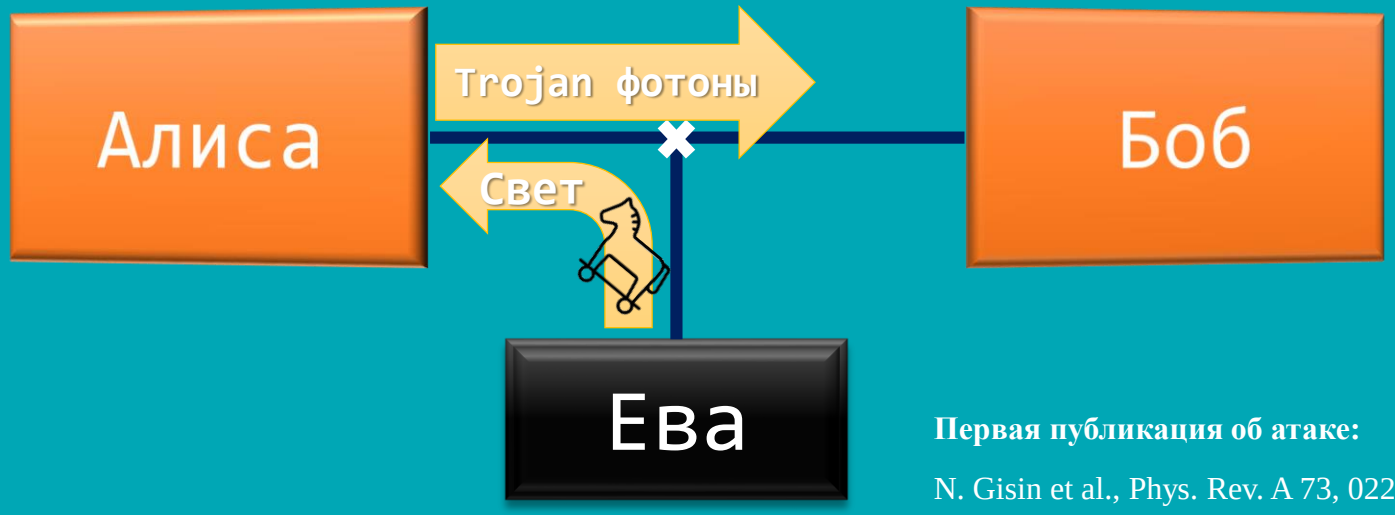
Атаки на квантовые состояния:
1. PNS – атака с разделение числа фотонов
2. BS – атака со светоделителем
3. Унитарная атака
4. UM – атака с определенным исходом

Оптические атаки на КРК:
1. Trojan-horse атака
2. Атака с лазерным повреждением компонентов
3. Атака с переизлучением (Backflash) детектора
4. Импульсное и непрерывное ослепление детектора
5. Time-shift атака и Efficiency mismatch атака

Актуальные оптические атаки

Атака «Trojan horse» на активно-модулирующие компоненты

- Отраженные фотоны от модулятора фазы Алисы приводят к возможности распознавания знака ключа

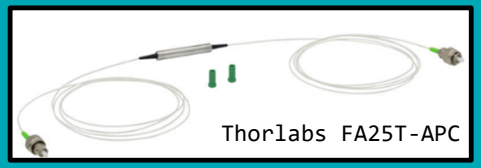


Первая публикация об атаке:

N. Gisin et al., Phys. Rev. A 73, 022320 (2006)

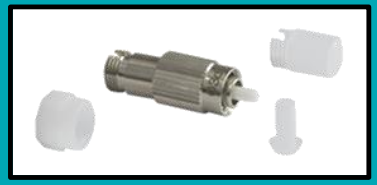
Основные способы борьбы:

- Изоляторы
- Циркуляторы
- Аттенюаторы



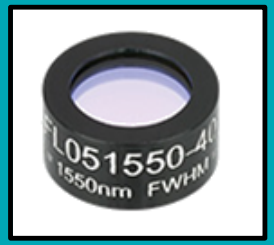
Thorlabs FA25T-APC

Thorlabs 6015-3-APC



Thorlabs FL051550-40

- Широкополосные фильтры
- Сторожевые детекторы



Thorlabs IO-H-1550

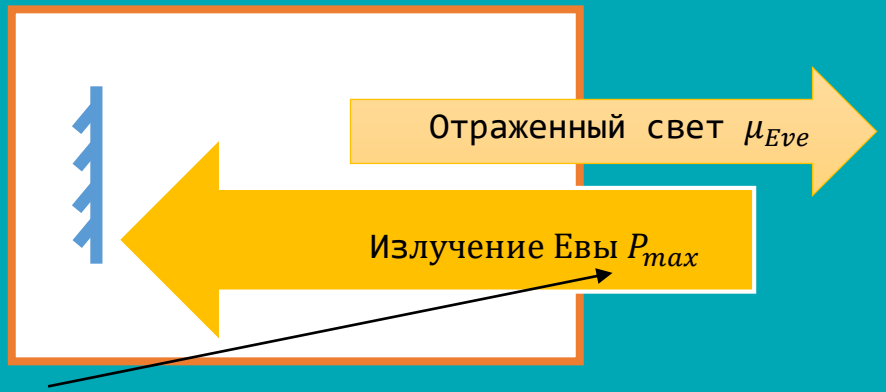
Thorlabs S154C

Оценка рисков атаки

$\mu_{Eve} \ll \mu$ – система защищена!

μ – среднее число фотонов на импульс по протоколу

μ_{Eve}– среднее число фотонов в отраженном импульсе



P_{max} - ограничен мощностью повреждения компонентов или чувствительностью сторожевого детектора

- Для квантового протокола BB84:

$$p_{Eve} = \frac{1}{2} + \frac{1}{2}\sqrt{1 - e^{-2\mu_{Eve}}}$$

S.N. Molotkov, JETP, 158, 6(12), pp. 1011-1031 (2020)

Оценка рисков атаки

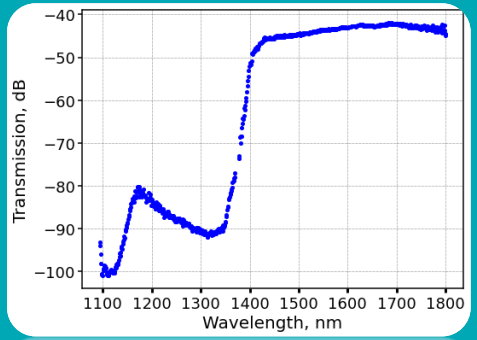
$$P_{Eve}[\text{дБм}] = P_{max}[\text{дБм}] + T[\text{дБ}] + R[\text{дБ}] \Rightarrow \mu_{Eve} = \frac{P_{Eve}[\text{Вт}]\lambda}{fhc}$$

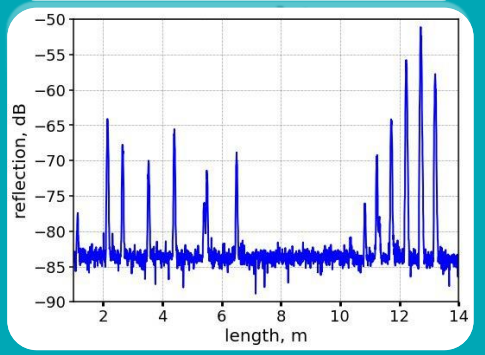
P_{max} – мощность повреждения компонентов (~ 10 Вт средней мощности)

Huang A. et al. Physical Review Applied, 13, 3, 034017 (2020)

T – измерение спектра пропускания

R – измерение отражения от системы





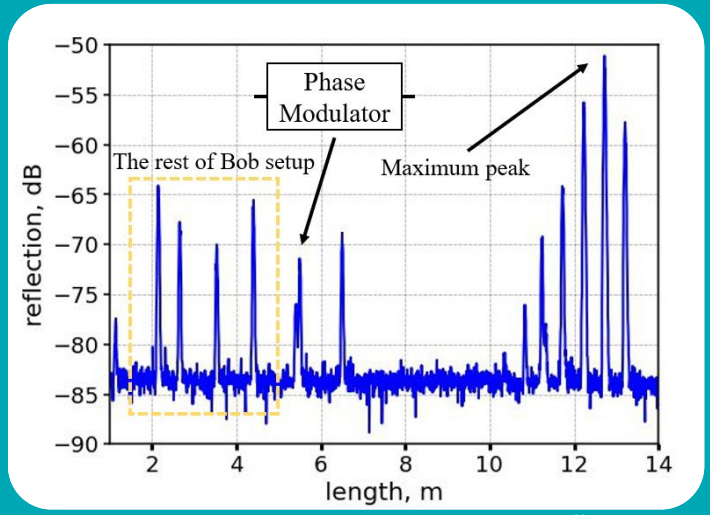
Измерение отражения Боба

Состав рефлектометра:

Лазер:
$\lambda = 1550$ нм
$\tau = 100$ пс
$f = 1$ МГц

InGaAs
SPAD:
$\eta = 7\%$

Максимальный пик отражения – поверхность SPAD
Уровень отражения $R \approx -50$ дБ



Рефлектограмма рассеяния коммерческой системы КРК (Боб) в отсутствии защиты

Оптический рефлектометр

I. Sushchev, et.al., Proceedings of SPIE Security + Defence 2021, paper 11868-15 (2021)

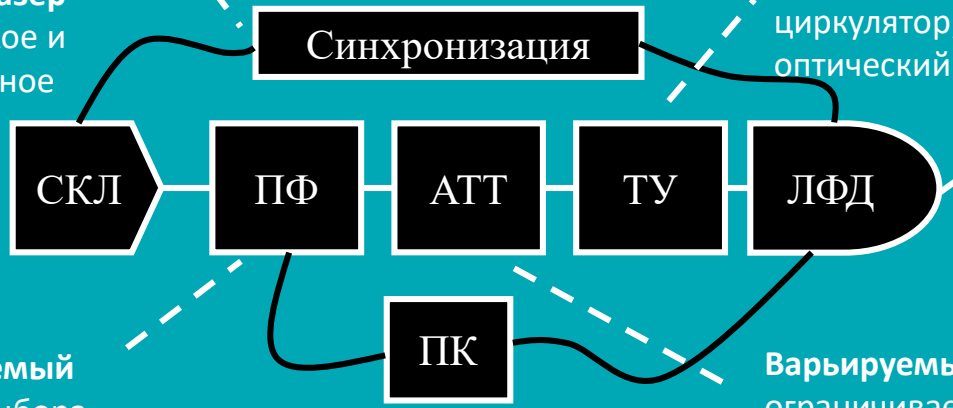
Измерение спектров пропускания

Экспериментальная схема

Синхронизация для СКЛ и ЛФД

Суперконтинуумный лазер (СКЛ) обеспечивает яркое и мощное широкополостное излучение

Тестируемое устройство (ТУ) (оптический изолятор; циркулятор; аттенюатор; оптический фильтр и т.д.)



Однофотонный детектор для приема излучения

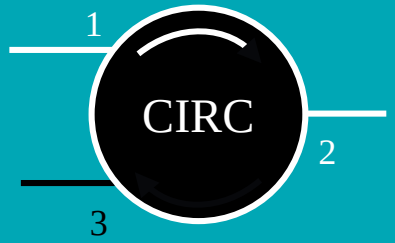
Перестраиваемый фильтр для выбора длины волны

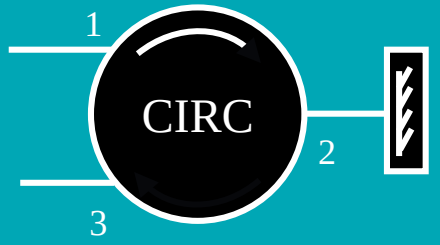
Персональный компьютер для управления установкой в целом

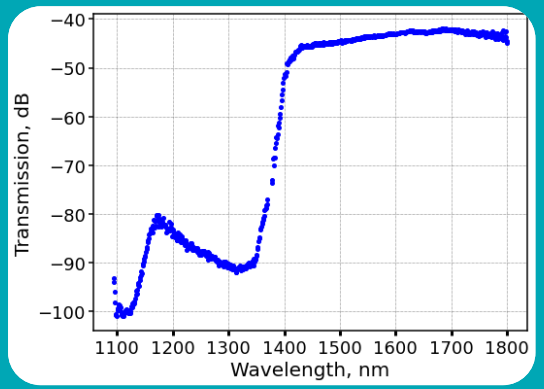
Варьируемый аттенюатор ограничивает среднее число фотонов, необходим для запуска ЛФД в режиме счета фотонов

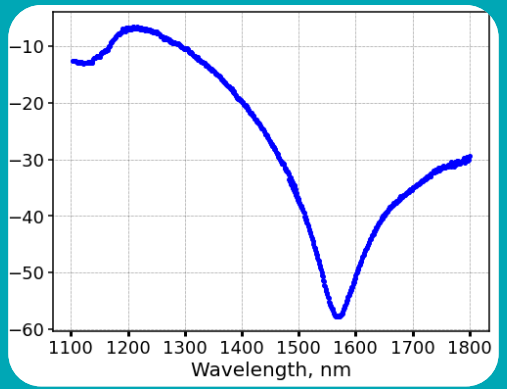
I. Sushchev, et.al., Proceedings of SPIE Security + Defence 2021, paper 11868-15 (2021)

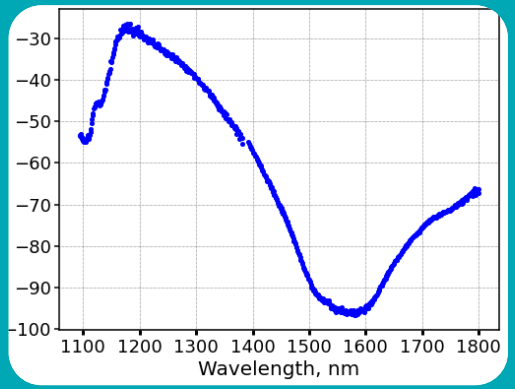
Спектры пропускания в широком спектральном диапазоне







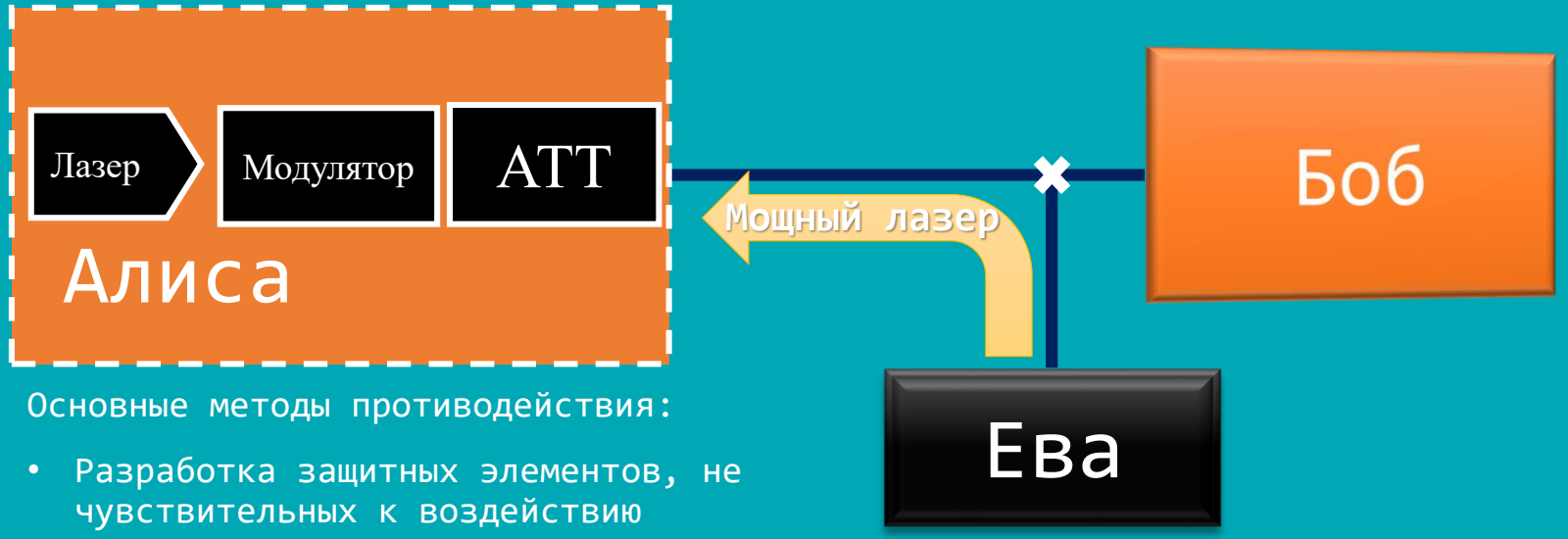




I. Sushchev, et.al., Proceedings of SPIE Security + Defence 2021, paper 11868-15 (2021)

Атака с лазерным повреждением компонентов

- Под действием мощного лазерного излучения аттенюатор просветляется, что приводит к возможности реализации атак на квантовые состояния и оптических атак



Основные методы противодействия:

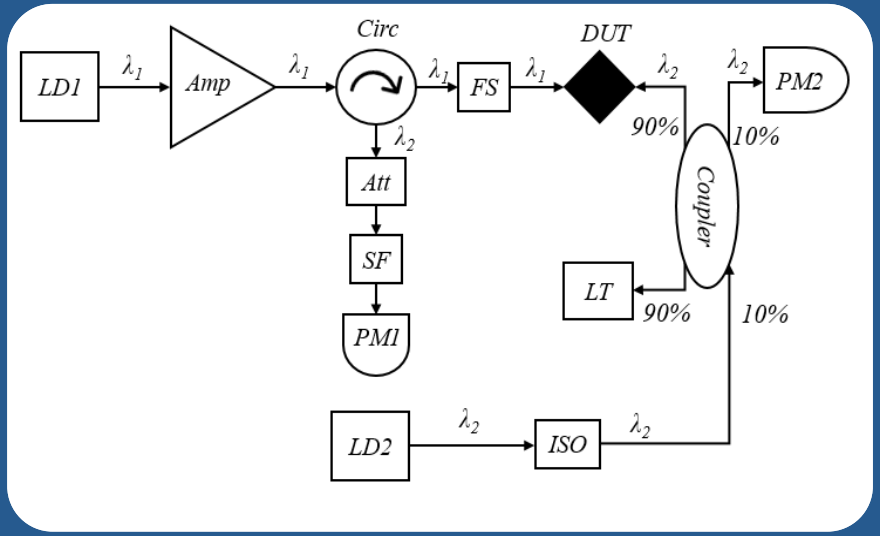
- Разработка защитных элементов, не чувствительных к воздействию
- Сторожевой детектор

Первая публикация об атаке:

Anqi Huang, et.al, Phys. Rev. Applied 13, 034017 (2020)

Атака с лазерным воздействием на простой оптический аттенюатор (широко используемый в волоконно-оптических системах КРК)

Структурная схема экспериментального стенда



LD1 – λ1 лазер ; Amp –легированный Эрбием волоконный усилитель, Circ– волоконно-оптический циркулятор; FS –катушка с волокном; Coupler – 90/10 волоконно-оптический разветвитель; PM1, PM2 –измерители мощности; SF –спектральный фильтр, Att – аттенюатор; ISO –мощный волоконно-оптический изолятор; DUT–тестируемый образец, LD2 – λ2 лазер; LT - волоконно-оптическая заглушка

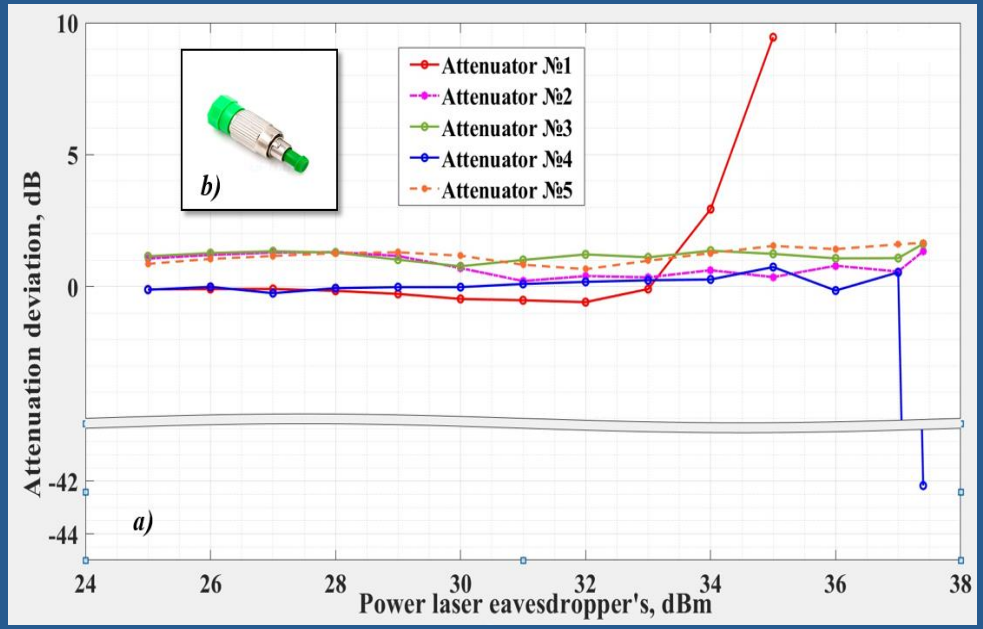
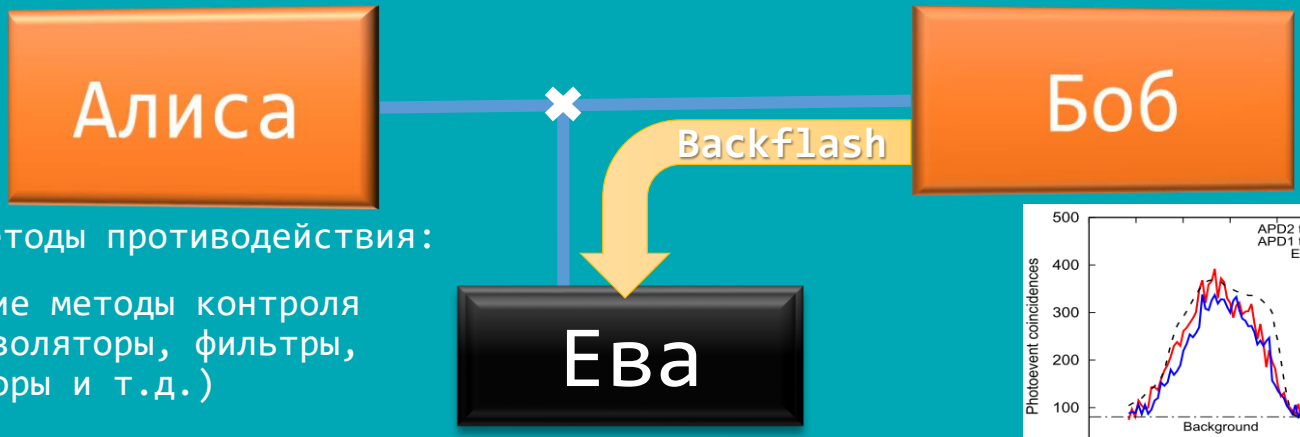


График зависимости изменения поглощения 5 одинаковых аттенюаторов на 20 дБ (b) относительно мощности разрушающего лазерного излучения (a)

Подробнее в докладе на конференции:
Bugai K.E., et.al, 20th International Conference Laser Optics, St. Petersburg, 20-24 June, 2022

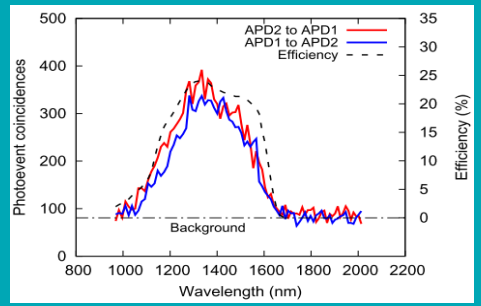
Backflash атака

- При срабатывании однофотонного детектора Боба происходит переизлучение фотонов в квантовый канал
- Например, фотоны пролетевшие оптическую для системы с фазовым кодированием несут информацию о фазе квантового состояния
- Вероятность возникновении вспышки не превышает 5% от срабатываний



Основные методы противодействия:

- Оптические методы контроля утечки(изоляторы, фильтры, циркуляторы и т.д.)
- Учет квантовой утечки ключа в протоколе



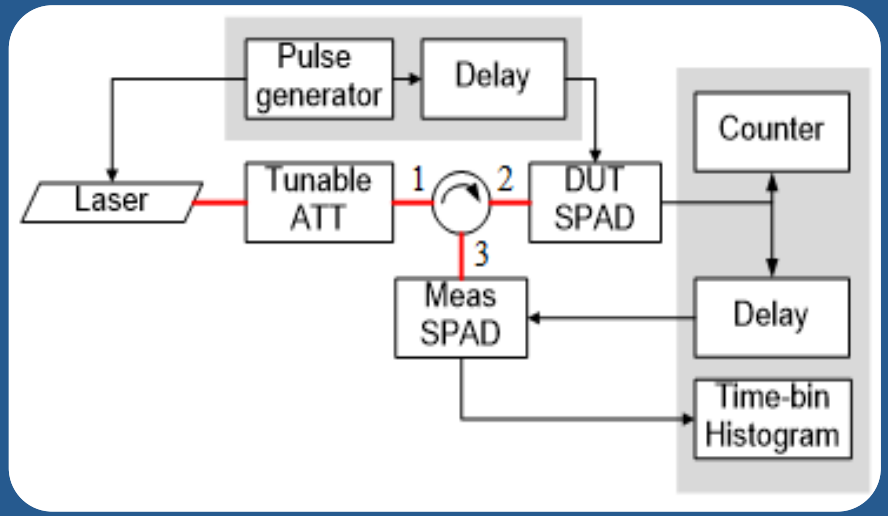
Первая публикация об атаке:

C. Kurtsiefer et al., J. Mod. Opt., 48(13), 2039-2047 (2001)

Исследование зависимостей вероятностей «backflash» от параметров ЛФД и среднего числа фотонов в импульсе

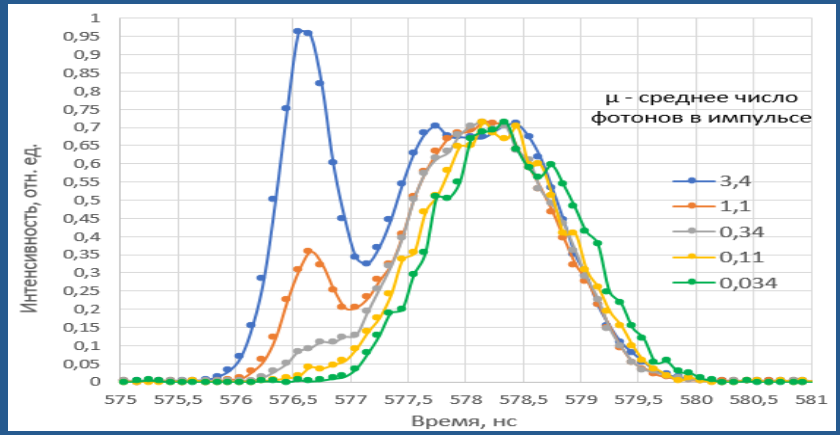
СФБ ЛАБ

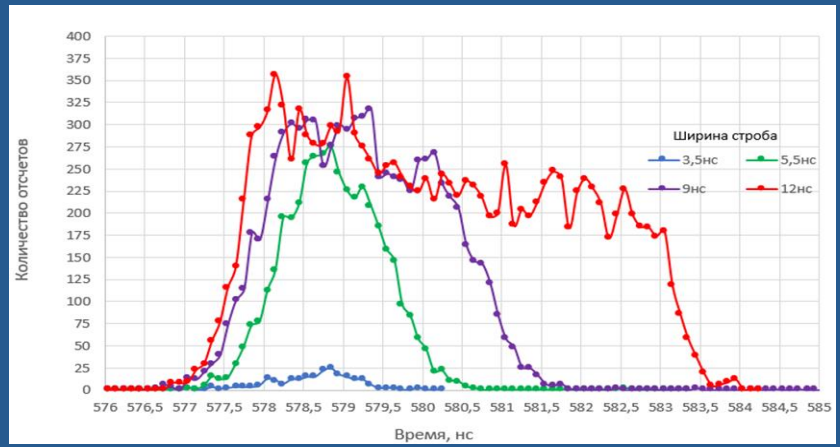
Структурная схема экспериментального стенда



Laser – импульсный лазер, ATT – аттенюатор, Meas SPAD – измерительный ЛФД, DUT SPAD – исследуемый ЛФД, Delay - Временной коррелятор для выставления задержек и настройки синхронизации

Гистограммы распределения отсчетов измерительного детектора

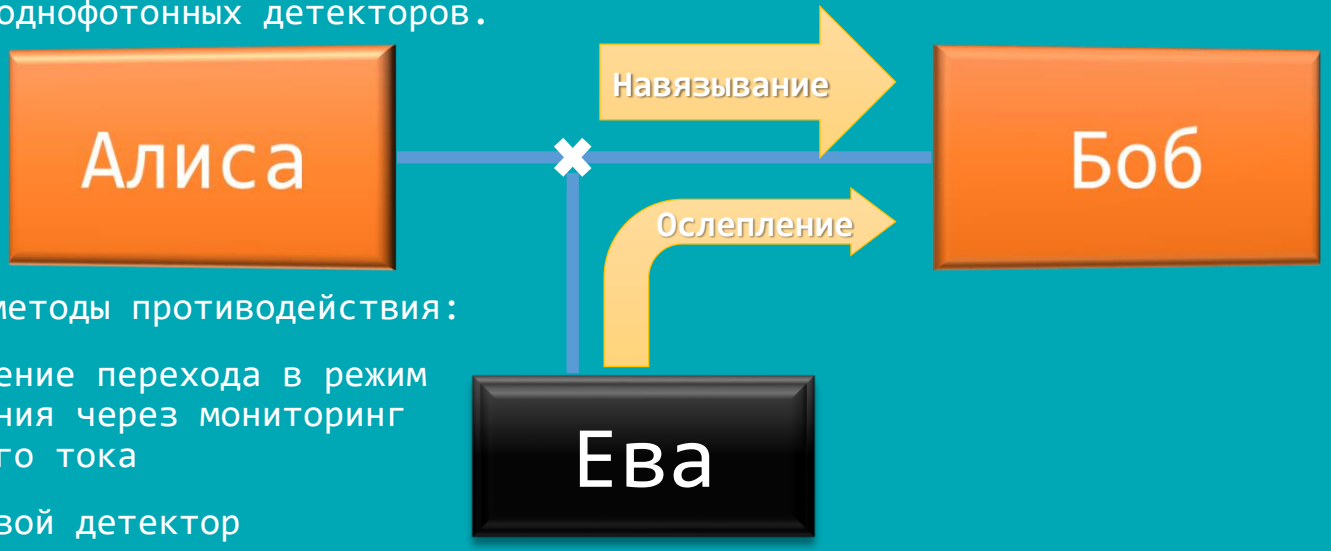




Подробнее в докладе на конференции:
Bogdanov S.A., et.al, SPIE Photonics Euro 2022, 3 - 7 April, Strasbourg, France

Импульсное и непрерывное ослепление детектора

- Детектор в состоянии ослепления не чувствителен к однофотонной компоненте и может контролироваться Евой;
- Атака приводит к полной компрометации ключа в результате особенности работы однофотонных детекторов.



Основные методы противодействия:

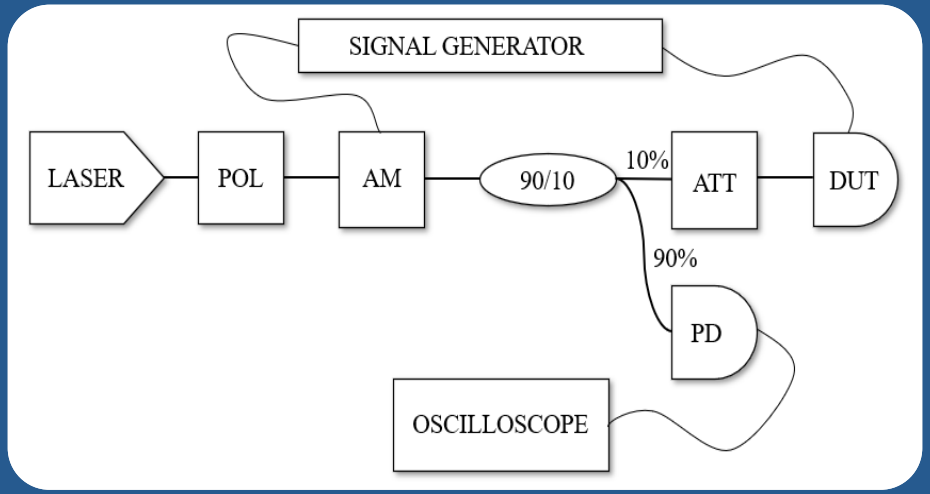
- Обнаружение перехода в режим ослепления через мониторинг лавинного тока
- Сторожевой детектор

Первая публикация об атаке:

L. Lydersen et al, Nat. Photonics, 4, 686-689 (2010)

Атака с ослеплением ЛФД системы КРК непрерывным и модулированным излучением

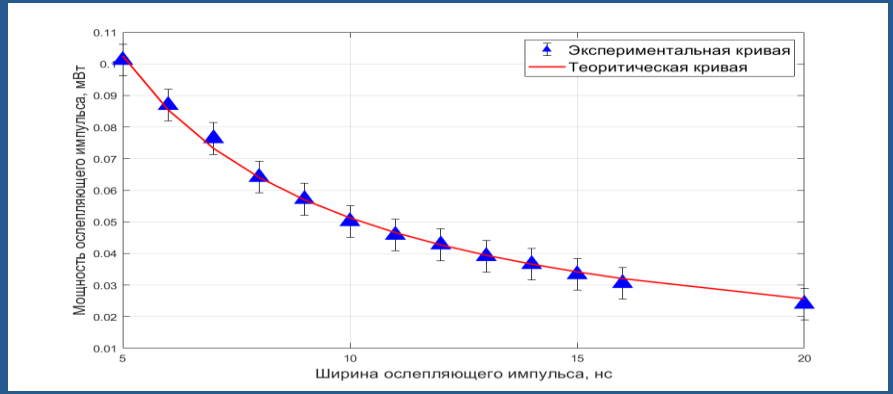
Структурная схема экспериментального стенда

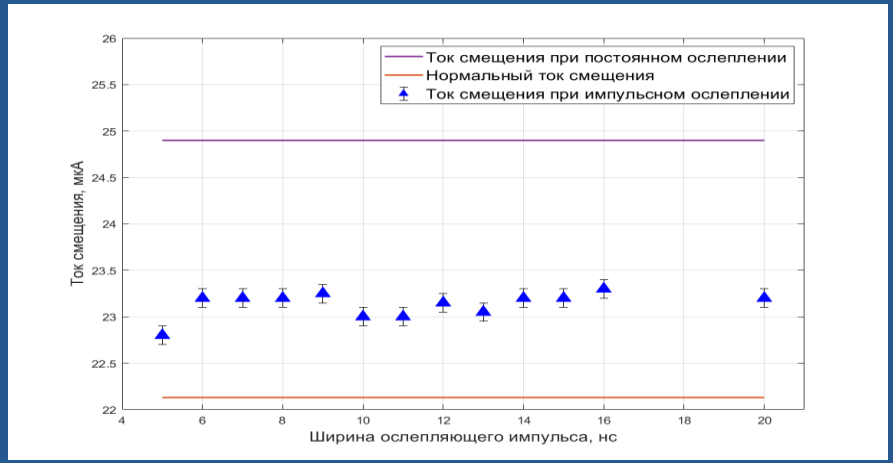


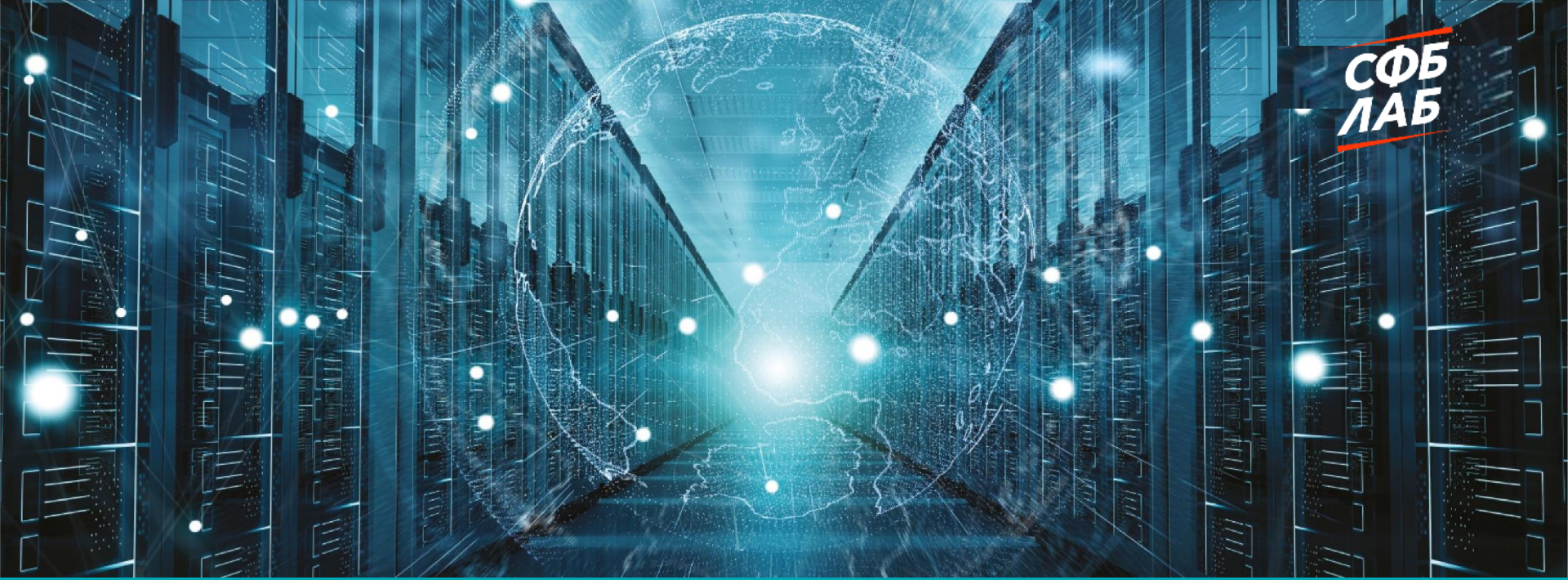
LASER- лазерный источник 1550 нм, POL - поляризатор, AM - амплитудный модулятор, оптический разветвитель 90/10 - 90/10, ATT - аттенюатор, PD - модуль широкополосного фотоприемника 20 ГГц, DUT - однофотонный лавинный диод.

Подробнее в докладе на конференции:
Bulavkin D.S. et.al, 20th International Conference Laser Optics, St. Petersburg, 20-24 June, 2022

Ток смещения в зависимости от ширины ослепляющего импульса







Выводы

Рассмотрены актуальные оптические атаки на квантовые криптографические системы выработки и распределения ключей

- Продемонстрирован способ оценки защищенности системы КРК против атаки Trojan-horse с учетом оценки рисков в широком спектральном диапазоне
- Продемонстрирована атака с лазерным воздействием на простой оптический аттенюатор, широко используемый в волоконно-оптических системах КРК
- Представлено исследование зависимостей вероятностей «backflash» от параметров ЛФД и среднего числа фотонов в импульсе
- Продемонстрирована атака с ослеплением ЛФД системы КРК непрерывным и модулированным излучением с оценкой эффективности защиты по току смещения

Вопросы

Спасибо за внимание!

Дворецкий Дмитрий Алексеевич

Ведущий специалист

e-mail: Dmitry.Dvoretsky@sfblaboratory.ru