РусКрипто

Особенности проведения анализа безопасности квантово-криптографических систем выработки и распределения ключа

Лохматов Роман Юрьевич
Ведущий специалист инженерно-квантовой лаборатории
ООО «СФБ Лаб»

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Введение

РусКрипто

- Квантово-криптографические системы выработки и распределения ключей (ККС ВРК) могут гарантировать безопасное распределение ключей при наличии побочных каналов утечки информации

- Специфика проведения анализа безопасности ККС ВРК подразумевает проведение ряда работ по обоснованию интегрального критерия секретности ключа и проверки правильности реализации квантово-криптографического протокола(ККП)

- При анализе ККС ВРК можно руководствоваться принципом, что злоумышленнику не имеет смысла проводить атаку, ведущую к обнаружению его действий.

Интегральный критерий секретности ключа

РусКрипто

В интегральном критерии секретности ключа (например, в форме оценочной длины криптографического стойкого ключа за один сеанс работы ККП) должны быть учтены потенциально актуальные для исследуемой квантовой системы атаки на техническую реализацию

В общем виде, оценочную длину секретного ключа можно представить в виде доли секретных бит:

$$l_{\text{оцен}} = 1 - QuantumLeak - ClassicLeak,$$

где $QuantumLeak$ – доля квантовой утечки информации, $ClassicLeak$ – доля классической утечки информации

Классическая утечка информации

РусКрипто

Классическая утечка информации принимает вид:

$$ClassicLeak = \frac{Leak + v}{N}$$

где N - количество бит просеянного ключа, $Leak$ – количество информации, переданной Алисой по открытому каналу при реализации процедуры исправления ошибок, v – количество информации, переданных Алисой по открытому каналу для верификации битовых последовательностей.

Величина v определяется используемым механизм верификации. При использовании хэш-кодов ключа Алисы и публичного(открытого), величина v определяется длиной выхода хэш-функции. При использовании механизма верификации на основе вычисления линейных соотношений, вычисляемых на битовой строке Алисы с помощью случайных равновероятных последовательностей, величина v равняется количеству линейных соотношений.

Классическая утечка информации

РусКрипто

Величина $Leak$ определяется количеством линейных соотношений, переданных Алисой по открытому каналу при реализации процедуры исправления ошибок, и зависит от используемой процедуры коррекции ошибок. При использовании модифицированного алгоритма* декодирования LDPC-кода классическая утечка рассчитывается по формуле:

$$Leak = M + b_p - b_s + D_{exp}$$

где M - длина LDPC-синдрома, b_p - количество «выколотых» бит (бит, принимающих случайное значения и предназначенных для оптимизации используемой LDPC-матрицы к оцененному уровню квантовой ошибки на бит в канале), b_s - количество «укороченных» бит (раскрытых бит при ошибке декодирования), D_{exp} - количество разглашенных бит для получения предполагаемого значения значение квантовой ошибки на бит (QBER).

Kiktenko E. O. et al. Journal of Russian Laser Research, 39 (2018)

Квантовая утечка информации

РусКрипто

Квантовая утечка информации используемым ККП и зависит от конкретной реализации системы. Для протокола BB84 квантовая утечка принимает вид:

$$QuantumLeak = h(Q) - \chi - m(\varepsilon, N),$$

где $h(x) \equiv -x \log_2 x - (1-x)\log_2(1-x)$ – бинарная энтропийная функция Шеннона; Q – коэффициент квантовой ошибки на бит; χ – величина Холево для побочных каналов утечки, соответствующая границе классической информации, которую можно извлечь из квантовой системы; m – поправка на конечную длину вырабатываемого ключа; ε - параметр секретности*; N - количество бит просеянного ключа.

Величина $h(Q)$ позволяет учесть коллективную атаку на квантовые состояния в канале связи. В случае использования протоколов с независимыми посылками, данная величина позволяет учесть когерентную атаку

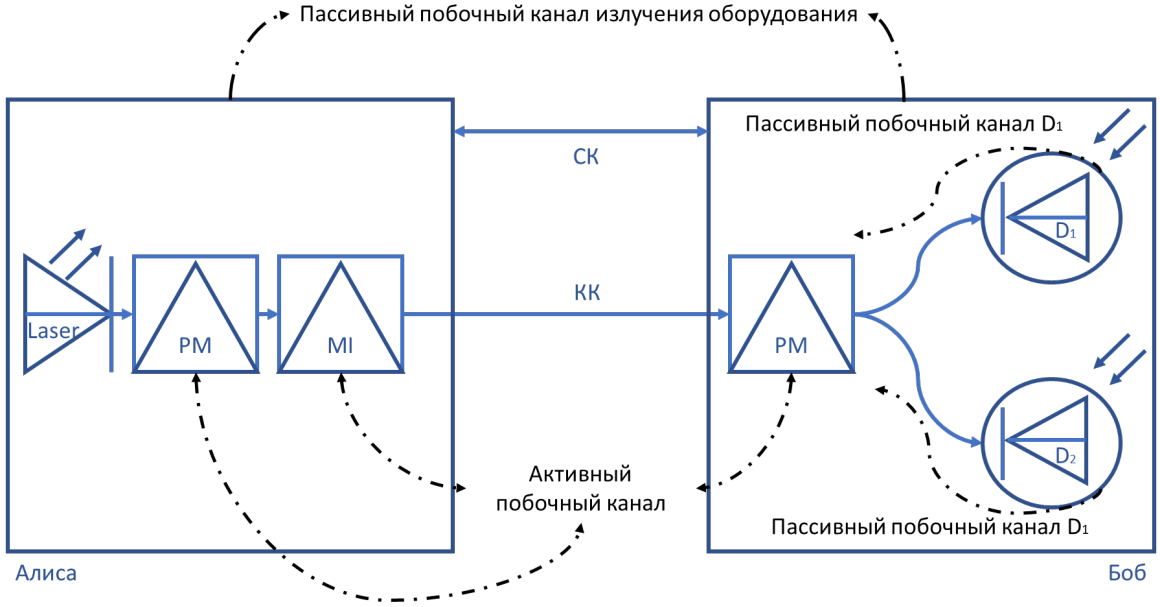
*Renner, R. International Journal of Quantum Information, 6(01) (2008)

Побочные каналы утечки информации

РусКрипто

В системах КРК присутствуют побочные каналы, считывание с которых не приводит к росту ошибки у приемной станции.

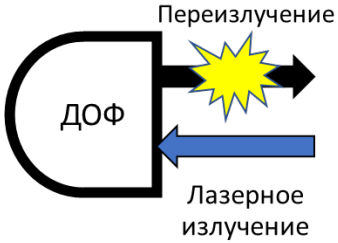
Для учета побочных каналов необходимы модельные соображения для расчета величины Холево



Побочные каналы утечки информации

РусКрипто

Электролюминисценция атака Backflash



$$\chi_{bf}\left(P_D^{0,1}\right)^{*}$$

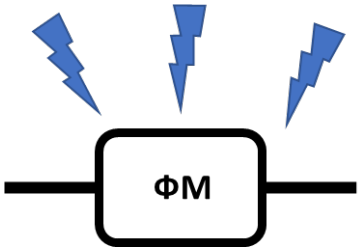
где $P_D^{0,1}$ - распределение числа фотонов при переизлучении детекторов при генерации аппаратурой 0 или 1

Отражение зондирующего импульса атака Троянский конь

$$\chi_{TH}\left(\mu_{\text{отр}}\right)^{**}$$

где $\mu_{\text{отр}}$ - среднее число фотонов в отраженном зондирующем сигнале

Радиоизлучение аппаратуры



$$\chi_{p}\left(P_{GX,GY}^{0,1}\right)^{*}$$

где $P_{GX,GY}^{0,1}$ - распределение сигнала в побочном канале при генерации аппаратурой 0 или 1

*Молотков С. Н., ЖЭТВ (2021)

**Sushchev I. S. et al. Phys. Rev. Appl., 22(3), 034032 (2024)

Интегральный критерий секретности ключа

РусКрипто

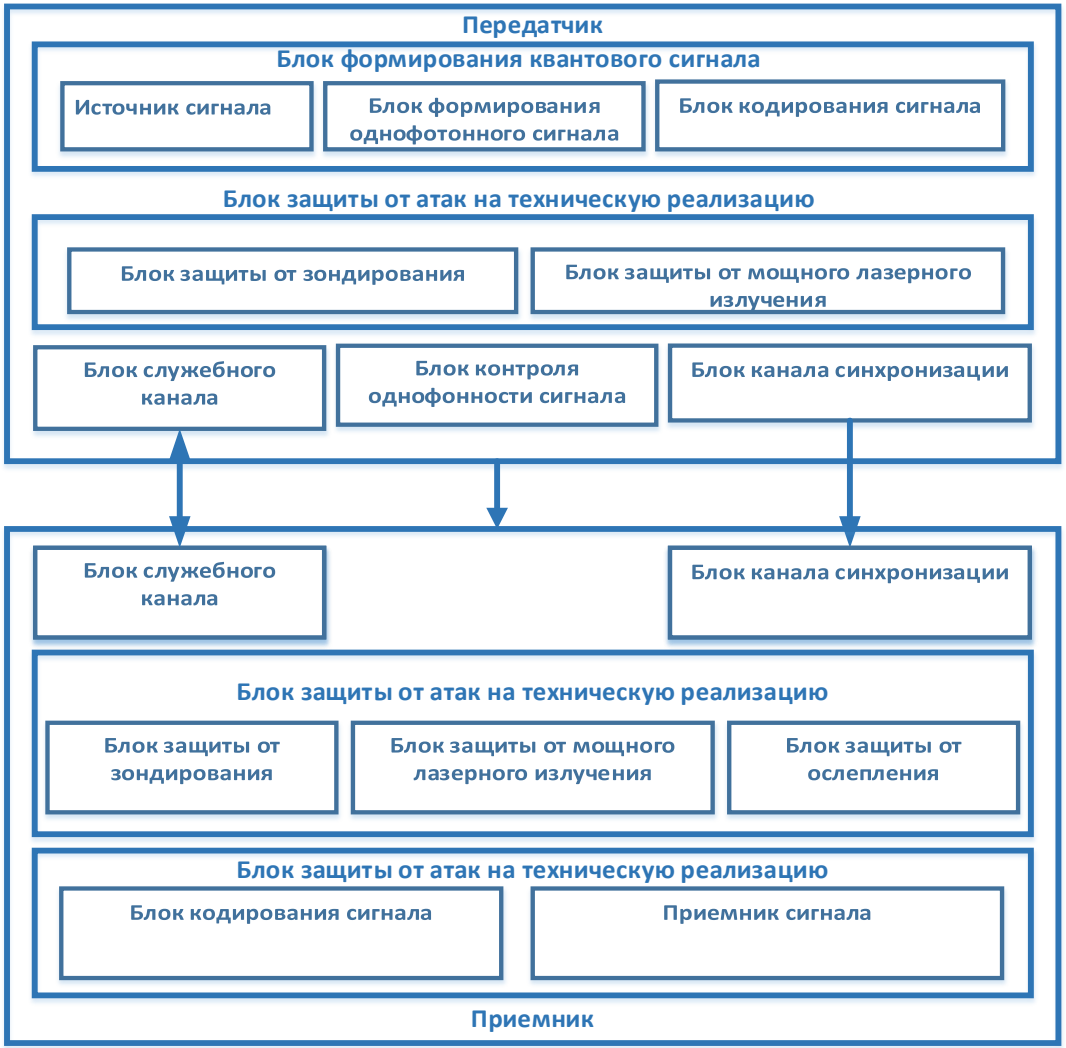
Оценочная длина секретного ключа представляется в виде :

$$l_{\text{оцен}} = 1 - h(Q) - \chi_{bf}\left(P_D^{0,1}\right) - \chi_{TH}\left(\mu_{\text{отр}}\right) - \chi_p\left(P_{GX,GY}^{0,1}\right) - m(\varepsilon, N) - \frac{Leak + v}{N}$$

В случае использования неоднофотонных источников длина секретного ключа в битах принимает вид:

$$l = N \cdot \lambda\left(1 - h(Q) - \chi_{bf}\left(P_D^{0,1}\right) - \chi_{TH}\left(\mu_{\text{отр}}\right) - \chi_{bf}\left(P_{GX,GY}^{0,1}\right) - m(\varepsilon, N)\right) - Leak - v$$

где λ-доля однофотонной компоненты, определяемая с помощью состояний-«ловушек» (метод decoy-state)


Передатчик
Блок формирования квантового сигнала
Источник сигнала
Блок формирования однофотонного сигнала
Блок кодирования сигнала
Блок защиты от атак на техническую реализацию
Блок защиты от зондирования
Блок защиты от мощного лазерного излучения
Блок служебного канала
Блок контроля однофонности сигнала
Блок канала синхронизации
Блок служебного канала
Блок канала синхронизации
Блок защиты от атак на техническую реализацию
Блок защиты от зондирования
Блок защиты от мощного лазерного излучения
Блок защиты от ослепления
Блок защиты от атак на техническую реализацию
Блок кодирования сигнала
Приемник сигнала
Приемник

РусКрипто

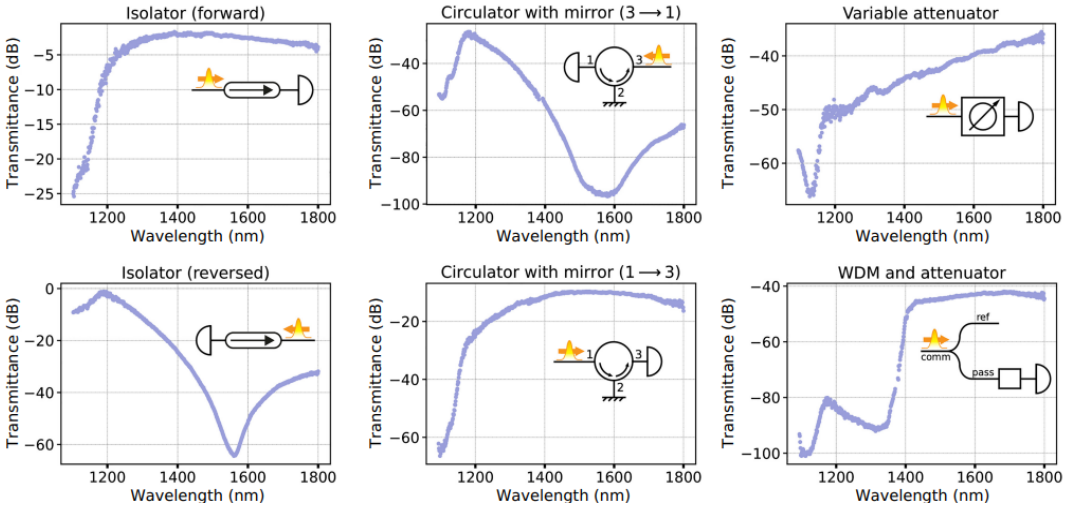
Блок защиты от зондирования

РусКрипто

Элементы защиты:

1. Изолятор
2. Циркулятор
3. Спектральные фильтр
4. Аттенюатор
5. Сторожевые детектор

Спектр пропускания оптических компонентов*



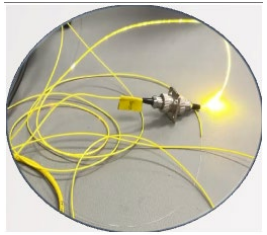
*Sushchev I. S. et al. Phys. Rev. Appl., 22(3), 034032 (2024)

Блок защиты от мощного лазерного излучения

РусКрипто

Элементы защиты:

1. Элементы, невосприимчивые к мощному лазерному излучению
2. Легкоплавкие предохранители



Патент № 2814062

Ponosova, V. Makarov, et al. // PRX Quantum 3, 040307 (2022).

Патент № 215524

V. G. Krishtop, K. E. Bugai, et al. // IV SNAIA. (2021)

Заключение

РусКрипто

- Интегральный критерий секретности зависит от квантовой и классической утечки информации. Квантовая утечка информации определяется конкретными характеристиками системы, в том числе побочными каналами, длиной ключевой последовательности и параметрами квазиоднофотонного источника.
- Соблюдение критерия секретности зависит от соответствия компонентов системы заданным параметрам, нарушение которых ведет к неправильной оценки доли бит секретного ключа, доступного злоумышленнику. В связи с чем необходимо обеспечивать систему механизмами контроля и обнаружения выхода параметров из заранее определенных границ.
- Качественный контроль и учет параметров компонентов системы может ограничить потенциальное воздействия нарушителя на ККС КРК.

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ