Стойкость квантовой криптографии при несовпадающих эффективностях однофотонных детекторов

Антон Трушечкин

Математический институт им. В.А. Стеклова РАН
Российский квантовый центр

Институт физики твердого тела РАН
Семинар «Квантовые вычисления»
11 декабря 2019 г.

Основной результат

Доказана стойкость протокола квантовой криптографии BB84 при несовпадающих эффективностях однофотонных детекторов и получена предельная скорость генерации секретного ключа.

M. Bochkov, A.T. “Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds”, Phys. Rev. A **99**, 032308 (2019); arXiv: 1810.04663.

Квантовая криптография

- Цель квантовой криптографии: две стороны, разделённые расстоянием, должны сгенерировать общий секретный ключ (случайную последовательность из нулей и единиц).

00111011001

Юстас

Алекс

- Имея общий секретный ключ, стороны могут обмениваться секретными сообщениями. Построение шифров и передача секретных сообщений при имеющемся ключе — задача классической (не квантовой) криптографии.

- Квантовая криптография = квантовое распределение ключей

Квантовая криптография vs Криптография с открытым ключом (1)

- В настоящее время задача распределения ключей решается при помощи криптографии с открытым ключом (сложность факторизации целых чисел, дискретного логарифмирования).
- Находится под угрозой в связи с перспективой появления квантового компьютера или эффективных классических алгоритмов.

Квантовая криптография vs Криптография с открытым ключом (2)

- В квантовой криптографии передаваемая информация кодируется в квантовые состояния.
- Стойкость обеспечивается за счёт невозможности (в общем случае) «прочитать» квантовое состояние, не испортив его. Благодаря этому попытка прослушивания обнаруживается.
- Квантовая криптография обеспечивает стойкость без каких-либо предположений о вычислительных мощностях и технологиях противника: он ограничен лишь законами природы.

Протокол BB84 (Bennett, Brassard, 1984)

Два базиса в пространстве $\mathbb{C}^2$:

- Базис z: $|0\rangle$ кодирует бит 0, $|1\rangle$ кодирует бит 1.

  Используется для формирования ключа.
- Базис x: $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ кодирует бит 0,
  $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ кодирует бит 1.

  Используется для проверки вмешательства противника.
  Выбирается с малой вероятностью.

Если противник измеряет одно из состояний $|\pm\rangle$ в базисе z, то с вероятностью $1/2$ возникает ошибка.

Доказательство стойкости

Mayers, 1996

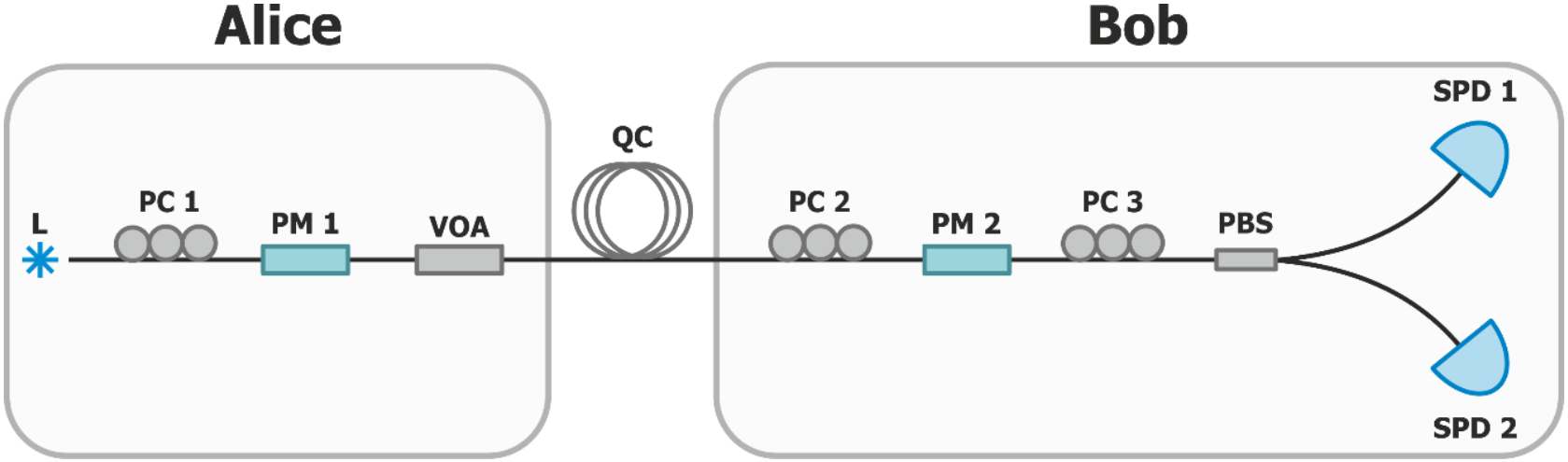
Shor, Preskill, 2000

Renner, 2005

Tomamichel, Lim, Gisin, Renner, 2012; Tomamichel, Leverrier, 2017: энтропийные соотношения неопределённостей

В настоящее время: доказательства стойкости при реалистичных предположениях об аппаратуре.

Проблема эффективностей однофотонных детекторов



Duplinskiy et al. Optics Express 25, 28886 (2017)

Упомянутые выше доказательства не работают, если эффективности однофотонных детекторов не совпадают.

Квантовая эффективность однофотонного детектора η: вероятность регистрации фотона.

Детектор на основе лавинного фотодиода: $\eta \approx 0.1$
Детектор на основе сверхпроводника: $\eta \approx 0.9$

Практически невозможно изготовить два детектора с равными эффективностями.

Важность этой проблемы отмечена на QCrypt 2019.

Модель измерения с неидеальными детекторами

η_0 — эффективность детектора «0»
η_1 — эффективность детектора «1»

Пусть $0 < \eta_1 < \eta_0 \leq 1$.

Общие потери η_0 на обоих детекторах можно отнести к потерям в канале и считать, что

детектор «0» обладает эффективностью единица,
детектор «1» — эффективностью $\eta = \eta_0/\eta_1$.

Известные результаты

- Fung, Tamaki, Qi, Lo, Ma, Quant. Inf. Comput. 9, 131 (2009): скорость генерации секретного ключа далека от оптимальной
- Winick, Lütkenhaus, Coles, Quantum 2, 77 (2018): точные численные оценки, но не аналитическая формула, что затрудняет дальнейшую работу с этой формулой (например, обобщение на случай не однофотонных, а когерентных импульсов)

Наш метод:

Используем сведение задачи нахождения предельной скорости генерации к задаче выпуклой оптимизации (минимизации квантовой относительной энтропии когерентности), разработанное в статье Winick, Lütkenhaus, Coles, но решаем задачу аналитически.

Эквивалентная схема протокола

Приготовление состояний Алисой можно математически эквивалентно представить как приготовление сцепленного состояния

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) = \frac{1}{\sqrt{2}}(|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B)$$

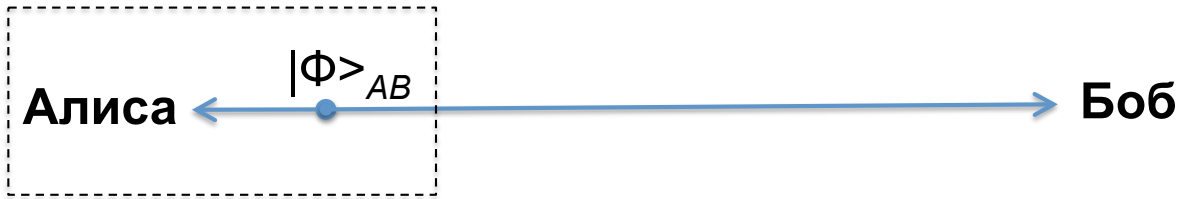
и измерение Алисой своей подсистемы в соответствующем базисе

Эквивалентная схема протокола

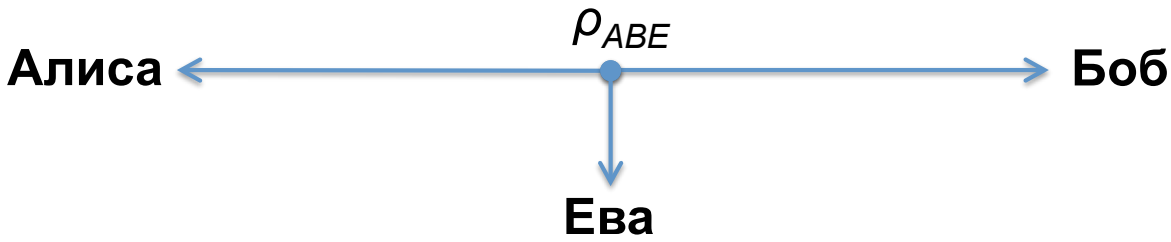
Приготовление состояний Алисой можно математически эквивалентно представить как приготовление сцепленного состояния

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) = \frac{1}{\sqrt{2}}(|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B)$$

и измерение Алисой своей подсистемы в соответствующем базисе



Атака противника: замена сцепленного состояния $|\Phi\rangle_{AB}\langle\Phi|$ на другое произвольное состояние ρ_{ABE}.



Задача для Алисы и Боба: по наблюдаемой статистике определить информационные характеристики неизвестного состояния (родственно задаче томографии).

Предельная скорость генерации секретного ключа

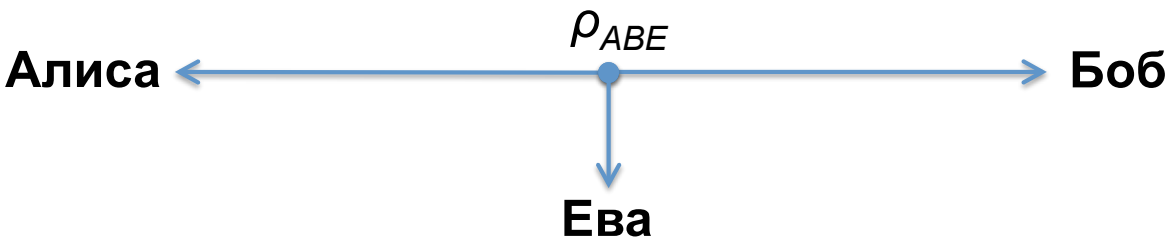
Неформальное определение: $R = \lim\limits_{N\to\infty} k/N$,

N — число посылок,
k — максимально возможное число битов в конечном ключе при условиях:

а) Ключи Алисы и Боба совпадают с точностью до бесконечно малой вероятности (при $N \to \infty$),

б) Информация Евы о ключах бесконечно мала.

Предельная скорость генерации секретного ключа (2)

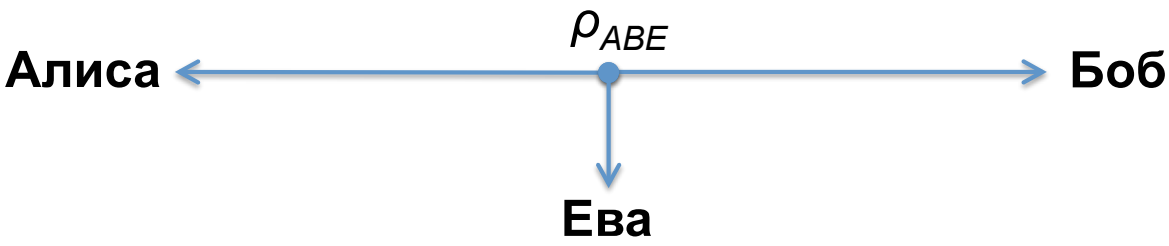


$$\boxed{R = H(A|E) - H(A|B)}$$

Неформально:

$$R = \text{Степень незнания Евы} - \text{Степень незнания Боба}$$

Предельная скорость генерации секретного ключа (2)



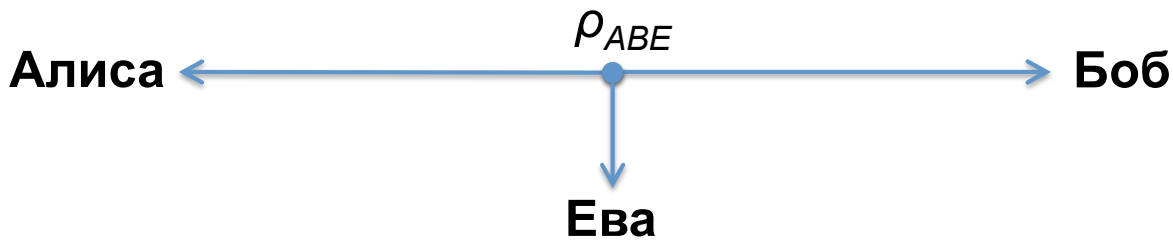
$$\boxed{R = H(A|E) - H(A|B)}$$

Неформально:

$$R = \text{Степень незнания Евы} - \text{Степень незнания Боба}$$

- $H(A|E) = H(\widetilde{\rho}_{AE}) - H(\widetilde{\rho}_{E}), \quad H(\rho) = -\operatorname{Tr} \rho \log_2 \rho,$
  - $\widetilde{\rho}_{ABE} = G \rho_{ABE} G^{\dagger}$ — затухание в неидеальном детекторе (G — на следующем слайде).

Предельная скорость генерации секретного ключа (2)



$$\boxed{R = H(A|E) - H(A|B)}$$

Неформально:

$$R = \text{Степень незнания Евы} - \text{Степень незнания Боба}$$

- $H(A|E) = H(\widetilde{\rho}_{AE}) - H(\widetilde{\rho}_E), \quad H(\rho) = -\operatorname{Tr} \rho \log_2 \rho,$
  - $\widetilde{\rho}_{ABE} = G \rho_{ABE} G^\dagger$ — затухание в неидеальном детекторе (G — на следующем слайде).
- $H(A|B) \leq h(Q_z)$,
  - Q_z — процент ошибок в базисе z (QBER — quantum bit error rate),
  - $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ — двоичная энтропия.
- Оценка $H(A|E)$ — ключевой момент.

Предельная скорость генерации секретного ключа (2)

$$\boxed{H(A|E) = \min_{\rho_{AB} \in \mathbf{S}} D\big(G\rho_{AB}G^\dagger \| \mathscr{Z}(G\rho_{AB}G^\dagger)\big)}$$

$D(\rho\|\sigma) = \operatorname{Tr}\rho\log\rho - \operatorname{Tr}\rho\log\sigma$ — квантовая относительная энтропия

Пространство Алисы: $\mathbb{C}^2 \ni \{|0\rangle, |1\rangle\}$;
Пространство Боба: $\mathbb{C}^3 \ni \{|0\rangle, |1\rangle, |\mathrm{vac}\rangle\}$

$$G = I_A \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\eta} & 0 \\ 0 & 0 & 0 \end{pmatrix} = I_A \otimes (|0\rangle\langle 0| + \sqrt{\eta}\,|1\rangle\langle 1|),$$

$$\mathscr{Z}(\rho_{AB}) = \sum_{a\in\{0,1\}} (|a\rangle_A\langle a| \otimes I_B)\,\rho_{AB}\,(|a\rangle_A\langle a| \otimes I_B),$$

$$p_{\mathrm{det}} = \operatorname{Tr}(G\rho_{AB}G^\dagger) = \operatorname{Tr}\mathscr{Z}(G\rho_{AB}G^\dagger).$$

Ограничения (наблюдаемая статистика регистраций)

$$\boxed{H(A|E) = \min_{\rho_{AB} \in \mathbf{S}} D\big(G\rho_{AB}G^\dagger \| \mathscr{Z}(G\rho_{AB}G^\dagger)\big)}$$

S: положительные операторы ρ_{AB}, удовлетворяющие следующим ограничениям:

$$\begin{aligned}
\mathrm{Tr}[(I_A \otimes |0\rangle_B \langle 0|)\rho_{AB}] &= p_0, \\
\mathrm{Tr}[(I_A \otimes \eta\,|1\rangle_B \langle 1|)\rho_{AB}] &= p_1, \\
\eta\,\mathrm{Tr}[(|-+\rangle\langle -+|\,\rho_{AB})] + \mathrm{Tr}[(\eta\,|+-\rangle\langle +-|)\rho_{AB}] &= t\eta Q_x,
\end{aligned}$$

p_0, p_1 — вероятности детектирования 0 и 1 в z-базисе,
$p_{\mathrm{det}} = p_0 + p_1$ — общая вероятность детектирования в z-базисе,
$t = p_0 + p_1/\eta$ — пропускание линии связи,
Q_x — доля ошибок (QBER) в x-базисе

Теорема о предельной скорости генерации

Указанная задача оптимизации имеет допустимые решения (т.е. решения, удовлетворяющие ограничениям) тогда и только тогда, когда

$$Q_x \geq \frac{1}{2} - \frac{1}{t}\sqrt{\frac{p_0 p_1}{\eta}}. \qquad (1)$$

В этом случае оптимальное значение целевой функции есть

$$R = p_{\mathrm{det}} \left[h\left(\frac{1-\delta_z}{2}\right) - h\left(\frac{1-\sqrt{\delta_z^2+\delta_x^2}}{2}\right) - h(Q_z) \right],$$

где

$$\delta_z = \frac{p_0 - p_1}{p_{\mathrm{det}}}, \quad \delta_x = \frac{(1-2Q_x)\sqrt{\eta}}{p_{\mathrm{det}}}.$$

Предельные случаи

$$R = p_{\mathrm{det}} \left[h\left(\frac{1-\delta_z}{2}\right) - h\left(\frac{1-\sqrt{\delta_z^2+\delta_x^2}}{2}\right) - h(Q_z) \right],$$

- Идеальные детекторы: $R = t[1 - h(Q_x) - h(Q_z)]$.
  При $Q_x = Q_z = Q$ критическая доля ошибок: $Q_{\mathrm{crit}} \approx 11\%$
  ($R > 0$ при $Q < Q_{\mathrm{crit}}$)

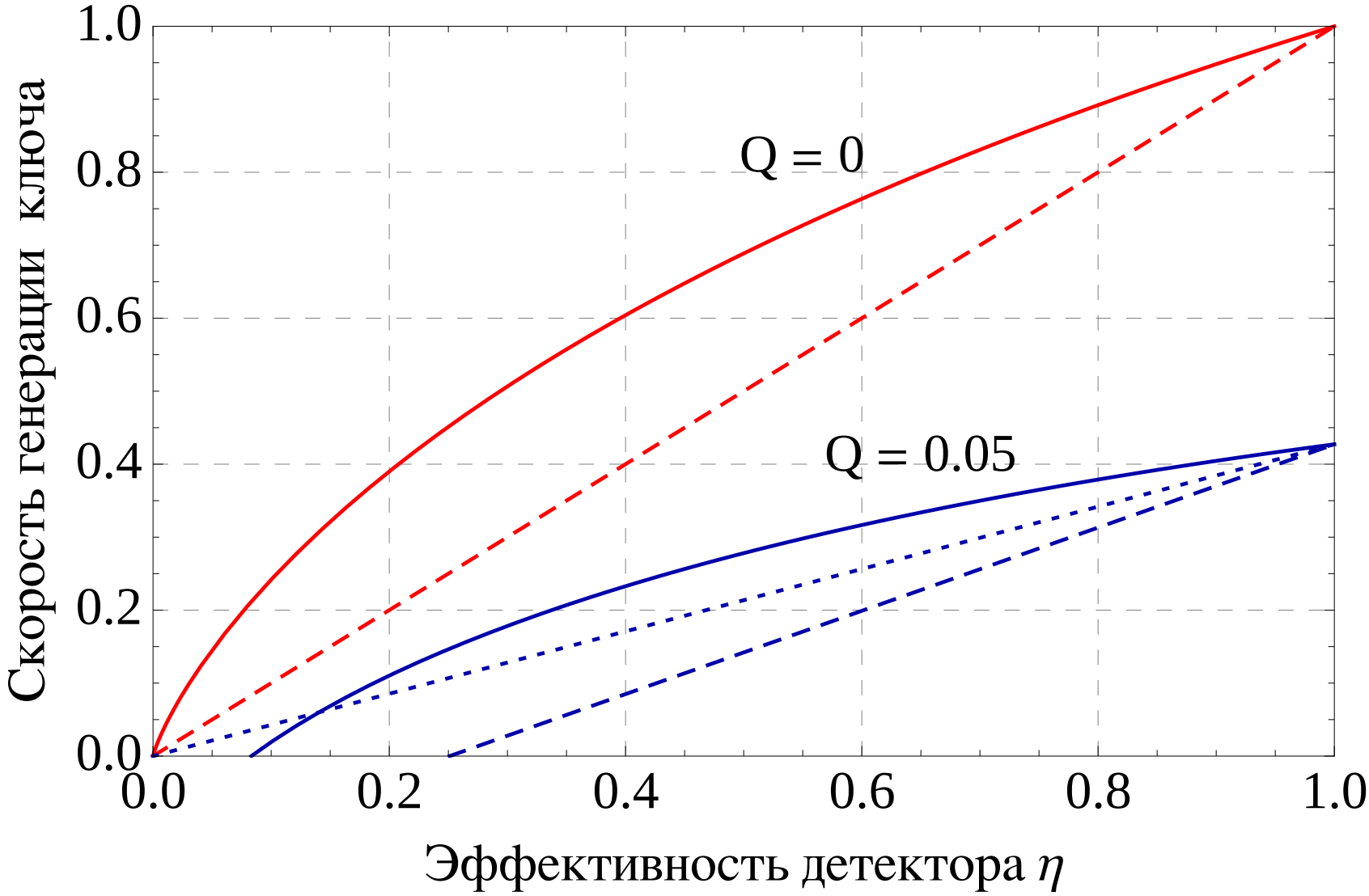
Предельные случаи

$$R = p_{\mathrm{det}} \left[h\left(\frac{1-\delta_z}{2}\right) - h\left(\frac{1-\sqrt{\delta_z^2+\delta_x^2}}{2}\right) - h(Q_z) \right],$$

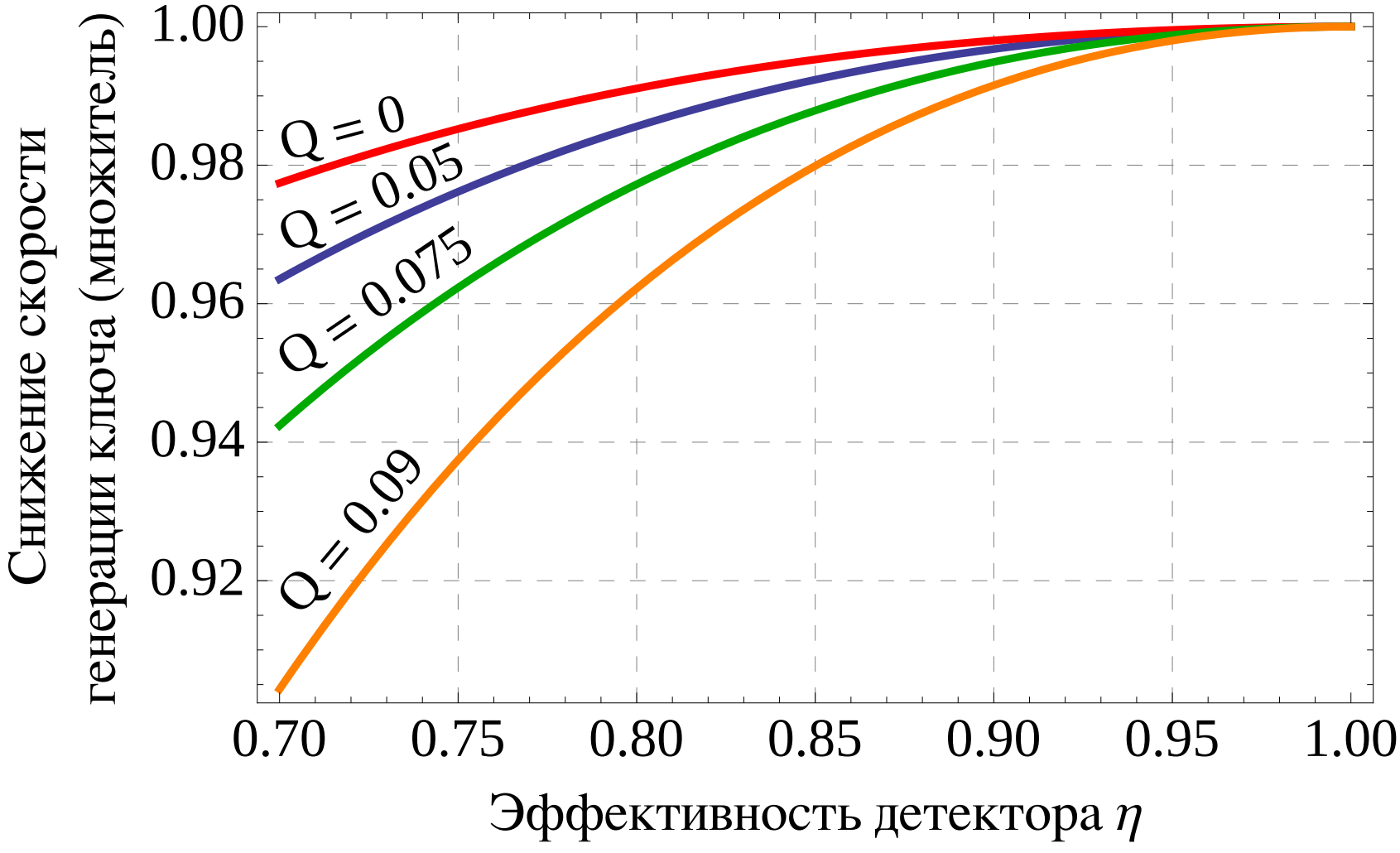
- Идеальные детекторы: $R = t[1 - h(Q_x) - h(Q_z)]$.
  При $Q_x = Q_z = Q$ критическая доля ошибок: $Q_{\mathrm{crit}} \approx 11\%$
  ($R > 0$ при $Q < Q_{\mathrm{crit}}$)

- Бесшумный канал ($Q_x = Q_z = 0$):

$$R = p_{\mathrm{det}} h\left(\frac{p_0}{p_0+p_1}\right) = p_{\mathrm{det}} h\left(\frac{1}{1+\eta}\right).$$



Сплошная ———: наша формула
Штриховая - - - - : Fung et al.
Пунктирная .....: отбрасывание части нулей



Сравнение со случаем совпадающих эффективностей, равных $(\eta_0 + \eta_1)/2$

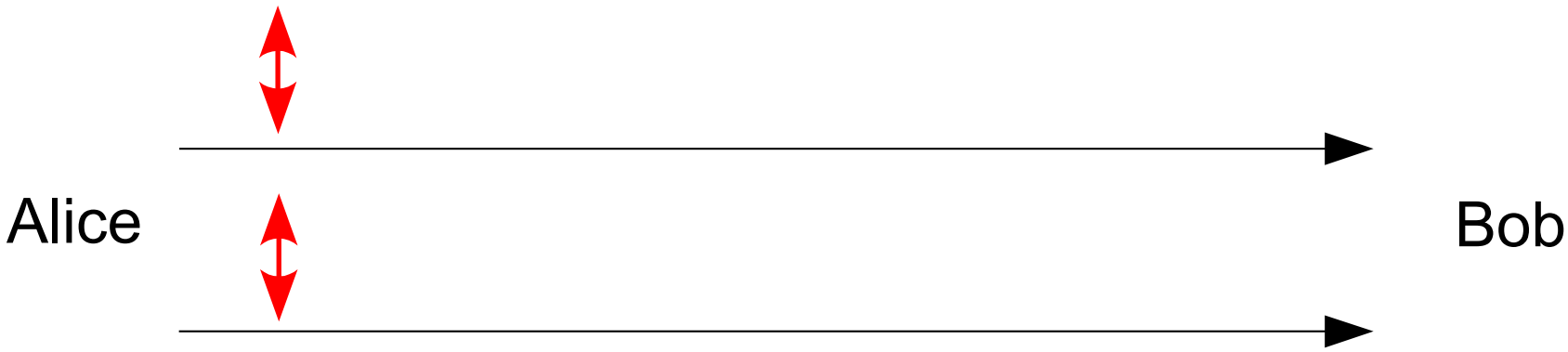
Часть 2: Адаптация метода обманных состояний к случаю несовпадающих эффективностей детекторов

Двухфотонные посылки ненадёжны

Слабый когерентный импульс с рандомизированной фазой:

$$\rho(\mu,\sigma) = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n,\sigma\rangle \langle n,\sigma| ,$$

μ — интенсивность импульса, $\mu < 1$,
$|n,\sigma\rangle$ — состояние с n фотонами поляризации σ.

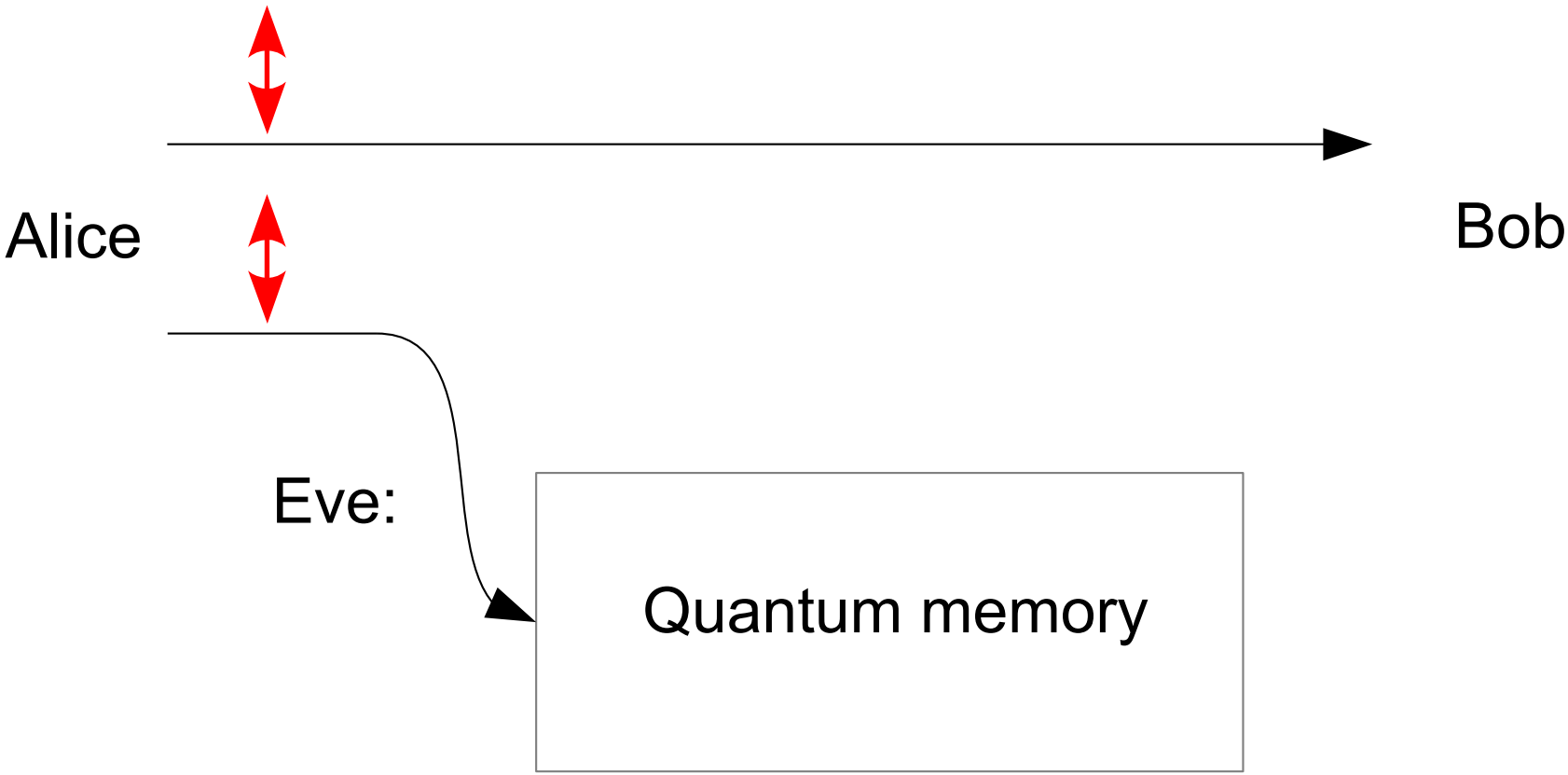


Двухфотонные посылки ненадёжны

Слабый когерентный импульс с рандомизированной фазой:

$$\rho(\mu,\sigma) = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n,\sigma\rangle \langle n,\sigma| ,$$

μ — интенсивность импульса, $\mu < 1$,
$|n,\sigma\rangle$ — состояние с n фотонами поляризации σ.

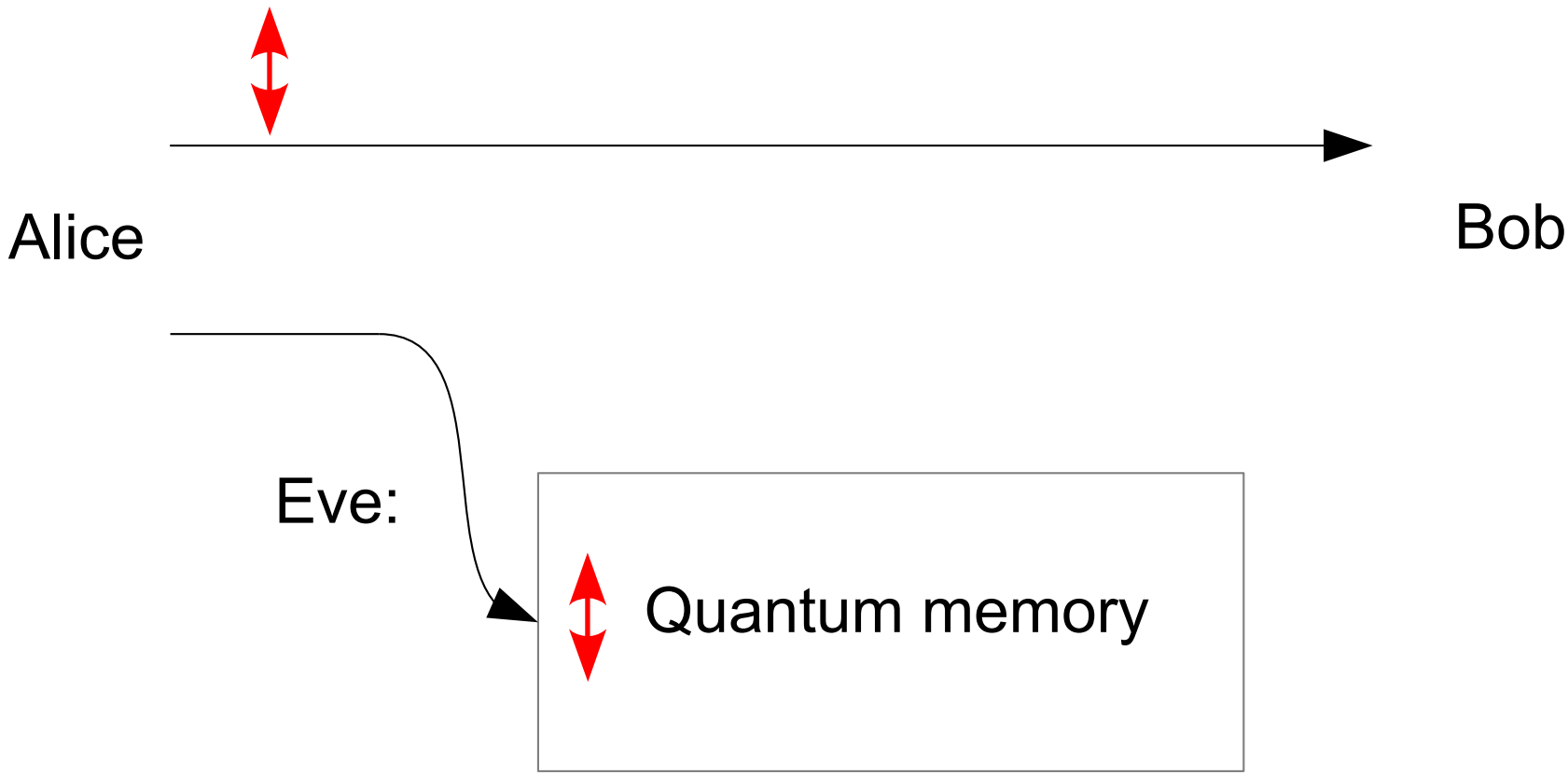


Двухфотонные посылки ненадёжны

Слабый когерентный импульс с рандомизированной фазой:

$$\rho(\mu,\sigma) = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n,\sigma\rangle \langle n,\sigma| ,$$

μ — интенсивность импульса, $\mu < 1$,
$|n,\sigma\rangle$ — состояние с n фотонами поляризации σ.



Сведение многофотонного случая к однофотонному

$$\rho(\mu,\sigma) = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\left|n,\sigma\right\rangle\left\langle n,\sigma\right|,$$

Φ — произвольный квантовый канал (линейное, вполне положительное, не увеличивающее след отображение), описывающее любые действия противника и затухание в неидеальном детекторе.

$$\frac{1}{2}\sum_{\sigma=0}^{1}\left|\sigma\right\rangle_A\left\langle\sigma\right|\otimes\rho(\mu,\sigma)\mapsto\frac{1}{2}\sum_{\sigma=0}^{1}\left|\sigma\right\rangle_A\left\langle\sigma\right|\otimes\Phi(\rho(\mu,\sigma))=$$

$$=\frac{1}{2}\sum_{\sigma=0}^{1}\left|\sigma\right\rangle_A\left\langle\sigma\right|\otimes e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\Phi(\left|n,\sigma\right\rangle\left\langle n,\sigma\right|)\equiv$$

$$\equiv\sum_{n=0}^{\infty}P_n^z\widetilde{\rho}_{ABE}^{(n)},$$

Сведение многофотонного случая к однофотонному

$$\rho(\mu,\sigma) = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\left|n,\sigma\right\rangle\left\langle n,\sigma\right|,$$

Φ — произвольный квантовый канал (линейное, вполне положительное, не увеличивающее след отображение), описывающее любые действия противника и затухание в неидеальном детекторе.

$$\frac{1}{2}\sum_{\sigma=0}^{1}\left|\sigma\right\rangle_A\left\langle\sigma\right|\otimes\rho(\mu,\sigma)\mapsto\frac{1}{2}\sum_{\sigma=0}^{1}\left|\sigma\right\rangle_A\left\langle\sigma\right|\otimes\Phi(\rho(\mu,\sigma))=$$

$$=\frac{1}{2}\sum_{\sigma=0}^{1}\left|\sigma\right\rangle_A\left\langle\sigma\right|\otimes e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}\Phi(\left|n,\sigma\right\rangle\left\langle n,\sigma\right|)\equiv$$

$$\equiv\sum_{n=0}^{\infty}P_n^z\widetilde{\rho}_{ABE}^{(n)},$$

$$P_n^z = e^{-\mu}\frac{\mu^n}{n!}\cdot\frac{1}{2}\,\mathrm{Tr}[\Phi(\left|n,0\right\rangle\left\langle n,0\right|)+\Phi(\left|n,1\right\rangle\left\langle n,1\right|)]$$

— совместная вероятность того, что посылка содержит n фотонов, и того, что она будет зарегистрирована при измерении в базисе z.

Сведение многофотонного случая к однофотонному (2)

$$\widetilde{\rho}_{ABE} = \sum_{n=0}^{\infty} P_n^z \widetilde{\rho}_{ABE}^{(n)}$$

$$H(A|E) \geq P_n^z \sum_{n=0}^{\infty} H(A|E)_{(n)} \geq P_1^z H(A|E)_{(1)} \qquad (2)$$

Сведение многофотонного случая к однофотонному (2)

$$\widetilde{\rho}_{ABE} = \sum_{n=0}^{\infty} P_n^z \widetilde{\rho}_{ABE}^{(n)}$$

$$H(A|E) \geq P_n^z \sum_{n=0}^{\infty} H(A|E)_{(n)} \geq P_1^z H(A|E)_{(1)} \qquad (2)$$

- $H(A|E)_{(1)}$ — формула, которая была прежде (для однофотонного случая)
- Для эффективной оценки P_1^z и величин, необходимых для оценки $H(A|E)_{(1)}$ (т.е. относящихся только к однофотонным посылкам), используется *метод обманных состояний* (состояний-ловушек, decoy state method).

NB: Оценка (2) универсальна и не зависит от вида атаки.

Метод обманных состояний

- Используем три интенсивности: $0 \leq \lambda < \nu < \mu$
- μ — сигнальная интенсивность, используется для формирования ключа
- ν и λ — обманные интенсивности, используются для оценки количества позиций в просеянном ключе, полученных из однофотонных посылок

Суть:

- Сбор статистики регистраций по каждой интенсивности в отдельности дает дополнительные уравнения для оценки искомых неизвестных
- Противник не знает, какая интенсивность была использована, он видит только количество фотонов

Метод обманных состояний

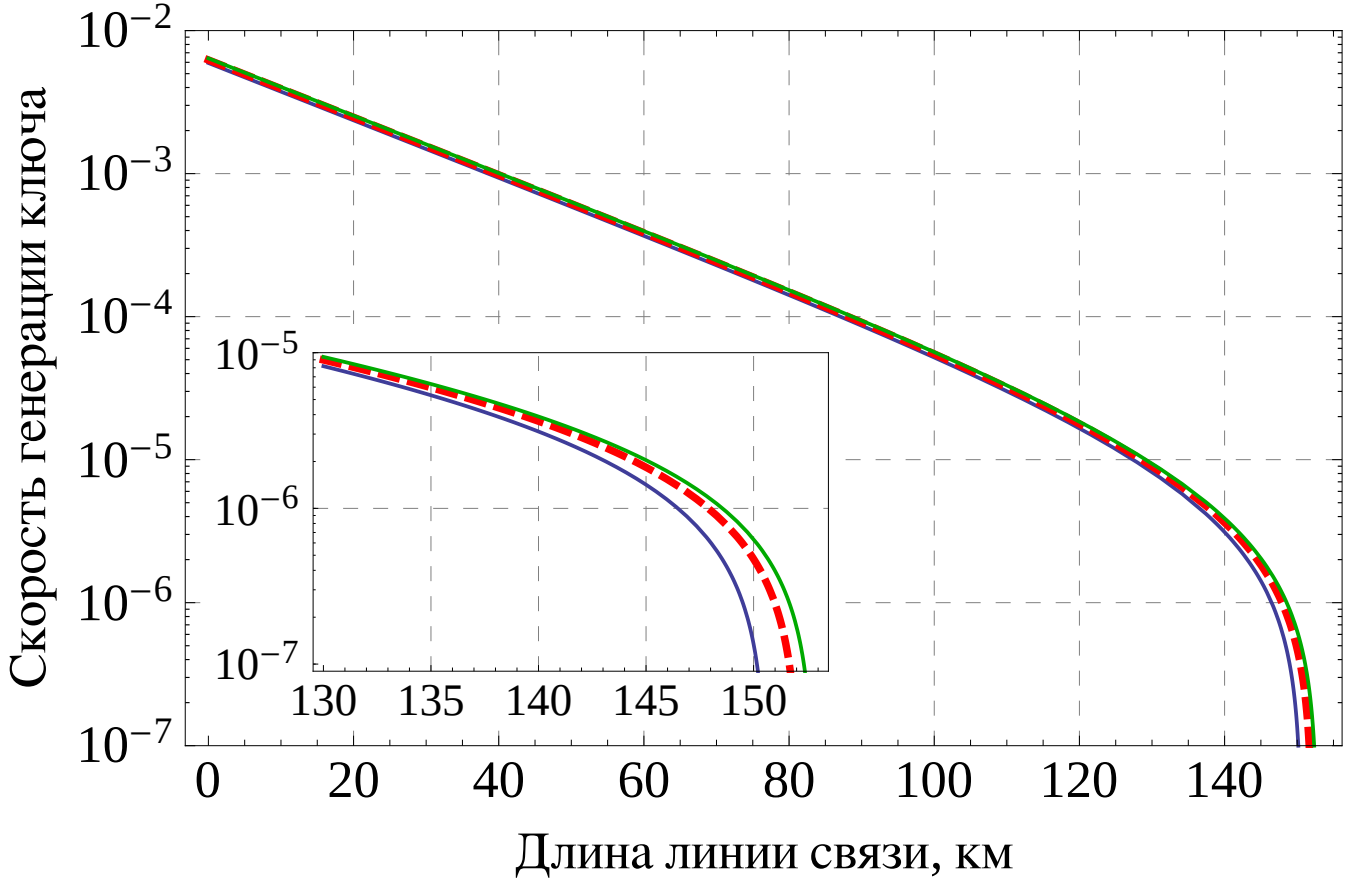
- Используем три интенсивности: $0 \leq \lambda < \nu < \mu$
- μ — сигнальная интенсивность, используется для формирования ключа
- ν и λ — обманные интенсивности, используются для оценки количества позиций в просеянном ключе, полученных из однофотонных посылок

Суть:

- Сбор статистики регистраций по каждой интенсивности в отдельности дает дополнительные уравнения для оценки искомых неизвестных
- Противник не знает, какая интенсивность была использована, он видит только количество фотонов

- **Адаптация к случаю несовпадающих эффективностей детекторов: сбор статистики отдельно по каждому базису и по каждому исходу измерения**

Расчёт по методу обманных состояний



Синяя линия: достижимая скорость по нашей формуле

Красная штриховая линия: предельно достижимая скорость

Зелёная линия: предельно достижимая скорость для случая детекторов с совпадающими эффективностями, равными $(\eta_0 + \eta_1)/2$

Открытые вопросы

- Противник может добавлять фотоны и через это влиять на вероятность детектирования
- Противник может управлять эффективностями детекторов

Заключение

Доказана стойкость протокола квантовой криптографии BB84 при несовпадающих эффективностях однофотонных детекторов и получена предельная скорость генерации секретного ключа.

Метод обманных состояний адаптирован для случая несовпадающих эффективностей детекторов.

M. Bochkov, A.T. “Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds”, Phys. Rev. A **99**, 032308 (2019); arXiv: 1810.04663.

Поддержано грантом РНФ №17-11-01388

Спасибо за внимание!