Оценка эффективности атаки «Trojan Horse» для протокола квантового распределения ключей на геометрически однородных квантовых состояниях

Гузаирова Д.М. (ООО «СФБ Лаб»)
Сущев И.С. (ООО «СФБ Лаб»; Центр квантовых технологий, физический факультет МГУ им. М. В. Ломоносова)

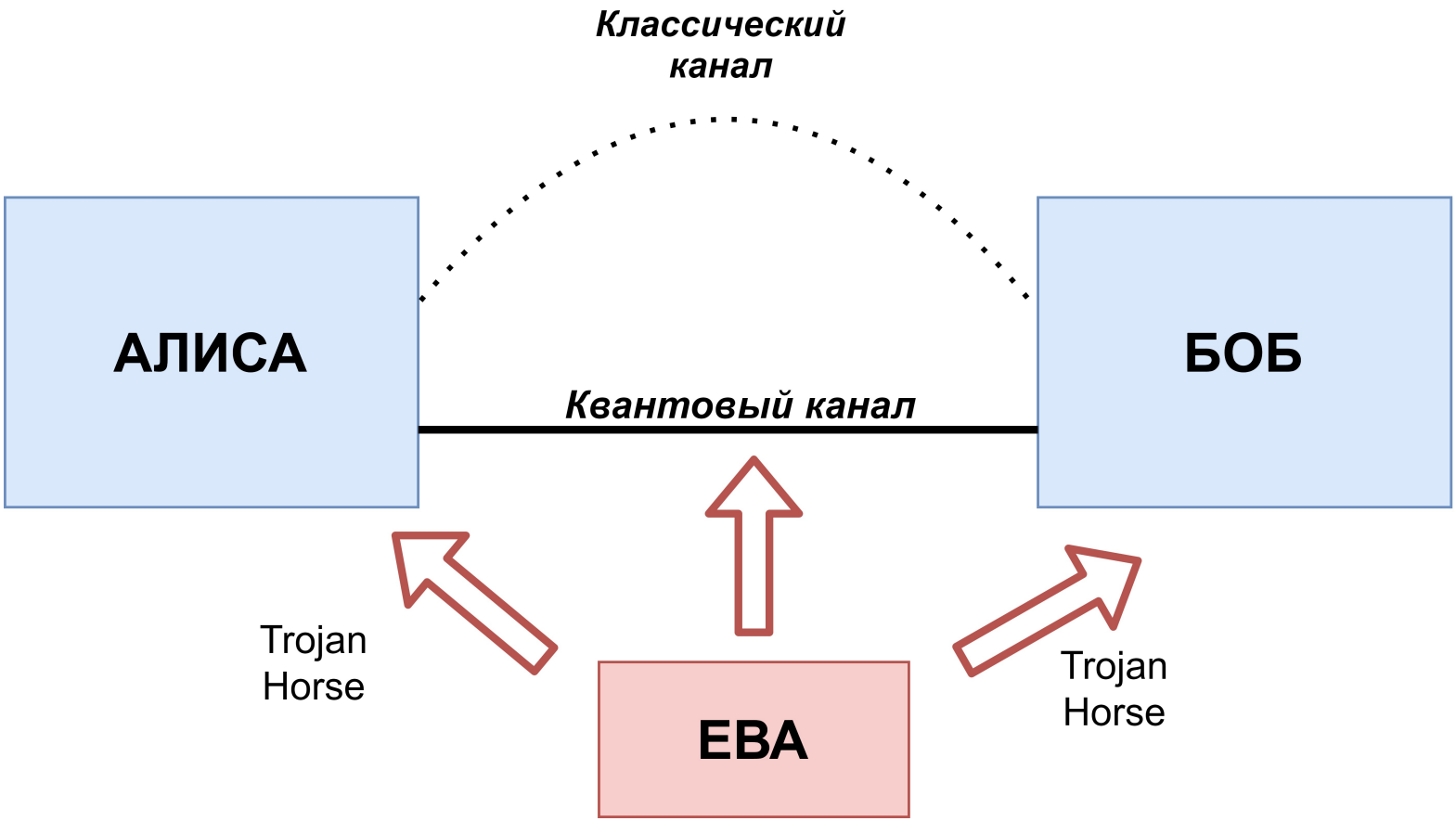
Diana.Guzairova@sfblaboratory.ru
Ivan.Sushchev@sfblaboratory.ru

РусКрипто'21
25 марта 2021

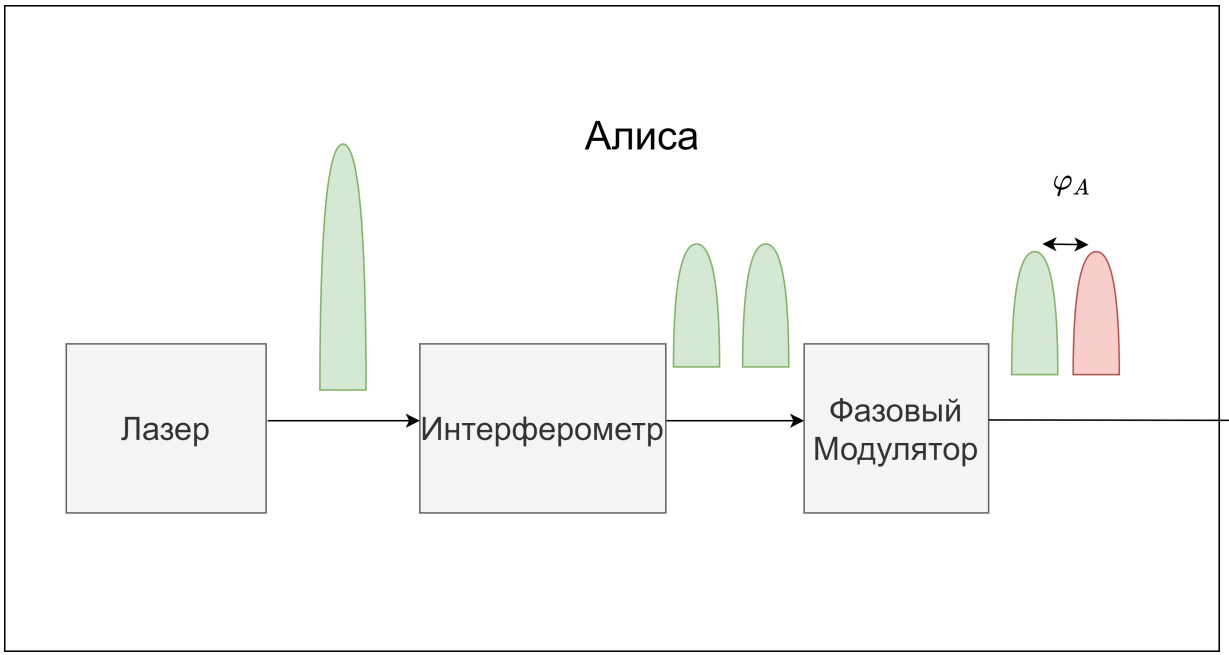
Источники

1. N. Gisin et al., «Trojan-horse attacks on quantum-key-distribution systems», 2006
2. V. Makarov et al., «Trojan-horse attacks threaten the security of practical quantum cryptography», 2014

Система КРК, атака Trojan Horse

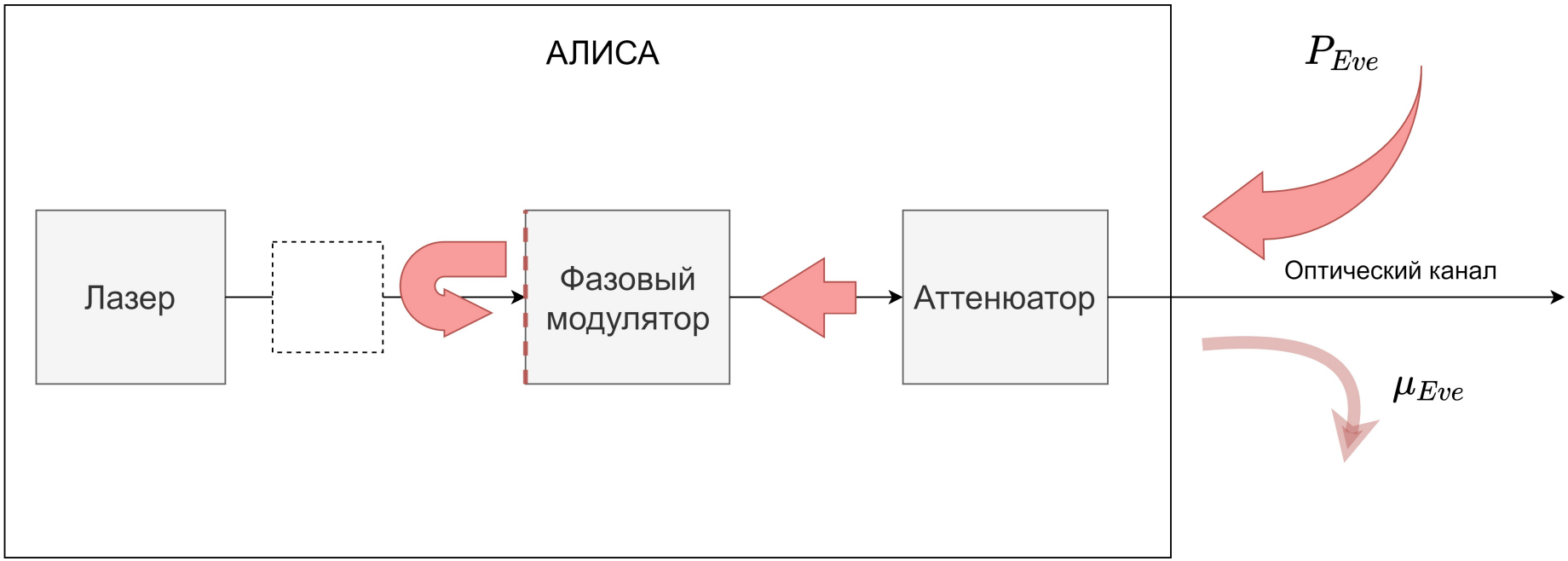


Фазовое кодирование



Базис	Бит	φ_A
1	0	0
	1	$\frac{\pi}{2}$
2	0	$\frac{\pi}{4}$
	1	$\frac{3\pi}{4}$
3	0	π
	1	$-\frac{\pi}{2}$
4	0	$-\frac{3\pi}{4}$
	1	$-\frac{\pi}{4}$

Принцип атаки Trojan Horse



μ_{Eve} – среднее число фотонов, которое получит Ева

P_{Eve} – мощность излучения, посылаемого Евой

Эффективность атаки Trojan Horse

Квантовые состояния Евы можно представить в виде:

$$\left|\alpha e^{i\varphi}\right\rangle = e^{-\frac{\alpha^2}{2}} \sum_{k=0}^{\infty} \frac{\left(\alpha e^{i\varphi_0}\right)^k}{\sqrt{k!}} \left|k\right\rangle = \sum_{k=0}^{\infty} c_k \left|k\right\rangle$$

$\{|k\rangle\}_0^\infty$– ортогональный базис, где $|k\rangle$ – вектор состояния, отвечающий k фотонам в импульсе

c_k – амплитуда вероятности

$$\mu_{Eve} = \alpha^2$$

Эффективность атаки Trojan Horse

Ева получает одно из когерентных квазиоднофотонных состояний, соответствующее фазам $\varphi_0 = 0$, $\varphi_1 = \frac{\pi}{2}$:

$$\left|\alpha e^{i\varphi_0}\right\rangle = e^{-\frac{\mu_{Eve}}{2}} \sum_{k=0}^{\infty} \frac{\left(\sqrt{\mu_{Eve}} e^{i\varphi_0}\right)^k}{\sqrt{k!}} \left|k\right\rangle = \sum_{k=0}^{\infty} c_k^{(0)} \left|k\right\rangle$$

$$\left|\alpha e^{i\varphi_1}\right\rangle = e^{-\frac{\mu_{Eve}}{2}} \sum_{k=0}^{\infty} \frac{\left(\sqrt{\mu_{Eve}} e^{i\varphi_1}\right)^k}{\sqrt{k!}} \left|k\right\rangle = \sum_{k=0}^{\infty} c_k^{(1)} \left|k\right\rangle$$

Эффективность атаки Trojan Horse

Вероятность ошибки различения состояний в выбранном базисе:

$$p = \frac{1}{2} - \frac{1}{2}\sqrt{1 - \left|\langle \alpha e^{i\varphi_0} \mid \alpha e^{i\varphi_1} \rangle\right|^2}$$

$\left\langle \alpha e^{i\varphi_0} \middle| \alpha e^{i\varphi_1} \right\rangle$ – скалярное произведение векторов квантовых состояний

Эффективность атаки Trojan Horse

$$\left\langle \alpha e^{i\varphi_0} \,\middle|\, \alpha e^{i\varphi_1} \right\rangle = \sum_{k=0}^{\infty} c_k^{(0)*} c_k^{(1)} = e^{-\mu_{Eve}} \sum_{k=0}^{\infty} \frac{\mu_{Eve}^k}{k!} e^{ik(\varphi_1-\varphi_0)}$$

$$\left| e^{-\mu_{Eve}} \sum_{k=0}^{\infty} \frac{\mu_{Eve}^k}{k!} e^{ik(\varphi_1-\varphi_0)} \right|^2 = e^{-4\mu_{Eve} sin^2\left(\frac{\varphi_0-\varphi_1}{2}\right)} = e^{-2\mu_{Eve}}$$

$$p = \frac{1}{2} - \frac{1}{2}\sqrt{1 - \left|\left\langle \alpha e^{i\varphi_0} \,\middle|\, \alpha e^{i\varphi_1} \right\rangle\right|^2} = \frac{1}{2} - \frac{1}{2}\sqrt{1 - e^{-2\mu_{Eve}}}$$

Как найти $\mu_{\mathbf{Eve}}$?

Методика измерения μ_{Eve}

Среднее число фотонов:

$$\mu = \frac{P}{f\hbar\omega}$$

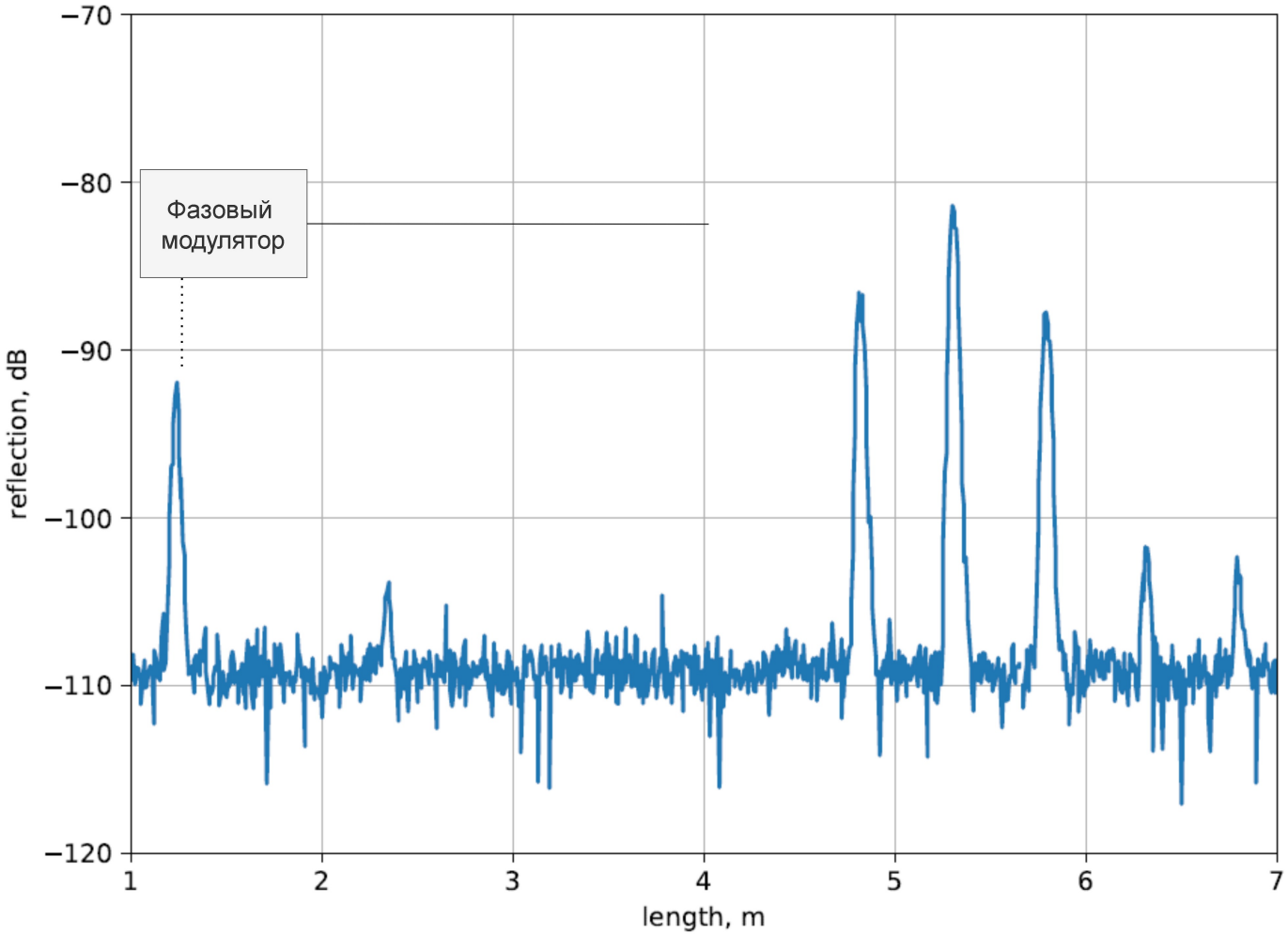
$\hbar\omega$ – энергия одного фотона

f – частота следования импульсов

P – мощность излучения

Методика измерения μ_{Eve}

Рефлектограмма, полученная со стороны Алисы



Методика измерения μ_{Eve}

Средняя мощность сигнала вернувшегося к Еве со стороны Алисы:

$$P_A = \mathbf{1,26 \cdot 10^{-24}} Вт$$

Среднее число фотонов в импульсе:

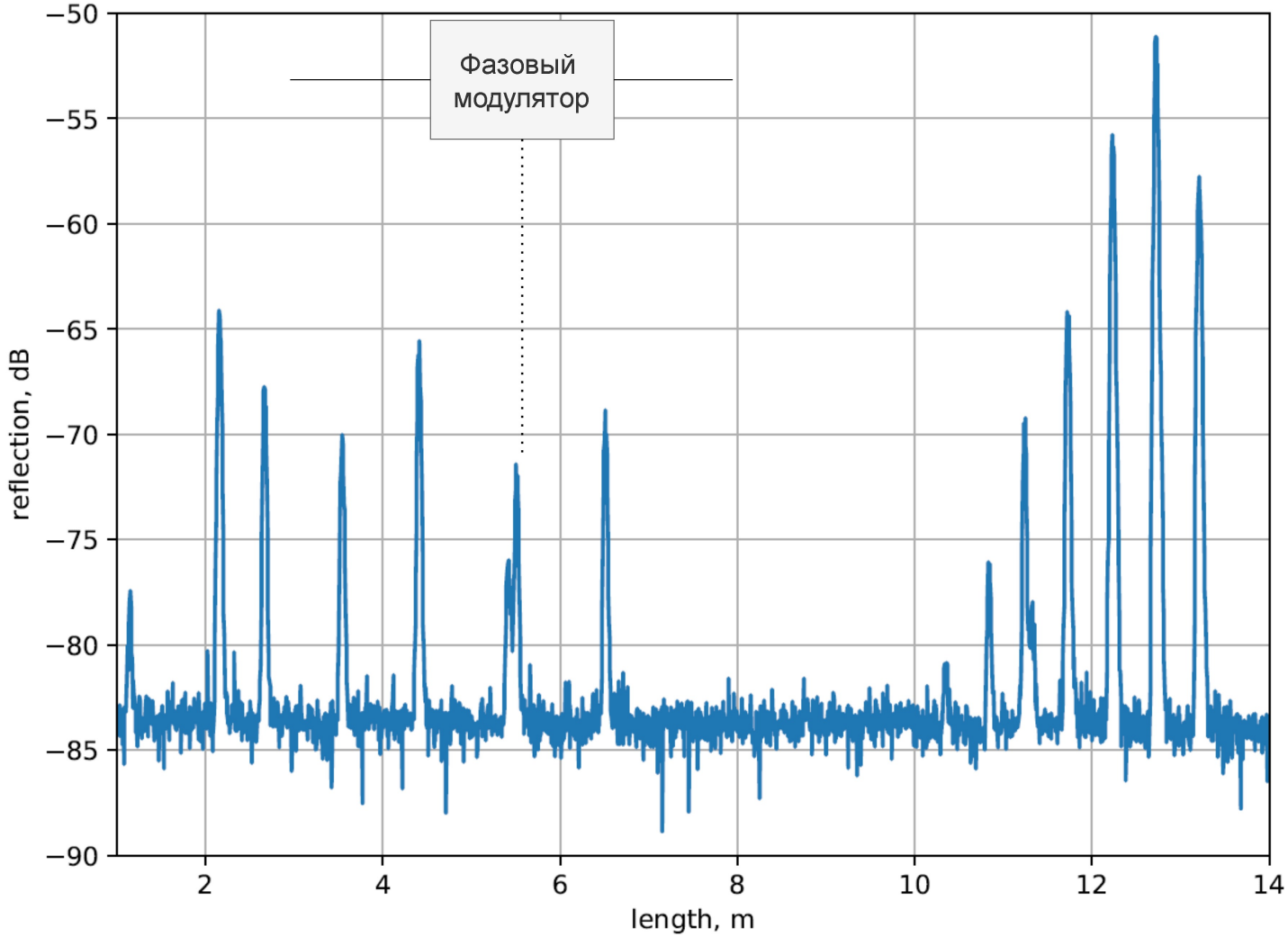
$$\mu_{Eve/Alice} = \frac{P_A}{f\hbar\omega} = \mathbf{1.23 \cdot 10^{-12}} \frac{\text{фот}}{\text{имп}}$$

Вероятность ошибки различения Евой состояний в базисе составляет:

$$p_{A \to E} = \frac{1}{2} - \frac{1}{2}\sqrt{1 - e^{-2\mu_{Eve/Alice}}} = \frac{1}{2} - 7,8 \cdot 10^{-7} = \mathbf{0,4999...}$$

Методика измерения μ_{Eve}

Рефлектограмма, полученная со стороны Боба



Методика измерения μ_{Eve}

Средняя мощность сигнала вернувшегося к Еве со стороны Алисы:

$$P_B = \mathbf{8 \cdot 10^{-15}\, Вт}$$

Среднее число фотонов в импульсе:

$$\mu_{Eve/Bob} = \frac{P_B}{f\hbar\omega} = \mathbf{7.8 \cdot 10^{-3}} \frac{\text{фот}}{\text{имп}}$$

Вероятность ошибки различения Евой состояний в базисе составляет:

$$p_{B\to E} = \frac{1}{2} - \frac{1}{2}\sqrt{1 - e^{-2\mu_{Eve/Bob}}} = \frac{1}{2} - 6,2 \cdot 10^{-2} = \mathbf{0,4378}$$

Итог

1. Получены данные:
   1. о величине отраженного сигнала от оптических элементов схемы
   2. о пропускании элементов защиты от атаки Trojan horse
2. Оценено значение среднего числа фотонов в отраженном сигнале
3. Рассчитана вероятность **ошибки различения логических бит**
4. Вероятность ошибки учитывается в формуле для квантовой утечки, определяющей **секретность ключа**

Благодарю за внимание!