Атака на протокол трех состояний.

Коновалов Матвей

Ментор: Кодухов Алексей Дмитриевич

Квантовая криптография

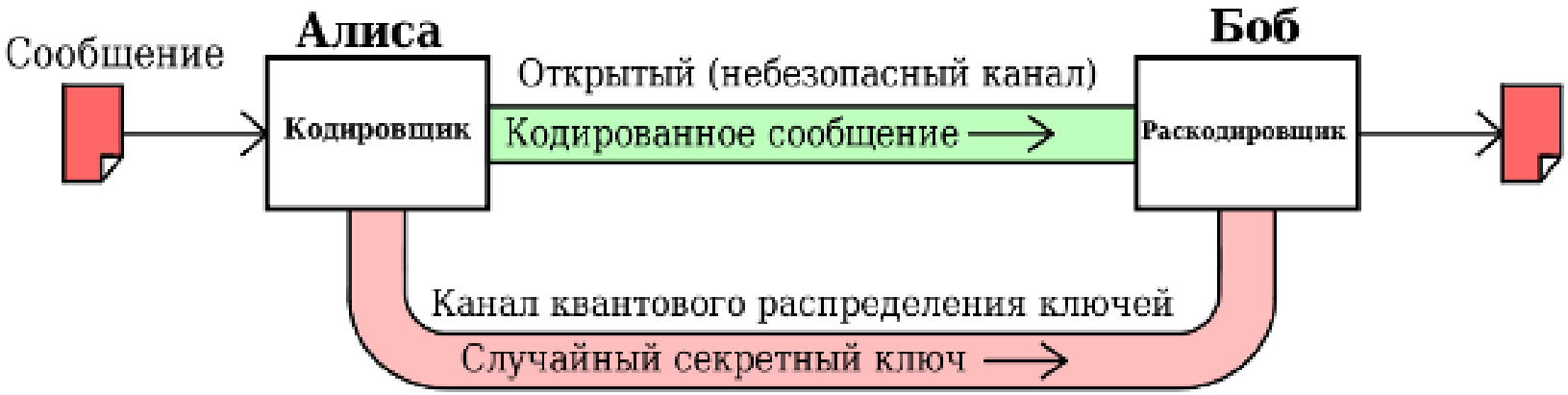


Рис. 1.1: Представление передачи информации между легитимными пользователями

Состояния и их измерения

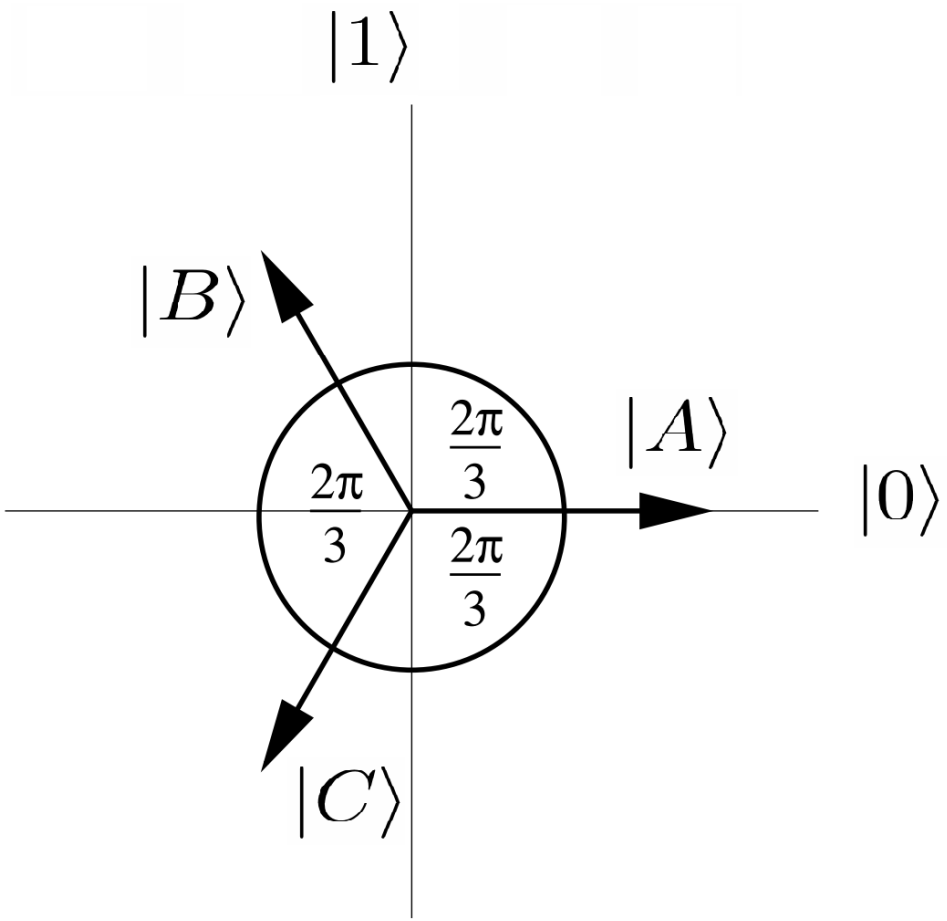


Рис. 1.2: Передаваемые кубиты, кодированные поляризацией

Протокол трех состояний

1. Алиса отправляет с равной вероятностью одно из трех состояний.
2. Боб измеряет с равной вероятностью в одном из трех наборов проективных операторов $|A\rangle\langle A|, |\overline{A}\rangle\langle\overline{A}|$.
3. В первом общении по открытому каналу оставляют те сигналы, в которых у Боба сработал оператор $|\overline{A}\rangle\langle\overline{A}|$.
4. Во втором общении по открытому каналу Алиса вскрывает состояние, которое она не отправляла. Если Боб уже знает, что это состояние не отправлялось, то оно далее не рассматривается, в ином случае Боб знает состояние Алисы. [3]

Протокол трех состояний

5

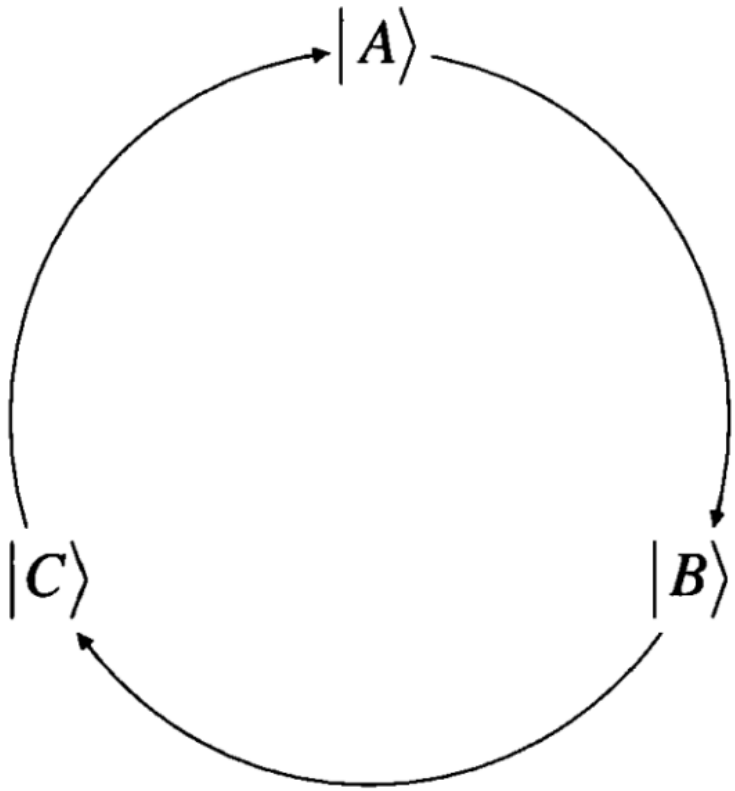


Рис. 1.3: Круг преобразования состояний в бит

Протокол трех состояний

Timeslot	1	2	3	4	5	6	7	8	9	10
Alice prepares	$\|A\rangle$	$\|B\rangle$	$\|C\rangle$	$\|C\rangle$	$\|C\rangle$	$\|B\rangle$	$\|A\rangle$	$\|A\rangle$	$\|B\rangle$	$\|A\rangle$
Bob measures	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{B}}$	$\hat{P}_{\bar{A}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{B}}$	$\hat{P}_{\bar{C}}$	$\hat{P}_{\bar{B}}$
Result	0	1	1	0	0	1	1	0	1	1
Alice says not		$\|C\rangle$	$\|B\rangle$			$\|A\rangle$	$\|B\rangle$		$\|C\rangle$	$\|C\rangle$
Bob says		✓	×			✓	✓		×	✓
Sequence		BC				BA	AB			AC
Inferred bit		0				1	0			1

Рис. 1.4: Пример передачи бита от Алисы к Бобу

Когерентные состояния

Мотивация: источник когерентных состояний - это самый доступный источник квантовых состояний. [2]
Можно ввести операторы аннигиляции $\hat{a}^\dagger$ и создания $\hat{a}$, для которых верно $[\hat{a}, \hat{a}^\dagger] = \hat{a}\hat{a}^\dagger - \hat{a}^\dagger\hat{a} = 1$. При определении оператора числа фотонов $\hat{n} = \hat{a}^\dagger\hat{a}$ можно заметить эрмитовости оператора и рассмотреть оператор на собственных векторах:

$$\hat{n}\,|n\rangle = n\,|n\rangle\,,$$

где n назовем числом фотонов.
Тогда собственное значение энергии будет $E_n = \hbar\omega(n + \frac{1}{2})$.

Можно показать, что $\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle$ и $\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle$, а также $n \in \mathbb{N}$, что объясняет названия $\hat{a}^\dagger$, $\hat{a}$ и n.

Когерентные состояния

Математическое описание когерентных состояний:

$$|\alpha\rangle = \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \exp(-\frac{1}{2}|\alpha|^2)\,|n\rangle\,,$$

где $|n\rangle$ — собственный вектор, соответствующий числу частиц n, α — комплексная амплитуда, такая что $|\alpha|^2 = \mu$ — среднее число частиц в импульсе света.

Теория информации

Энтропия (величина незнания информации) случайной величины $X = \{x_1, x_2, ...\}$:

$$H(X) = -\sum_{n=1}^{N} p(x_n) \log_2(p(x_n)).$$

Условная энтропия случайных величин X и Y:

$$H(Y|X) = \sum_{n=1}^{N} p(x_n) \cdot H(Y|x_n) = -\sum_{n=1}^{N} p(x_n) \sum_{m=1}^{M} p(y_m|x_n) \cdot \log_2(p(y_m|x_n)).$$

Взаимная информация (полученная информация об одной величине при наблюдении за другой):

$$I(X, Y) = H(Y) - H(Y|X).$$

Величина Холева

Величина Холева устанавливает верхнюю границу на количество информации, которую можно извлечь из ансамбля квантовых состояний.

$$I(X,Y) \leq \chi = S\left(\sum_n p_n \rho_n\right) - \sum_n p_n S(\rho_n),$$

где ρ — матрица плотности (описывает смешанное состояние), $S(\rho) = -\mathrm{Tr}(\rho \cdot \log_2(\rho))$ — энтропия фон Неймана.

PNS атака

PNS-атака (Photon Number Splitting) — самая популярная атака на QKD. В протокол вторгается Ева: [1]

1. измеряет без обнаружения количество фотонов в импульсе, отправленном Алисой по каналу с затуханием $\delta = 10^{-\alpha d}$, где α — коэффициент затухания, а d — расстояние между легитимными пользователями.
2. $(1 - q)$ часть однофотонных импульсов блокирует, а у многофотонных забирает фотон в квантовую память и отправляет импульс дальше без затухания.

Преимущество данной стратегии в том, что Ева может без заметного вмешательства производить измерения после того, как Алиса раскроет, какое состояние она не отправляла. Тогда задачей Евы будет различие двух неортогональных состояниях.

Информация Евы

При отличии двух неортогональных состояний информация Евы такая:

- пропускная способность (максимальная информация при измерении одного фотона) $C_1 = 1 - h_2\left(\frac{1-\sqrt{1-\cos^2\varphi}}{2}\right)$.
- граница Холево $\chi = h_2\left(\frac{1-\cos\varphi}{2}\right)$.

Где φ — угол между неортогональными состояниями Алисы, а $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ — бинарная энтропия.

Так как Ева проводит измерение состояния не у всех импульсов, то информация Евы будет умножена на долю тех импульсов, у которых Ева забрала фотон и которые перешли в сырой ключ у Алисы и Боба:

$$I_{Eve} = \frac{\sum_{n=2} p_n}{qp_1 + \sum_{n=2} p_n} C_1$$

Информация Евы

Ева производит атаку, в которой вероятность того, что отправленное состояние долетит до Боба, не меняется:

$$qp_1 + \sum_{n=2}^{\infty} p_n = \mu \cdot 10^{-\alpha d},$$

где $p_n = \mathrm{e}^{-\mu} \frac{\mu^n}{n!}$.

Можно показать:

$$I_{Eve}(d) = \frac{1 - \exp(-\mu) \cdot (1 + \mu)}{\mu \cdot 10^{-\alpha d}} C_1$$

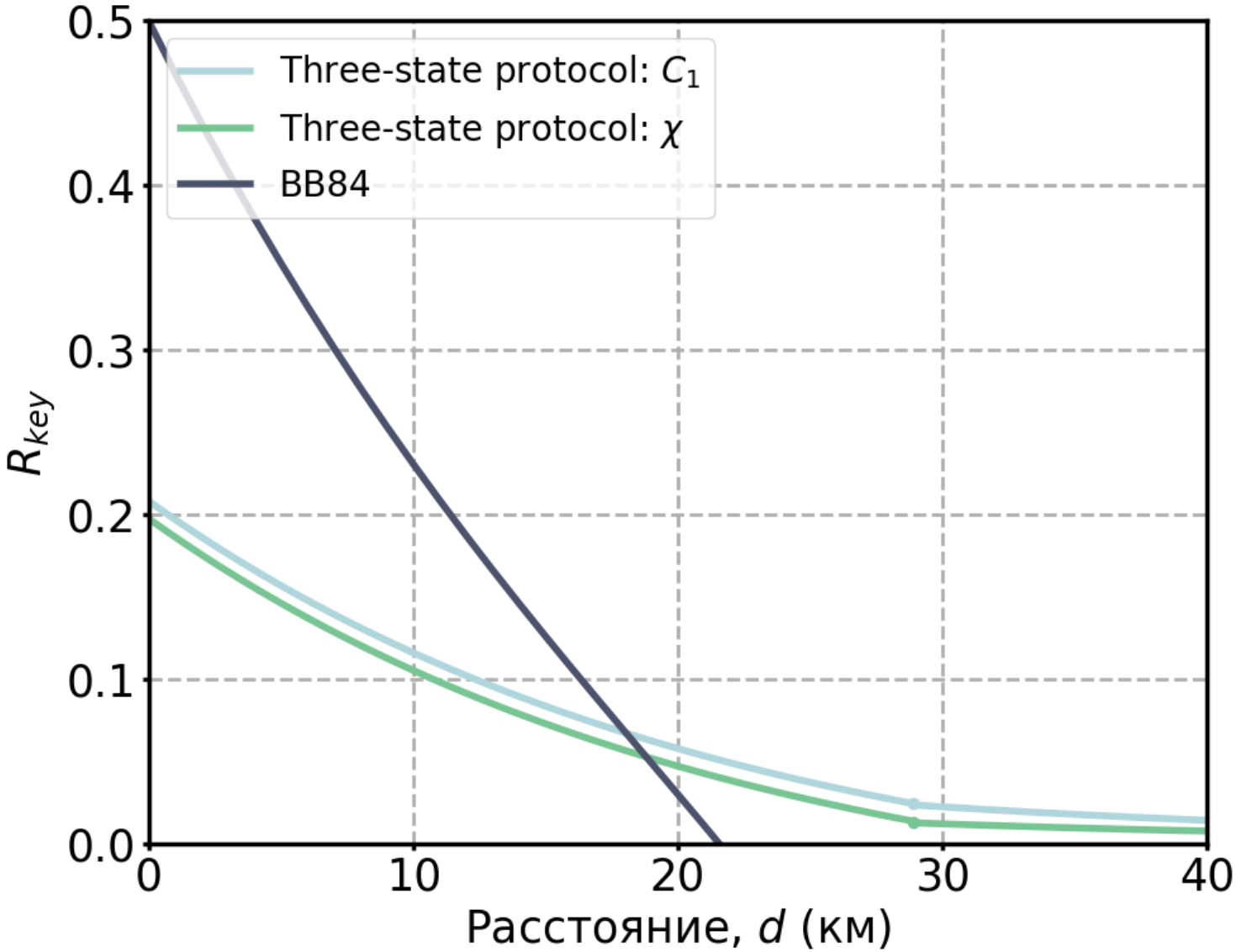
Скорость генерации ключа

Информацию легитимных пользователей можно определить $I_{AB} = 1 - h_2(Q_{\text{err}})$, где Q_{err} — ошибка битов у Алисы и Боба в сыром ключе. По протоколу ошибок нет, то есть $Q_{\text{err}} = 0$.

Можно показать:

$$R_{key}(d) = \frac{1}{4} \cdot 10^{-\alpha d}(1 - I_{Eve}(d))$$

График скорости генерации ключа



Выводы

В данной работе была учтена многофотонность источника квантовых состояний и продемонстрирована PNS-атака на протокол трех состояний.

Кроме того, проведены сравнительные исследования скоростей генерации ключа с протоколом BB84 в условиях аналогичных атак. Результаты показали, что протокол трех состояний обладает большей устойчивостью к PNS-атаке.

Список литературы

[1] Antonio Acin, Nicolas Gisin и Valerio Scarani. “Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks”. В: *Physical Review A* 69.1 (2004), с. 012309.

[2] Osamu Hirota. *Squeezed light*. Elsevier, 1992.

[3] Simon JD Phoenix, Stephen M Barnett и Anthony Chefles. “Three-state quantum cryptography”. В: *Journal of modern optics* 47.2-3 (2000), с. 507—516.