Квантовая криптография. Что в ней *криптографического*?

И.М. Арбеков

Академия криптографии Российской федерации

Семинар МГУ им. М.В. Ломоносова
27 сентября 2022

arbekov53@mail.ru

Цель квантовой криптографии

Цель

– снабдить Алису и Боба ключами, *недоступными* для нарушителя Евы

1. Передача:
   – логических бит, кодированных квантовыми состояниями, по оптическому каналу
2. Недоступность (секретность) ключей:
   – обеспечить выполнение критерия ε-секретности

Критерий ε-секретности

Совместная квантовая система при наличии нарушителя E, матрица плотности

$$\rho_{KE} = \sum_{k \in K} P_K(k) |k\rangle \langle k| \otimes \rho_E^k$$

Матрица плотности нарушителя

$$\rho_E = \sum_{k \in K} P_K(k) \rho_E^k$$

Матрица плотности равновероятного распределения ключей

$$\rho_U = \frac{1}{N} \sum_{k \in K} |k\rangle \langle k|$$

Следовое расстояние

$$\frac{1}{2} \|\rho_{KE} - \rho_U \otimes \rho_E\|_1$$

Критерий ε-секретности

$$\frac{1}{2} \|\rho_{KE} - \rho_U \otimes \rho_E\|_1 \leq \varepsilon$$

Критерий ε-секретности

Существуют классические распределения, где определяется *полное вариационное* расстояние

$$\frac{1}{2}\sum_{z\in Z}\sum_{k=1}^{N}\left|P_{KZ}(k,z)-\frac{1}{N}P_Z(z)\right|=$$

$$=\frac{1}{2}\sum_{z\in Z}P_Z(z)\sum_{k=1}^{N}\left|P_{K|Z}(k\mid z)-\frac{1}{N}\right|=$$

$$=\frac{1}{2}\left\|\rho_{KE}-\rho_U\otimes\rho_E\right\|_1\leq\varepsilon$$

[1] *Portmann C., Renner R.,*
Cryptographic security of quantum key distribution, 2014

[2] *Арбеков И. М., Молотков С. Н.,*
Различимость квантовых состояний и трудоемкость по Шеннону в квантовой криптографии,
ЖЭТФ, 2017, том 151, вып. 6

Где начинается криптография?

Криптография начинается там, где появляется *алгоритм нахождения ключа*.
Рассматриваются алгоритмы *опробования ключей*.
При этом имеется критерий *истинности ключа*.
Ключи *неравновероятны*, строим (формально) упорядоченный ряд *апостериорных* вероятностей

$$P_{K|Z}\left(k_1(z)\,|z\right) \geq P_{K|Z}\left(k_2(z)\,|z\right) \geq \ldots \geq P_{K|Z}\left(k_N(z)\,|z\right),$$

где $k_m(z)$ – номер ключа из множества $K = \{1, 2, \ldots, N\}$, стоящий в апостериорном ряду на m–м месте, $m = \overline{1, N}$,

$$k_1(z), k_2(z), \ldots, k_N(z)$$

– перестановка $1, 2, \ldots, N$, зависящая от z.

Алгоритмы опробования ключей

1. *Алгоритм* A_{guess} - опробование *единственного* варианта ключа $k_1(z)$.
Средняя вероятность успеха

$$P_{guess} = \sum_{z \in Z} P_{K|Z}\left(k_1(z)|z\right) P_Z(z) \leq \frac{1}{N} + \varepsilon$$

[3] *Portmann C., Renner R.,*
Cryptographic security of quantum key distribution, 2014

Алгоритмы опробования ключей

2. Алгоритм A_{total} *полного перебора* ключей.
Условная сложность (*трудоемкость*)

$$S_{A_{total}}(z) = \sum_{m=1}^{N} m P_{K|Z}\left(k_m(z)\,|z\right)$$

Средний объем работы

$$S_{A_{total}} = \sum_{z \in Z} P_Z(z)\, S_{A_{total}}(z) \geq \frac{N(1-2\varepsilon)+1}{2}$$

[4] *Молотков С. Н.,*
О сложности перебора ключей в квантовой криптографии, 2017

Алгоритмы опробования ключей

2. Алгоритм A_{total} *полного перебора* ключей.
Средний объем работы

$$S_{A_{total}} = \sum_{z \in Z} P_Z(z)\, S_{A_{total}}(z) \geq \frac{N(1-2\varepsilon)+1}{2}$$

Пример

$$P_{K|Z}(k|z) \sim \begin{pmatrix} 1 & 2 & \dots & N \\ \frac{1}{2} & \frac{1}{2(N-1)} & \dots & \frac{1}{2(N-1)} \end{pmatrix}$$

$$S_{A_{total}} \geq \frac{N+1}{4}$$

Но! Опробуя каждый раз 1-й ключ, «даром» получаем 50% передаваемой *секретной* информации

Алгоритмы опробования ключей

Вероятность успеха $\pi_U \leq 1$, средний объем работы ***на эксперимент*** S_U.
Сложность нахождения ключа, средний объем работы ***на один ключ*** *(практическая стойкость криптосистемы* по Шеннону) -

$$Q_U = \frac{S_U \cdot T}{\pi_U \cdot T} = \frac{S_U}{\pi_U}$$

[5] *C.E.Shannon, A Mathematical Theory of Communication, 1948*

Алгоритмы опробования ключей

3. *Усеченные* алгоритмы U, опробуются первые M наиболее вероятных ключей, $A_{guess} \preccurlyeq U \preccurlyeq A_{total}$.

$$Q_U(M) = \frac{S_U(M)}{\pi_U(M)} = \frac{\left(1 - \sum_{m=1}^{M} \overline{p}_m\right) M + \sum_{m=1}^{M} m\overline{p}_m}{\sum_{m=1}^{M} \overline{p}_m},$$

$$\overline{p}_m = \sum_{z \in Z} P_{K|Z}\left(k_m(z)\,|z\right) P_Z(z)$$

– средняя (по всем z) вероятность попадания ключа *шифрования* на m-е место в ряду апостериорных вероятностей

$$P_{K|Z}\left(k_1(z)\,|z\right) \geq P_{K|Z}\left(k_2(z)\,|z\right) \geq \ldots \geq P_{K|Z}\left(k_N(z)\,|z\right),$$

Сложность нахождения ключа *с границей* π_0

$$Q_{U,\pi_0} := \min_{M:\pi_U(M) \geq \pi_0} Q_U(M).$$

Усеченные алгоритмы, ε-секретность и сложность

1. Свойство ε-секретности

$$\frac{1}{2}\sum_{z\in Z} P_Z(z)\sum_{k=1}^{N}\left|P_{K|Z}(k\mid z)-\frac{1}{N}\right| = \frac{1}{2}\left\|\rho_{KE}-\rho_U\otimes\rho_E\right\|_1 \le \varepsilon$$

2. Упорядоченный ряд апостериорных вероятностей

$$P_{K|Z}\left(k_1(z)\,|z\right) \ge P_{K|Z}\left(k_2(z)\,|z\right) \ge \ldots \ge P_{K|Z}\left(k_N(z)\,|z\right)$$

3. Средняя трудоемкость на определение одного ключа

$$Q_U(M) = \frac{S_U(M)}{\pi_U(M)} = \frac{\left(1-\sum_{m=1}^{M}\overline{p}_m\right)M+\sum_{m=1}^{M}m\overline{p}_m}{\sum_{m=1}^{M}\overline{p}_m},$$

$$\overline{p}_m = \sum_{z\in Z} P_{K|Z}\left(k_m(z)\,|z\right)P_Z(z)$$

Усеченные алгоритмы, ε-секретность и сложность

4. Минимальная трудоемкость при ограничении на вероятность успеха

$$Q_{U,\pi_{\mathbf{0}}} := \min_{M:\pi_U(M)\geq\pi_{\mathbf{0}}} Q_U(M)$$

Имеет место неравенство

$$Q_{U,\pi_{\mathbf{0}}} \geq \left(1 - \frac{\varepsilon}{\pi_0}\right) \frac{N(1-4\varepsilon)+1}{2},$$

$$Q_{\max} = \frac{N+1}{2}$$

– максимальная сложность

[6] *И.М. Арбеков, Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой, 2022.*

Усеченные алгоритмы

Усеченные алгоритмы U_0 с *нулевым* опробованием.
Включаем точку $M = 0$ в множество опробуемых ключей. Тогда

$$Q_{U_0,\pi_0} \geq \left(1 - \frac{\varepsilon}{\pi_0}\right) \frac{N\left(1 - 4\varepsilon/\pi_0\right) + 1}{2}$$

Спасибо за внимание!