14 - Collective attacks

20 grudnia 2010
12:53

14.1 Prepare & measure vs Entanglement based QKD

Up to now we have been considering QKD in the P&M approach i.e.

with probability p_i A send state $|\psi_i\rangle$ to B

But we can equivalently think that, instead there is some state ρ_{AB} that A prepares and send the part B to B
Then A measures her part using operators Π_i such that

$$Tr_A(\Pi_i \otimes \mathbb{1}\ \rho_{AB}) = p_i |\psi_i\rangle\langle\psi_i|$$

So this measurement is just preparation of state $|\psi_i\rangle$ sent with probability p_i to B.
Note A may postpone her measurement after E attack on B's probe; which may be more convenient to analyze

Example: BB84 $\rho_{AB} = |\Phi^+\rangle_{AB}\langle\Phi^+|$

$\Pi_i^{(j)}$ <- basis, i <- logical bit

- $\Pi_{A\,i}^{(1)} = |i\rangle\langle i|$ $\Pi_{B\,i}^{(1)} = |i\rangle\langle i|$
- $\Pi_{A\,0}^{(2)} = |+\rangle\langle +|$ $\Pi_{B\,0}^{(2)} = |+\rangle\langle +|$ $\Pi_{A\,1}^{(2)} = |-\rangle\langle -|$ $\Pi_{B\,1}^{(2)} =$ $|-\rangle\langle -|$

14.2 Secure protocol against collective attacks

(we get a lower bound on $QBER_{th}$)

After distributing entangled state $|\Phi^+\rangle^{\otimes n}$ between A and B and possible E attack, ABE share the state

$$\rho_{ABE}^{\otimes n}$$

Without loss of generality we may assume $\rho_{ABE} = |\psi_{ABE}\rangle\langle\psi_{ABE}|$
(More information for E) - E holds a purification of ρ_{AB}.
Let us write ρ_{AB} in Bell basis $|\psi_1\rangle = |\psi_-\rangle$ $|\psi_2\rangle = |\psi_+\rangle$
$|\psi_3\rangle = |\phi_-\rangle$ $|\psi_4\rangle = |\phi_+\rangle$

$$\rho_{AB} = \sum_{ij} c_{ij} |\psi_i\rangle\langle\psi_j|$$

A & B apply correlated Locc operation

$$\rho_{AB}' = \frac{1}{4}\sum_k \sigma_k \otimes \sigma_k \rho_{AB} \sigma_k^\dagger \otimes \sigma_k^\dagger = \sum_k \underbrace{c_{kk}}_{\lambda_k} |\psi_k\rangle\langle\psi_k|$$

we have prepared a Bell diagonal state

What is the QBER A and B will detect
(we assume they measure $\Pi_A^{(j)}$ and $\Pi_B^{(j)}$ where $j=j'$

$$QBER = \frac{1}{2}\sum_{j=1}^{2} Tr\left(\rho_{AB}\left(\Pi_{A\,0}^{(j)}\otimes\Pi_{B\,1}^{(j)} + \Pi_{A\,1}^{(j)}\otimes\Pi_{B\,0}^{(j)}\right)\right) = \lambda_1 + \frac{1}{2}\lambda_2 + \frac{1}{2}\lambda_3$$

If moreover we assume that QBER in both basis is the same we can assume it by randomly rotating the state ρ_{AB} with

$\rho_{AB}'' = \frac{1}{2}\sum_i V_i\otimes V_i\ \rho_{AB}\ V_i^\dagger\otimes V_i^\dagger$ where $V_0 = \mathbb{1}$ $V_1 = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

this additionally introduces symetry $\lambda_2=\lambda_3$. So we can think we perform measurements always in logical basis.

So $\lambda_1+\lambda_2 = QBER$ $\lambda_3=\lambda_2 = QBER-\lambda_1$

$\lambda_4 = 1+\lambda_1-2QBER$

So only one free parameter remains.

What is the purification of ρ_{AB}?

$$|\psi\rangle_{ABE} = \sum_k \sqrt{\lambda_k}\,|\psi_k\rangle_{AB}\otimes|k\rangle$$

↑ there is freedom in choice of E basis

When A performs a measurement we may consider it as

$C\to QQ$ channel. $\quad x \longrightarrow \rho_{BE}^x = \frac{1}{p_x} Tr\left(\Pi_x\otimes\mathbb{1}_{BE}\,|\psi_{ABE}\rangle\langle\psi_{ABE}|\right)$

Secret capacity:

$$C \geq \chi_{AB} - \chi_{AE} \overset{\text{in our case B performs individual measurements so}}{=} I(A:B) - \chi_{AE}$$

Due to basis symetry it is enough to calculate in $j=1$ basis

For $i=0$ $\longrightarrow p_0\rho_E^0 := Tr_{AB}\left(|x\rangle\langle x|\otimes\mathbb{1}\,|\psi_{ABE}\rangle\langle\psi_{ABE}|\right) = \frac{1}{2}\begin{bmatrix}\lambda_1 & \sqrt{\lambda_1\lambda_2} & 0\\ \sqrt{\lambda_1\lambda_2} & \lambda_2 & \\ 0 & & \lambda_3 \ \sqrt{\lambda_3\lambda_4}\\ & & \sqrt{\lambda_3\lambda_4}\ \lambda_4\end{bmatrix}$

$i=1$ $\longrightarrow p_1\rho_E^1 = Tr_{AB}\left(|x\rangle\langle x|\otimes\mathbb{1}\,|\psi_{ABE}\rangle\langle\psi_{ABE}|\right) = \frac{1}{2}\begin{bmatrix}\lambda_1 & \sqrt{\lambda_1\lambda_2} & & \\ \sqrt{\lambda_1\lambda_2} & \lambda_2 & & \\ & & \lambda_3 & -\sqrt{\lambda_3\lambda_4}\\ & & -\sqrt{\lambda_3\lambda_4} & \lambda_4\end{bmatrix}$

$p_0 = p_1 = \frac{1}{2}$ $\quad S(\rho_E^0) = S(\rho_E^1) = h(\lambda_1+\lambda_2) = h(x) = -x\log x - (1-x)\log(1-x)$

$= h(QBER)$

$$S(\rho_E) = S\left(\frac{1}{2}(\rho_E^0+\rho_E^1)\right) = -\sum_i \lambda_i\log\lambda_i = -\lambda_1\log\lambda_1 - (QBER-\lambda_1)\log(QBER-\lambda_1) - (1+\lambda_1-2QBER)\log(1+\lambda_1-2QBER)$$

$$\frac{\partial S(\rho_E)}{\partial\lambda_1} = -\log\lambda_1 - 1 + 2\log(QBER-\lambda_1) + 2 - \log(1+\lambda_1-2QBER) - 1 = 0$$

$$(QBER-\lambda_1)^2 = \lambda_1(1+\lambda_1-2QBER) \quad QBER^2 - 2\lambda_1 QBER = \lambda_1(1-2QBER)$$

$$\lambda_1 = QBER^2$$

$QBER := Q$

$$S(\rho_E) = -Q^2\log Q^2 - 2(Q-Q^2)\log(Q-Q^2) - (1-Q)^2\log(1-Q)^2 =$$

$= (-2Q^2 - 2Q + 2Q^1)\log Q + (-2Q + 2Q^2 - 2 + 4Q - 2Q^2)\log(1-Q) =$

$= -2Q\log Q - 2(1-Q)\log(1-Q) = 2h(Q)$

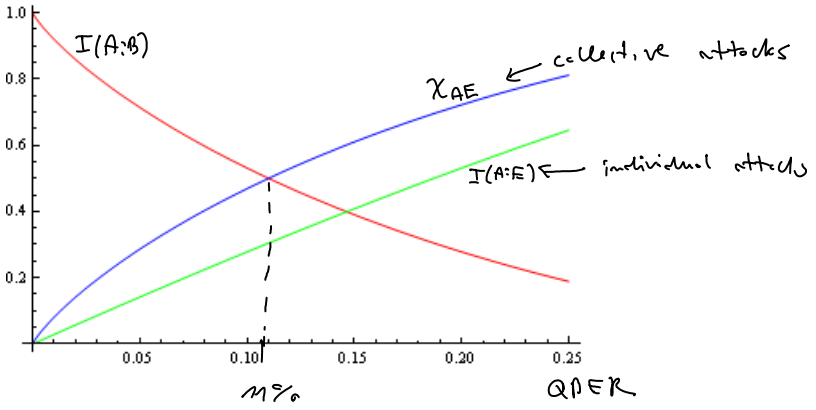
$\chi_{AE} = S(\rho_E) - S(\rho_E^0)$

$\chi_{AE} = h(Q)$

$C \geq (1 - h(Q)) - \chi_{AE} = 1 - 2h(Q)$

QBER$_{th}$: $2h(Q) = 1$ $\quad Q = 11\%$

Therefore we know that if QBER $< 11\%$ we can distill secret key, assuming attacks are collective.



Note: Recall the optimal individual attacks, where

$I(A:E) = 1 - h(p_e)$ $\quad p_e = \frac{1}{2}(1 - \sqrt{1-|\langle\psi_0|\psi_1\rangle|^2})$

↑ probability of distinguishing two states

$\langle\psi_0|\psi_1\rangle = 1 - 2\,\text{QBER}$

E can perform the same interaction between her probe and the flying qubit, but measure them collectively

So we can think that there is a $C \to Q$ channel from A to E, where $0 \to |\psi_0\rangle\langle\psi_0|$

$1 \to |\psi_1\rangle\langle\psi_1|$

We can calculate Holevo bound $\chi_{AE} = h(\text{QBER})$ so it is the attack that gives exactly the 11% QBER$_{th}$.

Note: We only analyzed one-way communication, if two way communication is allowed the QBER$_{th}$ can be raised significantly.

Even for one way communication it is possible to increase a bit the 11% using some preprocessing