Eavesdropping in quantum cryptography with six mixed states

Zahra Shadman, Hermann Kampermann, Tim Meyer and Dagmar Bruß

Institute For Theoretical Physics III,
Heinrich-Heine-University Düsseldorf (Germany)

September 2007, Kish-Iran

Introduction

Quantum Key Distribution (QKD) protocol :

- Quantum part: Distribution and measurement of quantum information
- Classical part: Parameter estimation and Classical post-processing

Introduction

Quantum Key Distribution (QKD) protocol :

It is shown if in the classical part of the protocol Alice or Bob adds some amount of noise to their measurement data, then the efficiency of the protocol can be increased (R. Rener, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005))

Introduction

Quantum Key Distribution (QKD) protocol :

It is shown if in the classical part of the protocol Alice or Bob adds some amount of noise to their measurement data, then the efficiency of the protocol can be increased (R. Rener, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005))

What will happen if we add some amount of noise in the quantum part ?

Six states protocol

Eavesdropping with pure states (D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998))

- $|0\rangle$
- $|1\rangle$
- $|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|\bar{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $|\bar{\bar{0}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
- $|\bar{\bar{1}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Alice sends one of these six pure states at random to Bob.

Six states protocol

Eavesdropping with pure states (D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998))

The most general Unitary transformation Eve can design is of the form :

$$U|0\rangle|X\rangle = \sqrt{F}|0\rangle|A\rangle + \sqrt{1-F}|1\rangle|B\rangle$$
$$U|1\rangle|X\rangle = \sqrt{F}|1\rangle|C\rangle + \sqrt{1-F}|0\rangle|D\rangle$$

Six states protocol

Eavesdropping with pure states (D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998))

The most general Unitary transformation Eve can design is of the form :

$$U|0\rangle|X\rangle = \sqrt{F}|0\rangle|A\rangle + \sqrt{1-F}|1\rangle|B\rangle$$
$$U|1\rangle|X\rangle = \sqrt{F}|1\rangle|C\rangle + \sqrt{1-F}|0\rangle|D\rangle$$

F is the fidelity of Bob's bit and is defined as

$$F = \langle\psi^{in}|\rho^B|\psi^{in}\rangle = 1 - D$$

Six states protocol

Eavesdropping with pure states (D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998))

The most general Unitary transformation Eve can design is of the form :

$$U|0\rangle|X\rangle = \sqrt{F}|0\rangle|A\rangle + \sqrt{1-F}|1\rangle|B\rangle$$
$$U|1\rangle|X\rangle = \sqrt{F}|1\rangle|C\rangle + \sqrt{1-F}|0\rangle|D\rangle$$

F is the fidelity of Bob's bit and is defined as

$$F = \langle\psi^{in}|\rho^{B}|\psi^{in}\rangle = 1 - D$$

It is assumed Eve is clever enough to treat all six states in the same way that means the same fidelity for Bob.

Eavesdropping with Mixed states

six mixed states

- $|0\rangle \Rightarrow (1-P)|0\rangle\langle 0| + I\frac{P}{2}$
- $|1\rangle \Rightarrow (1-P)|1\rangle\langle 1| + I\frac{P}{2}$
- $|\bar{0}\rangle \Rightarrow (1-P)|\bar{0}\rangle\langle\bar{0}| + I\frac{P}{2}$
- $|\bar{1}\rangle \Rightarrow (1-P)|\bar{1}\rangle\langle\bar{1}| + I\frac{P}{2}$
- $|\bar{\bar{0}}\rangle \Rightarrow (1-P)|\bar{\bar{0}}\rangle\langle\bar{\bar{0}}| + I\frac{P}{2}$
- $|\bar{\bar{1}}\rangle \Rightarrow (1-P)|\bar{\bar{1}}\rangle\langle\bar{\bar{1}}| + I\frac{P}{2}$

where, p is the noise parameter and I is the identity operator.

Eavesdropping with Mixed states

we consider that Eve uses the same unitary transformation.

Quantum Bit Error Rate [Q]

$$[Q] = [\bar{Q}] = [\bar{\bar{Q}}]$$

Eavesdropping with Mixed states

we consider that Eve uses the same unitary transformation.

Quantum Bit Error Rate [Q]

$$[Q] = [\bar{Q}] = [\bar{\bar{Q}}]$$

$$[Q] = \frac{1}{2}\langle 0|\rho_1^B|0\rangle + \frac{1}{2}\langle 1|\rho_0^B|1\rangle$$

$$\langle 0|\rho_1^B|0\rangle = \langle 1|\rho_0^B|1\rangle = \langle \bar{0}|\rho_{\bar{1}}^B|\bar{0}\rangle = ... = ... = ...$$

Eavesdropping with Mixed states

we consider that Eve uses the same unitary transformation.

Quantum Bit Error Rate [Q]

$$[Q] = \frac{1}{2}\langle 0|\rho_1^B|0\rangle + \frac{1}{2}\langle 1|\rho_0^B|1\rangle$$

$$\langle 0|\rho_1^B|0\rangle = \langle 1|\rho_0^B|1\rangle = \langle \bar{0}|\rho_{\bar{1}}^B|\bar{0}\rangle = ... = ... = ...$$

Constraints

- $\langle B|D\rangle = 0$
- $Re\langle A|C\rangle = 2 - \frac{1}{F}$
- $\langle A|B\rangle + \langle D|C\rangle = 0$

Eavesdropping with Mixed states

we consider that Eve uses the same unitary transformation.

Quantum Bit Error Rate [Q]

$$[Q] = \frac{1}{2}\langle 0|\rho_1^B|0\rangle + \frac{1}{2}\langle 1|\rho_0^B|1\rangle$$

$$\langle 0|\rho_1^B|0\rangle = \langle 1|\rho_0^B|1\rangle = \langle \bar{0}|\rho_{\bar{1}}^B|\bar{0}\rangle = ... = ... = ...$$

Constraints

- $\langle B|D\rangle = 0$
- $Re\langle A|C\rangle = 2 - \frac{1}{F}$
- $\langle A|B\rangle + \langle D|C\rangle = 0$
- $\langle A|D\rangle + \langle B|C\rangle = 0$

Eavesdropping with Mixed states

Mutual Information

$$I^{XY} = H(X) + H(Y) - H(X,Y) = \sum_{x,y} p(x,y) \log p(y|x) - \sum_{y} p(y) \log p(y)$$

Eavesdropping with Mixed states

Mutual Information

$$I^{XY} = H(X)+H(Y)-H(X,Y) = \sum_{x,y} p(x,y)\log p(y|x) - \sum_{y} p(y)\log p(y)$$

$$I^{AB} = 1 + Q\log Q + (1-Q)\log(1-Q)$$

Eavesdropping with Mixed states

Mutual Information

- $I^{AB} = 1 + Q \log Q + (1 - Q) \log(1 - Q)$
- $Q = D(1 - P) + \frac{P}{2}$

Eavesdropping with Mixed states

Mutual Information

$$I^{AE} = ?$$

Eavesdropping with Mixed states

Mutual Information

$$I^{AE} = ?$$

Eve's states

- $|B\rangle = |00\rangle$
- $|D\rangle = |11\rangle$
- $|A\rangle = \alpha_A|00\rangle + \beta_A|10\rangle + \gamma_A|01\rangle + \delta_A|11\rangle$
- $|C\rangle = \alpha_C|00\rangle + \beta_C|10\rangle + \gamma_C|01\rangle + \delta_C|11\rangle$

Eavesdropping with Mixed states

Mutual Information

$$I^{AE} = ?$$

Eve's states

- $|B\rangle = |00\rangle$
- $|D\rangle = |11\rangle$
- $|A\rangle = \alpha_A|00\rangle + \beta_A|10\rangle + \gamma_A|01\rangle + \delta_A|11\rangle$
- $|C\rangle = \alpha_C|00\rangle + \beta_C|10\rangle + \gamma_C|01\rangle + \delta_C|11\rangle$

Constraints between the coefficients of Eve'States

- $|\alpha_C|^2 + |\beta_C|^2 + |\gamma_C|^2 + |\delta_C|^2 = 1$
- $|\alpha_A|^2 + |\beta_A|^2 + |\gamma_A|^2 + |\delta_A|^2 = 1$
- $\alpha_A^* + \delta_C = 0$
- $\delta_A^* + \alpha_C = 0$
- $Re(\alpha_A^*\alpha_C + \beta_A^*\beta_C + \gamma_A^*\gamma_C + \delta_A^*\delta_C) = 2 - \frac{1}{F}$

Eavesdropping with Mixed states

Mutual Information

$$I^{AE} = 1+\tau\left[(1-\tfrac{P}{2})(F|\alpha_A|^2+1-F)+\tfrac{P}{2}F|\delta_A|^2, \tfrac{P}{2}(F|\alpha_A|^2+1-F)+F(1-\tfrac{P}{2})|\delta_A|^2\right]$$

$$+\tfrac{1}{2}(\tau\left[(1-\tfrac{P}{2})F|\beta_A|^2+\tfrac{P}{2}F|\beta_C|^2, \tfrac{P}{2}F|\beta_A|^2+(1-\tfrac{P}{2})F|\beta_C|^2\right])$$

$$+\tfrac{1}{2}(\tau\left[(1-\tfrac{P}{2})F|\gamma_A|^2+\tfrac{P}{2}F|\gamma_C|^2, F\tfrac{P}{2}|\gamma_A|^2+(1-\tfrac{P}{2})F|\gamma_C|^2\right])$$

$$\tau[x,y] = x\log x + y\log y - (x+y)\log(x+y)$$

Eavesdropping with Mixed states

Maximal Mutual Information (A & E)for pure states

$$\alpha_A = \delta_A = 0$$

$$|\beta_C|^2 = 1 - |\beta_A|^2$$

$$I^{AE} = 1 + (1-D)\Big\{|\beta_A|^2 \log|\beta_A|^2 + (1-|\beta_A|^2)\log(1-|\beta_A|^2)\Big\}$$

$$|\beta_A|^2 = \tfrac{1}{2}\Big(1 + \frac{1}{1-D}\sqrt{D(2-3D)}\,\Big)$$

Eavesdropping with Mixed states

Maximal Mutual Information (A & E)for Mixed states

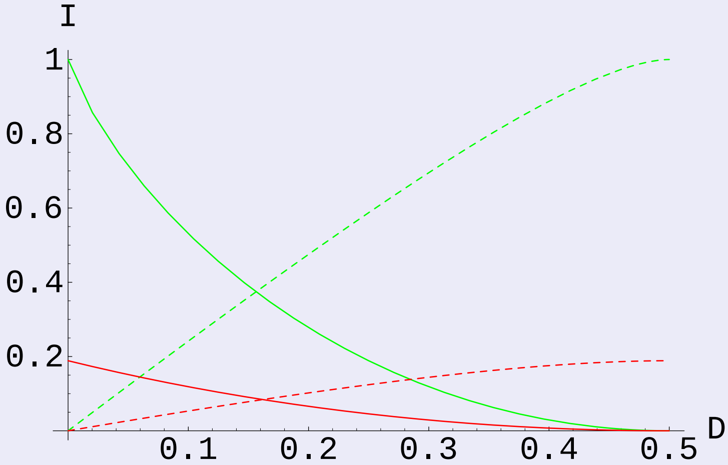
$$\alpha_A = \delta_A = 0$$

$$|\beta_C|^2 = 1 - |\beta_A|^2$$

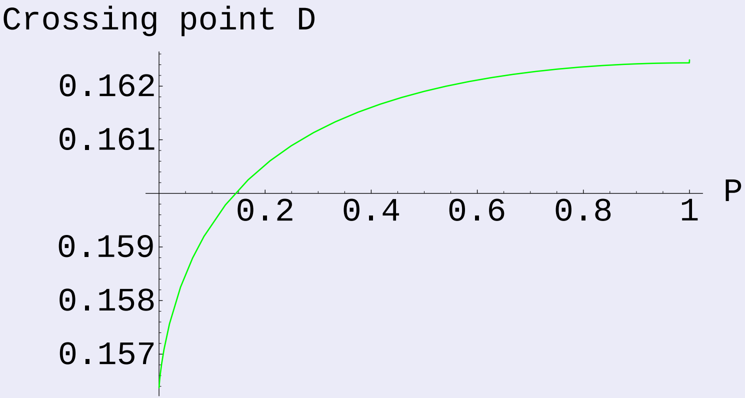
$$I^{AE} = 1 + (1-D)\Big\{ \big((1{-}P)|\beta_A|^2 + \tfrac{P}{2}\big) \log \big((1{-}P)|\beta_A|^2 + \tfrac{P}{2}\big) + \big((1{-}\tfrac{P}{2}) - (1{-}P)|\beta_A|^2\big) \log \big((1{-}\tfrac{P}{2}) - (1{-}P)|\beta_A|^2\big) \Big\} + D\Big\{ \tfrac{P}{2} \log \tfrac{P}{2} + (1 - \tfrac{P}{2}) \log (1{-}\tfrac{P}{2}) \Big\}$$

$$|\beta_A|^2 = \tfrac{1}{2}\Big(1 + \frac{1}{1-D}\sqrt{D(2-3D)}\,\Big)$$

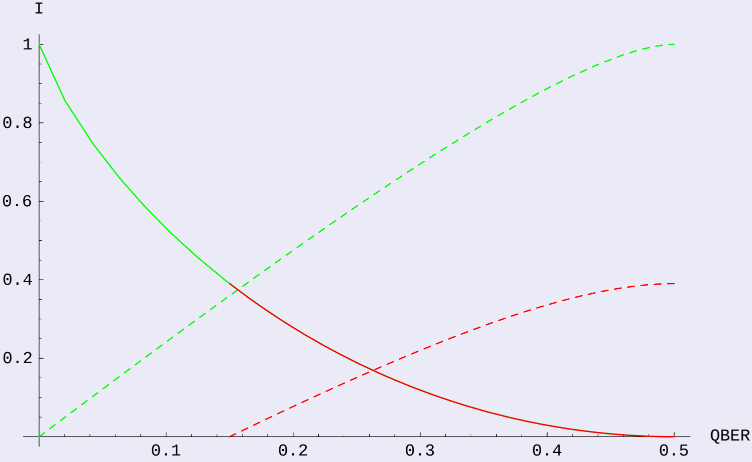
Comparing between mutual information in terms of D (p= $\frac{1}{2}$)



- Green curves for pure states
- Red curves for mixed states
- solid curves between Alice & Bob
- Dashed curves between Alice & Eve

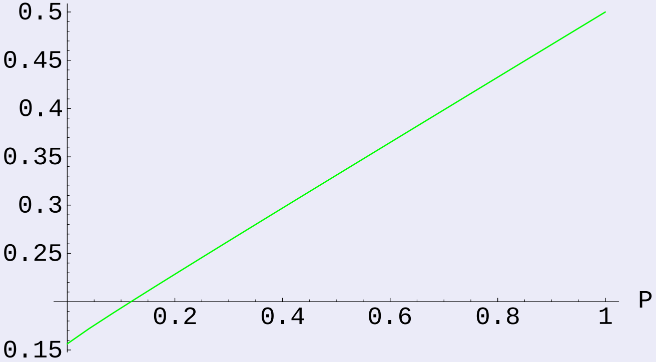

Crossing point D
0.162
0.161
0.159
0.158
0.157
0.2
0.4
0.6
0.8
1
P

Comparing between mutual information in terms of Q (p= $\frac{1}{2}$)



- Green curves for pure states
- Red curves for mixed states
- solid curves between Alice & Bob
- Dashed curves between Alice & Eve

Crossing point :QBER:



Summary

- Obtaining the mutual information for six mixed states.
- Optimal eavesdropping strategy for mixed states is the same for pure states .
- The mutual information for mixed states is less than for pure states(in terms of D), and depends on the noise parameter .
- The mutual information (A&E)for mixed states is less than for pure states(in terms of Q) and depends on the noise parameter.
- The crossing point moves to higher Q, that for establishing a secret key higher Q is desirable.