Uncertainty Relations and Quantum Information Security

Takayuki Miyadera
Research Center for Information Security
National Institute of Advanced Industrial Science and Technology

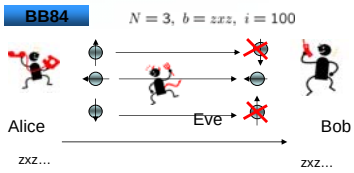
Introduction

The security of Quantum Key Distribution (BB84)

Mayers (1996), Biham-Boyer-Boykin-Mor-Roychowdhury (2000), Shor-Preskill (2000), Koashi (2005), Hayashi (2006)….

Based on Information-Disturbance theorem

An Information theoretical representation of the Uncertainty Relation



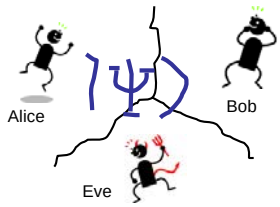
Information gain by Eve induces errors in Bob's outcome = Information-Disturbance theorem

⇩

Alice and Bob can notice the existence of Eve.

Our Generalization [MI4]

BB84= E91



Entropic Uncertainty Relation
Deutsch(1983), Maassen-Uffink(1998), Krishna-Parthasarathy (2002)

$$H(A) + H(B) \geq -2\log\left(\max_{a,b}\|A_a^{1/2}B_b^{1/2}\|\right)$$

$A = \{A_a\}, \quad B = \{B_b\}$ POVMs

A and *B* cannot be *certain* simultaneously, if they are *noncommutative*

noncommutativity

It enables us to treat the general source.

$$I(A:B) + I(\overline{A}:E) \leq H(A) + H(\overline{A}) + 2\log\max_{i,k}\|X[\{p_j,\rho_j\}]_i^{1/2}X[\{q_l,\sigma_l\}]_k^{1/2}\|,$$

Info. Gain by Bob
Ex.) Unbiased case $I(A:B) + I(\overline{A}:E) \leq N$

Info. Gain by Eve

Negative if noncommutative

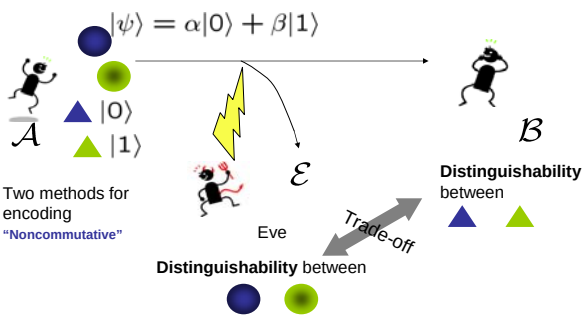
Info. vs. Randomness of Error

[MI1], Hayashi(2006)

$I(A:E|b) \leq H(A \oplus B|\vec{b})$

Another kind of Information-Disturbance

Another measure for dinstinguishability → Another Information-Disturbance theorem

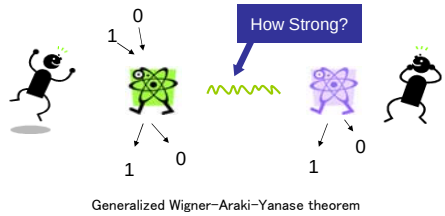


$$\|T^*_{\mathcal{E}}(|\psi\rangle\langle\psi|) - T^*_{\mathcal{E}}(\rho)\|_1 \leq 2|\alpha||\beta|F(T^*_{\mathcal{B}}(|0\rangle\langle 0|), T^*_{\mathcal{B}}(|1\rangle\langle 1|))$$

Measure for distinguishability =Trace distance & fidelity

This formulation can be applied to another quantum impossibility theorem.

The Problem – Information Distribution – [MI2, MI3]



No-cloning theorem for Orthogonal states!

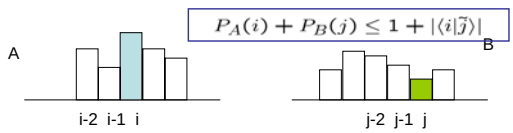
$$|\langle\psi_0|H_S|\psi_1\rangle| \leq \|H_A\|F(\rho_0^S,\rho_1^S) + \|H_S\|F(\rho_0^A,\rho_1^A) + 2\|V_{int}\|$$

If $2\|V_{int}\| < |\langle\psi_0|H_S|\psi_1\rangle|$ holds,

perfect information distribution cannot be attained!

Generalized Landau-Pollak Uncertainty Relation

Landau-Pollak Uncetainty Rel. in its original form Massen-Uffink 1987 (for PVM)



Generalization to Arbitrary num. of General Observables

Theorem [MI5]

Let us consider a Hilbert space $\mathcal{H}$ and a family of m positive operators $\{A_j\}_{j=1}^m$ satisfying $A_j \leq 1$. For any state ρ,

$$\sum_{i=1}^m \langle A_i\rangle_\rho \leq 1 + \left(\sum_{i\neq j}\|A_i^{1/2}A_j^{1/2}\|^2\right)^{1/2},$$

holds.

Summary

- Our generalization enables us to treat the general sources in cryptographic setting.
- Its derivation is based upon the entropic uncertainty relation.
- We can apply the Information-Disturbance theorem for the fidelity and the trace distance directly to the full protocol of BB84.
- It is useful in deriving other quantum impossibilities: Wigner-Araki-Yanase theorem, Heisenberg uncertainty relation.
- We generalize the Landau-Pollak uncertainty relation.

[MI1] T. Miyadera and H. Imai, Information-Disturbance theorem for Unbiased Observables, Phys.Rev.A 73 042317 (2006)
[MI2] T. Miyadera and H. Imai, Wigner-Araki-Yanase theorem on Distinguishability, Phys.Rev.A 74 024101 (2006)
[MI3] T. Miyadera and H. Imai, Strength of Interaction for Information Distribution, Phys.Rev.A **74** 064302 (2006)
[MI4] T. Miyadera and H. Imai, Information-Disturbance theorem and Uncertainty Relation, arxiv.0707.4559
[MI5] T. Miyadera and H. Imai, Generalized Landau-Pollak Uncertainty Relation, Phys.Rev.A **76**, 062108 (2007)