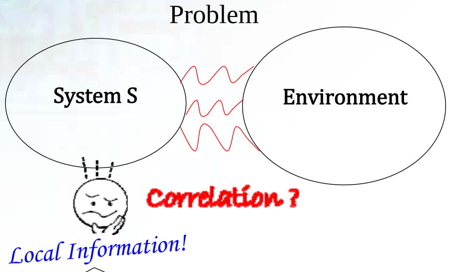
How to detect correlation from local information of subsystem ?

Gen Kimura
Research Center for Information Security
National Institute of Advanced Industrial Science and Technology

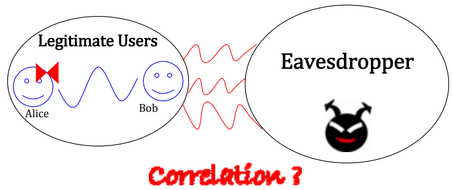
Problem



Can we get information on correlations only from the information of subsystem S ?

Note: Environment is generally infinite systems

Quantum Key Distribution



Problem: How to detect or estimate possible correlations, only from the information of local subsystem ??
Application: To achieve a secure Key Distribution, this problem should be considered
Theory: General Probabilistic Theory, including Classical and Quantum

General Probabilistic Theory

Each Physical System has

- $\mathcal{O}$: set of observables (with Measurable Space: $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$)
- $\mathcal{S}$: set of state (CONVEX (PRE)STRUCTURE)

$$T : (p, s, t) \in [0,1] \times \mathcal{S} \times \mathcal{S} \mapsto \langle p, s, t\rangle \in \mathcal{S}$$

$$\boxed{P : (\Delta, o, s) \in \mathcal{B}(\mathbb{R}) \times \mathcal{O} \times \mathcal{S} \mapsto \Pr\{\Delta \,\|\, s; o\} \in [0,1]}$$

(i) $\forall s \in \mathcal{S}, o \in \mathcal{O}$, $\Delta \in \mathcal{B}(\mathbb{R}) \mapsto \Pr\{\Delta \,\|\, s; o\}$: Probability Measure

(ii) $\forall o \in \mathcal{O}, \Delta \in \mathcal{B}(\mathbb{R})$, $s \in \mathcal{S} \mapsto \Pr\{\Delta \,\|\, s; o\}$: Affine Functional

$$(\Pr\{\Delta \,\|\, \langle p, s, t\rangle; o\} = p\Pr\{\Delta \,\|\, s; o\} + (1-p)\Pr\{\Delta \,\|\, t; o\})$$

Quantum Mechanics

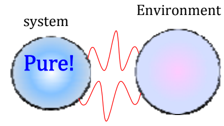
- $\mathcal{O}$: the set of observables $= \mathcal{L}(\mathcal{H})_{sa}$: Self-Adjoint Operators
- $\mathcal{S}$: the set of state $= \mathcal{T}_{+,1}(\mathcal{H})$: Density Operator

$$\langle p, s, t\rangle = ps + (1-p)t \in \mathcal{S}$$

$$\boxed{\Delta \in \mathcal{B}(\mathbb{R}), s \in \mathcal{S}, o \in \mathcal{O}, \Pr\{\Delta \,\|\, s; o\} = \mathrm{Tr}[E^o(\Delta) s]}$$

Static Information on Correlation

If system S is in a pure state,
we can conclude no correlations
with any other environment E

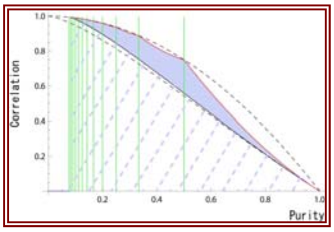


(von Neumann, Lindblad, d'Espagnat, Kimura)

Theorem 1 Let $\omega \in \mathcal{S}_{S+E}$ on No-signaling Physical System.
If the reduced state $\omega_S \in \mathcal{S}_S$ from ω is pure, then ω has no correlations

(Kimura, Koashi 2007)

Quantitative Estimation!



if $S(\rho) = 0$

$$1 + P^2 - \frac{6}{N}P + \frac{4}{N^2} - 2\frac{(N-2)(NP-1)}{N^2}\sqrt{\frac{NP-1}{N-1}}$$
$$\le C(\rho) \le$$
$$P^2 - \frac{6}{M}P + \frac{M^2+4}{M^2} + \frac{2(M-2)(MP-1)}{M^2}\sqrt{\frac{MP-1}{(M-1)}}.$$

$P(\rho_S) = \mathrm{Tr}_S[\rho_S^2]$: Reduced Purity

$C(\rho) = \|\rho - \rho_S \otimes \rho_E\|_2$: Correlation Measure with Hilbert-Schmidt Norm

(Kimura 2004)

Dynamical Information on Correlation

If purity of system S has non-zero time derivative, we "can" conclude non-zero correlation with environment E

(Kimura, Hayashi, Ohno 2007)

(Kimura, Ohno, Mosonyi 2008)

Theorem 4 Let H be a self-adjoint Hamiltonian.
If the variance of H with respect to ρ_{tot} is finite, we have

$$\rho_{tot}(t) = \rho_S \otimes \rho_E \;\Rightarrow P_S'(t) = 0.$$

Theorem 5 Let the Hamiltonian H be bounded with the form $H = H_S \otimes \mathbb{I}_E + \mathbb{I}_S \otimes H_E + H_{int}$, where H_S, H_E, and H_{int} are free Hamiltonian of system S, E and interaction Hamiltonian, respectively. Then, we have

$$|P_S'(t)| \le 4\sqrt{2}\|\rho_S\|\|H_{int}\|\sqrt{I(\rho_{tot})}$$

Future Problems:

* Where is the border of possible perfect correlations between legitimate users, provided that they are in pure state?

* Quantitative estimation for unbounded Hamiltonian

* Generalization of Theorem 4,5 in General Probabilistic Theory