Distillation of secret-key from a class of compound memoryless quantum sources

Gisbert Janßen

(joint work with Holger Boche)

Institute of Theoretical Information Technology
Technische Universität München

9th International Conference on Information Theoretic Security
Tacoma, Washington, USA

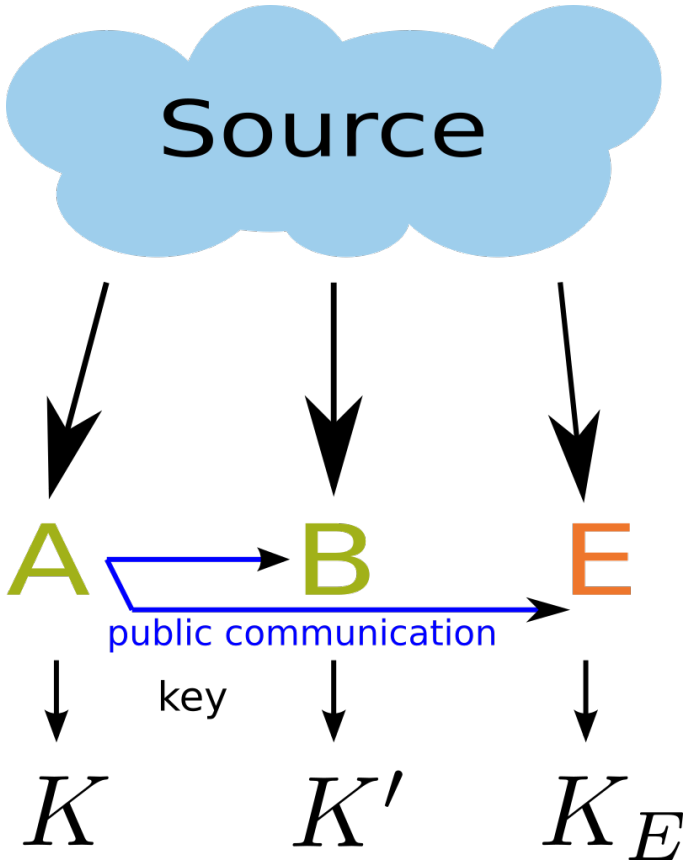
August 10th, 2016

Classical and Quantum IT - Dictionary of Correspondences

Classical Theory	Quantum Theory
Alphabet $\mathcal{X}$	Hilbert space $\mathcal{H}$
Probability distribution $p \in \mathfrak{P}(\mathcal{X})$	Quantum state / Density matrix, $\rho \in \mathcal{L}(\mathcal{H}),\ \rho$ p.s.d, $\mathrm{tr}\rho = 1$
Shannon entropy $H(X)$	von Neumann entropy $S(\rho) := -\mathrm{tr}(\rho \log \rho)$
Classsical mutual informtation $I(X;Y) := H(X) + H(Y) - H(XY)$	Quantum mutual information $I(A;B,\rho_{AB}) := S(\rho_A) + S(\rho_B) - S(\rho_{AB})$
Decision rule $\{D_m\}_{m\in M} \subset 2^{\mathcal{X}}, \bigcup_{m\in M} D_m = \mathcal{X}$	Positive operator valued measure (POVM) $\{E_m\}_{m\in M}, 0 \leq E_m \leq \mathbb{1}_{\mathcal{H}}, \sum_{m\in M} E_m = \mathbb{1}$

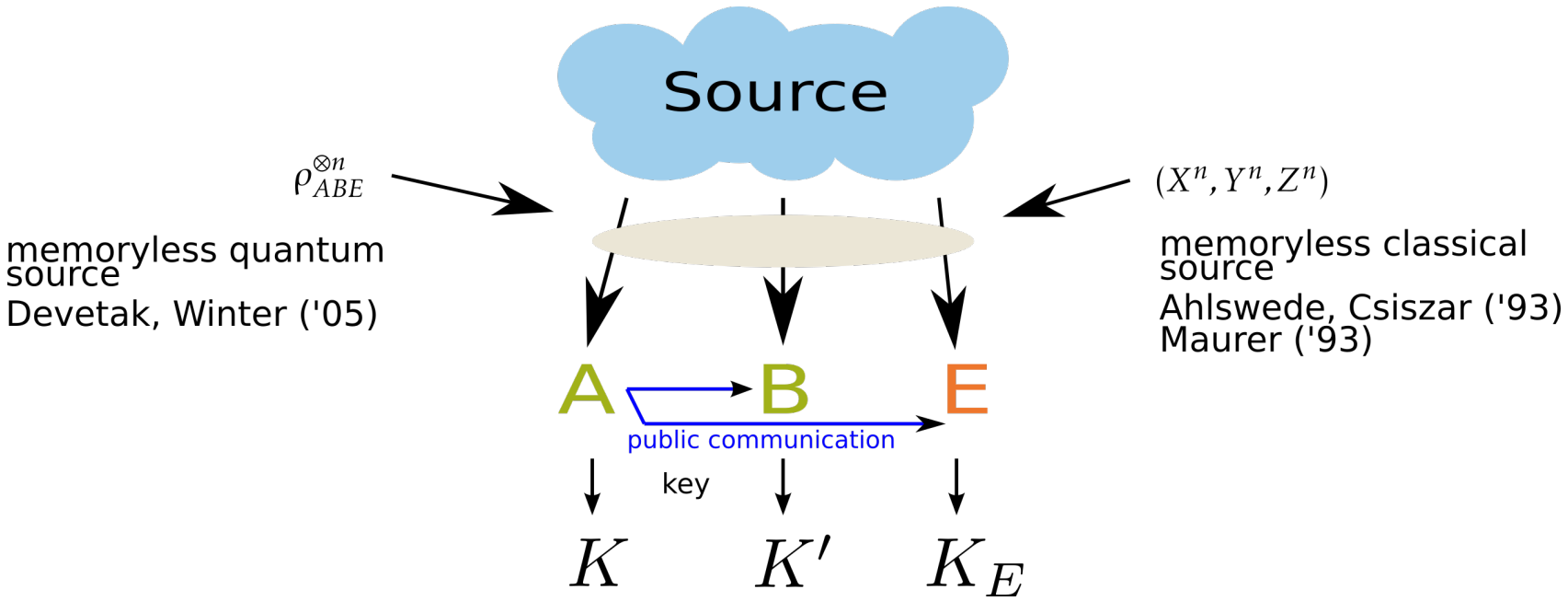
Introduction

- Common randomness shared by users being secure against eavesdropping third parties is a valuable resource in information theory.
- A possibility to obtain secret-keys is to generate it from noisy&insecure correlations distributed by sources.
- We allow public forward communication of classical messages.



Known results

- In case of perfectly known memoryless sources, the asymptotic key capacities where determined



- **Assumption of perfect knowledge of the generating p.d. or density matrix is hardly fulfilled in reality → Need for robust protocols in case of system uncertainty.**

Source model: Compound cqq sources

- n outputs of a compound quantum source $\mathfrak{I} = \{\rho_s\}_{s\in S}$ are described by a density matrix

$$\rho_s^{\otimes n} := \underbrace{\rho_s \otimes \cdots \otimes \rho_s}_{n \text{ times}} \qquad (n \in \mathbb{N})$$

  where s is any of S (unresolved to A and B).

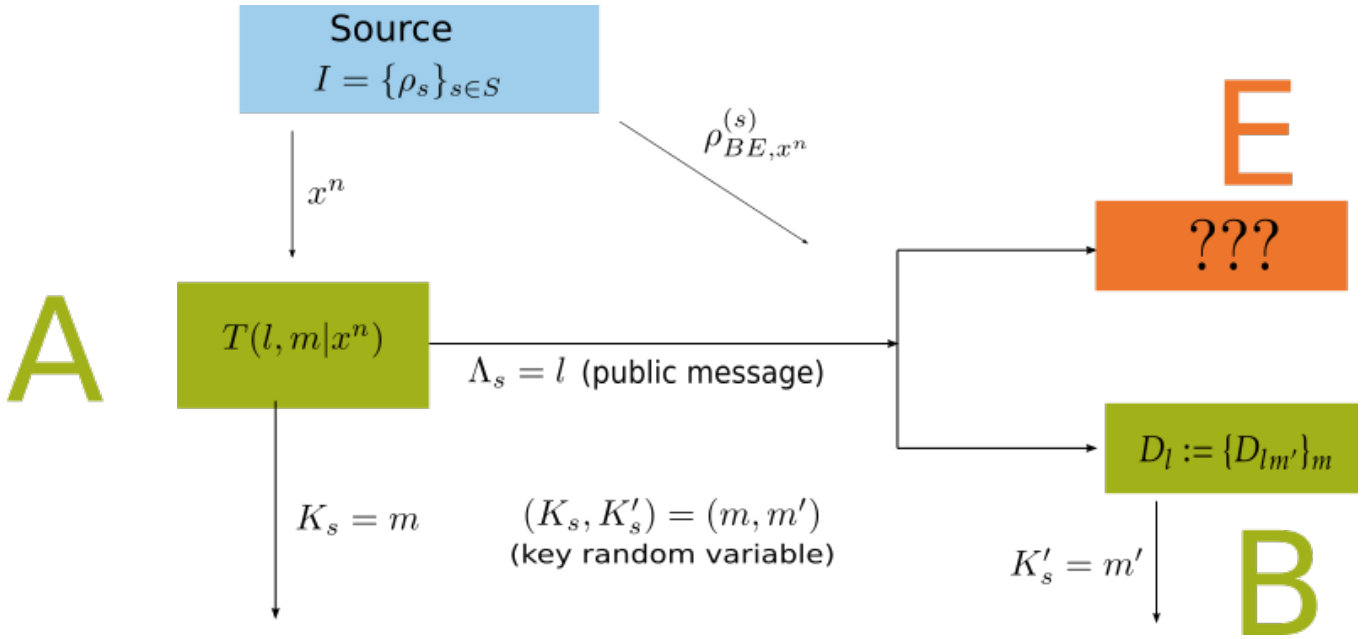
We do not restrict ourselves to $|S| < \infty$ or S countable!

- A compound classical-quantum-quantum (cqq) source is described by a set $\mathfrak{I} := \{\rho_s\}_{s\in S}$ of density matrices on $\mathcal{H}_{ABE}$ such that

$$\rho_s = \sum_{x\in\mathcal{X}} p_s(x)\ |e_x^A\rangle\langle e_x^A| \otimes \rho_{BE,x}^{(s)}$$

  with p_s being a p.d. on $\mathcal{X}$, and $\rho_{BE,x,s}$ a density matrix on $\mathcal{H}_{BE}$ for each $x \in \mathcal{X}$.

Forward secret-key distillation protocols



An (n, M, L, ϵ)-**protocol** for $\mathbb{I} = \{\rho_s\}_{s\in S}$ is a pair (T, D) with

- $(T(l,m|x^n))_{l\in[L],m\in[M],x^n\in\mathcal{X}^n}$ a stochastic matrix
- $D = \{\mathcal{D}_l := \{D_{lm}\}_{m\in[M]}\}_{l\in[L]}$ a collection of POVMs.

such that for all $s \in S$

1. $\Pr(K_s \neq K'_s) \leq \epsilon$, and
2. $\log M - H(K_s) + I(K; E^n\Lambda, \rho_{\Lambda K E^n, s}) \leq \epsilon$.

Operational Interpretation of the performance criteria

- The expression

$$\log M - H(K_s) + I(K; E^n \Lambda, \rho_{\Lambda K E^n, s})$$

quantifies equidistribution and security of the key.

$\rightarrow$ Quantum version of the **security index**.

- Operational significance:

$$I(K; E^n \Lambda, \rho_{\Lambda K E^n, s}) \geq I(K_s; \hat{K}_{E,s})$$

for each eavesdropper's estimate $\hat{K}_E$ of the key random variable ("Holevo bound", Holevo '73).

Definitions

$R \geq 0$ is called an **achievable forward secret-key distillation rate** for $\mathfrak{I}$, if there exists a sequence of $(n, M_n, L_n, \epsilon_n)$ secret-key distillation protocols with

1. $\liminf_{n\to\infty} \frac{1}{n} \log M_n \geq R$,
2. $\limsup_{n\to\infty} \frac{1}{n} \log L_n < \infty$
3. $\lim_{n\to\infty} \epsilon_n = 0$

The **forward secret-key capacity** of $\mathfrak{I}$ is defined by

$$K_{\rightarrow}(\mathfrak{I}) := \sup\{R \geq 0 : \ R \text{ achievable forward secret-key distillation rate}\}$$

Regularity condition

- Define for a set $\mathfrak{I}$ of cqq density matrices

$$\begin{aligned}\mathcal{P}_{\mathfrak{I}} &:= \{p : \ p \text{ marginal p.d. on the } A \text{ system}\}\\ \mathfrak{I}_p^{AE} &:= \{\rho_{AE} : \ \rho \in \mathfrak{I} \ \wedge \ \rho_A = p\}\\ \mathfrak{I}_p^{AB} &:= \{\rho_{AB} : \ \rho \in \mathfrak{I} \ \wedge \ \rho_A = p\}\end{aligned}$$

- **Oberservation**: Some compound cqq sources resist general protocol structures.

  $\rightarrow$ This happens, if members of $\mathfrak{I}$ with nearby A-marginals differ much regarding the sets of AB and AE marginals.

Definition

A set $\mathfrak{I}$ of cqq density matrices is called **regular**, if it fulfills

$$\forall p,q \in \mathcal{P}_{\mathfrak{I}} \ \forall \epsilon > 0 \exists \delta > 0 : \quad \|p-q\|_1 \leq \delta \ \Rightarrow \ d_H(\mathfrak{I}_p^{AB}, \mathfrak{I}_q^{AB}) + d_H(\mathfrak{I}_p^{AE}, \mathfrak{I}_q^{AE}) < \epsilon$$

with $d_H(X,Y)$ being the Hausdorff distance of sets X, Y.

Main result

Theorem

Let $\mathfrak{I}$ be a regular set of cqq density matrices in $\mathcal{H}_{ABE}$. It holds

$$K_{\rightarrow}(\mathfrak{I}) \;=\; \lim_{k\to\infty} \frac{1}{k}\, K_{\rightarrow}^{(1)}(\mathfrak{I}^{\otimes k}),$$

where

$$K_{\rightarrow}^{(1)}(\mathfrak{I}^{\otimes k}) := \inf_{p\in\mathcal{P}_{\mathfrak{I}}} \sup_{\Gamma:=T\leftarrow U\leftarrow p^k} \left(\inf_{\sigma\in\mathfrak{I}_p^{AB}} I(U;B^k|T,\sigma_{k,\Gamma}) - \sup_{\sigma\in\mathfrak{I}_p^{AE}} I(U;E^k|T,\sigma_{k,\Gamma}) \right)$$

with the maximization being over all Markov chains $T \leftarrow U \leftarrow p^k$ resulting from application of Markov transition matrices $P_{T|U}$, $P_{U|Y}$ and

$$\sigma_{k,\Gamma} := \sum_{x^k\in\mathcal{X}^k} \sum_{t\in\mathcal{T}} \sum_{u\in\mathcal{U}} P_{T|U}(t|u)\, P_{U|X^k}(u|x^k)\, p^k(x^k)\; |t\rangle\langle t| \otimes |u\rangle\langle u| \otimes \sigma_{x^k}$$

$I(X;YZ|T) := \sum_{t\in\mathcal{T}} P_T(t) I(X;Y|T=t)$ conditional quantum mutual information of cqq state.

Operational significance of regularity

- Regularity of cqq sources is not only a technical issue.
- If A has additional perfect knowledge of his/her distribution p, regularity plays no role.
- Define $K_{\rightarrow,SMI}$ to be the forward secret-key capacity with sender marginal knowledge.

Theorem

For each set $\mathfrak{I}$ of cqq density matrices, it holds

$$K_{\rightarrow,SMI}(\mathfrak{I}) = \lim_{k\rightarrow\infty} \frac{1}{k} K_{\rightarrow}^{(1)}(\mathfrak{I}^{\otimes k}).$$

Consequently

$$K_{\rightarrow}(\mathfrak{I}) = K_{\rightarrow,SMI}(\mathfrak{I}),$$

if $\mathfrak{I}$ is regular.

Advantage of SMI - Example

We present, with $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}_E = \mathbb{C}^2 \otimes \mathbb{C}^2$ example of a compound cqq source $\mathfrak{I}$ with

$$0 = K_{\rightarrow}(\mathfrak{I}) < K_{\rightarrow,SMI}(\mathfrak{I}) = \log \dim \mathcal{H}_A.$$

Define with π being the bit equidistribution, and $\Pi := \frac{\mathbb{1}_{\mathbb{C}^2}}{2}$ the maximally mixed qubit density matrix

$$\rho_p := \begin{cases} \sum_{x,y=1}^{2} \pi(x) \cdot \pi(y) \cdot |x,y\rangle\langle x,y|_A \otimes |x\rangle\langle x|_B \otimes \Pi_B \otimes \Pi_E \otimes |y\rangle\langle y|_E & \text{if } p = \pi \\ \sum_{x,y=1}^{2} \pi(x) \cdot p(y) \cdot |x,y\rangle\langle x,y|_A \otimes \Pi_B \otimes |y\rangle\langle y|_B \otimes |x\rangle\langle x|_E \otimes \Pi_E & \text{otherwise,} \end{cases}$$

The compound cqq source generated by $\mathfrak{I} := \{\rho_p\}_{p \in \mathcal{P}(\{0,1\})}$ has the stated properties.

References

H. Boche, G. Janßen.
"Distillation of secret-key from a class of compound memoryless quantum sources",
J. Math. Phys. **57**, 082201 (2016).

(or on the purple USB Stick)