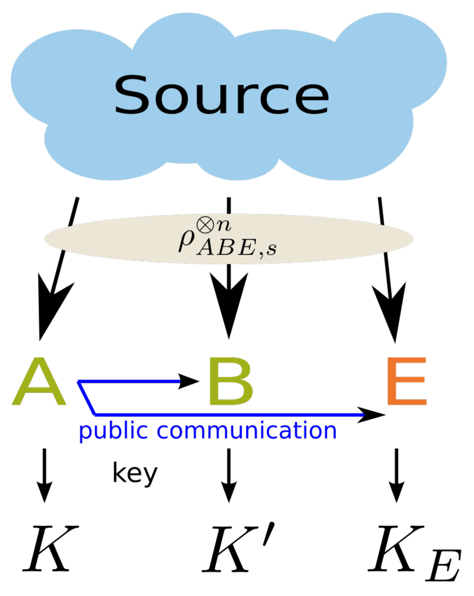
Forward secret-key distillation from compound memoryless classical-quantum-quantum sources

H. Boche, G. Janßen
Lehrstuhl für Theoretische Informationstechnik, TU München

Introduction

- Common randomness shared by users being secure against eavesdropping third parties is a valuable resource in information theory.
- Seminal results are determination of key capacities with free public forward communication for memoryless classical [3] and quantum [2] sources.

Assumption: perfectly known source state $\rightarrow$ Need for results with system uncertainty

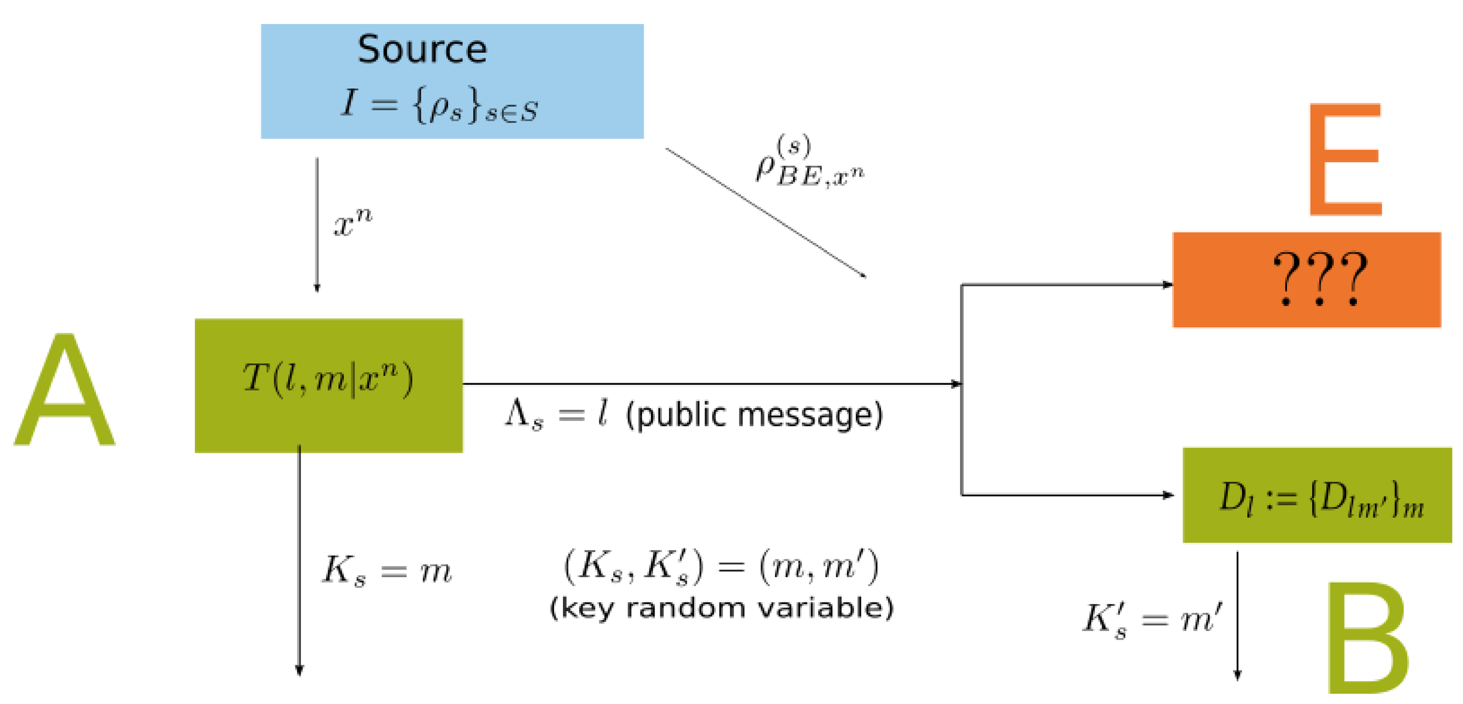


Source model - Compound memoryless cqq source

- We consider tripartite **memoryless classical-quantum-quantum (cqq) sources** on $\mathcal{H}_{ABE}$ with generating states of the form
$$\rho = \sum_{x\in\mathcal{X}} p(x)\,|x\rangle\langle x| \otimes \rho_{BE,x}$$
- A **compound cqq source** is generated by a set $\mathfrak{I} := \{\rho_s\}_{s\in S}$ of cqq density matrices, i.e. each n block of source outputs has density matrix
$$\rho_s^{\otimes n} := \rho_s \otimes \cdots \otimes \rho_s, \qquad \text{with any } s \in S.$$

Forward secret-key distillation protocols

A schematic view of a **forward-secret key distillation protocol**:



An (n, M, L, ϵ)**-protocol** for $\mathfrak{I} = \{\rho_s\}_{s\in S}$ 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

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

Operational Interpretation of the performance criteria

- The second performance criterion quantifies equidistribution and security of the key $\rightarrow$ Quantum version of the **security index**.
- Operational significance:
$$I(K; E^n\Lambda, \rho_{\Lambda KE^n,s}) \geq I(K; \hat{K}_E)$$
for each eavesdropper's estimate $\hat{K}_E$ of the key random variable (Holevo bound).

Definitions

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

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

The **forward secret-key capacity** of $\mathfrak{I}$ is given by
$$K_{\rightarrow}(\mathfrak{I}) := \sup\{R \geq 0 : \ R \text{ achievable forward secret-key distillation rate}\}$$

Regularity condition

- **Oberservation**: Some compound cqq sources resist general protocol structures, if members of $\mathfrak{I}$ with nearby A-marginals differ much regarding the sets of AB and AE marginals.
- A set $\mathfrak{I}$ of cqq density matrices is called **regular**, if for each $\epsilon > 0$ there exists a $\delta > 0$, such that the implication
$$\|p - q\|_1 \leq \delta \Rightarrow d_H(\mathfrak{I}^{AB}_p, \mathfrak{I}^{AB}_q) + d_H(\mathfrak{I}^{AE}_p, \mathfrak{I}^{AE}_q) < \epsilon$$
holds for each p, q being possible A-marginals. $d_H(X, Y)$ denotes the Hausdorff distance of sets X, Y, and $\mathfrak{I}^{AB}_p, \mathfrak{I}^{AE}_p$ being the sets of AB (AE) marginal states deriving from $\mathfrak{I}$ with A-marginal P.D. p.

Theorem

Let $\mathfrak{I}$ be a regular set of cqq density matrices in $\mathcal{H}_{ABE}$. It holds
$$K_{\rightarrow}(\mathfrak{I}) = \lim_{k\to\infty} \frac{1}{k} K^{(1)}_{\rightarrow}(\mathfrak{I}^{\otimes k}),$$
where for a set $\mathfrak{A} := \{\sum_{y\in\mathfrak{Y}} p(y)\,|y\rangle\langle y| \otimes \sigma_y\}$,
$$K^{(1)}_{\rightarrow}(\mathfrak{A}) := \inf_{p\in\mathcal{P}_{\mathfrak{A}}} \sup_{\Gamma := T\leftarrow U\leftarrow Y_p} \left(\inf_{\sigma\in\mathfrak{A}_p} I(U; B|T, \sigma_\Gamma) - \sup_{\sigma\in\mathfrak{A}_p} I(U; E|T, \sigma_\Gamma) \right)$$
with the maximization being over all Markov chains $T \leftarrow U \leftarrow Y_p$ resulting from application of Markov transition matrices $P_{T|U}$, $P_{U|Y}$ and
$$\sigma_\Gamma := \sum_{y\in\mathcal{Y}} \sum_{t\in\mathcal{T}} \sum_{u\in\mathcal{U}} P_{T|U}(t|u) P_{U|Y}(u|y) p(y)\,|t\rangle\langle t| \otimes |u\rangle\langle u| \otimes \sigma_y$$

Operational significance of regularity

- Regularity of cqq sources is not only a technical issue.
- If A has additional perfect knowledge of his distribution p, regularity plays no role.
- For the forward secret-key capacity with **Sender Marginal Information**, it holds regardless of regularity
$$K_{\rightarrow,SMI}(\mathfrak{I}) = \lim_{k\to\infty} \frac{1}{k} K^{(1)}_{\rightarrow}(\mathfrak{I}^{\otimes k}),$$
- 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
$$\rho_p := \begin{cases} \sum_{x,y=1}^{2} \pi(x)\cdot\pi(y)\cdot|x,y\rangle\langle x,y|_A \otimes |x\rangle\langle x|_B \otimes \Pi_B \otimes \Pi_E \otimes |y\rangle\langle y|_E & \text{if } p = \pi \\ \sum_{x,y=1}^{2} \pi(x)\cdot p(y)\cdot|x,y\rangle\langle x,y|_A \otimes \Pi_B \otimes |y\rangle\langle y|_B \otimes |x\rangle\langle x|_E \otimes \Pi_E & \text{otherwise,} \end{cases}$$
The compound cqq source generated by $\mathfrak{I} := \{\rho_p\}_{p\in\mathcal{P}(\{0,1\})}$ has the stated properties.

Weak regularity - hemi-continuity of set-valued maps

- The class of regular compound cqq sources can even be enlarged by considering the general theory of set-valued maps.
$$p \mapsto \mathfrak{I}^{AB}_p \text{ and } p \mapsto \mathfrak{I}^{AE}_p \text{ lower hemi-continuous } \Rightarrow \exists \text{ regular approximation of } \mathfrak{I}$$
- More information on weak regularity $\rightarrow$ [1].

References

[1] H. Boche, G. Janßen, arXiV:1604.05530 (2016).
[2] I. Devetak, A. Winter, Proc. R. Soc. A **461**, 207–235 (2005).
[3] R. Ahlswede, I. Csiszár, IEEE Trans. Inf. Th. **39**, 1121–1139 (1993).
[4] N. Tavangaran et al., arXiv:1601.07513 (2016).

{boche, gisbert.janssen}@tum.de