Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression

(arXiv:2009.08823 [quant-ph])

Toyohiro Tsurumaru

Mitsubishi Electric Corporation

Abstract: Privacy amplification (PA) is an indispensable component in classical and quantum cryptography. Error correction (EC) and data compression (DC) algorithms are also indispensable in classical and quantum information theory. We here study these three algorithms (PA, EC, and DC) in the presence of quantum side information, and show that they all become equivalent in the one-shot scenario. As an application of this equivalence, we take previously known security bounds of PA, and translate them into coding theorems for EC and DC which have not been obtained previously. Further, we apply these results to simplify and improve our previous result that the two prevalent approaches to the security proof of quantum key distribution (QKD) are equivalent. We also propose a new method to simplify the security proof of QKD.

Outline

- We show that the following three classical algorithms are equivalent:
  Privacy amplification (PA), Error correction (EC), Data compression (DC)
  in the sense that their performance indices(security parameter or failure probability) exactly equal.
- Conditions: 1. Security of PA is evaluated by the purified distance.
  2. All Classical algorithms are linear (linear hash functions, linear codes).

Security criteria using the purified distance

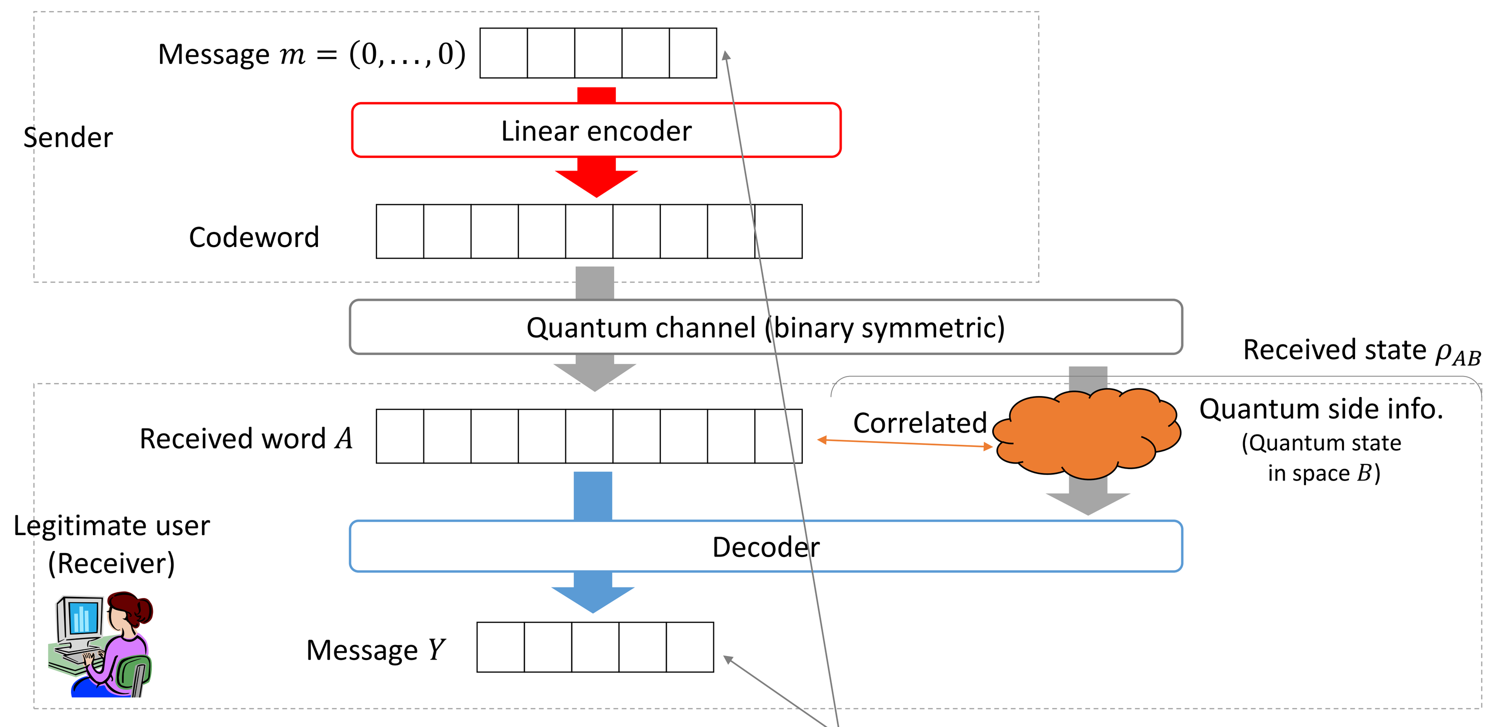
- The security is usually evaluated by the trace distance between the actual and ideal states.

$$d_1(\rho_{KE}) := \left\|\rho_{KE} - \rho_{KE}^{\mathrm{ideal}}\right\|_1$$

- Here we instead use the purified distance [1]: $Q^{\mathrm{PA}}(\rho_{AE}) := 1 - F\left(\rho_{KE}, \rho_{KE}^{\mathrm{ideal}}\right)^2$
- We do not lose the generality since $1 - \sqrt{1 - Q^{\mathrm{PA}}(\rho_{AE})} \leq d_1(\rho_{KE}) \leq 2\sqrt{Q^{\mathrm{PA}}(\rho_{AE})}$

Setting: Two classical algorithms (We here omit data compression for the sake of simplicity)

Error correction (EC) with quantum side information



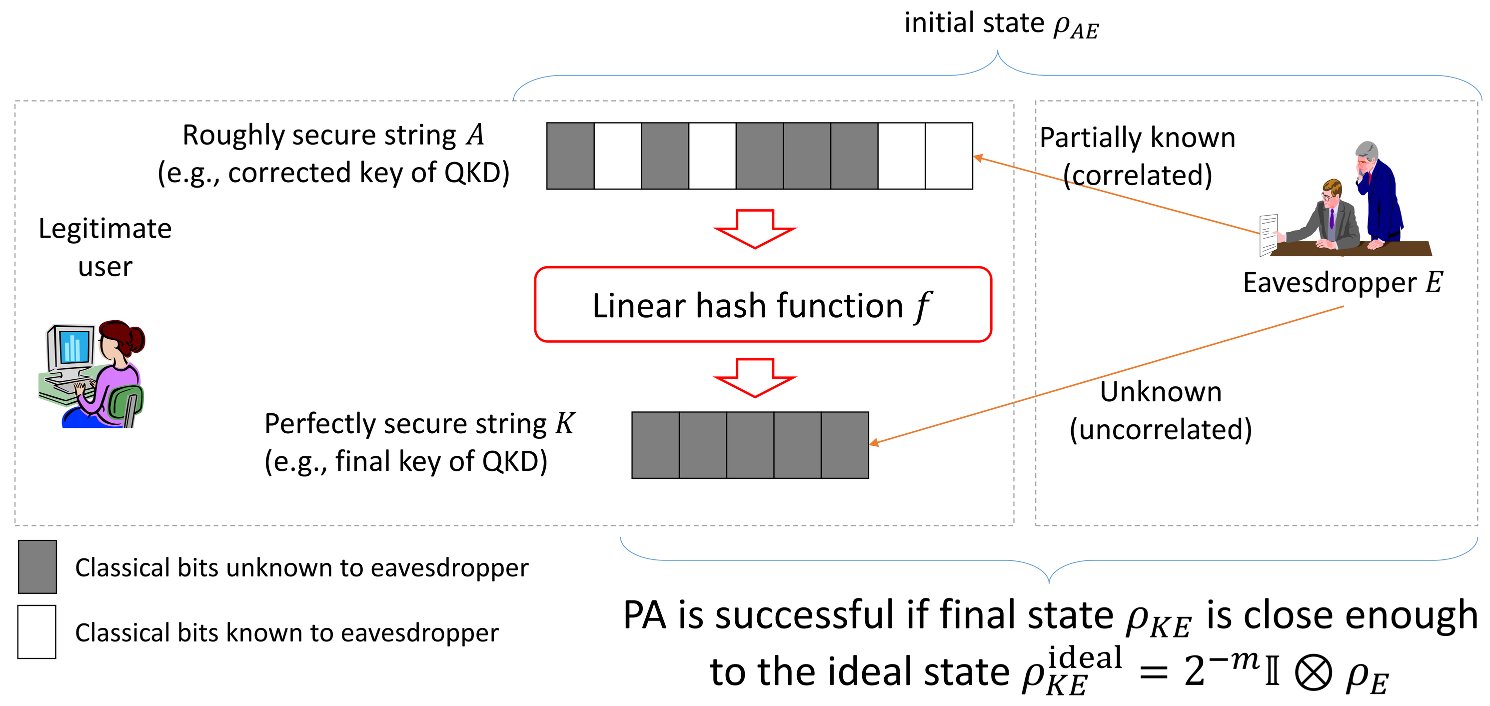
EC is successful if these two strings equal.

We evaluate the performance of EC by the failure probability:

$$Q^{\mathrm{EC},g}(\rho_{AB}) = \Pr[Y \neq 0 \mid \rho_{AB}]$$

Privacy Amplification (PA)

- A process of converting a "roughly secure" string into a "perfectly secure" string



PA is successful if final state ρ_{KE} is close enough to the ideal state $\rho_{KE}^{\mathrm{ideal}} = 2^{-m}\mathbb{I} \otimes \rho_E$

We evaluate the security of PA by the purified distance:

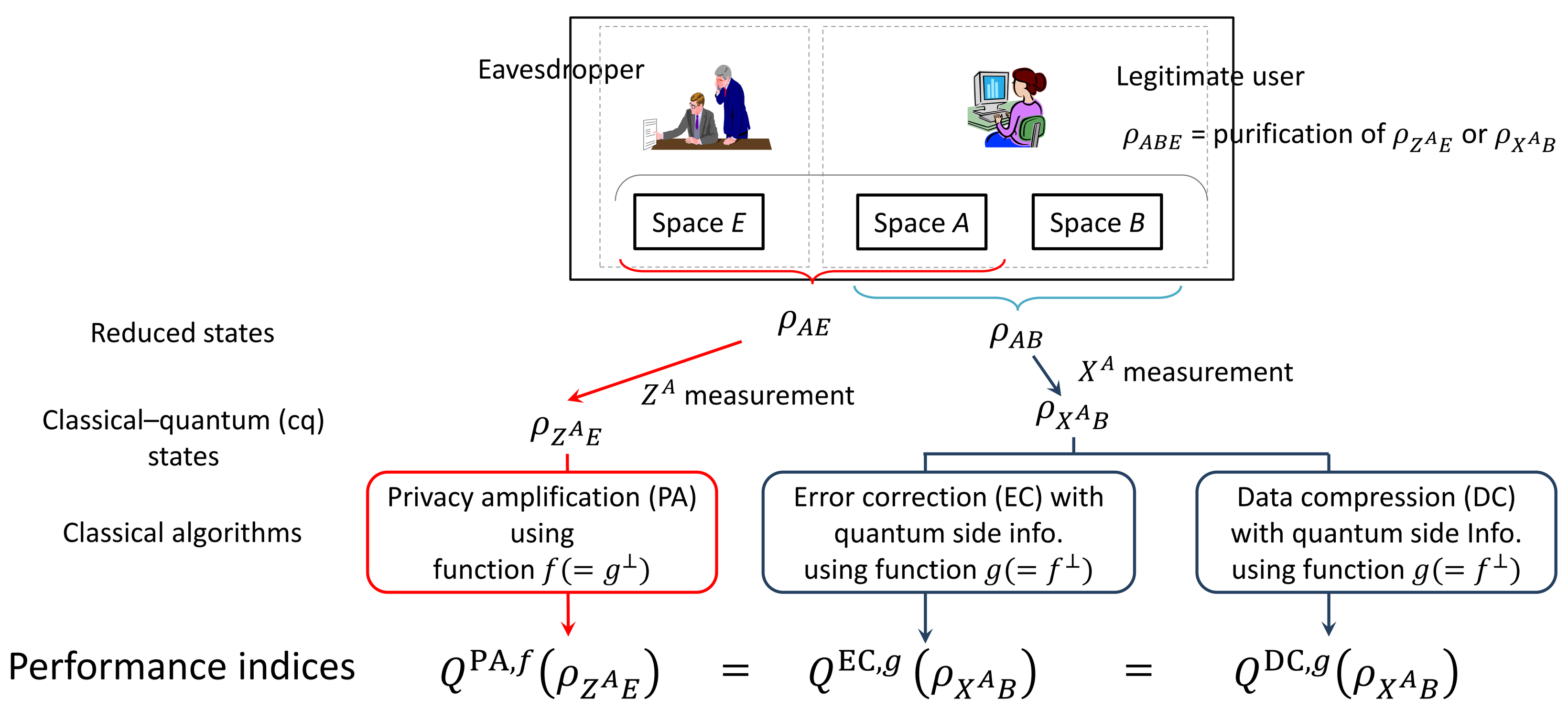
$$Q^{\mathrm{PA}}(\rho_{AE}) := 1 - F\left(\rho_{KE}, \rho_{KE}^{\mathrm{ideal}}\right)^2$$

Main Theorems

1. PA, EC, and DC are equivalent in that: (in fact obtained previously by Renes 2017 [2])
   - There is a one-to-one correspondence between each situations† of PA, EC, and DC.
     †Initial states $\rho_{Z^A E}, \rho_{X^A B}$ and functions f, g.
   - Their performance indices all equal: $Q^{\mathrm{PA},f}(\rho_{Z^A E}) = Q^{\mathrm{EC},g}(\rho_{X^A B}) = Q^{\mathrm{DC},g}(\rho_{X^A B})$,
2. (When functions f, g are randomized) The security bounds for PA, and the coding theorems for EC and DC are also equivalent:
   - Leftover hashing lemma (LHL) for PA: $\mathrm{E}_F Q^{\mathrm{PA},F}(\rho_{Z^A E}) \leq r\left(H_{\min}(Z^A|E)_\rho\right)$
   - Coding theorem for EC: $\mathrm{E}_F Q^{\mathrm{EC},F^\perp}(\rho_{X^A B}) \leq r\left(n - H_{\max}(X^A|B)_\rho\right)$
   - Coding theorem for DC: $\mathrm{E}_F Q^{\mathrm{DC},F^\perp}(\rho_{X^A B}) \leq r\left(n - H_{\max}(X^A|B)_\rho\right)$

   (With r being any function)

Conditions: 1. There exists a pure state ρ_{ABE}, which is a purification of $\rho_{Z^A E}$ or $\rho_{X^A B}$,
2. Classical linear functions f, g are dual to each other:
$f = g^\perp$ (meaning $\ker f = (\ker g)^\perp$).



Application to QKD

The main theorems give a direct connection between Renner's approach and the Shor-Preskill approach to the security proof (Refinement of our previous result [3]).

Renner's approach:

LHL in the purified distance:

$$\mathrm{E}_F Q^{\mathrm{PA},F}(\rho_{Z^A E}) \leq 2^{m - H_{\min}(Z^A|E)_\rho}$$

⇕ Equivalent (main theorems)

The Shor-Preskill approach:

Coding theorem for phase error correction:

$$\mathrm{E}_F Q^{\mathrm{EC},F^\perp}(\rho_{X^A E}) \leq 2^{H_{\max}(X^A|B)_\rho - (n-m)}$$

One can also derive

The conventional LHLs (in terms of the trace distance):

$$\mathrm{E}_F \ \frac{1}{2}\left\|\rho_{KE}^F - \rho_{KE}^{\mathrm{ideal}}\right\|_1 \leq \sqrt{\mathrm{E}_F Q^{\mathrm{PA},F}(\rho_{Z^A E})} \leq \sqrt{2^{m - H_{\min}(Z^A|E)_\rho}}$$

$$\mathrm{E}_F \ \frac{1}{2}\left\|\rho_{KE}^F - \rho_{KE}^{\mathrm{ideal}}\right\|_1 \leq \sqrt{\mathrm{E}_F Q^{\mathrm{EC},F^\perp}(\rho_{X^A B})} \leq \sqrt{2^{H_{\max}(X^A|B)_\rho - (n-m)}}$$

References:

[1] R. Koenig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," ," IEEE Transactions on Information Theory, Volume 55, Issue 9, 4337 - 4347 (2009).
[2] R. Renes, "Duality of channels and codes," IEEE Transactions on Information Theory 64, 577 (2018).
[3] T. Tsurumaru, "Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution," IEEE Transactions on Information Theory, Volume 66, Issue 6, 3465 - 3484 (2020).