Presentation for the Quantum Seminar

José Manuel Rodríguez Caballero

University of Tartu

Spring 2020

Subject

My presentation is about the paper[1]:

> *Bouman, Niek J., and Serge Fehr. "Sampling in a quantum population, and applications." Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2010. URL = https://arxiv.org/pdf/0907.4246.pdf*

[1] I will not repeat the notation from the paper in this presentation. If someone needs a clarification, please, either ask me during the presentation or read Bouman-Fehr paper.

Outline

The main contributions of Bouman-Fehr paper are the following.

(I) Introduction of a theory of *sampling and estimate strategies* for classical and quantum populations.

(II) A new proof of the security of the protocol for quantum key distribution BB84 (and the entanglement-based version of it).

(III) A new proof of the security of the protocol Quantum Oblivious Transfer[2] (QOT).

[2] We consider that (i) and (ii) are enough in order to understand the technique developed Bouman-Fehr paper. So, we will omit (iii) in this presentation because of time constrains.

Brief History

(i) The protocol BB84, developed by Charles Bennett and Gilles Brassard[3] in 1984, was the first quantum key distribution protocol.

(ii) An entanglement-based version of BB84 was proposed by Artur K. Ekert[4] in 1991. The security of this version of BB84 implies the security of the original protocol.

(iii) The first security proof of BB84 was published by Dominic Mayers[5] in 1996.

---

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, (IEEE Press, 1984), pp. 175–179

[4] Artur K. Ekert. Quantum cryptography based on Bell's theorem. Physical Review Letter, 67(6):661–663, August 1991.

[5] Mayers, D. 1996. Quantum key distribution and string oblivious transfer in noisy channels. Advances in Cryptology–Proceedings of Crypto '96 (Aug.). Springer-Verlag, New York, pp. 343–357

Description

Let $n \geq 2$ and $1 \leq k \leq \frac{n}{2}$ be the integer parameters of the following protocol. The entanglement-based BB84 protocol can be divided into the following steps[6].

(i) Qubit distribution.

(ii) Error estimation.

(iii) Error correction.

(iv) Key distillation.

[6] The explanation of each step will be developed in the next slides

Qubit distribution

(i) Alice prepare n EPR pairs $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

(ii) Alice sends one qubit for each pair to Bob.

(iii) Bob confirms the receipt of the qubits.

(iv) Alice picks random $\theta \in \{0,1\}^n$ and send it to Bob.

(v) Alice and Bob measure their respective qubits in basis θ (0 for computational, 1 for Hadamard) and the results of the measurements are registered in x and y respectively.

Error estimation

(i) Alice chooses a random subset $s \subset [n]$ of size k and send it to Bob.

(ii) Alice and Bob exchange x_s and y_s.

(iii) Alice and Bob both compute $\omega\left(x_s \oplus y_s\right)$.

Error correction

(i) Alice send the syndrome **syn** of $x_{\overline{S}}$ to Bob with respect to a suitable linear error correcting code. Let m be the bit-size of **syn**.

(ii) Bob uses **syn** to correct the errors in $y_{\overline{S}}$ and obtains $\hat{x}_{\overline{S}}$.

Key distillation

(i) Alice chooses a random seed r for a universal hash function g with range $\{0,1\}^{\ell}$, where $\ell < (1 - h(\beta))\, n - k - m$ (or $\ell = 0$ if the right-hand side is not positive).

(ii) Alice sends r to Bob.

(iii) Alice and Bob compute their keys $\mathbf{k} := g(r, x_{\overline{s}})$ and $\hat{\mathbf{k}} := g(r, \hat{x}_{\overline{s}})$.

Security claim (statement)

Consider an execution of the entanglement-based BB84 in the presence of an adversary Eve. Let $\mathbf{K}$ be the key obtained by Alice, and let E be Eve's quantum system at the end of the protocol. Let $\tilde{\mathbf{K}}$ be chosen uniformly at random of the same bit-length as $\mathbf{K}$. Then, for any $0 < \delta \leq \frac{1}{2} - \beta$, the inequality

$$\begin{aligned} \Delta\left(\rho_{\mathbf{K}E}, \rho_{\tilde{\mathbf{K}}E}\right) \quad &\leq \quad \frac{1}{2}\exp\left[-\frac{\ln 2}{2}\Big((1-h(\beta+\delta))n - k - m - \ell\Big)\right] \\ &\quad\; +2\exp\left(-\frac{\delta^2 k}{6}\right) \end{aligned}$$

holds.

Security claim (application)

Let $\varepsilon > 0$. The security claim can be used in order compute a possible value for ℓ such that $\Delta\left(\rho_{\mathbf{K}E}, \rho_{\tilde{\mathbf{K}}E}\right) \leq \varepsilon$.

Security proof (sketch)

There is a quantum state $\rho_{\beta,\delta}$ satisfying the following conditions.

(i) Quantum error:

$$\Delta\left(\rho_{\mathbf{K}E}, \rho_{\beta,\delta}\right) \leq 2\exp\left(-\frac{\delta^2 k}{6}\right).$$

(ii) Privacy amplification:

$$\Delta\left(\rho_{\beta,\delta}, \rho_{\tilde{\mathbf{K}}E}\right) \leq \frac{1}{2}\exp\left[-\frac{\ln 2}{2}\Big((1-h(\beta+\delta))n - k - m - \ell\Big)\right].$$

Applying triangular inequality we get the desired result.

Motivation

In this presentation, the motivation for introducing the theory of sampling and estimation strategies for quantum and classical populations is to guarantee the existence of the quantum state $\rho_{\beta,\delta}$ satisfying the conditions of the previous slide.

Main definition

Let $\mathcal{I}$ be a finite set of indices, $\mathcal{S}$ be a finite set of seeds and $\mathcal{A}$ be a finite alphabet. Define $\mathcal{T} := 2^{\mathcal{I}}$. A *sampling and estimation strategy* (a *strategy* for short) is given[7] by $\Psi := (\mathcal{A}, \mathcal{I}, \mathcal{S}, P_{TS}, f)$, where P_{TS} is a probability distribution over $\mathcal{T} \times \mathcal{S}$ and f is a real-valued function over

$$\mathrm{Dom}_f := \bigcup_{(t,s)\in\mathcal{T}\times\mathcal{S}} \left\{(t, q, s) : \quad q \in \mathcal{A}^t\right\}.$$

[7] Our definition is slightly different of the definition given in Bouman-Fehr paper, but equivalent to it.

Main example

Strategy $\Psi_{n,k}$: Pairwise one-out-of-two sampling, using only part of the sample.

Consider the integer parameters $n \geq 2$ and $1 \leq k \leq \frac{n}{2}$. Let $\mathcal{A} := \{0,1\}$, $\mathcal{I} := [n] \times \{0,1\}$ and $\mathcal{S} := \mathcal{T}$. The probability distribution P_{TS} is given by

$$P_{TS}(t,s) = \frac{1}{2^n \binom{n}{k}}$$

if for some $(j_1, \ldots, j_n) \in \{0,1\}^n$ we have $t = \{(\ell, j_\ell) : \quad 1 \leq \ell \leq n\}$, $|s| = k$ and $s \subset t$. Otherwise, $P_{TS}(t,s) := 0$. Furthermore, $f(t,q,s) := \omega(q_s)$.

Existence of $\rho_{\beta,\delta}$ and quantum error (sketch)

(i) The error estimation phase in the protocol is interpreted as strategy $\Psi_{n,k}$.

(ii) The classical error of the strategy is bounded above by $4\exp\left(-\frac{\delta^2 k}{3}\right)$ using well-known techniques from probability theory (Hoeffding's inequality).

(iii) The quantum error of the strategy is bounded above by the square root of the classical error of the strategy, i.e., $2\exp\left(-\frac{\delta^2 k}{6}\right)$.

(iv) According to the definition of the quantum error, there exists a state $\rho_{\beta,\delta}$, which is a superposition of states having relative Hamming weight[8] δ-close to β, for which $\Delta\left(\rho_{\mathbf{K}E}, \rho_{\beta,\delta}\right)$ is bounded above by the quantum error, *a fortiori* by $2\exp\left(-\frac{\delta^2 k}{6}\right)$.

[8] The basis from which the Hamming weight is taken are the Hadamard basis for Alice and the computational basis for Bob.

Privacy amplification (sketch)

(i) The fact that $\rho_{\beta,\delta}$ is a superposition of states having relative Hamming weight δ-close to β implies the inequality

$$H_{\min}(W|\Theta\, Z\, S\, E_0) \geq (1 - h(\beta + \delta))\, n.$$

(ii) Applying the chain rule to the inequality above, we get

$$H_{\min}(X_{\overline{S}}|\Theta\, Z\, X_S\, \mathbf{SYN}\, E_0) \geq (1 - h(\beta + \delta))\, n - k - m.$$

(iii) In virtue of the privacy amplification inequality, $\Delta\left(\rho_{\beta,\delta}, \rho_{\tilde{\mathbf{K}}E}\right) \leq \frac{1}{2} \cdot 2^{\left(H_{\min}(X_{\overline{S}}|\Theta\, Z\, X_S\, \mathbf{SYN}\, E_0) - \ell\right)/2}$.

From (ii) and (iii) we conclude the desired inequality.

End of my presentation