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 a 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 $\mathbf{k} := g(r, x_{\bar{s}})$ and $\hat{\mathbf{k}} := g(r, \hat{x}_{\bar{s}})$.

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

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

holds.

Security claim (application)

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

Sketch of the proof

There is a quantum state

$$\rho = \sum_{\substack{b \in \{0,1\}^n \\ |\omega(b) - \beta| \le \delta}} |b\rangle |\varphi_E^b\rangle$$

satisfying

(i) Quantum error inequality:

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

(ii) Privacy amplification:

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

Applying triangular inequality we get the desired result.

End of my presentation