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.*

My presentation may differ in some points with respect of the presentation given by the authors, because sometimes I prefer to use my own interpretation of the results rather than to repeat the authors.

[1] I will not repeat the notation from the paper in this presentation. If any listener is interested in clarification, either read the paper or ask me.

Contributions of the paper

Contribution 1. The authors introduce a framework in for *sampling quantum population*.

Contribution 2. This framework is used in a new proof of the security of the *quantum key distribution protocol BB84* (entanglement-based version).

Contribution 3. This framework is used in a new proof of the security of the *quantum oblivious-transfer from bit-commitment*.

Presentation of Contribution 1.

The authors introduce a framework in for *sampling quantum population*.

Classical sampling strategy

Let $\mathcal{A}$ be a finite alphabet. A *classical sampling strategy* is a triplet $\Psi = (P_T, P_S, f)$, where P_T is a distribution over $\mathcal{T} := 2^{[n]}$, P_S is a distribution over a finite set $\mathcal{S}$, P_T and P_S are assumed to be independent, and f is a function of type[2]

$$\begin{aligned} \mathcal{T} \times \mathcal{S} \times \mathcal{A}^* &\longrightarrow \mathbb{R} \\ (t, s, q) &\mapsto f_{t,s}(q) \end{aligned}$$

satisfying $f_{t,s}(q) = 0$ whenever $|t| \neq |q|$.

[2] Here $\mathcal{A}^*$ is the free monoid over $\mathcal{A}$.

Presentation of Contribution 2.

This framework is used in a new proof of the security of the *quantum key distribution protocol BB84* (entanglement-based version).

Presentation of Contribution 3.

This framework is used in a new proof of the security of the *quantum oblivious-transfer from bit-commitment*.

End of my presentation