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.

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

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 n be a positive integer, $\mathcal{A}$ be a finite alphabet and $\mathcal{S}$ be a finite set of seeds[2]. A *classical sampling strategy* is a triplet (P_T, P_S, f), where P_T is a probability distribution over $\mathcal{T} := 2^{[n]}$, P_S is a probability distribution over $\mathcal{S}$ and f is a real-valued function defined on the set

$$\{(t, q, s) \in \mathcal{T} \times \mathcal{A}^* \times \mathcal{S} : \quad |t| = |q|\}.$$

[2] Both "alphabet" and "seeds" are informal labels notions here in order to show the motivation for introducing these sets.

δ-estimation

Let δ be a positive real number. We define

$$B_{t,s}^{\delta} := \left\{ q \in \mathcal{A}^n : \quad \left| \omega\left(q_{\bar{t}}\right) - f\left(t, q_t, s\right) \right| < \delta \right\}.$$

δ-estimation random variable

Let T and S be random variables associated to the probability distributions P_T and P_S respectively. Notice that the pair (T, S) is a random variable. Furthermore, the evaluation of $(t, s) \mapsto B^{\delta}_{t,s}$ at (T, S) determines a random variable, denoted $B^{\delta}_{T,S}$ and associated to the probability distribution

$$\Pr\left[B^{\delta}_{T,S} \in X\right] := \Pr\left[(T, S) \in \left\{(t, s) \in \mathcal{T} \times \mathcal{S} : \quad B^{\delta}_{t,s} \in X\right\}\right]$$

where $X \subset 2^{\mathcal{A}^n}$.

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