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 and quantum sampling strategies

The quantum sampling strategy is defined in terms of the classical sampling strategy. The "quantum error bound" is bounded by the square root of the "classical error bound", thus reducing the quantum information-theoretical problem to a well-studied probabilistic problem.

Classical sampling strategy

Let n be a positive integer, $\mathcal{A}$ be a finite alphabet and $\mathcal{S}$ be a finite set of seeds. Assume that $|\mathcal{A}| \geq 2$ and $|\mathcal{S}| \geq 1$. 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 finite set

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

Remark. The number of degrees of freedom of a sampling strategy is finite and it is asymptotically equivalent to $|\mathcal{S}|^2 \left(2|\mathcal{A}| + 2\right)^n$ as $n \to \infty$.

Set of classical δ-close states

Let δ be a positive real number. We define the *set of classical δ-close states* as

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

where $\omega(q)$ is the Hamming density of q, i.e., the Hamming weight of q divided by the length of q.

Heuristic idea: for δ, t and s fixed, the larger the set $B_{t,s}^{\delta}$ is, the better the function f is for estimation (with respect to t and s).

Random set of classical δ-close states

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

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

where $\Gamma \subset 2^{\mathcal{A}^n}$. The call $B^{\delta}_{T,S}$ the *random set of classical δ-close states*.

Heuristic idea: for δ fixed, the larger the random set $B^{\delta}_{T,S}$ is, the better the strategy is for estimation.

Classical δ-error

The *classical δ-error* is defined as

$$\varepsilon_c^\delta := \max_{q \in \mathcal{A}^n} \Pr\left[B_{T,S}^\delta \in \left\{ X \in 2^{\mathcal{A}^n} : \quad q \notin X \right\} \right].$$

Heuristic idea: ε_c^δ measures the probability that the sampling strategy fails in the worst-case scenario[2].

[2] Notice that the expression inside the bracket is equivalent to $q \notin B_{T,S}^\delta$.

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