Presentation for the Quantum Seminar

José Manuel Rodríguez Caballero

University of Tartu

Spring 2020

Motto of this presentation

"As above, so below"

Hermes Trismegistus

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.*

I will not present the paper, but the main ideas of the paper (ideas that I consider as secondary or redundant will be omitted in this presentation).

[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.

Introduction

In 1984, Charles Bennett and Gilles Brassard introduced the first quantum cryptography protocol, known as BB84. Shor and Preskill, among other authors, proved that BB84 was secure. In the paper of my presentation, a new method for security proof of BB84 is presented. For reasons of time, BB84 will not be explained here. Instead, I will go directly to a claim in the new security proof of BB84 where the techniques of the papers are applied (next two slide). The rest of the security proof is just standard quantum cryptography and it will not be discussed here.

Preparation for the claim

Let $n \geq 2$ and $1 \leq k \leq \frac{n}{2}$ be two integers. Consider three finite dimensional Hilbert spaces $\mathcal{H}_A$ (Alice), $\mathcal{H}_B$ (Bob) and $\mathcal{H}_E$ (Eve). Assume that both $\mathcal{H}_A$ and $\mathcal{H}_B$ have dimension n. Let $|\varphi_{ABE}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ be the quantum state of the system consisting of Alice, Bob and Eve. Take a uniformly random $\Theta \in \{0,1\}^n$. For each $i \in [n]$, if $\Theta_i = 0$, then measure i-th qubit of Bob in the computational basis, else measure the i-th qubit of Alice in the Hadamard basis, and assign the bit obtained in this way to the variable Z_i. Now, choose a uniformly random $S \subseteq [n]$ of size k and compute $\beta := \omega(Z_S)$.

Main claim

The goal of this presentation is to understand the following claim and why it is true.

Let $\delta > 0$ be a real. The post-measurement state is at most $2\exp\left(-\frac{\delta^2 k}{6}\right)$-close to a superposition of states having relative Hamming weigh in a δ-neighborhood of β.

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 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

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

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 $(j_1, ..., j_n) \in \{0,1\}^n$ 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, $f(t,q,s) := \omega(q_s)$.

End of my presentation