QUANTUM COMMUNICATION NETWORKS WORKSHOP

PORTUGUESE QUANTUM COMMUNICATION INFRASTRUCTURE

Performance of Computationally Secure Oblivious Transfer in the Quantum Setting

Mariano Lemus, Peter Schiansky, Manuel Goulão, Mathieu Bozzio, David Elkouss, Nikola Paunković, Paulo Mateus, Philip Walther.
mariano.lemus@tecnico.ulisboa.pt

Motivation

Privacy is critical in the context of an information society, where data is collected from multiple devices (smartphones, home appliances, computers, street cameras, sensors, etc.) and subjected to intensive analysis through data mining. Technologies capable of protecting the privacy of citizens and companies, while simultaneously allowing for profit through data mining, are becoming increasingly relevant. Secure Multiparty Computation (MPC) is a general resource that allow parties to jointly compute an *arbitrary* function that depends on their private information while keeping it secret.

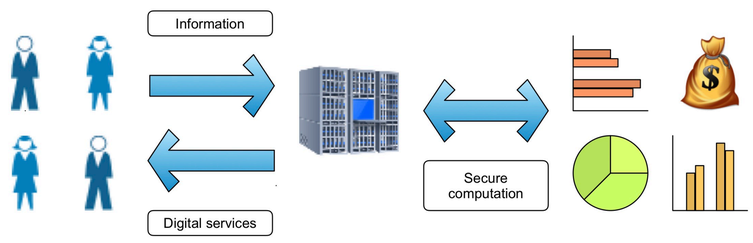

Figure 1: Private data mining, an example application of secure MPC

One of the best known ways of achieving MPC is through the oblivious circuit evaluation technique, which relies solely on symmetric cryptographic resources (hash functions, pseudorandom generators) and the cryptographic primitive known as Oblivious Transfer (OT).

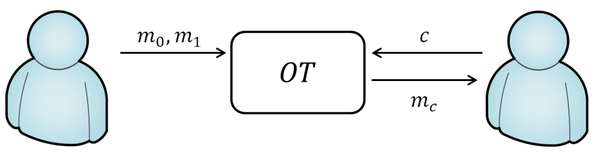

Figure 2: One-out-of-two oblivious transfer functionality

Let Alice and Bob be two agents. A 1-out-of-2 OT service receives strings m_0, m_1 as input from Alice and $b \in \{0,1\}$ as input from Bob, then outputs m_b to Bob. This is done in a way that Bob gets no information about the other message, i.e., $m_{\bar{b}}$, and Alice gets no information about Bob's choice, i.e., the value of b.

Main Problem: Current implementations of secure MPC require use of public key cryptography, which is considered to be a stronger requirement than symmetric cryptography, and for which the security against attacks from quantum computers is still not well understood.

A Quantum Protocol for Randomised OT

The proposed protocol π_{OKD} is based on the standard construction of quantum OT (originally by Yao,1995) from commitments. It uses one-way functions to instantiate a computationally secure commitment scheme, used in conjunction with a cut-and-choose technique to fix measurement bases and outcomes from Bob's measurements.

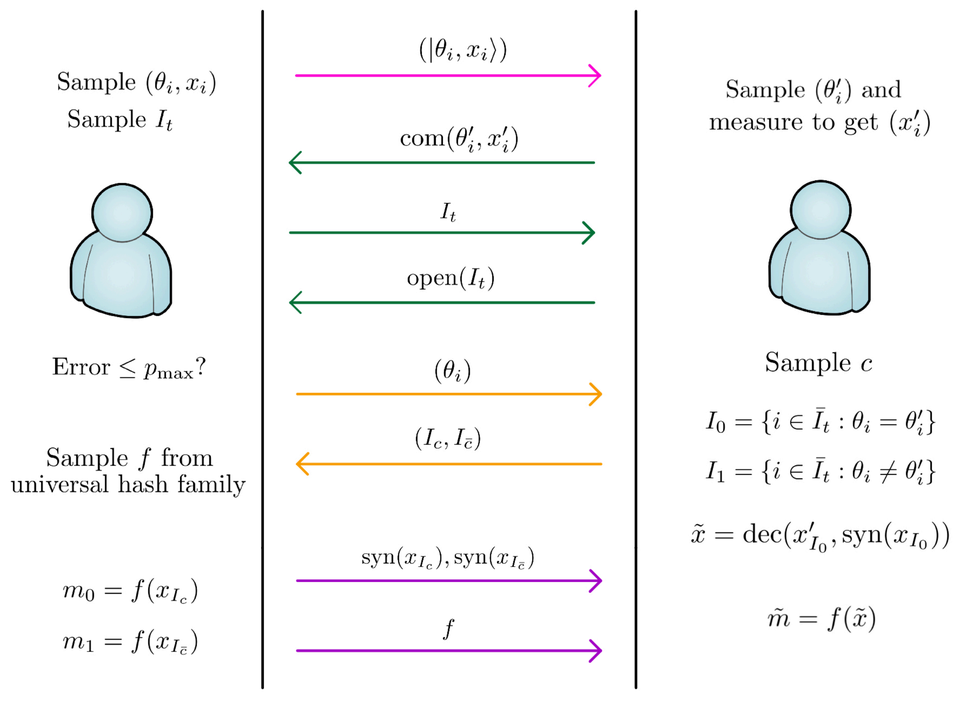

Figure 3: High level diagram of the π_{OKD} protocol

An experiment was implemented to test the performance of the π_{OKD} protocol with current technology. Data was acquired using a polarization entangled photon source at 1550nm, implemented through a Sagnac configuration setup using a picosecond pulsed pump laser.

In this setup, entangled photons were produced via spontaneous parametric down conversion (SPDC) by applying a laser pump beam into a 30mm long periodically-poled potassium titanyl phosphate (ppKTP) crystal. The photon pairs were split using a half-wave plate (HWP) and a polarizing beam splitter (PBS), and then sent to each party where they are detected using superconducting nanowire single-photon detectors.

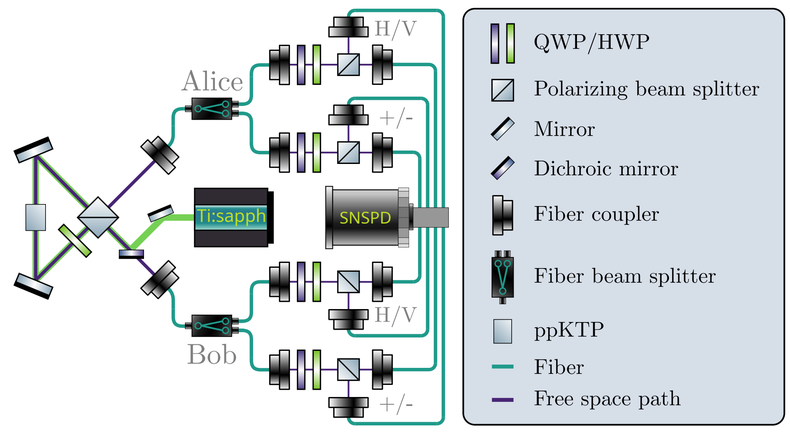

Figure 4: Experimental setup. Alice's and Bob's photons are individually fiber coupled and each sent to 50/50 fiber beam splitters, which probabilistically route them to free-space polarization projection stages to measure in the linear and diagonal basis each for Bob and Alice.

Security and Performance

The protocol was proven to be information theoretically secure against dishonest Bob (receiver) and computationally secure against dishonest Alice (sender), under the assumption of the existence of quantum-secure pseudorandom generators.

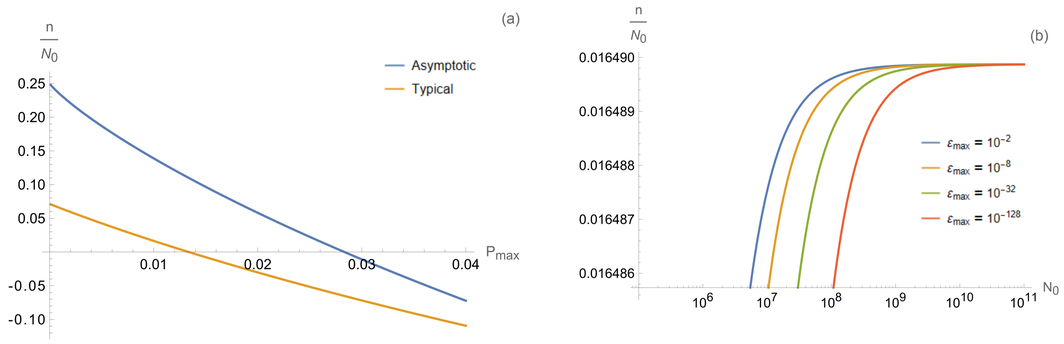

Figure 5: (a) Maximum key rate output versus qubit error rate P_{max}. (b) Maximum key rate behaviour as a function of the number of shared signals N_0 for different security levels.

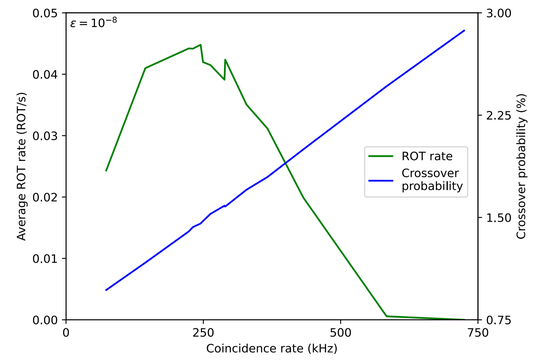

Figure 6: Experimental qubit error rates and maximum potential ROT rates for maximum cheating probability $\varepsilon = 10^{-8}$. We see that the best performance is obtained at a coincidence rate close to 2.45 kHz, corresponding to a laser pump power of 170 mW.

Conclusions

- We developed a quantum protocol for OKD, which can be implemented alongside QKD without the need of additional infrastructure
- Enhances the practical services quantum networks can provide: Symmetric keys → *Secure Communication*; Asymmetric keys → *Secure Computation*
- The protocol provides security advantages over classical counterparts by eliminating the need for public-key cryptography assumptions at the cost of speed, which can be mitigated using oblivious transfer extension protocols.

Aknowledgements

This work is supported by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020), under the project QuantumPrime reference: PTDC/EEI-TEL/8017/2020.

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101091730.

Co-funded by the European Union EuroQCI