Enhancing privacy with quantum networks

P. Mateus N. Paunković J. Rodrigues A. Souto

SQIG- Instituto de Telecomunicações and
DM - Instituto Superior Técnico - Universidade de Lisboa

Abstract

Using quantum networks to distribute symmetric keys has become a usable and commercial technology available under limitations that are acceptable in many application scenarios. The fact that the security is implemented directly at the hardware level, and moreover, relies on the laws of physics instead of conjectured hardness assumptions, justifies the use of quantum security in many cases. Limitations include 100 km communication range and installation of quantum channels between each pair of users of the network. Presently, with the current lack of trust in commercial security solutions, mostly due to the Snowden crisis, there is the need to improve such solutions. In this paper we discuss how quantum networks can be used to setup secure multiparty computation (SMC), allowing for instance for private data mining, electronic elections among other security functionalities. SMC relies mostly on establishing an efficient oblivious transfer protocol. We present a bit-string quantum oblivious transfer protocol based on single-qubit rotations that can be implemented with current technology based on optics and whose security relies only on the laws of physics.

1 Introduction

Security is the most important factor for building trust and confidence between consumers/population and companies/State; this trust has been severely damaged with many recent events such as the "Snowden crisis" and the Open SSL critical bug, and as such, private companies and state providers are pressured to improve the security of their products. In this paper we discuss how quantum security protocols can be integrated in a classical setting to provide multiparty-secure computation.

Two seminal works have driven most of the research in the area quantum security: the quantum polynomial time factorization algorithm proposed by Shor [7]; and the quantum public key agreement protocol BB84, proposed by Bennett and Brassard [1]. While Shor's algorithm raises the threat of making widely used cryptographic systems (via classic communication channels) completely obsolete by a breakthrough in quantum hardware, the BB84 protocol shows that quantum communication channels allow public perfect security in the context of an authenticated channel.

Due to Shor's factoring algorithm, research on (asymmetric) cryptography shifted significantly. Presently, one of the most important problems in the area is to find one-way functions robust to quantum attacks. Indeed, Shor's algorithm is able to attack all cryptosystems based on factorization and discrete logarithm, even in the elliptic curve setting, which accounts for essentially everything that is used in practice and is based on asymmetric keys.

On the other hand, BB84 is already commercially available through peer-to-peer optical networks. It is worth pointing out that quantum channels sending an arbitrarily amount of quantum information can already be produced using cheap technology. Moreover, much research is being done to develop quantum networks and routers using traditional optical fibers and laser satellite communications. It is expected that quantum networks will be available much sooner than quantum computers and thus, it is fundamental to understand which security and distributed protocols can benefit from quantum technology.

Secure multiparty computation is an abstraction of many security functionalities, including private data mining, e-voting, verifiable secret sharing, verifiable computing, among others. In general terms, the goal of secure multiparty computation among n parties is to compute a function of n secret inputs, one for each party, such that at the end of the computation the output of the function is known to all parties, while keeping the inputs secret.

It is well known that to setup secure multiparty computation it is enough to establish oblivious transfer (OT) protocol between two-parties using Yao's garbled circuits [8] (see a more modern discussion in [3]). The first OT protocol was presented by Rabin [6] and its security relies on the hardness assumption that factoring large integers is difficult in polynomial time. OT can be seen as a game played by two parties, Alice and Bob. Alice wants to share a number of secret messages with Bob such that, on average, Bob receives half of those messages (the protocol is *concealing*), while keeping Alice unaware to which messages Bob got (the protocol is *oblivious*). A protocol achieving these properties is called an OT Protocol. An OT protocol is made out of two parts: the transferring phase and the opening phase. In the former Alice sends the secret message to Bob; in the latter Alice unveil enough information that allows Bob to recover the secret with probability $1/2$.

The main contribution of this paper is to propose an OT protocol that can be implemented over quantum optical networks using currently available technology. Such OT protocol can then be used to establish a secure multiparty computation using classical infrastructure. We introduce a quantum oblivious transfer protocol for bit-strings, based on the recently proposed public key crypto-system in [5]. Each bit of the string to be transferred is encoded in a qubit (quantum bit), a particular quantum state, in such a way that states corresponding to bit-values 0 and 1, respectively, form an orthonormal basis. The key point of the protocol is that for each qubit, the encoding basis is chosen at random, from some discrete set of bases.

Next section provides a brief survey of quantum information, including basic definitions and important results necessary for understanding our proposal. Section 3 describes our proposal for a bit-string oblivious transfer protocol and discusses its correctness and security. Finally, we summarize the results and discuss future directions of research.

2 Preliminaries

In this section, we provide notation, necessary definitions and results for defining and reasoning about the security of our proposal.

For a complete study of quantum information we suggest the reading of [4]. Here we present some relevant notions. According to the postulates of quantum mechanics, the state of a closed quantum system is represented by a unit vector from a complex Hilbert space $\mathcal{H}$, and its evolution is described by a unitary transformation on $\mathcal{H}$. In this paper we work only with finite-dimensional Hilbert spaces reflecting the realistic examples of systems with finite number degrees of freedom (strings of quantum bits, i.e. qubits).

Contrarily to the classical case where a bit can only have values 0 or 1, in the quantum case, a *qubit* can be in a unit superposition of 0 or 1 denoted by $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$ with complex coefficients α and β such that $|\alpha|^2 + |\beta|^2 = 1$. The Dirac notation $\left|0\right\rangle$ and $\left|1\right\rangle$ denotes vectors forming an orthonormal basis of a 2-dimensional complex vector space. Note that we can define many orthonormal bases for that space, such as $\left\{\frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle), \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)\right\}$, but it is common to distinguish the basis $\{\left|0\right\rangle, \left|1\right\rangle\}$ from all the others, and call it the *computational basis.*

The state of two qubits is from the tensor product of single-qubit spaces, that is,

$$\left|\psi\right\rangle = \alpha\left|00\right\rangle + \beta\left|01\right\rangle + \gamma\left|10\right\rangle + \delta\left|11\right\rangle$$

with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. The state $\left|\psi\right\rangle$ is said to be *separable* if

$$\left|\psi\right\rangle = (\alpha\left|0\right\rangle + \beta\left|1\right\rangle) \otimes (\alpha'\left|0\right\rangle + \beta'\left|1\right\rangle) = \alpha\alpha'\left|00\right\rangle + \alpha\beta'\left|01\right\rangle + \alpha'\beta\left|10\right\rangle + \beta\beta'\left|11\right\rangle.$$

Otherwise, it is called *entangled.* Although entangled states are particularly important in quantum information, in this paper we only work with separable states. Note that a system with k qubits can be described by a unit vector over a space with dimension 2^k.

One of the most important results of quantum information states that the maximal information that can be stored in a qubit is the same as that contained in a bit. This means that we cannot extract more than a bit of information from a qubit, although there is potentially an infinite number of states available to encode in a qubit. The reason for this is that it is impossible to obtain coefficients α and β from a single qubit in a state $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$. Indeed, what is possible is to perform a measurement given by an orthogonal decomposition of the Hilbert space $\mathcal{H} = \bigoplus_{i=1}^{d} \mathcal{H}_i$, with P_i being the projectors onto $\mathcal{H}_i$. Then, upon performing such a measurement on a qubit in state $\left|\psi\right\rangle \in \mathcal{H}$, there are d possible outcomes $\{1, \ldots, d\}$, where the probability of observing $i \in \{1, \ldots, d\}$ is given by $\|P_i \left|\psi\right\rangle \|$, and then the state evolves to $P_i \left|\psi\right\rangle / \|P_i \left|\psi\right\rangle \|$. For instance, the outcome of a measurement of a qubit can only take two possible values.

To understand the protocol we need to consider a function that is easy to compute, but, without the help of a secret trapdoor, it is impossible to invert with non-negligible probability according to the laws of quantum physics. One candidate for such a function was proposed in [5] which uses sinlge-qubit rotations and is given by

$$f(s) = R(s\theta_n)\left|0\right\rangle = \cos\left(s\theta_n/2\right)\left|0\right\rangle + \sin\left(s\theta_n/2\right)\left|1\right\rangle$$

where, for some fixed n, $s \in \{0, \dots, 2^n - 1\}$, $\theta_n = \pi/2^{n-1}$ and $\{\left|0\right\rangle, \left|1\right\rangle\}$ is a fixed computational basis (i.e., f is not a function of a quantum state). Moreover, f can be used to construct a quantum trapdoor function $F(s, b)$, where s is the trapdoor information for learning an unknown bit b [5]:

$$F(s, b) = R(b\pi)f(s) = R(b\pi)R(s\theta_n)\left|0\right\rangle = R(s\theta_n + b\pi)\left|0\right\rangle .$$

Note that inverting F (learning both s and b) is at least as hard as inverting f. In [5] it was shown that every binary measurement that could be used to infer unknown bit b would outcome a completely random value. Nevertheless, if s is known, by applying the rotation $R(-s\theta_n)$ to $F(s, b)$ and measuring the result in the computational basis, one obtains b with certainty.

Using the properties of f and F a secure public key cryptographic protocol was proposed in [5]: using the private key s, the public key is generated by computing $f(s)$; the encryption of a secret message corresponds to computing $F(s, b)$; and the decryption of the message corresponds to inversion of $F(s, b)$, using the trapdoor information s.

Finally, in order to guarantee that at the end of the OT protocol Bob knows if he got the message m or not, Alice is required to send both m and $h(m)$, where h is a *universal hash function.* A hash function maps strings to other strings of smaller size . Bellow, we present a definition of universal hash function and a basic result.

Definition 2.1 *Consider two sets A and B of size a and b, respectively, such that $a > b$, and consider a collection $\mathbb{H}$ of hash functions $h : A \to B$. If*

$$\Pr_{h \in \mathbb{H}}[h(x) = h(y)] \leq \frac{1}{b}$$

then $\mathcal{H}$ is called a universal family of hash functions.

Theorem 2.1 *Let $\mathbb{H}$ be a collection of hash functions $h : A \to B$, where A and B are sets of size a and b, respectively, such that $a > b$. The size of a set A_x of strings $x \in A$ mapped to the same hash value $h(x)$ is at most N/b.*

In our particular case we consider A and B as the sets of strings of length ℓ and $\ell/2$ respectively. Hence, there are $2^{\ell/2}$ different strings for each hash value (for an overview see [2]).

3 Oblivious Transfer

Having set the required definitions and results, our protocol works as follows:

Protocol 1 (Oblivious transfer)

Message to transfer *$m = m_1 \dots m_k$;*

Security parameter *$n, \theta_n = \pi/2^{n-1}$ and a hash function $h : \{0,1\}^k \to \{0,1\}^{k/2}$;*

Secret key *$s = (s_1, \dots, s_{3k/2})$, where each $s_i \in \{0, \dots, 2^n - 1\}$.*

Transfer phase:

1. *Alice chooses uniformly at random a bit $a \in \{0,1\}$ and prepares the following state:*

$$|\psi\rangle = \bigotimes_{i=1}^{k} R(m_i\pi + (-1)^a \times s_i\theta_n)\,|0\rangle \bigotimes_{i=1}^{k/2} R(h_i(m)\pi + (-1)^a \times s_{i+k}\theta_n)\,|0\rangle$$

   (Note that $h_i(m)$ represents the i^{th} bit of the binary string $h(m)$).

2. *Alice sends the state $|\psi\rangle$ to Bob.*

Opening phase:

3. *Alice sends $s = (s_1, \dots, s_{3k/2})$ and n to Bob.*
4. *Bob checks if s is likely to be a possible output of a random process by performing a statistical test.*
5. *Bob chooses uniformly at random $a' \in \{0,1\}$ and applies $R((-1)^{a'}s_i\theta_n)$ to each qubit of $|\psi\rangle$.*
6. *Bob applies the measurement operator $M = (0\times|0\rangle\langle 0|+1\times|1\rangle\langle 1|)^{\otimes 3k/2}$.*
7. *Let $m' \cdot h'$ be the message that Bob recovers. He checks if $h' = h(m')$. If that is the case then Bob is almost sure that $m' = m$, otherwise he knows that m' is not the correct message.*

In the following, we discuss the security of our oblivious transfer protocol, showing that: if both agents are honest, Bob will obtain the message m with probability 1/2 (the protocol is sound); if Alice plays fair, Bob is not able to recover m before the opening phase (the protocol is concealing); if Bob is honest, then Alice is unaware if Bob got m or not (the protocol is oblivious).

To state the results we need the notion of negligible function. $\varepsilon : \mathbb{N} \to \mathbb{R}$, a nonnegative function is called *negligible* if for every polynomial p and sufficiently large k we have $\varepsilon(k) \leq 1/p(k)$.

First, we provide the reasoning for the soundness of our protocol.

Theorem 3.1 *If both parties are honest, then with probability $1/2 + \varepsilon(k)$ Bob will get the right message, where $\varepsilon(k)$ is negligible function on the size of the message $m = m_1 \dots m_k$.*

Notice that if Alice and Bob are honest then the choice of rotation direction of both will differ with probability 1/2. Only when they are different, i.e., Bob undo Alice's rotation and obtains the states in computational bases, Bob is ensured to recover the message. When Bob rotates in the same direction of Alice, the results of Bob's measurement are random and hence the probability of recovering m in this case is a negligible function on the size of the message m.

We proceed by discussing the concealing property of the protocol.

Theorem 3.2 *If Alice is honest, the probability of Bob recovering Alice's message before the opening phase is negligible. Furthermore, after the opening phase Bob recovers the message, up to a negligible value, with probability $1/2$.*

The first part of the theorem follows directly from the security of the public key encryption schemes presented in in [5]: without knowing the secret key s and the rotation direction a, Bob's description of a message m is given by a completely mixed state. The second part follows from a similar argument to the previous theorem.

To finish the security discussion we argue that the protocol is unconditionally oblivious for practical attacks.

Theorem 3.3 *The Protocol 1 is oblivious, i.e., at the end of the protocol Alice does not know whether Bob received the right message of not.*

During the execution of the protocol, there is no information traveling from Bob to Alice. Therefore, in order to increase the probability of learning if Bob received the message m or not, Alice has to perform the following cheating strategy: instead of sending $|\psi\rangle$, Alice sends a cheating state $|\psi_{ch}\rangle$ for which Bob will open the desired message with a probability greater than 1/2 (possibly with certainty). This is impossible, unless with negligible increase $\varepsilon(l)$, bounded above by $\frac{1}{2}\left(1 + \cos^{2l}(\pi/8)\right)$, where l is the number of s_i's for which $s_i\theta_n \in [\pi/8; 3\pi/8]$.[1]

4 Conclusions

In this paper we proposed a scheme for oblivious transfer of a bit-string message. Its security is based on laws of quantum physics. We reasoned about its security and showed that the protocol is unconditionally oblivious and concealing for practical attacks. Our protocol can be implemented with today's technology using optical equipment. Moreover, the protocol can be integrated with existing

[1] Since the values of s_i's are required to be random, the expected value of l is $k/4$, with the standard deviation $\sigma = \sqrt{k}/4$.

classical networks to achieve secure multiparty computation, and promote an extra level of security on such functionality.

Using single-qubit rotations have been proved useful in designing quantum security protocols, such as the presented oblivious transfer and the previously proposed public key cryptographic scheme [5]. This opens a number of possible future applications of single-qubit rotations in designing several secure protocols such as quantum bit-string commitment protocol and undeniable signatures.

Acknowledgments

This work was partially supported by FCT projects ComFormCrypt PTDC/EIA-CCO/113033/2009 and PEst-OE/EEI/LA0008/2013, and SQIG's initiative PQDR (Probabilistic, Quantum and Differential Reasoning). João Rodrigues and André Souto also acknowledges respectively the FCT grants SFRH / BD / 75085 / 2010 and SFRH / BPD / 76231 / 2011.

References

[1] C. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984. IEEE Press.

[2] J. Carter and M. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[3] Y. Lindell and H. Zarosim. On the feasibility of extending oblivious transfer. In *TCC*, pages 519–538, 2013.

[4] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 1 edition, January 2004.

[5] G. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A*, 77:032348, Mar 2008.

[6] M. Rabin. How to exchange secrets by oblivious transfer, 1981.

[7] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[8] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, SFCS '86, pages 162–167, Washington, DC, USA, 1986. IEEE Computer Society.