Quantum walks public key cryptographic system

(Extended Abstract)

C. Vlachou[3] J. Rodrigues[1,2] P. Mateus[1,2] N. Paunković[1,2] A. Souto[1,2]

[1] SQIG - Instituto de Telecomunicações
[2] Departamento de Matemática - IST - UL
[3] Departamento de Física - IST - UL

October 5, 2015

Abstract

We present a quantum public-key crypto-system based on quantum walks. We show its security and analyze the complexity of public-key generation and encryption/decryption procedures.

1 Introduction

Since the invention of writing, the need for secret/secure communication resulted in the development of cryptography – the art of "hidden communication". It started by using simple symbols as code words and evolved to the stage where the security is based on various mathematical hardness assumptions: widely used RSA-based crypto-system [RSA78] relies on the conjecture that factoring large number is not feasible using standard computers. With the advent of quantum computation, and in particular the celebrated Shor's algorithm for factoring [Sho97], the security of most crypto-systems currently in use has became jeopardized. Since then, the interest in quantum cryptography, introduced by Wiesner in the seventies (and published only a decade later [Wie83]), and developed by Bennet and Brassard by the famous quantum key distribution BB84 protocol [BB84]. Subsequently, Mayers showed the unconditional security of BB84 protocol [May01], i.e., the security that is based on the laws of (quantum) physics. Rapid development of experimental techniques resulted in the implementation of quantum key distribution [SMWF$^+$07] and nowadays one can even buy devices implementing it on the online market from Clavis QKD Platform `http://www.idquantique.com/photon-counting/clavis-qkd-platform/`.

Another approach to secure communication is based on the exchange of public keys, such as the mentioned RSA scheme. Recently, Nikolopoulos presented a secure quantum public-key crypto-system based on single qubit rotations [Nik08]. In this paper we propose a quantum crypto-system in which public keys are generated by running a quantum walk, rather than by performing single-qubit rotations.

The paper is organized as follows: in the next section we start with basic definitions and notations used through out the paper. In Section 3 we present our public-key crypto-system and discuss its security and efficiency. In Section 4 we summarize the results obtained and point some future research direction.

2 Preliminaries

2.1 1D Quantum walk

2.1.1 Basic dynamics

In a discrete-time quantum walk on a line, we consider a movement of a walker along discrete positions on it, labeled by $i \in \mathbb{Z}$. At each step the particle moves to the left or to the right, depending on the state of the internal degree of freedom, commonly called the coin. Both position and coin states of the particle are from the Hilbert spaces $\mathcal{H}_p = span\{|i\rangle : i \in \mathbb{Z}\}$ and $\mathcal{H}_c = span\{|R\rangle, |L\rangle\}$, respectively.

The evolution of the system at each step of the walk is described by the unitary operator:

$$\hat{U} = \hat{S}\left(\hat{I}_p \otimes \hat{U}_c\right).$$

In the above expression $\hat{I}_p$ is the identity operator on $\mathcal{H}_p$, $\hat{S}$ is the shift operator

$$\hat{S} = \sum_{i\in\mathbb{Z}} \left(|i+1\rangle\langle i| \otimes |R\rangle\langle R| + |i-1\rangle\langle i| \otimes |L\rangle\langle L|\right)$$

and $\hat{U}_C \in U(2)$ is the coin operator acting on $\mathcal{H}_c$. The general expression for $\hat{U}_C$ is:

$$\hat{U}_C = e^{i\phi}\begin{bmatrix} e^{i\xi}\cos\theta & e^{i\zeta}\sin\theta \\ -e^{-i\zeta}\sin\theta & e^{-i\xi}\cos\theta \end{bmatrix}.$$

2.1.2 Shift operator on the circle

To simulate the walk on a circle, one could either identify positions $-N$ and N, or connect the two, thus altering the corresponding shift operator. In the former, the circle has even number of positions ($2N$), while in the latter it has an odd number of positions ($2N+1$).

With the position Hilbert space $\mathcal{H}_p = span\{|i\rangle : i \in \{0, \ldots, N-1\}\}$, the general expression for a shift operator on a circle with N positions is:

$$\begin{aligned}
\hat{S} &= \sum_{i=0}^{N-1} \Big(|i+1\,(\mathrm{mod}\ N)\rangle \langle i| \otimes |R\rangle \langle R| + |i-1\,(\mathrm{mod}\ N)\rangle \langle i| \otimes |L\rangle \langle L| \Big) \\
&= \hat{T}_1 \otimes |R\rangle \langle R| + \hat{T}_{-1} \otimes |L\rangle \langle L|
\end{aligned}$$

where

$$\hat{T}_m = \sum_{i=0}^{N-1} |i+m\,(\mathrm{mod}\ N)\rangle \langle i|$$

is the $m-$position translation operator.

3 Public-key encryption based on discrete-time quantum walks

We now present the public key cryptographic system using quantum walks on a circle.

Protocol 1 (Public-key encryption scheme)**.**

Inputs for the protocol

- *Message to transfer:*
  $m \in \{0, \ldots, 2^n - 1\}$*, i.e., a message of at most* n *bits;*
- *Secret key* $K = (\hat{U}_i, t, l)$ *where:*
  $\hat{U}_i$ *with* $i \in \mathcal{I} = \{1, 2, \ldots, d\}$*,* $t \in \mathcal{T} = \{t_0, \ldots, t_{max}\} \subset \mathbb{N}$ *and* $l \in \{0, \ldots, 2^n - 1\}$
  (below, for simplicity, we often write just $\hat{U}$*, without explicitly notifying the subscript)*

Public-key generation

- *Alice chooses uniformly at random* $l \in \{0, \dots, 2^n - 1\}$ *and* $s \in \{L, R\}$*, and generates the initial state* $|l\rangle\,|s\rangle$*;*
- *Then she chooses, also at random, the walk* $\hat{U} = \hat{S}(\hat{I}_p \otimes \hat{C})$ *and the number of steps* $t \in \mathcal{T}$*.*
- *Finally, she generates the public key:*

$$|\psi_i\rangle = \hat{U}^t\,|l\rangle\,|s\rangle = \left[\hat{S}(\hat{I}_p \otimes \hat{C})\right]^t |l\rangle\,|s\rangle$$

Message Encryption

- *Bob obtains Alice's public key* $|\psi_i\rangle$
- *He encrypts* m *by applying spatial translation to obtain:*

$$|\psi(m)\rangle = (\hat{T}_m \otimes \hat{I}_c)\,|\psi_i\rangle$$

- *Bob sends* $|\psi(m)\rangle$ *to Alice.*

Message Decryption

- *Alice applies* $\hat{U}^{-t}$ *to the state* $|\psi(m)\rangle$*.*
- *She performs the measurement*

$$\hat{M} = \sum_i |i\rangle\,\langle i| \otimes \hat{I}_c$$

and obtains the result i_0*.*
The message sent by Bob is $m = i_0 - l\,(\mathrm{mod}\ N)$*.*

3.1 Correctness of the protocol

Theorem 1. *The above protocol is correct, in the sense that if Alice and Bob follow it, and no third party intervenes during its execution, at the end of the decryption phase Alice recovers the message sent by Bob with probability* 1*.*

Proof. The correctness of the protocol when Alice and Bob follow the prescribed steps follows directly from the fact that the quantum walk $\hat{U}^k$ commutes with any translation $\hat{T}_m$. Thus, the state of the system before the final step of the decryption phase (measurement), is:

$$\begin{aligned}
|\psi_f\rangle &= \hat{U}^{-t}\,|\psi(m)\rangle \\
&= \hat{U}^{-t}(\hat{T}_m \otimes \hat{I}_c)\,|\psi_i\rangle \\
&= \hat{U}^{-t}(\hat{T}_m \otimes \hat{I}_c)\hat{U}^{t}\,|l\rangle\,|s\rangle \\
&= (\hat{T}_m \otimes \hat{I}_c)\hat{U}^{-t}\hat{U}^{t}\,|l\rangle\,|s\rangle \\
&= (\hat{T}_m \otimes \hat{I}_c)\,|l\rangle\,|s\rangle \\
&= |l + m\,(\mathrm{mod}\ N)\rangle\,|s\rangle\,. \qquad (1)
\end{aligned}$$

Upon measuring $\hat{M}$ and obtaining $l+m\,(\mathrm{mod}\ N)$, the decrypted message is indeed m. □

Below, we prove in detail that $\hat{U}^t$ and $(\hat{T}_m \otimes \hat{I}_c)$ commute.

Lemma 1. *Let $N \geq 2^n$ where n is a fixed integer. Let $\hat{U}^t$ be a random walk from Protocol 1 and let $\hat{T}_m$ denote the translation operator for m positions modulo N. Then $\hat{U}^t$ and $(\hat{T}_m \otimes \hat{I}_c)$ commute.*

Proof. Notice that the action of any U used in Protocol 1 can be written as:

$$\hat{U}\,|l\rangle\,|s\rangle = \alpha_{L(s)}\,|l-1\rangle\,|L\rangle + \alpha_{R(s)}\,|l+1\rangle\,|R\rangle$$

where $|L\rangle$ and $|R\rangle$ are the orthogonal coin states and $\alpha_{L/R(s)}$ is the probability amplitude to find the walker in position $l-1$ or $l+1$, depending on its spin. Notice also that $\hat{T}_m$ is defined as:

$$\hat{T}_m\,|l\rangle = |l+m\,(\mathrm{mod}\ N)\rangle$$

Then, for any element of the form $|l\rangle\,|s\rangle$ we have:

$$\begin{aligned}
(\hat{T}_m \otimes \hat{I}_c)\hat{U}\,|l\rangle\,|s\rangle &= (\hat{T}_m \otimes \hat{I}_c)\left[\alpha_{L(s)}\,|l-1\rangle\,|L\rangle + \alpha_{R(s)}\,|l+1\rangle\,|R\rangle\right] \\
&= \alpha_{L(s)}\,|l-1+m\,(\mathrm{mod}\ N)\rangle\,|L\rangle + \alpha_{R(s)}\,|l+1+m\,(\mathrm{mod}\ N)\rangle\,|R\rangle
\end{aligned}$$

On the other hand, we also have:

$$\begin{aligned}\hat{U}(\hat{T}_m \otimes \hat{I}_c)\left|l\right\rangle\left|s\right\rangle &= \hat{U}\left|l+m\,(\mathrm{mod}\ N)\right\rangle\left|s\right\rangle\\ &= \alpha_{L(s)}\left|l-1+m\,(\mathrm{mod}\ N)\right\rangle\left|L\right\rangle+\alpha_{R(s)}\left|l+1+m\,(\mathrm{mod}\ N)\right\rangle\left|R\right\rangle.\end{aligned}$$

□

Observe that this lemma can be extended to more general shift operations, which allow jumps for two or more positions, or leave position state unchanged, depending on the coin state.

3.2 Security of the protocol

The protocol consists of two phases. In the first, Alice sends a public key $|\psi_i\rangle$ to Bob. In the second, upon encrypting the message m, Bob sends back the state $|\psi(m)\rangle$ to Alice. Therefore, one has to show the security of the secret key during the first phase and the security of the message during the second phase.

Our proof of the security is based on Holevo's Theorem, that bounds the amount of classical information that an eavesdropper can retrieve from a given quantum mixed state by means of a POVM measurement.

Let us denote by $\hat{\rho}_K$ the mixed state of the key, as perceived by Eve, who does not know *a priori* the secret key K chosen by Alice. Even if Eve were to know $\hat{U}$ and t, $\hat{\rho}_K$ is completely mixed:

$$\begin{aligned}\hat{\rho}_K &= \hat{U}^t\left[\frac{1}{2^{n+1}}\sum_{l=0}^{2^n-1}\sum_{s\in\{L,R\}}\left|l\right\rangle\left\langle l\right|\otimes\left|s\right\rangle\left\langle s\right|\right](\hat{U}^t)^\dagger\\ &= \hat{U}^t\left(\frac{1}{2^{n+1}}\hat{I}_p\otimes\hat{I}_c\right)(\hat{U}^t)^\dagger\\ &= \frac{1}{2^{n+1}}(\hat{I}_p\otimes\hat{I}_c)\hat{U}^t(\hat{U}^t)^\dagger\\ &= \frac{1}{2^{n+1}}\hat{I}_p\otimes\hat{I}_c. \qquad (2)\end{aligned}$$

Assuming that Eve performs a measurement on $\hat{\rho}_K$, Holevo's Theorem implies that the mutual information $I(K, E)$ between the key K and her inference E is bounded from above by the Von Neumann entropy of this state:

$$I(K, E) \leq S(\hat{\rho}_K) = -\operatorname{Tr}(\hat{\rho}_K \log \hat{\rho}_K) = n + 1.$$

To conclude that the protocol is secure we have to show that the mutual information is very small compared to the Shannon entropy of the secret key. Indeed, the Shannon entropy of the secret key depends on the probability to choose $\hat{U}$, t and the initial state $|l\rangle\,|s\rangle$. In the following we denote by p_i the probability to choose $\hat{U}_i$ from the set $\{\hat{U}_i | i \in \mathcal{I} = \{1, 2, \ldots, d\}\}$, by p_t the probability to run the walk for t steps, with $t \in \mathcal{T}$, and by $p_{l,s}$ the probability to choose $|l\rangle\,|s\rangle$ as the initial state, where $l \in \{0, 1, \ldots, 2^n - 1\}$ and $s \in \{L, R\}$. Since this choices are random and independent, the probability of a certain secret key K is given by:

$$p_K = p_i\; p_t\; p_{l,s} = \frac{1}{d\; |\mathcal{T}|\; 2^{n+1}},$$

where $|\mathcal{T}|$ is the cardinality of $\mathcal{T}$.

The above probability distributions are uniform, so the Shannon entropy of the secret key is:

$$\begin{aligned} H(p_K) &= -\sum_{i \in I} \sum_{t \in \mathcal{T}} \sum_{l=0}^{2^{n+1}} p_i\; p_t\; p_{l,s} \log_2(p_i\; p_t\; p_{l,s}) \\ &= \log_2(d\; |\mathcal{T}|\; 2^{n+1}) \\ &= \log_2(d\; |\mathcal{T}|) + n + 1. \end{aligned}$$

Thus, we have:

$$I(K, E) \leq S(\hat{\rho}_K) << H(p_K),$$

since $\log_2(d\; |\mathcal{T}|) >> 1$ with an appropriate choice of $|\mathcal{T}|$ and d, e.g., $|\mathcal{T}|, d \approx poly(n)$, for sufficiently large n.

For the rest of this section we discuss the security of the message m during the second phase of the protocol. We show that the security of the encrypted message can be reduced to the security of the secret key. In this case, Eve intercepts the state of the encrypted message that Bob sends to Alice, which she perceives as the mixed state $\hat{\rho}_B$:

$$\begin{aligned}\hat{\rho}_B &= (\hat{T}_m \otimes \hat{I}_c)\left(\frac{1}{2^{n+1}}\hat{I}_p \otimes \hat{I}_c\right)(\hat{T}_m \otimes \hat{I}_c)^\dagger \\ &= \frac{1}{2^{n+1}}(\hat{T}_m \otimes \hat{I}_c)(\hat{T}_m \otimes \hat{I}_c)^\dagger(\hat{I}_p \otimes \hat{I}_c) \\ &= \frac{1}{2^{n+1}}\hat{I}_p \otimes \hat{I}_c. \qquad (3)\end{aligned}$$

This is exactly the same statistical mixture we had before, thus its Von Neumann entropy is:

$$S(\hat{\rho}_B) = n + 1.$$

Consequently, the information that Eve can access by means of a POVM measurement is bounded by the same quantity:

$$I(m, E) \leq S(\hat{\rho}_B) = n + 1.$$

Moreover, in order to encrypt his message, Bob performs a shift on the state of the public key. This operation does not affect the Shannon entropy, hence the security of the encrypted message can be reduced to the security of the secret key, yielding that it is also secure.

3.3 Efficiency of the protocol

In this last section we focus on the efficiency of the proposed protocol. The public key generation is an efficient procedure, since the quantum walk can be efficiently performed. Indeed, denoting by $\Delta\tau_w$ the time required for each step of the walk, the full walk $\hat{U}^t$ is completed in time $\tau = t \cdot \Delta\tau_w$. In the previous section we proposed $t \approx poly(n)$ for security purposes, a choice which is also adequate for the efficiency of the public key generation.

On the other hand, the encryption of the message requires $\boldsymbol{O}(2^n)$ single-position translations. This is exponentially large in the size (number of bits) of the message. We argue that this is not necessarily a non-efficient procedure. We start by writing the translation operator used for the message encryption $\hat{T}_m$ as:

$$\hat{T}_m = (\hat{T}_1)^m.$$

Now, let us denote by $\Delta\tau_s$ the time required to complete the operation $\hat{T}_1$. Hence, the message encryption takes time $\tau' = m \cdot \Delta\tau_s$. Observing that $\hat{T}_1$ is a trivial operation compared to the quantum walk U, we obtain:

$$\Delta\tau_s << \Delta\tau_w.$$

The above inequality ensures the efficiency of the protocol.

In addition to this, in case the physical realization has a rotational symmetry, instead of performing position translations, Bob can just rotate the entire system by an angle $\phi = m \cdot \frac{2\pi}{2^n}$, using the operator:

$$\hat{R}_m = R\left(m \cdot \frac{2\pi}{2^n}\right) = \left[R\left(\frac{2\pi}{2^n}\right)\right]^m$$

This is clearly an efficient procedure and we claim that it is also equivalent to the previous one.

Indeed, it is quite straightforward to conclude that they both yield the same result. When we rotate the circle by an angle $\phi = m \cdot \frac{2\pi}{2^n}$, we move each $|i\rangle$ to $|i+m\rangle$ at the same time. Thus, after this operation, the probability distribution is exactly the same as after the $\boldsymbol{O}(2^n)$ position translations we had before.

Moreover, the protocol is still correct and secure, as it can be easily shown.

4 Conclusions

In this paper we presented a quantum public-key crypto-system based on quantum walks. Unlike the recently proposed protocol [Nik08] that uses single-qubit rotations to generate the public key, in our scheme the execution of a quantum walk in general results in entangled quantum states as public keys, thus increasing the practical security of our scheme (an eavesdropper has to, in general, perform more complex operations to extract information from entangled than from product states). Using Holevo's theorem, we proved the protocol's security. We also analyzed the complexity of our public-key generation and message encryption/decryption and showed their efficiency, i.e., that the complexity of our protocol scales polynomially with the size of the message.

Future research include designing other security protocols based on the use of quantum walks, such as oblivious transfer (along the lines of the recently proposed protocols [MPRS14, SMAP15]), commitment schemes and other privacy functionalities.

Acknowledgements

This work was partially supported, under the CV-Quantum internal project at IT, by FCT PEst-OE/EEI/LA0008/2013 and UID/EEA/50008/2013 and EU FEDER, namely via the FCT projects ComFormCrypt PTDC/EIA-CCO/113033/2009, and CaPri initiative. A. Souto also acknowledges the FCT postdoc grant SFRH/BPD/76231/2011. C. Vlachou also acknowledges the FCT grant PD/BD/52652/2014.

References

[BB84] 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.

[May01] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, May 2001.

[MPRS14] P. Mateus, N. Paunkovic, J. Rodrigues, and A. Souto. Enhancing privacy with quantum networks. In *Proceedings of CMS 2014*, volume 8735 of *Lecture Notes in Computer Science*, pages 147–153. Springer, 2014.

[Nik08] G. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A*, 77:032348, Mar 2008.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[Sho97] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[SMAP15] A. Souto, P. Mateus, P. Adao, and N. Paunković. Bit-string oblivious transfer based on quantum state computational distinguishability. *Phys. Rev. A*, 91:042306, Apr 2015.

[SMWF$^+$07] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. Rarity, A.n Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, Jan 2007.

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.