Quantum walks public key cryptographic system

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

SQIG - Instituto de Telecomunicações
Departamento de Matemática - IST - UL

Abstract

Quantum Cryptography is a rapidly developing field of research that benefits from the properties of Quantum Mechanics in performing cryptographic tasks. Quantum walks are a powerful model for quantum computation and very promising for quantum information processing. In this paper, we present a quantum public-key cryptographic system based on quantum walks. In particular, in the proposed protocol the public key is given by a quantum state generated by performing a quantum walk. We show that the protocol is secure and analyze the complexity of public-key generation and encryption/decryption procedures.

Keywords: Quantum walks; Public-key cryptographic systems; Holevo bound

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: a widely used RSA-based cryptographic system[1] relies on the conjecture that factoring large numbers is not feasible using standard computers, while the alternative lattice-based public-key cryptographic system[2] is based on the assumed difficulty of the so-called "shortest and closest vector problems" (also related to the well known $P \neq NP$ conjecture[3]). With the advent of quantum computation, and in particular after the discovery of the celebrated Shor's algorithm for factoring,[4] the security of most cryptographic systems currently in use became jeopardized and as a consequence the need for new cryptographic systems resilient to quantum adversaries arose. The above mentioned lattice-based cryptographic system is resilient to particular quantum adversaries that execute Shor's algorithm, as its security is not based on the factoring problem; nevertheless, it does rely on another mathematical assumption, thus leaving open the question of whether it is more than just computationally secure. A completely different approach is the one that takes advantage of quantum mechanics and assumes that both sender and receiver have access to a quantum computer. The major advantage of this approach is that the security, rather than relying on mathematical/computational hardness assumptions, is now based on the laws of quantum mechanics.

Quantum cryptography has been among hot subjects of research in the last decades. It was firstly considered by Wiesner in the late sixties and early seventies, who introduced the notions of quantum multiplexing and money (which was only published a decade later, see Reference [5]), and further developed by Bennet and Brassard [6] in their famous Quantum Key Distribution (QKD) BB84 protocol. Subsequently, Mayers showed the unconditional security of BB84 protocol i.e., the security that is based on the

laws of (quantum) physics (see Reference [7]). Rapid development of experimental techniques resulted in the implementation of QKD, see for example Reference [8], and nowadays one can even buy devices implementing it on the online market from Clavis QKD Platform.[9]

As an alternative to QKD, another way for two parties to communicate privately has been developed, using quantum public-key cryptosystems: in Reference [10] the authors propose a scheme based on quantum trapdoor one-way functions, and in Reference [11] a system is presented whose security is based on (quantum) computational indistinguishability of quantum states. More recently, Nikolopoulos[12] presented a secure public-key cryptographic system based on single-qubit rotations.

In this paper we propose a new quantum public-key cryptographic system in which the public keys are quantum states generated by running a quantum walk, rather than by performing single-qubit rotations, while the private key consists of: (i) the quantum walk, (ii) the number of steps of the walk and (iii) the initial state. Regarding the use of quantum walks in cryptography, see for example the recent work by Yan *et al.*[13]

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

2 Quantum walks

The concept of random walk was introduced to describe the behavior of a "walker" over a path who, at each step, can choose to follow one of the possible directions with a certain *a priori* fixed probability. It was shown to be very useful in computer science (sampling massive online graphs, image

3

segmentation, estimating the size of the World Wide Web, wireless networking, etc.), physics (modeling the Brownian motion, studying polymers, etc.), and many other fields of research (financial economics, medicine and biology, psychology, etc.).

Quantum walks are the quantum counterpart of random walks and were first considered in Reference [14]. Unlike the classical case, in which the state of the walker is described by a probability distribution over the allowed positions, in the quantum scenario the state of the walker is given by a superposition of positions. Quantum walks are a successful tool in algorithmic theory since they provide an exponential speedup over classical computations for several oracular problems[15, 16, 17] and polynomial speedup for many important classical solutions of problems such as determining whether all the elements of a list are distinct[18], and in search problems in general [19]. Moreover, they are an important computational primitive, since they permit universal quantum computation [20, 21]. For practical implementations, see for example the recent book [22]. One can study different types of quantum walks, determined by their time evolution (discrete- vs continuous-time), underlying position space and their topology (walks on the line, lattice, circle, graphs, etc.). In this work we use discrete-time quantum walks on the circle.

2.1 One-dimensional discrete-time quantum walks

2.1.1 Basic dynamics

In a discrete-time quantum walk on an infinite line, we consider the movement of a walker along discrete positions on it, labeled $i \in \mathbb{Z}$. 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 state. The position and the coin state 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:

$$\hat{U} = \hat{S}\left(\hat{I}_p \otimes \hat{U}_c\right). \tag{1}$$

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

$$\hat{S} = \sum_{i \in \mathbb{Z}} \left(|i+1\rangle \langle i| \otimes |R\rangle \langle R| + |i-1\rangle \langle i| \otimes |L\rangle \langle L|\right), \tag{2}$$

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

$$\hat{U}_c = \hat{U}_c(\theta, \xi, \zeta) = \begin{bmatrix} e^{i\xi}\cos\theta & e^{i\zeta}\sin\theta \\ -e^{-i\zeta}\sin\theta & e^{-i\xi}\cos\theta \end{bmatrix}. \tag{3}$$

2.1.2 Shift operator on the circle

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

Without loss of generality, we consider 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:

$$
\begin{aligned}
\hat{S} &= \sum_{i=0}^{N-1} \Big(|i+1\,(\mathrm{mod}\ N)\rangle \langle i| \otimes |R\rangle \langle R| \\
&\qquad + |i-1\,(\mathrm{mod}\ N)\rangle \langle i| \otimes |L\rangle \langle L| \Big) \\
&= \hat{T}_1 \otimes |R\rangle \langle R| + \hat{T}_{-1} \otimes |L\rangle \langle L|
\end{aligned} \tag{4}
$$

where

$$\hat{T}_m = \sum_{i=0}^{N-1} |i+m\,(\mathrm{mod}\ N)\rangle \langle i| \tag{5}$$

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. To generate the public key, we use a discrete number of possible walks $\hat{U}_k = \hat{S}[\hat{I} \otimes \hat{U}_c(\theta_k, \xi_k, \zeta_k)]$, with $\theta_k = \xi_k = \zeta_k = k\frac{2\pi}{d}$, $k \in \mathcal{I} = \{1, 2, \ldots, d\}$ and $d \in \mathbb{N}$.

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 $SK = (\hat{U}_k, t, l)$ where:*
  $\hat{U}_k$ with $k \in \mathcal{I} = \{1, 2, \ldots, d\}$, $t \in \mathcal{T} = \{t_0, \ldots, t_{max}\} \subset \mathbb{N}$ and $l \in \{0, \ldots, 2^n - 1\}$.

Public-key generation

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

$$|\psi_{PK}\rangle = \hat{U}_k^t\,|l\rangle\,|s\rangle = \left[\hat{S}(\hat{I}_p \otimes \hat{U}_c)\right]^t |l\rangle\,|s\rangle . \qquad (6)$$

Message Encryption

- *Bob obtains Alice's public key $|\psi_{PK}\rangle$;*
- *He encrypts m by applying spatial translation to obtain:*

$$|\psi(m)\rangle = (\hat{T}_m \otimes \hat{I}_c)\,|\psi_{PK}\rangle ; \qquad (7)$$

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

Message Decryption

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

$$\hat{M} = \sum_i |i\rangle \langle i| \otimes \hat{I}_c \qquad (8)$$

and obtains the result m'. The message sent by Bob is $m = m' - l$ (mod N).

3.1   Correctness of the protocol

Proposition 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 is a direct consequence of the fact that the quantum walk $\hat{U}_k^t$ commutes with any translation $\hat{T}_m$. Thus, the state of the system before the final step of the decryption phase (measurement), is:

$$
\begin{aligned}
|\psi_f\rangle &= \hat{U}_k^{-t} |\psi(m)\rangle \\
&= \hat{U}_k^{-t} (\hat{T}_m \otimes \hat{I}_c) \hat{U}_k^t |l\rangle |s\rangle \\
&= (\hat{T}_m \otimes \hat{I}_c) |l\rangle |s\rangle \\
&= |l + m \,(\text{mod } N)\rangle |s\rangle.
\end{aligned}
\qquad (9)
$$

Hence, upon measuring $\hat{M}$ and obtaining $m' = l + m \,(\text{mod } N)$, the last modular operation performed in the last step of the *Message Decryption* reveals that the decrypted message is indeed m. $\qquad \square$

In the previous Proposition the crucial point is the fact that the quantum walk commutes with the translation. Below, we prove in detail that $\hat{U}_k^t$ and $(\hat{T}_m \otimes \hat{I}_c)$ commute.

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

Proof. Notice that the action of any $\hat{U}_k$ used in Protocol 1 can be written as:

$$\hat{U}_k \left|l\right\rangle \left|s\right\rangle = \alpha_{L(s)} \left|l-1\right\rangle \left|L\right\rangle + \alpha_{R(s)} \left|l+1\right\rangle \left|R\right\rangle , \tag{10}$$

where $\left|L\right\rangle$ and $\left|R\right\rangle$ 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:

$$\hat{T}_m \left|l\right\rangle = \left|l+m \,(\mathrm{mod}\ N)\right\rangle . \tag{11}$$

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

$$
\begin{aligned}
(\hat{T}_m \otimes \hat{I}_c)\hat{U}_k \left|l\right\rangle \left|s\right\rangle &= (\hat{T}_m \otimes \hat{I}_c)[\alpha_{L(s)} \left|l-1\right\rangle \left|L\right\rangle + \alpha_{R(s)} \left|l+1\right\rangle \left|R\right\rangle] \\
&= \alpha_{L(s)} \left|l-1+m \,(\mathrm{mod}\ N)\right\rangle \left|L\right\rangle \\
&\quad +\alpha_{R(s)} \left|l+1+m \,(\mathrm{mod}\ N)\right\rangle \left|R\right\rangle .
\end{aligned}
\tag{12}
$$

On the other hand, we also have:

$$
\begin{aligned}
\hat{U}_k(\hat{T}_m \otimes \hat{I}_c) \left|l\right\rangle \left|s\right\rangle &= \hat{U}_k \left|l+m \,(\mathrm{mod}\ N)\right\rangle \left|s\right\rangle \\
&= \alpha_{L(s)} \left|l-1+m \,(\mathrm{mod}\ N)\right\rangle \left|L\right\rangle \\
&\quad +\alpha_{R(s)} \left|l+1+m \,(\mathrm{mod}\ N)\right\rangle \left|R\right\rangle .
\end{aligned}
\tag{13}
$$

$\square$

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 $|\psi_{PK}\rangle$ 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 $\hat{\rho}_{PK}$ the mixed state of the public key, as perceived by Eve, who does not know *a priori* the secret key SK chosen by Alice. Even if Eve were to know $\hat{U}_k$ and t, $\hat{\rho}_{PK}$ is completely mixed:

$$
\begin{aligned}
\hat{\rho}_{PK} &= \hat{U}_k^t \left[\frac{1}{2^{n+1}} \sum_{l=0}^{2^n-1} \sum_{s\in\{L,R\}} |l\rangle\langle l| \otimes |s\rangle\langle s| \right] (\hat{U}_k^t)^\dagger \\
&= \hat{U}_k^t \left(\frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c \right) (\hat{U}_k^t)^\dagger \\
&= \frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c.
\end{aligned}
\tag{14}
$$

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

$$
I(SK, E) \le S(\hat{\rho}_{PK}) = -\operatorname{Tr}(\hat{\rho}_{PK} \log \hat{\rho}_{PK}) = n + 1.
\tag{15}
$$

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 $\hat{U}_k$, t and the initial state $|l\rangle\,|s\rangle$. In the following we denote by p_k the probability to choose $\hat{U}_k$ from the set $\left\{ \hat{U}_k | k \in \mathcal{I} = \{1, 2, \ldots, d\} \right\}$, by p_t the

9

probability to run the walk for t steps, with $t \in \mathcal{T} = \{t_0, \ldots, t_{max}\}$, 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 SK is given by:

$$p_{SK} = p_k \, p_t \, p_{l,s} = \frac{1}{d \, |\mathcal{T}| \, 2^{n+1}}, \tag{16}$$

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

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

$$
\begin{aligned}
H(p_{SK}) &= -\sum_{k \in \mathcal{I}} \sum_{t \in \mathcal{T}} \sum_{l=0}^{2^n - 1} \sum_{s \in \{L,R\}} p_k \, p_t \, p_{l,s} \log_2(p_k \, p_t \, p_{l,s}) \\
&= \log_2(d \, |\mathcal{T}| \, 2^{n+1}) \tag{17} \\
&= \log_2(d \, |\mathcal{T}|) + n + 1.
\end{aligned}
$$

Thus, we have:

$$I(SK, E) \leq S(\hat{\rho}_{PK}) < H(p_{SK}). \tag{18}$$

With the appropriate choice of $|\mathcal{T}|$ and d, e.g., $|\mathcal{T}|, \log d \approx poly(n)$, for sufficiently large n, the Shannon entropy of the secret key has a polynomial overhead over the von Neumann entropy of the public key as seen by Eve,

$$H(p_{SK}) - S(\hat{\rho}_{PK}) = \log_2(d \, |\mathcal{T}|) \approx poly(n). \tag{19}$$

This way, upon obtaining the maximal possible information about the secret key, given by $S(\hat{\rho}_{PK})$, Eve's uncertainty (in the number of bits) of the SK is still polynomial in n, i.e., the number of keys consistent with the information she has is exponential in n. We note that the choice of $d \approx \exp(n)$ secures the secrecy of the encrypted message, while $|\mathcal{T}| \approx poly(n)$ was chosen to maintain the protocol's efficiency, discussed in the next section.

For the rest of this section we discuss the security of the message m during the second phase of the protocol, when Bob sends the encrypted message

10

$|\psi(m)\rangle = (\hat{T}_m \otimes \hat{I}_c)|\psi_{PK}\rangle$ to Alice. Without knowing the secret key, the state perceived by Eve is still a complete mixture:

$$\hat{\rho}_E = (\hat{T}_m \otimes \hat{I}_c)\left(\frac{1}{2^{n+1}}\hat{I}_p \otimes \hat{I}_c\right)(\hat{T}_m \otimes \hat{I}_c)^\dagger = \frac{1}{2^{n+1}}\hat{I}_p \otimes \hat{I}_c. \qquad (20)$$

The most that Eve can learn is the very quantum state $|\psi(m)\rangle$ (although, as proven above, even that is impossible, unless with negligible probability). Nevertheless, without knowing the secret key, this information is not enough for Eve to infer the message encrypted by Bob. This is a simple consequence of the fact that for each allowed encryption state, there exists a suitably chosen secret key that can decrypt *any* message m. Indeed, a state $|\psi(m)\rangle$ that for the secret key $SK = (\hat{U}_k, t, l)$ corresponds to the message m, for the secret key $SK' = (\hat{U}_k, t, l - \Delta l)$ corresponds to the message $m + \Delta l$ (below, the subscripts SK and SK' explicitly denote the secret key used to encrypt the corresponding messages m and $m + \Delta l$, respectively):

$$\begin{aligned}
|\psi(m)\rangle_{SK} &= (\hat{T}_m \otimes \hat{I}_c)|\psi_{PK}\rangle \\
&= (\hat{T}_m \otimes \hat{I}_c)\hat{U}_k^t(\hat{T}_{\Delta l} \otimes \hat{I}_c)|l - \Delta l\rangle|s\rangle \qquad (21) \\
&= (\hat{T}_{m+\Delta l} \otimes \hat{I}_c)\hat{U}_k^t|l - \Delta l\rangle|s\rangle \\
&= |\psi(m + \Delta l)\rangle_{SK'}.
\end{aligned}$$

3.3   Efficiency of the protocol

In this section we show the efficiency of the proposed protocol, i.e. the overall time τ required for its execution (public-key generation, message encryption and message decryption) scales polynomially with the length n of the message.

The public-key generation as well as the message decryption are efficient procedures, since the quantum walks used to perform them are efficient. Indeed, denoting by $\Delta\tau_w$ the time required for a single step $\hat{U}$ of the walk, the full walk $\hat{U}^t$ is completed in time $\tau = t \cdot \Delta\tau_w$. In the previous section we took $t \approx poly(n)$ for security purposes, a choice which is also adequate for

the efficiency of the quantum walk: the time required to perform the walk is polynomial in n.

In addition to this, for the overall protocol to be efficient, the message encryption, given by the translation operator $\hat{T}_m$, has to be efficient as well. It might seem at first that the encryption of the message is not efficient, as it requires $\boldsymbol{O}(2^n)$ single-position translations, $\hat{T}_m = (\hat{T}_1)^m$. Below, we show that this is not necessarily a non-efficient procedure, i.e., various practical implementations of $\hat{T}_m$ are indeed efficient.

In case the system that performs the quantum walk consists of $n + 1$ qubits (n carrying the position of the walker plus the coin one), such that the states of the computational basis encode different positions (see for example Reference [23]), the translation operator $\hat{T}_m$ is nothing but the addition by m, which is an efficient operation for a quantum computer. Alternatively, in those cases of physical realizations in which different position states $|i\rangle$ are given by distinct spatial positions (see for example implementations based on integrated photonics[24]), Bob can simply re-label the positions on the device that carries the quantum state of the public key, i.e. $i \to i - m$, which is also efficient, as he can do it in parallel at the same time for all position states.

4   Conclusions

In this paper we presented a quantum public-key cryptographic system based on quantum walks. Unlike the recently proposed protocol[12] 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 rather 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 includes designing other security protocols based on the use of quantum walks, such as oblivious transfer (along the lines of the recently proposed protocol presented in Reference [25]), commitment schemes and other privacy functionalities.

Acknowledgements

References

[1] 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.

[2] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In *Proceedings of the 17th Annual Inter-*

national Cryptology Conference on Advances in Cryptology, CRYPTO '97, pages 112–131, London, UK, UK, 1997. Springer-Verlag.

[3] L. Fortnow. *The Golden Ticket - P, NP, and the Search for the Impossible.* Princeton University Press, 2013.

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

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

[6] 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.

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

[8] 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.

[9] IdQuantic. Clavis QKD Platform, `http://www.idquantique.com/photon-counting/clavis-qkd-platform/`, 2015.

[10] T. Okamoto, K. Tanaka, and S. Uchiyama. Quantum public-key cryptosystems. In *in Proc. of CRYPT0 2000*, pages 147–165. Springer-Verlag, 2000.

[11] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In *Proceedings of Advances in Cryptology - EUROCRYPT*

2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, volume 3494 of *Lecture Notes in Computer Science*, pages 268–284. Springer, 2005.

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

[13] Y. Yang, Q. Pan, S. Sun, and P. Xu. Novel image encryption based on quantum walks. *Scientific Reports*, 5:7784, 01 2015.

[14] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random walks. *Phys. Rev. A*, 48:1687–1690, Aug 1993.

[15] A. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing*, STOC '03, pages 59–68, New York, NY, USA, 2003. ACM.

[16] J. Kempe. Quantum random walks: An introductory overview. *Contemporary Physics*, 44(4):307–327, 2003.

[17] A. Ambainis. Quantum walks and their algorithmic applications. *International Journal of Quantum Information*, 01(04):507–518, 2003.

[18] M. Santha. Quantum walk based search algorithms. In M. Agrawal, D. Du, Z. Duan, and A. Li, editors, *Theory and Applications of Models of Computation*, volume 4978 of *Lecture Notes in Computer Science*, pages 31–46. Springer Berlin Heidelberg, 2008.

[19] R. Portugal. *Quantum walks and search algorithms.* Quantum Science and Technology. New York, NY: Springer., 2013.

[20] Neil B. Lovett, Sally Cooper, Matthew Everitt, Matthew Trevers, and Viv Kendon. Universal quantum computation using the discrete-time quantum walk. *Phys. Rev. A*, 81:042330, Apr 2010.

[21] Andrew M. Childs, David Gosset, and Zak Webb. Universal computation by multiparticle quantum walk. 339(6121):791–794, 2013.

[22] K. Manouchehri and J. Wang. *Physical Implementation of Quantum Walks*. Springer Publishing Company, Incorporated, 2013.

[23] C. Ryan, M. Laforest, J. Boileau, and R. Laflamme. Experimental implementation of a discrete-time quantum random walk on an nmr quantum-information processor. *Phys. Rev. A*, 72:062317, Dec 2005.

[24] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi, and R. Osellame. Two-particle bosonic-fermionic quantum walk via integrated photonics. *Phys. Rev. Lett.*, 108:010502, Jan 2012.

[25] 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.