Chapter 1

A public-key cryptographic system based on quantum walks

In this chapter, we present a quantum public-key cryptographic system, in which the public keys are states generated by means of a QW, while the secret key consists of: (i) the QW operator, (ii) the number of steps that the walk is performed and (iii) the starting position and coin of the QW. In the next section we present the protocol and prove its correctness, while in the following Sections 1.2 and 1.3, we prove its security and efficiency. Finally, in the last section we summarise our results and point out some possible directions for future work.

*The work presented in this chapter corresponds to the work published in [**?**].

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

For our public-key cryptographic system we will consider DTQWs on a circle, as presented in Section 1.4 of the introductory Chapter 1. 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 $d \in \mathbb{N}$, given by the standard shift and coin operations $\hat{U}_c(\theta_k, \xi_k, \zeta_k)$, presented in Section 1.4.

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

Public-key generation

- *A 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:*

$$|\psi_{PK}\rangle = \hat{U}_k^t |l\rangle |s\rangle = \left[\hat{S}(\hat{I}_p \otimes \hat{U}_c)\right]^t |l\rangle |s\rangle . \tag{1.1}$$

Message Encryption

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

$$|\psi(m)\rangle = (\hat{T}_m \otimes \hat{I}_c) |\psi_{PK}\rangle ; \tag{1.2}$$

- *B sends* $|\psi(m)\rangle$ *to A.*

Message Decryption

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

$$\hat{M} = \sum_i |i\rangle \langle i| \otimes \hat{I}_c \tag{1.3}$$

and obtains the result m'*. The message sent by B is* $m = m' - l \pmod N$.

1.1.1 Correctness of the protocol

Proposition 1. *The above protocol is correct, that means that if A and B follow it, and no third party intervenes during its execution, at the end of the decryption phase A recovers the message sent by B with probability* 1.

Proof. The correctness of the protocol when both parties follow the prescribed steps is a direct consequence of the fact that the QW $\hat{U}_k^t$ commutes with any translation $\hat{T}_m$ (see the following Lemma 1). Thus, the state of the system before the final step of the decryption phase (measurement), is:

$$\begin{aligned} |\psi_f\rangle &= \hat{U}_k^{-t} |\psi(m)\rangle \\ &= \hat{U}_k^{-t} (\hat{T}_m \otimes \hat{I}_c) \hat{U}_k^t |l\rangle |s\rangle \\ &= (\hat{T}_m \otimes \hat{I}_c) |l\rangle |s\rangle \\ &= |l + m \,(\mathrm{mod}\ N)\rangle |s\rangle . \end{aligned} \tag{1.4}$$

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

Below, we prove 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 QW 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:

$$\hat{U}_k |l\rangle |s\rangle = \alpha_{L(s)} |l-1\rangle |L\rangle + \alpha_{R(s)} |l+1\rangle |R\rangle , \tag{1.5}$$

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:

$$\hat{T}_m |l\rangle = |l + m \,(\mathrm{mod}\ N)\rangle . \tag{1.6}$$

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

$$\begin{aligned} (\hat{T}_m \otimes \hat{I}_c) \hat{U}_k |l\rangle |s\rangle &= (\hat{T}_m \otimes \hat{I}_c)[\alpha_{L(s)} |l-1\rangle |L\rangle + \alpha_{R(s)} |l+1\rangle |R\rangle] \\ &= \alpha_{L(s)} |l - 1 + m \,(\mathrm{mod}\ N)\rangle |L\rangle \\ &\quad + \alpha_{R(s)} |l + 1 + m \,(\mathrm{mod}\ N)\rangle |R\rangle . \end{aligned} \tag{1.7}$$

On the other hand, we also have:

$$\begin{aligned}\hat{U}_k(\hat{T}_m \otimes \hat{I}_c)\,|l\rangle\,|s\rangle &= \hat{U}_k\,|l+m\,(\mathrm{mod}\ N)\rangle\,|s\rangle \\ &= \alpha_{L(s)}\,|l-1+m\,(\mathrm{mod}\ N)\rangle\,|L\rangle \\ &\quad +\alpha_{R(s)}\,|l+1+m\,(\mathrm{mod}\ N)\rangle\,|R\rangle\,. \end{aligned} \tag{1.8}$$

□

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

1.2 Security of the protocol

The protocol consists of two phases. In the first, A sends a public key $|\psi_{PK}\rangle$ to B. In the second, upon encrypting the message m, B sends back to A the state $|\psi(m)\rangle$. 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 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 E, who does not know *a priori* the secret key SK chosen by A. Even if E were to know $\hat{U}_k$ and t, $\hat{\rho}_{PK}$ is completely mixed:

$$\begin{aligned}\hat{\rho}_{PK} &= \hat{U}_k^t \left[\frac{1}{2^{n+1}} \sum_{l=0}^{2^n-1} \sum_{s\in\{L,R\}} |l\rangle\langle l| \otimes |s\rangle\langle s|\right] (\hat{U}_k^t)^\dagger \\ &= \hat{U}_k^t \left(\frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c\right) (\hat{U}_k^t)^\dagger \qquad (1.9) \\ &= \frac{1}{2^{n+1}} (\hat{I}_p \otimes \hat{I}_c) \hat{U}_k^t (\hat{U}_k^t)^\dagger \qquad (1.10) \\ &= \frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c. \end{aligned}$$

Assuming that E 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 is bounded from above by the Von Neumann entropy of this state:

$$I(SK, E) \leq S(\hat{\rho}_{PK}) = -\,\mathrm{Tr}(\hat{\rho}_{PK} \log \hat{\rho}_{PK}) = n+1. \tag{1.11}$$

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 $\hat{U}_k, t, l$ and s. 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 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 from $\{0, 1, \ldots, 2^n - 1\}$ and s from $\{L, R\}$ in order to generate the initial state $|l\rangle |s\rangle$. Since these choices are random and independent, the probability of a certain secret key SK is given by:

$$p_{SK} = p_k \, p_t \, p_{l,s} = \frac{1}{d \, |\mathcal{T}| \, 2^{n+1}}, \tag{1.12}$$

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

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

$$\begin{aligned} H(p_{SK}) &= -\sum_{k \in \mathcal{I}} \sum_{t \in \mathcal{T}} \sum_{l=0}^{2^n - 1} \sum_{s \in \{L,R\}} p_k \, p_t \, p_{l,s} \log_2(p_k \, p_t \, p_{l,s}) \\ &= \log_2(d \, |\mathcal{T}| \, 2^{n+1}) \\ &= \log_2(d \, |\mathcal{T}|) + n + 1. \end{aligned} \tag{1.13}$$

Thus, we have:

$$I(SK, E) \leq S(\hat{\rho}_{PK}) < H(p_{SK}), \tag{1.14}$$

since $\log_2(d \, |\mathcal{T}|) >> 1$. 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 E,

$$H(p_{SK}) - S(\hat{\rho}_{PK}) = \log_2(d \, |\mathcal{T}|) \approx poly(n). \tag{1.15}$$

This way, upon obtaining the maximal possible information about the secret key, given by $S(\hat{\rho}_{PK})$, E'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.

Notice that d could be exponential on n, since in the protocol we only need to provide information to specify the walk (in fact, $\log(d)$ bits). However, in order for the protocol to be efficient as we discuss in the next section, $|\mathcal{T}|$ must be polynomial on n.

For the rest of this section we will discuss the security of the message m during the second phase of the protocol, when B sends the encrypted message $|\psi(m)\rangle = (\hat{T}_m \otimes \hat{I}_c) |\psi_{PK}\rangle$ to A. Without knowing the secret key, the state perceived by E is still a complete mixture:

$$\begin{aligned} \hat{\rho}_E &= (\hat{T}_m \otimes \hat{I}_c) \left(\frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c \right) (\hat{T}_m \otimes \hat{I}_c)^\dagger = \\ &= \frac{1}{2^{n+1}} (\hat{T}_m \otimes \hat{I}_c)(\hat{T}_m \otimes \hat{I}_c)^\dagger (\hat{I}_p \otimes \hat{I}_c) = \frac{1}{2^{n+1}} \hat{I}_p \otimes \hat{I}_c. \end{aligned} \tag{1.16}$$

The most that E 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 E to infer the message encrypted by B. 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):

$$\begin{aligned} |\psi(m)\rangle_{SK} &= (\hat{T}_m \otimes \hat{I}_c)\,|\psi_{PK}\rangle = (\hat{T}_m \otimes \hat{I}_c)\hat{U}_k^t\,|l\rangle\,|s\rangle \\ &= (\hat{T}_m \otimes \hat{I}_c)\hat{U}_k^t(\hat{T}_{\Delta l} \otimes \hat{I}_c)\,|l - \Delta l\rangle\,|s\rangle \\ &= (\hat{T}_m \otimes \hat{I}_c)(\hat{T}_{\Delta l} \otimes \hat{I}_c)\hat{U}_k^t\,|l - \Delta l\rangle\,|s\rangle \\ &= (\hat{T}_{m+\Delta l} \otimes \hat{I}_c)\hat{U}_k^t\,|l - \Delta l\rangle\,|s\rangle \\ &= |\psi(m + \Delta l)\rangle_{SK'}\,. \end{aligned} \tag{1.17}$$

1.3 Efficiency of the protocol

In this section we show the efficiency of the proposed protocol, i.e. that 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 performing the respective QWs is 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 QW: 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 QW 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 [**?**]), the translation operator $\hat{T}_m$ is nothing but the addition by m, which is an efficient operation in a quantum computer. Alternatively, in those cases of physical realisations in which different position states $|i\rangle$ are given by distinct spatial positions (see for example implementations based on integrated photonics [**?**]), B can simply relabel 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 the position states.

1.4 Conclusions

We presented a quantum public-key cryptographic system based on QWs. Unlike a recent similar protocol [**?**], which uses single-qubit rotations to generate the public key, in our scheme the execution of a QW, in general, results in entangled quantum states as public keys, thus increasing the practical security (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 analysed the complexity of our public-key generation and message encryption/ decryption procedures and showed their efficiency, i.e., the complexity of our protocol scales polynomially with the size of the message.

In the next chapter, we will use QWs to design QKD protocols. However, we should mention here that the applications of QWs in cryptography are not yet exhausted. A relevant path of future research would be to design other kinds of security protocols based on QWs, such as oblivious transfer (along the lines of the protocol proposed in [**?**]) and commitment schemes, as well as privacy functionalities, like message authentication and quantum digital signatures.