

Quantum key distribution with quantum walks

C. Vlachou^{1,2,6}, W. Krawec³, P. Mateus^{1,2},
N. Paunković^{1,2,6} and A. Souto^{1,4,5}

¹ SQIG – Instituto de Telecomunicações

² Dep. de Matemática – Instituto Superior Técnico, Universidade de Lisboa

³ Computer Science and Engineering Department,
University of Connecticut, Storrs, CT 06268 USA

⁴ LaSige – Faculdade de Ciências, Universidade de Lisboa

⁵ Dep. de Informática – Faculdade de Ciências, Universidade de Lisboa

⁶ CeFEMA, Instituto Superior Técnico, Universidade de Lisboa

October 4, 2018

Abstract

Quantum key distribution is one of the most fundamental cryptographic protocols. Quantum walks are important primitives for computing. In this paper we take advantage of the properties of quantum walks to design new secure quantum key distribution schemes. In particular, we introduce a secure quantum key-distribution protocol equipped with verification procedures against full man-in-the-middle attacks. Furthermore, we present a one-way protocol and prove its security. Finally, we propose a semi-quantum variation and prove its robustness against eavesdropping.

1 Introduction

Quantum Key Distribution (QKD) is the most secure and practical instance of quantum cryptography. We recall that a key distribution scheme is a protocol between two parties with the purpose of sharing a common string (the key), which afterwards, they can use to communicate privately, in a pre-agreed encryption scheme. Therefore, it is required that any third party that might be eavesdropping is not able to extract information about the key, and thus compromising the privacy of the communication. Bennet and Brassard [1] in 1984, and Ekert [2] in 1991, proposed the first QKD protocols, upon which all QKD protocols

are based. Since then a lot of modifications and improvements have been proposed in order to achieve unconditionally secure and practical QKD schemes, by taking advantage of the physical laws of quantum mechanics. For a review, see [3]. Several QKD experiments over long distances have been reported [4, 5, 6, 7], and QKD is already commercial.¹ Furthermore, the recent successful launch of a satellite [8] paved the way for intercontinental QKD.

Quantum walks (QW) have been introduced in 1993, in [9], as the quantum analogue of classical random walks. Since then, they have been playing a major role in quantum computing theory, as their applications vary from quantum algorithms [10, 11, 12, 13, 14] to universal quantum computing schemes [15, 16, 17].

Recently, the application of QWs to the creation of actual quantum cryptographic protocols has been investigated. For instance, in [18], Rohde *et al.*, proposed a limited form of quantum homomorphic encryption using multi-particle QWs. In their protocol, a server could manipulate data sent by a client in such a way that, first, the server has limited information on the client's data while, second, the client has limited information on the server's computation.

In this paper, we revisit the public-key cryptosystem [19], which is based on QWs, in order to construct secure QKD protocols. First, we suitably modify [19], so that the quantum state generated by means of a QW encodes the secret key as opposed to the message; such a key could be used later as input to a one-time-pad encryption system gaining information theoretic security for message delivery. Our motivation is that QKD schemes have several advantages, which we present in due course, over public-key cryptosystems. The modification of the original public-key system is non-trivial, however, and requires care as we can no longer rely on the existence of a trusted mechanism for public-key delivery (such as a public-key infrastructure), as is typically assumed in quantum public-key cryptography [20, 21, 19].

While the above QKD protocol is two-way, i.e., both Alice (A) and Bob (B) perform QW operations, we also construct a one-way QKD protocol, where again the key is encoded in a QW state. In this case, it is only Alice that chooses randomly the precise QW to encode the key, while Bob is randomly choosing in which basis (computational or QW) to measure in order to obtain it. After disclosing their choices by means of classical communication, they are able to establish a shared key. We prove that the protocol is secure against general attacks, even if the eavesdropper Eve (E) has great advantage over Alice and Bob.

As a third contribution in this paper, we propose a new *semi-quantum* key-distribution (SQKD) protocol based on QWs. Semi-quantum cryptography was first introduced in 2007 by Boyer *et al.*, in [22, 23] as a way to study “how quantum” does a protocol need to be in order to gain an advantage over its classical counterpart – namely, how quantum do the parties need to be in order to establish a secret key secure against an all powerful adversary. Using classical communication alone, this task is impossible – indeed, any key distribution protocol, relying only on classical communication, cannot be unconditionally secure and, instead, requires computational hardness assumptions to be made on the adversary. On the other hand, QKD protocols do have provable unconditional security. A semi-quantum

¹Currently there are three companies offering commercial QKD systems: ID Quantique (Geneva), MagiQ Technologies, Inc. (New York) and QuintessenceLabs (Australia).

protocol places severe restrictions on one of the participating users (typically Bob) in that he may only operate in a “classical” or “semi-quantum” manner. Namely, this limited user can only directly work with the computational Z basis. No restrictions are placed on the other participant Alice, and of course, no restrictions are placed on Eve.

The paper is organized as follows: In Section 2, we provide a brief introduction to QWs, with all the information and notation used throughout the paper. In Section 3, we present a secure two way QKD scheme based on QWs, which is a modification of the public-key cryptosystem in Ref. [19]. We give motivation for this modification and furthermore, we propose two different verification procedures against full man-in-the-middle attacks. In Section 4, we introduce a one-way QKD protocol, which we prove to be unconditionally secure, by reducing it to an equivalent entanglement-based protocol. We provide our numerical results for the optimal choice of the QW parameters that maximize the noise tolerance of the protocol. Finally, in Section 5 we provide a SQKD protocol and we show its robustness against eavesdropping.

2 Quantum Walk Preliminaries

In this paper we consider QWs on a circle. In this case, the walker hops along discrete positions on a circle. The Hilbert space \mathcal{H} , describing the QW, is the tensor product of the positions Hilbert space \mathcal{H}_p and the coin Hilbert space \mathcal{H}_c , i.e. $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$. The positions Hilbert space is spanned by the points on a circle $\{|x\rangle | x \in \{0, \dots, P-1\}\}$, while \mathcal{H}_c is spanned by the two possible coin states $\{|R\rangle, |L\rangle\}$, corresponding to heads and tails. The evolution for one step of the QW is given by the unitary operator

$$U = S \cdot (I_p \otimes R_c)$$

where I_p is the identity operator in \mathcal{H}_p , $R_c \in SU(2)$ is a rotation in \mathcal{H}_c , which in matrix form we can write it as:

$$R_c(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}, \quad (1)$$

and

$$S = \sum_{x=0}^{P-1} [|x+1 \pmod{P}\rangle \langle x| \otimes |R\rangle \langle R| \quad (2)$$

$$+ |x-1 \pmod{P}\rangle \langle x| \otimes |L\rangle \langle L|] \quad (3)$$

is the shift operator that moves the walker one position to the right or to the left on the circle, depending on its coin state. Notice that, since we are on a circle, the P -th position is identified with the 0 position.

3 Quantum Walk Key-Distribution Scheme

In this section we introduce a QKD scheme based on QWs. In this context, the key for the QKD is encrypted as the message in the public-key cryptosystem introduced in [19]. This

modification is motivated by the fact that QKD schemes are more flexible than public-key protocols, as the key can be used by both Alice and Bob to send or authenticate messages. Also, more post-processing techniques (e. g. privacy amplification) can be applied, since we have as input a random string and not a plaintext message. In the latter case we should be careful during the post-processing not to degrade the message (we are left with less techniques). Furthermore, in the case of information leakage, we can safely abort the protocol, while during message transmission it would be late for that.

Our QW-QKD scheme is depicted in Fig. 1 and presented below. We assume that the key can be chosen among P possible keys. We also assume that the QW can be chosen from a prefixed discrete set known by both parties.

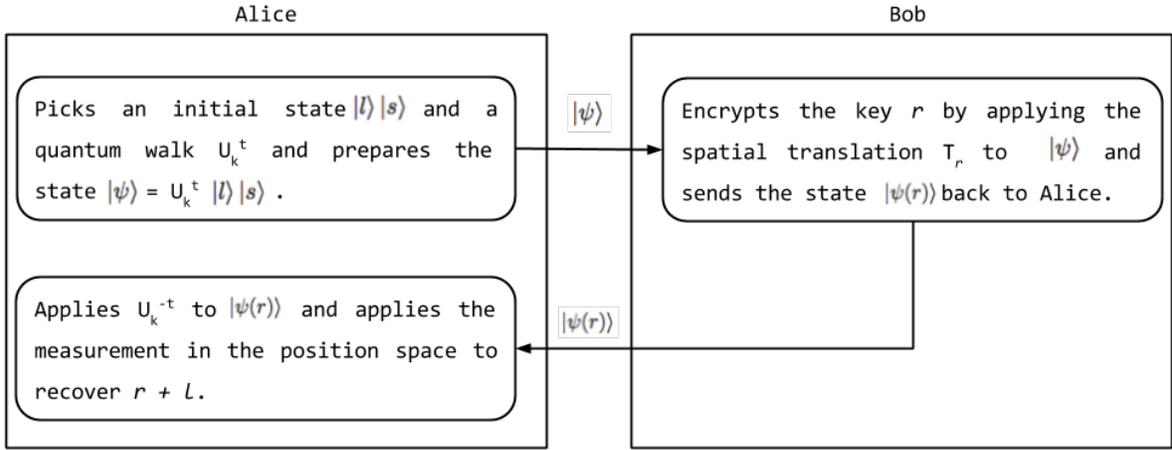


Figure 1: Description of the basic steps of Protocol 1.

Protocol 1. Quantum key-distribution scheme

Inputs for the protocol

- Key:
 $r \in \{0, \dots, P - 1\}$, i.e., a key of at most $\log P$ bits, chosen by Bob uniformly at random;
- Quantum state generation:
 The QW operator U_k with $k \in \mathcal{K} = \{1, 2, \dots, K\}$, the number of steps $t \in \mathcal{T} = \{T_0, \dots, T_{max}\} \subset \mathbb{N}$, and the initial state $|l\rangle \otimes |s\rangle$, where $l \in \{0, \dots, P - 1\}$, $s \in \{R, L\}$.

In the above, U_k , the QW operator is defined as $U_k = S \cdot (I_p \otimes R_c(\theta_k))$, where S is the shift operator and $R_c(\theta_k)$ is a rotation of $\theta_k = k \cdot 2\pi/K$ in the coin space, see Eq. 1 and 2.

Quantum state generation

- Alice chooses uniformly at random $l \in \{0, \dots, P-1\}$ and $s \in \{R, L\}$, and generates the initial state $|l\rangle |s\rangle$.
- Then she chooses, also at random, the QW $U_k = S \cdot (I_p \otimes R_c(\theta_k))$ and the number of steps $t \in \mathcal{T}$.
- Finally, she generates the quantum state:

$$|\psi\rangle = U_k^t |l\rangle |s\rangle = [S \cdot (I_p \otimes R_c(\theta_k))]^t |l\rangle |s\rangle,$$

and sends it to Bob.

Key encryption

- Upon obtaining the quantum state $|\psi\rangle$ from Alice, Bob encrypts the key r by applying spatial translation $T_r = \sum_{i=0}^{P-1} |i+r \pmod{P}\rangle \langle i|$ to obtain:

$$|\psi(r)\rangle = (T_r \otimes I_c) |\psi\rangle,$$

where I_c is the identity operator in the coin space.

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

Key decryption

- Alice applies U_k^{-t} to the state $|\psi(r)\rangle$.
- She performs the position measurement

$$M = \sum_{i=0}^{P-1} |i\rangle \langle i| \otimes I_c$$

and obtains the result i_0 .

The key sent by Bob is $r = i_0 - l \pmod{P}$.

It is clear, from the design of the protocol and the proof of correctness of the original quantum encryption scheme presented in [19] that, if no one interferes with the quantum states, then the protocol is correct and at the end, Alice and Bob will share a common string of length $\log P$, that they can use as a key. In the next section we prove the security of the protocol.

3.1 Security of the Scheme

In [19], the authors use the Holevo theorem to show that Eve can extract information about the key, by means of the quantum states $|\psi\rangle$ and $|\psi(r)\rangle$ that Alice and Bob exchange, only with negligible probability. Here, we do not present this proof of security for the sake of brevity, but the interested reader can find it in [19] with all the details. There, it was shown that the protocol is secure if the size of the space of parameters, which are chosen uniformly at random, is exponentially large with respect to the length of the message transmitted (the key in our case of a QKD protocol), see Equation (19) and the comment below it, in Section 3.2 of [19]. Moreover, for the protocol to be efficient, it was shown that the size of the \mathcal{T} (set of possible number of steps) should be polynomial with respect to the length of the message/key transmitted, see Section 3.3 of [19]. Therefore, to maintain the protocol's security, it is necessary that the size of \mathcal{K} , the set of possible coin unitaries U_k , is exponentially large with respect to the size of the key. As a consequence, while it is possible to fix the number of steps of the QW, and thus somewhat simplify its implementation, to maintain the security, it is necessary to keep the parameter k of the protocol.

Another type of attack that Eve can perform is a full man-in-the-middle attack, in which she impersonates Alice to Bob and vice versa, while they think that they are communicating directly. This attack gives Eve the chance to intercept and alter the communication between them. In public-key cryptosystems such attacks can be prevented by using a public-key infrastructure, which is assumed to work as a trusted third party. In our QKD modification though, such an assumption could not be used, therefore we should complete the security analysis of the scheme, by taking into account full man-in-the-middle attacks. To this end, we propose two different verification procedures, that allow Alice and Bob to verify that what they receive is actually coming from each other and not from an eavesdropper pretending to be either of them. We should note that for both verification methods, Alice and Bob need to share a classical public authenticated channel (a common requirement in QKD protocols, such as the well-known BB84 scheme [1]).

3.1.1 Standard Verification

The first technique we propose is a standard cut-and-choose verification, which is achieved by adding redundancy to our scheme. Clearly, the verification is needed twice in our protocol: once when Alice sends the QW state to Bob and once when Bob sends the encoded key to Alice.

Verification 1: *Bob verifies that it was Alice who sent him the quantum state.*

It is needed to prevent Eve from sending her choice of quantum states to Bob, which would allow her to read the encrypted key while he is sending it back to Alice.

- Alice sends to Bob $\bigotimes_{i=1}^m |\psi_i\rangle$, that is, several quantum states $|\psi_i\rangle$, generated by a QW as described in the previous section. Each $|\psi_i\rangle$ is generated using independently chosen walk parameters and initial states (k_i, t_i, l_i, s_i) .

- After Bob receiving $\bigotimes_{i=1}^m |\psi_i\rangle$, Alice, through a classical authenticated channel, sends him a string $v = v_1 v_2 \dots v_m$ of m bits, such that $v_i = 1$ if the corresponding $|\psi_i\rangle$ is going to be used for verification and $v_i = 0$ otherwise, that is, if the corresponding $|\psi_i\rangle$ will be used by Bob to encode part of the key. Through the classical channel, she also sends (j, k_j, t_j, l_j, s_j) , for some uniformly at random chosen j 's that belong in the set $\{1, \dots, m\}$. Let the number of these j 's be $m/3$.
- Bob verifies that for all these j 's, the received states $\rho_j = |\psi_j\rangle \langle \psi_j|$ are indeed equal to the pure states

$$|\psi_j\rangle = U_{k_j}^{t_j} |l_j\rangle |s_j\rangle.$$

In order to verify that, he applies $U_{k_j}^{-t_j}$ to the states $|\psi_j\rangle$, for all j and then performs a measurement for each j in the positions space as well as in the spin space. This measurement (for each j) is described by the operator:

$$\begin{aligned} M_{l_j, s_j} &= \sum_{l_j, s_j} \alpha_{l_j, s_j} |l_j, s_j\rangle \langle l_j, s_j| \\ &= \sum_{l_j} l_j |l_j\rangle \langle l_j| \otimes \sum_{s_j} s_j |s_j\rangle \langle s_j|. \end{aligned}$$

This way, he traces out all these $|\psi_j\rangle$'s and he is left with $2m/3$ quantum states. We call the reader's attention to the fact that if the verification fails for any j , the protocol is stopped.

Verification 2: *Alice verifies that it was Bob who sent her the encrypted key.*

This procedure is needed to prevent Eve from sending to Alice a message that would decrypt a key different from the one sent by Bob. In this case, Alice and Bob would not be able to communicate, while Eve would be able to decrypt messages sent by Alice (not vice versa). To prevent this from happening, Alice and Bob repeat the verification procedure 1, with the roles switched. In particular, the two are performing the following steps:

- Bob encrypts $r_i \in \{0, \dots, P-1\}$ in each of the states of the remaining product state $\bigotimes_{i=1}^{2m/3} |\psi_i\rangle$ as follows:

$$|\psi(r_i)\rangle = (T_{r_i} \otimes I_c) |\psi_i\rangle, \forall i \in \{1, \dots, 2m/3\}$$

that is, translating each state $|\psi_i\rangle$ by r_i in the positions space, leaving the spin part of the state unaltered.

- He sends the product state $\bigotimes_{i=1}^{2m/3} |\psi(r_i)\rangle$ to Alice.
- Then he chooses $m/3$ uniformly at random j 's out of the $2m/3$ unused indices from the previous verification procedure. Through the classical public authenticated channel he sends a classical string $v' = v'_1 v'_2 \dots v'_{2m/3}$ of $2m/3$ bits, such that $v'_i = 1$ if the

corresponding $|\psi(r_i)\rangle$ is going to be used for verification and $v'_i = 0$ otherwise, that is, if the corresponding $|\psi(r_i)\rangle$ contains part of the key. For each j' chosen (for which $v'_i = 1$), he also sends through the classical public authenticated channel the index and the respective $r_{j'}$'s used to generate the state $|\psi(r_i)\rangle$.

- In the last step, Alice applies $U_{k_i}^{-t_i}$ on the $2m/3$ states $|\psi(r_i)\rangle$ and then, for each i , she performs a measurement on the positions space. Let the outcomes be denoted by $\alpha_i, i \in \{1, \dots, 2m/3\}$. For all the indices she computes $r_i = \alpha_i - l_i$, where l_i are the initial positions on the circle that she used for the generation of the quantum states $|\psi_i\rangle$. Finally, for each $j', r_{j'}$ sent by Bob, Alice verifies the consistency of their results.
- The key is given by the concatenation of the bits r_i that were not used during the two verification procedures and it has $m \cdot (\log P)/3$ bits. Usually, the choice of m is dependent on the desired length, $\log P$, of the key, and in order to make the success probability of a man-in-the-middle attack negligible on $\log P$, it is common to use $m = (\log P)/3$.

3.1.2 Verification using maximally entangled states

In this section, we present an alternative verification procedure, which prevents Eve from trying to infer the key by first entangling her ancillas with the systems sent by Alice, and then performing an additional operation (say, a measurement) on the joint system of her ancillas and those carrying the encrypted key sent back to Alice by Bob; a method which in general would give her access to some non-negligible amount of information, so that Alice and Bob are not able to securely communicate. Note that this verification procedure could also be used against the previous attack in which Eve simply impersonates Alice to Bob, and vice versa.

During the first step of the protocol (“Quantum state generation”), in addition to generating QW states

$$|\psi\rangle_{qw} = U_k^t |l\rangle |s\rangle \quad (4)$$

used to encode the key, for the verification purposes Alice also creates a number of Bell-like maximally entangled states

$$|\psi\rangle_{qw} = \frac{1}{\sqrt{(\log 2P)!}} \sum_{i=0}^{2P-1} |i\rangle_a |i\rangle_{qw}. \quad (5)$$

between the ancilla systems (denoted by a) and the QW systems (denoted by qw), each of dimension $2P$ (the dimension of the actual QW). At the end of the first step, Alice sends to Bob a random sequence of QW states, each either in the form $|\psi\rangle_{qw}$, or $\rho_{qw} = \text{Tr}_a |\psi\rangle \langle \psi|_{qw}$, while keeping the ancillas with her. Alice also sends through a classical public authenticated channel a classical string $v = v_1 \dots v_n$, where $v_i = 0$ if the i -th system is going to be used for the encoding of the key, while $v_i = 1$ if the i -th system is going to be used for verification.

The proportion of states used to obtain the key and used for the verification can be chosen in a similar way as in the previous case. Usually, the dimension of the total Hilbert

space $2P$ is of the form 2^n which, in turn, is isomorphic to the Hilbert space resulting from the tensor product of n 2-dimensional Hilbert spaces, and thus this state can be written as the tensor product of n standard two-qubit $|\phi^+\rangle$ Bell states.

After Bob receives the systems, he and Alice perform Bell-like measurements on the states meant for the verification and they observe a maximal violation of the Bell's inequalities, since those states are maximally entangled. This way, these states are traced out and Bob is left with the states (4) in which he will encode the key (as previously).

The same procedure is repeated again, when Bob sends the encoded key to Alice. He will send a sequence of states, some of the form $(\hat{T}_r \otimes \hat{I}_c)U_k^t |l\rangle |s\rangle$, in which part of the key is encoded and some of the form (4) (with his ancillary system $|i\rangle_B$ maximally entangled to the system sent to Alice), which are going to be used for the verification, as explained above. In the end of the key decryption phase and if all the verifications were okay, Alice will concatenate the parts of the key to obtain the full key.

3.2 Efficiency and quantum memory requirements

In [19] it has been proven that the protocol is efficient, i.e., it requires only polynomial time (on the length of the message, say n) to transfer n bits of information encoded in $n + 1$ qubits. By introducing the verification steps in this QKD scheme we increase the complexity of the system to n^2 , in order to make the probability of eavesdropping negligible. However, we should notice that, out of this scheme, the size of the key that Alice and Bob share at the end is also increased to $n^2/3$, considering $m = n$. Therefore, the number of bits in the key is linear in the number of qubits sent to Bob. As a conclusion, our QKD scheme is efficient, since the complexity increased, but only polynomially.

As already mentioned in the Introduction, the lack of stable quantum memories is a major issue in quantum cryptography, since it is a practical constraint that is not likely to be solved, at least in the near future. Short-term quantum memories already exist, however it is not always straightforward to argue about the security of a protocol, relying on their existence. In our case, though, things are quite clear. If Eve does not interfere, Alice and Bob do not need quantum memories to execute the protocol, thus the key distribution is independent of such practical constraints. However, the presence of Eve and the need of verification for Alice and Bob introduce memory requirements for *all* the parties.

Below, we present the memory requirements for the case of Section 3.1.1, noting that the case of Section 3.1.2 is analogous. To conduct her attack, Eve needs a stable quantum memory, in order to keep the states she intercepted by Alice, while waiting for Bob to encrypt and send the key. Subsequently, she will encode it in Alice's states and send it to her. Also, in this scenario, Alice and Bob need a quantum memory, in order to perform the verification. They need to save the quantum states for some time, while waiting for the other party to send the classical information. Observe that Eve's memory should be more stable than Alice's and Bob's, as the time Eve needs to save the quantum states for, is clearly longer than the time that Alice and Bob need for the same purpose.

Hence, we conclude that our QKD scheme is secure, as long as Alice and Bob have at least as powerful equipment as the adversary Eve. Obviously, if the adversary is technologically

more advanced, then virtually any real-life implementation of a security protocol becomes potentially vulnerable.

4 One-way quantum walk key-distribution protocol

In this section we present a one-way QKD protocol based on QWs and we prove that it is secure. First, we state it in its prepare-and-measure form. The protocol procedure is depicted in Figure 2.

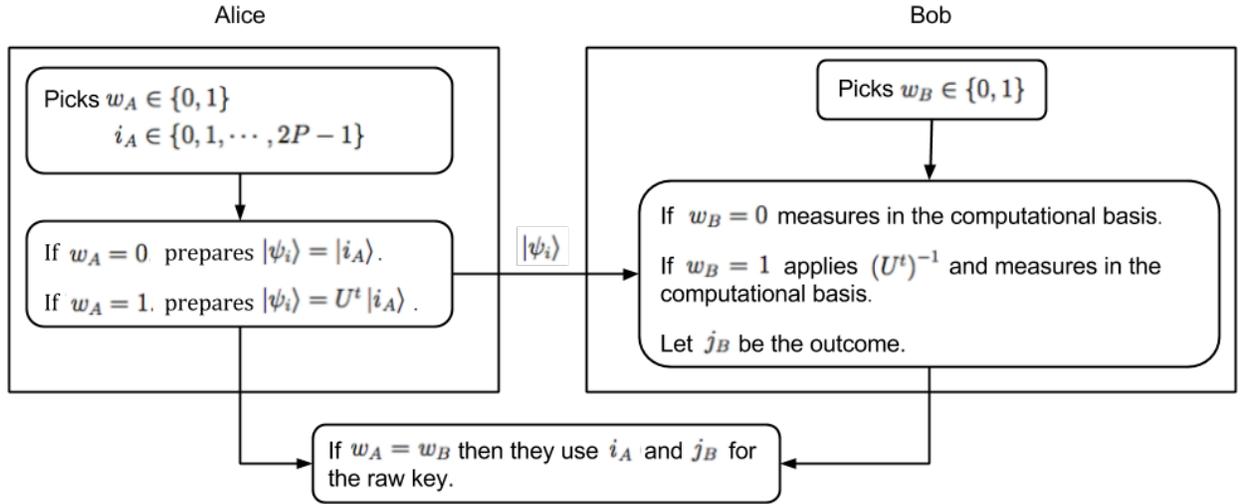


Figure 2: Description of the basic steps of Protocol 2.

Protocol 2. Let θ_k, t , and P be publicly known where P is the dimension of the position space of the QW, t is the number of steps to perform the QW, and θ_k the coin parameter (see Equation (1)). Let U_k be the QW operator $U_k = S \cdot (I_p \otimes R_c(\theta_k))$ that is also known by the parties (i.e., it is also publicly known) and let F be an operator acting only on \mathcal{H}_c . F 's action is to “flip” the coin to some initial state before evolving the walk and is optional (in which case $F = I_c$). Finally, let $|\psi_i\rangle = U_k^t(I_p \otimes F)|i\rangle$ for $|i\rangle \in \mathcal{H}_p \otimes \mathcal{H}_c$. We call the orthonormal basis $\{|\psi_i\rangle\}$ the QW basis and denote the computational basis by Z . This means that the QW basis is obtained from the computational basis Z , when performing the QW with respect to the initial state $|i\rangle$ or, in other words, the unitary operator that describes the basis change is the unitary of the QW.

The protocol consists of N iterations of the following steps:

1. Alice picks a random bit $w_A \in \{0, 1\}$ and a value $i_A \in \{0, 1, \dots, 2P - 1\}$.

- If $w_A = 0$: Alice will prepare and send to Bob the $2P$ -dimensional state $|\psi_i\rangle = |i_A\rangle$.
- If $w_A = 1$: Alice will prepare and send to Bob the $2P$ -dimensional state $|\psi_i\rangle = U_k^t(I_p \otimes F) |i_A\rangle$.

2. Bob picks a random bit $w_B \in \{0, 1\}$.

- If $w_B = 0$: Bob measures the received $2P$ dimensional state in the computational Z basis resulting in outcome j_B .
- If $w_B = 1$: Bob measures in the QW basis (alternatively, he inverts the QW by applying $(U_k^t)^{-1}$ and measures the resulting state in the Z basis). The result is translated, in the obvious way, into an integer j_B .

Note that he measures both the position and coin, as opposite to the previous protocol, where the measurement for the key was only on the positions space.

3. Alice and Bob reveal, via the authenticated classical channel, their choice of w_A and w_B . If $w_A = w_B$, they will use their values i_A and j_B to contribute towards their raw key. Otherwise, if $w_A \neq w_B$, they will discard this iteration.

After the above process, Alice and Bob will use a cut-and-choose technique similar to Yao's [24], to check eavesdropping by choosing a suitable subset of non-discarded iterations for parameter estimation in the usual manner (discarding those chosen iterations from the raw key). This allows them to estimate the disturbance Q_Z and Q_W in the Z and QW bases respectively (i.e., in the absence of noise $Q_Z = Q_W = 0$). If this disturbance is "sufficiently low" (to be discussed below) the users proceed with error correction and privacy amplification in the usual manner.

4.1 Security

In order to prove the security of Protocol 2, we will construct, in the usual way, an equivalent entanglement-based protocol [25, 26]. Proving security of this entanglement-based protocol will show the security of the prepare-and-measure version. This equivalence between entanglement-based and prepare-and-measure QKD protocols was first established by Bennett, Brassard and Mermin in [25]. Since then, the relationship between the presence of entanglement (and specifically the ability of the involved parties to certify or distil entanglement) and the security of prepare-and-measure QKD protocols has been developed and thoroughly investigated [27, 28]. In this context, a quite common technique, when it comes to proving security of prepare-and-measure QKD protocols (such as the ones we present in this work), is to consider an equivalent entanglement-based protocol and prove its security [25, 26]. We should stress that it can also hold even in the case that the devices are not trusted (device-independent QKD), given that some specific assumptions about the devices are made [29].

For this entanglement-based version, for each one of the N iterations, we make changes to steps (1) and (2), replacing them as follows:

New Step (1): Alice prepares the entangled state:

$$|\phi_0\rangle = \frac{1}{\sqrt{2P}} \sum_{i=0}^{2P-1} |i, i\rangle_{AB}$$

which lives in the $4P^2$ dimensional Hilbert space: $(\mathcal{H}_p \otimes \mathcal{H}_c)^{\otimes 2}$. She sends the second half (the Bob portion of $|\phi_0\rangle$) to Bob while keeping the first half (the Alice portion) in her private lab.

New Step (2): Alice and Bob choose independently two random bits w_A and w_B . If $w_A = 0$, Alice will measure her half of the entangled state in the computational Z basis; otherwise she will measure her half in the QW basis. Similarly for Bob and w_B . Let their measurement results in values be i_A on Alice's side and j_B on Bob's side.

We now show the security of this entanglement-based version of the protocol. In the following proof, we will initially make three assumptions:

- A1:** Alice and Bob only use those iterations where $w_A = w_B = 0$ for their raw key.
- A2:** Eve is restricted to collective attacks (those whereby she attacks each iteration of the protocol independently and identically, but is free to perform a joint measurement of her ancilla at any future time of her choosing).
- A3:** Eve is the party that actually prepares the states which Alice and Bob hold.

Assumption A1 is made only to simplify the computation and may be discarded later (alternatively, one may bias the basis choice so that w_A and w_B are chosen to be 0 with high probability, thus increasing the efficiency of the protocol as is done for instance for BB84 in [30]). Assumption A2 may be removed later using a de Finetti-type argument [31, 32, 33] (in this paper, we are only concerned with the asymptotic scenario, so the key-rate expression we derive will not be degraded). Note that removing A2 gives us the security. Assumption A3 gives greater advantage to the adversary; if we prove security using A3, then the “real-world” case, where assumption A3 is not used, will certainly be just as secure, if not even more.

In light of A2 and A3, Alice, Bob, and Eve, after N iterations of the protocol, hold a quantum state $\rho_{ABE}^{\otimes N}$, where $\rho_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ with $\mathcal{H}_A \equiv \mathcal{H}_B \equiv \mathcal{H}_p \otimes \mathcal{H}_c$. We should note that, since we consider Eve to be an all-powerful adversary, there are no restrictions on the specific form of her Hilbert space \mathcal{H}_E . Following error correction and privacy amplification, Alice and Bob will hold a secret key of size $\ell(N)$. Under the assumption of collective attacks (A2), we may use the Devetak-Winter key-rate expression [34] to compute:

$$r = \lim_{N \rightarrow \infty} \frac{\ell(N)}{N} = S(A|E) - H(A|B).$$

Let A_Z and A_W be the random variables describing Alice's system, when she measures in the Z or QW basis, respectively. Similarly, define B_Z and B_W . Under assumption A1, we are actually interested in the value:

$$r = S(A_Z|E) - H(A_Z|B_Z).$$

Computing $H(A_Z|B_Z)$ is trivial, given the observable probabilities:

$$p_{i,j}^Z = Pr(i_A = i \text{ and } j_B = j \mid w_A = w_B = 0). \quad (6)$$

The challenge is to determine a bound on the von Neumann entropy $S(A_Z|E)$.

To do so, we will use an uncertainty relation, proven in [35], which states that for any density operator σ_{ABE} acting on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$, if Alice and Bob make measurements using POVMs $\mathcal{M}_0 = \left\{ M_x^{(0)} \right\}_x$ or $\mathcal{M}_1 = \left\{ M_x^{(1)} \right\}_x$, then

$$S(A_0|E) + H(A_1|B) \geq \log \frac{1}{c}, \quad (7)$$

where

$$c = \max_{x,y} \left\| M_x^{(0)} M_y^{(1)} \right\|_{\infty}^2 \quad (8)$$

where we take $\| \cdot \|_{\infty}$ to be the operator norm and A_i to be the random variable describing Alice's system after measuring \mathcal{M}_i (we will later, similarly, define B_i). Assuming measurements \mathcal{M}_0 are used for key distillation, simple algebra, as discussed in [35], yields the Devetak-Winter key-rate:

$$\begin{aligned} r = S(A_0|E) - H(A_0|B_0) &\geq \log \frac{1}{c} - H(A_0|B_0) - H(A_1|B) \\ &\geq \log \frac{1}{c} - H(A_0|B_0) - H(A_1|B_1). \end{aligned}$$

The last inequality follows from the basic fact that measurements can only increase entropy.

In our case, we have $M_x^{(0)} = |x\rangle \langle x|$ and $M_x^{(1)} = |\psi_x\rangle \langle \psi_x|$ for $x \in \{0, 1, \dots, 2P-1\}$. Let $|\psi_x\rangle = \sum_{i=0}^{2P-1} \alpha_{x,i} |i\rangle$; then it is easy to see that for all x, y

$$\left\| M_x^{(0)} M_y^{(1)} \right\|_{\infty}^2 = |\alpha_{y,x}|^2,$$

and therefore

$$c = \max_{x,y} |\alpha_{x,y}|^2, \quad (9)$$

a quantity which depends exclusively on the choice of the QW parameters and not on the noise in the channel. Therefore, Alice and Bob should choose optimal t, θ_k and P in order to minimize c (thereby maximizing the key-rate equation).

As we show in the next section, this analysis is sufficient to derive good key-rate bounds.

4.2 Evaluation

As mentioned above, the value of c depends solely on the QW parameters which are under Alice and Bob’s control; therefore it is to their advantage to choose a QW which minimizes this value (i.e., such that, after evolving for t steps, the probability of finding the walker at any particular position is small). It is easy to see that, as $t \rightarrow \infty$, the values $|\alpha_{x,y}|$ do not converge to a steady state which is why, usually, one considers the time-averaged distribution when analyzing QWs on the cycle [36, 37]. However, in our QKD protocol, we do not care what happens at large t ; instead, we wish to find an optimal t and one that is preferably not “too large” (the larger it is, the longer, in general, it might take Alice to prepare the state and Bob to reverse it). Notice that, while in the previous two-way protocol the choice of large t increased the security of the protocol, here the role of t is different. Larger t does not mean that it is harder for Eve to distinguish. It’s just a parameter that Alice and Bob can tune to get optimal noise resistance, and in this context, small t (even $t = 1$ or 2) can lead to secure systems, as well. Different values of t correspond to different noise tolerances and our investigation is looking for optimal values of t where “optimal” means the highest theoretical noise tolerance for a *given* walk setting. If our system were to be implemented in practice, “optimal” would probably take a much different form and Alice and Bob would have to consider their device imperfections, etc. Such an investigation, though very interesting, is outside the scope of this paper, but it presents a relevant direction of future work.

We begin by looking at various walk parameters and finding the minimal value of c when $F = I_c$, the identity operator. Note that, on the circle, it makes sense only to consider odd P as even P would force the support of the probability amplitudes onto even or odd numbered nodes only thereby increasing the overall value of $|\alpha_{x,y}|$. We wrote a computer program to simulate the walk for time steps $t = 1, 2, \dots, T_{\max}$ (for user-specified value T_{\max}) searching for the optimal value of t (i.e., a value for t whereby c is minimum). For the evaluation we used a more general form of the coin rotation operator:

$$R_c(\theta, \phi) = \begin{pmatrix} e^{i\phi} \cos(\theta) & e^{i\phi} \sin(\theta) \\ -e^{-i\phi} \sin(\theta) & e^{-i\phi} \cos(\theta) \end{pmatrix},$$

The results for $\theta = \pi/4$, $\phi = 0$, and for various P are shown in Figure 3.

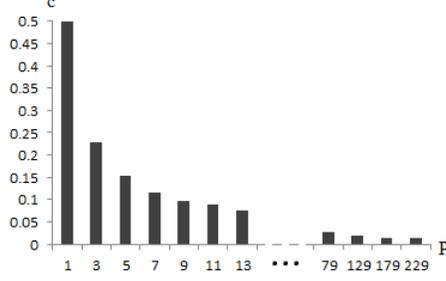


Figure 3: Showing minimal value of c found by our program for given position space dimension P when $\theta = \pi/4, \phi = 0$ and $F = I_c$. When $P \leq 13$ we set $T_{\max} = 5000$; when $P \geq 79$ we set $T_{\max} = 50000$. Note that, the smaller c is, the better for Alice and Bob. Note also that P is the dimension of the position space, *not* the number of qubits sent which would actually be $\lceil \log P \rceil + 1$ (where the extra “+1” is due to the coin).

Now that we can find the optimal choice of QW parameters for particular values of P and, more importantly for our work here, the resulting value of c . To this end, we have to compute our bound r and determine for what noise levels we can have $r > 0$. In practice, one would observe values $p_{i,j}^Z$ and $p_{i,j}^W$ (see Equation (6) and define $p_{i,j}^W$ analogously) and use these to directly compute $H(A_Z|B_Z)$ and $H(A_W|B_W)$ as required by the key-rate equation. For the purpose of illustration in this paper, however, we will evaluate our key-rate bound assuming a generalized Pauli channel as discussed in [38] (see, in particular, Section 7 of that source). This channel maps an input state ρ to an output state $\mathcal{E}(\rho)$ defined as:

$$\mathcal{E}(\rho) = \sum_{m=0}^{2P-1} \sum_{n=0}^{2P-1} p_{m,n} \mathcal{U}_{m,n} \rho \mathcal{U}_{m,n}^* \quad (10)$$

where

$$\mathcal{U}_{m,n} = \sum_{k=0}^{2P-1} e^{\pi i \cdot k \cdot n / P} |k+m\rangle \langle k|. \quad (11)$$

That is, this channel $\mathcal{E}(\cdot)$ models an adversary’s attack which induces phase and flip errors with probabilities denoted by $p_{m,n}$. In our numerical computations to follow, we will use:

$$p_{i,j} = \begin{cases} 1 - E_r & \text{if } i = j = 0 \\ \frac{E_r}{(2P)^2 - 1} & \text{otherwise} \end{cases} \quad (12)$$

It is clear that $\sum_{i,j} p_{i,j} = 1$. Furthermore, when $E_r = 0$, we have $\sum_i p_{i,i}^Z = \sum_i p_{i,i}^W = 1$ (i.e., there is no disturbance in the channel) while as E_r increases, the disturbance also increases.

Finally, we define the total noise in the channel to be:

$$Q = \sum_{a \neq b} p_{a,b}^Z = \sum_{a \neq b} Pr(A_Z = a \text{ and } B_Z = b \mid w_A = w_B = 0).$$

That is to say, Q represents the quantum error rate (QER) of the channel.

The maximally tolerated QER, for those QWs analyzed in Figure 3, and using the above described noise model, is shown in Figure 4. Note that, when $P = 1$ and $t = 1$, we recover the BB84 limit of 11% which is to be expected since, with these choice of parameters, we are essentially running the BB84 protocol.

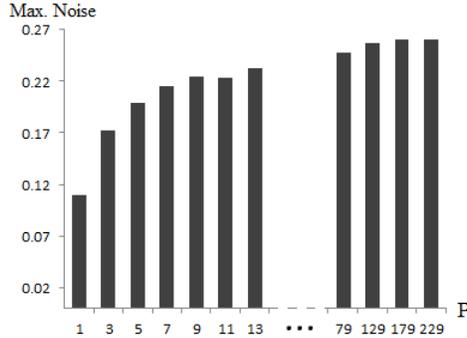


Figure 4: Showing the maximally tolerated noise level for our protocol using parameters found in Figure 3 and using the quantum channel described by Equations (10) and (12). The lack of increase in noise tolerance from $P = 9$ to $P = 11$ (while other choices caused an increase) indicates that T_{\max} was too low. Note that, when $P = 1$, we recover the BB84 tolerance of $Q = 0.11$ as expected. Also note that, when $P = 229$, the maximal tolerated noise is $Q = 0.261$.

Observe in Figure 4 that there is a lack of increase when $P = 9$ and $P = 11$; this indicates that our choice of $T_{\max} = 5000$ was too low. Running our simulator again with $T_{\max} = 50000$ for these small P values yields a maximally tolerated noise level shown in Figure 5.

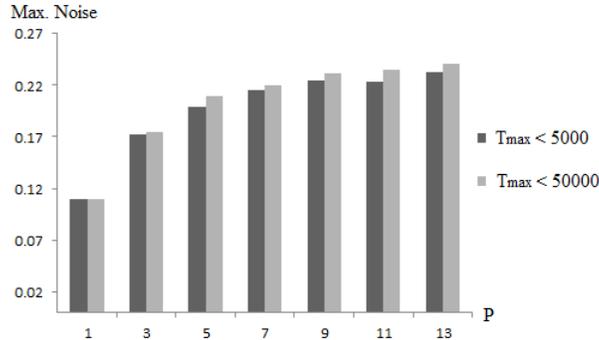


Figure 5: Comparing the maximally tolerated noise when t is allowed to be as large as 50000 (light gray) or only 5000 (dark gray); again when $F = I$ and $\phi = 0$. In this case, when $P = 13$ and $T_{\max} = 50000$, the maximal tolerated noise Q is $Q = 0.241$.

Finally, we re-run the simulator, using $T_{\max} = 5000$ and $T_{\max} = 50000$ for a different QW parameter of $\theta = \sqrt{2}\pi/4$ which, for these particular upper-bounds on t yield a higher

tolerated noise as shown in Figures 6 and 7. We comment that, if T_{\max} were larger, the two QWs may produce a QKD protocol with the same tolerated noise; however for these “smaller” bounds on t the QW with parameter $\theta = \sqrt{2}\pi/4$ produces a more secure protocol than when $\theta = \pi/4$. Since smaller t implies a more efficient protocol, this is an advantage. This opens two very interesting questions: first, do these QWs produce equivalent noise tolerances as $T_{\max} \rightarrow \infty$? Second, what other values of θ produce even more secure QKD protocols for small T_{\max} ? We comment that we also ran this numerical experiment for $\theta = \pi/5$ and $\theta = \pi/3$ but got worse noise tolerances.

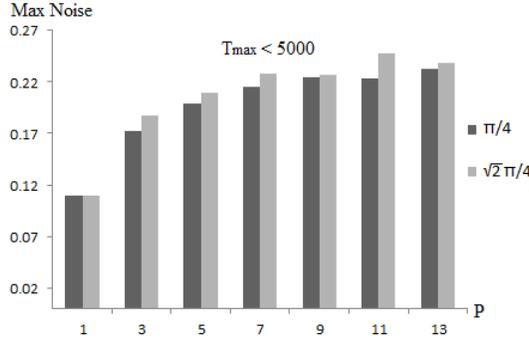


Figure 6: Comparing the maximal tolerated noise levels of the QKD protocol when $\theta = \pi/4$ (dark gray) and $\theta = \sqrt{2}\pi/4$ (light gray). In this chart, $T_{\max} = 5000$ which, observing the “drop” in tolerated noise when P goes from 11 to 13, is too small. See also Figure 7 for the same chart when $T_{\max} = 50000$.

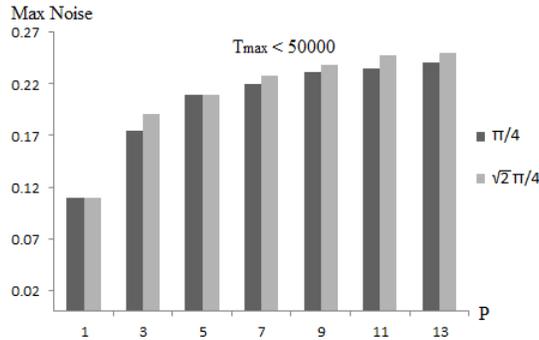


Figure 7: Comparing the maximal tolerated noise levels of the QKD protocol when $\theta = \pi/4$ (dark gray) and $\theta = \sqrt{2}\pi/4$ (light gray). In this chart, $T_{\max} = 50000$. In all cases, the QW parameter $\theta = \sqrt{2}\pi/4$ produces a more secure QKD protocol for this upper-bound on t . Note that, as $T_{\max} \rightarrow \infty$, they may produce equally secure protocols; this, as discussed in the text, is an open question. In this case, when $P = 13$ and $\theta = \sqrt{2}\pi/4$, the maximally tolerated noise is 0.25 (compared to 0.241 when $\theta = \pi/4$).

From the above it is clear that careful choice of the QW parameters is vital for producing a QKD protocol tolerant of high noise channels. To investigate this further, we simulate the

QW for all $\theta, \phi \in \{k\pi/10 \mid k = 0, 1, \dots, 10\}$. Furthermore, for each setting, we also consider the use of $F = I$, $F = X$, and $F = Y$, where:

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad Y = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}.$$

For each setting, we find the optimal choice of time $t \leq 5000$ which produces a minimal c . We then take this value and determine the highest disturbance the resulting protocol can withstand. The respective data is summarized in Table 1.

P	$F = I$					$F = X$					$F = Y$				
	θ	ϕ	t	c	Q_{\max}	θ	ϕ	t	c	Q_{\max}	θ	ϕ	t	c	Q_{\max}
3	0.4π	0.2π	4584	0.171	0.220	0.8π	0.8π	3994	0.181	0.211	0.7π	0	1502	0.167	0.225
5	0.7π	π	4340	0.147	0.205	0.9π	0.5π	3870	0.132	0.22	0.3π	0	3748	0.106	0.253
7	0.6π	0.9π	3946	0.088	0.252	0.7π	0.8π	3391	0.099	0.236	0.3π	0.5π	1275	0.083	0.261
9	0.6π	0.6π	1269	0.077	0.252	0.9π	0.7π	3041	0.079	0.250	0.3π	0.5π	965	0.069	0.267
11	0.6π	0.4π	1221	0.069	0.252	0.8π	0.4π	481	0.0724	0.245	0.7π	0.5π	277	0.054	0.284

Table 1: Showing the optimal choice of QW parameters to maximize the noise tolerance (Q_{\max}) of the resulting protocol. For this data, we searched for QWs with at most $T_{\max} = 5000$ steps and with parameters $\theta, \phi \in \{k\pi/10 \mid k = 0, 1, \dots, 10\}$.

Note that, for some data points (e.g., when $P = 5$ and $F = I$) there is a drop in the maximum tolerated noise. This is a consequence either of setting T_{\max} too small, or we need to simulate more QW parameters (as is done in Table 2). For example, when we set $T_{\max} = 50000$, for $P = 5$ and $F = I$, we get a maximum noise tolerance of 0.236 when $t = 40847$. Note also, that setting $F = Y$ achieves the best result for this test, $Q_{\max} = 0.284$.

In Table 2, we carried out the same experiment, however this time searching over QW parameters in the set $\theta, \phi \in \{k\pi/20 \mid k = 0, 1, \dots, 20\}$. Again, the best result for this case is $Q_{\max} = 0.284$ and is achieved when considering $F = Y$.

As mentioned at the beginning of this Section, all the numerical results were obtained by simulating the evolution of the QW on a custom QW simulator that we wrote. However, we also verified the results through an alternative technique, namely by computing the probability amplitudes of the QW using the standard Fourier method (see, e.g. [39, 40]) of analyzing QWs. The results obtained by both methods agree with each other.

We would also like to stress that, while the use of high-dimensional walks is “ideal” from a noise-tolerance perspective, this is not required – indeed, even with very small dimensions our protocol can tolerate the same level of noise as BB84. In particular, notice in Figure 4,

P	$F = I$					$F = X$					$F = Y$				
	θ	ϕ	t	c	Q_{\max}	θ	ϕ	t	c	Q_{\max}	θ	ϕ	t	c	Q_{\max}
3	0.4π	0.2π	4584	0.171	0.220	0.25π	0.15π	2402	0.173	0.218	0.7π	0	1502	0.167	0.225
5	0.6π	0.85π	3258	0.116	0.239	0.8π	0.25π	4659	0.124	0.229	0.3π	0	3748	0.106	0.253
7	0.6π	0.9π	3946	0.088	0.252	0.05π	0.95π	3739	0.091	0.248	0.35π	0.5π	517	0.081	0.265
9	0.45π	0.95π	2531	0.075	0.257	0.85π	0.05π	1669	0.078	0.251	0.45π	0.5π	1240	0.064	0.276
11	0.55π	0.75π	1826	0.059	0.272	0.25π	0.25π	2223	0.069	0.252	0.7π	0.5π	277	0.054	0.284

Table 2: Showing the optimal choice of QW parameters to maximize the noise tolerance (Q_{\max}) of the resulting protocol. For this data, we searched for QWs with at most $T_{\max} = 5000$ steps and with parameters $\theta, \phi \in \{k\pi/20 \mid k = 0, 1, \dots, 20\}$.

that already for the minimum $P = 1$ we obtain the BB84 noise tolerance, which increases further for relatively small dimensions $P = 3, P = 5$ and so on. We also simulated higher dimensions to investigate the theoretical properties of our systems for different walks. However, such high dimensions are not required to get a robust protocol. Therefore, while the practical implementation of a high-dimensional protocol might be quite complex, our protocol is robust even for relatively small dimensions, thus the experimental challenges in a potential practical implementation could be reduced. Moreover, we should emphasise that recently there has been a remarkable progress in the experimental generation and manipulation of high-dimensional entangled states. In particular, in [41, 42, 43, 44, 45] the experimental generation of bipartite high-dimensional entangled states has been demonstrated, while in [46, 47, 48, 49] there have been proposed experimental techniques for performing measurements in such states. Furthermore, the generation of multi-partite high-dimensional entangled states has been reported [50, 51, 52], as well as the generation of big arrays of such states [53].

Finally, we note that the protocol’s security is not compromised by considering the existence or not of quantum memories. It is sufficient to consider the prepare-and-measure form of the protocol. Eve needs a quantum memory to perform her attack, as she needs to save her ancillary system throughout the execution of the protocol. In the contrary, the secure key distribution between Alice and Bob does not require any quantum memory. Therefore, if Eve does not have a quantum memory she cannot attack, while if even she has one and attacks, Alice and Bob can defend against it and securely share a key at the end. Notice, that even if we consider the entanglement-based version of the protocol, again the security is independent of any quantum memory requirements, as Eve for her attack needs a more stable quantum memory than Alice and Bob need to defend against it and securely distill the key.

5 Semi-Quantum Key-Distribution Scheme

In this section we will present a SQKD protocol based on QWs. Semi-quantum protocols can be seen as practical instances of QKD, since they involve less quantum hardware, as one of the parties is completely classical. Also, they are interesting from a theoretical point of view, as they can be treated as a measure of the “quantumness” needed for a protocol to

surpass the security of its classical counterparts. It is assumed that one of the parties, e.g. Alice, is fully quantum, i.e., possesses quantum equipment, while the other party, e.g. Bob, is restricted to classical operations only, and for that reason is usually called the *classical party*.

Semi-quantum protocols rely on a two-way quantum channel allowing a quantum state to travel from Alice to Bob, then back to Alice. When first introduced by Boyer *et al.* in [22], these classical operations involved Bob either measuring the incoming qubit in the $Z = \{|0\rangle, |1\rangle\}$ basis, or reflecting the incoming qubit, bouncing it back to Alice undisturbed. For our purposes, we extend this definition of “classical” operations to operate with higher dimensional systems. As we do not want to restrict ourselves necessarily to qubit encodings (and thus, dimensions that are powers of two), we will say that Bob, on receipt of an D dimensional quantum state $|\psi\rangle$, may choose to do one of two operations:

1. Measure and Resend: Bob may subject the D -dimensional quantum state to a measurement in the computational basis spanned by states: $\{|0\rangle, |1\rangle, \dots, |D-1\rangle\}$. He will then prepare a new D -dimensional quantum state in this same computational basis based on the result of his measurement. Namely, if he observes $|r\rangle$ for $r \in \{0, 1, \dots, D-1\}$, he will send to Alice the quantum state $|r\rangle$.
2. Reflect: Bob may ignore the incoming D -dimensional quantum state and reflect it back to Alice. In this case he learns nothing about its state.

With these restrictions on the part of the classical user defined, we now depict and describe our protocol:

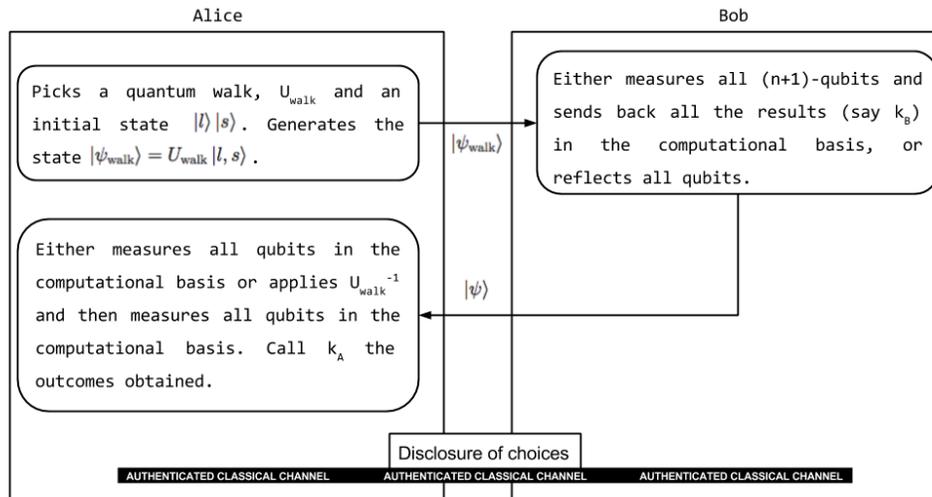


Figure 8: Description of the basic steps of Protocol 3.

Protocol 3. Semi-quantum key-distribution scheme

Inputs for the protocol

- $|l, s\rangle$, the initial state of the QW, where $l \in \mathcal{L} = \{0, \dots, P-1\}$ is the initial position of the walker, and $s \in \mathcal{S} = \{R, L\}$ gives the initial coin state.
- $U_{\text{walk}} = (U_k)^t \in \mathcal{Q}$, the evolution of the QW, where $k \in \mathcal{K} = \{1, 2, \dots, K\}$ is the choice of a single step unitary U_k , and $t \in \mathcal{T} = \{T_0, \dots, T_{\text{max}}\}$ is the number of steps of the QW. Thus, \mathcal{Q} is the set of all possible QWs. Note that \mathcal{Q} is publicly known.

Quantum state Generation

- Alice chooses uniformly at random $l \in \mathcal{L} = \{0, 1, \dots, P-1\}$ and $s \in \mathcal{S} = \{R, L\}$. She also chooses a random QW operator $U_{\text{walk}} \in \mathcal{Q}$ according to a publicly known distribution (e.g., uniform). She then prepares the following state:

$$|\psi_{\text{walk}}\rangle = U_{\text{walk}} |l, s\rangle.$$

- Alice sends this state to Bob.

Classical operations by Bob

Bob chooses either to measure-and-resend the quantum state in the computational basis $\{|0\rangle, |1\rangle, \dots, |2P-1\rangle\}$ (note that, in this protocol as well, he measures both the position and coin in order to obtain the key, thus his measurement, and subsequent preparation, is of dimension $2P$); or he will reflect the quantum state back to Alice.

Alice's final step

Alice chooses one of the following two options:

- She measures the returning quantum state in the computational basis and saves the result as κ_A .
- She first applies the inverse QW, U_{walk}^{-1} , and then measures in the computational basis. Note that, in the absence of noise, if Bob reflects, her measurement outcome should be $|l, s\rangle$.

Disclosure

Alice discloses her choice of operation and Bob discloses his choice either to measure and resend or reflect.

Iterations

The above process is repeated N times.

Results

- Every time Bob measures and resends and Alice measures in the computational basis, the parties add $1 + \log P$ bits to their final raw key. After N iterations, the raw key will consist of $N(1 + \log P)/4$ bits, on average. Considering that Alice and Bob choose independently, uniformly and at random their actions at each iteration, then – on average – $N/4$ iterations will contribute to the raw key.
- Every time Bob reflects and Alice measures after applying the inverse QW, the outcome of her measurement (l_m, s_m) should be what she initially used to generate the QW state (i.e., it should be that $l = l_m$ and $s = s_m$). These iterations, together with some randomly chosen iterations of the first type (where Bob measures and resends), are used for error detection.
- The other iterations are discarded.

5.1 Proof of robustness

As with the first protocol we proposed in this paper, the reliance on a two-way quantum channel greatly complicates the security analysis. It was only recently that several SQKD protocols were proven secure [54, 55, 56, 57]. However, the proof techniques developed in those works assumed qubit-level systems. In our case, not only must we contend with a two-way channel, but also with the fact that the quantum states traveling between Alice and Bob are of dimensions higher than 2. This leads to significant challenges in any security analysis.

Therefore, to analyze the security of this protocol, we will prove that it is *robust* as defined in [22, 23]. That is, for any attack which Eve may perform which causes her to gain information on the raw key, this attack must necessarily lead to a disturbance in the channel which can be detected with non-zero probability by Alice and Bob. Typically proving robustness is a first-step in the security analysis of semi-quantum cryptographic protocols.

Theorem 1. If $I \in \mathcal{Q}$ (where I is the identity operator on the joint $2P$ dimensional system) and if, for every $(l, s), (l', s') \in \{0, 1, \dots, P-1\} \times \{R, L\}$ there exists a $U_{\text{walk}} \in \mathcal{Q}$ and initial state $|l_0, s_0\rangle$ (all possibly depending on the choice of (l, s) and (l', s')) such that $\langle l, s | U_{\text{walk}} | l_0, s_0 \rangle \neq 0$ and $\langle l', s' | U_{\text{walk}} | l_0, s_0 \rangle \neq 0$, then the SQKD protocol based on QWs is robust.

Proof. We will assume, similarly to [58, 59], that Alice sends each (in our case $2P$ -dimensional) quantum state, only after she receives one from Bob (excepting, of course, the first iteration). In this case, Eve's most general attack consists of a collection of unitary operators $\left\{ (U_F^{(i)}, U_R^{(i)}) \right\}_{i=1}^N$ where, on iteration i of the protocol, she applies $U_F^{(i)}$ in the forward channel

(as the quantum state travels from Alice to Bob) and $U_R^{(i)}$ in the reverse channel. These operators act on the $2P$ -dimensional quantum state and Eve's private quantum memory. We make no assumptions about how these operators are chosen – for instance, Eve may choose them “on the fly”; that is, she may choose operator $U_F^{(2)}$ after attacking with $U_F^{(1)}$.

Consider the first iteration $i = 1$. We assume, without loss of generality, that Eve's quantum memory is cleared to some pure “zero” state, denoted by $|\chi\rangle$, known to her.

In the remainder of this proof, we will treat the position space and the coin space as a single space Σ of dimension $2P$.

We may describe the action of $U_F^{(1)}$ on basis states as follows

$$U_F^{(1)} |i, \chi\rangle = \sum_{j=0}^{2P-1} |j, e_i^j\rangle,$$

where $|e_i^j\rangle$ are arbitrary states in Eve's ancillary system. These states are not necessarily normalized nor orthogonal; the unitarity of $U_F^{(1)}$ imposes some restrictions on them which we will use later.

With non-zero probability, this iteration may be used for error detection. It is also possible that Alice chose to use $I \in \mathcal{Q}$ in this iteration and, thus, she sends the quantum state $|\sigma\rangle$ to Bob, for $\sigma \in \Sigma$. Furthermore, Bob chooses to measure and resend with non-zero probability. Therefore, to avoid detection, it must be that $|e_i^j\rangle \equiv 0$ for all $i \neq j$, and the unitarity of $U_F^{(1)}$ yields $\langle e_i^i | e_i^i \rangle = 1$ for all i . Thus:

$$U_F^{(1)} |i, \chi\rangle = |i, e_i^i\rangle, \forall i = 0, 1, \dots, 2P - 1.$$

Now, consider $U_R^{(1)}$, the attack applied in the reverse channel. We may write its action as follows:

$$U_R^{(1)} |i, e_i^i\rangle = \sum_{w=0}^{2P-1} |w, e_{i,i}^w\rangle.$$

The same argument as before applies: in particular, with non-zero probability Alice and Bob will use this iteration to check for errors, and so it must be that $|e_{i,i}^w\rangle \equiv 0$ for $i \neq w$. Thus

$$U_R^{(1)} |i, e_i^i\rangle = |i, e_{i,i}^i\rangle = |i, f_i\rangle, \forall i = 0, 1, \dots, 2P - 1,$$

where we defined $|f_i\rangle \equiv |e_{i,i}^i\rangle$ for ease of notation.

Now, assume that Alice chooses a QW operator $U_{\text{walk}} \in \mathcal{Q}$, with $U_{\text{walk}} \neq I$. Let $|\sigma\rangle$ be the initial state she prepares (σ chosen at random from Σ). In this case, the quantum state she sends to Bob may be written as:

$$U_{\text{walk}} |\sigma\rangle = |\psi_\sigma\rangle = \sum_{i=0}^{2P-1} \alpha_i |i\rangle.$$

Assume that U_{walk} is chosen so that at least two of the α_i 's are non-zero (such QWs exist by hypothesis). If Bob reflects, the qubit state arriving at Alice's lab, after Eve's attack on both channels, is

$$U_R^{(1)}U_F^{(1)}(U_{\text{walk}} \otimes I_E) |\sigma, \chi\rangle = \sum_i \alpha_i |i, f_i\rangle, \quad (13)$$

where I_E is the identity operator on Eve's ancilla.

Alice will subsequently apply the inverse QW operator and measure the resulting state, expecting to find $|\sigma\rangle$. This is equivalent to her measuring in the QW basis $\{|\psi_0\rangle, |\psi_1\rangle, \dots, |\psi_{2P-1}\rangle\}$, where $|\psi_i\rangle = U_{\text{walk}} |i\rangle$, and expecting to observe $|\psi_\sigma\rangle$. In this QW basis, we clearly have

$$|i\rangle = \sum_{j=0}^{2P-1} \langle\psi_j|i\rangle |\psi_j\rangle,$$

from which, we may write Equation (13) as:

$$\sum_{i=0}^{2P-1} \alpha_i \left(\sum_{j=0}^{2P-1} \langle\psi_j|i\rangle |\psi_j\rangle \right) \otimes |f_i\rangle \quad (14)$$

$$(15)$$

$$= \sum_{j=0}^{2P-1} |\psi_j\rangle \otimes \left(\sum_{i=0}^{2P-1} \alpha_i \langle\psi_j|i\rangle |f_i\rangle \right). \quad (16)$$

Let p be the probability that this iteration does not result in an error – i.e., the probability that Alice measures $|\psi_\sigma\rangle$. From the above equation:

$$p = \left| \sum_{i=0}^{2P-1} \alpha_i \langle\psi_\sigma|i\rangle |f_i\rangle \right|^2.$$

Noticing that $\langle\psi_\sigma|i\rangle = \alpha_i^*$ (since $|\psi_\sigma\rangle = \sum_i \alpha_i |i\rangle$), and also $\langle f_i|f_i\rangle = 1$ (due to the unitarity of $U_R^{(1)}$), we find:

$$p = \left| \sum_i |\alpha_i|^2 |f_i\rangle \right|^2 = \sum_i |\alpha_i|^4 + 2 \sum_{i>j\geq 0} |\alpha_i|^2 |\alpha_j|^2 \text{Re}(\langle f_i|f_j\rangle).$$

When $|f_i\rangle \equiv |f_j\rangle = |F\rangle$, for all i, j , the above quantity attains its maximum of $p = 1$. In this case, after Eve's attack, the system described by Equation (13) is $\sum_i \alpha_i |i\rangle \otimes |F\rangle = |\psi_\sigma\rangle \otimes |F\rangle$. Due to the Cauchy-Schwarz inequality $\text{Re}(\langle f_i|f_j\rangle) \leq 1$. If, however, one or more of the $\text{Re}(\langle f_i|f_j\rangle) < 1$ for any of the $(|f_i\rangle, |f_j\rangle)$ pairs which appear in the expression above (i.e., for those where α_i and α_j are non-zero), it is obvious that $p < 1$ and so Eve would be detected.

Therefore, to avoid detection, it must be that $\text{Re}(\langle f_i | f_j \rangle) = 1$ for all i, j where α_i and α_j are non-zero, implying $|f_i\rangle \equiv |f_j\rangle$. Indeed, if we write $|f_j\rangle = x|f_i\rangle + y|\zeta\rangle$, where $\langle f_i | \zeta \rangle = 0$, then $\text{Re}(\langle f_i | f_j \rangle) = 1 = \text{Re}(x)$. Of course $|x|^2 + |y|^2 = 1$ (since $\langle f_j | f_j \rangle = 1$) and so:

$$|x|^2 + |y|^2 = 1 \Rightarrow \text{Re}^2 x + \text{Im}^2 x + |y|^2 = 1 \Rightarrow \text{Im}^2 x + |y|^2 = 0.$$

This implies both $\text{Im}(x) = 0$ and $y = 0$. Since $\text{Re}(x) = 1$, we conclude $x = 1$ and so $|f_i\rangle = |f_j\rangle$.

Since Alice could have chosen any QW in \mathcal{Q} , all possible (i, j) pairs are covered (i.e., at least one QW in \mathcal{Q} is guaranteed to produce a state where α_i and α_j are non-zero) and since Eve does not know which QW was chosen, it must be that $|f_i\rangle \equiv |f_j\rangle \equiv |F\rangle$ for all i, j .

Thus, after the first iteration, to avoid detection, it must be that the state of Eve's quantum memory is in the state $|F\rangle$, independently of Alice's and Bob's raw key and operations. Thus, Eve is not able to extract any information during the first iteration. Furthermore, since she is fully aware of the state of her quantum memory in this case (i.e., she knows the state $|F\rangle$), the above arguments may be repeated inductively for the remaining iterations of the protocol, leading to the conclusion that the protocol is robust. \square

The above proof of robustness placed certain requirements on the set of QW \mathcal{Q} , but can such a set even exist? We show that, at least for all odd P , such a set may be easily constructed.

Lemma 1. If P is odd, then there exists a set of QWs \mathcal{Q} which satisfy the requirements of Theorem 1.

Proof. Let $(l, s), (l', s') \in \{0, 1, \dots, P-1\} \times \{R, L\}$. We construct a QW $U_{l,s,l',s'}$ and an initial state $|l_0, s_0\rangle$ such that $\langle l, s | U_{l,s,l',s'} | l_0, s_0 \rangle \neq 0$ and $\langle l', s' | U_{l,s,l',s'} | l_0, s_0 \rangle \neq 0$.

Since P is odd, there exists a position index $q \in \{0, 1, \dots, P-1\}$ and a value $q_0 \in \mathbb{Z}$ such that $|q_0| < P$, $q - q_0 \equiv l \pmod{P}$, and $q + q_0 \equiv l' \pmod{P}$. We assume that $q_0 \geq 0$; if $q_0 < 0$ the result is symmetric by simply "flipping" l with l' (in which case q_0 becomes non-negative).

The shift operator S for our QW is simply the usual

$$S = \sum_{i=0}^{P-1} |i-1\rangle \langle i| \otimes |R\rangle \langle R| + \sum_{i=0}^{P-1} |i+1\rangle \langle i| \otimes |L\rangle \langle L|,$$

where all arithmetic, of course, is done modulo P . Our coin operator will simply be the Hadamard coin:

$$R_c = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

We claim the desired operator is $U_{l,s,l',s'} = [(I_p \otimes R_c) \cdot S]^{t+1}$. (Note that the shift operator is applied before the coin in this case to simplify the construction) Now, consider the initial state $|q+1, R\rangle$. After the first step of the QW (i.e., after applying $(I_p \otimes R_c) \cdot S$), the QW evolves to the state $\frac{1}{\sqrt{2}} |q\rangle (|R\rangle + |L\rangle)$. It is not difficult to see that, after t additional steps

with this QW, *but before the final application of $I_p \otimes R_c$ on the $(t+1)$ -th step*, the quantum state evolves to:

$$\alpha |l, R\rangle + \beta |l', L\rangle + |\phi\rangle,$$

where $|\alpha| \neq 0$, $|\beta| \neq 0$, and $|\phi\rangle$ is a non-normalized state orthogonal to both $|l, R\rangle$ and $|l', L\rangle$. Finally, after the last $I_p \otimes R_c$, the state becomes

$$U_{l,s,l',s'} |q+1, R\rangle = \frac{1}{\sqrt{2}}(\alpha |l, R\rangle + \alpha |l, L\rangle + \beta |l', R\rangle - \beta |l', L\rangle) + |\phi'\rangle,$$

with $|\phi'\rangle$ being a state orthogonal to $|l, R\rangle$, $|l, L\rangle$, $|l', R\rangle$, and $|l', L\rangle$, thus yielding the desired state. Taking $\mathcal{Q} = \bigcup_{l,s,l',s'} \{U_{l,s,l',s'}\} \cup \{I\}$ proves the result. \square

Finally, we should notice that the robustness of this SQKD protocol is independent of the existence or absence of quantum memories. In fact, Eve's attack requires a stable quantum memory, in which she keeps her ancillary system during the execution of the protocol. On the other hand, Alice does not need any quantum memory in order to share the key with Bob at the end, and Bob is, of course, restricted to classical operations. Therefore, without a quantum memory Eve cannot even conduct the attack, whereas even if she has access to a quantum memory, she is not able to extract any useful information about the key without being detected by Alice and Bob.

6 Practical attacks

While our paper presents theoretical cryptographic proposals, and a detailed analysis of practical attacks is out of its scope, it is worthy presenting a short discussion of possible attacks and countermeasures for the case of optical implementations. The term practical attacks refers to attacks during which Eve is taking advantage of possible loopholes in the implementation of the protocols, i.e., the fact that the setups used for the implementation of the protocols are not perfect, can seriously compromise the security of the key. Such attacks have been thoroughly investigated in the literature and several countermeasures have been proposed in different setups and scenarios. For an overview of the recent progress and current status of this area of QKD, see the following detailed reviews [60, 61, 62, 63, 64].

One of the most studied of such attacks is the photon number splitting attack (PNS), which is based on the fact that there are no perfect single-photon sources [65, 66, 67]. Instead, the current sources emit in general multi-photon pulses, whose photon number statistics are described by a Poisson distribution. Eve, who is considered all powerful and bounded only by the laws of physics, can thus, by placing herself in front of Alice, detect genuine multi-photon pulses, extract one photon from each, and send the rest to Bob through a lossless channel, while blocking single-photon pulses. Due to the fact that the quantum channel connecting Alice and Bob has losses exponential in the channel length, there exists a maximal distance, known to Eve, below which Bob is not able to spot Eve's interference. By storing the

extracted photons in her quantum memory, Eve can measure them in the correct basis upon the classical communication between Alice and Bob, during which they publicly reveal their choices of preparation/measurement bases. Since all the photons of the same pulse are in the same state, Eve thus has the key shared by Alice and Bob.

The standard technique used to defend against a PNS attack is by introducing the so-called decoy states [68]. In addition to the signal states, from which the key is obtained, Alice sends coherent states $|e^{i\theta}|\alpha|\rangle$, with phase θ chosen uniformly at random, and the variable intensity $I \propto |\alpha|$. Note that such decoy pulses are to Eve indistinguishable from the signal ones. Thus, Alice and Bob can subsequently detect Eve's interference (extracting single photons from multi-photon pulses) by comparing the yields of signal and decoy states (given the channel loss ℓ , the yield y is defined as $y = 1 - \ell$ [68]). For more details, see [69], as well as subsequent improvements and modifications [70, 71, 72, 73, 74, 75, 76]. This method, developed for standard one-way QKD schemes, can be straightforwardly applied to our second proposal, which is a one-way protocol as well. It can also be applied to our first and third two-way proposals. Indeed, in our first proposal, as Bob does not perform any measurement, it is Alice who performs the yield estimation upon receiving back the pulses. The same can be done by Alice alone for the photons reflected by Bob in our third proposal, in which in addition the yield check could be done for the pulses measured by Bob. As mentioned above, the details of the techniques depend on particular implementations and are beyond the scope of our theoretical study.

While the PNS attack is applicable to most of the protocols that use imperfect photon sources, the above description of its particular implementation is given on the example of a standard QKD *one-way* scheme. Thus, it has to be re-examined when applied to different protocols. The crucial feature of the standard QKD protocol is the exchange of classical information between Alice and Bob, which allows Eve to extract the key exchanged. Therefore, since such exchange is present in our second and third protocol, the above described PNS attack is applicable to those protocols as well. Note though that in the case of the third, *two-way* protocol, Eve can possibly extract information only upon intercepting the pulses re-sent from Bob to Alice. Indeed, in the third protocol the key is obtained from the cases in which Bob and, upon receiving them back, Alice too, perform measurements in the computational basis, thus sharing the same set of bits. Extracting photons from the pulse before it came to Bob, and consequently before his measurement, gives Eve no information about the key.

Nevertheless, our first, *two-way* QKD protocol, is considerably different from the standard QKD ones, as Alice and Bob reveal *no classical information* regarding their quantum operations (they only exchange information regarding the cases used for verification procedure, which do not contribute to the key generation). Thus, Eve's task is more difficult than in the case of standard QKD protocols. What Eve can do is to extract *two* photons from each pulse, one on the way from Alice to Bob, and another on the way back to Alice, and compare their states, $|\psi\rangle$ and $|\psi(r)\rangle$, in the attempt to learn the key r . Note that, even in the noiseless scenario, the described comparison does not have perfect efficiency, unlike the standard application of the PNS attack in which Eve learns the key with certainty. More-

over, in the case of our protocol, Eve can attack only three or more photon pulses, thus decreasing the efficiency of her attack with respect to the standard one, which makes use of more probable two-photon pulses as well. For example, for the commonly used order of the mean photons per pulse, $\mu = 0.2$, the probability for emitting three or more photons is $p(n \geq 3) \approx 0.001$, while the probability to emit exactly two photons (the “deficit” with respect to the standard PNS attack) is of the order of magnitude higher, $p(n = 2) \approx 0.016$, where n is the number of photons per pulse emitted.

Finally, we would like to note that, although in practical attacks Eve is assumed to be all powerful, exceeding the current technological equipment used by everyday users, not all practical attacks are based on the same level of subtle equipment. In the case of the PNS attack, Eve should be able to perform photon non-demolition number measurements, a task beyond any current and (at least mid-term) foreseeable technology.

Nevertheless, there exist other practical protocols that do not require such sophisticated technology. Below, we briefly analyse three such kinds of attacks, extensively studied in the literature: the Trojan horse, the detector blinding and the time-shift attacks.

The Trojan horse attack is one of the first attacks ever considered and since then it has been thoroughly investigated and continuously developed in different contexts. In a nutshell, Trojan horse attacks benefits from the imperfections in the quantum channel between Alice and Bob that allows for Eve’s interference by modulating Alice’s pulses, sending them to Bob and analysing the reflected/backscattered signal [77, 78, 79]. The first such attack benefitted from the detector imperfections, by collecting the light emitted upon the detection of the photons [80]. To counter such attacks, introducing simple optical isolators suffice in one-way protocols, while for two-way protocols one needs to introduce additional monitoring detectors [81].

Furthermore, we would like to briefly discuss two more attacks, namely the detector blinding and the time-shift attacks, which are both considered in the broader context of intercept and resend with faked states attacks [82]. In general, during an intercept and resend with faked states attack, Eve is not trying to extract information about the key from the original states that the legitimate parties exchange. Instead, she generates and sends to them classical or quantum light pulses, which are tailored in a way that she can control their measurement outcomes, while she is blocking the original states. At the end of such an attack, Eve and the legitimate parties share the same key, without Alice and Bob being able to detect Eve’s interference. In both the aforementioned attacks, Eve is taking advantage of loopholes in the performance and efficiency of the detectors of the legitimate parties.

First, we consider the detector blinding attacks to standard one-way QKD protocols [83, 84]. Eve first intercepts the state that Alice sends to Bob and measures it in one of the two possible bases, that she randomly chooses. Then, she sends to one of Bob’s detectors a bright light pulse according to her measurement outcome. Note that the intensity of the bright light pulse is just a bit above the detector’s threshold. If Bob chooses to measure in the same basis as Eve, all the light will be directed to one of his detectors, due to the interference. The detector, which is now operating in the linear instead of the Geiger mode (avalanche photon diode), will click and Eve will now share the same key bit with Bob. If Bob chooses

to measure in the complementary basis, the light will be divided in two components and its intensity will not be enough to trigger neither of the detectors, therefore Bob will not get a click and this iteration will be discarded. Subsequently, Alice and Bob will keep for the key the bits for which Alice’s preparation basis and Bob’s measuring basis agree. During their classical communication, Eve will learn exactly which are these bits, therefore she will share the same key, while her interference remains unnoticed.

This attack is ineffective for the case of our first, two-way, protocol, in which only Alice is performing the measurement on the pulses received back from Bob. Note that her performing the inverse QW, followed by the measurement in the computational basis, is equivalent to measuring in an *unknown* to Eve (ensured by our Holevo argument mentioned in Section 3.1, and presented with details in [19]), “rotated” basis, with respect to the computational one. Therefore, virtually all Eve attempts to perform the detector blinding attack would result in no detection events for Alice. Moreover, even the (rare) detections, being uncorrelated with the initial state sent by Alice, would not pass the verification procedure described in Section 3.1.1, as well as the analogous checking rounds of the third, two-way semi-quantum protocol (when Bob reflects the pulses back to Alice and she performs the inverse walk and measures in the computational basis).

Regarding our second, one-way key distribution protocol, Bob’s action is similar to the one in the standard protocols: he measures in one of the two publicly known bases. To counter such an attack, Bob can apply one of the known counter-measures proposed and analysed in [85, 86, 87, 88, 89]. Nevertheless, we would like to note again that our QW protocol is more complex than the standard ones based on few (typically four) quantum states, and thus its implementations might possibly invoke new challenges, a topic worth a separate study.

Time-shift attacks take advantage of the different timing responses of the detectors. Assuming Eve knows the timings of during which each detector is (in)sensitive, allows her to, similarly as in the previous case of the detector blinding, enforce the particular outcomes of Bob’s/Alice’s measurements. Analogously as in the case of detector blinding attacks, such strategy cannot pass the two-way verification procedures and checking rounds of our first and third protocols. In the case of our one-way protocol, one could employ similar methods to the ones proposed in [90, 91, 92, 93], in order to defend against a time-shift attack.

7 Conclusions and future work

In this paper we employed, for the first time to our knowledge, QWs in order to design and analyze new secure QKD protocols.

Perhaps the most important contribution of this work is that it introduces the exciting possibility of using QWs for QKD purposes and may spur new research in both cryptography, and also in QWs. By themselves, QWs exhibit many fascinating properties which, as we’ve shown here, translate to interesting properties of QKD protocols.

Besides the theoretically interesting intersection of two unique and fascinating fields of quantum information science, there are also potential practical benefits in pursuing this in-

vestigation. Recently, it has been shown in numerous studies [94, 95, 96, 97, 98, 99, 100, 101] that when Alice and Bob exchange higher dimensional systems (qudits instead of qubits), the respective QKD protocols (in fact both kinds of prepare-and-measure and entanglement-based) *tolerate more noise* than the 2-dimensional ones. This is also confirmed by our results for the high-dimensional states generated by means of QWs, where the noise tolerance increases for higher dimensions. While such systems hold interesting theoretical properties, it could also be that, in a future quantum infrastructure, the generation of these QW states would be easier compared to other higher dimensional systems. Indeed, producing such states may not need the high entanglement of many qubits – instead they could be generated through the evolution of a single-qubit walker on, for instance, a multi-node quantum network.

In what follows, we point out some directions of future work. First, it would be interesting to perform a more detailed study on the two verification procedures presented in Sections 3.1.1 and 3.1.2 and compare them with respect to various attack strategies. Moreover, one could analyze the relation between the two for concrete cases of Eve’s cheating strategies in the presence of noise.

We have presented our protocols in the case that the parties use lossless channels, which is the common first step, when it comes to proving security of new theoretical QKD protocols [60, 102, 31, 103, 99]. A relevant future direction of work would be to conduct a detailed analysis of the effects of lossy channels on the number of secret key bits that the parties share in the end, and determine the relevant measures, such as distance vs key-rate, etc.

In Section 4, we proved the security of the one-way protocol, but still some improvements could be done. In particular, one could find an analytical solution for the optimal choice of QW parameters or, alternatively, given particular QW parameters, to find an analytical solution for the value of c from Equation (9). Another interesting question would be to understand the maximally tolerated noise as the dimension of the QW $P \rightarrow \infty$ (and also $T_{\max} \rightarrow \infty$). For instance, in [99], a high-dimensional QKD protocol was introduced (not using QWs, but simpler states), which could suffer a disturbance up to 50% as the dimension of the state sent by Alice approached infinity (for a novel protocol for multiparty quantum key management that implements d -level measurements, see [104]). Can we construct a QW-QKD protocol with similar features? Does our protocol approach this disturbance level for high P ? Moreover, studying and employing other QW models (perhaps the memory-based QWs described and analyzed in, e.g., [105, 106, 107, 108, 36, 109]) or QWs on different graphs, would be interesting – our key-rate equation would generalize to these cases, the only change would be the value of c ; perhaps different QW models, or different graphs, would produce more optimal values, thus increasing the key-rate.

The SQKD protocol we proposed lacks of a proof of security beyond robustness. As we already mentioned in Section 5, this proof is technically very challenging due to the high-dimensional QW states and the use of a two-way channel. Hence, computing analytically the key-rate is extremely hard and moreover, the numerical simulation is equally challenging, even for low-dimensional walks. Nevertheless, we believe that obtaining the key rate is not impossible, and we expect that this analysis will yield quite high error-tolerance. A first step

towards this direction would be to try to reduce this protocol to a simpler one (for instance, the one in [22], for which there is a security proof [54]) and prove that it is at least as secure. This reduction does not seem to be a straightforward task and requires a thorough analysis.

Finally, concrete proposals for possible practical implementations of our protocols deserve a separate investigation, and we leave them as future work. While such practical implementations can be non-trivial, we believe that our theoretical proposals are quite promising. In particular, we are optimistic that the experimental advances in the field of the generation and manipulation of high-dimensional states mentioned above, combined with the on-going progress in the field of QW realisations, will permit the implementation of our protocols in higher dimensions. Furthermore, as we argued before, high-dimensional QW states (at least in the case of our second protocol) are not necessary in order to obtain a secure and robust protocol. Along these lines, our proposals could be seen as alternatives to the already existing QKD protocols, which can be implemented with the current technology. Perhaps, the most relevant setups for QKD purposes would be the optical implementations of QWs [110, 111, 112, 113, 114, 115, 116, 117, 118]. For a detailed and complete review of QW experimental realisations, we refer to the book [119].

Acknowledgements

WK would like to acknowledge the hospitality of SQIG–Security and Quantum Information Group in IT – Instituto de Telecomunicações, in Lisbon, during his visit while working on this project. CV acknowledges the support from DP-PMI and FCT (Portugal) through the grant PD/BD/ 52652/2014. CV, PM, NP and AS acknowledge the support of SQIG-Security and Quantum Information Group. PM, NP and AS also acknowledge the support from UID/EEA/50008/2013. NP acknowledges the IT project QbigD funded by FCT PEst-OE/ EEI/LA0008/2013. PM and AS acknowledges the FCT project Confident PTDC/EEI-CTP/4503/2014. A.S. also acknowledges the support of LaSIGE Research Unit, ref. UID/CEC/00408/2013.

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] A. K. Ekert. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

- [4] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144km. *Nat Phys*, 3:481–486, 2007.
- [5] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi. Experimental quantum key distribution without monitoring signal disturbance. *Nature Photonics*, 9:827–831, 2015.
- [6] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein. Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology*, 2:024009, Jun 2017.
- [7] ID Quantique. Quantum key distribution record. <http://www.idquantique.com/record-breaking-qkd>, 2017.
- [8] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356:1140–1144, 2017.
- [9] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random walks. *Phys. Rev. A*, 48:1687–1690, Aug 1993.
- [10] E. Farhi and S. Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915–928, Aug 1998.
- [11] 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.
- [12] A. Ambainis. Quantum walks and their algorithmic applications. *International Journal of Quantum Information*, 01(04):507–518, 2003.
- [13] 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.
- [14] R. Portugal. *Quantum walks and search algorithms*. Quantum Science and Technology. New York, NY: Springer, 2013.
- [15] A. M. Childs. Universal computation by quantum walk. *Phys. Rev. Lett.*, 102:180501, May 2009.

- [16] N. B. Lovett, S. Cooper, M. Everitt, M. Trevers, and V. Kendon. Universal quantum computation using the discrete-time quantum walk. *Phys. Rev. A*, 81:042330, Apr 2010.
- [17] A. M. Childs, D. Gosset, and Z. Webb. Universal computation by multiparticle quantum walk. *Science*, 339(6121):791–794, 2013.
- [18] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist. Quantum walks with encrypted data. *Physical review letters*, 109(15):150501, 2012.
- [19] C. Vlachou, J. Rodrigues, P. Mateus, N. Paunković, and A. Souto. Quantum walk public-key cryptographic system. *International Journal of Quantum Information*, 13(07):1550050, 2015.
- [20] G. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A*, 77:032348, Mar 2008.
- [21] U. Seyfarth, G.M. Nikolopoulos, and G. Alber. Symmetries and security of a quantum-public-key encryption based on single-qubit rotations. *Physical Review A*, 85(2):022342, 2012.
- [22] M. Boyer, D. Kenigsberg, and T. Mor. Quantum key distribution with classical bob. *Phys. Rev. Lett.*, 99:140501, Oct 2007.
- [23] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor. Semiquantum key distribution. *Phys. Rev. A*, 79:032341, Mar 2009.
- [24] A. C. Yao. How to generate and exchange secrets. In *Foundations of Computer Science, 1986., 27th Annual Symposium on*, pages 162–167. IEEE, 1986.
- [25] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell’s theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.
- [26] H. K. Lo and H. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.
- [27] M. Curty, M. Lewenstein, and N. Lutkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, May 2004.
- [28] M. Curty, O. Guhne, M. Lewenstein, and N. Lutkenhaus. Detecting two-party quantum correlations in quantum-key-distribution protocols. *Phys. Rev. A*, 71:022306, Feb 2005.
- [29] E. Woodhead and S. Pironio. Secrecy in prepare-and-measure clauser-horne-shimony-holt tests with a qubit bound. *Phys. Rev. Lett.*, 115:150501, Oct 2015.
- [30] H.-K. Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.*, 18(2):133–165, April 2005.

- [31] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.
- [32] M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.
- [33] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nat. Phys.*, 3:645–649, Jul 2007.
- [34] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. 461(2053):207–235, 2005.
- [35] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nat. Phys.*, 6:659–662, Jul 2010.
- [36] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. *Proceedings of ACM Symposium on Theory of Computation (STOC '01)*, pages 50–59, July 2001.
- [37] J. Kempe. Quantum random walks: An introductory overview. *Contemporary Physics*, 44(4):307–327, 2003.
- [38] J. Bae and A. Acín. Key distillation from quantum channels using two-way communication protocols. *Phys. Rev. A*, 75:012334, Jan 2007.
- [39] N. Ashwin and V. Ashvin. Quantum walk on the line. Technical report, 2000.
- [40] Salvador Elías Venegas-Andraca. Quantum walks: a comprehensive review. *Quantum Information Processing*, 11(5):1015–1106, Oct 2012.
- [41] F. Wang, M. Erhard, A. Babazadeh, M. Malik, M. Krenn, and A. Zeilinger. Generation of the complete four-dimensional bell basis. *Optica*, 4:1462–1467, 2017.
- [42] A. K. Jha, M. Malik, and R. W. Boyd. Exploring energy-time entanglement using geometric phase. *Phys. Rev. Lett.*, 101:180405, Oct 2008.
- [43] A. Martin, T. Guerreiro, A. Tiranov, S. Designolle, F. Frowis, N. Brunner, M. Huber, and N. Gisin. Quantifying photonic high-dimensional entanglement. *Phys. Rev. Lett.*, 118:110501, Mar 2017.
- [44] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson. Experimental high-dimensional two-photon entanglement and violations of generalized bell inequalities. *Nature Physics*, 7:677–680, May 2011.
- [45] M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger. Generation and confirmation of a (100 x 100)-dimensional entangled quantum system. *Proceedings of the National Academy of Science of the United States of America*, 111:6243–6247, 2014.

- [46] J. Bavaresco, N. Herrera Valencia, C. Klöckl, M. Pivoluska, N. Friis, M. Malik, and M. Huber. Two measurements are sufficient for certifying high-dimensional entanglement. *arXiv preprint*, page 1709.07344, 2017.
- [47] M. P. J. Lavery, D. J. Robertson, G. C. G. Berkhout, G. D. Love, M. J. Padgett, and J. Courtial. Refractive elements for the measurement of the orbital angular momentum of a single photon. *Optics Express*, 20:2110–2115, 2012.
- [48] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd. Efficient separation of the orbital angular momentum eigenstates of light. *Nature Communications*, 4:2781, 2013.
- [49] N. T. Islam, C. Cahall, A. Aragonese, A. Lezama, J. Kim, and D. J. Gauthier. Robust and stable delay interferometers with application to d -dimensional time-frequency quantum key distribution. *Phys. Rev. Applied*, 7:044010, Apr 2017.
- [50] m. Erhard, M. Malik, M. Krenn, and A. Zeilinger. Experimental ghz entanglement beyond qubits. *arXiv preprint*, page 1708.03881, 2017.
- [51] M. Malik, M. Erhard, M. Huber, M. Krenn, Fickler R., and A. Zeilinger. Multi-photon entanglement in high dimensions. *Nature Photonics*, 10:248–252, Feb 2016.
- [52] B. C. Hiesmayr, M. J. A. de Dood, and W. Löffler. Observation of four-photon orbital angular momentum entanglement. *Phys. Rev. Lett.*, 116:073601, Feb 2016.
- [53] Mario Krenn, Mehul Malik, Robert Fickler, Radek Lapkiewicz, and Anton Zeilinger. Automated search for new quantum experiments. *Phys. Rev. Lett.*, 116:090405, Mar 2016.
- [54] W. O. Krawec. Security proof of a semi-quantum key distribution protocol. In *Information Theory (ISIT), 2015 IEEE International Symposium on*, pages 686–690. IEEE, 2015.
- [55] W. O. Krawec. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Information Processing*, 15(5):2067–2090, 2016.
- [56] W. O. Krawec. Quantum key distribution with mismatched measurements over arbitrary channels. *arXiv preprint arXiv:1608.07728*, 2016.
- [57] W. Zhang, D. Qiu, and P. Mateus. Security of a single-state semi-quantum key distribution protocol. *arXiv preprint arXiv:1612.03170*, 2016.
- [58] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A*, 79:052312, May 2009.
- [59] W. O. Krawec. Restricted attacks on semi-quantum key distribution protocols. *Quantum Information Processing*, 13(11):2417–2436, November 2014.

- [60] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lutkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.
- [61] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, 57(3):366–387, 2016.
- [62] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan. Practical challenges in quantum key distribution. *Npj Quantum Information*, 2:16025, 2016.
- [63] R. Bedington, J. M. Arrazola, and A. Ling. Progress in satellite quantum key distribution. *Npj Quantum Information*, 3:30, 2017.
- [64] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields. Quantum key distribution with hacking countermeasures and long term field trial. *Scientific Reports*, 7:1978, 2017.
- [65] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders. Security aspects of practical quantum cryptography. In *In Advances in Cryptology? EUROCRYPT’2000*, pages 289–299, 2000.
- [66] N. Lutkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, Apr 2000.
- [67] N. Lutkenhaus and M. Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4(1):44, 2002.
- [68] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.
- [69] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.
- [70] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005.
- [71] X.-B. Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A*, 72:012322, Jul 2005.
- [72] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt. Enhancing practical security of quantum key distribution with a few decoy states. *arXiv preprint arXiv:0503002*, 2005.

- [73] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.
- [74] Q. Wang, X.-B. Wang, G. Björk, and A. Karlsson. Improved practical decoy state method in quantum key distribution with parametric down-conversion source. *EPL (Europhysics Letters)*, 79(4):40001, 2007.
- [75] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt. Practical long-distance quantum key distribution system using decoy levels. *New Journal of Physics*, 11(4):045009, 2009.
- [76] M. Lucamarini, J. F. Dynes, B. Frohlich, Z. Yuan, and A. J. Shields. Security bounds for efficient decoy-state quantum key distribution. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):1–8.
- [77] A. Vakhitov, V. Makarov, and D. R. Hjelle. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 48(13):2023–2038, 2001.
- [78] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields. Practical security bounds against the trojan-horse attack in quantum key distribution. *Phys. Rev. X*, 5:031030, Sep 2015.
- [79] S. Sajeed, C. Minshull, N. Jain, and V. Makarov. Invisible trojan-horse attack. *Scientific Reports*, 7:8403, 2017.
- [80] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter. The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks? *Journal of Modern Optics*, 48(13):2039–2047, 2001.
- [81] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73:022320, Feb 2006.
- [82] L. A. Lizama-Pérez, J. M. López, and E. De Carlos López. Quantum key distribution in the presence of the intercept-resend with faked states attack. *Entropy*, 19(1):4.
- [83] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686, 2010.
- [84] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, Ch. Marquardt, V. Makarov, and G. Leuchs. After-gate attack on a quantum cryptosystem. *New Journal of Physics*, 13(1):013043, 2011.

- [85] Q. Liu, A. Lamas-Linares, C. Kurtsiefer, J. Skaar, V. Makarov, and I. Gerhardt. A universal setup for active control of a single-photon detector. *Review of Scientific Instruments*, 85(1):013108, 2014.
- [86] M. Stipcević. Preventing detector blinding attack and other random number generator attacks on quantum cryptography by use of an explicit random number generator. *arXiv preprint arXiv:1403.0143*, 2014.
- [87] M.S. Elezov, R.V. Ozhegov, Y.V. Kurochkin, G.N. Goltsman, and V.S. Makarov. Countermeasures against blinding attack on superconducting nanowire detectors for qkd. *EPJ Web of Conferences*, 103:10002, 2015.
- [88] J. Wang, H. Wang, X. Qin, Z. Wei, and Z. Zhang. The countermeasures against the blinding attack in quantum key distribution. *The European Physical Journal D*, 70(1):5, Jan 2016.
- [89] M. S. Lee, B. K. Park, M. K. Woo, C. H. Park, Y.-S. Kim, S.-W. Han, and S. Moon. Countermeasure against blinding attacks on low-noise detectors with a background-noise-cancellation scheme. *Phys. Rev. A*, 94:062321, Dec 2016.
- [90] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74:022313, Aug 2006.
- [91] A. Lamas-Linares and C. Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Optics Express*, 15:9388–9393, 2007.
- [92] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008.
- [93] B. Qi, C.-H. F. Fung, H.-K Lo, and X. Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation*, 7:73–82, 2007.
- [94] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000.
- [95] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002.
- [96] D. Bruss, M. Christandl, A. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello. Tomographic quantum cryptography: Equivalence of quantum and classical key distillation. *Phys. Rev. Lett.*, 91:097901, Aug 2003.
- [97] G. M. Nikolopoulos and G. Alber. Security bound of two-basis quantum-key-distribution protocols using qudits. *Phys. Rev. A*, 72:032320, Sep 2005.

- [98] L. Sheridan and V. Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82:030301, Sep 2010.
- [99] H. F. Chau. Quantum key distribution using qudits that each encode one bit of raw key. *Phys. Rev. A*, 92:062324, Dec 2015.
- [100] G. M. Nikolopoulos, K. S. Ranade, and G. Alber. Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication. *Phys. Rev. A*, 73:032325, Mar 2006.
- [101] H. F. Chau. Unconditionally secure key distribution in higher dimensions by depolarization. *IEEE Transactions On Information Theory*, 51:1451–1468, 2005.
- [102] H. Lu, C.-H. F. Fung, X. Ma, and Q.-Y. Cai. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phys. Rev. A*, 84:042344, Oct 2011.
- [103] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner. Security of two-way quantum key distribution. *Physical Review A*, 88(6):062302, 2013.
- [104] Gang Xu, Xiu-Bo Chen, Zhao Dou, Yi-Xian Yang, and Zongpeng Li. A novel protocol for multiparty quantum key management. *Quantum Information Processing*, 14(8):2959–2980, August 2015.
- [105] M. McGettrick. One dimensional quantum walks with memory. *Quantum Info. Comput.*, 10(5):509–524, May 2010.
- [106] M. Gettrick and J. A. Miszczyk. Quantum walks with memory on cycles. *Physica A: Statistical Mechanics and its Applications*, 399:163 – 170, 2014.
- [107] P. P. Rohde, G. K. Brennen, and A. Gilchrist. Quantum walks with memory provided by recycled coins and a memory of the coin-flip history. *Phys. Rev. A*, 87:052302, May 2013.
- [108] W. O. Krawec. History dependent quantum walk on the cycle with an unbalanced coin. *Physica A: Statistical Mechanics and its Applications*, 428:319 – 331, 2015.
- [109] T. A. Brun, H. A. Carteret, and A. Ambainis. Quantum walks driven by many coins. *Phys. Rev. A*, 67:052317, May 2003.
- [110] M. A. Broome, A. Fedrizzi, B. P. Lanyon, I. Kassal, A. Aspuru-Guzik, and A. G. White. Discrete single-photon quantum walks with tunable decoherence. *Phys. Rev. Lett.*, 104:153602, Apr 2010.
- [111] 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.

- [112] S. K. Goyal, F. S. Roux, A. Forbes, and T. Konrad. Implementing quantum walks using orbital angular momentum of classical light. *Phys. Rev. Lett.*, 110:263602, Jun 2013.
- [113] S. K. Goyal, F. S. Roux, A. Forbes, and T. Konrad. Implementation of multidimensional quantum walks using linear optics and classical light. *Phys. Rev. A*, 92:040302, Oct 2015.
- [114] P. L. Knight, E. Roldan, and J. E. Sipe. Quantum walk on the line as an interference phenomenon. *Phys. Rev. A*, 68:020301, Aug 2003.
- [115] A. Schreiber, K. N. Cassemiro, V. Potocek, A. Gabris, P. J. Mosley, E. Andersson, I. Jex, and Ch. Silberhorn. Photons walking the line: A quantum walk with adjustable coin operations. *Phys. Rev. Lett.*, 104:050502, Feb 2010.
- [116] E. Roldan and J. C. Soriano. Optical implementability of the two-dimensional quantum walk. *Journal of Modern Optics*, 52:2649–2657, 2006.
- [117] A. Schreiber, A. Gabris, K. Rohde, P. P. and Laiho, M. Stefanak, V. Potocek, I. Hamilton, C. and Jex, and C. Silberhorn. A 2d quantum walk simulation of two-particle dynamics. *Science*, 336:55–58, 2012.
- [118] F. Cardano, F. Massa, H. Qassim, E. Karimi, S. Slussarenko, D. Paparo, C. de Lisio, F. Sciarrino, E. Santamato, R. W. Boyd, and L. Marrucci. Quantum walks and wavepacket dynamics on a lattice with twisted photons. *Science Advances*, 1:e1500087, 2015.
- [119] K. Manouchehri and J. Wang. *Physical Implementation of Quantum Walks*. Springer Publishing Company, Incorporated, 2013.