Quantum Information Processing (2020) 19:77
https://doi.org/10.1007/s11128-019-2573-2

Authenticated semi-quantum key distribution without entanglement

Sofia Zebboudj[1] · Hizia Djoudi[2] · Dalila Lalaoui[2] · Mawloud Omar[1]

Received: 17 March 2019 / Accepted: 31 December 2019 / Published online: 10 January 2020

Abstract
One important challenge of quantum key distribution is to preserve its unconditional security when a scheme is implemented. In semi-quantum key distribution (SQKD), one of the parties is only able to perform classical operations, thus alleviating the cost of its implementation. Authenticated SQKD (ASQKD) ensures also better security than SQKD against attacks aiming at the identity of the parties. In this regard, Li et al. have proposed a new ASQKD scheme that ensures better efficiency than the first proposed ASQKD scheme of Yu et al. However, both schemes present loopholes in their security. This study presents a new ASQKD without using entanglement, able to achieve higher security than the schemes of Yu et al. and Li et al. Our scheme is also simpler and demands less advanced quantum devices than ASQKD schemes using entanglement.

Keywords Semi-quantum key distribution · Authentication · Security analysis

1 Introduction

Quantum cryptography is about using the laws of quantum physics to establish secure communication between remote parties. Although some classical cryptosystems are considered computationally unbreakable with today's technology, the great potential of quantum computing is making current cryptosystems vulnerable toward quantum algorithms for prime factorization and discrete logarithm problems [1], on which the security of most classical cryptosystems is based [2,3]. An important example of quantum cryptography is quantum key distribution, which distributes a secret key

✉ Mawloud Omar
mawloud.omar@gmail.com; mawloud.omar@univ-bejaia.dz

Sofia Zebboudj
sofiazebboudj@gmail.com; sofia.zebboudj@univ-bejaia.dz

1 Unité de recherche LAMOS, Faculté des Sciences Exactes, Université de Bejaia, Bejaia, Algérie

2 Département d'Informatique, Faculté des Sciences Exactes, Université de Bejaia,, Bejaia, Algérie

between two remote parties while ensuring the security of the transmission through laws of quantum physics and information theory. Indeed, the detection of intruders and the unconditional security of the shared information are two naturally attainable characteristics of quantum cryptography [4–7]. The distributed secret key can then be used in a symmetric encryption algorithm, such as the one-time pad ciphering algorithm [8], to encrypt and decrypt confidential data. Although it appears natural to reach such a level of security, the current technology is not yet able to achieve it in practice. In fact, many of the existing schemes require each participant to be able to perform quantum operations, which makes them more expensive and difficult to realize in practice [9]. To solve such a problem, semi-quantum key distribution (SQKD) schemes have been introduced. In this class of schemes, a sender, most commonly referred as Alice, uses quantum operations on the particles to transmit a secret key to a receiver, Bob, who can only perform classical operations on the particles, namely [10,11]:

(i) Measuring a particle in the classical basis $Z = \{|0\rangle, |1\rangle\}$,
(ii) Preparing a particle in the classical basis Z and sending it,
(iii) Reordering particles via different delay lines,
(iv) Reflecting a particle without measurement,
(v) Any other classical operation on a classical computer.

The operations (i) and (ii) are considered classical because they are performed on qubits within the classical basis Z only and never on a superposition of states [10].

In addition to a quantum channel, an authenticated classical channel is used to guarantee the authenticity of the exchanged information and avoid attacks aiming at the identity of the two parties when performing information reconciliation and privacy amplification. In this regard, Yu et al. [9] have proposed an Authenticated SQKD (ASQKD) scheme that does not require the classical public channel to be authenticated. Their scheme uses the entanglement of Bell states and pre-shared secret keys to ensure the authenticity of the communication. As in SQKD schemes, two variants of the scheme are proposed: a randomization-based scheme and a measure-resend one. The difference between the two variants lies in what classical operations can Bob perform on the particles. Following the same idea, Li et al. [12] have proposed an ASQKD scheme with two variants in which no classical public channel is used unless an attack is suspected. In their schemes, Alice, the legitimate sender, introduces checking particles prepared randomly in the Z or X bases within a sequence of particles representing the key to be shared with Bob, the legitimate receiver. The checking particles and the key particles are ordered according to a pre-shared secret key known only by the two legitimate parties. In this way, an eavesdropper, Eve, who does not have access to the pre-shared key, cannot distinguish between the checking particles and the key particles when they are sent to Bob.

Although the above ASQKD schemes can be useful in different practical environments such as in a client-server archetype as proposed in [12], both of them present loopholes in their security. For example, Meslouhi et al. [13] have proposed an attack against the scheme of Yu et al. [9] where Eve, pretending to be Alice, can recover the pre-shared secret keys after communicating with Bob. This is because, for each received particle from Alice/Eve, Bob uses a pre-shared secret key, K_2, to decide

whether he has to reflect the particles or measure them without first checking the identity of Alice/Eve. Eve can then impersonate Alice in both the quantum and public channels and perform an entanglement test based on the technique in [14] to deduce Bob's operations on each particle and recover K_2. Once the pre-shared secret key is recovered, Eve can use it to also recover K_3, another pre-shared secret key used in the scheme. It is also possible to execute this attack in the measure-resend scheme of Li et al. [12], since the scheme also depends on Bell states. Other attacks, presented further in this paper, can be executed by Eve to efficiently and rapidly discover both the pre-shared keys and the key to be shared in the schemes of Yu et al. [9] and Li et al. [12].

In this paper, we first propose two ASQKD schemes which allow two parties, Alice and Bob, to distribute a secret key via a quantum channel as well as to ensure authentication during the process. While Alice is assumed to be equipped with quantum devices, Bob is fully classical. In most SQKD and ASQKD schemes, no restrictions are made on Alice's capacities, which are still assumed to have advanced quantum devices. Therefore, our schemes aim to alleviate Alice's process while ensuring better security than the schemes of Yu et al. [9] and Li et al. [12]. Unlike these latter, our schemes do not use Bell states. Therefore, there is no need to store particles in a quantum memory for later Bell state measurements. This simplifies the authentication process and makes our schemes more practical and robust against the attack of Meslouhi et al. [13]. In the second part of this paper, we analyze the security of the schemes of Yu et al. [9] and Li et al. [12] and show their vulnerability against various attacks that allow Eve, through few iterations, to fully recover the pre-shared secret keys. Another important attack where Eve recovers completely the secret key to be shared and half of the pre-shared key without detection is presented. Through these attacks, we also show the robustness and reliability of our schemes to deliver a secret key while protecting the pre-shared keys.

2 The scheme

As in the original scheme of Boyer et al. [10], two variants are proposed: a randomization-based ASQKD and a measure-resend one. The difference between the two schemes lies in which classical operations can Bob perform on the particles. In both schemes, Bob and Alice pre-share a secret key which is used to determine their operations on the transmitted information and authenticate Bob. Similarly to the scheme of Li et al. [12], additional particles, named checking particles, are used to detect Eve. A hash function, H_{auth}, is also used along with the pre-shared secret key in order to ensure both the integrity of the sent information and the authenticity of Alice and Bob. Given the imperfection of channels in practice, error-correcting codes are to be applied when performing the hash function H_{auth} in order to correct small errors and let the major ones be used to detect the presence of Eve.

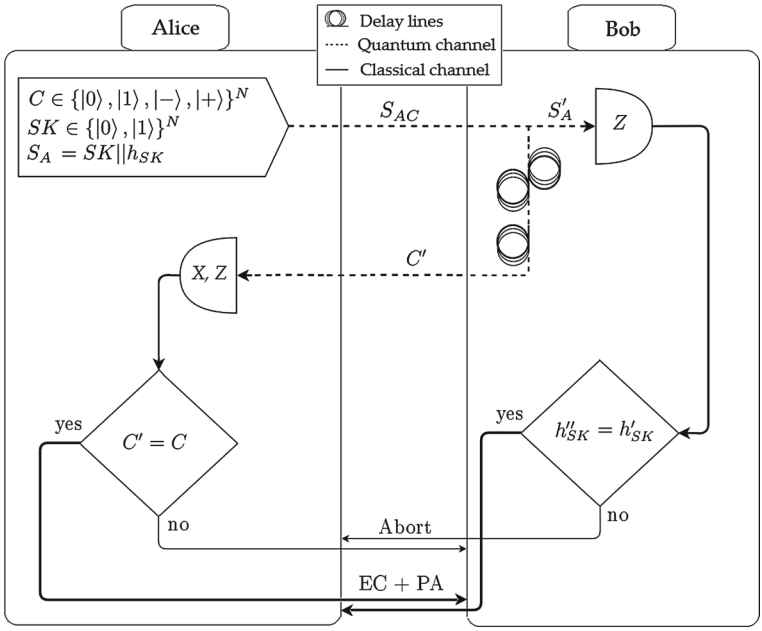

Fig. 1 Proposed randomization-based ASQKD scheme

2.1 The randomization-based scheme

Alice and Bob both have access to a pre-shared secret key K_1 which is used to conceal the secret key into a sequence of checking particles, and to determine their positions. Nevertheless, for security purposes, Alice and Bob use universal hashing to also conceal the pre-shared key as follows:

- Alice uniformly chooses a function H from a family of hash functions and announce it to Bob over a public channel along with the sequence $H_{\text{auth}}(H||K_1)$ to confirm her identity.
- Bob generates a timestamp T and sends it to Alice along with $H_{\text{auth}}(T||K_1)$ so she can check his identity too.
- They both calculate $K_{HT} = H(K_1||T) \in \{0, 1\}^{N+M}$ which will be used instead of K_1 for reordering the particles.

Note that H and T are both chosen/generated independently by Alice and Bob, which prevent Eve from controlling the value of K_{HT} even if she impersonates one of them. H and T are also updated before each iteration of the protocol which guarantees the freshness of K_{HT}.

In the randomization-based scheme, Bob is restricted to perform the operations (i), (iii), (iv), and (v). The randomization-based scheme is shown in Fig. 1 and works as follows:

– *Phase 01* Alice randomly generates the secret key to be distributed:

$$SK = \{0, 1\}^N. \tag{1}$$

She performs a hash function, H_{auth}, on the concatenation of SK and K_1 to obtain h_{SK}:

$$h_{SK} = H_{\text{auth}}(SK||K_1) \in \{0, 1\}^M. \tag{2}$$

Alice then generates two independent sequences of $N + M$ particles: the S_A particles, generated in the $Z = \{|0\rangle, |1\rangle\}$ basis and corresponding to the classical sequence $SK||h_{SK}$, and the C particles, generated in either the Z or $X = \{|-\rangle, |+\rangle\}$ basis at random, and representing the checking particles.

– *Phase 02* Alice forms the sequence S_{AC} by joining the two sequences S_A and C according to the concealed pre-shared key K_{HT}: for each particle of S_A, if $K^i_{HT} = 0$, a checking particle is placed in front of the S_A particle, else, it is placed in the back of it. Alice then sends the sequence S_{AC} to Bob.

– *Phase 03* Based on K_{HT}, Bob can tell which particles are from S_A and which ones are from C. He will, therefore, measure each arrived particle that is part of S_A to obtain $SK'||h'_{SK}$. As for the arriving checking particles C', Bob will reorder them according to K_{HT} before sending them to Alice. For instance, Bob can use two delay lines: if $K^i_{HT} = 0$, the received C'_{2i} will be put in the first delay line and C'_{2i+1} in the second one. Else, C'_{2i} will be put in the second delay line and C'_{2i+1} in the first one. Note that the traveling time of the first delay line should be long enough to wait for the last sent particle to enter, while the time traveling of the second delay line should be at least twice as long as the first one. The reordering of the checking particles, C', which can also be done by more than 2 delay lines prevents Bob from sending valuable information to Alice/Eve before verifying her identity. This will be discussed further in Sect. 3.

– *Phase 04* Bob verifies the integrity of the received secret key by calculating

$$h''_{SK} = H_{\text{auth}}(SK'||K_1), \tag{3}$$

and compares it with the received h'_{SK}: if $h''_{SK} \neq h'_{SK}$, Bob will conclude that the sequence representing SK has been altered and informs Alice to abort the protocol. On the other hand, Alice uses K_{HT} to measure the checking particles in the same basis she has prepared them and in the right order. If the measurement results correspond to the initial states, then Alice is sure that the received checking particles C' are from Bob, since only he have access to K_1 in order to calculate K_{HT} and distinguish between C and S_A. However, if the results are different, Alice informs Bob to abort the protocol.

2.2 The measure-resend scheme

In this scheme, Bob and Alice pre-share a secret key, $K \in \{0, 1\}^{2(N+M)}$, and divide it in two equal parts: K_1 and K_2. Bob cannot reorder the particles; however, he can prepare a particle in the classical basis and send it to Alice. In other words, he is

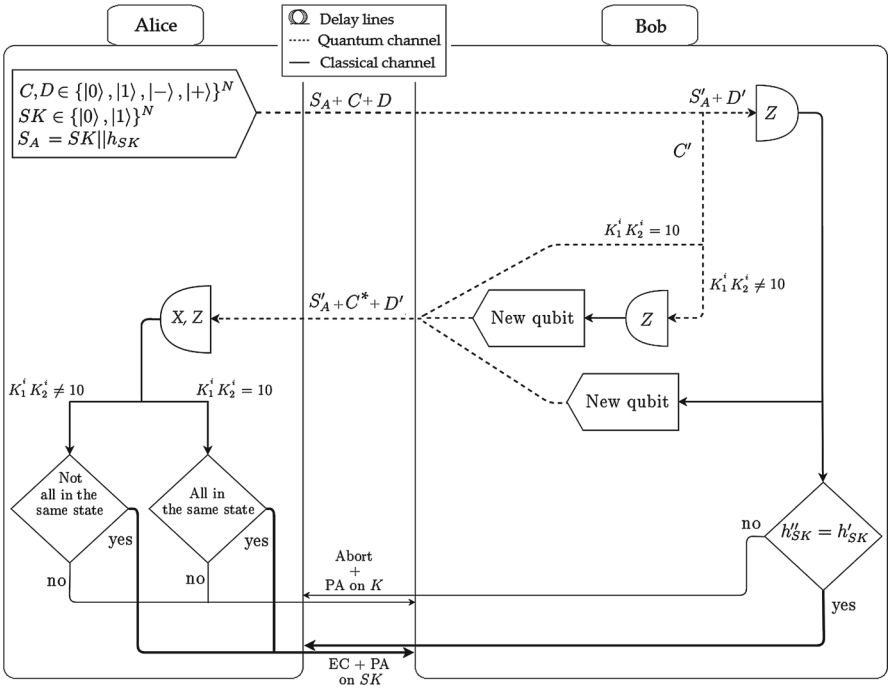

Fig. 2 Proposed measure-resend ASQKD scheme

Table 1 Positions of the particles according to K_1 and K_2

K_1^i	K_2^i	S_{ACD}^{3i}	S_{ACD}^{3i+1}	S_{ACD}^{3i+2}
0	0	C_i	S_i	D_i
0	1	D_i	C_i	S_i
1	0	C_i	D_i	S_i
1	1	S_i	C_i	D_i

restricted to perform the operations (i), (ii), (iv), and (v). The measure-resend scheme is shown in Fig. 2 and works as follows:

- *Phase 01* Alice follows the same steps as in Phase 01 of the randomization-based scheme to obtain h_{SK}. Additional particles, D, are prepared in the X and Z bases at random.
- *Phase 02* Alice forms the sequence S_{ACD} that she will send to Bob by joining the sequences S_A, C, and D depending on both K_1 and K_2.
  The ordering of the sequences is illustrated in Table 1.
- *Phase 03* For each set of three received particle of S_{ACD}:
  1. When $K_1^i = 1$ and $K_2^i = 0$: (1) Bob reflects the C particle directly to Alice without any modification, (2) he measures the D particle in the Z basis and sends back a new particle in the same state, and (3) he measures the S_A particle,

extracts the ith classical bit of $SK'||h'_{SK}$, stores it, and sends back a new particle in the same state to Alice.
2. For all the other cases, Bob measures the particles (S_A, C and D) and sends clones to Alice. He, however, extracts a bit of $SK'||h'_{SK}$ each time he measures the S_A particle.

Once Bob has sent back all the reflected/generated particles to Alice and extracted all bits of $SK'||h'_{SK}$ from his measurements, he verifies the integrity and authenticity of the received secret key SK' by comparing the extracted h'_{SK} with the calculated $h''_{SK} = H(SK'||K_1)$. If the two sequences are different, Bob aborts the protocol.

– *Phase 04* Alice measures each received particle in the same basis of preparation:

1. If all the C particles are in the same state when $K_1^i = 1$ and $K_2^i = 0$, then Alice knows that Bob has used the secret key K_1 to avoid measuring the checking particles. Else, Alice concludes that the other party has not access to K and has measured some C particles in the wrong bases. Therefore, Alice aborts the protocol.
2. If all the particles are still in the same state in all the other cases, Alice concludes that Bob has not measured them, i.e., the particles have been intercepted and sent back directly by Eve. Alice then aborts the protocol for a reflecting attack that has been detected.

Using the extra particles, D randomizes the location of the particles C and S_A and secures the scheme against various attacks given in Sect. 3.

Note that if Eve impersonates Alice, she will be detected by Bob in Phase 03, when he checks the received hash value h'_{SK}. However, she may gain some information about what Bob may have done on the particles since he manipulates them according to the pre-shared keys and sends them back to a still unauthenticated Alice. The min-entropy of the key is nevertheless still high enough (See Sect. 3.1 for more details). We propose, thus, that Alice and Bob update the pre-shared keys K_1 and K_2 by performing a privacy amplification on both of them when an attack is suspected or after a certain number of iterations of the protocol, that is, to reduce Eve's information about the pre-shared keys and guarantee that their reusability does not affect the security of the scheme after many iterations. Since privacy amplification reduces the size of the key, we propose to use the hash value of secret keys shared in previous successful executions of the protocol to increase their size.

3 Security analysis

Intuitively, it is important during a key distribution for the shared key to stay secret and known only by the legitimate participants, Alice and Bob. Whenever an attack is suspected, the protocol is aborted and another key is to be shared during another session. On the other hand, it is very important that any leakage of information that occurred during the attack should concern only the key to be shared and not other pre-shared secret keys. In fact, the pre-shared keys are generated and distributed off-line. A

successful attack aiming at them would force Alice and Bob to generate new keys and get to share them in person or via a trusted third party. This would make the following key distribution session meaningless. The pre-shared keys are thus more difficult to be distributed and cannot be changed frequently. They are, in addition, more important than the key to be shared as the secrecy of the latter depends on them.

In QKD, the secrecy of the key to be shared is assured mainly by the laws of quantum physics, since it is in general possible for Alice and Bob to detect intrusions by comparing a subset of the shared key as in the first QKD protocols [4–7]. However, in ASQKD, the secret keys may still be vulnerable to various attacks with a classical Bob. In this section, we analyze the security of the schemes of Yu et al. [9] and Li et al. [12] to justify the improvements brought by our schemes, according to different attacks:

- In the schemes of Yu et al. [9]:
  - K_2 can be recovered with an impersonation attack.
  - K_3 can be recovered with an intercept-resend attack.
  - Encrypted messages can be recovered with a replay attack [13].
- In the randomization-based scheme of Li et al. [12]:
  - K_1 can be recovered with an intercept-resend attack or a Man-in-the-middle attack.
  - SK can be recovered with a Man-in-the-middle attack.
- In the measure-resend scheme of Li et al. [12]:
  - K_1 and K_2 can be recovered with an impersonation attack.

Once the pre-shared keys are successfully recovered, Eve can impersonate one of the two legitimate parties to share a key with the other without being detected.

3.1 Impersonation attack

In this attack, Eve tries to gain secret information by pretending to be Alice or Bob. In both the schemes of Yu et al. [9] and Li et al. [12], as in ours, when Eve pretends to be Bob and communicates with Alice, she cannot obtain any information concerning the key to be shared SK if she does not have the secret pre-shared keys.

3.1.1 Recovering K_1 and K_2 in the measure-resend schemes of Li et al. and Yu et al.

Eve can recover K_2 by performing the attack presented by Meslouhi et al. [13], originally proposed against the measure-resend scheme of Yu et al. [9], on the measure-resend scheme of Li et al. [12]. She can also recover some bits of K_1 by analyzing Bob's behavior toward the particles. To do so,

- Eve pretends to be Alice and prepares a set, S_{EB}, of particles in Bell states of the form

$$|\psi(\alpha)\rangle = \cos(\alpha)|00\rangle + \sin(\alpha)|11\rangle, \tag{4}$$

where $\alpha \in [0, 2\pi]$. She divides each pair of S_{EB} and forms two sequences: S_E, which she keeps, and S_B, which she sends to Bob.

– When receiving a couple of particles, Bob uses K_1 to distinguish between the checking particles, C, and the key particles from which he will extract the shared key, SK. For example, if $K_1^i = 0$, the first particle is a key particle and is measured by Bob, who prepares a clone of it and sends it back to Eve. As for the checking particles, if $K_2^i = 0$, Bob reflects it. Else, he measures it in the Z basis and sends back a clone to Eve.
– For each couple of the received particles, Eve performs an entanglement test based on the technique presented in [14] to recover a bit of K_1 and K_2:

1. If the pair S_B^{2i} and S_E^{2i} are entangled and the pair S_B^{2i+1} and S_E^{2i+1} are not, then Eve knows that the particle S_B^{2i} has been reflected without breaking the entanglement, while the second particle, S_B^{2i+1}, has been measured in the Z basis to extract the shared key SK. Eve concludes that $K_1^i = 1$ and $K_2^i = 0$.
2. If the pair S_B^{2i+1} and S_E^{2i+1} are entangled while the pair S_B^{2i} and S_E^{2i} are not, Eve concludes that the second one has been reflected while the first particle has been measured, and hence, that $K_1^i = 0$ and $K_2^i = 0$.
3. If none of the particles are entangled, then Eve can only conclude that both of the particles have been measured, and hence, that $K_2^i = 1$.

To illustrate this attack, we consider $K_1 = 0101$, $K_2 = 1001$ and $\alpha = \frac{\pi}{4}$. Thus:

– Eve generates the sequence $S_{EB} = |\psi\rangle \ldots |\psi\rangle$ of eight pairs of particles, divides it into S_E and S_B and sends S_B to Bob.
– While Eve sees S_B as a sequence of particles in the maximally mixed state, Bob sees it as a sequence of key (K) and checking (C) particles ordered according to K_1: $S_B = KCCKKCCK$.
– Bob measures all the key particles in the Z basis and only measures the first and last checking particles as determined by K_2.
– When Bob measures the particles in the Z basis, the larger states $|\psi\rangle$ collapses to $|zz\rangle$, where $z \in \{0, 1\}$, while the states of the reflected particles remain unchanged. Thus, $S_{EB} = |zz\rangle|zz\rangle|\psi\rangle|zz\rangle|zz\rangle|\psi\rangle|zz\rangle|zz\rangle$.
– Eve performs her test and recovers K_1 and K_2 as follows:

1. The first and second pairs of particles are not entangled $\Leftrightarrow K_2 = 1 - -$ and $K_1 = - - - -$.
2. The third pair is entangled, while the fourth pair is not $\Leftrightarrow K_2 = 10 - -$ and $K_1 = -1 - -$.
3. The fifth pair is not entangled, while the sixth pair is entangled $\Leftrightarrow K_2 = 100-$ and $K_1 = -10-$.
4. The seventh and eighth pairs are not entangled $\Leftrightarrow K_2 = 1001$ and $K_1 = -10-$.

Whenever Eve can interpret the entanglement test of the received particles as a bit of K_2, she can also recover a bit of K_1 with probability $1/2$. Other iterations of the protocol will permit Eve to fully recover K_2, as in [13], and K_1 as in the intercept-resend attack given in Sect. 3.2.

Table 2 Eve's possible X measurement outcomes

K_1^i	K_2^i	Positions	X measurement outcomes
0	0	CSD	$\|+kl\rangle$ or $\|-kl\rangle$
0	1	DCS	$\|+kl\rangle$ or $\|-kl\rangle$
1	0	CDS	$\|+kl\rangle$
1	1	SCD	$\|+kl\rangle$ or $\|-kl\rangle$

3.1.2 Recovering K_1 and K_2 in our scheme

Since both our schemes do not depend on entanglement, this attack cannot be performed to recover the pre-shared keys. Eve can, nevertheless, try to prepare a special sequence of single particles, send it to Bob, and depending on what she receives back, learn some information about the key:

– *In our measure-resend scheme* Eve can prepare, for example, the sequence $S_{EB} = |+\rangle|+\rangle|+\rangle\cdots|+\rangle$ and send it to Bob. This latter will then, depending on K_1, measure them in the Z basis and send back a clone or reflect them directly. Eve then measures them in the X basis and gets the outcomes given in Table 2.

1. If Eve receives back a sequence of the form $|+\rangle|k\rangle|l\rangle$, where $|k\rangle, |l\rangle \in X$, her measurement outcomes when Bob reflects or measures the particles overlap. She will, thus, not know which operation Bob performed on them.
2. If Eve receives back a sequence of the form $|-\rangle|k\rangle|l\rangle$, she will know that Bob has measured the checking particle. However, she still does not know if $(K_1^i, K_2^i) = (0, 0)$, $(0, 1)$, or $(1, 1)$.

Let ρ_{BE} be the joint state of the system, B, representing a classical bit of the pre-shared key K_1 and, E, representing the quantum information that Eve gathers from her X measurement. Considering K_1 as uniformly distributed, ρ_{BE} is given by

$$\rho_{BE} = \frac{1}{2}|0\rangle\langle 0|_B \otimes \rho_E^0 + \frac{1}{2}|1\rangle\langle 1|_B \otimes \rho_E^1, \tag{5}$$

where

$$\rho_E^0 = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|, \tag{6}$$

and

$$\rho_E^1 = \frac{3}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|. \tag{7}$$

We are interested in calculating the min-entropy defined as

$$H_{\min}(B|E) = -log_2(P_{\text{guess}}(B|E)). \tag{8}$$

In our case,

$$\begin{aligned} P_{\text{guess}}(B|E) &= \max_{\substack{M_0,M_1\geq 0\\ M_0+M_1=I}} \left[\frac{1}{2}tr(M_0\rho_E^0)+\frac{1}{2}tr(M_1\rho_E^1)\right] \\ &= \max_{0\leq M_0\leq I} \left[\frac{1}{2}tr(M_0\rho_E^0)+\frac{1}{2}tr\big((I-M_0)\rho_E^1\big)\right] \\ &= \max_{0\leq M_0\leq I} \left[\frac{1}{2}tr(M_0\rho_E^0)+\frac{1}{2}tr\big((I\rho_E^1)-\frac{1}{2}tr(M_0\rho_E^1)\big)\right] \\ &= \frac{1}{2}+\frac{1}{2}\max_{0\leq M_0\leq I}\left[tr\left(M_0(\rho_E^0-\rho_E^1)\right)\right] \\ &= \frac{1}{2}+\frac{1}{2}\max_{0\leq M_0\leq I}\left[tr\big(M_0\big(-\frac{1}{4}|+\rangle\langle+|+\frac{1}{4}|-\rangle\langle-|\big)\big)\right]. \end{aligned} \tag{9}$$

Note that the maximum is reached for $M_0 = |-\rangle\langle-|$. Thus,

$$P_{\text{guess(B|E)}} = \frac{5}{8}. \tag{10}$$

Finally, the min-entropy is $H_{\min}(B|E) \approx 0.67$, which is high enough [15] for Alice and Bob to perform a privacy amplification protocol to obtain new uniform pre-shared keys.

– *In our randomization-based scheme* Eve can prepare the sequence $S_{EC} = |1\rangle|0\rangle|0\rangle\cdots|0\rangle$, in which $|1\rangle$ is used as a flag and put in the same position as the targeted bit, similar to the attack explained in [13] against the randomization-based scheme of Yu et al. [9]. Eve sends S_{EC} to Bob, who will measure some particles and reflect back the others after reordering them. If the flag particle is missing from the reflected particles, Eve will know that Bob has measured the first particle and she will thus gain the first qubit of K_{HT}. However, unlike the randomization-based scheme of Yu et al. [9], other iterations of the process with different positions of the flag will not give additional information to Eve since K_{HT} is updated before each iteration of the protocol. Eve could increase the number of flags in the sequence; however, the reordering of the reflected particles prevents her from knowing which particles have been reflected. Note that even if Eve recovers an important part of K_{HT}, the pre-shared secret key K_1 is still secure due to universal hashing.

3.2 Intercept-resend attack

In this attack, a classical Eve aims to gain some information about the secret keys by intercepting the transmitted messages between Alice and Bob.

3.2.1 Recovering K_1 in the randomization-based scheme of Li et al.

In the randomization-based scheme of Li et al. [12], Eve can theoretically get half of the secret key K_1 in a single iteration. Other iterations of the scheme will allow her to fully recover the secret key K_1. For this purpose,

- Eve intercepts each transmitted particle of S_{AC} from Alice to Bob and measures them in the Z basis. She forms the classical sequence R, generates a corresponding sequence of particles QR, and sends them to Bob.
- Bob measures the S_A particles to extract the key and checks the sender's identity. Note that Eve's measurement will not modify the state of the S_A particles. Eve will, thus, not be detected by Bob and the checking particles will be reflected back to Alice.
- These latter reflected particles will be intercepted and measured again in the Z basis by Eve, who can then compare their positions in her first and second measurement results to gain many bits of the secret key K_1. If in Eve's first measurement result $R_i \neq R_{i+1}$ and Bob reflects the particle corresponding to R_i (R_{i+1}), Eve will know that the checking particle was placed by Alice in front (in the back) of the key particle. She will then recover a bit of K_1.

We have simulated this attack on the randomization-based scheme of Li et al. [12] and our scheme. As shown in Fig. 3, about half of the secret key K_1 is recovered in the first iteration of the scheme of Li et al. [12]. Upon the 3^{rd} iteration, about 88% of the secret key can be recovered. Thus, on the 4th iteration of the scheme, Eve can use those recovered bits of the secret key K_1 to aim at some of the S_A particles and discover

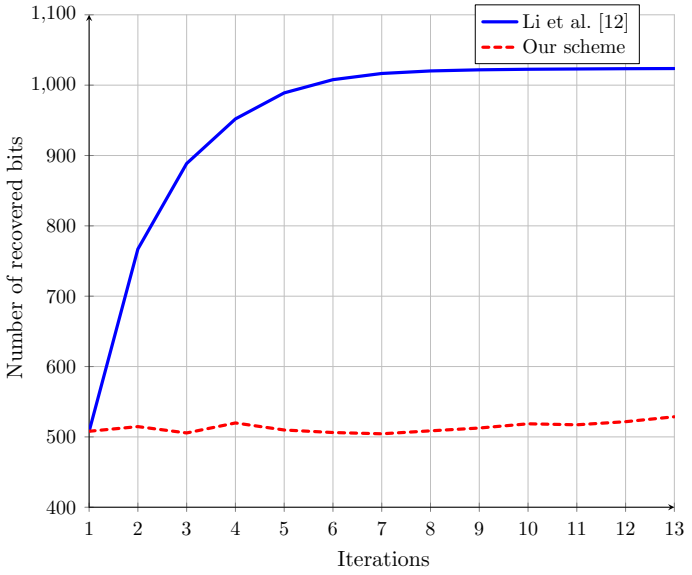

Fig. 3 Number of iterations to fully recover the 1024 key bits of K_1 in [12] and K_{HT} in our scheme

88% of the shared secret key SK with which she can recover encrypted information without being detected by Alice or Bob.

3.2.2 Recovering K_1 in our schemes

- *In our randomization-based scheme*, reordering the checking particles before sending them back prevents Eve from distinguishing between the checking particles and the key particles, and hence, from recovering K_{HT}. Executing the proposed attack on our randomization-based scheme is equivalent to guessing bit by bit the hash value of the secret key without knowing with certainty which are the correct bits and which are the wrong ones in each iteration.
- *In our measure-resend scheme*, if Eve intercepts the particles and measures them, she will be detected by Alice and Bob. Similar to the impersonation attack presented in Sect. 3.1, Eve would know, in some cases, when Bob measures the particles by comparing the sent and received sequences. However, the min-entropy of K_1 and K_2 will be still high enough to perform a privacy amplification and reduce Eve's knowledge about them.

3.2.3 Recovering K_3 in the schemes of Yu et al.

An intercept-resend attack can also be performed against the schemes of Yu et al. [9] to recover the pre-shared key K_3. An example of this attack is given in [13].

- *In the randomization scheme of Yu et al.* [9],

  1. Eve first intercepts the particles sent by Alice to Bob and, assuming that K_2 has already been recovered following the impersonation attack of Meslouhi et al. [13], she measures the particles in the Z basis when $K_2^i = 0$ to form the classical sequence MR_E representing her measurement outcomes. She generates new qubits in the same state to replace the measured ones before forwarding the intercepted particles to Bob.
  2. Bob measures the same particles as Eve and forms the same sequence as her ($MR_B = MR_E$) since they have the same K_2. He then reorders the remaining particles and sends them back to Alice.
  3. According to Bob's reordering, which he announces publicly, Alice will either check for Eve's presence by performing a Bell state measurements on her stored particles and the received ones, or measure the remaining stored particles to form $MR_A = MR_B = MR_E$.
  4. According to the key K_3, Alice will then extract from MR_A the classical secret key SK and a classical checking sequence MR_C.
  5. When Alice sends the sequence MR_C to Bob, Eve will intercept it and will follow the algorithm described in [13] to build a set of all possible keys $K_{3,i}$ satisfying
  $$MR_E \oplus K_3 = MR_C, \tag{11}$$
  where $\oplus$ represents the function used by Alice to extract MR_C from $MR_A = MR_E$.

6. To obtain the final pre-shared key, K_3, in the randomization-based scheme of Yu et al. [9], Eve will have to build new sets of possible $K_{3,i}$ according to different MR_E and MR_C sequences from different iterations of the attack until the intersection of these sets narrows down to K_3.

$$\{K_{3,1}, K_{3,2}, \ldots\}_1 \cap \{K_{3,1}, K_{3,2}, \ldots\}_2 \cap \ldots = \{K_3\}. \tag{12}$$

– *In the measure-resend scheme of Yu et al.* [9], Eve can only make a partial form of K_3 with at least $N/4$ exactly positioned bits of value 1 [13]. This is because Alice keeps secret half of the checking sequence, corresponding to the first half of the secret key of value 1, for entanglement correlation tests, and sends publicly the other half, MR_C, to Bob. Nevertheless, given a partial K_3, Eve can gain partial information about the subsequent shared keys SK with which she can partially decrypt a message encrypted with SK and, in some cases, recover the whole message.

3.3 Man-in-the-middle attack

In the Man-in-the-middle attack, Eve initiates two sessions of the protocol: in one session, she impersonates Alice to Bob and in another, she impersonates Bob to Alice.

3.3.1 Recovering K_1 and SK in the randomization-based scheme of Li et al.

With this attack, Eve can successfully share a secret key with Bob in the randomization-based scheme of Li et al. [12] without having any information about the pre-shared key, K_1. To do so,

– Eve first pretends to be Bob and initiates a session of the protocol with Alice.
– When Eve receives the particles from Alice, she measures them all in the Z basis and saves the corresponding bit sequence, R, in her classical memory.
– Eve terminates her session with Alice and initiates another one with Bob pretending to be Alice.
– She generates a sequence, QR, of particles in the Z basis representing R and sends it to Bob.
– According to K_1, Bob either measures some particles of QR in the Z basis to extract SK and $H(SK||K_1)$, or reflects back what he thinks to be checking particles. Note that Eve's measurement did not alter SK nor $H(SK||K_1)$. Therefore, when Bob checks the identity of the sender, the result will be positive and Eve can, thus, successfully pretend to be Alice without knowing K_1.
– Depending on which particles are reflected back, Eve will also know the initial position of some checking particles and will recover K_1 following the same steps as in the intercept-resend attack presented in Sect. 3.2.
– She also completely recovers the remaining fraction of SK by comparing the measurement result, MR, of the received particles with the sequence R.

1. If $R_{2i} = R_{2i+1}$, then SK_i is simply R_{2i}, independently of the position of the checking particle.

2. If $R_{2i} \neq R_{2i+1}$, Eve measures the reflected particle and performs a bit flip operation on the resulted bit.

Once Eve has complete knowledge of SK, she can gain private information from Bob without his knowledge. Eve can also recover a bit of K_1 whenever $R_{2i} \neq R_{2i+1}$, which occurs 50% of the time, since she will know the position of the checking particle in relation to the key particle. When Eve completely recovers K_1 by repeating the process few times (see Fig. 3), she can also gain private information from Alice by impersonating Bob and sharing a secret key with her.

To illustrate this attack, we consider $K_1 = 11{,}0010$, $SK = 1010$, $H(SK||K_1) = 10$, and $C = |+\rangle|-\rangle|0\rangle|1\rangle|0\rangle|+\rangle$. Thus:

– Firstly, Eve impersonates Bob and initiates a session with Alice:

1. Alice will send the sequence

$$S_A = |+1\rangle_1|-0\rangle_2|10\rangle_3|01\rangle_4|01\rangle_5|0+\rangle_6, \tag{13}$$

where $|ab\rangle_i$ is the i-th pair of key and checking particles.
2. Eve measures the sequence S_A and obtains the bit sequence

$$R = (a1)_1(b0)_2(10)_3(01)_4(01)_5(0c)_6, \tag{14}$$

where $a, b, c \in \{0, 1\}$ and the notation $(ab)_i$ is used only for the sake of distinguishing between the pairs of key and checking particles. For convenience, we consider $abc = 000$. Thus,

$$R = (01)_1(00)_2(10)_3(01)_4(01)_5(00)_6. \tag{15}$$

– Secondly, Eve impersonates Alice and initiates a session with Bob:

1. Eve generates in the Z basis a sequence QR of particles corresponding to R:

$$QR = |01\rangle_1|00\rangle_2|10\rangle_3|01\rangle_4|01\rangle_5|00\rangle_6, \tag{16}$$

which she sends to Bob.
2. According to K_1, Bob reflects back the checking particles and measures in the Z basis the key particles from each pair. The key particles correspond to the underlined particles of the sequence

$$QR = |0\underline{1}\rangle_1|0\underline{0}\rangle_2|\underline{1}0\rangle_3|\underline{0}1\rangle_4|0\underline{1}\rangle_5|\underline{0}0\rangle_6. \tag{17}$$

He thus obtains $SK = 1010$ and $h_{SK} = 10$.
3. Bob calculates the hash value and obtains $H(SK||K_1) = h_{SK}$ since the Z measurements of Eve did not alter the states of the key particles.
4. Eve measures the received particles and obtains the bit sequence

$$MR = 000100. \tag{18}$$

Table 3 Recovering SK and K_1

R	0	1	0	0	1	0	0	1	0	1	0	0
MR	0		0			0		1	0		0	
$SK\|\|h_{SK}$		1	0		1		0			1	0	
K_1	1		–		0		0		1		–	

5. She then compares R with MR:
   - Since in $(01)_1$, the bits are different and the first particle $MR_1 = 0$ was reflected, then she deduces that $SK = 1$ and $K_1 = 1$.
   - Since in $(00)_2$, the bits are similar, then $SK = MR_2 = 0$.
   - The following deductions are given in Table 3.

3.3.2 Recovering K_1 and SK in our schemes

In our randomization-based scheme, reordering the checking particles C before reflecting them back will prevent Eve from recovering K_{HT} and, consequently, from knowing which were checking particles and which were key particles.

As for the measure-resend scheme,

- If Eve follows the same strategy as in the randomization-based scheme and measures the sequence received by Alice in the Z basis, she will receive back exactly the same sequence from Bob, and will, therefore, gain nothing from him about neither SK nor K_{HT}. Although the authentication holds in Bob's side, Eve will gain nothing about the messages encrypted with different SKs received from Bob.
- Suppose now that Eve measures all the particles received from Alice in the X basis and sends them to Bob. This latter will either measure them or reflect them back. When he verifies the hash value of the received particles, he will abort the protocol since SK and $H(SK||K_1)$ have been altered. Following the same idea as in the impersonation attack scenario in Sect. 3.1, Eve will know in some cases when Bob has measured the checking particle. In these cases, she still will not be able to deduce K_1 and K_2 and their min-entropy will remain high enough for performing a privacy amplification.

3.4 Replay attack

In the schemes of Yu et al. [9], Eve can successfully recover SK with a replay attack presented in [13] by first intercepting information between Alice and Bob and reuse it in subsequent key distribution sessions.

- In a first session,
  1. Eve intercepts the particles sent from Alice to Bob.
  2. According to a previously recovered K_2, she either forwards the particles directly to Bob or measures the particles in the Z basis, form the sequence MR_E and replace the particles by clones.

3. Later in the same session, when Alice sends the checking sequence MR_C to Bob, Eve will intercept it, store a copy in her memory and forward the original sequence to Bob.

– Once the session between Alice and Bob is terminated, Eve can generate a sequence S where the particles of the previously obtained MR_E are placed in the positions corresponding to $K_2^i = 0$ and particles in random states are placed in the remaining positions, corresponding to $K_2^i = 1$.
– In a second session,

1. Eve impersonates Alice to Bob and sends him S.
2. Bob will extract $MR_B = MR_E$ from S according to K_2 and sends back the reordered remaining particles.
3. Eve, when still pretending to be Alice, will ask for the order of the particles. Once she receives it, she will declare, without performing any check, that the checking process was correct and send the previously intercepted MR_C to Bob.
4. Since the MR_C was correctly extracted from MR_E by Alice using the right K_3, the checking process will be successful in Bob's side. He will then accept to use the received SK.

When Eve receives a message encrypted with SK from Bob, she stores it and initiates another ASQKD session with him where she uses the same MR_E and MR_C with different random particles and forces Bob to accept again the use of SK. Given that the security of the one-time pad ciphering algorithm requires SK to be used only once, if Bob sends a second encrypted message using again SK, the secrecy of the messages will be compromised [16].

3.4.1 Recovering *SK* with a replay attack in our scheme

– *In our randomization-based scheme,* Eve cannot force Bob to accept the same key SK by manipulating the S_A sequence transmitted from Alice to Bob since she does not know K_{HT}, which would allow her to distinguish between S_A and the checking particles. Eve can, nevertheless, intercept all the sequence S_{AC}, measure it in the Z basis and store it. Later, she will impersonate Alice and sends to Bob a sequence of particles according to her measurement outcomes. However, due to the use of a different K_{HT}, Bob will extract a different SK and a non-corresponding h_{SK}. He will then abort the protocol.
– *In our measure-resend scheme,* Eve follows this same strategy and intercepts the sequence S_{ACD} transmitted from Alice to Bob. If she measures the sequence in the Z or X basis, Alice's tests on the checking particles or Bob's tests on the hash values will not hold. They will thus abort the protocol and will perform a privacy amplification on K_1 and K_2. Therefore, with new pre-shared keys, replaying the sequence S_{ACD} in another session will not allow Eve to force Bob or Alice into using the key SK concealed in S_{ACD}.

4 Conclusion

Although semi-quantum key distribution has alleviated the challenge of implementing quantum cryptography, it did not improve its security against attacks aiming at the identity of the legitimate parties. Authenticated SQKD schemes have been proposed to secure the communication against various attacks aiming at the identity of the participants. In this paper, we have proposed an ASQKD scheme with two variants: a randomization-based ASQKD and a measure-resend one. The two schemes are simplified and more secure compared to the schemes of Li et al. [12] and Yu et al. [9]. In fact, in the security analysis, we have described how a classical Eve can recover the secret key, SK, in the scheme of Li et al. [12], through a Man-in-the-middle attack and how she can also force Bob to use the same key, SK, more than once [13] in the scheme of Yu et al. [9], which compromises the security of the encrypted messages. We have also demonstrated that even though some attacks may lead Alice and Bob to abort the protocol, information about the pre-shared keys can be gained and used in other iterations of the scheme to gain more information about the secret key SK. Through this security analysis, we have proven the reliability of our scheme to secure the key distribution against the presented attacks.

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Sci. Stat. Comput. **26**, 1484 (1997)
2. Rivest, R., Shamir, A., Adelman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
3. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inform. Theory **22**, 644–654 (1976)
4. Bennett, C.H., Brassard, G.: Quantum cryptography, Public key distribution and coin tossing. In: International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179 (1984)
5. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
6. Bechmann-Pasquinucci, H., Gisin, N.: Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. Phys. Rev. A **59**, 4238 (1999)
7. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**, 557 (1992)
8. Miller, F.: Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams. C.M. Cornwell, New York (1882)
9. Yu, K.F., Yang, C.W., Liao, C.H., Hwang, T.: Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf. Process. **13**, 1457 (2014)
10. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A **79**, 032341 (2009)
11. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. Phys. Rev. Lett. **99**, 140501 (2007)
12. Li, C.M., Yu, K.F., Kao, S.H., Hwang, T.: Authenticated semi-quantum key distribution without classical channel. Quantum Inf. Process. **15**, 2881 (2016)
13. Meslouhi, A., Hassouni, Y.: Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf. Process. **16**, 18 (2017)
14. Barbieri, M., De Martini, F., Di Nepi, G., Mataloni, P., D'Ariano, G.M., Macchiavello, C.: Detection of entanglement with polarized photons: experimental realization of an entanglement witness. Phys. Rev. Lett. **91**, 227901 (2003)

15. Aggrawal, D., Dodis, Y., Jafargholi, Z., Miles, E., Reyzin, L.: Amplifying Privacy in Privacy Amplification, Advances in Cryptology–CRYPTO 2014, pp. 183–198. Springer, Berlin (2014)
16. Benson, R.L., Warner, M.: Venona: Soviet Espionage and the American Response 1939–1957, 1st edn. NSA-Central Intelligence Agency, Maryland (1996)