Theoretical Computer Science 801 (2020) 96–109

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Composable security against collective attacks of a modified BB84 QKD protocol with information only in one basis [☆]

Michel Boyer [a], Rotem Liss [b,*], Tal Mor [b]

[a] Département IRO, Université de Montréal, Montréal (Québec) H3C 3J7, Canada
[b] Computer Science Department, Technion, Haifa 3200003, Israel

ARTICLE INFO

Article history:
Received 14 February 2018
Accepted 11 August 2019
Available online 16 August 2019
Communicated by S. Hallgren

Keywords:
Collective attacks
Quantum key distribution
Cryptography
Error rate
Test bits
Information bits

ABSTRACT

Quantum Cryptography uses the counter-intuitive properties of Quantum Mechanics for performing cryptographic tasks in a secure and reliable way. The Quantum Key Distribution (QKD) protocol BB84 has been proven secure against several important types of attacks: collective attacks and joint attacks. Here we analyze the security of a modified BB84 protocol, for which information is sent only in the z basis while testing is done in both the z and the x bases, against collective attacks. The proof follows the framework of a previous paper [1], but it avoids a classical information-theoretical analysis and proves a fully composable security. We show that this modified BB84 protocol is as secure against collective attacks as the original BB84 protocol, and that it requires more bits for testing.

1. Introduction

Cryptography is the science of protecting the security and correctness of data against adversaries. One of the most important cryptographic problems is the problem of *encryption* – namely, of transmitting a secret message from a sender to a receiver. Two main encryption methods are used today:

1. In symmetric-key cryptography, the same *secret key* is used for both the sender and the receiver: the sender uses the secret key for encrypting his or her message, and the receiver uses the same secret key for decrypting the message. Examples of symmetric-key ciphers include the Advanced Encryption Standard (AES) [3], the older Data Encryption Standard (DES), and one-time pad ("Vernam cipher").
2. In public-key cryptography [4], a *public key* (known to everyone) and a *secret key* (known only to the receiver) are used: the sender uses the public key for encrypting his or her message, and the receiver uses the secret key for decrypting the message. Examples of public-key ciphers include RSA [5] and elliptic curve cryptography.

One of the main problems with current public-key cryptography is that its security is usually not formally proved. Moreover, its security relies on the computational hardness of specific computational problems, such as integer factorization and discrete logarithm (that can both be efficiently solved on a quantum computer, by using Shor's factorization algorithm [6];

[☆] A preliminary version of this paper appeared in *Proceedings of the 2nd International Conference on Complexity, Future Information Systems and Risk – COMPLEXIS, 24–26 April, 2017, Porto, Portugal* [2].

[*] Corresponding author.
E-mail addresses: boyer@iro.umontreal.ca (M. Boyer), rotemliss@cs.technion.ac.il (R. Liss), talmo@cs.technion.ac.il (T. Mor).

https://doi.org/10.1016/j.tcs.2019.08.014
0304-3975/© 2019 Elsevier B.V. All rights reserved.

therefore, if a scalable quantum computer is successfully built in the future, the security of many public-key ciphers, including RSA and elliptic curve cryptography, will be broken). Symmetric-key cryptography requires a secret key to be shared *in advance* between the sender and the receiver (in other words, if the sender and the receiver want to share a secret message, they must share a secret key beforehand). Moreover, no security proofs for many current symmetric-key ciphers, such as AES and DES, are known (even if one is allowed to rely on the computational hardness of problems), and unconditional security proofs against computationally-unlimited adversaries are impossible unless the secret key is used only once and is at least as long as the secret message [7].

The one-time pad (symmetric-key) cipher, that, given a message M and a secret key K of the same length, defines the encrypted message C to be $C = M \oplus K$ (and then decryption can be performed by computing $M = C \oplus K$), is fully and unconditionally secure against any adversary [7]: namely, even if the adversary Eve intercepts the encrypted message C, she gains no information about the original message M (assuming that she has no information about the secret key K). This means that, for obtaining perfect secrecy, all that is needed is an efficient way for sharing a random secret key between the sender and the receiver; unfortunately, "classical key distribution" cannot be achieved in a fully secure way if the adversary can listen to all the communication between the sender and the receiver.

Quantum key distribution (QKD) protocols take advantage of the laws of quantum mechanics for achieving fully and unconditionally secure key distribution, so that their resulting final key can later be used by other cryptographic primitives (e.g., one-time pad encryption). Most of the QKD protocols have security proofs applicable even against adversaries whose only limitations are the laws of nature (and who are otherwise capable of solving any computational problem and of performing any physically-allowed operation). The two parties (the first party is usually named "Alice", and the second party is usually named "Bob") want to create a shared random key, and they use an insecure quantum channel and an unjammable classical channel (to which the adversary may listen, but not interfere). The adversary (eavesdropper), Eve, tries to get as much information as she can on the final shared key. The first and most important QKD protocol is BB84 [8], that uses four possible quantum states (see details below), and it has been proven fully and unconditionally secure.

Boyer, Gelles, and Mor [1] discussed the security of BB84 against collective attacks. The class of the "collective attacks" [9–11] is an important and powerful subclass of the joint attacks; the class of the "joint attacks" includes all the theoretical attacks allowed by quantum physics. [1] improved the security proof of Biham, Boyer, Brassard, van de Graaf, and Mor [11] against collective attacks, by using some techniques of Biham, Boyer, Boykin, Mor, and Roychowdhury [12] (that proved security against joint attacks). In this paper, too, we restrict the analysis to collective attacks, because security against collective attacks is conjectured (and, in some security notions, proved [13,14]) to imply security against joint attacks. In addition, proving security against collective attacks is much simpler than proving security against joint attacks.

Other QKD protocols, either similar to BB84 or ones that use different approaches, have also been suggested, and in some cases have also been proven fully secure. In particular, the "three-state protocol" [15] uses only three quantum states, and it has been proven secure [16–18]; the "classical Bob" protocol [19] is a two-way protocol such that only Alice has quantum capabilities and Bob has only classical capabilities, and it has been proven robust [19] and secure [20]; and the "classical Alice" protocol [21] is similar to "classical Bob" with Alice being the classical participant instead of Bob, and it has been proven robust [22].

The above QKD protocols are all "Discrete-Variable" protocols. Two other classes of QKD protocols, "Continuous-Variable" protocols and "Distributed-Phase-Reference" protocols, have also been suggested; their security proofs are still weaker than the security proofs of "Discrete-Variable" protocols (see [23] for details).

QKD protocols can be used as a subroutine (secure key distribution) of more complicated cryptographic protocols. In other words, they can be integrated into a system in order to improve its security. See [24] for more details about this integration and about the practical usability of QKD compared to other methods.

In many QKD protocols, including BB84, Alice and Bob exchange several types of bits (encoded as quantum systems, usually qubits): INFO bits, that are secret bits shared by Alice and Bob and are used for generating the final key (via classical processes of error correction and privacy amplification); and TEST bits, that are publicly exposed by Alice and Bob (by using the classical channel) and are used for estimating the error rate. In BB84, each bit is sent from Alice to Bob in a random basis (the z basis or the x basis).

In this paper, we extend the analysis of BB84 done in [1] and prove the security of a QKD protocol we shall name *BB84-INFO-z*. This protocol is almost identical to BB84, except that all its INFO bits are in the z basis. In other words, the x basis is used only for testing. The bits are thus partitioned into three disjoint sets: INFO, TEST-Z, and TEST-X. The sizes of these sets are arbitrary (n INFO bits, n_z TEST-Z bits, and n_x TEST-X bits).

We note that, while this paper follows a line of research that mainly discusses a specific approach of security proof for BB84 and similar protocols (this approach, notably, considers finite-key effects and not only the asymptotic error rate), many other approaches have also been suggested: see for example [25,26,13,27]. For comparison, see Section 4.

In the other papers ([9–12,1]) that discussed the same approach of security proofs as discussed here, the classical mutual information between Eve and the final key was calculated and bounded, which caused problems with composability (see definition in [13] and in Subsection 1.1). In contrast to those papers, in this paper we suggest a method to prove a fully composable security – namely, to calculate and bound the trace distance between the quantum state at the end of the real protocol and the quantum state at the end of an ideal protocol. This method is fully composable, because it bounds the distance between *quantum* states instead of bounding the *classical* information Eve has (bounding the classical information means, in particular, that we assume that Eve measures at the end of the protocol, while in reality she is not required to measure then, but is allowed to wait until Alice and Bob use the final key). This method is implemented in this paper for proving the fully composable security of BB84-INFO-z against collective attacks; it also directly applies to the BB84 security proof in [1] against collective attacks, proving the fully composable security of BB84 against collective attacks. It may be extended in the future to show that the BB84 security proof of [12] proves the fully composable security of BB84 against joint attacks. (We note that in the conference version of this paper [2], we used a weaker security definition: it was not sufficient for proving fully composable security, but it was more composable than in the previous papers.)

The "qubit space", $\mathcal{H}_2$, is a 2-dimensional Hilbert space. The states $|0^0\rangle, |1^0\rangle$ form an orthonormal basis of $\mathcal{H}_2$, called "the computational basis" or "the z basis". The states $|0^1\rangle \triangleq \frac{|0^0\rangle+|1^0\rangle}{\sqrt{2}}$ and $|1^1\rangle \triangleq \frac{|0^0\rangle-|1^0\rangle}{\sqrt{2}}$ form another orthonormal basis of $\mathcal{H}_2$, called "the x basis". Those two bases are said to be *conjugate bases*.

In this paper, we denote bit strings (of t bits, with $t \geq 0$ being some integer) by a bold letter (e.g., $\mathbf{i} = i_1 \dots i_t$ with $i_1, \dots, i_t \in \{0,1\}$); and we refer to those bit strings as elements of $\mathbf{F}_2^t$ – that is, as elements of a t-dimensional vector space over the field $\mathbf{F}_2 = \{0,1\}$, where addition of two vectors corresponds to a XOR operation between them. The number of 1-bits in a bit string $\mathbf{s}$ is denoted by $|\mathbf{s}|$, and the Hamming distance between two strings $\mathbf{s}$ and $\mathbf{s}'$ is $d_H(\mathbf{s}, \mathbf{s}') = |\mathbf{s} + \mathbf{s}'|$.

1.1. Security definitions of quantum key distribution

Originally, a QKD protocol was defined to be secure if the (classical) *mutual information* between Eve's information and the final key, maximized over all the possible attack strategies and measurements by Eve, is exponentially small in the number of qubits, N. Examples of security proofs of BB84 that use this security definition are [25,12,26]. Those security proofs used the observation that one cannot analyze the *classical* data held by Eve before privacy amplification (as done in [28]), but must analyze the *quantum* state held by Eve [29]. In other words, they assumed that Eve could keep her quantum state until the end of the protocol, and only *then* choose the optimal measurement (based on all the data she observed) and perform the measurement.

Later, it was noticed that this security definition may not be "composable". In other words, the final key is secure if Eve measures the quantum state she holds at the end of the QKD protocol, but the proof does not apply to *cryptographic applications* (e.g., encryption) of the final key: Eve might gain non-negligible information after the key is used, even though her information on the key itself was negligible. This means that the proof is not sufficient for practical purposes. In particular, those applications may be insecure if Eve keeps her quantum state until Alice and Bob use the key (thus giving Eve some new information) and only *then* measures.

Therefore, a new notion of "(composable) full security" was defined [30,27,13] by using the trace distance between quantum states, following universal composability definitions for non-quantum cryptography [31,32]. Intuitively, this notion means that the final joint quantum state of Alice, Bob, and Eve at the end of the protocol is *very close* (namely, the trace distance is exponentially small in N) to their final state at the end of an *ideal* key distribution protocol, that distributes a *completely random* and *secret* final key to both Alice and Bob. In other words, if a QKD protocol is secure, then except with an exponentially small probability, one of the two following events happens: the protocol is aborted, *or* the secret key generated by the protocol is the same as a perfect key that is uniformly distributed (i.e., each possible key having the same probability), is the same for both parties, and is independent of the adversary's information.

Formally, ρ_{ABE} is defined as the final quantum state of Alice, Bob, and Eve at the end of the protocol (with Alice's and Bob's states being simply the "classical" states $|k_A\rangle_A$ and $|k_B\rangle_B$, where k_A and k_B are bit strings that are the final keys held by Alice and Bob, respectively (note that usually $k_A = k_B$); and with Eve's state including both her quantum probe and the classical information published in the unjammable classical channel); ρ_U is defined as the complete mixture of all the possible keys that are the same for Alice and Bob (namely, if the set of possible final keys is K, then $\rho_U = \frac{1}{|K|}\sum_{k\in K}|k\rangle_A|k\rangle_B\langle k|_A\langle k|_B$); and ρ_E is defined as the partial trace of ρ_{ABE} over the system AB. For the QKD protocol to be fully (and composably) secure, it is required that

$$\frac{1}{2}\operatorname{tr}|\rho_{ABE} - \rho_U \otimes \rho_E| \leq \epsilon, \tag{1}$$

where ϵ is exponentially small in N. Intuitively, ρ_{ABE} is the *actual* joint state of Alice, Bob, and Eve at the end of the QKD protocol; ρ_U is the *ideal* final state of Alice and Bob (an equal mixture of all the possible final keys, that is completely uncorrelated with Eve and is the same for Alice and Bob); and ρ_E is the state of Eve, uncorrelated with the states of Alice and Bob. Note that cases in which the protocol is aborted are represented by the zero operator: see [13, Subsection 6.1.2] for details.

Composable security of many QKD protocols, including BB84, has been proved [30,27,13].

2. Full definition of the "BB84-INFO-z" protocol

Below we formally define all the steps of the BB84-INFO-z protocol, as used in this paper.

1. Before the protocol, Alice and Bob choose some shared (and public) parameters: numbers n, n_z, and n_x (we denote $N \triangleq n + n_z + n_x$), error thresholds $p_{a,z}$ and $p_{a,x}$, an $r \times n$ parity check matrix P_C (corresponding to a linear error-correcting

code C), and an $m \times n$ privacy amplification matrix P_K (representing a linear key-generation function). It is required that *all* the $r+m$ rows of the matrices P_C and P_K put together are linearly independent.

2. Alice randomly chooses a partition $\mathcal{P} = (\mathbf{s}, \mathbf{z}, \mathbf{b})$ of the N bits by randomly choosing three N-bit strings $\mathbf{s}, \mathbf{z}, \mathbf{b} \in \mathbf{F}_2^N$ that satisfy $|\mathbf{s}| = n$, $|\mathbf{z}| = n_z$, $|\mathbf{b}| = n_x$, and $|\mathbf{s}+\mathbf{z}+\mathbf{b}| = N$. Thus, $\mathcal{P}$ partitions the set of indexes $\{1, 2, ..., N\}$ into three disjoint sets:
   - I (INFO bits, where $s_j = 1$) of size n;
   - T_Z (TEST-Z bits, where $z_j = 1$) of size n_z; and
   - T_X (TEST-X bits, where $b_j = 1$) of size n_x.
3. Alice randomly chooses an N-bit string $\mathbf{i} \in \mathbf{F}_2^N$ and sends the N qubit states $|i_1^{b_1}\rangle, |i_2^{b_2}\rangle, \ldots, |i_N^{b_N}\rangle$, one after the other, to Bob using the quantum channel. Notice that Alice uses the z basis for sending the INFO and TEST-Z bits, and that she uses the x basis for sending the TEST-X bits. Bob keeps each received qubit in quantum memory, not measuring it yet.[1]
4. Alice sends to Bob over the classical channel the bit string $\mathbf{b} = b_1 \ldots b_N$. Bob measures each of the qubits he saved in the correct basis (namely, when measuring the i-th qubit, he measures it in the z basis if $b_i = 0$, and he measures it in the x basis if $b_i = 1$).
   The bit string measured by Bob is denoted by $\mathbf{i}^B$. If there is no noise and no eavesdropping, then $\mathbf{i}^B = \mathbf{i}$.
5. Alice sends to Bob over the classical channel the bit string $\mathbf{s}$. The INFO bits (that will be used for creating the final key) are the n bits with $s_j = 1$, while the TEST-Z and TEST-X bits (that will be used for testing) are the $n_z + n_x$ bits with $s_j = 0$. We denote the substrings of $\mathbf{i}, \mathbf{b}$ that correspond to the INFO bits by $\mathbf{i_s}$ and $\mathbf{b_s}$, respectively.
6. Alice and Bob both publish the bit values they have for all the TEST-Z and TEST-X bits, and they compare the bit values. If more than $n_z \cdot p_{a,z}$ TEST-Z bits are different between Alice and Bob *or* more than $n_x \cdot p_{a,x}$ TEST-X bits are different between them, they abort the protocol. We note that $p_{a,z}$ and $p_{a,x}$ (the pre-agreed error thresholds) are the maximal allowed error rates on the TEST-Z and TEST-X bits, respectively – namely, in each basis (z and x) separately.
7. The values of the remaining n bits (the INFO bits, with s_j =1) are kept in secret by Alice and Bob. The bit string of Alice is denoted $\mathbf{x} = \mathbf{i_s}$, and the bit string of Bob is denoted $\mathbf{x}^B$.
8. Alice sends to Bob the *syndrome* of $\mathbf{x}$ (with respect to the error-correcting code C and to its corresponding parity check matrix P_C), that consists of r bits and is defined as $\boldsymbol{\xi} = \mathbf{x} P_C^{\mathrm{T}}$. By using $\boldsymbol{\xi}$, Bob corrects the errors in his $\mathbf{x}^B$ string (so that it is the same as $\mathbf{x}$).
9. The final key consists of m bits and is defined as $\mathbf{k} = \mathbf{x} P_K^{\mathrm{T}}$. Both Alice and Bob compute it.

The protocol is defined similarly to BB84 (and to its description in [1]), except that it uses the generalized bit numbers n, n_z, and n_x (numbers of INFO, TEST-Z, and TEST-X bits, respectively); that it uses the partition $\mathcal{P} = (\mathbf{s}, \mathbf{z}, \mathbf{b})$ for dividing the N-bit string $\mathbf{i}$ into three disjoint sets of indexes (I, T_Z, and T_X); and that it uses two separate thresholds ($p_{a,z}$ and $p_{a,x}$) instead of one (p_a).

3. Proof of security for the BB84-INFO-*z* protocol against collective attacks

3.1. The general collective attack of Eve

Before the QKD protocol is performed (and, thus, independently of $\mathbf{i}$ and $\mathcal{P}$), Eve chooses some collective attack to perform. A *collective attack* is bitwise: it attacks each qubit separately, by using a separate probe (ancillary state). Each probe is attached by Eve to the quantum state, and Eve saves it in a quantum memory. Eve can keep her quantum probes indefinitely, even after the final key is used by Alice and Bob; and she can perform, at any time of her choice, an optimal measurement of all her probes together, chosen based on all the information she has at the time of the measurement (including the classical information sent during the protocol, and including the information she acquires when Alice and Bob use the key).

Given the j-th qubit $|i_j^{b_j}\rangle_{T_j}$ sent from Alice to Bob ($1 \le j \le N$), Eve attaches a probe state $|0^E\rangle_{E_j}$ and applies some unitary operator U_j of her choice to the compound system $|0^E\rangle_{E_j}|i_j^{b_j}\rangle_{T_j}$. Then, Eve keeps to herself (in a quantum memory) the subsystem E_j, which is her probe state; and sends to Bob the subsystem T_j, which is the qubit sent from Alice to Bob (which may have been modified by her attack U_j).

The most general collective attack U_j of Eve on the j-th qubit, represented in the orthonormal basis $\{|0^{b_j}\rangle_{T_j}, |1^{b_j}\rangle_{T_j}\}$, is

$$U_j|0^E\rangle_{E_j}|0^{b_j}\rangle_{T_j} = |E_{00}^{b_j}\rangle_{E_j}|0^{b_j}\rangle_{T_j} + |E_{01}^{b_j}\rangle_{E_j}|1^{b_j}\rangle_{T_j} \tag{2}$$

$$U_j|0^E\rangle_{E_j}|1^{b_j}\rangle_{T_j} = |E_{10}^{b_j}\rangle_{E_j}|0^{b_j}\rangle_{T_j} + |E_{11}^{b_j}\rangle_{E_j}|1^{b_j}\rangle_{T_j}, \tag{3}$$

[1] Here we assume that Bob has a quantum memory and can delay his measurement. In practical implementations, Bob usually cannot do that, but is assumed to measure in a randomly-chosen basis (z or x), so that Alice and Bob later discard the qubits measured in the wrong basis. In that case, we need to assume that Alice sends more than N qubits, so that N qubits are finally detected by Bob and measured in the correct basis. In the original scheme, the probability of choosing each basis (z or x) was $\frac{1}{2}$, which caused half of the sent qubits to be lost; in the improved scheme suggested by [33], the probability of choosing the z basis can be much higher, which means that much less qubits get lost.

where $|E_{00}^{b_j}\rangle_{E_j}$, $|E_{01}^{b_j}\rangle_{E_j}$, $|E_{10}^{b_j}\rangle_{E_j}$, and $|E_{11}^{b_j}\rangle_{E_j}$ are non-normalized states in Eve's probe system E_j attached to the j-th qubit.

We thus notice that Eve can modify the original *product state* of the compound system, $|0^E\rangle_{E_j}|i_j^{b_j}\rangle_{T_j}$, into an *entangled state* (e.g., $|E_{00}^{b_j}\rangle_{E_j}|0^{b_j}\rangle_{T_j} + |E_{01}^{b_j}\rangle_{E_j}|1^{b_j}\rangle_{T_j}$). Eve's attack may thus cause Bob's state to become entangled with her probe. On the one hand, this may give Eve some information on Bob's state; on the other hand, this causes disturbance that may be detected by Bob. The security proof shows that the information obtained by Eve and the disturbance caused by Eve are inherently correlated: this is the basic reason QKD protocols are secure.

3.2. Results from [1]

The security proof of BB84-INFO-z against collective attacks is very similar to the security proof of BB84 itself against collective attacks, that was detailed in [1]. Most parts of the proof are not affected at all by the changes made to BB84 to get the BB84-INFO-z protocol (changes detailed in Section 2 of the current paper), because those parts assume fixed strings **s** and **b**, and because the attack is collective (so the analysis is restricted to the INFO bits).

Therefore, the reader is referred to the proof in Section 2 and Subsections 3.1 to 3.5 of [1], that applies to BB84-INFO-z without any changes (except changing the total number of bits, $2n$, to N, which does not affect the proof at all), and that will not be repeated here.

We denote the rows of the error-correction parity check matrix P_C as the vectors $v_1, \ldots, v_r$ in $\mathbf{F}_2^n$, and the rows of the privacy amplification matrix P_K as the vectors $v_{r+1}, \ldots, v_{r+m}$. We also define, for every r', $V_{r'} \triangleq \mathrm{Span}\{v_1, ..., v_{r'}\}$; and we define

$$d_{r,m} \triangleq \min_{r \le r' < r+m} d_H(v_{r'+1}, V_{r'}) = \min_{r \le r' < r+m} d_{r',1}. \tag{4}$$

For a 1-bit final key $k \in \{0, 1\}$, we define $\widehat{\rho}_k$ to be the state of Eve corresponding to the final key k, given that she knows $\boldsymbol{\xi}$. Thus,

$$\widehat{\rho}_k = \frac{1}{2^{n-r-1}} \sum_{\mathbf{x} \,\big|\, \substack{\mathbf{x}P_C^{\mathrm{T}} = \boldsymbol{\xi} \\ \mathbf{x} \cdot v_{r+1} = k}} \rho_{\mathbf{x}}^{\mathbf{b}'}, \tag{5}$$

where $\rho_{\mathbf{x}}^{\mathbf{b}'}$ is Eve's state after the attack, given that Alice sent the INFO bit string $\mathbf{x}$ encoded in the bases $\mathbf{b}' = \mathbf{b_s}$. In [1], the state $\widetilde{\rho}_k$ was also defined: it is a lift-up of $\widehat{\rho}_k$ (which means that $\widehat{\rho}_k$ is a partial trace of $\widetilde{\rho}_k$), in which the states $\rho_{\mathbf{x}}^{\mathbf{b}'}$ appearing in $\widehat{\rho}_k$ are replaced by their purifications (see full definition in Subsection 3.4 of [1]).

In the end of Subsection 3.5 of [1], it was found that (in the case of a 1-bit final key, i.e., $m = 1$)

$$\frac{1}{2}\,\mathrm{tr}\,|\widetilde{\rho}_0 - \widetilde{\rho}_1| \le 2\sqrt{P\left[|\mathbf{C}_I| \ge \frac{d_{r,1}}{2} \;\mid\; \mathbf{B}_I = \overline{\mathbf{b}'}, \mathbf{s}\right]}, \tag{6}$$

where $\mathbf{C}_I$ is a random variable whose value is the n-bit string of errors on the n INFO bits; $\mathbf{B}_I$ is a random variable whose value is the n-bit string of bases of the n INFO bits; $\overline{\mathbf{b}'}$ is the bit-flipped string of $\mathbf{b}' = \mathbf{b_s}$; and $d_{r,1}$ (and, in general, $d_{r,m}$) was defined above.

Now, according to [34, Theorem 9.2 and page 407], and using the fact that $\widehat{\rho}_k$ is a partial trace of $\widetilde{\rho}_k$, we find that $\frac{1}{2}\,\mathrm{tr}\,|\widehat{\rho}_0 - \widehat{\rho}_1| \le \frac{1}{2}\,\mathrm{tr}\,|\widetilde{\rho}_0 - \widetilde{\rho}_1|$. From this result and from inequality (6) we deduce that

$$\frac{1}{2}\,\mathrm{tr}\,|\widehat{\rho}_0 - \widehat{\rho}_1| \le 2\sqrt{P\left[|\mathbf{C}_I| \ge \frac{d_{r,1}}{2} \;\mid\; \mathbf{B}_I = \overline{\mathbf{b}'}, \mathbf{s}\right]}. \tag{7}$$

3.3. Bounding the differences between Eve's states

We define $\mathbf{c} \triangleq \mathbf{i} + \mathbf{i}^B$: namely, $\mathbf{c}$ is the XOR of the N-bit string $\mathbf{i}$ sent by Alice and of the N-bit string $\mathbf{i}^B$ measured by Bob. For all indexes $1 \le l \le N$, $c_l = 1$ if and only if Bob's l-th bit value is different from the l-th bit sent by Alice. The partition $\mathcal{P}$ divides the N bits into n INFO bits, n_z TEST-Z bits, and n_x TEST-X bits. The corresponding substrings of the error string $\mathbf{c}$ are $\mathbf{c_s}$ (the string of errors on the INFO bits), $\mathbf{c_z}$ (the string of errors on the TEST-Z bits), and $\mathbf{c_b}$ (the string of errors on the TEST-X bits). The random variables that correspond to $\mathbf{c_s}$, $\mathbf{c_z}$, and $\mathbf{c_b}$ are denoted by $\mathbf{C}_I$, $\mathbf{C}_{T_Z}$, and $\mathbf{C}_{T_X}$, respectively.

We define $\widetilde{\mathbf{C}}_I$ to be a random variable whose value is the string of errors on the INFO bits *if Alice had encoded and sent the INFO bits in the x basis* (instead of the z basis dictated by the protocol). In those notations, inequality (7) reads as

$$\frac{1}{2}\,\mathrm{tr}\,|\widehat{\rho}_0 - \widehat{\rho}_1| \le 2\sqrt{P\left[|\widetilde{\mathbf{C}}_I| \ge \frac{d_{r,1}}{2} \;\mid\; \mathcal{P}\right]} = 2\sqrt{P\left[|\widetilde{\mathbf{C}}_I| \ge \frac{d_{r,1}}{2} \;\mid\; \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}, \tag{8}$$

using the fact that Eve's attack is collective, so the qubits are attacked independently, and, therefore, the errors on the INFO bits are independent of the errors on the TEST-Z and TEST-X bits (namely, of $\mathbf{c_z}$ and $\mathbf{c_b}$).

As explained in [1], inequality (8) was not derived for the actual attack $U = U_1 \otimes \ldots \otimes U_N$ applied by Eve, but for a virtual flat attack (that depends on $\mathbf{b}$ and therefore could not have been applied by Eve). That flat attack gives the same states $\widehat{\rho}_0$ and $\widehat{\rho}_1$ as given by the original attack U, and it gives a lower (or the same) error rate in the conjugate basis. Therefore, inequality (8) holds for the original attack U, too. This means that, starting from this point, all our results apply to the original attack U rather than to the flat attack.

So far, we have discussed a 1-bit key. We will now discuss a general m-bit key $\mathbf{k}$. We define $\widehat{\rho}_{\mathbf{k}}$ to be the state of Eve corresponding to the final key $\mathbf{k}$, given that she knows $\boldsymbol{\xi}$:

$$\widehat{\rho}_{\mathbf{k}} = \frac{1}{2^{n-r-m}} \sum_{\mathbf{x} \mid \substack{\mathbf{x}P_C^{\mathrm{T}} = \boldsymbol{\xi} \\ \mathbf{x}P_K^{\mathrm{T}} = \mathbf{k}}} \rho_{\mathbf{x}}^{\mathbf{b}'} \tag{9}$$

Proposition 1. *For any two keys $\mathbf{k}, \mathbf{k}'$ of m bits,*

$$\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}| \leq 2m \sqrt{P\left[|\widetilde{\mathbf{C}}_I| \geq \frac{d_{r,m}}{2} \mid \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}. \tag{10}$$

Proof. We define the key $\mathbf{k}_j$, for $0 \leq j \leq m$, to consist of the first j bits of $\mathbf{k}'$ and the last $m-j$ bits of $\mathbf{k}$. This means that $\mathbf{k}_0 = \mathbf{k}$, $\mathbf{k}_m = \mathbf{k}'$, and $\mathbf{k}_{j-1}$ differs from $\mathbf{k}_j$ at most on a single bit (the j-th bit).

First, we find a bound on $\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}|$: since $\mathbf{k}_{j-1}$ differs from $\mathbf{k}_j$ at most on a single bit (the j-th bit, given by the formula $\mathbf{x} \cdot v_{r+j}$), we can use the same proof that gave us inequality (8), attaching the other (identical) key bits to $\boldsymbol{\xi}$ of the original proof; and we find that

$$\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}| \leq 2 \sqrt{P\left[|\widetilde{\mathbf{C}}_I| \geq \frac{d_j}{2} \ \mid \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}, \tag{11}$$

where we define d_j as $d_H(v_{r+j}, V'_j)$, and $V'_j \triangleq \operatorname{Span}\{v_1, v_2, \ldots, v_{r+j-1}, v_{r+j+1}, \ldots, v_{r+m}\}$.

Now we notice that d_j is the Hamming distance between v_{r+j} and some vector in V'_j, which means that $d_j = \left|\sum_{i=1}^{r+m} a_i v_i\right|$ with $a_i \in \mathbf{F}_2$ and $a_{r+j} \neq 0$. The properties of Hamming distance assure us that d_j is at least $d_H(v_{r'+1}, V_{r'})$ for some $r \leq r' < r+m$. Therefore, we find that $d_{r,m} = \min_{r \leq r' < r+m} d_H(v_{r'+1}, V_{r'}) \leq d_j$.

The result $d_{r,m} \leq d_j$ implies that if $|\widetilde{\mathbf{C}}_I| \geq \frac{d_j}{2}$ then $|\widetilde{\mathbf{C}}_I| \geq \frac{d_{r,m}}{2}$. Therefore, inequality (11) implies

$$\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}| \leq 2 \sqrt{P\left[|\widetilde{\mathbf{C}}_I| \geq \frac{d_{r,m}}{2} \ \mid \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}. \tag{12}$$

Now we use the triangle inequality for norms to find

$$\begin{aligned} \frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}| &= \frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_0} - \widehat{\rho}_{\mathbf{k}_m}| \leq \sum_{j=1}^{m} \frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}| \\ &\leq 2m \sqrt{P\left[|\widetilde{\mathbf{C}}_I| \geq \frac{d_{r,m}}{2} \ \mid \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}, \end{aligned} \tag{13}$$

as we wanted. □

We would now like to bound the expected value (namely, the average value) of the trace distance between two states of Eve corresponding to two final keys. However, we should take into account that if the test fails, no final key is generated, in which case we define the distance to be 0. We thus define the random variable $\Delta_{\mathrm{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}')$ for any two final keys $\mathbf{k}, \mathbf{k}'$:

$$\Delta_{\mathrm{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}' | \mathcal{P}, \boldsymbol{\xi}, \mathbf{c_z}, \mathbf{c_b}) \triangleq \begin{cases} \frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}| & \text{if } \frac{|\mathbf{c_z}|}{n_z} \leq p_{a,z} \text{ and } \frac{|\mathbf{c_b}|}{n_x} \leq p_{a,x} \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

We need to bound the expected value $\langle \Delta_{\mathrm{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}') \rangle$, that is given by:

$$\langle \Delta_{\mathrm{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}') \rangle = \sum_{\mathcal{P}, \boldsymbol{\xi}, \mathbf{c_z}, \mathbf{c_b}} \Delta_{\mathrm{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}' | \mathcal{P}, \boldsymbol{\xi}, \mathbf{c_z}, \mathbf{c_b}) \cdot p(\mathcal{P}, \boldsymbol{\xi}, \mathbf{c_z}, \mathbf{c_b}) \tag{15}$$

(In Subsection 3.6 we prove that this expected value is indeed the quantity we need to bound for proving fully composable security, defined in Subsection 1.1.)

Theorem 2.

$$\langle \Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}')\rangle \le 2m\sqrt{P\left[\left(\frac{|\widetilde{\mathbf{C}}_I|}{n} \ge \frac{d_{r,m}}{2n}\right) \wedge \left(\frac{|\mathbf{C}_{T_Z}|}{n_z} \le p_{a,z}\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}\right)\right]} \qquad (16)$$

where $\frac{|\widetilde{\mathbf{C}}_I|}{n}$ is a random variable whose value is the error rate on the INFO bits if they had been encoded in the x basis, $\frac{|\mathbf{C}_{T_Z}|}{n_z}$ is a random variable whose value is the error rate on the TEST-Z bits, and $\frac{|\mathbf{C}_{T_X}|}{n_x}$ is a random variable whose value is the error rate on the TEST-X bits.

Proof. We use the convexity of x^2, namely, the fact that for all $\{p_i\}_i$ satisfying $p_i \ge 0$ and $\sum_i p_i = 1$, it holds that $\left(\sum_i p_i x_i\right)^2 \le \sum_i p_i x_i^2$. We find that:

$$\begin{aligned}
&\langle \Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}')\rangle^2 \\
&= \left[\sum_{\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}} \Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}'|\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b})\right]^2 && \text{(by (15))} \\
&\le \sum_{\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}} \left(\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}'|\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b})\right)^2 \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) && \text{(by convexity of } x^2\text{)} \\
&= \sum_{\mathcal{P},\boldsymbol{\xi},\frac{|\mathbf{c_z}|}{n_z}\le p_{a,z},\frac{|\mathbf{c_b}|}{n_x}\le p_{a,x}} \left(\tfrac{1}{2}\operatorname{tr}|\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}|\right)^2 \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) && \text{(by (14))} \\
&\le 4m^2 \cdot \sum_{\mathcal{P},\boldsymbol{\xi},\frac{|\mathbf{c_z}|}{n_z}\le p_{a,z},\frac{|\mathbf{c_b}|}{n_x}\le p_{a,x}} P\left[|\widetilde{\mathbf{C}}_I| \ge \tfrac{d_{r,m}}{2} \mid \mathbf{c_z},\mathbf{c_b},\mathcal{P}\right] \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) && \text{(by (10))} \\
&= 4m^2 \cdot \sum_{\mathcal{P},\frac{|\mathbf{c_z}|}{n_z}\le p_{a,z},\frac{|\mathbf{c_b}|}{n_x}\le p_{a,x}} P\left[|\widetilde{\mathbf{C}}_I| \ge \tfrac{d_{r,m}}{2} \mid \mathbf{c_z},\mathbf{c_b},\mathcal{P}\right] \cdot p(\mathcal{P},\mathbf{c_z},\mathbf{c_b}) \\
&= 4m^2 \cdot \sum_{\mathcal{P}} P\left[\left(|\widetilde{\mathbf{C}}_I| \ge \tfrac{d_{r,m}}{2}\right) \wedge \left(\frac{|\mathbf{C}_{T_Z}|}{n_z} \le p_{a,z}\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}\right) \mid \mathcal{P}\right] \cdot p(\mathcal{P}) \\
&= 4m^2 \cdot P\left[\left(|\widetilde{\mathbf{C}}_I| \ge \tfrac{d_{r,m}}{2}\right) \wedge \left(\frac{|\mathbf{C}_{T_Z}|}{n_z} \le p_{a,z}\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}\right)\right] && (17)
\end{aligned}$$

as we wanted. □

3.4. Proof of security

Following [1] and [12], we choose matrices P_C and P_K such that the inequality $\frac{d_{r,m}}{2n} > p_{a,x} + \epsilon$ is satisfied for some ϵ (we will explain in Subsection 3.7 why this is possible). This means that

$$\begin{aligned}
&P\left[\left(\frac{|\widetilde{\mathbf{C}}_I|}{n} \ge \frac{d_{r,m}}{2n}\right) \wedge \left(\frac{|\mathbf{C}_{T_Z}|}{n_z} \le p_{a,z}\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}\right)\right] \\
&\le P\left[\left(\frac{|\widetilde{\mathbf{C}}_I|}{n} > p_{a,x} + \epsilon\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}\right)\right]. && (18)
\end{aligned}$$

We will now prove the right-hand-side of (18) to be exponentially small in n.

As said earlier, the random variable $\widetilde{\mathbf{C}}_I$ corresponds to the bit string of errors on the INFO bits if they had been encoded in the x basis. The TEST-X bits are also encoded in the x basis, and the random variable $\mathbf{C}_{T_X}$ corresponds to the bit string of errors on those bits. Therefore, we can treat the selection of the indexes of the n INFO bits and the n_x TEST-X bits as a random sampling (after the numbers n, n_z, and n_x *and* the indexes of the TEST-Z bits have all already been chosen) and use Hoeffding's theorem (that is described in Appendix A of [1]).

Therefore, for each bit string $c_1 \dots c_{n+n_x}$ that consists of the errors in the $n + n_x$ INFO and TEST-X bits *if the INFO bits had been encoded in the x basis*, we apply Hoeffding's theorem: namely, we take a sample of size n without replacement from the population $c_1, \dots, c_{n+n_x}$ (this corresponds to the random selection of the indexes of the INFO bits and the TEST-X bits, as defined above, given that the indexes of the TEST-Z bits have already been chosen). Let $\overline{X} = \frac{|\widetilde{\mathbf{C}}_I|}{n}$ be the average of the sample (this is exactly the error rate on the INFO bits, assuming, again, that the INFO bits had been encoded in the x basis); and let $\mu = \frac{|\widetilde{\mathbf{C}}_I| + |\mathbf{C}_{T_X}|}{n+n_x}$ be the expectancy of $\overline{X}$ (this is exactly the error rate on the INFO bits and TEST-X bits together). Then

$\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}$ is equivalent to $(n+n_x)\mu - n\overline{X} \le n_x \cdot p_{a,x}$, and, therefore, to $n \cdot (\overline{X} - \mu) \ge n_x \cdot (\mu - p_{a,x})$. This means that the conditions $\left(\frac{|\widetilde{\mathbf{C}}_I|}{n} > p_{a,x} + \epsilon\right)$ and $\left(\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}\right)$ rewrite to

$$(\overline{X} - \mu > \epsilon + p_{a,x} - \mu) \wedge \left(\frac{n}{n_x} \cdot (\overline{X} - \mu) \ge \mu - p_{a,x}\right), \tag{19}$$

which implies $\left(1 + \frac{n}{n_x}\right)(\overline{X} - \mu) > \epsilon$, which is equivalent to $\overline{X} - \mu > \frac{n_x}{n+n_x}\epsilon$. Using Hoeffding's theorem (from Appendix A of [1]), we get:

$$P\left[\left(\frac{|\widetilde{\mathbf{C}}_I|}{n} > p_{a,x} + \epsilon\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \le p_{a,x}\right)\right] \le P\left[\overline{X} - \mu > \frac{n_x}{n+n_x}\epsilon\right] \le e^{-2\left(\frac{n_x}{n+n_x}\right)^2 n\epsilon^2} \tag{20}$$

In the above discussion, we have actually proved the following Theorem:

Theorem 3. *Let us be given $\delta > 0$, $R > 0$, and, for infinitely many values of n, a family $\{v_1^n, \ldots, v_{r_n+m_n}^n\}$ of linearly independent vectors in $\mathbf{F}_2^n$ such that $\delta < \frac{d_{r_n,m_n}}{n}$ and $\frac{m_n}{n} \le R$. Then for any $p_{a,z}, p_{a,x} > 0$ and $\epsilon_{\text{sec}} > 0$ such that $p_{a,x} + \epsilon_{\text{sec}} \le \frac{\delta}{2}$, and for any $n, n_z, n_x > 0$ and two m_n-bit final keys $\mathbf{k}, \mathbf{k}'$, the distance between Eve's states corresponding to $\mathbf{k}$ and $\mathbf{k}'$ satisfies the following bound:*

$$\langle \Delta_{\text{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}') \rangle \le 2R\, n e^{-\left(\frac{n_x}{n+n_x}\right)^2 n\epsilon_{\text{sec}}^2} \tag{21}$$

In Subsection 3.7 we explain why the vectors required by this Theorem exist.

We note that the quantity $\langle \Delta_{\text{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}') \rangle$ bounds the expected values of the Shannon Distinguishability and of the mutual information between Eve and the final key, as done in [1] and [12], which is sufficient for proving non-composable security; but it also avoids composability problems: Eve is not required to measure immediately after the protocol ends, but she is allowed to wait until she gets more information. In Subsection 3.6 we use this bound for proving a fully composable security.

3.5. Reliability

Security itself is not sufficient; we also need the key to be reliable (namely, to be the same for Alice and Bob). This means that we should make sure that the number of errors on the INFO bits is less than the maximal number of errors that can be corrected by the error-correcting code. We demand that our error-correcting code can correct $n(p_{a,z} + \epsilon_{\text{rel}})$ errors (we explain in Subsection 3.7 why this demand is satisfied). Therefore, reliability of the final key with exponentially small probability of failure is guaranteed by the following inequality: (as said, $\mathbf{C}_I$ corresponds to the actual bit string of errors on the INFO bits in the protocol, when they are encoded in the z basis)

$$P\left[\left(\frac{|\mathbf{C}_I|}{n} > p_{a,z} + \epsilon_{\text{rel}}\right) \wedge \left(\frac{|\mathbf{C}_{T_Z}|}{n_z} \le p_{a,z}\right)\right] \le e^{-2\left(\frac{n_z}{n+n_z}\right)^2 n\epsilon_{\text{rel}}^2} \tag{22}$$

This inequality is proved by an argument similar to the one used in Subsection 3.4: the selection of the indexes of the INFO bits and the TEST-Z bits is a random partition of $n + n_z$ bits into two subsets of sizes n and n_z, respectively (assuming that the indexes of the TEST-X bits have already been chosen), and thus it corresponds to Hoeffding's sampling.

3.6. Proof of fully composable security

We now prove that the BB84-INFO-z protocol satisfies the definition of composable security for a QKD protocol: namely, that it satisfies equation (1) presented in Subsection 1.1. We prove that the expression $\frac{1}{2}\operatorname{tr}|\rho_{ABE} - \rho_U \otimes \rho_E|$ is exponentially small in n, with ρ_{ABE} being the actual joint state of Alice, Bob, and Eve; ρ_U being an ideal (random, secret, and shared) key distributed to Alice and Bob; and ρ_E being the partial trace of ρ_{ABE} over the system AB.

To make reading easier, we use the following notations, where $\mathbf{i}$ is the bit string sent by Alice, $\mathbf{i}^B$ is the bit string received by Bob, and $\mathbf{c} = \mathbf{i} \oplus \mathbf{i}^B$ is the string of errors:

$$\mathbf{i}_T^{AB} \triangleq \left(\mathbf{i_z}, \mathbf{i_b}, \mathbf{i_z}^B, \mathbf{i_b}^B\right) \tag{23}$$

$$\mathbf{T} \triangleq \begin{cases} 1 & \text{if } \frac{|\mathbf{c_z}|}{n_z} \le p_{a,z} \text{ and } \frac{|\mathbf{c_b}|}{n_x} \le p_{a,x} \\ 0 & \text{otherwise} \end{cases} \tag{24}$$

In other words, $\mathbf{i}_T^{AB}$ consists of all the TEST-Z and TEST-X bits of Alice and Bob; and $\mathbf{T}$ is the random variable representing the result of the test.

According to the above definitions, the states ρ_{ABE} and ρ_U are

$$\rho_{ABE} = \sum_{\mathbf{i},\mathbf{i}^B,\mathcal{P}|\mathbf{T}=1} P\left(\mathbf{i},\mathbf{i}^B,\mathcal{P}\right) \cdot |\mathbf{k}\rangle_A\langle\mathbf{k}|_A \otimes |\mathbf{k}'\rangle_B\langle\mathbf{k}'|_B \otimes \left(\rho^{\mathbf{b}'}_{\mathbf{x},\mathbf{x}^B}\right)_E \otimes |\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\rangle_C\langle\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}|_C \tag{25}$$

$$\rho_U = \frac{1}{2^m}\sum_{\mathbf{k}} |\mathbf{k}\rangle_A\langle\mathbf{k}|_A \otimes |\mathbf{k}\rangle_B\langle\mathbf{k}|_B, \tag{26}$$

where $\left(\rho^{\mathbf{b}'}_{\mathbf{x},\mathbf{x}^B}\right)_E$ is defined to be Eve's quantum state if Alice sends the INFO string $\mathbf{x} = \mathbf{i_s}$ in the bases $\mathbf{b}' = \mathbf{b_s}$ and Bob gets the INFO string $\mathbf{x}^B = \mathbf{i}^B_{\mathbf{s}}$. All the other states actually represent classical information: subsystems A and B represent the final keys held by Alice ($\mathbf{k} = \mathbf{x}P_K^{\mathrm{T}}$) and Bob ($\mathbf{k}'$, that is obtained from $\mathbf{x}^B$, $\boldsymbol{\xi} = \mathbf{x}P_C^{\mathrm{T}}$, and P_K), and subsystem C represents the information published in the unjammable classical channel during the protocol (this information is known to Alice, Bob, and Eve) – namely, $\mathbf{i}^{AB}_{\mathcal{T}}$ (all the test bits), $\mathcal{P}$ (the partition), and $\boldsymbol{\xi} = \mathbf{x}P_C^{\mathrm{T}}$ (the syndrome).

We note that in the definition of ρ_{ABE}, we sum only over the events in which the test is *passed* (namely, in which the protocol is not aborted by Alice and Bob): in such cases, an m-bit key is generated. The cases in which the protocol aborts do not exist in the sum – namely, they are represented by the zero operator, as required by the definition of composable security (see Subsection 1.1 and [13, Subsection 6.1.2]). Thus, ρ_{ABE} is a non-normalized state, and $\mathrm{tr}(\rho_{ABE})$ is the probability that the test is passed.

To help us bound the trace distance, we define the following intermediate state:

$$\rho'_{ABE} \triangleq \sum_{\mathbf{i},\mathbf{i}^B,\mathcal{P}|\mathbf{T}=1} P\left(\mathbf{i},\mathbf{i}^B,\mathcal{P}\right) \cdot |\mathbf{k}\rangle_A\langle\mathbf{k}|_A \otimes |\mathbf{k}\rangle_B\langle\mathbf{k}|_B \otimes \left(\rho^{\mathbf{b}'}_{\mathbf{x},\mathbf{x}^B}\right)_E \otimes |\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\rangle_C\langle\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}|_C \tag{27}$$

This state is identical to ρ_{ABE}, except that Bob holds the Alice's final key ($\mathbf{k}$) instead of his own calculated final key ($\mathbf{k}'$). In particular, the similarity between ρ_{ABE} and ρ'_{ABE} means, by definition, that $\rho_E \triangleq \mathrm{tr}_{AB}(\rho_{ABE})$ and $\rho'_E \triangleq \mathrm{tr}_{AB}\left(\rho'_{ABE}\right)$ are the same state: namely, $\rho_E = \rho'_E$.

Proposition 4. *Under the same conditions as Theorem 3, it holds that*

$$\frac{1}{2}\,\mathrm{tr}\left|\rho'_{ABE} - \rho_U \otimes \rho_E\right| \le 2R\,n e^{-\left(\frac{n_x}{n+n_x}\right)^2 n\epsilon^2_{\mathrm{sec}}}, \tag{28}$$

for ρ'_{ABE} and ρ_U defined above and for the partial trace $\rho_E \triangleq \mathrm{tr}_{AB}(\rho_{ABE})$.

Proof. We notice that in ρ'_{ABE}, the only factors depending directly on $\mathbf{x}$ and $\mathbf{x}^B$ (and not only on $\mathbf{k}$ and $\boldsymbol{\xi}$) are the probability $P\left(\mathbf{i},\mathbf{i}^B,\mathcal{P}\right)$ and Eve's state $\left(\rho^{\mathbf{b}'}_{\mathbf{x},\mathbf{x}^B}\right)_E$. The probability can be reformulated as:

$$\begin{aligned} P\left(\mathbf{i},\mathbf{i}^B,\mathcal{P}\right) &= P\left(\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \cdot P\left(\mathbf{k} \mid \mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \\ &\quad \cdot P\left(\mathbf{x} \mid \mathbf{k},\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \cdot P\left(\mathbf{x}^B \mid \mathbf{x},\mathbf{k},\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \\ &= P\left(\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \cdot \frac{1}{2^m} \cdot \frac{1}{2^{n-r-m}} \cdot P\left(\mathbf{x}^B \mid \mathbf{x},\mathbf{k},\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \end{aligned} \tag{29}$$

(Because all the possible n-bit values of $\mathbf{x}$ have the same probability, $\frac{1}{2^n}$; and because all the $r+m$ rows of the matrices P_C and P_K are linearly independent, so there are exactly 2^{n-r-m} values of $\mathbf{x}$ corresponding to each specific pair $(\boldsymbol{\xi},\mathbf{k})$.)

Therefore, the state ρ'_{ABE} takes the following form:

$$\rho'_{ABE} = \frac{1}{2^m}\sum_{\mathbf{k},\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}|\mathbf{T}=1} P\left(\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \cdot |\mathbf{k}\rangle_A\langle\mathbf{k}|_A \otimes |\mathbf{k}\rangle_B\langle\mathbf{k}|_B \otimes \left[\frac{1}{2^{n-r-m}} \sum_{\mathbf{x},\mathbf{x}^B \,\middle|\, \substack{\mathbf{x}P_C^{\mathrm{T}}=\boldsymbol{\xi} \\ \mathbf{x}P_K^{\mathrm{T}}=\mathbf{k}}} P\left(\mathbf{x}^B \mid \mathbf{x},\mathbf{k},\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\right) \cdot \left(\rho^{\mathbf{b}'}_{\mathbf{x},\mathbf{x}^B}\right)_E\right] \otimes |\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}\rangle_C\langle\mathbf{i}^{AB}_{\mathcal{T}},\mathcal{P},\boldsymbol{\xi}|_C$$

$$\begin{aligned}&= \frac{1}{2^m} \sum_{\mathbf{k}, \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi} | \mathbf{T}=1} P\left(\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\right) \cdot |\mathbf{k}\rangle_A \langle \mathbf{k}|_A \otimes |\mathbf{k}\rangle_B \langle \mathbf{k}|_B \\ &\otimes (\widehat{\rho}_{\mathbf{k}})_E \otimes |\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\rangle_C \langle \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}|_C\end{aligned} \tag{30}$$

($\widehat{\rho}_{\mathbf{k}}$ was defined in equation (9).)

The partial trace $\rho'_E = \mathrm{tr}_{AB}\left(\rho'_{ABE}\right)$, that (as proved above) is the same as ρ_E, is

$$\rho_E = \rho'_E = \frac{1}{2^m} \sum_{\mathbf{k}, \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi} | \mathbf{T}=1} P\left(\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\right) \cdot (\widehat{\rho}_{\mathbf{k}})_E \otimes |\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\rangle_C \langle \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}|_C, \tag{31}$$

and the state $\rho_U \otimes \rho_E$ is

$$\begin{aligned}\rho_U \otimes \rho_E = \frac{1}{2^{2m}} &\sum_{\mathbf{k}, \mathbf{k}'', \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi} | \mathbf{T}=1} P\left(\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\right) \cdot |\mathbf{k}\rangle_A \langle \mathbf{k}|_A \otimes |\mathbf{k}\rangle_B \langle \mathbf{k}|_B \\ &\otimes (\widehat{\rho}_{\mathbf{k}''})_E \otimes |\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\rangle_C \langle \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}|_C.\end{aligned} \tag{32}$$

By using the triangle inequality for norms, since ρ'_{ABE} and $\rho_U \otimes \rho_E$ are the same (except the difference between Eve's states, $(\widehat{\rho}_{\mathbf{k}})_E$ and $(\widehat{\rho}_{\mathbf{k}''})_E$), we get, by using the definition of $\langle \Delta_{\mathrm{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}'')\rangle$ (equation (15)) and Theorem 3:

$$\begin{aligned}\frac{1}{2}\,\mathrm{tr}\left|\rho'_{ABE} - \rho_U \otimes \rho_E\right| &\le \frac{1}{2^{2m}} \sum_{\mathbf{k}, \mathbf{k}'', \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi} | \mathbf{T}=1} P\left(\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\right) \cdot \frac{1}{2}\,\mathrm{tr}\left|(\widehat{\rho}_{\mathbf{k}})_E - (\widehat{\rho}_{\mathbf{k}''})_E\right| \\ &= \frac{1}{2^{2m}} \sum_{\mathbf{k}, \mathbf{k}''} \langle \Delta_{\mathrm{Eve}}^{(p_{a,z}, p_{a,x})}(\mathbf{k}, \mathbf{k}'')\rangle \\ &\le 2R\,n e^{-\left(\frac{n_x}{n+n_x}\right)^2 n \epsilon_{\mathrm{sec}}^2}\end{aligned} \tag{33}$$

as we wanted. □

We still have to bound the following difference:

$$\begin{aligned}\rho_{ABE} - \rho'_{ABE} = &\sum_{\mathbf{i}, \mathbf{i}^B, \mathcal{P} | \mathbf{T}=1} P\left(\mathbf{i}, \mathbf{i}^B, \mathcal{P}\right) \\ &\cdot\ |\mathbf{k}\rangle_A \langle \mathbf{k}|_A \otimes \left[|\mathbf{k}'\rangle_B \langle \mathbf{k}'|_B - |\mathbf{k}\rangle_B \langle \mathbf{k}|_B\right] \\ &\otimes \left(\rho_{\mathbf{x}, \mathbf{x}^B}^{\mathbf{b}'}\right)_E \otimes |\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\rangle_C \langle \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}|_C \\ &= P\left(\left(\mathbf{k} \ne \mathbf{k}'\right) \wedge (\mathbf{T}=1)\right) \\ &\cdot\ \sum_{\mathbf{i}, \mathbf{i}^B, \mathcal{P}} P\left(\mathbf{i}, \mathbf{i}^B, \mathcal{P} \mid \left(\mathbf{k} \ne \mathbf{k}'\right) \wedge (\mathbf{T}=1)\right) \\ &\cdot\ |\mathbf{k}\rangle_A \langle \mathbf{k}|_A \otimes \left[|\mathbf{k}'\rangle_B \langle \mathbf{k}'|_B - |\mathbf{k}\rangle_B \langle \mathbf{k}|_B\right] \\ &\otimes \left(\rho_{\mathbf{x}, \mathbf{x}^B}^{\mathbf{b}'}\right)_E \otimes |\mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}\rangle_C \langle \mathbf{i}_T^{AB}, \mathcal{P}, \boldsymbol{\xi}|_C\end{aligned} \tag{34}$$

Because the trace distance between every two normalized states is bounded by 1, and because of the reliability proof in Subsection 3.5, we get:

$$\frac{1}{2}\,\mathrm{tr}\left|\rho_{ABE} - \rho'_{ABE}\right| \le P\left(\left(\mathbf{k} \ne \mathbf{k}'\right) \wedge (\mathbf{T}=1)\right) \le e^{-2\left(\frac{n_z}{n+n_z}\right)^2 n \epsilon_{\mathrm{rel}}^2} \tag{35}$$

(Because if $\mathbf{k} \ne \mathbf{k}'$, Alice and Bob have different final keys, and this means that the error correction stage did not succeed. According to the discussion in Subsection 3.5, this can happen only if there are too many errors in the information string – namely, if $\frac{|\mathbf{C}_I|}{n} > p_{a,z} + \epsilon_{\mathrm{rel}}$.)

To sum up, we get the following bound:

$$\begin{aligned}\frac{1}{2}\,\mathrm{tr}\left|\rho_{ABE} - \rho_U \otimes \rho_E\right| &\le \frac{1}{2}\,\mathrm{tr}\left|\rho_{ABE} - \rho'_{ABE}\right| + \frac{1}{2}\,\mathrm{tr}\left|\rho'_{ABE} - \rho_U \otimes \rho_E\right| \\ &\le e^{-2\left(\frac{n_z}{n+n_z}\right)^2 n \epsilon_{\mathrm{rel}}^2} + 2R\,n e^{-\left(\frac{n_x}{n+n_x}\right)^2 n \epsilon_{\mathrm{sec}}^2}\end{aligned} \tag{36}$$

This bound is exponentially small in n. Thus, we have proved the composable security of BB84-INFO-z.

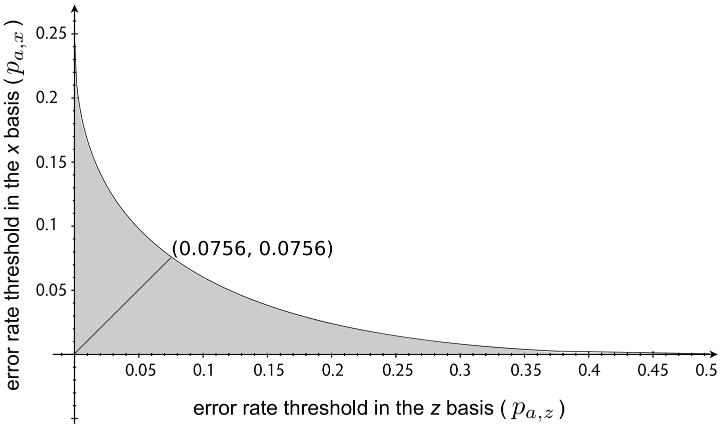

Fig. 1. The secure asymptotic error rates zone for BB84-INFO-*z* (below the curve).

3.7. *Security, reliability, and error rate threshold*

According to Theorem 3 and to the discussion in Subsection 3.5, to get both security and reliability we only need vectors $\{v_1^n, \ldots, v_{r_n+m_n}^n\}$ satisfying both the conditions of the Theorem (distance $\frac{d_{r_n,m_n}}{2n} > \frac{\delta}{2} \geq p_{a,x} + \epsilon_{\text{sec}}$) and the reliability condition (the ability to correct $n(p_{a,z} + \epsilon_{\text{rel}})$ errors). Such families were proven to exist in Appendix E of [12], giving the following upper bound on the bit-rate:

$$R_{\text{secret}} \triangleq \frac{m}{n} < 1 - H_2(2p_{a,x} + 2\epsilon_{\text{sec}}) - H_2\left(p_{a,z} + \epsilon_{\text{rel}} + \frac{1}{n}\right) \tag{37}$$

where $H_2(x) \triangleq -x\log_2(x) - (1-x)\log_2(1-x)$.

Note that we use here the error thresholds $p_{a,x}$ for security and $p_{a,z}$ for reliability. This is possible, because in [12] those conditions (security and reliability) on the codes are discussed separately.

To get the asymptotic error rate thresholds, we require $R_{\text{secret}} > 0$, and we get the condition:

$$H_2(2p_{a,x} + 2\epsilon_{\text{sec}}) + H_2\left(p_{a,z} + \epsilon_{\text{rel}} + \frac{1}{n}\right) < 1 \tag{38}$$

The secure asymptotic error rate thresholds zone is shown in Fig. 1 (it is below the curve), assuming that $\frac{1}{n}$ is negligible. Note the trade-off between the error rates $p_{a,z}$ and $p_{a,x}$. Also note that in the case $p_{a,z} = p_{a,x}$, we get the same threshold as BB84 ([12] and [1]), which is 7.56%.

4. Discussion

In the current paper, we have proved the BB84-INFO-*z* protocol to be fully secure against collective attacks. We have discovered that the results of BB84 hold very similarly for BB84-INFO-*z*, with only two exceptions:

1. The error rates must be separately checked to be below the thresholds $p_{a,z}$ and $p_{a,x}$ for the TEST-Z and TEST-X bits, respectively, while in BB84 the error rate threshold p_a applies to all the TEST bits together.
2. The exponents of Eve's information (security) and of the failure probability of the error-correcting code (reliability) are different than in [1], because different numbers of test bits are now allowed (n_z and n_x are arbitrary). This implies that the exponents may decrease more slowly (or more quickly) as a function of n. However, if we choose $n_z = n_x = n$ (thus sending $N = 3n$ qubits from Alice to Bob), then we get exactly the same exponents as in [1].

The asymptotic error rate thresholds found in this paper allow us to tolerate a higher threshold for a specific basis (say, the x basis) if we demand a lower threshold for the other basis (z). If we choose the same error rate threshold for both bases, then the asymptotic bound is 7.56%, exactly the bound found for BB84 in [12] and [1].

We conclude that even if we change the BB84 protocol to have INFO bits only in the z basis, this does not harm its security and reliability (at least against collective attacks). This does not even change the asymptotic error rate threshold. The only drawbacks of this change are the need to check the error rate for the two bases separately, and the need to either send more qubits ($3n$ qubits in total, rather than $2n$) or get a slower exponential decrease of the exponents required for security and reliability.

We thus find that the feature of BB84, that both bases are used for information, is not very important for security and reliability, and that BB84-INFO-*z* (that lacks this feature) is almost as useful as BB84. This may have important implications on the security and reliability of other protocols that, too, use only one basis for information qubits, such as [15] and some two-way protocols [19,21].

We also present a better approach for the proof, that uses the quantum distance between two states rather than the classical information. In [1], [11], and [12], the classical mutual information between Eve's information (after an optimal measurement) and the final key was calculated (by using the trace distance between two quantum states); although we should note that in [1] and [12], the trace distance was used for the proof of security of a single bit of the final key even when all other bits are given to Eve, and only the last stages of the proof discussed bounding the classical mutual information. In the current paper, on the other hand, we use the trace distance between the two quantum states until the end of the proof, which allows us to prove fully composable security.

Therefore, our proof shows the fully composable security of BB84-INFO-z against collective attacks (and, in particular, security even if Eve keeps her quantum states until she gets more information when Alice and Bob use the key, rather than measuring them at the end of the protocol); and a very similar approach can be applied to [1], immediately proving the composable security of BB84 against collective attacks. Our proof also makes a step towards making the security proof in [12] (security proof of BB84 against joint attacks) prove the *composable* security of BB84 against joint attacks.

Our results show that the BB84-INFO-z protocol can be securely used for distributing a secret key; the security is of an ideal implementation and against an adversary limited to collective attacks (it may be possible to generalize the proof, so that it applies to the most general attacks (joint attacks), by using the methods of [12], but such generalization is beyond the scope of the current paper). Moreover, the security of the final key is universally composable, which means that the key may be used for any cryptographic purpose without harming the security, even if Eve keeps her quantum states and uses all the information she gets in the future in an optimal way.

The techniques described in our proof may be applied in the future for proving the security of other protocols by using similar methods, and, in particular, for proving the security of other QKD protocols that use only one basis for the information bits, such as [15,19,21] mentioned above.

We note that this paper strengthens the security proofs described in [1,11,12], both because it slightly generalizes them (from security of BB84 to security of BB84-INFO-z) and because it makes them composable. Those security proofs have various advantages over other methods to prove security: first of all, they are mostly self-contained, while other security proofs require many results from other areas of quantum information (such as various notions of entropy needed for the security proof of [13,27], and entanglement purification and quantum error correction needed for the security proof of [26]); second, they give tight finite-key bounds, unlike several other methods (see details below); and finally, at least in some sense, they are simpler than other proof techniques. On the other hand, their generality and their asymptotic error-rate threshold (7.56%, rather than 11% given by [27,26]) are yet to be improved by future research.

Our method for proving security gives explicit and tight finite-key bounds. In contrast to this, the security proof of [26] gives only asymptotic results (for infinitely long keys). For the security proof of [13,27], it is proved today that for some protocols (including BB84), one can get tight finite-key bounds [35] that are the same as the ones found by our method; but at first that security method gave very pessimistic bounds (by using the de Finetti theorem [13,36]), and later, the bounds were improved for several protocols (including BB84) [37], but were still not tight (see [35] for comparison).

We also note that the existence of many different proof techniques is important, because some proofs may be more adjustable to various QKD protocols or to practical scenarios; some proofs may be clearer to different readers with different backgrounds; analyzing the differences between the proofs and between their obtained results may lead to important insights on the strengths and weaknesses of various techniques; and the existence of many proofs makes the security result more certain and less prone to errors.

We note that our security proof, similarly to many other full security proofs of QKD, assumes an ideal implementation (of ideal quantum systems consisting of exactly one qubit) and theoretical attacks. Practical implementations of QKD, almost always using photons, exist (see [38,23] for details); their security analysis is much more complicated, because both Alice's photon source and Bob's detector devices have weaknesses and deviations from the theoretical protocol (especially when more than one photon is emitted by Alice or is sent by the eavesdropper). Those imperfections give rise to various practical attacks, such as the "Photon-Number Splitting" attack [39] (in which the eavesdropper takes advantage of emissions of two or more photons by Alice and gets full information) and the "Bright Illumination" attack [40] (in which the eavesdropper takes advantage of a weakness of specific detectors used by Bob and gets full information).

Possible solutions to those problems of actual physical realizations (see [38,23] for more details) include a much more careful analysis of the practical devices and of practical implementations; "Measurement-Device Independent" QKD protocols [41–44], that may be secure even if the measurement devices are controlled by the adversary; and "Device Independent" QKD protocols [45–47], that may be secure even if all the quantum devices are controlled by the adversary (under certain assumptions).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The work of TM and RL was partly supported by the Israeli MOD Research and Technology Unit.

References

[1] M. Boyer, R. Gelles, T. Mor, Security of the Bennett-Brassard quantum key distribution protocol against collective attacks, Algorithms 2 (2) (2009) 790–807, https://doi.org/10.3390/a2020790, http://www.mdpi.com/1999-4893/2/2/790.

[2] M. Boyer, R. Liss, T. Mor, Security against collective attacks of a modified BB84 QKD protocol with information only in one basis, in: Proceedings of the 2nd International Conference on Complexity, Future Information Systems and Risk, COMPLEXIS, Porto, Portugal, INSTICC, 24–26 April, 2017, ScitePress, 2017, pp. 23–29, http://www.scitepress.org/DigitalLibrary/PublicationsDetail.aspx?ID=DhwGgQvTxH4=&t=1.

[3] J. Daemen, V. Rijmen, The Design of Rijndael: AES – the Advanced Encryption Standard, Springer Science & Business Media, 2013.

[4] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (6) (1976) 644–654, https://doi.org/10.1109/TIT.1976.1055638, http://ieeexplore.ieee.org/document/1055638/.

[5] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126, https://doi.org/10.1145/359340.359342, http://doi.acm.org/10.1145/359340.359342.

[6] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) (1999) 303–332, https://doi.org/10.1137/S0036144598347011, http://epubs.siam.org/doi/10.1137/S0036144598347011.

[7] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (4) (1949) 656–715, https://doi.org/10.1002/j.1538-7305.1949.tb00928.x, http://ieeexplore.ieee.org/document/6769090/.

[8] C.H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in: International Conference on Computers, Systems & Signal Processing, IEEE, 1984, pp. 175–179.

[9] E. Biham, T. Mor, Security of quantum cryptography against collective attacks, Phys. Rev. Lett. 78 (1997) 2256–2259, https://doi.org/10.1103/PhysRevLett.78.2256, http://link.aps.org/doi/10.1103/PhysRevLett.78.2256.

[10] E. Biham, T. Mor, Bounds on information and the security of quantum cryptography, Phys. Rev. Lett. 79 (1997) 4034–4037, https://doi.org/10.1103/PhysRevLett.79.4034, http://link.aps.org/doi/10.1103/PhysRevLett.79.4034.

[11] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, T. Mor, Security of quantum key distribution against all collective attacks, Algorithmica 34 (4) (2002) 372–388, https://doi.org/10.1007/s00453-002-0973-6, https://link.springer.com/article/10.1007/s00453-002-0973-6.

[12] E. Biham, M. Boyer, O.P. Boykin, T. Mor, V. Roychowdhury, A proof of the security of quantum key distribution, J. Cryptology 19 (4) (2006) 381–439, https://doi.org/10.1007/s00145-005-0011-3, https://link.springer.com/article/10.1007/s00145-005-0011-3.

[13] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. 6 (01) (2008) 1–127, https://doi.org/10.1142/S0219749908003256, http://www.worldscientific.com/doi/abs/10.1142/S0219749908003256.

[14] M. Christandl, R. König, R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett. 102 (2009) 020504, https://doi.org/10.1103/PhysRevLett.102.020504, http://link.aps.org/doi/10.1103/PhysRevLett.102.020504.

[15] T. Mor, No cloning of orthogonal states in composite systems, Phys. Rev. Lett. 80 (1998) 3137–3140, https://doi.org/10.1103/PhysRevLett.80.3137, https://link.aps.org/doi/10.1103/PhysRevLett.80.3137.

[16] C.-H.F. Fung, H.-K. Lo, Security proof of a three-state quantum-key-distribution protocol without rotational symmetry, Phys. Rev. A 74 (2006) 042342, https://doi.org/10.1103/PhysRevA.74.042342, https://link.aps.org/doi/10.1103/PhysRevA.74.042342.

[17] C. Branciard, N. Gisin, N. Lütkenhaus, V. Scarani, Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography, Quantum Inf. Comput. 7 (7) (2007) 639–664, http://www.rintonpress.com/xqic7/qic-7-7/639-664.pdf.

[18] W.O. Krawec, Asymptotic analysis of a three state quantum cryptographic protocol, in: 2016 IEEE International Symposium on Information Theory, ISIT, 2016, pp. 2489–2493, http://ieeexplore.ieee.org/document/7541747/.

[19] M. Boyer, D. Kenigsberg, T. Mor, Quantum key distribution with classical Bob, Phys. Rev. Lett. 99 (2007) 140501, https://doi.org/10.1103/PhysRevLett.99.140501, http://link.aps.org/doi/10.1103/PhysRevLett.99.140501.

[20] W.O. Krawec, Security proof of a semi-quantum key distribution protocol, in: 2015 IEEE International Symposium on Information Theory, ISIT, IEEE, 2015, pp. 686–690, http://ieeexplore.ieee.org/document/7282542/.

[21] X. Zou, D. Qiu, L. Li, L. Wu, L. Li, Semiquantum-key distribution using less than four quantum states, Phys. Rev. A 79 (2009) 052312, https://doi.org/10.1103/PhysRevA.79.052312, http://link.aps.org/doi/10.1103/PhysRevA.79.052312.

[22] M. Boyer, T. Mor, Comment on “semiquantum-key distribution using less than four quantum states”, Phys. Rev. A 83 (2011) 046301, https://doi.org/10.1103/PhysRevA.83.046301, http://link.aps.org/doi/10.1103/PhysRevA.83.046301.

[23] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, Rev. Modern Phys. 81 (2009) 1301–1350, https://doi.org/10.1103/RevModPhys.81.1301, https://link.aps.org/doi/10.1103/RevModPhys.81.1301.

[24] D. Stebila, M. Mosca, N. Lütkenhaus, The case for quantum key distribution, in: A. Sergienko, S. Pascazio, P. Villoresi (Eds.), Quantum Communication and Quantum Networking: First International Conference. Revised Selected Papers, QuantumComm 2009, Naples, Italy, October 26–30, 2009, Springer, Berlin–Heidelberg, 2010, pp. 283–296, https://link.springer.com/chapter/10.1007/978-3-642-11731-2_35.

[25] D. Mayers, Unconditional security in quantum cryptography, J. ACM 48 (3) (2001) 351–406, https://doi.org/10.1145/382780.382781, http://doi.acm.org/10.1145/382780.382781.

[26] P.W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2000) 441–444, https://doi.org/10.1103/PhysRevLett.85.441, http://link.aps.org/doi/10.1103/PhysRevLett.85.441.

[27] R. Renner, N. Gisin, B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A 72 (2005) 012332, https://doi.org/10.1103/PhysRevA.72.012332, http://link.aps.org/doi/10.1103/PhysRevA.72.012332.

[28] C.H. Bennett, G. Brassard, C. Crépeau, U.M. Maurer, Generalized privacy amplification, IEEE Trans. Inform. Theory 41 (6) (1995) 1915–1923, https://doi.org/10.1109/18.476316, http://ieeexplore.ieee.org/document/476316/.

[29] C.H. Bennett, T. Mor, J.A. Smolin, Parity bit in quantum cryptography, Phys. Rev. A 54 (1996) 2675–2684, https://doi.org/10.1103/PhysRevA.54.2675, http://link.aps.org/doi/10.1103/PhysRevA.54.2675.

[30] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, J. Oppenheim, The universal composable security of quantum key distribution, in: J. Kilian (Ed.), Theory of Cryptography: Second Theory of Cryptography Conference. Proceedings, TCC 2005, Cambridge, MA, USA, February 10–12, 2005, Springer, Berlin–Heidelberg, 2005, pp. 386–406, https://link.springer.com/chapter/10.1007/978-3-540-30576-7_21, 2005.

[31] R. Canetti, Universally composable security: a new paradigm for cryptographic protocols, in: Proceedings 42nd IEEE Symposium on Foundations of Computer Science, 2001, pp. 136–145, http://ieeexplore.ieee.org/document/959888/.

[32] B. Pfitzmann, M. Waidner, Composition and integrity preservation of secure reactive systems, in: Proceedings of the 7th ACM Conference on Computer and Communications Security, CCS '00, ACM, New York, 2000, pp. 245–254, http://dl.acm.org/citation.cfm?doid=352600.352639.

[33] H.-K. Lo, H. Chau, M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptology 18 (2) (2005) 133–165, https://doi.org/10.1007/s00145-004-0142-y, https://link.springer.com/article/10.1007/s00145-004-0142-y.

[34] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, 10th anniversary edition, Cambridge University Press, 2000.

[35] M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. 3 (634) (2012) 1–6, https://doi.org/10.1038/ncomms1631, https://www.nature.com/articles/ncomms1631.

[36] R. Renner, Symmetry of large physical systems implies independence of subsystems, Nat. Phys. 3 (9) (2007) 645–649, https://doi.org/10.1038/nphys684, https://www.nature.com/nphys/journal/v3/n9/abs/nphys684.html.

[37] V. Scarani, R. Renner, Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing, Phys. Rev. Lett. 100 (2008) 200501, https://doi.org/10.1103/PhysRevLett.100.200501, https://link.aps.org/doi/10.1103/PhysRevLett.100.200501.

[38] H.-K. Lo, M. Curty, K. Tamaki, Secure quantum key distribution, Nat. Photon. 8 (8) (2014) 595–604, https://doi.org/10.1038/nphoton.2014.149, https://www.nature.com/nphoton/journal/v8/n8/full/nphoton.2014.149.html.

[39] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. 85 (2000) 1330–1333, https://doi.org/10.1103/PhysRevLett.85.1330, http://link.aps.org/doi/10.1103/PhysRevLett.85.1330.

[40] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. 4 (10) (2010) 686–689, https://doi.org/10.1038/nphoton.2010.214, http://www.nature.com/nphoton/journal/v4/n10/abs/nphoton.2010.214.html.

[41] E. Biham, B. Huttner, T. Mor, Quantum cryptographic network based on quantum memories, Phys. Rev. A 54 (1996) 2651–2658, https://doi.org/10.1103/PhysRevA.54.2651, https://link.aps.org/doi/10.1103/PhysRevA.54.2651.

[42] H. Inamori, Security of practical time-reversed EPR quantum key distribution, Algorithmica 34 (4) (2002) 340–365, https://doi.org/10.1007/s00453-002-0983-4, https://link.springer.com/article/10.1007/s00453-002-0983-4.

[43] H.-K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. 108 (2012) 130503, https://doi.org/10.1103/PhysRevLett.108.130503, https://link.aps.org/doi/10.1103/PhysRevLett.108.130503.

[44] S.L. Braunstein, S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. 108 (2012) 130502, https://doi.org/10.1103/PhysRevLett.108.130502, https://link.aps.org/doi/10.1103/PhysRevLett.108.130502.

[45] D. Mayers, A. Yao, Quantum cryptography with imperfect apparatus, in: Proceedings 39th Annual Symposium on Foundations of Computer Science, 1998, pp. 503–509, http://ieeexplore.ieee.org/document/743501/.

[46] L. Masanes, A. Acín, S. Pironio, Secure device-independent quantum key distribution with causally independent measurement devices, Nat. Commun. 2 (238) (2011) 1–7, https://doi.org/10.1038/ncomms1244, https://www.nature.com/articles/ncomms1244.

[47] U. Vazirani, T. Vidick, Fully device-independent quantum key distribution, Phys. Rev. Lett. 113 (2014) 140501, https://doi.org/10.1103/PhysRevLett.113.140501, https://link.aps.org/doi/10.1103/PhysRevLett.113.140501.