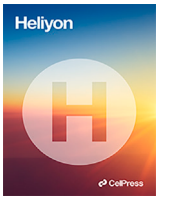
Heliyon 10 (2024) e23578

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

# Bases selection with pseudo-random functions in BB84 scheme

Emir Dervisevic [a,*], Miroslav Voznak [b], Miralem Mehic [a,b]

[a] Department of Telecommunications, Faculty of Electrical Engineering, University of Sarajevo, Sarajevo, 71000, Bosnia and Herzegovina
[b] Department of Telecommunications, Faculty of Electrical Engineering and Computer Science, VSB – Technical University of Ostrava, Ostrava, 708 00, Czechia

ARTICLE INFO

*Keywords:*
Cryptography
Quantum key distribution
BB84
Protocols

ABSTRACT

Because the spectrum of services available in modern telecommunication networks is constantly expanding, security has become increasingly important. Simultaneously, in an era of constant progress in mathematics and computing, the security of existing cryptographic solutions becomes questionable. Quantum Key Distribution (QKD) is a promising secret key agreement primitive that enables long-awaited practical Information-Theoretical Secure (ITS) communications. The key generation rate, however, is one of the limitations of its widespread application to secure high throughput data flows. This paper addresses the aforementioned limitation by employing perfectly correlated bases selection defined by the output of Pseudo-Random Functions based on the keyed-Hash Message Authentication Code construction. In theory, the proposed variant of the BB84 scheme is ITS, reduces memory requirements, and reduces communication overhead during the post-processing stage. It can benefit QKD networks as a service by increasing capacity and accommodating users with varying security needs.

## 1. Introduction

Many modern digital services necessitate a secure means of communication. This is especially noticeable in the emerging new generation of mobile networks, where the spectrum of digital services is becoming more diverse and includes the manipulation of highly sensitive data. However, as the field of quantum computing continues to advance, it is expected that the current widespread public-key cryptographic solutions will soon become unusable. Without adequate cryptographic alternatives, we can expect our digital lives to be significantly altered and many services to be rendered inoperable [1].

Quantum Key Distribution (QKD) [2] is a novel cryptographic method based on quantum physics laws that are unaffected by future advances in computing or mathematics. QKD accomplishes one of the most essential and oldest roles of public-key cryptography, namely secret key exchange, in an Information-Theoretical Secure (ITS) manner. This makes possible ITS communications if QKD keys are combined with the One-Time Pad (OTP) cipher in such a fashion that each key is used only once and is as long as the plain text [3,4]. QKD is a point-to-point technology that allows the exchange of keys between two physically linked parties, as illustrated in Fig. 1. A QKD link is a logical connection formed by a quantum and an authenticated public channel. Random bits are transmitted in non-orthogonal states of quantum systems – particles like photons that unlock unique security features. The authenticated public channel is used to verify and correlate shared information, resulting in symmetric binary sequences known only to the legitimate parties.

* Corresponding author.
*E-mail address:* emir.dervisevic@etf.unsa.ba (E. Dervisevic).

https://doi.org/10.1016/j.heliyon.2023.e23578
Received 19 July 2023; Received in revised form 5 December 2023; Accepted 6 December 2023

Available online 11 December 2023

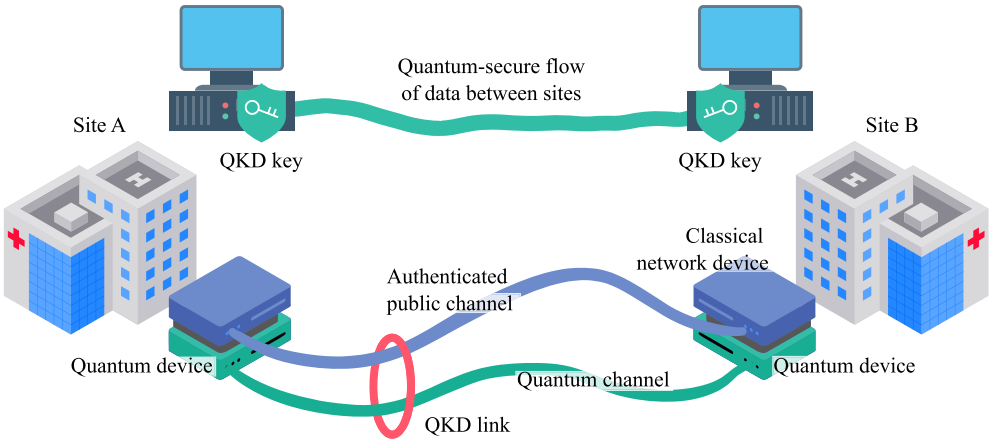



**Fig. 1.** Quantum key distribution.

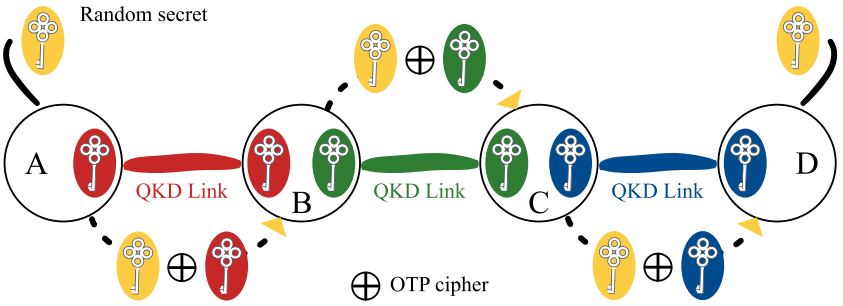



**Fig. 2.** Distribution of the cryptographic key from node A to node D over the QKD network in a hop-by-hop manner. Intermediate nodes must be trusted, for the distributed key to have an ITS security profile. In addition, for the distribution process shown here, the random secret must be truly random, i.e. the output of a quantum random number generator.

For wide-scale QKD application, a network of point-to-point QKD links has been introduced and demonstrated in several testbeds [5]. Based on intermediate trusted-repeater nodes, such networks allow key distribution between any arbitrary network nodes and provide a more robust service than individual QKD links [6]. The key distribution process is illustrated in Fig. 2 as a hop-by-hop process from a trusted node to a trusted node in a connected chain. Networks based on untrusted nodes are also feasible and are commonly deployed as access networks [7–9]. Due to the high cost of deploying QKD networks for individual organizations and similar entities, the goal is for multiple organizations hosting thousands of users to share the infrastructure of a single QKD network [10]. This is accomplished through the use of sophisticated key and network management methodologies on QKD networks. The primary resource that defines the capabilities of a QKD network as a service is cryptographic keys. The supply of cryptographic keys generated by the QKD process is limited, at best a few Mbps [11,12], which is low in comparison to data throughput in modern networks. Intelligent key allocation is essential to satisfy the demands of as many users as feasible with restricted network resources [13,14]. Recent study [15] indicates that in order to offer efficient key resource allocation and high service success probability, client requirements should be relaxed, or investment in the infrastructure layer should be made to increase secret key rates on QKD links. As a result, it appears like an incessant attempt is being made to improve key generation rates [16–18] while also broadening QKD's reach [19–23]. Due to the aforementioned limits, QKD's usefulness is confined to low-throughput data flows because it is primarily featured as the key agreement primitive to be utilized with ITS cryptographic techniques. As a result, it is common to feed QKD-derived key material to traditional computationally secure cryptographic algorithms like Advanced Encryption Standard (AES). This broadens the applicability of QKD technology across many critical infrastructures (5G [24–27], 6G [28,29], SCADA [30], and smart grids [31–33]) and allows it to accommodate users with varying security requirements.

This paper proposes a concept that considerably improves the efficiency of the BB84 scheme, the first QKD scheme, thereby shifting the upper bounds of achievable key rates. It has the potential to boost QKD utilization in maintaining security for data flows on high-capacity links by supplying keys at a faster rate. In particular, a variant of the BB84 scheme is proposed in which communication parties use perfectly correlated bases for photon preparation and measurement, which are defined by the output of a Pseudo-Random Functions (PRF) based on keyed-Hash Message Authentication Code (HMAC). The scheme boosts BB84's efficiency from 50 to 100 percent and completely eliminates public announcement of bases during the key establishment process. In theory, the scheme offers ITS profile, and we briefly discuss its security in real-world implementations.

The paper is organized as follows: Section 2 provides a brief overview of QKD and the BB84 protocol. Furthermore, variants of BB84 without public announcement of bases are described, which are closely related to the suggestion made in this paper. Section 3

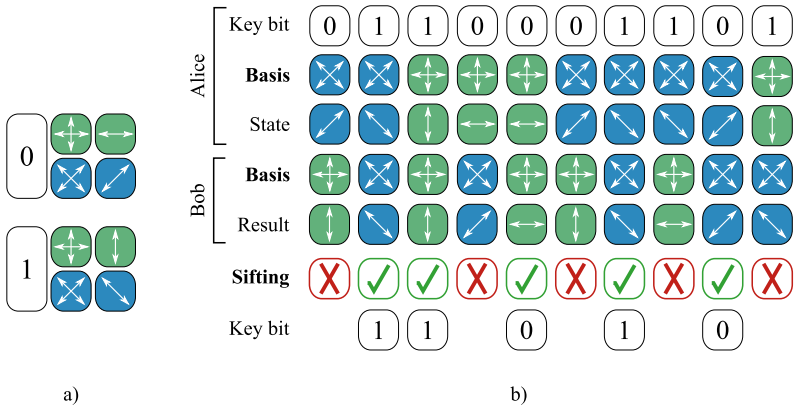



**Fig. 3.** a) A coding dictionary in BB84 scheme. A bit value is encoded in one of two polarization states based on the basis; b) The quantum transfer and the public announcement of bases (sifting) in the BB84 scheme. Because the basis selections of Alice and Bob are independent and random, half of the transmitted information (i.e., the raw key) is discarded, making the basic BB84 scheme 50% efficient.

describes a proposed variant of the BB84 scheme, including a brief discussion of its theoretical and practical security. Our variant of BB84 is then compared with previously researched variants in Section 4. Within the same Section 4, we emphasize the advantages of using our scheme to increase the capacity of QKD networks and accommodate users with varying security needs. Section 5 concludes the study.

## 2. State of the art

This section begins with an overview of QKD and its most well-known protocol, the BB84. Following that, variants of the BB84 protocol that do not require a public announcement of bases are summarized.

### *2.1. Quantum key distribution*

The concepts of QKD were established in 1984 [2], when Bennett and Brassard discovered that quantum phenomena could be used to establish a communication channel, i.e., a quantum channel, with prominent security features. These security features, which are a direct result of quantum mechanics rules, prevent adversaries from reliably reading or copying information in transit. As a result, attempts by adversaries to eavesdrop on the quantum channel leave a trace in the transmitted data, revealing their presence to legitimate parties. The secure transmission over the quantum channel, on the other hand, only allows the establishment of correlated, but not symmetric, (partial) secrets between legitimate parties. The authenticated public channel is required to test the correlation, which can reveal eavesdroppers and, in their absence, extract the ITS symmetric keys. The established key is then used within conventional security frameworks (e.g., IPsec [34]) to establish secure communication between the distant parties.

### *2.2. BB84*

Bennett and Brassard's original concepts and scheme, proposed in 1984, are now known as the BB84 protocol. The BB84 and its slightly modified variants [35,36], which improve security in practical implementations, are the most widely used. In the BB84 scheme, the quantum channel transmits single photons with encoded information in their polarization state. To leverage the inclusiveness of quantum measurements, information is encoded in four polarization states that form two conjugate polarization bases, rectilinear and diagonal. Fig. 3a depicts the BB84 coding scheme, and Fig. 3b depicts the starting steps in basic BB84 scheme, where Alice and Bob are legitimate parties involved in the key distribution process.

The BB84 scheme is explained as follows. Alice encodes bits of a random secret in the polarization states of individual photons, with the basis chosen at random. A quantum channel is used to transmit a sequence of single photons from Alice to Bob. Bob measures individual photons in a random basis and remembers the basis and measurement result. When the measurement basis matches Alice's choice of basis, Bob obtains the correct bit value unless an attacker or noise disrupts the transmission. Otherwise, as the laws of quantum mechanics indicate, the outcome is entirely random.

Once a quantum transfer, or communication over the quantum channel, is complete, Alice and Bob proceed to align the shared, correlated bits, which are called the raw keys. To avoid a man-in-the-middle attack, all subsequent communication between Alice and Bob takes place over an authenticated public channel. The first step that follows the quantum transfer is a public announcement of bases, also known as the sifting phase, in which Bob publicly announces his measurement bases, and Alice informs him which measurements were correct. They then retain the portion of the raw key where the bases match. Because Alice and Bob's bases selections are *random* (with equal probability ($\frac{1}{2}$) of occurrence) and completely *independent* of one another, the probability that they choose the same bases is given by Equation (1), where A and B are two bases, rectilinear and diagonal, respectively. Therefore, the efficiency, i.e., protocol gain of the BB84 is 50% ($g_p = 0.5$).

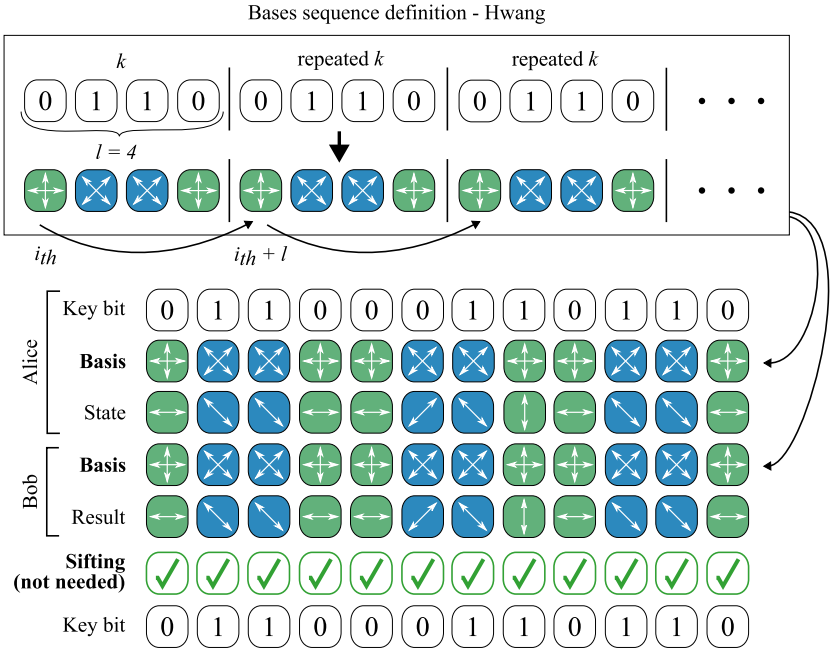



**Fig. 4.** The basic concept underlying the Hwang protocol. Figure shows a smaller-scale example where the pre-shared secret $k$ is $l = 4$ bits long. Due to perfectly correlated bases selections the protocol efficiency is 100%.

$$P(A \cap A) + P(B \cap B) = P(A) \cdot P(A) + P(B) \cdot P(B) = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} \tag{1}$$

Following the public announcement of bases, Alice and Bob perform error estimation and reconciliation [37–39], as well as privacy amplification [40] steps. After their public discussion, Alice and Bob successfully rendezvous a secret symmetric key.

### 2.3. BB84 without public announcement of bases

As a result of Alice and Bob's uncorrelated, random choice of bases, half of the raw key bits are discarded at the public announcement of bases (see equation (1)). Alice and Bob may always agree to utilize one of the bases with higher probability $\delta$ ($\frac{1}{2} < \delta < 1$), resulting in increased BB84 efficiency [41]. This scheme is known as the asymmetric BB84 protocol, and its efficiency can be made asymptotically close to 100%. Equation (2) gives the protocol gain [42].

$$g_p = P(A \cap A) + P(B \cap B) = P(A) \cdot P(A) + P(B) \cdot P(B) = \delta \cdot \delta + (1 - \delta) \cdot (1 - \delta) = 2\delta^2 - 2\delta + 1 \tag{2}$$

When the number of transmitted photons $m_t$ approaches infinity ($m_t \to \infty$), $\delta$ can approach the value of 1 ($\delta \to 1$), implying that the protocol's efficiency approaches 100% ($g_p \to 1$). However, on a finite set of transmitted photons (as is the case in practice), $\delta$ cannot take on value arbitrary close to 1, because the number of photons prepared and measured in a basis with a low probability of occurrence $(1 - \delta)$ would be insufficient to make an accurate estimate of error and detect the eavesdropper.

On the other hand, there are less known variants in which Alice and Bob's basis selections are perfectly correlated, eliminating the need for public announcement of bases (note that the asymmetric BB84 still requires this step). BB84's efficiency is maximized in this manner ($g_p = 1$). These variants are described in the following paragraphs. The emphasis is on the fundamental approaches, with little thought given to the security of the variants under consideration.

To the best of our knowledge, the Hwang protocol [43], illustrated in Fig. 4, is the first variant of the BB84 scheme that does not require public announcement of bases. A perfectly correlated bases sequence $k$ must be known a priori to legitimate parties and is suggested to be established using the basic BB84 scheme. The scheme is only effective if the bases sequence can be safely reused multiple times; otherwise, the resulting keys would be entirely used to define a new bases sequence. Convenient enough, the authors suggest that bases sequence can be safely reused because the eavesdropper, even knowing which of the quantum carriers, i.e., single photons carrying the information, are encoded in the same basis, cannot determine the basis itself. In theory, the Hwang protocol is proven to achieve ITS security profile [44].

In [45], a Quantum Key Expansion (QKE) scheme based on a varied version of Hwang protocol is introduced. A common preshared secret key, whose length is required to be twice the length, donated as $N$, of the secret key being distributed, defines the polarization state in which single photons are prepared and the encoding operation which generate transformation of the eigenstates within the

basis. A newly distributed key of length $N$ is reconciled (privacy amplification is optional) and merged with a preshared key that has been privacy amplified.[1] The scheme works as long as the merged key size is greater than $2N$. Additionally, the authors have proposed a higher-dimension extension of their scheme, which significantly improves security and demonstrates that the maximum distance for secure key distribution can be greatly increased compared to the basic BB84 scheme.

In [46], a floating basis protocol is introduced. In the suggested protocol, a possible number of bases in a single-dimensional Hilbert space is infinite.[2] To improve protocol's characteristics, Alice and Bob share a secret key a priori (referred to as an auxiliary key) that allows them to correlate their choice of bases. In addition to the maximum efficiency, the benefits of this protocol are as follows: The eavesdropper's trace is more visible (i.e., the eavesdropper introduces more errors), the eavesdropper's knowledge of the secret key is diminished, and the threshold for Quantum Bit Error Rate (QBER) corresponding to the secure transmission increases. The protocol and its security are discussed in [47], while the combination of the floating bases and decoy states is presented in [48].

A protocol with pseudo-random choice of bases (PRB) has been proposed in [49] as a formalization of the floating basis protocol. The pseudo-random sequence, generated by a Legendre symbol Pseudo-Random Number Generator (PRNG), determines the rotations by an arbitrary angle (from a finite set) of the standard basis (i.e., rectilinear). A small secret, known a priori, is used as a seed to the PRNG. The authors showed that the multi-bases variant of the suggested scheme outperforms the BB84 and the asymmetric BB84 protocol regarding the secret key rates. However, the protocol crucially requires single-photon sources. Otherwise, the eavesdropper could guess the initial secret (and thus, the pseudo-random bases) with a non-negligible probability of intercepting only a small number of three-photon pulses using the Photon Number Splitting (PNS) attack [50].

Similarly, the authors of [51] suggest that the secret key be used as a seed in the PRNG, resulting in a so-called running key that defines the bases sequence. The authors of [52] propose a variant of the Hwang protocol in which the base sequence is defined in a pseudo-random manner using cipher block chaining. A priori, Alice and Bob must share two secrets: the bases sequence and the initialization vector required in the cipher block chaining algorithm. Furthermore, a family of coherent-state quantum key distribution protocols with correlated pseudo-random bases sequence has been introduced in [53,54].

Most recently, in [55] improved variant of the Hwang protocol has been proposed in which shift register, filled with secret bits, is used to define the basis sequence. Assuming the key distribution technique yields a secret key of length $m$, the content of the register is shifted to the left by $m$ bits, and the distributed secret key is appended to the shift register. In this manner, a bases sequence is updated for each protocol's round. The leftmost bits pushed out of the register due to the shift are passed through the key derivation function based on universal hash functions. The outcome provides key that is used for cryptographic purposes.

## 3. Bases selection with PRFs based on HMAC construction

Assuming that Alice and Bob share an ITS secret, they can utilize it to define a significantly larger secret in the traditional manner. Because the expanded form is not truly random (true randomness of expanded form can only be achieved through the proven process of QKD), it would be naive and incorrect to use it as an ITS secret key in any cryptographic task. If, on the other hand, the secret or its expanded form is never revealed, the adversary has a negligible chance of guessing it. This section describes a specific method for expanding the secret in a traditional manner, as well as the benefits obtained when such expanded form is used as a definition of correlated bases selection in the BB84 scheme.

### 3.1. Bases selection

In the proposed scheme, Alice and Bob use a small amount of preshared key material obtained from the basic BB84 scheme or the previous execution of the scheme proposed here to create a (larger) shared secret that defines bases selection. By concentrating the outputs of the PRFs based on the HMAC construction, the bases sequence is defined by Equation (3), where $K$ and $S$ are the ITS symmetric keys known a priori to the communication parties, $0x01$, $0x02$, etc. are single octets,[3] and a symbol | represents a concentration. In general, an input message $S$ does not need to be secret; however, we argue that a secret message $S$ provides additional security.

$$\begin{aligned} &bases\ sequence = T1 \mid T2 \mid T3 \mid T4 \mid ... \\ &T1 = PRF(K,\ S \mid 0x01) \\ &T2 = PRF(K,\ T1 \mid S \mid 0x02) \\ &T3 = PRF(K,\ T2 \mid S \mid 0x03) \\ &T4 = PRF(K,\ T3 \mid S \mid 0x04) \\ &... \end{aligned} \tag{3}$$

[1] The authors suggest that there is no way for an eavesdropper to obtain information about the distributed key, so privacy amplification is optional. However, the eavesdropper may obtain partial information about the preshared key, necessitating privacy amplification prior to the merging operation.

[2] In theory, there are an infinite number of possible bases, but in practice, this number is limited by the ability to represent basis position accurately.

[3] Instead of a single octet, two or more octets may be used to allow for greater expansion, i.e., calculation of many $Ti$ outputs without restarting the octet counter.

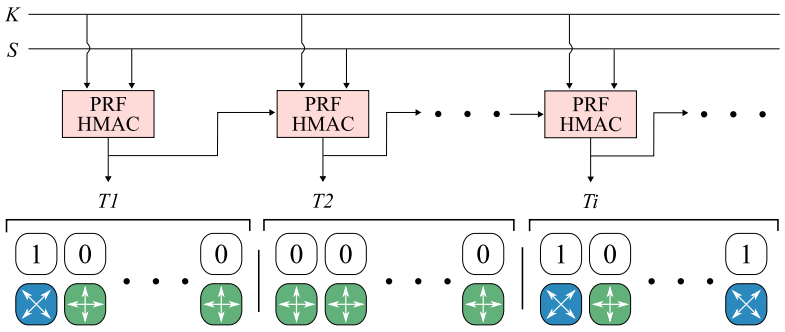



**Fig. 5.** The general idea of bases selection with PRF based on HMAC construction; $K$ and $S$ are ITS secrets established with basic BB84 scheme or previous execution of scheme proposed here; $Ti$ are outputs of PRF functions based on HMAC construction and thus, are uniform in distribution and indistinguishable from a true-random sequence. This figure does not depict additional octet inputs to PRFs.

Fig. 5 depicts this procedure, which is none other than HMAC-based extract–and–expand Key Derivation Function (HKDF) [56]. However, only the second step – expand – is used in this case, with the first step – extract – skipped. Randomness extractors (which may or may not be based on HMAC) are used to extract highly random output with a uniform distribution from a weak random entropy source [57]. In our case, the secret key $K$ is a true–random sequence, so the randomness extractor is not applied. It should be noted that for each QKD protocol round, $K$ and $S$ are refreshed.

The key consumption during the bases selection process (3) is minuscule (e.g., if HMAC SHA-512 is used as a PRF, the key $K$ must be 512 bits in size, and the secret message $S$ can be as short as 128 bits) in comparison to the efficiency benefits provided by the scheme, i.e., roughly doubling the final key size/rate of the basic BB84 scheme. The final key rate is directly proportional to the sifted key rate, which can be defined in a simplified form by the Equation (4), where $\nu$ is source repetition rate, $\mu$ is mean photon number ($\mu \simeq 0.1$),[4] $T_{link}$ is attenuation of the fiber, i.e., a probability of photon to arrive the detection suite, and $\eta$ is detection efficiency [58,59].

$$R_{sifted} = g_p \cdot R_{raw} = g_p \cdot (\nu \cdot \mu \cdot T_{link} \cdot \eta) \tag{4}$$

Because the bases selections are perfectly correlated, our proposed scheme has a 100% efficiency factor ($g_p = 1$), which is double the 50% efficiency factor of the basic BB84 scheme. As a result, the sifted key rate (4) is also doubled as shown by Equation (5).

$$\frac{g_{p-proposed} \cdot R_{raw}}{g_{p-bb84} \cdot R_{raw}} = \frac{1 \cdot R_{raw}}{0.5 \cdot R_{raw}} = 2 \tag{5}$$

### 3.2. Security considerations

To jeopardize the proposed scheme's security, the eavesdropper would have to break the (3) by disclosing $K$ and $S$. However, this appears to be impossible without knowing the bases sequence itself (how can one disclose inputs of HMAC, without knowing the output?). The laws of quantum mechanics prevent the eavesdropper from gaining any knowledge on the bases of the intercepted quantum carriers. The eavesdropper can intercept and measure quantum carriers; however, the result does not reveal any information about the basis, and the eavesdropper cannot be certain that the measurement was compliant. As a result, because the eavesdropper knows nothing about $K$, $S$, and outputs $Ti$, there is no attack strategy to reveal the bases sequence. To the eavesdropper, the bases sequence appears as a true-random sequence. Because it is a slight variation of the Hwang protocol, the exact security proofs apply, and thus the proposed scheme is, in theory, ITS secure [44].

Furthermore, because the proposed scheme does not require public announcement of bases at all, the eavesdropper uncertainty is not alleviated, and the amount of leaked information under incoherent attacks is lower when compared to the basic BB84 scheme [43]. As a result, the secret key rate of the proposed scheme $S$ is no worse than that of the BB84 scheme, and is given with Equation (6), where $I(X;Y)$ is a mutual information shared by Alice and Bob, $I(X;Z)$ is a mutual information shared by Alice and the eavesdropper, i.e., the amount of leaked information, $h$ is a binary entropy, and $e$ is the QBER [59].

$$\begin{aligned} S \geq S_{BB84} &= I(X;Y) - I(X;Z) \\ &= 1 - h(e) - 2 \cdot e \end{aligned} \tag{6}$$

The equation (6) applies to a full intercept and resend attack in which the amount of information shared by Alice and the eavesdropper is $I(X;Z) = 2 \cdot e = \frac{1}{2}$ [42].[5] In this attack, the eavesdropper listens to the public announcement of bases to eliminate measurement

[4] Due to the lack of perfect single photon sources, practical implementations rely on faint laser pulses with very low mean photon number [58].

[5] If the eavesdropping applies to all quantum carriers, the amount of errors $e$ introduced by the eavesdropper in the BB84 scheme is $e = \frac{1}{4}$. If however, only a fraction $p_{IR}$ of quantum carriers are intercepted, the QBER is defined as $e = \frac{p_{IR}}{4}$ and the amount of leaked information is given as $I(X;Z) = \frac{p_{IR}}{2} = 2 \cdot e$.

uncertainties. Because our protocol does not require public announcement of bases, neither the full intercept and resend attack nor the intercept and resend attack in the Breidbart basis apply. As a possible strategy, the eavesdropper is left with a naive intercept and resend attack. In this case, the amount of information leaked is significantly less $I(X;Z) \simeq 0.2$ [42] and the secret key rate is $S = 1 - h(e) - \frac{4}{5} \cdot e$.

For the purposes of discussing a practical security, let's assume that the eavesdropper has partial information about the bases sequence defined by (3). The output of the PRFs based on HMAC construction is uniform in distribution and indistinguishable from random. We argue that it is challenging to reveal secrets $K$ and $S$ with only partial knowledge of the PRFs' outputs $T_i$. The fact that only a small percentage of pulses are non-empty ($\mu \approx 0.1$), and only about 5% of them contain more than one photon [58], means that the eavesdropper can determine only a few bits of the output $Ti$ using PNS attack.[6] The cryptographic hash functions (which are an integral part of HMAC), have a one-way, or pre-image resistance property, which means that given the output $H(x)$ and the hash function $H$, it is still computationally infeasible to find the input $x$ [60]. But given only a fraction of the output $H(x)$ (as in the proposed application), finding the input $x$ would certainly be much more difficult. In general, most hash function attacks assume knowledge of the output (and, in some cases, the input) and hash function, but in the proposed application for bases selections, only a fraction of the output (thus, the input for the following $T_{i+1}$ calculation) can be known. The computational security of the one-way property, or other properties of the underlying hash function, raises concerns. However, even the large-scale quantum computing is expected to weaken rather than break the security of hash functions [1]. As a result, the use of quantum-resistant hash functions (e.g., SHA-2, SHAKE, SHA-3, RIPEMD, Blake2 [1]), is required, preferably in 256 bit and higher variants. It should be noted that a successful attack on (3) is only beneficial for a short period of the quantum transfer, and if this short-term security can be guaranteed, the security of distributed key can also be guaranteed under that assumption.[7] If a hash function is broken in the future, it will not affect the security of previously established keys or sensitive data protected by them. The scheme can then be easily modified by implementing a new quantum-resistant hash function. This is not the case with other computationally secure key distribution protocols, in which key exchange and confidential data can be recorded, cracked, and reviled after the fact. To improve security in practical implementations, a scheme can be combined with decoy states, primarily to detect passive eavesdropping on multi-photon pulses. However, we do not provide quantitative amounts of security in practical realizations in this paper, instead focusing on the possibilities that the proposed method would provide in light of current trends in QKD networks. We discuss this in Section 4, where we share the light on how our protocol compares to others in some practical sense, as well as the benefits of using our proposed method.

Furthermore, because Alice and Bob use perfectly correlated bases selections, a multi-base variant of the proposed scheme is feasible without sacrificing efficiency. In this case, the proposed scheme can be viewed as a formalization of the floating basis protocol (see Section 2.3), which includes all the advantages of this protocol.

## 4. Discussion

This paper presents a variant of the BB84 scheme that does not require public discussion of base selections. In theory, the proposed variant is ITS. This security is inherited from the base Hwang protocol, whose security has been proven. However, the question arises as to how to benefit from these QKD schemes, whose security in practical applications is not known. It is justifiable to conclude that some of the suggested solutions do not work in practical environments because they fail to take into account a drawback of realistic single-photon sources (i.e., faint laser pulses with very low mean photon number $\mu$): most of the pulses are empty [58]. This is why the Hwang protocol would necessitate numerous repetitions of a basis sequence $k$ to accumulate sufficient raw key material, or the pre-shared secret $k$ would be impractically large. Similarly, source and medium capabilities are disregarded in solutions that assume that a $N$ bit base sequence is sufficient to provide an equal number of raw/sifted key bits.[8] Therefore, these solutions cannot be implemented in practice without reusing, i.e., repeating, the base sequence. Significant correlation may threaten security in a real-world setting by simply reusing the bases sequence, as in the Hwang protocol. This is because of an additional drawback where light pulses in practical single-photon sources may contain more than one photon [58]. Using the PNS attack on the Hwang protocol, after 50 reuses, one can obtain all of the basis's information without being detected [55]. To overcome these limitations, the basis sequence cannot be arbitrarily long, since this would result in a protocol that uses more secret key material than it produces. The most recent method, based on a shift register [55], is an exception. The memory requirements, however, would be substantial, and there would still be a significant correlation between succeeding generation repetitions. This is because a considerable amount of the base sequence remains unchanged and is simply sifted by the length of the newly generated key. During the key distillation process, an adversary can discover the length of the generated key and thus the sift. As a result, the identical problem revealed in the Hwang protocol is present here. Our scheme, on the other hand, does not have these limitations and does not require the storage of base sequences other than the two outputs (of relatively small size, 256, 512 bits, or larger, depending on the hash function used), $T_{i-1}$ and $T_i$ at the time. The quantity of key material to keep the scheme functioning, i.e., key consumption, is minimal.

Compared to more practical variants [49,51,52], we argue that PRFs based on HMAC construction are more secure than a simple PRNG or one based on cipher block chaining. It is no accident that this method is the most often used to generate several

[6] If SHA-512 is considered as PRF, the PNS attack can only yield about 2 to 3 bits on given $T_i$ on average.

[7] It should be noted that similar assumptions are sometimes made for public channel authentication, where instead of ITS authentication, parties choose to use quantum-resistant schemes. This decision is most likely to be made during the initial execution of the QKD process, when the parties have not previously shared any ITS key material. The subsequent rounds of the QKD process may use ITS authentication with previously established keys.

[8] Losses in the transmission medium might prevent light particles from reaching the detection suite.

cryptographic keys from a single secret. However, quantitative security analysis is still lacking in our proposal. Compared to the asymmetric BB84 protocol, which has relatively large memory requirements, our method requires fewer resources. This is due to the fact that in order to provide the same level of security as the standard BB84 protocol, the asymmetric BB84 protocol needs a significantly higher quantity of raw key material. This increases the load since successive key generation instances need a longer time frame, especially if one of the rounds fails due to inordinate noise. This may affect achievable key rates in continuous operation in practical deployments.

Compared with traditional key exchange methods, the method proposed here has considerable security advantages, even in the case of imperfect practical technology. Classical key exchange algorithms that are commonly used, as well as potential post-quantum ones, may be simply captured with the encrypted data they protect. If the algorithm has been broken or weakened by technological advancements, the key is revealed along with the encrypted data. This "store now and decrypt later" attack does not apply to the method described here. An attack on our key exchange method is only effective while it is being executed. Breaking the HKDF algorithm after the fact has no effect on previously established secret keys and does not put previously transmitted confidential data at risk. As a result, as long as we can affirm with certainty that HKDF is secure during a quantum transfer, the established key can be used with the OTP cipher to provide long-term security to confidential data. This is a novel middle ground between QKD's overly strict ITS security profile and the dubious long-term security of post-quantum algorithms. The QKD network is anticipated to support an extensive user base with a range of security requirements. As a result, users that depend on computationally secure algorithms, such as AES, only require to have a key that is at least as secure as the encryption algorithm itself, rather than an ITS cryptographic key. We argue that the scheme proposed here is more secure (in practical applications, using imperfect quantum technologies; in theory it is proven to be ITS) than classical and post-quantum key exchange methods, and can provide secret keys with everlasting security based on guaranteed short-term security. It should be recognized as such and utilized within present QKD networks to supply keys at a faster rate, drawing greater attention as a viable key exchange primitive. The advantage is that we can simply switch between the standard BB84 protocol and the one presented here, allowing us to serve customers with various security needs.

## 5. Conclusion

In this study, we propose that PRFs based on the HMAC construction be used to define the perfectly correlated selection of bases in the BB84 scheme, eliminating the need for the public announcement of bases. This concept not only leads to increased scheme efficiency (from BB84's original 50% to a 100%) and key rates, but it also allows for significant additional benefits in multi-bases variants. The scheme requires only a small amount of preshared ITS bits (in each QKD protocol round) to operate, which may be obtained from the basic BB84 scheme or the previous execution of the proposed scheme. The proposed scheme is, in theory, ITS secure. Quantitative amounts of security in practical deployments are lacking and have yet to be provided. The scheme has the potential to expand the capacity of QKD networks, allowing them to serve more users while meeting their diverse security requirements.

## CRediT authorship contribution statement

**Emir Dervisevic:** Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Miroslav Voznak:** Funding acquisition, Formal analysis. **Miralem Mehic:** Supervision, Formal analysis.

## 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.

## Data availability

No data was used for the research described in the article.

## Acknowledgement

The research leading to the published results was supported by the European Union within the REFRESH project - Research Excellence For Region Sustainability and High-tech Industries ID No. CZ.10.03.01/00/22 003/0000048 of the European Just Transition Fund and under the NATO SPS G5894 project "Quantum Cybersecurity in 5G Networks (QUANTUM5)". The work was partly supported by the H2020 project OPENQKD under grant agreement No. 857156. This work was also supported by the Ministry of Science, Higher Education and Youth of Canton Sarajevo, Bosnia and Herzegovina under Grant No. 27-02-35-37082-1/23, within the project DQKDNM 2023.

## References

[1] R.A. Grimes, Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto, John Wiley & Sons, 2019.

[2] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, 1984, p. 8.
[3] G.S. Vernam, Cipher printing telegraph systems: for secret wire and radio telegraphic communications, J. AIEE 45 (2) (1926) 109–115.
[4] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (4) (1949) 656–715.
[5] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, et al., Quantum key distribution: a networking perspective, ACM Comput. Surv. 53 (5) (2020) 1–41.
[6] C. Elliott, Building the quantum network, New J. Phys. 4 (1) (2002) 46.
[7] P.D. Townsend, Quantum cryptography on multiuser optical fibre networks, Nature 385 (6611) (1997) 47–49.
[8] B. Fröhlich, J.F. Dynes, M. Lucamarini, A.W. Sharpe, Z. Yuan, A.J. Shields, A quantum access network, Nature 501 (7465) (2013) 69–72.
[9] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, et al., Robust and adaptable quantum key distribution network without trusted nodes, Optica 9 (7) (2022) 812–823.
[10] P.K. Tysowski, X. Ling, N. Lütkenhaus, M. Mosca, The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD), Quantum Sci. Technol. 3 (2) (2018) 024001.
[11] A.R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, A. Shields, Continuous operation of high bit rate quantum key distribution, Appl. Phys. Lett. 96 (16) (2010).
[12] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, A. Shields, Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks, Appl. Phys. Lett. 104 (5) (2014).
[13] M. Mehic, P. Fazio, S. Rass, O. Maurhart, M. Peev, A. Poppe, J. Rozhon, M. Niemiec, M. Voznak, A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks, IEEE/ACM Trans. Netw. 28 (1) (2020) 168–181.
[14] M. Mehic, S. Rass, E. Dervisevic, M. Voznak, Tackling denial of service attacks on key management in software-defined quantum key distribution networks, IEEE Access 10 (2022) 110512–110520.
[15] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, J. Zhang, SDQaaS: software defined networking for quantum key distribution as a service, Opt. Express 27 (5) (2019) 6892–6909.
[16] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, et al., Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area, Commun. Phys. 5 (1) (2022) 162.
[17] F. Grünenfelder, A. Boaron, G.V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, et al., Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems, Nat. Photonics 17 (5) (2023) 422–426.
[18] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, et al., High-rate quantum key distribution exceeding 110 Mb s–1, Nat. Photonics 17 (5) (2023) 416–421.
[19] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, et al., Satellite-based entanglement distribution over 1200 kilometers, Science 356 (6343) (2017) 1140–1144.
[20] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, et al., Satellite-to-ground quantum key distribution, Nature 549 (7670) (2017) 43–47.
[21] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, et al., Twin-field quantum key distribution over 830-km fibre, Nat. Photonics 16 (2) (2022) 154–161.
[22] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, et al., Quantum key distribution over 658 km fiber with distributed vibration sensing, Phys. Rev. Lett. 128 (18) (2022) 180502.
[23] S.P. Neumann, A. Buchner, L. Bulla, M. Bohmann, R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, Nat. Commun. 13 (1) (2022) 6134.
[24] V. Lopez, A. Pastor, D. Lopez, A. Aguado, V. Martin, Applying QKD to improve next-generation network infrastructures, in: 2019 European Conference on Networks and Communications (EuCNC), IEEE, 2019, pp. 283–288.
[25] P. Wright, C. White, R.C. Parker, J.-S. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R.V. Penty, et al., 5G network slicing with QKD and quantum-safe security, J. Opt. Commun. Netw. 13 (3) (2021) 33–40.
[26] M. Mehic, S. Rass, P. Fazio, M. Voznak, Modern trends in quantum key distribution networks, in: Quantum Key Distribution Networks, 2022, pp. 209–223.
[27] M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, N. Mahovac, F. Richter, E. Kaljic, F. Lauterbach, et al., Quantum cryptography in 5G networks: a comprehensive overview, IEEE Commun. Surv. Tutor. (2023).
[28] C. Wang, A. Rahman, Quantum-enabled 6G wireless networks: opportunities and challenges, IEEE Wirel. Commun. 29 (1) (2022) 58–69.
[29] H.A. Al-Mohammed, E. Yaacoub, On the use of quantum communications for securing IoT devices in the 6G era, in: 2021 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2021, pp. 1–6.
[30] A. Nadia, S.B. Sadkhan, Cryptography techniques within SCADA system-asurvey, in: 2020 3rd International Conference on Engineering Technology and Its Applications (IICETA), IEEE, 2020, pp. 89–94.
[31] P.-Y. Kong, A review of quantum key distribution protocols in the perspective of smart grid communication security, IEEE Syst. J. 16 (1) (2020) 41–54.
[32] M. Kaur, S. Kalra, Security in IoT-based smart grid through quantum key distribution, in: Advances in Computer and Computational Sciences, Springer, 2018, pp. 523–530.
[33] R. Diovu, J. Agee, Enhancing the security of a cloud-based smart grid AMI network by leveraging on the features of quantum key distribution, Trans. Emerg. Telecommun. Technol. 30 (6) (2019) e3587.
[34] E. Dervisevic, M. Mehic, Overview of quantum key distribution technique within IPsec architecture, in: Proceedings of the 18th International Conference on Information Systems for Crisis Response and Management ISCRAM 2021, ACM, 2021, pp. 1–10.
[35] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, Phys. Rev. Lett. 92 (5) (2004) 057901.
[36] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Phys. Rev. Lett. 91 (5) (2003) 057901.
[37] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, Experimental quantum cryptography, J. Cryptol. 5 (1992) 3–28.
[38] M. Mehic, M. Niemiec, H. Siljak, M. Voznak, Error reconciliation in quantum key distribution protocols, in: Reversible Computation: Extending Horizons of Computing: Selected Results of the COST Action IC1405, vol. 12070, 2020, p. 222.
[39] M. Mehic, S. Rass, P. Fazio, M. Voznak, Fundamentals of quantum key distribution, in: Quantum Key Distribution Networks, Springer, 2022, pp. 1–28.
[40] C.H. Bennett, G. Brassard, J.-M. Robert, How to reduce your enemy's information, in: Conference on the Theory and Application of Cryptographic Techniques, Springer, 1985, pp. 468–476.
[41] H.-K. Lo, H.F. Chau, M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptol. 18 (2) (2005) 133–165.
[42] C. Kollmitzer, M. Pivk, Applied Quantum Cryptography, vol. 797, Springer, 2010.
[43] W.Y. Hwang, I.G. Koh, Y.D. Han, Quantum cryptography without public announcement of bases, Phys. Lett. A 244 (6) (1998) 489–494.
[44] W.-Y. Hwang, X.-B. Wang, K. Matsumoto, J. Kim, H.-W. Lee, Shor-Preskill-type security proof for quantum key distribution without public announcement of bases, Phys. Rev. A 67 (1) (2003) 012302.
[45] S. Ji, H. Lee, G.L. Long, Secure quantum key expansion between two parties sharing a key, J. Korean Phys. Soc. 51 (4) (2007) 1245.
[46] Y. Kurochkin, Quantum cryptography with floating basis protocol, in: Quantum Informatics 2004, vol. 5833, International Society for Optics and Photonics, 2005, pp. 213–221.

[47] V. Kurochkin, Y. Kurochkin, Principles of the new quantum cryptography protocols building, Phys. Part. Nucl. Lett. 6 (7) (2009) 605–607.
[48] Y.V. Kurochkin, A. Fedorov, V. Kurochkin, Quantum key distribution with floating bases and decoy states, in: QCrypt, 2016.
[49] A. Trushechkin, P. Tregubov, E.O. Kiktenko, Y.V. Kurochkin, A.K. Fedorov, Quantum-key-distribution protocol with pseudorandom bases, Phys. Rev. A 97 (1) (2018) 012311.
[50] B. Huttner, N. Imoto, N. Gisin, T. Mor, Quantum cryptography with coherent states, Phys. Rev. A 51 (3) (1995) 1863.
[51] H.P. Yuen, Key generation: foundations and a new quantum approach, IEEE J. Sel. Top. Quantum Electron. 15 (6) (2009) 1630–1645.
[52] S. Lin, X.-F. Liu, A modified quantum key distribution without public announcement bases against photon-number-splitting attack, Int. J. Theor. Phys. 51 (8) (2012) 2514–2523.
[53] A.S. Avanesov, D.A. Kronberg, Coherent-state quantum cryptography using pseudorandom number generators, Quantum Electron. 49 (10) (2019) 974.
[54] A.S. Avanesov, D.A. Kronberg, On applying pseudorandom number generators in quantum cryptography with coherent states, in: AIP Conference Proceedings, vol. 2241, AIP Publishing LLC, 2020, p. 020026.
[55] Q. Jia, K. Xue, Z. Li, M. Zheng, D.S. Wei, N. Yu, An improved QKD protocol without public announcement basis using periodically derived basis, Quantum Inf. Process. 20 (2) (2021) 1–11.
[56] H. Krawczyk, P. Eronen, HMAC-based extract-and-expand key derivation function (HKDF), RFC 5869, RFC Editor, https://www.rfc-editor.org/rfc/rfc5869, May 2010.
[57] O. Chevassut, P.-A. Fouque, P. Gaudry, D. Pointcheval, Key derivation and randomness extraction, Cryptology ePrint Archive, 2005.
[58] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (1) (2002) 145.
[59] G. Van Assche, Quantum Cryptography and Secret-Key Distillation, Cambridge University Press, 2006.
[60] R. Sobti, G. Geetha, Cryptographic hash functions: a review, Int. J. Comput. Sci. Issues 9 (2) (2012) 461.