Quantum Information Processing (2019) 18:7
https://doi.org/10.1007/s11128-018-2124-2

Quantum identity authentication without entanglement

Piotr Zawadzki[1]

Received: 7 August 2018 / Accepted: 10 November 2018 / Published online: 19 November 2018

Abstract
An interesting protocol for quantum identity authentication on a basis of the classic shared secret has been presented recently (Hong et al. in Quantum Inf Process 16(10): 236, 2017). It requires few resources and it is technologically feasible. Its seminal analysis focuses on average eavesdropper's information gain per single protocol run—a parameter suitable for estimation of the security margin applicable to the protocols aiming at provision of confidentiality. However, the security requirements of the authentication process are very stringent—no single bit of the secret can be revealed, otherwise the eavesdropper can collect subsequent bits of the secret in successive protocol runs. The failure of the seminal version to meet this requirement is demonstrated. The sequential processing of qubits and the static nature of the compared data is the rationale behind the improvement. The introduced changes make that partial information gained in some authentication attempt gives the eavesdroppers no advantage in breaking the next ones. They are forced to consider each authentication transaction as a separate puzzle that can be solved according to all-or-nothing paradigm. The improvement retains conceptual simplicity and technological feasibility of the seminal version of the protocol.

Keywords Quantum cryptography · Quantum communication · Quantum identity authentication

1 Introduction

The quantum cryptography, since the pioneering works of Wiesner [1], Ingarden [2] and Bennett et al. [3], grew up into a full-blown research discipline. It aims at provision of cryptographic primitives with security driven by the laws of physics [4,5]. Quantum key distribution (QKD) [3,4,6–8], quantum direct communication (QDC) [9–12], quantum secret sharing (QSS) [13,14], quantum private comparison (QPC)

✉ Piotr Zawadzki
Piotr.Zawadzki@polsl.pl

[1] Institute of Electronics, Akademicka 16, 44-100 Gliwice, Poland

[15] and quantum identity authentication (QIA) [16] are subject of ongoing research on exploiting the nonclassicallity of physical systems to provide features not available within classical paradigm. Some of the these new protocols have been realized in laboratory [17–21] or deployed in the field [22].

The authentication is a cryptographic primitive that aims at verification of some unique feature of the data. It involves two entities—the supplicant that states the claim and the authenticator who checks whether the claim is true. The term "authentication" is used in two different contexts in cryptography. In data authentication, the authenticator checks the claim in offline mode using only the received chunk of data. Contrary, in user or identity authentication, the parties perform an interactive protocol in which supplicant proves possession of some unique data, i.e. that he knows some shared secret or he posseses some token or he has some attribute. The security of the protocol requires that no sensitive information exchanged during its execution can leak to the potential eavesdropper. The classical solutions of the problem rely on a challenge-response protocol: (a) the authenticator feeds the supplicant with random data, (b) the authenticator requests the supplicant to perform computations that involve the data and the shared secret, (c) the authenticator checks whether the result provided by the supplicant matches the result computed earlier locally. The challenge-response protocol draws the security from computational complexity of inverting the function that mixes shared secret with random parameter known to eavesdropper. It is susceptible to brute force or dictionary attacks when the shared secret is too simple. To avoid that, the protocol is frequently executed in encrypted tunnel, which is set up with the help of public key algorithms. However, it has been demonstrated that quantum computers can potentially provide exponential speed-up of some calculations, and that they can be used to break public key cryptography [23]. All that renders potential insecurity of classical solutions.

QIA aims at the design of protocols with security resulting from the laws of physics. Quantum mechanics guarantee that even most powerful eavesdropper with a full access to the quantum channel cannot perfectly distinguish non-orthogonal or partially accessible quantum states and his actions inevitably introduce disturbances which can be detected by authenticating parties. Many authors have sought for the improvement in the authentication process in the quantum nature of the shared secret, i.e. its partial accessibility to the eavesdropper. Zeng et al. [24] proposed an identity verification system based on entanglement distribution centre which also serves as an arbitrator in the protocol eavesdropping detection phase. Ljunggren [25] proposed authentication scheme based on the fully trusted arbitrator and a family of entanglement-based protocols for shared secret distribution. Shi et al. [26] and Wei et al. [27] proposed a scheme based on a shared entangled state between two participants which can authenticate each other without classical channel. Zhou et al. [28] proposed two authentication schemes based on teleportation and entanglement swapping. The schemes are accomplished by transmitting identity information via quantum channels using shared EPR pairs and by exchanging necessary commands through public, unprotected classical channels.

Provision of entangled secrets that can be shared for a long time in a room temperature is a challenging task for the present day technology because of the inevitable decoherence. QIA protocols based on classic shared secret avoid this difficulty. In this class of protocols, quantum mechanics is used as a tool for provision of privacy for the authentication process, i.e. it is used as a replacement of an encrypted tunnel used in

classic variants of user authentication. In the simplest case, this encrypted tunnel can be provided by links protected by QKD technology along with the one-time-pad cipher as in Dušek et al. [29]. However, bootstrap of QKD requires authenticated classic channel which is achieved by classic cryptographic techniques. A method of classic secret verification based on purely quantum communication and employing techniques used in QDC has been proposed by Zhang et al. [30]. Lee et al. [31] proposed protocol in which an arbitrator shares separate classic secret keys with registered parties. On data transmission request, the arbitrator generates GHZ states and posts single particles to communicating peers. The entanglement of GHZ states is used to verify users' identities and transfer confidential information. The arbitrator is involved not only in the authentication process but also he has to cooperate in the communication process. Thus it is implicitly assumed that he is fully trusted. That fact has been demonstrated by Yen et al. [32] and the protocol's improvement exploiting entanglement swapping to isolate the arbitrator from the communication process has been presented. Recently, Hong et al. [33] proposed an interesting method of classic secret verification that can be regarded as an adaptation of the famous BB84 protocol [3] for this specific task. However, it has some security deficiencies in operation mode described in the seminal paper—the authenticated classic channel is required and some bits of the shared secret may leak out.

This contribution proposes improvement in the Hong et al. [33] protocol and it provides comparison of both versions. The paper is organized as follows. Section 2 summarizes Hong et al. proposal and provides discussion of identified deficiencies. The remedy and its rationale, which is the main contribution of the paper, is presented in Sect. 3. Concluding remarks constitute the last section.

2 Analysis

Security requirements for the identity authentication protocols are very stringent:

- none of the bits of the shared secret can be exposed to the eavesdropper,
- shared secret is unchanged between subsequent unsuccessful protocol runs,
- no prior authentication of the supporting classical channel can be assumed.

The following discussion of the protocol under consideration takes the aforementioned aspects into account.

The seminal protocol [33] operates in message or control modes that are randomly interwoven. Alice and Bob:

- share a secret k composed of even number of bits,
- can communicate with the classic public channel and an unprotected quantum one,
- agree to use rectilinear $\mathscr{B}_0 = \{|0\rangle, |1\rangle\}$ and diagonal $\mathscr{B}_1 = \{|+\rangle, |-\rangle\}$ bases,
- use rules from Table 1 to encode a pair of classic bits into a quantum state.

The protocol continues as follows:

1. Both parties set counter $n = 0$.
2. If n is greater that length of the secret—authentication successful, otherwise proceed.
3. Alice randomly selects message or control mode:

Table 1 Encoding rules used by Alice and Bob

Even bit value (k_n)	Basis	Odd bit value (k_{n+1})	Quantum state
0	$\mathscr{B}_0$	0	$\|0\rangle$
0	$\mathscr{B}_0$	1	$\|1\rangle$
1	$\mathscr{B}_1$	0	$\|+\rangle$
1	$\mathscr{B}_1$	1	$\|-\rangle$

4. Message mode:
   (a) Alice takes bits (k_n, k_{n+1}) of the shared secret and she constructs a quantum state according to Table 1.
   (b) Alice sends the state to Bob.
   (c) Bob measures the incoming state. He selects the measurement basis using bit k_n of his own copy of the shared secret. The measurement outcome equals to k'_{n+1}.
   (d) Bob announces reception. Alice communicates that they operate in message mode.
   (e) Bob compares the received and the expected value of the bit. If $k'_{n+1} = k_{n+1}$ then proceed: confirm cycle success to Alice, $n = n + 2$, then go to step 2; otherwise abort the protocol.
5. Control mode
   (a) Alice creates the pair (k_n, d) from the even bit of the shared secret and some random bit d and then, on their basis, she constructs a quantum state according to Table 1.
   (b) Alice sends the state to Bob.
   (c) Bob measures incoming state. He selects the measurement basis using bit k_n of his own copy of the shared secret. The measurement outcome equals to d'.
   (d) Bob announces reception. Alice communicates that they operate in control mode and the value of d.
   (e) Bob compares the received and the expected value of the bit. If $d' = d$ then proceed: confirm cycle success to Alice, $n = n + 2$, go to step 2, otherwise abort the protocol.

2.1 Man-in-the-middle attack

Let Eve impersonates Alice. The MITM attack assumes that Eve measures photons coming from Alice and forwards fake ones in a state derived from the measurement outcome. If Eve selects measurement basis correctly, nothing special happens: (a) her outcome is in agreement with Alice's encoding, (b) the reconstructed photon is in a correct state, (c) secret bit decoded by Bob has the expected value so the protocol continues. However, if Eve selects basis incorrectly there is a 50% chance that Bob's decoding fails. This happens independent on operation mode selected by Alice. The

situation in which Bob's measurement yields, by an accident, the expected result is not interesting—the protocol simply continues and Eve has no clue what was the basis and value of the encoded qubit—it can be correct one because of two reasons: (a) proper basis selection, (b) random nature of quantum measurement outcome in improper basis. On the other hand, if Bob's measurement yields an incorrect result then the protocol is aborted (points 4e and 5e of the seminal protocol specification). This is a sign for Eve, that the basis she has selected is incorrect. Eve learns that way the value of the even numbered bit k_n of the shared secret that is responsible for the basis selection. Alice probably takes another try to authenticate. In the next protocol run, Eve will select the correct basis for the protocol cycle controlled by the known bit and she will learn the value of the odd numbered bit k_{n+1} responsible for the photon polarization. For the rest of photons, she might still use the measure and resend strategy. In case of protocol abortion, she will learn the value of another evenly numbered bit. Smart policy of selection of protocol cycles to be attacked permits Eve to learn bits of the shared secret as long as Alice and Bob won't be changing the shared secret frequently.

2.2 Entangle and discriminate attack

The seminal proposal [33] includes analysis of the entangle and measure attack, in which Eve entangles the travel qubit with her own probe register. Depending on the outcome of Bob's measurement, the probe is left in different states and, on this basis, Eve can draw information on the state of the travel qubit. The price she pays for her knowledge is a nonzero error rate observed by Bob. Various entangling strategies and probe states discrimination techniques result in distinct trade-offs between Eve's information gain and induced error rate. The seminal analysis estimates Eve's information gain assuming minimum error discrimination and availability of infinite number of copies of the state to be examined. The discussion presented below addresses the success rate of entangle and measure attack with Eve having an access to only one copy of the state to be discriminated. It is shown that under this restriction, the seminal version of the protocol is not secure in the context of constraints quoted at the beginning of this section.

It is known that for the BB84 protocol, which is mimicked by the protocol under consideration, the optimal information gain is provided by the Brandt probe [34,35] that uses non-orthogonal probe states and $\overline{CNOT}$ gate as the entangling operation. Let the bases used by Alice and Bob be denoted $\mathscr{B}_0 = \{|u\rangle, |\bar{u}\rangle\}$ and $\mathscr{B}_1 = \{|v\rangle, |\bar{v}\rangle\}$ and be rotated for $\pm\pi/8$ relative to the computational basis used by Eve in construction of the entangling operation, as depicted in Fig. 1.

The bases are related to each other with the following formulas

$$|0\rangle = c|u\rangle + s|\bar{u}\rangle \qquad |1\rangle = -s|u\rangle + c|\bar{u}\rangle \tag{1}$$

$$|0\rangle = c|v\rangle - s|\bar{v}\rangle \qquad |1\rangle = s|v\rangle + c|\bar{v}\rangle \tag{2}$$

where $c = \cos\frac{\pi}{8} = \frac{1}{2}\sqrt{2+\sqrt{2}}$ and $s = \sin\frac{\pi}{8} = \frac{1}{2}\sqrt{2-\sqrt{2}}$. It is assumed that cbit 0 is encoded as $\{|u\rangle, |v\rangle\}$ depending on basis choice, while cbit 1 is encoded as

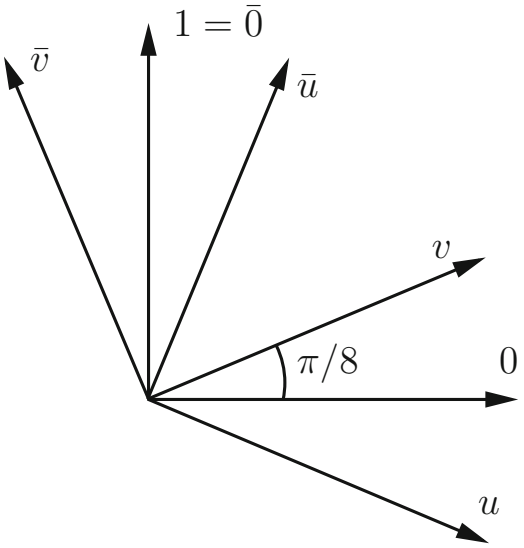

Fig. 1 Orientation of bases in Brandt probe setup

$\{|\bar{u}\rangle, |\bar{v}\rangle\}$ (see Table 1). Eve simply entangles the travel qubit with the probe register using $\overline{CNOT}$ gate controlled by the travel qubit

$$\overline{CNOT} = |0\rangle\langle 0| \otimes \overline{I} + |1\rangle\langle 1| \otimes \overline{X} \tag{3}$$

where $\overline{I}$ is the identity operator and $\overline{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$ denotes bit flip applied to the target register. Eve has a freedom of selection of the initial state $|\chi\rangle$ placed in the probe register. The following identities hold true, independent on its value

$$|u\rangle|\chi\rangle \xrightarrow{\overline{CNOT}} |u\rangle\left(c^2\overline{I} + s^2\overline{X}\right)|\chi\rangle + |\bar{u}\rangle sc\left(\overline{I} - \overline{X}\right)|\chi\rangle \tag{4}$$

$$|v\rangle|\chi\rangle \xrightarrow{\overline{CNOT}} |v\rangle\left(c^2\overline{I} + s^2\overline{X}\right)|\chi\rangle - |\bar{v}\rangle sc\left(\overline{I} - \overline{X}\right)|\chi\rangle \tag{5}$$

$$|\bar{u}\rangle|\chi\rangle \xrightarrow{\overline{CNOT}} |\bar{u}\rangle\left(s^2\overline{I} + c^2\overline{X}\right)|\chi\rangle + |u\rangle sc\left(\overline{I} - \overline{X}\right)|\chi\rangle \tag{6}$$

$$|\bar{v}\rangle|\chi\rangle \xrightarrow{\overline{CNOT}} |\bar{v}\rangle\left(s^2\overline{I} + c^2\overline{X}\right)|\chi\rangle - |v\rangle sc\left(\overline{I} - \overline{X}\right)|\chi\rangle \tag{7}$$

The second terms on the right-hand side are responsible for errors observed by Bob. Eve can tune the error rate by proper selection of the initial state. Let us assume its following parameterization

$$|\chi\rangle = \sqrt{1 - 2P_E}|+\rangle + \sqrt{2P_E}|-\rangle \tag{8}$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Then $|e\rangle = sc\left(\overline{I} - \overline{X}\right)|\chi\rangle = \sqrt{P_E}|-\rangle$ so the probability that Bob detects Eve is equal to P_E. If Bob's measurement is correct, i.e. he

does not observe an error, then there are two possible states of Eve's register

$$|\chi_0\rangle = \left(c^2\overline{I} + s^2\overline{X}\right)|\chi\rangle = \sqrt{1-2P_E}|+\rangle + \sqrt{P_E}|-\rangle \tag{9}$$

$$|\chi_1\rangle = \left(s^2\overline{I} + c^2\overline{X}\right)|\chi\rangle = \sqrt{1-2P_E}|+\rangle - \sqrt{P_E}|-\rangle \tag{10}$$

Please note that $|\chi_0\rangle$ occurs always when Alice encoded classic bit 0, independent on the selected basis. Similarly $|\chi_1\rangle$ occurs always when Alice's bit equals to 1, so detection which one of these two states is in the register is sufficient for Eve to decode odd numbered bit k_{n+1}. But the states $|\chi_0\rangle$ and $|\chi_1\rangle$ are not orthogonal, so no perfect technique to do that exists. The minimum error discrimination gives maximum average information at the price of limited confidence, so Eve is never 100% sure what was the value of the eavesdropped bit. She has to repeat the discrimination procedure multiple times on identical copies of the state to enlarge her confidence level. In contrary, an unambiguous discrimination gives Eve 100% confident information on which one state is in the register at the price of obtaining inconclusive results with some finite rate. This technique seems to be more appropriate in the context of shared secret recovery.

The rate of inconclusive measurements is equal to the overlap between discriminated states [36,37], so Eve has no clue on bit value with probability

$$Q = \frac{\langle\chi_0|\chi_1\rangle}{\|\chi_0\|\|\chi_1\|} = \frac{1-3P_E}{1-P_E} \tag{11}$$

Protocol continues until Bob observes an error. The expected number of consecutive successful protocol cycles followed by a detection event depends on induced error rate

$$L = \sum_{l=0}^{\infty} l(1-P_E)^l P_E = \frac{1-P_E}{P_E} \tag{12}$$

where $(1-P_E)^l P_E$ represents probability of occurrence of exactly l successful protocol cycles followed by a failure. Eve conclusively eavesdrops only $(1-Q)$ fraction of these cycles. Her average information gain per protocol run equals to

$$I_E = (1-Q)L = \frac{2P_E}{1-P_E}\frac{1-P_E}{P_E} = 2 \tag{13}$$

so she learns two classic bits independent on induced error rate. This is a result of two mutually balancing effects: (a) small error rate permits for long sequences before detection but the unambiguous discrimination is then inefficient, (b) high induced error rate permits effective discrimination at the price of quicker detection.

Analysis of the presented version of entangle and measure attack may be concluded with some optimistic observation. The Brandt probe design is founded on the assumption that during reconcillation phase of BB84, Eve will learn the basis that was used for encoding of classic bits. In the considered protocol, this is no longer true. Eve

assumes apriori the encoding method: 0 is encoded as $|v\rangle$ or $|u\rangle$ and 1 is encoded as $|\bar{v}\rangle$ or $|\bar{u}\rangle$. The eavesdropping works because probe permits discrimination of horizontal ($|v\rangle$, $|u\rangle$) and vertical ($|\bar{v}\rangle$, $|\bar{u}\rangle$) states and 0 (1) is encoded always as horizontal (vertical) state. The technique used above simply would not work for Alice and Bob using the following encoding rules: $0 \rightarrow (|u\rangle \text{ or } |\bar{v}\rangle)$, $1 \rightarrow (|\bar{u}\rangle \text{ or } |v\rangle)$. Then probe would differentiate between horizontal and vertical states but it would be not known which basis the identified state came from and Eve would be unable to make the decision whether Alice encoded "0" or "1" (see Table 2). The problem of constructing the entangling probe for this version of encoding remains an open question.

3 Results

It has been shown in the preceding section that analysis provided by the seminal presentation of the protocol is not complete as it does not take into account requirements specific for the authentication process. The static value of the compared secret and its sequential processing bit by bit are the main properties that seriously diminish offered security margin. These deficiencies can be removed by supplementing the quantum communication with the classical data processing. Please note that such an approach is a common practice—both killer applications of quantum data processing, i.e. the Shor's factorization and QKD simply would not work without support of dedicated classic algorithms. The main idea of this contribution is related to the exploitation of the hash function properties to introduce a pseudorandom nature of the compared bit string. In consequence, the eavesdropper is faced with the all-or-nothing task, that he can successfully complete with probability close to zero.

Let Alice and Bob share a sequence k consisting of an even number of bits. Let they also agree on some hash function $H(\cdot)$ and two mutually unbiased bases—for instance computational basis $\mathscr{B}_0 = \{|0\rangle, |1\rangle\}$ and its dual basis $\mathscr{B}_1 = \{|+\rangle, |-\rangle\}$ where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. They can communicate via the quantum and classic channels that are not protected by any means. Alice task is to convince Bob that she knows the sequence k without revealing none of its bits to the potential eavesdropper possibly hanging on a classic and/or quantum channel. The steps of the improved procedure are similar to the message mode of the seminal protocol. The control mode is removed.

1. Alice generates random number r_A and she calculates the session secret s_A using the hash function

$$s_A = H(r_A, k) \tag{14}$$

2. Bob listens on a classic channel. Alice sends to him the random number r_A. He receives number r_B possibly equal to r_A. Bob calculates his own copy of a session secret

$$s_B = H(r_B, k) \tag{15}$$

then he starts to listen on a quantum channel.

Table 2 Encoding rules used by Alice and Bob in the improved protocol

Alice and Bob				Eve	
Even bit value ($s_A[2l]$)	Basis	Odd bit value ($s_A[2l+1]$)	Quantum state	Control	Probe
0	$\mathscr{B}_0$	0	$\|0\rangle$	$\|u\rangle$	$\|\chi_0\rangle$
0	$\mathscr{B}_0$	1	$\|1\rangle$	$\|\bar{u}\rangle$	$\|\chi_1\rangle$
1	$\mathscr{B}_1$	0	$\|-\rangle$	$\|\bar{v}\rangle$	$\|\chi_1\rangle$
1	$\mathscr{B}_1$	1	$\|+\rangle$	$\|v\rangle$	$\|\chi_0\rangle$

3. Alice encodes sequence of qubits using rules summarized in Table 2. The even bits of s_A select the basis and odd bits encode qubit state. Alice encodes qubits sequentially and she sends them one by one with a constant speed known to Bob.
4. Bob expects qubits in a specified time slots—that way he may decide how many qubits were lost. The even bits of the session secret ($s_B[2l]$) determine detection basis and the measurement outcome is decoded to classical bits using Table 2. The received bits form the sequence $s'_B[2l+1]$. Bob continues detection process until entire sequence of qubits is received without communicating anything to Alice.
5. Bob estimates the number of lost qubits and bit error rate by comparing received sequence $s'_B[2l+1]$ with respective values of $s_B[2l+1]$. He decides then whether the requirements imposed by the security policy are met and signals that to Alice with the classic channel. Bob rejects authentication request if the number of lost qubits and/or observed BER are too large.

These simple modifications cause that each authentication event looks differently, in the sense, that Eve cannot exploit the knowledge gained in a given protocol run in eavesdropping of the next ones. Bob signals only authentication success or failure, but not the reception status of single qubits. The net result is Eve faced with all-or-nothing problem.

Let us analyse MITM attack against modified version of the protocol. Eve measures incoming qubits. The obtained outcomes determine the states that she sends further to Bob. This is equivalent to local construction of the bit string s_E. The features of the hash function $H(\cdot)$ guarantee that Eve‘ is unable to deduce the correct measurement basis from the knowledge of r_A alone. Eve has to select basis randomly and, contrary to the seminal protocol, she has no feedback from Bob whether the selection is correct. In consequence, strings s_E and s_A are uncorrelated. The introduced BER is equal to 25% but Eve gains no knowledge which protocol cycles were successful. Her attack succeeds only if, by an accident, the introduced errors in a given protocol instance are sufficiently low to be accepted by Bob. The probability of such event may be made arbitrarily small by the elongation of the compared string s_A. Even in this extremely improbable situation, she is still unable to recover the shared secret as the extremely improbable inversion of the hash

$$s_E = H\left(r_A, k'\right) \tag{16}$$

leads to wrong value of $k' \neq k$ when at least one bit of s_E differs from the corresponding bit of s_A. In fact, Eve can check whether the recovered shared secret is the correct one only by impersonation of Alice and undertaking the next authentication attempt. The difference of a single bit between k' and k leads to large differences between $H\left(r_A, k'\right)$ and $H\left(r_A, k\right)$ and, in consequence, makes fake authentication impossible.

The analysis of the entangle and measure attack presented in [33] is still valid for the modified version. But the information gain estimated therein results from the implicitly assumed minimum error discrimination. The values of the secret are recovered with the limited confidence and Eve has to eavesdrop multiple instances of the same looking authentication to make her guess less or more probable. In contrary, the Brandt probe gives the confident knowledge of the value of two bits of the shared secret. The proposed version of the protocol uses encoding immune to the commonly known version of this attack. However, it remains secure even if taking the pessimistic assumption that analogue of the Brandt probe do exists for other encoding rules. Again, recovery of the whole secret requires availability of the multiple instances of the same looking authentication.

The proposed protocol introduces random coefficient that makes each verification of the same secret to look differently for the eavesdropper, and the knowledge on the guessed bits cannot be accumulated. Moreover, the bits of the shared secret are behind the shield of the hash function as they are not used directly. The recovery of the shared secret k requires inversion of (14). However, the successful application of the Brandt probe gives the knowledge on two bits of s_A only. Thus most bits of the left-hand side of (14) are unknown. This results in a plethora of possible values of k that satisfy the equation. The correctness of guessed k can be verified only by the interrogation of Bob–Eve has to impersonate Alice and initiate multiple authentication attempts with the same value of r_A. The length of k can be easily extended to the value that makes this task impossible due to time constraints of the protocol execution. Bob can also keep a cache of recently used r_A's and he can refuse to authenticate clients that use the same value of this parameter multiple times.

4 Conclusion

The identity authentication protocol based on classic shared secret which exploits indistinguishability of non-orthogonal quantum states proposed by Hong et al. [33] is experimentally feasible. However, some of its features make it vulnerable to known quantum attacks. The improved version with better security profile is proposed. The introduced modifications are threefold: (a) the change in classic to quantum encoding makes it immune to Brandt probe, (b) the introduction of a random factor makes an attack on each authentication event a separate cryptographic task, (c) the introduced hash function works as a shield that protects a shared secret which is never directly used. The improved version does not require an authenticated classic channel—Bob simply confirms or denies the entire authentication transaction and Eve is faced with all-or-nothing problem. Any manipulation with the classic or quantum messages result in denial of service and it gives no useful information to Eve.

Acknowledgements Author acknowledges support by the Ministry of Science and Higher Education funding for statutory activities.

References

1. Wiesner, S.: Conjugate coding. SIGACT News **15**(1), 78–88 (1983)
2. Ingarden, R.S.: Quantum information theory. Rep. Math. Phys. **10**(1), 43–72 (1976)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of International Conference on Computers, Systems and Signal Processing, New York, pp. 175–179 (1984)
4. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002)
5. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301–1350 (2009)
6. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991)
7. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Phys. Rev. A **79**, 032341 (2009)
8. Sasaki, T., Yamamoto, Y., Koashi, M.: Practical quantum key distribution protocol without monitoring signal disturbance. Nature **509**, 475 (2014)
9. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: Secure communication with a publicly known key. Act. Phys. Pol. **101**(3), 357–368 (2002)
10. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
11. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
12. Shukla, C., Thapliyal, K., Pathak, A.: Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf. Process. **16**(12), 295 (2017)
13. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
14. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**(4), 247–251 (2003)
15. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. **42**(5), 055305 (2009)
16. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Phys. Rev. A **64**, 062309 (2001)
17. Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., Zeilinger, A.: Entanglement-based quantum communication over 144 km. Nat. Phys. **3**, 481 (2007)
18. Ostermeyer, M., Walenta, N.: On the implementation of a deterministic secure coding protocol using polarization entangled photons. Opt. Commun. **281**(17), 4540–4544 (2008)
19. Wang, S., Yin, Z.Q., Chen, W., He, D.Y., Song, X.T., Li, H.W., Zhang, L.J., Zhou, Z., Guo, G.C., Han, Z.F.: Experimental demonstration of a quantum key distribution without signal disturbance monitoring. Nat. Photonics **9**, 832–836 (2015)
20. Schmid, C., Trojek, P., Bourennane, M., Kurtsiefer, C., Żukowski, M., Weinfurter, H.: Experimental single qubit quantum secret sharing. Phys. Rev. Lett. **95**, 230505 (2005)
21. Zhu, F., Zhang, W., Sheng, Y., Huang, Y.: Experimental long-distance quantum secure direct communication. Sci. Bull. **62**(22), 1519–1524 (2017)
22. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., Zbinden, H.: Quantum key distribution over 67 km with a plug and play system. New J. Phys. **4**, 41–41 (2002)
23. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

24. Zeng, G., Zhang, W.: Identity verification in quantum key distribution. Phys. Rev. A **61**, 022303 (2000)
25. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication in quantum key distribution. Phys. Rev. A **62**, 022305 (2000)
26. Shi, B.S., Li, J., Liu, J.M., Fan, X.F., Guo, G.C.: Quantum key distribution and quantum authentication based on entangled state. Phys. Lett. A **281**(2–3), 83–87 (2001)
27. Wei, T.S., Tsai, C.W., Hwang, T.: Comment on quantum keydistribution and quantum authentication based on entangle state. Int. J. Theor. Phys. **50**, 2703–2707 (2011)
28. Zhou, N., Zeng, G., Zeng, W., Zhu, F.: Cross-center quantum identification scheme based on teleportation and entanglement swapping. Opt. Commun. **254**(4–6), 380–388 (2005)
29. Dušek, M., Haderka, O.C.V., Hendrych, M., Myška, R.: Quantum identification system. Phys. Rev. A **60**, 149–156 (1999)
30. Zhang, Z., Zeng, G., Zhou, N., Xiong, J.: Quantum identity authentication based on ping-pong technique for photons. Phys. Lett. A **356**(3), 199–205 (2006)
31. Lee, H., Lim, J., Yang, H.: Quantum direct communication with authentication. Phys. Rev. A **73**(4), 042305 (2006)
32. Yen, C.A., Horng, S.J., Goan, H.S., Kao, T.W., Chou, Y.H.: Quantum direct communication with mutual authentication. Quantum Inf. Comput. **9**(5), 376–394 (2009)
33. Hong, C.H., Heo, J., Jang, J.G., Kwon, D.: Quantum identity authentication with single photon. Quantum Inf. Process. **16**(10), 236 (2017)
34. Brandt, H.E.: Quantum-cryptographic entangling probe. Phys. Rev. A **71**, 042312 (2005)
35. Brandt, H.E.: Unambiguous state discrimination in quantum key distribution. Quantum Inf. Process. **4**(5), 387–398 (2005)
36. Jaeger, G., Shimony, A.: Optimal distinction between two non-orthogonal quantum states. Phys. Lett. A **197**(2), 83–87 (1995)
37. Rudolph, T., Spekkens, R.W., Turner, P.S.: Unambiguous discrimination of mixed states. Phys. Rev. A **68**, 010301 (2003)