BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 69(4), 2021, Article number: e137729
DOI: 10.24425/bpasts.2021.137729

Semiquantum authentication of users resistant to multisession attacks

Piotr ZAWADZKI *

Department of Telecommunications and Teleinformatics, Silesian University of Technology, ul. Akademicka 2A, 44-100 Gliwice, Poland

Abstract. User authentication is an essential element of any communication system. The paper investigates the vulnerability of the recently published first semiquantum identity authentication protocol (Quantum Information Processing 18: 197, 2019) to the introduced herein multisession attacks. The impersonation of the legitimate parties by a proper combination of phishing techniques is demonstrated. The improved version that closes the identified loophole is also introduced.

Key words: quantum cryptography; quantum identity authentication; semi-quantum communication.

1. INTRODUCTION

Quantum Cryptography (QC) is a well-developed field of research. Contrary to its classical counterpart, it provides cryptographic primitives whose security results from the laws of physics, i.e., it is independent of the computational resources of the adversary. It aims not only at the delivery of functional equivalents of the already known primitives but also at the provision of quite new primitives with properties impossible to realize within the classical information processing paradigm.

The idea of information protection based on the laws of quantum mechanics can be dated to the 70s of the previous century when Steven Wiesner proposed a quantum cryptocurrency system with security founded on information encoding in nonorthogonal quantum states. Unfortunately, the manuscript was rejected by many journals [1] and was published later in 1983 [2], after Benioff's [3] paper that provided a quantum mechanical model of Turing machine. A little later, using Wiesner's idea, Bennett et al. proposed the famous BB84 protocol [4, 5] that provides distant, truly random number generators working synchronously – a cryptographic primitive unachievable by classical information processing. Although this milestone result, QC has been considered an interesting niche of research with no serious impact on the existing communication infrastructure. The real impetus to research in this field has been given a decade later by Shor's paper [6] demonstrating that asymmetric algorithms – the foundation of Internet security – can be efficiently broken using a hypothetical quantum computer.

The interests of present-day QC encompass very diverse domains including Quantum Key Distribution (QKD), Quantum Direct Communication (QDC), Quantum Secret Sharing (QSS), Quantum Digital Signature (QDS), Quantum Oblivious Transfer (QOT), Quantum Secure Multiparty Computations (QSMC) to name a few [7]. The research on quantum-assisted confidentiality provides the most mature solutions. Private communication can be achieved by the joint use of QKD protocols [8] with classical encryption, namely, One-Time Pad (OTP). Alternatively, QDC [9,10] provides a private communication without referring to classical ciphers at all. Presently, QKD solutions are commercially available [11] and QDC test installations are deployed in the field [12]. However, most of the above-mentioned protocols assume directly or implicitly, that legitimate parties already have an authenticated classical channel at their disposal. That assumption makes authentication of users an essential element of both classical and quantum Information and Communication Technology (ICT) systems.

The goal of Quantum Identity Authentication (QIA) protocol is to accomplish this task using a quantum information processing paradigm. The use of entangled quantum states as a shared secret is intensively investigated in the quest for cryptographic primitives with properties unachievable in classical systems [13]. However, the difficulties related to entanglement management make such protocols difficult to deploy. The need to design protocols that can be implemented using available technology has led to the idea of QIA protocols that verify user identities on the basis of classical cryptographic keys [14–16]. The cost of massive deployment of quantum cryptography can be further significantly reduced by the introduction of semiquantum protocols, in which the selected parties only have full technical capabilities for the manipulation of quantum states. The remaining users, referred to as classical, need support for limited interactions with quantum information carriers: (a) prepare and measure their states in a single base, (b) send them back without interaction and optionally (c) change their order using delay lines [17,18]. The semiquantum QKD [19–21] provides benefits equivalent to a fully quantum formulation [22]. The usefulness of semiquantum information processing for other cryptographic domains is presently intensively investigated [23–32]. A survey of the results achieved in this research area can be found in [33].

Recently, Zhou et al. [34] have proposed the first semiquantum QIA protocol. It will be further referred to as Zhou's Semi-

*e-mail: pzawadzki@polsl.pl

Manuscript submitted 2021-01-11, revised 2021-06-11, initially accepted for publication 2021-06-14, published in August 2021

quantum QIA (ZSQIA). The protocol is advantageous compared to many other proposals as it is an entanglement-free solution that supports authentication on the basis of a shared classical secret. It is also resistant to standard quantum attacks [34]. However, ZSQIA is stateful, as the shared secret is updated after every successful authentication. It follows that authentication transactions are not independent in a general case. Unfortunately, its security has not been analyzed in this context. This contribution: a) demonstrates scenarios that enable a quantum adversary to phish useful information, b) two attacks that combine the mentioned above phishing techniques to impersonate legitimate parties – quantum or classical, c) the improved version of the protocol that closes the identified loopholes.

2. ANALYSIS OF ZSQIA

The analyzed protocol is semiquantum and provides authentication of quantum (Alice) and classical (Bob) users, therefore Alice and Bob can act as both the supplicant and the authenticator. Alice can perform any operation on quantum information carriers. In particular, she can prepare qubits and make measurements in computational ($\mathscr{B}_c = \{|0\rangle, |1\rangle\}$) and dual ($\mathscr{B}_d = \{|+\rangle = H|0\rangle, |-\rangle = H|1\rangle\}$) bases ($H$ denotes Hadamard gate). Bob's capabilities are limited to: (a) preparation and measurement of qubits in a single base, (b) returning the received qubits without modification and (c) changing the ordering of qubits. It is assumed that the parties share a classical secret key composed of $4n$ bits prior to the protocol execution. The logical grouping of key material into two-bit tuples $K = (b, v)$ is introduced in the provided analysis. Only even-numbered tuples K_{2l} (i.e. $2n$ bits) are directly used in a process of supplicant authentication. The protocol is stateful and both parties update the secret after every successful authentication. The remaining odd-numbered tuples K_{2l-1} parametrize that action. The state machine for each peer is shown in Fig. 1. The actions embraced by the "*verify*" block depend on the role of the peer and its quantum processing capabilities. They are described in detail in the following paragraphs. On the other hand, the "*key update*" block is the same for all cases and it depends on the data used in the authentication process. Parties independently update the secret key after every successful authentication. This is a two-step process. First they create the key S composed of n tuples:

$$S_l = \begin{cases} \{0, v_l\} & K_{2l}.b = 0 \\ \{1, K_{2l}.v\} & K_{2l}.b = 1 \end{cases}, \tag{1}$$

where v_l are the bits agreed on at the verification stage. Next, the tuples of a new key K'' are calculated as follows:

$$K''_{2l-1} = K_{2l}\,, \tag{2a}$$

$$K''_{2l} = K_{2l} \oplus K_{2l-1} \oplus S_l\,. \tag{2b}$$

One should note that details of the key update are irrelevant for further protocol (in)security analysis. The immutability of the verified secret in case of failed authentication and the possibility to phish some useful information are the decisive observations to the construction of a successful attack. In the following two sections, the identity verifications of classical and quantum

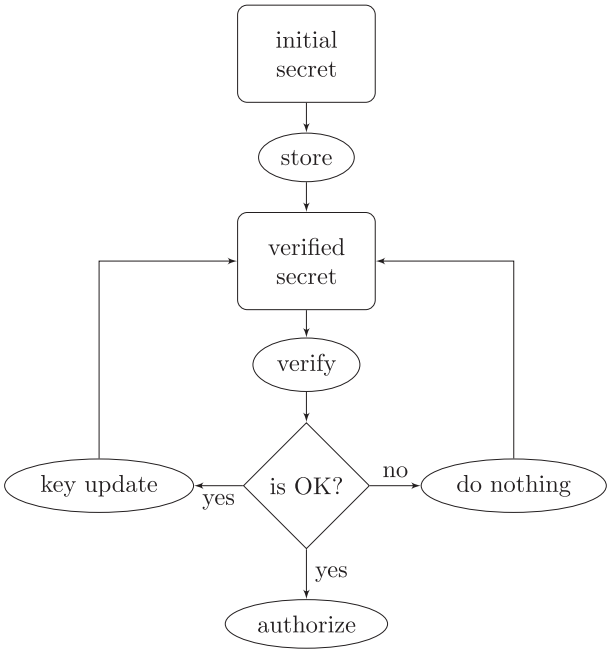

Fig. 1. State machine of the peer in ZSQIA

parties are summarized [34]. The properties of these procedures are exploited in Section 2.3 to demonstrate attacks that permit impersonation of legitimate parties.

2.1. Authentication of a quantum user

Procedure of Alice authentication is composed of the following steps:

Q.1 *Creation of authenticating sequence*. Alice uses only even tuples K_{2l} of the key. She prepares a sequence B of n classical bits: pn $(0 < p < 1)$ of them have random values and they are randomly dispersed over the sequence, the remaining $(1-p)n$ ones are copied from the corresponding key tuples: $B_l = K_{2l}.v$. Alice uses bit strings $\{B_l\}_{l=1}^n$ and $\{K_{2l}.b\}_{l=1}^n$ to prepare the authenticating sequence:

$$|\phi\rangle = \bigotimes_{l=1}^{n} |\phi_l\rangle = \bigotimes_{l=1}^{n} H^{K_{2l}.b} |B_l\rangle \ . \tag{3}$$

The values of $\{B_l\}$ for which $K_{2l}.b = 0$ form the $\{v_l\}$ sequence in key update procedure (1).

Q.2 *Authentication request*. Alice sends to Bob the authentication request followed by qubits $|\phi_l\rangle$ from sequence (3). States $|\phi_l\rangle$ that carry on random bits from sequence B are further referred as decoys.

Q.3 *Response*. Bob processes $|\phi_l\rangle$ differently depending on the value of $K_{2l}.b$ of his local key. If he expects that the received qubit is encoded in a dual base, $(K_{2l}.b \neq 0)$ then he returns it back to Alice. Otherwise, he measures the qubit in the computational base and sends no response. These outcomes are further used as the $\{v_l\}$ sequence in key update procedure (1).

Q.4 *Measurement*. Alice measures the returned qubits in a dual base.

Q.5 *Announcement*. Alice announces the positions of decoy qubits and the values of random bits encoded on them.

Q.6 *Eavesdropping detection*. a) Bob compares the outcomes of his measurements with the values of bits announced by Alice. The discrepancy is a sign of the eavesdropper's presence. b) Alice also compares values of the returned bits with the ones used in sequence (3) preparation. Again, the discrepancy means that Eve is on the line.

Q.7 *Verification*. Bob's outcomes for qubits that are not decoys form an authentication string A. Alice's identity is accepted only if the bits of the string A are equal to the corresponding bits $K_{2l}.v$ of his local copy of the key.

2.2. Authentication of a classical user

The authentication procedure of the classical user is significantly different.

C.1 *Authentication request*. Bob sends classically authentication request.

C.2 *Authenticating sequence*. In response to Bob's request, Alice prepares an authenticating sequence in the same way as in point Q.1. Then she sends qubits from sequence (3) to Bob.

C.3 *Insertion*. a) When Bob receives the sequence (3), he does not measure the incoming qubits, but inserts after each one the state $|K_{2l}.b\rangle$ prepared in the computational base. The resulting sequence has the form:

$$|\psi\rangle = \bigotimes_{l=1}^{n} \left(H^{K_{2l}.b} |B_l\rangle \otimes |K_{2l}.b\rangle \right). \tag{4}$$

This time the bits of $\{K_{2l}.b\}$ are used as a sequence $\{v_l\}$ in key update procedure.

C.4 *Permutation*. Bob creates a new sequence $|\psi'\rangle$ by random rearrangement of the qubits in $|\psi\rangle$. It is noteworthy that the operation of random rearrangement requires some form of short-term quantum memory. Bob sends $|\psi'\rangle$ back to Alice. Alice stores the received sequence in quantum memory.

C.5 *Announcement*. Bob announces the permutation he has used to prepare a new sequence $|\psi'\rangle$.

C.6 *Measurement*. Alice applies the reverse permutation to qubits received from Bob. Alice measures each pair of corresponding qubits $|\phi_l'\rangle|K_{2l}.b'\rangle$ – a qubit prepared by herself, who traveled back and forth, and the associated qubit prepared by Bob. She measures her qubits in the base determined by the secret key and Bob's qubits in the computational base. Consequently, Alice recovers two strings of bits – B_l' and $K_{2l}.b'$.

C.7 *Verification*. Eavesdropping attempts inevitably lead to transmission errors and thus to different B_l and B_l' sequences. Bob is authenticated based on the compliance of the received $K_{2l}.b'$ values with the values of $K_{2l}.b$ retrieved from the local copy of the key.

2.3. Impersonation of legitimate parties

The QIA protocols, unlike the QKD and QSDC ones, cannot assume the authentication of the classical channel used to exchange control data. As a consequence, Eve is free to modify all messages at will, and Alice or Bob are solely on their own in deciding whether the entity they are communicating with can successfully pass the authentication process. Unfortunately, the parties that authenticate themselves according to the rules summarized in Sections 2.1 and 2.2 can be impersonated.

Let us note that the knowledge of the entire secret key is not required to successfully pass the authentication procedure: Bob proves only the knowledge of $K_{2l}.b$ and Alice additionally must be able to create the valid sequence B. All these elements can be phished by Eve.

P.1 *Phishing of $K_{2l}.b$*. The sequence $K_{2l}.b$ can be phished from Bob. Eve pretends Alice in the procedure of classical user authentication. She just waits for Bob's authentication request from point C.1. In response, she sends to Bob a sequence of arbitrary qubits instead of sequence (3). Legitimate Bob acts as usual and according to point C.3 he appends $|K_{2l}.b\rangle$ to every received qubit. The resulting sequence is reordered and sent back. Eve keeps the received sequence in memory and waits for the permutation announcement in point C.5. Now Eve knows the positions of qubits appended by Bob. She measures them in the computational base to recover $K_{2l}.b$. Eve breaks communication when all bits of $K_{2l}.b$ are gathered. That way, the same shared secret will be used by Bob in the next authentication attempt.

P.2 *Phishing of B*. Phishing of B requires knowledge of $K_{2l}.b$, therefore Eve must complete point P.1 beforehand. Eve pretends Bob and plays the role of the authenticator in the procedure of quantum user authentication. She waits for an authentication request from Alice. It is followed by a sequence (3) from point Q.1. However, unlike classical Bob in point Q.4, she measures all incoming qubits in the base that corresponds to $K_{2l}.b$ value. The outcomes form a valid sequence B. Eve does not know yet which of them are decoys, so she continues the protocol. She recreates qubits from the dual base ($K_{2l}.b = 1$) and sends them back to the unsuspecting Alice. In point Q.5, Alice reveals the positions of decoy qubits. Now Eve can break the communication.

By a proper combination of the above phishing techniques, Eve can impersonate (i.e., authenticate on behalf of) Alice or Bob.

I.1 *Bob impersonation*. Eve pretends to be Alice and learns $K_{2l}.b$ from Bob with the method described in point P.1. With this information, she turns to Alice and authenticates on behalf of Bob.

I.2 *Alice impersonation*. Eve pretends to be Alice and learns $K_{2l}.b$ as described in point P.1. Then she pretends to be Bob and phish a valid sequence B as in point P.2. Then she turns out to Bob again and authenticates on behalf of Alice.

It should be noted that in both cases Eve does not recover the secret key, so she is unable to follow the key update procedures. Therefore, Eve has to repeat phishing every time she wants to impersonate victims.

3. RESULTS

The possibility of reusing information obtained during unsuccessful authentication attempts is the direct cause of the vulnerability described in Section 2.3. Unfortunately, updating the

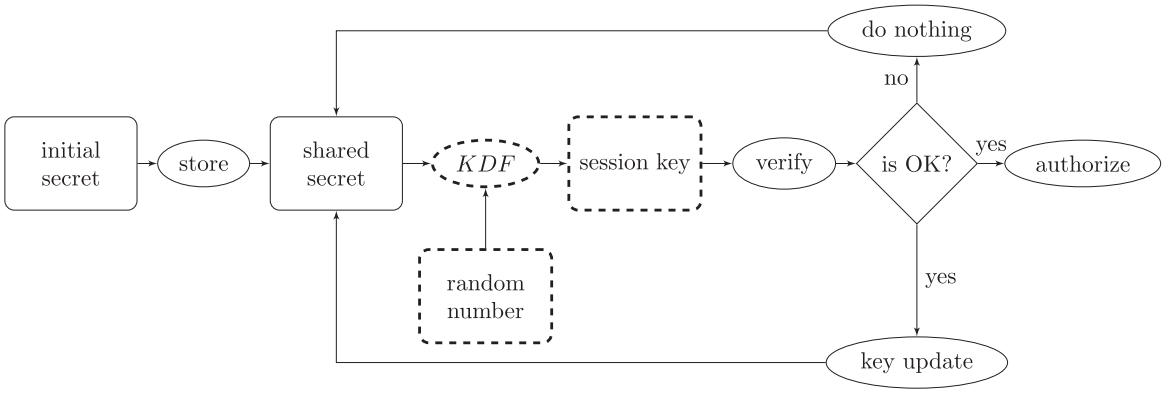

Fig. 2. Improved State machine

key after unsuccessful authentication attempts is not an option because it would lead to a loss of synchronism between the legitimate parties. The introduction of the verified secret randomization in a way that it is unique for each authentication attempt is an alternative solution. Of course, the random data enabling such transformation must come from both parties participating in the protocol. Moreover, the value of the verified key should also be dependent on all bits of the shared secret to exclude authentication with partial information. The instantation of the above ideas is shown in Fig. 2. The new elements of the state machine are marked with a dashed line. The random data provided by both parties are mixed with the shared secret using some cryptographic Key Derivation Function (KDF). The verified secret is in practice unique for each session as random inputs are negotiated before each authentication attempt. Successive authentication attempts are also well-separated due to the one-way nature of the KDF function. The detailed actions of parties in the improved version of the protocol are summarized below.

3.1. Improved authentication of a quantum user

The procedure presented below generally follows the corresponding fragment of ZSQIA described in Section 2.1. The new elements are the randomization introduced in step QS.0 and the modified Bob and Alice behaviour in steps QS.2 and QS.3, respectively.

QS.0 *Session randomization*. a) Alice and Bob locally generate random numbers r_A and r_B, respectively, of $2n$ bits each. Then they exchange them with the classical channel. b) Each party locally generates a session key based on the secret key and random numbers. This step aims to randomize the compared bit strings. A cryptographic KDF function with a recognized reputation can be used for this purpose, e.g., PBKDF2 [35] or Argon2 [36]:

$$\mathscr{K} = KDF\left(K, r_A || r_B\right), \tag{5}$$

where $||$ denotes concatenation of the binary representations. The above transformation guarantees the uniqueness of the session because both communicating parties are responsible for the preparation of random material. The derived quantity $\{\mathscr{K}_l\}_{l=1}^{n}$ plays a role analogous to that of $\{K_{2l}\}_{l=1}^{n}$ in ZSQIA. It is noteworthy that the session key $\mathscr{K}$ now depends on all bits of the shared secret K.

QS.1 *Authenticating sequence*. Alice and Bob behave the same as in points Q.1 and Q.2.

QS.2 *Response*. In this and the next point, some small modifications to the classical participant's behavior have been introduced. They aim to hide the information about the $\mathscr{K}_l.b$ bits. The modified actions of Bob are emphasized. If $\mathscr{K}_l.b = 1$, then Bob sends the received qubit back to Alice, otherwise he measures it *and sends back a qubit prepared in the computational base that corresponds to the measurement outcome*.

QS.3 *Measurement*. Alice measures the received qubits in the dual base ($\mathscr{K}_l.b = 1$) *and ignores the ones prepared in the computational base* ($\mathscr{K}_l.b = 0$).

QS.4 *Announcement, Eavesdropping check, Verification*. The remaining actions of Alice and Bob are the same as in steps Q.5÷Q.7 of the base protocol.

3.2. Improved authentication of a classical user

The procedure presented below generally follows the corresponding fragment of ZSQIA described in Section 2.1. The new elements are the randomization introduced in step CS.1 and the modified encoding of the returned quantum states in step CS.3.

CS.0 *Authentication request*. Bob sends classically an authentication request.

CS.1 *Session randomization*. Alice and Bob behave the same as in step QS.0.

CS.2 *Authenticating sequence*. Alice and Bob behave the same as in step C.2.

CS.3 *Insertion*. a) Bob prepares a sequence $|C_l\rangle$ of states encoded in the computational base according to rule:

$$C_l = \begin{cases} \mathscr{K}_l.v & \text{for } \mathscr{K}_l.b = 0\,, \\ \text{random} & \text{otherwise}\,. \end{cases} \tag{6}$$

The values randomly inserted into the above sequence will hereinafter be referred to as mask bits. Similarly to point C.3, Bob creates a sequence

$$|\psi\rangle = \bigotimes_{l=1}^{n} \left(H^{K_{2l}.b} |B_l\rangle \otimes |C_l\rangle \right). \tag{7}$$

CS.4 *Permutation*. *Announcement*. *Measurement*. Parties behave exactly as in points C.4÷C.6. The only difference is that this time Alice's measurements recover the values of B'_l and C'_l.

CS.5 *Verification*. Eavesdropping attempts inevitably lead to transmission errors and hence to differences in the sequences of B_l and B'_l. Bob is authenticated based on the match of the obtained $\mathscr{K}_l.v'$ values with the corresponding values taken from the local copy of the session key.

3.3. Security analysis

The rules of encoding classical information in quantum states remain unchanged in the modified protocol. Therefore, the security analysis presented in [34] also applies as long as a single session is considered. Thus, it can be considered that the modified protocol is robust too.

Eve must risk detection of the attack with nonzero probability to learn with limited certainty the value of the verified key bit. Therefore, the probability of recovering the entire key tends to zero, and an attack providing this information will be detected with a probability that tends to certainty with the length of the key. The difference compared to the previous version is that this time the session key $\mathscr{K}$ is verified instead of the shared secret K. Further paragraphs concentrate on the resistance assessment of the improved protocol to the introduced herein multisession attacks.

The purpose of the proposed patches is twofold: they reduce the amount of sensitive data that Eve can phish and limit the lifetime of information gained by the eavesdropper to a single session. The behavior of the classical participant has been modified as the first line of defense. First, Eve cannot infer the value of $\mathscr{K}_l.b$ from Bob's behavior in point QS.2 (compare with Q.3). The adopted measure-and-resent strategy also provides resistance to Double-CNOT attack [37]. Eve's register is never modified by the double application of the *CNOT* gate to the qubit travelling forth and back between Alice and Bob when $\mathscr{K}_l.b = 1$, because in this case Bob does not touch the qubit. However, this can be no longer true when parties operate on qubits prepared in the computational base as shown in Fig. 3. In general, Bob's outcome may be m and he can send back a qubit prepared in state $|p\rangle$. The value of Eve's register is not affected only if $m = p$, i.e. Bob has to prepare state that agrees with the received outcome. Otherwise, Eve can detect the act of measurement, and that way infer the value of $\mathscr{K}_l.b$.

Moreover in point CS.3 half of the key's bits, namely $\mathscr{K}_l.b$, are never sent – they are only used indirectly to control the base

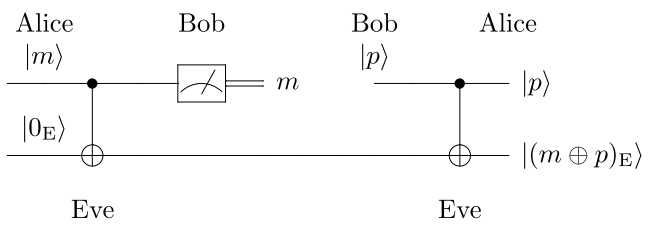

Fig. 3. Double CNOT attack when $\mathscr{K}_l.b = 0$. The time arrow is from left to right

in which the states of the authenticating sequence are prepared. This way, the phishing scenario described in P.1 is excluded. The attack P.2 is also eliminated because of the dependence on P.1. Phishing the used $\mathscr{K}_l.v$ bits is also problematic. They are intermixed with random ones therefore the attacker cannot extract them without knowing $\mathscr{K}_l.b$. However, no benefits come for free. The lower number of significant bits used for authentication increases the probability that Eve playing the role of Bob in CS.3 will simply guess those bits. The shared key of adequate length should be used to keep that probability sufficiently low.

Let us assume that Eve using some techniques has eavesdropped all the session key bits that are in transit. The problem to be solved by Eve resembles a well-known preimage attack, but unlike the typical situation, she only knows part of the output $\mathscr{K}$

$$\mathscr{K} = KDF\left(K, r_A||r_B\right). \tag{8}$$

Thus, there are many authentication keys K that are possible solutions to the problem. Eve has no idea which one is correct, and the only way to test the hypothesis is to try to authenticate herself on behalf of the victim. She is limited to one try only because each authentication session is parameterized with a unique set of random numbers r_A and r_B. Clearly, she also knows the random numbers r_A and r_B and, in the phishing scenario, she is also capable to set the value of one of these numbers. Therefore, one should assume that only legitimate party contributes to the entropy of $r_A||r_B$ parameter.

Let us estimate the chances of the multisession attack when the protocol uses parameters typical to modern cryptography. Suppose Eve has recovered the entire 256-bit session key $\mathscr{K}$. Her task is to find the correct value of the 512-bit shared key, i.e., preimage K. Only that way she can successfully set up an authentication session for a different set of random numbers. The classical preimage attack requires 2^{256} KDF calls. It is unclear to what extent this complexity can be reduced with quantum computers. National Institute of Standards and Technology (NIST) recommended doubling the hash size to counter the attacks based on the Grover algorithm [38], which has a complexity $(2^{256})^{1/2}$. However, recent reports indicate that a brutal force quantum attack on the hash function can be further reduced to $(2^{256})^{1/3}$ queries [39]. It should be noted that despite the tremendous progress in this field, the complexity of KDF inversion still remains exponential for classical and quantum computers.

Even if Eve finds a preimage that reduces to a session key, she still does not know whether it is a valid shared secret. The properties of the KDF function ensure that the 2^{256} preimages reduce to the same session key. However, Eve needs a correct shared secret to continue with a different set of random numbers. Thus, her chances of guessing it are as low as 2^{-256}. That probability can be further reduced by selecting a longer shared secret and/or cryptographic primitives that support longer hashes. Moreover, Eve's uncertainty is increased by incomplete knowledge of the KDF output, i.e., the session key $\mathscr{K}$. According to the rules of the protocol, she knows at most half of its bits, so the space of potential solutions is increased by an additional 2^{128} possibilities. It follows that the

difficulty of impersonating in multisession attacks depends not only on the complexity of the inversion of the KDF function, but also on the way the data are organized in the protocol. The exhaustive attack also should be excluded. The verification of the hypothesis regarding the value of the key requires the participation of one of the legitimate parties. Limiting the number of authentication attempts per unit of time makes the size of the searchable space negligible.

4. CONCLUSION

The proposed mechanism of indirect use of the authentication key and the introduction of random factors make each authentication attempt unique. As a consequence, multisession attacks are not applicable because breaking each authentication session is a separate problem. The protocol combines primitives known from classical cryptography with robust transmission of quantum symbols. As a result, its security is founded not only on the hardness of the computational problem but also on the indistinguishability principle. However, the described solution is not ideal – legitimate parties must track changes of the shared key during the execution of the protocol. This introduces state synchronization problems and opens up new attack vectors. The work on stateless semiquantum authentication of users seems to be a challenge for the close future.

REFERENCES

[1] M.M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2013, doi: 10.1017/CBO9781139525343.

[2] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983, doi: 10.1145/1008908.1008920.

[3] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *J. Stat. Phys*., vol. 22, no. 5, pp. 563–591, 1980, doi: 10.1007/BF01011339.

[4] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[5] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci*., vol. 560, pp. 7–11, 2014, doi: 10.1016/j.tcs.2014.05.025.

[6] P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput*., vol. 26, no. 5, pp. 1484–1509, 1997, doi: 10.1137/S0097539795293172.

[7] A. Shenoy-Hejamadi, A. Pathak, and S. Radhakrishna, "Quantum cryptography: Key distribution and beyond," *Quanta*, vol. 6, no. 1, pp. 1–47, 2017, doi: 10.12743/quanta.v6i1.57.

[8] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys*., vol. 92, p. 025002, 2020, doi: 10.1103/RevModPhys.92.025002.

[9] D. Pan, K. Li, D. Ruan, S.X. Ng, and L. Hanzo, "Single-photon-memory two-step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs," *IEEE Access*, vol. 8, pp. 121 146–121 161, 2020, doi: 10.1109/ACCESS.2020.3006136.

[10] P. Zawadzki, "Advances in quantum secure direct communication," *IET Quant. Comm*., vol. 2, no. 2, pp. 54–62, 2021, doi: 10.1049/qtc2.12009.

[11] A. Pljonkin and P.K. Singh, "The review of the commercial quantum key distribution system," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, 2018, pp. 795–799, doi: 10.1109/PDGC.2018.8745822.

[12] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. Long, "Implementation and security analysis of practical quantum secure direct communication," vol. 8, p. 22, 2019, doi: 10.1038/s41377-019-0132-3.

[13] X. Li and D. Zhang, "Quantum authentication protocol using entangled states," in *Proceedings of the 5th WSEAS International Conference on Applied Computer Science*, Hangzhou, China, 2006, pp. 1004–1009. [Online]. Available: https://www.researchgate.net/publication/242080451_Quantum_authentication_protocol_using_entangled_states.

[14] G. Zeng and W. Zhang, "Identity verification in quantum key distribution," *Phys. Rev. A*, vol. 61, p. 022303, 2000, doi: 10.1103/PhysRevA.61.022303.

[15] Y. Kanamori, S.-M. Yoo, D.A. Gregory, and F.T. Sheldon, "On quantum authentication protocols," in *GLOBECOM '05. IEEE Global Telecommunications Conference, 2005*., vol. 3, 2005, pp. 1650–1654, doi: 10.1109/GLOCOM.2005.1577930.

[16] P. Zawadzki, "Quantum identity authentication without entanglement," *Quantum Inf. Process*., vol. 18, no. 1, p. 7, 2019, doi: 10.1007/s11128-018-2124-2.

[17] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical Bob," Phys. Rev. Lett., vol. 99, p. 140501, 2007, doi: 10.1103/PhysRevLett.99.140501.

[18] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, "Semiquantum key distribution," *Phys. Rev. A*, vol. 79, no. 3, p. 032341, 2009, doi: 10.1103/PhysRevA.79.032341.

[19] W.O. Krawec, "Security of a semi-quantum protocol where reflections contribute to the secret key," *Quantum Inf. Process*., vol. 15, no. 5, pp. 2067–2090, 2016, doi: 10.1007/s11128-016-1266-3.

[20] Z.-R. Liu and T. Hwang, "Mediated semi-quantum key distribution without invoking quantum measurement," *Ann. Phys*., vol. 530, no. 4, p. 1700206, 2018, doi: 10.1002/andp.201700206.

[21] C.-W. Tsai and C.-W. Yang, "Cryptanalysis and improvement of the semi-quantum key distribution robust against combined collective noise," *Int. J. Theor. Phys*., vol. 58, no. 7, pp. 2244–2250, 2019, doi: 10.1007/s10773-019-04116-5.

[22] W.O. Krawec, "Security proof of a semi-quantum key distribution protocol," in *2015 IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 686–690, doi: 10.1109/ISIT.2015.7282542.

[23] Y.-P. Luo and T. Hwang, "Authenticated semi-quantum direct communication protocols using Bell states," *Quantum Inf. Process*., vol. 15, no. 2, pp. 947–958, 2016, doi: 10.1007/s11128-015-1182-y.

[24] J. Gu, P.-h. Lin, and T. Hwang, "Double C-NOT attack and counterattack on 'Three-step semi-quantum secure direct communication protocol'," *Quantum Inf. Process*., vol. 17, no. 7, p. 182, 2018, doi: 10.1007/s11128-018-1953-3.

[25] M.-H. Zhang, H.-F. Li, Z.-Q. Xia, X.-Y. Feng, and J.-Y. Peng, "Semiquantum secure direct communication using EPR pairs," *Quantum Inf. Process*., vol. 16, no. 5, p. 117, 2017, doi: 10.1007/s11128-017-1573-3.

[26] L.-L. Yan, Y.-H. Sun, Y. Chang, S.-B. Zhang, G.-G. Wan, and Z.-W. Sheng, "Semi-quantum protocol for deterministic secure quantum communication using Bell states," *Quantum Inf. Process*., vol. 17, no. 11, p. 315, 2018, doi: 10.1007/s11128-018-2086-4.

[27] C. Xie, L. Li, and D. Qiu, "A novel semi-quantum secret sharing scheme of specific bits," Int. J. Theor. Phys., vol. 54, no. 10, pp. 3819–3824, 2015, doi: 10.1007/s10773-015-2622-2.

[28] A. Yin and F. Fu, "Eavesdropping on semi-quantum secret sharing scheme of specific bits," *Int. J. Theor. Phys*., vol. 55, no. 9, pp. 4027–4035, 2016, doi: 10.1007/s10773-016-3031-x.

[29] K.-F. Yu, J. Gu, T. Hwang, and P. Gope, "Multi-party semi-quantum key distribution-convertible multi-party semi- quantum secret sharing," *Quantum Inf. Process*., vol. 16, no. 8, p. 194, 2017, doi: 10.1007/s11128-017-1631-x.

[30] X. Gao, S. Zhang, and Y. Chang, "Cryptanalysis and improvement of the semi-quantum secret sharing protocol," *Int. J. Theor. Phys*., vol. 56, no. 8, pp. 2512–2520, 2017, doi: 10.1007/s10773-017-3404-9.

[31] Z. Li, Q. Li, C. Liu, Y. Peng, W. H. Chan, and L. Li, "Limited resource semiquantum secret sharing," *Quantum Inf. Process*., vol. 17, no. 10, p. 285, 2018, doi: 10.1007/s11128-018-2058-8.

[32] K. Sutradhar and H. Om, "Efficient quantum secret sharing without a trusted player," *Quantum Inf. Process*., vol. 19, no. 2, p. 73, 2020, doi: 10.1007/s11128-019-2571-4.

[33] H. Iqbal and W.O. Krawec, "Semi-quantum cryptography," *Quantum Inf. Process*., vol. 19, no. 3, p. 97, 2020, doi: 10.1007/s11128-020-2595-9.

[34] N.-R. Zhou, K.-N. Zhu, W. Bi, and L.-H. Gong, "Semi-quantum identification," *Quantum Inf. Process*., vol. 18, no. 6, p. 197, 2019, doi: 10.1007/s11128-019-2308-4.

[35] K. Moriarty, B. Kaliski, and A. Rusch, "Pkcs #5: Password-based cryptography specification version 2.1," Internet Requests for Comments, RFC Editor, RFC 8018, January 2017. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8018.html.

[36] A. Biryukov, D. Dinu, D. Khovratovich, and S. Josefsson, "The memory-hard Argon2 password hash and proof-of-work function," Working Draft, IETF Secretariat, Internet-Draft draft-irtf-cfrg-argon2-12, 2020. [Online]. Available: https://tools.ietf.org/id/draft-irtf-cfrg-argon2-03.html.

[37] P.-H. Lin, T. Hwang, and C.-W. Tsai, "Double CNOT attack on 'Quantum key distribution with limited classical Bob'," *Int. J. Quantum Inf*., vol. 17, no. 02, p. 1975001, 2019, doi: 10.1142/S0219749919750017.

[38] D. Moody, L. Chen, S. Jordan, Y.-K. Liu, D. Smith, R. Perlner, and R. Peralta, "Nist report on post-quantum cryptography," National Institute of Standards and Technology, U.S. Department of Commerce, Tech. Rep., 2016, doi: 10.6028/NIST.IR.8105.

[39] P. Wang, S. Tian, Z. Sun, and N. Xie, "Quantum algorithms for hash preimage attacks," *Quantum Eng*., vol. 2, no. 2, p. e36, 2020, doi: 10.1002/que2.36.