Quantum Information Processing (2024) 23:357
https://doi.org/10.1007/s11128-024-04564-x

COMMENT

Comment on “quantum identity authentication with single photon”

Davide Li Calsi[1] · Paul Kohl[1]

Received: 17 May 2024 / Accepted: 2 October 2024 / Published online: 19 October 2024
© The Author(s) 2024

Abstract

A few years ago Hong et al. (Quantum Inf Process 16:236, 2017) proposed a quantum identity authentication protocol using single photons and executable on currently available quantum hardware. Zawadzki later published two attacks on this protocol, and suggested a mitigation in the same work. In this comment we point out an additional vulnerability that causes the prover Alice to leak a percentage of her secret key at every authentication attempt. The latter is due to a problematic policy in the generation and management of decoy states. We conclude by showing a simple mitigation that addresses the issue.

Keywords Quantum identity authentication · Quantum cryptography · Quantum communication

1 Introduction

Quantum cryptography aims for information theoretically secure protocols relying only on noiseless communication and the laws of quantum mechanics. Ever since the pioneering works of Wiesner [1] and Bennett and Brassard [2] this field has produced several proposals to exploit the quirks of quantum information for cryptographic purposes. In particular, quantum authentication [3] has been a popular topic among researchers. It is a valuable cryptographic task, as it allows users to prove their identity to each other or to a server. "Authentication" is an umbrella term encompassing both message authentication and identity authentication. A message authentication code (MAC) is a scheme allowing a receiver to attest the integrity and authenticity of incoming messages. This requires that the sender and receiver pre-share a secret key, which they use to generate message tags to send alongside the messages. On the other

Davide Li Calsi and Paul Kohl have contributed equally to this work.

✉ Davide Li Calsi
davide.li-calsi@tum.de

[1] TUM School of Computation, Information and Technology, Technical University of Munich (TUM), Theresienstraße 90, 80333 Munich, Bavaria, Germany

hand, identity authentication consists of proving your identity to another user or party. In this work, we focus on the latter type of authentication.

Identity authentication is of practical interest, as it can be used to verify a user's identity before granting them access to exclusive resources or privileges. For instance, a bank may authenticate its users before letting them access their bank accounts. In this example, authentication ensures that only the legitimate owner of the account has access to it. This is necessary to prevent malicious attackers from accessing the user's account and causing financial damage.

The concept of identity is hard to rigorously define, and for practical purposes one often resorts to one of three paradigms, namely: authenticate based on knowledge, possession, or biometrics. The first requires users to provide some secret pre-shared information, such as a binary key or a password. Password-based identity authentication is the most widespread, and is used worldwide on a daily basis. Despite its simplicity, its security comes with non-trivial problems, such as the secure storage of password hashes [4]. The second requires users to provide a physical token to prove their identity, such as a physical unclonable function (PUF). Finally, the third paradigm authenticates users based on biometric features, such as their fingerprints.

Thanks to the quirks of quantum information, quantum authentication protocols achieve information-theoretic security. The latter is notoriously the strongest notion of security, as it does not rely on unproven computational assumptions and is effective even against computationally unbounded adversaries. Quantum identity authentication protocols are quite diverse. Some assume pre-shared entanglement [5–8] as a shared key for authentication. These proposals make use of the non-local correlations of entangled states to attest a user's identity. Despite their theoretical security, storing entanglement requires reliable quantum memories, an achievement beyond today's capabilities. Furthermore, many entanglement-based proposals consume entanglement to perform authentication, eventually reaching a case in which parties run out of entanglement and can no longer authenticate their identities.

Alternatively, thanks to the famous no-cloning theorem, one can construct quantum tokens that are efficiently verifiable but not clonable. This idea is known in the literature as quantum money [1, 9, 10], due to the (theoretical) possibility to use this technology to create unforgeable currency. One can distribute said tokens to users and use them as authentication keys, yielding a possession-based authentication. The main advantage of this solution is that, unlike classical keys, quantum tokens are guaranteed to be unclonable. However, as argued for entanglement-based schemes, such proposals are technically challenging due to requiring quantum memories.

Others do not use any entanglement or quantum keys [11–13], but encode classical keys into qubits to hide classical information from malicious eavesdroppers. The use of classical keys is an advantage due to removing the need for quantum memories. This class of protocols is quite heterogeneous, with protocols exploiting various quantum properties such as superposition, state indistinguishability, and more. Finally, recent proposals use a physical token for authentication such as a quantum PUF (QPUF) [14, 15]. QPUFs are the quantum extension of classical PUFs, and the resulting authentication schemes are similar to the classical ones. The major advantage is that classical PUFs base their unclonability on the current inability to control manufacturing processes (which may become predictable or controllable at some point in the future), while QPUFs are unclonable due to the laws of physics.

Not long ago Hong et al. [16] proposed a simple and efficient quantum protocol for identity authentication. The protocol requires relatively simple quantum hardware components, and is therefore implementable using currently available technology. Specifically, it only requires hardware to generate BB84 states and a standard measurement device. Unfortunately, few years lately Zawadzki [17] pointed out a few weaknesses in the original design. In the same work, he proposed a simple mitigation based on hash functions, but the latter was found not to be information theoretically secure [18], though nothing prevents it from achieving computational security. In this work we point out a new vulnerability in Hong et al.'s proposal due to a misuse of decoy states.

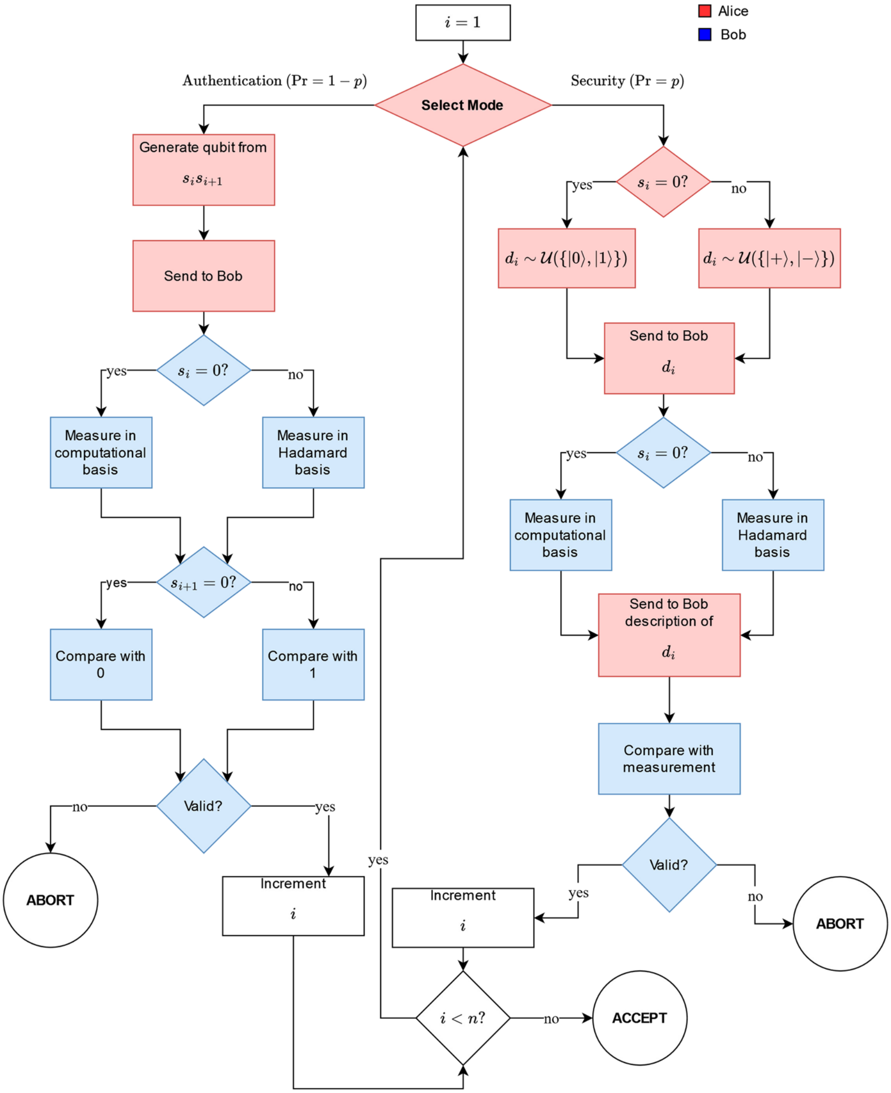
The paper is organized as follows: Sect. 2 presents preliminary concepts beneficial for the understanding of our argumentation, that is the original protocol in Subsection 2.1 and a vulnerability and its mitigation by Zawadzki in Sect. 2.2; Sect. 3 outlines the new vulnerability; Sect. 4 proposes a mitigation; finally, we draw our conclusions in Sect. 5.

2 Preliminaries

Quantum identity authentication protocols have been proposed since the 1990s [3]. Many proposals exploit one of the most distinctive properties of quantum mechanics, namely entanglement. While being theoretically secure, reliably and cheaply manipulating entangled particles has been a long-lasting challenge from the engineering viewpoint. Thus, researchers have devoted to the design and analysis of simpler alternatives. For instance, Yuan et al.'s protocol [19] was one of the earliest to require the preparation and measurement of independent single-photon states encoding pre-shared classical keys, a paradigm followed by the aforementioned scheme by Hong et al. too. Furthermore, both protocols use BB84 states to hide classical information. However, [19] prescribes a more complex four-stage interaction, during which the authentication key is updated.

2.1 Review of Hong et al.'s protocol

In the work of Hong et al. [16] a quantum identity authentication protocol was introduced (see Fig. 1), which does not rely on shared entanglement between the party to be authenticated (Alice) and the verifying party (Bob). Instead, this protocol relies on a pre-shared secret bitstring $s = (s_1, s_2, \ldots, s_l)$ with $(l = 2n) \wedge (n \in \mathbb{N})$, i.e. an even number of secret classical bits. From a high-level viewpoint, the protocol's goal is to compare the key on Alice's side with that on Bob's side without revealing its content to an eavesdropper. In practice, this can be useful to implement a sort of quantum username-and-password authentication scheme, e.g. to regulate access to users' accounts. The protocol has two different operating modes called *authentication mode* and *security mode*. Alice chooses randomly between security mode with some



$i = 1$
🟥 Alice
🟦 Bob
Authentication ($\Pr = 1 - p$)
Select Mode
Security ($\Pr = p$)
Generate qubit from $s_i s_{i+1}$
Send to Bob
$s_i = 0?$
yes
no
Measure in computational basis
Measure in Hadamard basis
$s_{i+1} = 0?$
yes
no
Compare with 0
Compare with 1
Valid?
no
yes
ABORT
Increment i
yes
$s_i = 0?$
yes
no
$d_i \sim \mathcal{U}(\{|0\rangle, |1\rangle\})$
$d_i \sim \mathcal{U}(\{|+\rangle, |-\rangle\})$
Send to Bob d_i
$s_i = 0?$
yes
no
Measure in computational basis
Measure in Hadamard basis
Send to Bob description of d_i
Compare with measurement
Valid?
yes
no
Increment i
ABORT
$i < n?$
no
ACCEPT

Fig. 1 Visual description of Hong et al.'s protocol [16]. Red boxes represent Alice's actions, while the blue ones represent Bob's steps. The notation $\mathcal{U}(S)$ represents the uniform distribution on set S. Adapted from [16] (Color figure online)

probability p or authentication mode with probability $1 - p$. The following protocol is carried out $l/2 = n$ times, viz. for each pair of two consecutive bits (s_i, s_{i+1}) from s for even i. In the different modes the procedure is as follows:

In authentication mode Alice generates a qubit to be sent to Bob from (s_i, s_{i+1}). In case s_i is 0 Alice chooses the rectilinear/computational basis $\{|0\rangle, |1\rangle\}$ for encoding and subsequently chooses the state $|0\rangle$ if $s_{i+1} = 0$ and $|1\rangle$ if $s_{i+1} = 1$. On the other hand, if s_i is 1 Alice chooses the diagonal/Hadamard basis $\{|+\rangle, |-\rangle\}$ and picks the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ if $s_{i+1} = 0$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ if $s_{i+1} = 1$. The state is then sent to Bob.

In security mode Alice generates a decoy state $d_i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ from the corresponding part of the secret (s_i, s_{i+1}) as follows. Again, s_i determines the choice of basis as before. $s_i = 0$ implies the choice of the rectilinear basis $\{|0\rangle, |1\rangle\}$ and $s_i = 1$ implies the diagonal basis $\{|+\rangle, |-\rangle\}$. The difference is now that the second bit s_{i+1} in the pair is irrelevant for the choice of the state from the respective basis. Alice chooses the state randomly from the selected basis, independent of s_{i+1}. d_i is now sent to Bob.

This is the procedure on Alice's side for now. Bob receives a qubit unknown to him. He measures it according to the basis which is dictated by s_i – again, $(s_i = 0 \Rightarrow \{|0\rangle, |1\rangle\}) \wedge (s_i = 1 \Rightarrow \{|+\rangle, |-\rangle\})$. s_i is the same for him and Alice, thus in authentication mode Bob will extract the correct result from the qubit 100% of the time (for perfect equipment) if the state was not tampered with. *Correct* in this case means that the measurement result coincides with s_{i+1}. After Bob measured the state he received, Alice communicates what mode she used and in security mode she additionally communicates the decoy state d_i for Bob to be able to check it. Then Bob will abort the protocol if there is a mismatch in measurement result and his secret/the decoy state, otherwise the procedure will be repeated for every pair of bits in s [16].

The security of this protocol is based upon the notions of conjugate coding [1], which is in turn an application of quantum state indistinguishability. Specifically, to an eavesdropper with no information on the secret key, Alice generates random BB84 states. By the principles of quantum information, these qubits provide no information on the corresponding secret key. On the other hand, if Bob knows Alice's key, he possesses enough information to distinguish the incoming qubits and validate their state. The main advantage is the minimal requirements in terms of quantum hardware. Unlike other quantum proposals, this protocol does not assume complex quantum hardware such as quantum memories or devices for entanglement distillation and management. The involved parties only need to generate BB84 states and perform relatively simple measurements. Overall, modern quantum hardware can easily support both tasks, thus making the protocol implementable in the short term.

2.2 Review of Zawadzki's attack and mitigation

According to Zawadzki the protocol by Hong et al. does not fulfil the requirements imposed on identity authentication protocols, as with a man-in-the-middle attack where the measurement basis is guessed randomly one bit of the pre-shared secret is leaked per authentication attempt by analysing the behaviour of Bob. Bob aborts the protocol if his measurement result was incorrect, thus leaking that the eavesdropper has chosen the wrong basis (corresponding to an even bit of the secret). Additionally, the bit corresponding to the encoded state (the odd bit of the secret belonging to the leaked even bit) is leaked in the subsequent protocol run. For the entangle-and-measure attack discussed by Hong et al., Zawadzki also shows that 2 bits of information of the secret are leaked per protocol run [17].

Additionally, Zawadzki provides a mitigation of the problems he showed. This mitigation includes the removal of the security mode and usage of a hash function in order to not directly compare the pre-shared secret but a session key. The session key is generated by the hash function from a random number and the pre-shared secret. Thus every authentication looks different and a modified communication behaviour presents any eavesdropper with an all-or-nothing problem every authentication attempt [17].

But it also has to be stated that this approach can just yield computational security. In fact, González-Guillén et al. [18] proved that, even with Zawadzki's modification, the unconditional security of the protocol would violate the no-go theorems on quantum secure two-party computation [20]. Therefore, this approach must leak some information at each authentication round. González-Guillén et al. showed a concrete attack to reduce the number of candidate keys at each authentication round. The attack itself is not guaranteed to be computationally efficient though, thus opening the door to computationally secure authentication if the hash function is computationally hard to invert.

3 Vulnerability

With this information in mind there seems to be another problem with Hong et al.'s protocol. At least in classical identity authentication protocols it is the normal case that there is a limited amount of pre-shared secret information, which is used multiple times. It seems reasonable to assume that the pre-shared secret is also reused in [16] and it is not stated otherwise in the paper. This is also one of the requirements for identity authentication stated by Zawadzki. But this fact opens up the protocol to some attacks. As mentioned in Sect. 2.2 the behaviour of Bob leads to information leakage, because he reveals some facts about the secret by aborting the protocol under certain conditions.

But one can argue that there is an even simpler attack vector. In every run of the protocol there are some rounds of security mode. Every time in security mode Alice reveals which decoy state d_i was sent. Even if an eavesdropper (Eve) does not alter any state but only takes note of the classical communication happening between Alice and Bob there is significant leakage of pre-shared secret information.[1] Every d_i that is communicated reveals the bit s_i of the corresponding pair of bits used in that instance of security mode *directly*. Because of this after a certain number of uses of the key Eve knows every even bit in s because statistically every pair (s_i, s_{i+1}) was used for security mode at some point. We can apply standard probability theory to estimate such a number.

Let us focus on an index i. During each authentication, the key bit s_i is revealed with probability p. Let N_i be a random variable representing the number of rounds after which s_i is revealed. It is easy to verify that N_i follows a geometric distribution $\mathrm{Geo}(p)$ so that

$$\Pr(N_i = k) = (1 - p)^{k-1} p$$

[1] It is a reasonable assumption that Eve can directly do this, because the identity authentication procedure is generally the first step before a secure channel between Alice and Bob is established.

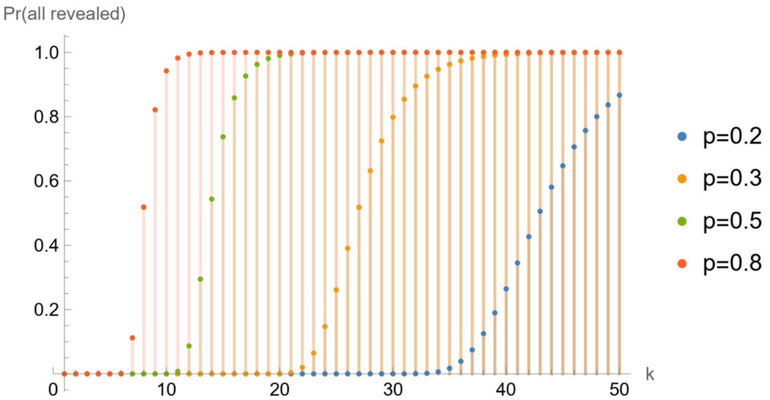


Fig. 2 Probability that all key bits in odd positions are revealed after k rounds or less for various values of p and $n = 10000$ (Color figure online)

This holds for any other index $j \in \{1, \ldots, n\}$ of the pair in question. Furthermore, each position is independent of all others. Hence the random variables $(N_1, \ldots, N_n)$ are independent geometric random variables. The probability that all of them are less or equal than k is the nth power of the cumulative distribution function for the geometric distribution. For integer k, this equals

$$\Pr(N_1 \le k, \ldots, N_n \le k) = (1 - (1 - p)^k)^n.$$

Figure 2 shows such a probability for a fixed $n = 10^4$ and various values of p. It clearly shows that even for low values of p, about 40 authentications suffice to leak all the key bits in odd position with high probability. For $p = 1/2$ the probability is close to one for $k \approx 15$.

At this point Eve can also recover the rest of the secret as follows. If the basis for encoding the key information is known Eve can measure the sent qubits in the appropriate basis and will get a certain measurement result. Because Eve knows that the basis of encoding is correct, after measuring she also knows with certainty (if the equipment is perfect) what state was used in the respective basis, which means she will get back the bit s_{i+1} of the respective round. Thus she can also create a new qubit in the correct state, which makes it possible for her to hide that the qubit was intercepted and measured.

To the authors’ knowledge nobody seems to comment on this problem. At least the following review of quantum identity authentication protocols [3] only mentions Hong et al.’s protocol [16] itself, Zawadzki’s analysis of it [17], and in turn González-Guillén et al.’s analysis of that [18]. More specifically, [18] even mentions that their attack that reduces the size of the key space is also applicable to Hong et al.’s protocol in authentication mode. Hong et al. themselves only consider three attack strategies, but do not take into account the situation when the secret is reused, which opens it up to the problems mentioned by Zawadzki and us [16].

Zawadzki points out that by running the protocol multiple times it is opened up to the possibility of collecting more and more bits of the secret, albeit not in the same way as we do here. Zawadzki proposes to extract information via looking at when the protocol is aborted, i.e. only one s_i bit is extracted per run [17].

Thus it is interesting that nobody seems to directly comment on the vulnerability we have shown, even though seemingly more involved attacks were found.

4 Mitigation

Decoy states have proven to be powerful against eavesdroppers in quantum cryptography ever since their first proposal by Hwang [21]. Due to their value, we show a simple mitigation to Hong et al.'s protocol allowing to generate and send decoy states without leaking precious key bits.

The latter consists of a modification to the decoy state generation policy adopted by Hong et al. (see Fig. 3). Alice still chooses between authentication and security mode at random, with probability p. When in security mode, instead of generating a decoy state whose basis depends on the key bits, decoy states can be uniformly random states from the set of BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Upon generating such a state, say $|\psi\rangle$, Alice sends it to Bob. On his side, Bob measures it according to his key bits, as if he was in authentication mode. To avoid confusion: if the ith bit of Bob's key $s_i = 0$ he measures in the computational basis, else he measures in the Hadamard basis. Once Bob confirms to Alice that he measured the incoming qubit she announces her mode of operation (security) and the state of her decoy qubit. Bob can now compare this information with his measurement result, and detect the presence of malicious eavesdroppers.

Unfortunately, this is only possible if Bob's measurement basis matches the basis of $|\psi\rangle$, which only happens with probability 50%. Without loss of generality, suppose Alice prepared a decoy state in the computational basis. If $s_i = 0$, Bob can perform the check after receiving the classical description of $|\psi\rangle$. If $s_i = 1$, then Bob cannot conclude anything about malicious eavesdropping, and the check is passed by default. However, if $2m$ decoy states are sent over one authentication round, on average Bob will guess the correct basis m times. Hence, it suffices to double the number of decoy states to still get the same security guarantees. It is not hard to see why this mitigation works: by making the decoy states independent and uncorrelated from Alice's key, they convey no information to an adversary. Furthermore, due to the well-known no-signalling theorem [22], Bob's measurement cannot convey any information on his key to Alice or Eve.

Although our mitigation covers the decoy states vulnerability, the work by Zawadzki [17] highlighted other vulnerabilities in the authentication phase. In the same paper, he suggested another mitigation using a random nonce and a hash function to turn Alice's key into a randomized one-time session key. Our mitigation addresses an orthogonal problem, and can in principle be combined with Zawadzki's proposal to increase the overall robustness. Recent work [18] showed that Zawadzki's proposal cannot achieve information theoretic security, as that would violate Lo's no-go theorem [20] on secure two-party computation. Nevertheless, one may still combine the two mitigations to achieve computational security through computationally secure hash function

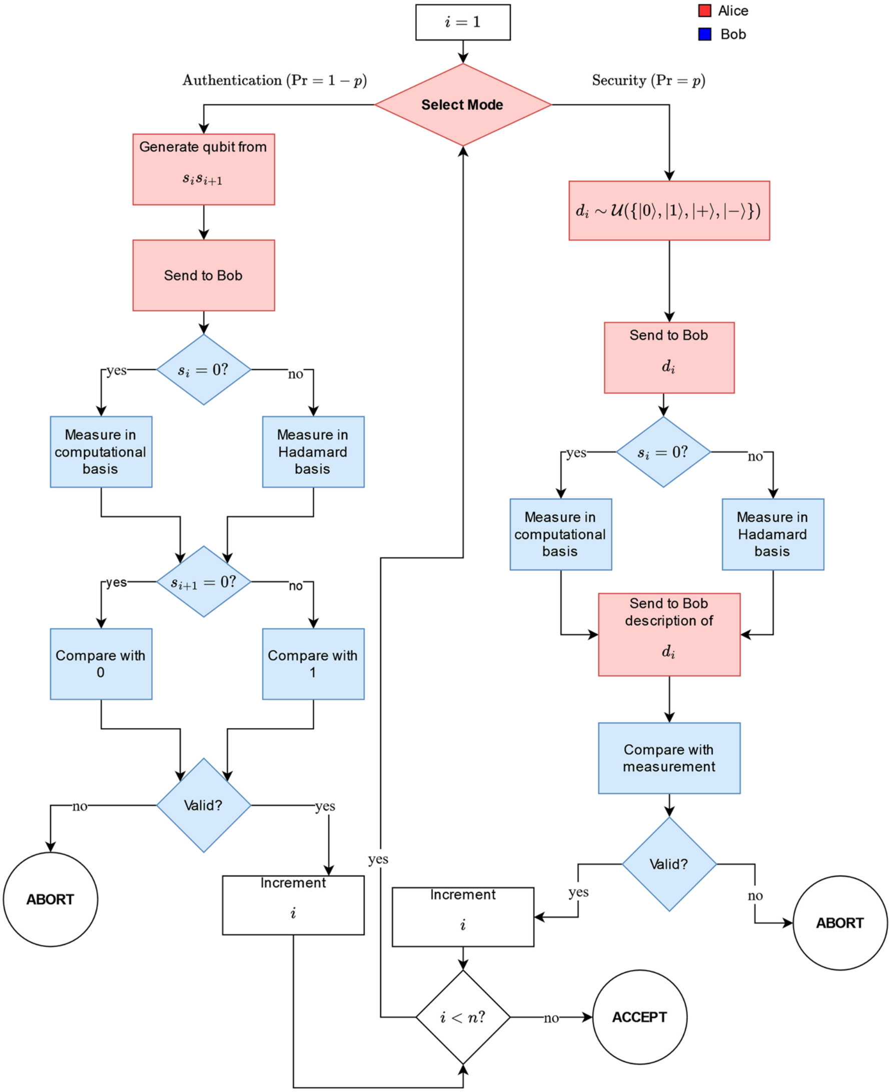

🟥 Alice
🟦 Bob
$i = 1$
Authentication ($\Pr = 1 - p$)
Select Mode
Security ($\Pr = p$)
Generate qubit from $s_i s_{i+1}$
Send to Bob
$s_i = 0?$
yes
no
Measure in computational basis
Measure in Hadamard basis
$s_{i+1} = 0?$
yes
no
Compare with 0
Compare with 1
Valid?
no
yes
ABORT
Increment i
$d_i \sim \mathcal{U}(\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\})$
Send to Bob d_i
$s_i = 0?$
yes
no
Measure in computational basis
Measure in Hadamard basis
Send to Bob description of d_i
Compare with measurement
Valid?
yes
no
ABORT
Increment i
yes
$i < n?$
no
ACCEPT

Fig. 3 Visual description of our modification. Red boxes represent Alice's actions, while the blue ones represent Bob's steps. The notation $\mathcal{U}(S)$ represents the uniform distribution on set S

for Zawadzki's modified protocol without removing security mode. A summary of all the described vulnerabilities and their mitigations can be found in Table 1.

5 Conclusions

This comment points out an additional weakness of Hong et al.'s identity authentication protocol due to a misuse of decoy states. By breaking the dependency between

Table 1 Overview of important attacks and vulnerabilities of Hong et al.'s protocol [16] and their mitigation

Vulnerability	Mitigation	Source
Direct leakage of odd bit of pre-shared secret bit pair in every use of security mode, subsequent recovery of even bit with hidden measure-and-resend attack	Generate uniformly random decoy states instead of using pre-shared secret bits for their generation. Problems in authentication mode untouched by this	This work
Impersonation attack with random guesses of sent state	By construction: Sufficient number of security mode rounds leads to eavesdropper detection	[16]
Measure-and-resend man-in-the-middle attack with random guess of measurement basis	By construction: Eavesdropper detection probability tends to 1 for increasing number of decoy states. But still information leaks due to multi-use of secret [17]	[16]
Entangle-and-measure attack with an ancilla for eavesdropper	By construction: Even for no information gained operation on both ancilla and sent state yields significant detection probability. But still information leaks due to multi-use of secret [17]	[16]
Information leaks due to multi-use of secret in authentication mode	Removal of security mode and hashing pre-shared secret with random number for single-use session secret. Relies on computational security of hash function. Also susceptible to attacks from [18]	[17]
Key space size reduction in authentication mode	No mitigation given; prepare-and-measure authentication susceptible to key space size reduction	[18]

decoy states and the secret key bits one may fix this problem at little to no cost. Furthermore, despite other works pointing out other vulnerabilities, one can combine previously suggested mitigations with ours to result in a secure protocol. However, such a combination can only guarantee at best computational security.

Author Contributions DLC wrote Sections 1 and 4 and prepared Figure 1. PK wrote Sections 2 and 3. Both authors wrote Section 5 and reviewed the manuscript.

Funding Open Access funding enabled and organized by Projekt DEAL. The authors acknowledge funding from the Federal Ministry of Education and Research of Germany via the Q-TREX and QDCamNetz projects (Grant Numbers 16KISR026 and 16KISQ077)

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Wiesner, S.: Conjugate coding. SIGACT News **15**(1), 78–88 (1983). https://doi.org/10.1145/1008908.1008920
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7–11 (2014). https://doi.org/10.1016/j.tcs.2014.05.025
3. Dutta, A., Pathak, A.: A short review on quantum identity authentication protocols: How would Bob know that he is talking with Alice? Quantum Inform. Process. **21**(11), 369 (2022). https://doi.org/10.1007/s11128-022-03717-0
4. Gasti, P., Rasmussen, K.B.: On the security of password manager database formats. In: Foresti, S., Yung, M., Martinelli, F. (eds.) Computer Security – ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10–12, 2012. Proceedings 17. ESORICS 2012. Lecture Notes in Computer Science, vol. 7459, pp. 770–787. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33167-1_44
5. Curty, M., Santos, D.J.: Quantum authentication of classical messages. Phys. Rev. A **64**(6), 062309 (2001). https://doi.org/10.1103/PhysRevA.64.062309
6. 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). https://doi.org/10.1016/s0375-9601(01)00129-3
7. Li, X., Barnum, H.: Quantum authentication using entangled states. Int. J. Found. Comput. Sci. **15**(04), 609–617 (2004). https://doi.org/10.1142/S0129054104002649
8. Zhang, S., Chen, Z.-K., Shi, R.-H., Liang, F.-Y.: A novel quantum identity authentication based on bell states. Int. J. Theor. Phys. **59**(1), 236–249 (2020). https://doi.org/10.1007/s10773-019-04319-w
9. Aaronson, S., Christiano, P.: Quantum money from hidden subspaces. In: Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing. STOC '12, pp. 41–60. Association for Computing Machinery, New York (2012). https://doi.org/10.1145/2213977.2213983
10. Gavinsky, D.: Quantum money with classical verification. In: 2012 IEEE 27th Conference on Computational Complexity. CCC '12, pp. 42–52. IEEE Computer Society, USA (2012). https://doi.org/10.1109/CCC.2012.10
11. Barnum, H., Crépeau, C., Gottesman, D., Smith, A., Tapp, A.: Authentication of quantum messages. In: The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings, pp. 449–458 (2002). https://doi.org/10.1109/SFCS.2002.1181969 . IEEE
12. Kanamori, Y., Yoo, S.-M., Gregory, D.A., Sheldon, F.T.: On quantum authentication protocols. In: GLOBECOM '05. IEEE Global Telecommunications Conference, 2005., vol. 3, p. 5 (2005). https://doi.org/10.1109/GLOCOM.2005.1577930
13. Zhu, H., Wang, L., Zhang, Y.: An efficient quantum identity authentication key agreement protocol without entanglement. Quantum Inform. Process. **19**(10), 381 (2020). https://doi.org/10.1007/s11128-020-02887-z
14. Arapinis, M., Delavar, M., Doosti, M., Kashefi, E.: Quantum physical unclonable functions: possibilities and impossibilities. Quantum **5**, 475 (2021). https://doi.org/10.22331/q-2021-06-15-475
15. Doosti, M., Kumar, N., Delavar, M., Kashefi, E.: Client-server identification protocols with quantum PUF. ACM Trans. Quantum Comput. **2**(3), 1–40 (2021). https://doi.org/10.1145/3484197
16. Hong, C.H., Heo, J., Jang, J.G., Kwon, D.: Quantum identity authentication with single photon. Quantum Inform. Process. **16**(10), 236 (2017). https://doi.org/10.1007/s11128-017-1681-0
17. Zawadzki, P.: Quantum identity authentication without entanglement. Quantum Inform. Process. **18**(1), 7 (2019). https://doi.org/10.1007/s11128-018-2124-2

18. González-Guillén, C.E., González Vasco, M.I., Johnson, F., Pozo, Á.L.: An attack on Zawadzkiâ€™s quantum authentication scheme. Entropy **23**(4), 389 (2021). https://doi.org/10.3390/e23040389
19. Yuan, H., Liu, Y.-M., Pan, G.-Z., Zhang, G., Zhou, J., Zhang, Z.-J.: Quantum identity authentication based on ping-pong technique without entanglements. Quantum Inform. Process. **13**(11), 2535–2549 (2014). https://doi.org/10.1007/s11128-014-0808-9
20. Lo, H.-K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997). https://doi.org/10.1103/PhysRevA.56.1154
21. Hwang, W.-Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**(5), 057901 (2003). https://doi.org/10.1103/physrevlett.91.057901
22. Hall, M.J.W.: Imprecise measurements and non-locality in quantum mechanics. Phys. Lett. A **125**(2–3), 89–91 (1987). https://doi.org/10.1016/0375-9601(87)90127-7

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.