Quantum password authentication against man-in-the-middle attack

E. Karpov
Centre for Quantum Information and Communication (QuIC), Ecole Polytechnique de Bruxelles, CP 165/59, Université libre de Bruxelles, 1050 Brussels, Belgium
(Dated: June 30, 2016)

Authentication with recently proposed quantum password protocol is secure against impersonation. Here we show that original version of the protocol is not secure against active malicious prover and verifier, however a slight modification provides a possibility for a legitimate party to detect the attacks. The password is reusable in the absence of the attacks. Otherwise the security of the authentication scheme should be provided by password change. In this way the overall scheme becomes resistant to man-in-the-middle attack.

Authentication is one of the cornerstones of secure communications. This is a crucial issue for cloud applications because they imply the access of data and services over the network only. This increases the risk of man-in-the-middle attack via credentials theft. Zero-knowledge proofs and one-time tokens are promising means for protection of the user access credentials like PIN (Personal Identification Number) during authentication process. Eventual arrival of quantum computers threatens the security of cryptographic protocols based on computational complexity. This is not the case for Quantum protocols because their security is based on the laws of physics like no-cloning principle. Quantum Key Distribution is the most successful example. However, the quantum realization of other cryptographic primitives is more problematic and sometimes even impossible like quantum bit commitment. Among them is quantum one-way oblivious password identification, which is impossible because all *one-sided* two party computations are insecure [1]. However, under a realistic assumption of bounded quantum storage model [2] and noisy-quantum storage model [3] provably-secure two-party computation is possible, which makes possible secure identification. Here we present the results of our study of a recently proposed and implemented quantum protocol [4, 5], which allows secure user identification. The protocol uses the same set of states as the QKD protocol with six-states [6]. It assumes the knowledge of the password by both communicating parties, prover and verifier. For each symbol of the password the verifier prepares a state corresponding to the symbol and sends it to the prover who should return to the verifier the orthogonal one. More than one state is associated to any password symbol and therefore prover should invert the state without knowing it as if he applied a universal not (UNOT) operation. The security of the protocol is based on the impossibility of any physical realization of UNOT operation with quantum states because of its anti-unitarity.

The protocol uses the following properties of Pauli operators acting on states of three mutually unbiased bases: $\{|0\rangle, |1\rangle\}$, $\{|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$, $|\{\pm_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)\}$. Each Pauli operator $\hat{\sigma}_x$, $\hat{\sigma}_y$, and $\hat{\sigma}_z$ flips the states of two bases to the orthogonal ones and leaves the states of the third base unchanged (up to a global phase/sign). The sets of states being flipped by one of the Pauly operators determine circles on the Bloch sphere so that one can encode a trit into the sets and corresponding Pauli operators.

so-called real circle

$$\hat{\sigma}_y : \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} = \text{“0”}, \tag{1}$$

“complex” meridian

$$\hat{\sigma}_z : \{|+\rangle, |-\rangle, |+_i\rangle, |-_i\rangle\} = \text{“1”}, \tag{2}$$

and the equator

$$\hat{\sigma}_x : \{|0\rangle, |1\rangle, |+_i\rangle, |-_i\rangle\} = \text{“2”}. \tag{3}$$

Note that, although each Pauli operator realizes NOT operation on the states of a particular set the unitarity of the transformation is preserved by its *non-universality*, namely the states of the third basis are left unchanged so that the realized NOT operation is not universal.

The original protocol has following steps [4, 5]: The password is a string of n trits known to both prover and verifier before the protocol starts.

1. For first trit of the password verifier randomly chooses one of four states encoding the value of the trit, prepares an optical pulse in this state and sends it to the prover.

2. Knowing the password prover knows the value of the trit. He applies corresponding Pauly operator and sends the state back to the verifier. By doing this, the prover flips the received state into the orthogonal one.

3. By applying the von Neumann measurement to the received state verifier checks whether the state was properly flipped.

4. The above steps are repeated for all trits of the password and verifier counts the number of errors (trits for which his measurement does not confirm the state flip).

5. After the last trit of the password was checked verifier calculates the error rate. If the error rate is lower than the security threshold set for the protocol he accepts.

The security analysis of the protocol against impersonation by malicious prover is simple. In case of classical password of n, brut force attack corresponds to random guess of password sequence, one of 3^n possible. The probability to get accepted by verifier (answer YES) after having been rejected m times (m answers NO) is

$$P_{\rm cl}({\rm YES}|{\rm NO}^{\otimes m}) = \frac{1}{3^n - m}. \quad (4)$$

In the quantum setting, the attacker may be accepted even if he applies an operator corresponding to a wrong "trit", because each state sent by verifier can be flipped by two Pauli operators. For example, the set corresponding to trit "1" is defined by the two bases, whose states are flipped by $\hat{\sigma}_z$, however the states $|+\rangle$ and $|-\rangle$ are flipped by $\hat{\sigma}_y$ as well and the states $|+_i\rangle$ and $|-_i\rangle$ are flipped also by $\hat{\sigma}_x$. For any sequence of states chosen by verifier, there exists 2^n sequences of operations leading to answer YES . Then the probability to be accepted after m trials is

$$P_{\rm q}({\rm YES}|{\rm NO}^{\otimes m}) = \frac{2^n}{3^n - m}. \quad (5)$$

This probability is higher than the one for a classical password however the acceptance gives to the attacker the knowledge of a the true password only with probability 2^{-n}. This probability is always smaller than the probability to be accepted after $m < 3^n$ random trials, hence the knowledge of the sequence of operations which happens to be accepted does not provide the correct password. Nevertheless, it increases the probability to guess successfully the value of the password symbol at the next random trial from 1/3 to 1/2. However, the security analysis of the repeated password use requires the consideration of active attacks on the password.

An active malicious verifier trying to infer the password send arbitrary choses one of three bases and sends one of two basis states to the prover. Then he receives back the same or orthogonal state. By applying the von Neumann measurement int he same basis he can discriminates the received states unambiguously. If the state was not changed then the operation applied by the prover is determined uniquely thus providing the value of the password symbol. If the flipped state was received two possibilities are left for the operation, which was applied as for the value of the password symbol. At the end of the run the malicious verifier determines uniquely one third of the password symbols and for two third the ambiguity reduces from one out of three to one out of two. He can remove this ambiguity at the second run by choosing another basis at the place of still ambiguous symbols. By determining the received stases as being flipped or not allows him to determine the operation applied and thus the value of the symbol uniquely. The password is not secure against an active malicious verifier however the prover can detect this attack if he sacrifices a part of received states. He applies the von Neumann measurement in chosen randomly one of two bases corresponding to the trit value of the symbol and asks the verifier to reveal the state sent. On average in half of cases there should be a perfect match between the measurement result and the state sent. In the other half the result will be perfectly random. The discussed above attack of the malicious verifier will be detected due to the change in the statistics of the results. The security thresholds can be calculated. If they are exceeded one considers that an attack takes place and the password is compromised. A new password should be developed. If not, the "sacrificed" symbols are removed from the password and the rest of the password can be reused.

The task of an active malicious prover trying to identify the correct operations and thus the corresponding trit values is more difficult, because he has neither control nor knowledge of the basis choice. At the same time, in order to be not noticed he should return correctly flipped states one by one. Hence he has two possibilities. One is to attack each traveling state individually trying to get the best possible knowledge on the state and thus make the best possible choice of the state to be returned. Even this attack was perfect this would still leave the eavesdropper with two possible candidates for the correct unitary which had to be applied to the state and thus with two possible trit values. In order to find out the correct value eavesdropper would need the second round. However, any such attack is not perfect, and therefore the eavesdropper will return some wrong states. By observing his measurement statistics the verifier would detect the attack and renew the password. Moreover the individual attack may reveal only a partial information on the state. In order to get more information, the eavesdropper may use another possibility by applying a coherent attack to the whole password. However, in this case the only possible choice of the states to be sent back is random because the information from such attack comes after all exchanges of states are made. In this case more errors is introduced into the returned states and the attack is even better detected forcing the verifier to renew the password. The new password prevents the eavesdropper from getting more information of the password at the subsequent rounds and makes useless the information he already obtained.

In conclusion, we has shown that the quantum password, which is secure against a passive impersonation by malicious prover, is not resistant to the attacks by active prover and /or verifier who want to learn the password. However a slight modification of the protocol allows detection of the attacks. If an attack is detected the security of the authentication scheme against man-in-the-middle attack can be provided by password change. Although the protocol does not provide the password renewal scheme as for example [7, 8] no entangles states are required.

[1] Hoi-Kwong Lo, *Insecurity of quantum secure computations*, Phys. Rev. A **56**, 1154 (1997).

[2] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, *in 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society, Pittsburgh, PA, USA, 2005), p. 449.

[3] C. Schaffner, *Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model*, Phys. Rev. A **82**, 032308 (2010).

[4] J. Niset, L.-P. Lamoureux, and N. J. Cerf, *Quantum password*, In: Proc. 32nd WIC Symposium on Information Theory in the Benelux. First joint WIC/IEEE SP Symposium on Information Theory and Signal Processing in the Benelux, Brussels, May 11, 2011

[5] L.-P. Lamoureux, *Theoretical and experimental aspects of quantum cryptographic protocols*, PhD thesis (Université libre de Bruxelles, 2006).

[6] D. Bruß, *Optimal Eavesdropopig in QUantulm Cryptography with Six States*, Phys. Rev. Lett. **81**, 3018 (1998).

[7] K. Boström, T. Felbinger, Phys. Rev. Lett. **90**, 187902 (2002).

[8] Z. Znag, G. Zeng, N. Zhou, J. Xiong, *Quantum identity authentication based on ping-pong technique for photons*, Phys. Lett. A 356, 199, (2006).