Analysis of one semi-quantum-honest key agreement scheme in MSTSA structure without entanglement

Zhengjun Cao[1], Lihua Liu[2]

Abstract. We show that the key agreement scheme [Quantum Inf. Process., 20:188, 2021] is flawed. (1) It requires that the quantum channel must be intact so as to keep the transferred photon sequences complete and undamaged, even if the channel is tapped. But this is unrealistic because of quantum non-cloning theorem. (2) The user's capability is artificially assumed, who can measure a hybrid photon sequence only with Z-basis, unable to measure with X-basis. (3) It requires an authenticated classical channel for the negotiation between Alice and Server_B. If such a channel is available, the scheme can be greatly simplified using the mechanism in BB84 protocol.
Keywords: Unregistered quantum server, Key agreement, Key transport, Mutual authentication

1 Introduction

Cryptography is a discipline of studying the techniques that prevent an adversary from recovering messages or cheating users. The former means that the adversary cannot retrieve the information encoded in physical signals even if all transferred signals were captured, called confidentiality or privacy. The latter means that the adversary cannot use any false identities or falsified signals to cheat users, called authentication, including identity authentication and message authentication.

The transmitted signals could be altered due to some interferences, such as ambient noises and sudden faults in equipments. To make sure that the receiver can retrieve the right signals, the sender should add some redundancies into the original string and obtain a longer string which is truly sent. The dependencies of all bits in the new string can be used for checking and correcting errors occurred in the transmission. The theory about the above process is called channel error-correcting code.

The modulation and measurement of classical states of photoelectric signals have become easy. So an adversary can capture all transferred signals by monitoring communication channels. In classical cryptography, it is always assumed that all transferred signals are available to an adversary. Since classical states of transferred signals are not dramatically disturbed by an eavesdropper, the intended receiver can recover the signals. Both the sender and the receiver cannot detect the existence of eavesdropping. That is to say, the classical cryptography cannot detect eavesdropping. As for as confidentiality, the classical cryptography aims to prevent an adversary from recovering the message encoded in signals, which is *an art of intelligence to study what mathematical transformations are not invertible and how to insert trapdoors into these transformations.*

[1]Department of Mathematics, Shanghai University, Shanghai, 200444, China
[2]Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

In daily life, eavesdropping is everywhere. Should we tolerate eavesdropping or eradicate it? For a common communication, the first thing we are concerned is to ensure that the intended receiver can recover the right signals. The second thing is to prevent an adversary from retrieving plaintext. The classical cryptography assumes that an adversary has complete access to the communication between the sender and the receiver. That is, the classical cryptography tolerates eavesdropping, not having the intention to eradicate it.

In 1984, Bennett and Brassard [1] published a paper which claimed that quantum cryptography, based on Heisenberg's uncertainty principle, can detect eavesdropping and was absolutely secure. As we know the states of classical communication signals include magnitude of voltage, light frequency and intensity, electromagnetic wave frequency, and so on. But the states measured in quantum communication are polarizations of a single photon (not a beam of light), spins of a single electron, etc. Since an unknown quantum state cannot be copied, it has 1/2 chance to change the state when an adversary tries to measure it. Hence, the intended receiver could fail to recover the original state. After the sender and the intended receiver finish the process of transferring quantum states, they make use of an authenticated classical channel to publicly compare a portion of quantum states. If the compared quantum states which are measured by a same measurement choice are not consistent, then the inconsistency possibly results from the disturbance generated by an eavesdropper.

The advantage that quantum cryptography can prevent an adversary from obtaining right signals has attracted much attention [2, 3, 6–11, 13–18, 21]. Actually, quantum cryptography aims to prevent an adversary from capturing signals, which is *an art of physical technology to study the modulation and measurement of quantum signals, and how to increase the spatial distance of transferring quantum signals*. It must make use of some classical channels for identity authentication and transferring messages. Naturally speaking, quantum cryptography is an extension of classical cryptography by using additional quantum channels to detect eavesdropping.

In 2019, Yang *et al.* [20] have presented a quantum key agreement protocol based on Bell states. It has shown its flaws [5], and clarified the difference between key transfer and key agreement. Very recently, Yang *et al.* [19] have also presented one key agreement scheme in multi-server to server architecture without entanglement. In this note, we show its flaws and clarify some unrealistic requirements for the scheme.

2 Review of the scheme

Let $Z = \{|0\rangle, |1\rangle\}$ be the computational basis of a qubit, and $X = \{|+\rangle, |-\rangle\}$ be another basis, where $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ and $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$. The polarization code is

$$\begin{array}{llllll} Z\text{-basis}: & |0\rangle & \text{polarized as} & \rightarrow, & |1\rangle & \text{polarized as} \quad \uparrow \\ X\text{-basis}: & |0\rangle & \text{polarized as} & \nearrow, & |1\rangle & \text{polarized as} \quad \nwarrow \end{array}$$

There are three entities, Alice, Server_A, and Server_B. Alice is a legal user, who is registered on quantum Server_A, but unregistered on Server_B. She wants to log in to Server_B via Server_A.

It assumes that both Server_A and Server_B have the capabilities to process quantum bits, including preparing and measuring quantum bits (Z-basis, X-basis). But Alice can only perform classical operations, such as preparing, measuring, sending, rearranging, and reflecting a particle in the basis Z, and any other classic operation on a classic computer.

Table 1: The Yang *et al.*'s key agreement scheme

Alice (owning key K_{AS_A})	Server$_A$ (owning keys $K_{AS_A}, K_{S_AS_B}$)	Server$_B$ (owning key $K_{S_AS_B}$)
Pick a random number r_A.	Compute $M_{S_A} = ID_A \| ID_{S_B} \|$	
$\xrightarrow{Request \| r_A}$ [authenticated & confidential channel]	$F(K_{S_AS_B}) \| H(K_{AS_A} \| ID_A \| ID_{S_B} \| r_A)$, where $F(\cdot)$ is a pseudo-random function.	
	Use Z-basis to encode M_{S_A} into a photon sequence M'_{S_A}.	
	Convert M'_{S_A} into Q'_{S_A} by Rule 1.	Parse Q_{S_A} to get Q'_{S_A}, M'_{S_B}.
	Compute $M_{S_B} = r_A \| ID_A \| ID_{S_A} \| H(K_{S_AS_B} \| ID_A \| ID_{S_B})$.	Decode M'_{S_B} into classical bits sequence by Z-basis or X-basis, to get M_{S_B}. Parse it to get ID_A, $r_A, H(K_{S_AS_B} \| ID_A \| ID_{S_B})$.
	Use Z-basis or X-basis to encode M_{S_B} into a photon sequence M'_{S_B} based on $K_{S_AS_B}$. Construct Q_{S_A} from M'_{S_B} and Q'_{S_A} by Rule 2.	Check $H(K_{S_AS_B} \| ID_A \| ID_{S_B})$. If OK, pick a random number r_{S_B}.
Parse the received photon sequence to get Q'_{S_A}, r_{S_B}. Remove the decoy photons in Q'_{S_A} by Rule 1 to get M'_{S_A}.	$\xrightarrow{Q_{S_A}}$ [quantum channel]	Construct the sequence $Q'_{S_A} \| r_{S_B}$.
Decode it by Rule 1 to get M_{S_A}.	$\xleftarrow{Q'_{S_A} \| r_{S_B}}$ [quantum channel]	Transfer it to Alice.
Parse it to get $ID_{S_B}, F(K_{S_AS_B})$. Check $H(K_{AS_A} \| ID_A \| ID_{S_B} \| r_A)$. If OK, ask for some subscripts prepared with Z-basis for r_{S_B}.		Tell Alice the subscripts of some photons prepared with Z-basis. Negotiate with Alice to get $Sub(r_{S_B})$. Compute $F(K_{S_AS_B})$.
Negotiate to get $Sub(r_{S_B})$.	$\xleftarrow{\text{negotiation}}$ [authenticated channel]	Set the session key as $SK_{AS_B} = H(F(K_{S_AS_B}) \| Sub(r_{S_B}) \| r_A)$.
Set the session key as $SK_{AS_B} = H(F(K_{S_AS_B}) \| Sub(r_{S_B}) \| r_A)$.		

Table 2: The Rule 1 and Rule 2

Rule 1.	If a bit in K_{AS_A} is 0, insert a decoy photon behind. Otherwise, insert it before. See the below example.
key K_{AS_A}:	1 1 0 1 0 0 1 0
message M_{S_A}:	1 0 1 0 1 1 0 0
photons M'_{S_A}:	↑ → ↑ → ↑ ↑ → →
Decoy photons:	↑ ↖ → ↑ ↗ → ↗ ↑
hybrid sequence Q'_{S_A}:	↑↑↖→↑→↑→↑↗↑→↗→→↑
Rule 2.	If a bit in $K_{S_AS_B}$ is 0, measure with Z-basis, otherwise, with X-basis. If a bit in $K_{S_AS_B}$ is 0, insert two photons $Q'_{S_{A_i}} Q'_{S_{A_{i+1}}}$ behind $M'_{S_{B_i}}$. Otherwise, insert it before. See the below example.
key $K_{S_AS_B}$:	1 0 0 1 0 0 1 1
message M_{S_B}:	0 1 1 0 1 0 1 0
photons M'_{S_B}:	↗ ↑ ↑ ↗ ↑ → ↖ ↗
hybrid sequence Q'_{S_A}:	↑↑↖→↑→↑→↑↗↑→↗→→↑
hybrid sequence Q_{S_A}:	↑↑↗↑↖→↑↑→↑→↗↑↑↗→↑→↗→↖→↑↗

In the proposed scenario, Server_A is assumed to be semi-honest and having two pre-shared secret keys K_{AS_A} and $K_{S_AS_B}$ with Alice and Server_B, respectively. Server_A follows protocol steps but could try to extract information about inputs or outputs from other entities. For conveniences, we now revisit the scheme and depict it as follows (see Table 1 and Table 2).

3 Analysis of the scheme

Though the considered scenario in Yang *et al.*'s scheme [19] is novel and interesting, we find the scheme itself has some flaws.

3.1 A false requirement

The scheme requires that the used quantum channel must be intact so as to keep the transferred photon sequences complete and undamaged, even if the channel is tapped. Concretely, the quantum channel between Server_A and Server_B must be usable to ensure Server_B can recover the quantum sequence Q_{S_A}, which is a hybrid photon sequence modulated with Z-basis and X-basis, not a unique basis. By the well-known quantum non-cloning theorem, we know, Server_B cannot measure a photon with two bases concurrently.

To ensure Alice can recover the quantum sequence $Q'_{S_A}\|r_{S_B}$ sent by Server_B, the scheme requires that there exists a classical channel for negotiation, which must be authenticated so as to Alice and Server_B can authenticate each other. But Alice shall fail to recover $Q'_{S_A}\|r_{S_B}$ if an adversary taps the quantum channel, because any eavesdropping behavior will change the polarization direction of an unknown photon with a probability of $1/2$.

We want to stress that the requirement of intact quantum channels is incompatible with the well-known BB84 protocol [1], in which a quantum channel is only used to transmit a sequence, shared between Alice and Bob but equal only in a portion of the positions. A smaller "sifted" sequence is finally obtained which is equal for Alice and Bob. In the presence of eavesdropping, some transmitted photons will be certainly changed by this interference. Therefore, the users can find the existence of such interference by publicly comparing the consistency of a small part of photons.

We find some quantum information researchers have confused key secret sharing [4], key transport, and key agreement. The idea of secret sharing is to start with a secret, and divide it into pieces called shares which are distributed among users such that the pooled shares of specific subsets of users allow reconstruction of the original secret. In a key transport protocol one party creates or otherwise obtains a secret value, and securely transfers it to the other(s). But in a key agreement protocol a shared secret is derived by two (or more) parties as a function of information contributed by each of these, such that no party can predetermine the resulting value [12]. Note that in the presence of adversaries, a quantum channel even associated with an authenticated classical channel, cannot be used for transporting data.

3.2 An inconsistent assumption

The user's capability is artificially assumed, who can measure a hybrid photon sequence only with Z-basis, unable to measure with X-basis. To make up for this defective assumption, it requires a classical channel for negotiation between the user and Server_B. From the practical point of view, it

is easy for Alice to own the capability of measuring with X-basis, if she is already able to measure with Z-basis. The two kind of measuring equipments are really inexpensive and broadly used. It seems that the scheme mixes up the following two things:

- a user cannot measure a photon with two bases concurrently, which is true;
- a user cannot measure a photon sequence with two bases, which is false.

3.3 An associated channel

It specified (see §3.2.4, [19]): *Alice uses Z-basis to measure r_{S_B}. Then because Alice can't use X-basis measurement, Server$_B$ will* ***tell*** *Alice the subscript of some photons prepared with Z-basis after all Alice has measured. Finally, Alice and Server$_B$* ***negotiate*** *to choose parts of Z-basis prepared photons to get $Sub(r_{S_B})$*. Clearly, the scheme requires an authenticated classical channel for the negotiation between Alice and Server$_{\rm B}$. We want to stress that:

(1) If such a classical channel is accessible and Alice can measure a photon sequence with both Z-basis and X-basis as usual, the scheme can be greatly simplified using the mechanism in BB84 protocol, which is just for two participants without any registration key to create a session key for the later using. In the considered scenario, Alice has just no registration key on Server$_{\rm B}$, and is assumed to access to the authenticated classical channel. The mechanism in BB84 protocol will work well for this case.

(2) If such a classical channel is inaccessible to Alice and Server$_{\rm B}$, they cannot authenticate each other, and the semi-honest party, Server$_{\rm A}$, can launch man-in-the-middle attack to cheat Alice and Server$_{\rm B}$, because Server$_{\rm A}$ knows either $F(K_{S_AS_B})$ or r_A. To do this, Server$_{\rm A}$ masquerades as Alice to negotiate with Server$_{\rm B}$ to get $Sub(r_{S_B})$. Then it masquerades as Server$_{\rm B}$ to negotiate with Alice to agree on the same $Sub(r_{S_B})$. Finally, Server$_{\rm A}$ can compute the resulting key $SK_{AS_B} = H(F(K_{S_AS_B})\|Sub(r_{S_B})\|r_A)$.

The original security analysis for man-in-the-middle attack (see §4.3.2, [19]) has simply claimed that "*Eve does not know the secret $K_{S_AS_B}$, ...*" It does not consider that Server$_{\rm A}$ is just a semi-honest entity, who can act as the role of Eve, after he honestly performs the first half procedure in which he is really involved (see Table 1). In this case, Eve does know the secret $K_{S_AS_B}$.

The security analysis for internal attack (§4.2, [19]) is not sound. It claims that: " *After Server$_B$ receives the request, the r_{S_B} is directly rebounded to Alice with Q'_{S_A}. In this process, Server$_A$ cannot participate.*" As discussed before, in this case Server$_{\rm B}$ cannot ensure that the photon sequence $Q'_{S_A}\|r_{S_B}$ is indeed sent to Alice.

By the way, the classical channel for Alice to transfer $Request\|r_A$, is either authenticated or confidential. Though the scheme has not specified the procedure to authenticate Alice's identity and her request, the registration key K_{AS_A} can be used to achieve this target.

4 Conclusion

We show that the Yang *et al.*'s quantum key agreement scheme is flawed. The scheme has confused key transport model with key agreement model, and wrongly required that the quantum channels

were intact to enable the participants to recover the whole data transferred via these channels. We hope this note could correct some misunderstandings about quantum key agreement scheme.

References

[1] C. Bennett and G. Brassard. Quantum cryptography, public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[2] D. Boschi and *et al.* Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels. *Physics*, 80(6):1121–1125, 1997.

[3] D. Bouwmeester and *et al.* Experimental quantum teleportation. *Nature*, (390):575, 1997.

[4] Z. J. Cao and O. Markowitch. A note on some quantum secret sharing schemes. *International Journal of Quantum Information*, 8(3):451–456, 2010.

[5] Z. J. Cao and O. Markowitch. A note on "new quantum key agreement protocols based on Bell states". *Quantum Information Processing*, 20(2):74, 2021.

[6] T. Jennewein and *et al.* Quantum cryptography with entangled photons. *Physical Review Letters*, (84):4729–4732, 2000.

[7] X. M. Jin and *et al.* Experimental free-space quantum teleportation. *Nature Photonics*, 4(6):376–381, 2010.

[8] Y. H. Kim, S. Kulik, and Y. Shih. Quantum teleportation of a polarization state with a complete Bell state measurement. *Physical Review Letters*, 86(7):1370–3, 2001.

[9] N. Lee and *et al.* Teleportation of nonclassical wave packets of light. *Science*, 332(6027):330–333, 2011.

[10] X. S. Ma and *et al.* Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489(7415):269–273, 2012.

[11] K. Mattle and *et al.* Dense coding in experimental quantum communication. *Physical Review Letters*, 76(25):4656–4659, 1996.

[12] A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, USA, 1996.

[13] C. Nolleke and *et al.* Efficient teleportation between remote single-atom quantum memories. *Physical Review Letters*, 110(140403), 2013.

[14] S. Olmschenk and *et al.* Quantum teleportation between distant matter qubits. *Science*, 323(5913):486–489, 2009.

[15] J. W. Pan and *et al.* Experimental realization of freely propagating teleported qubits. *Nature*, 421(6924):721–725, 2003.

[16] D. Rideout and *et al.* Fundamental quantum optics experiments conceivable with satellites-reaching relativistic distances and velocities. *Quantum Gravity*, (29):224011, 2012.

[17] M. Riebe and *et al.* Deterministic quantum teleportation with atoms. *Nature*, 429(6993):734–737, 2004.

[18] R. Ursin and *et al.* Communications: quantum teleportation across the Danube. *Nature*, 430(7002):849, 2004.

[19] J. J. Yang and *et al.* One-round semi-quantum-honest key agreement scheme in MSTSA structure without entanglement. *Quantum Information Processing*, 20:188, 2021.

[20] Y. G. Yang and *et al.* New quantum key agreement protocols based on Bell states. *Quantum Information Processing*, 18(10):322, 2019.

[21] J. Yin and *et al.* Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488(7410):185–188, 2012.