Quantum Information Processing (2021) 20:74
https://doi.org/10.1007/s11128-021-03004-4

COMMENT

A note on "new quantum key agreement protocols based on Bell states"

Zhengjun Cao[1] · **Olivier Markowitch**[2]

Received: 12 July 2020 / Accepted: 15 January 2021 / Published online: 19 February 2021

Abstract
We remark that the quantum key agreement protocol (Yang et al. in Quantum Inf Process 18(10):322, 2019) is flawed. It is unnecessary for Bob to prepare his secret key K_B, because it is finally announced and accessible to adversaries. We find, K_B has no relation to the confidentiality of the final agreed key $K_{AB} = K_A \oplus K_B$. It is just a key transfer scheme, not a general key agreement scheme. We also find there is short of a code for Bob to extract bits from the measured results.

Keywords Quantum cryptography · Key agreement · Key transfer · Bell state

1 Introduction

Very recently, Yang et al. [4] have presented a quantum key agreement protocol based on Bell states. It relies on that the intended receiver, Bob, cannot discriminate between the particles in Bell states and decoy particles. If two particles Bob measures with Bell basis are uncorrelated, the measurement result can be any of the four Bell states with equal probability.

Though the Yang et al.'s scheme is interesting, we find it is flawed. Since Bob's secret key K_B is finally announced and accessible to adversaries, K_B has no relation to the confidentiality of the final agreed key $K_{AB} = K_A \oplus K_B$. Naturally, it is just a key transfer scheme, not a general key agreement scheme. We also find it does not specify a code for Bob to extract bits from the measured results.

This comment refers to the article available online at https://doi.org/10.1007/s11128-019-2434-z.

✉ Zhengjun Cao
caozhj@shu.edu.cn

[1] Department of Mathematics, Shanghai University, Shangda Road 99, Shanghai 200444, China

[2] Computer Sciences Department, Université Libre de Bruxelles, Boulevard du Triomphe - CP 212, 1050 Bruxelle, Belgium

2 Review of the scheme

There are two entities, Alice and Bob, who randomly generate the secret keys K_A and K_B, respectively

$$K_A = \{k_1^A, k_2^A, \ldots, k_{2N}^A\},\ K_B = \{k_1^B, k_2^B, \cdots, k_{2N}^B\},$$

where $k_i^A, k_i^B \in \{0, 1\}$. The intended receiver, Bob, will measure the decoy particles with X or Z basis randomly, where

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Alice is responsible for generating the Bell states,

$$|\beta_{ij}\rangle = \frac{1}{\sqrt{2}}\left(|0\, j\rangle + (-1)^i |1\, \bar{j}\rangle\right),$$

where $i, j \in \{0, 1\}$, $\bar{j} = j \oplus 1$. The scheme can be described as follows.

1. Alice prepares the sequence S_A of N Bell states. For the i-th Bell state, where $i \in \{1, 2, \cdots, N\}$, she prepares it in the state

$$|\beta_{k_{2i-1}^A k_{2i}^A}\rangle = \frac{1}{\sqrt{2}}\left(|0 k_{2i}^A\rangle + (-1)^{k_{2i-1}^A} |1 \overline{k_{2i}^A}\rangle\right)$$

   and prepares $2N$ decoy particles each of which is randomly chosen from the four non-orthogonal states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. She inserts them into S_A randomly to obtain a new sequence S'_A. Send S'_A to Bob via the quantum channel.
2. Bob *announces* K_B to Alice via an *authenticated classical channel*.
3. Alice *tells* Bob the positions of decoy particles in the sequence S'_A, and computes the agreement key $K_{AB} = K_A \oplus K_B$.
4. Bob measures the corresponding decoy particles with X or Z basis randomly. Publish his measurement outcomes and the basis corresponding to the decoy particles.
5. Alice computes the error rate. If it exceeds the preset threshold, she abandons the process and restart.
6. Bob removes the decoy particles from the sequence S'_A to recover S_A. He then performs Bell-basis measurement on the N Bell states to recover K_A and obtain $K_{AB} = K_A \oplus K_B$.

3 Analysis

The Yang et al.'s scheme can be depicted as below (see Table 1). We now remark that the scheme has some shortcomings.

• *It is unnecessary for Bob to prepare his secret key* K_B. As we see, K_B is finally announced and accessible to the adversary. If it is not accessible to the adversary, there

Table 1 Yang et al.'s quantum key agreement scheme

Alice (K_A)		Bob (K_B)
Generate the sequence S_A, and		
insert decoy particles to obtain S'_A.	$\xrightarrow[\text{(quantum channel)}]{S'_A}$	
	$\xleftarrow[\text{(authenticated classical channel)}]{K_B}$	Announce K_B
Compute $K_{AB} = K_A \oplus K_B$	positions of decoy particles $\longrightarrow$	Measure the decoy particles with the X or Z basis
	measurement outcomes and basis $\longleftarrow$	Publish the measurement
Compute the error rate		outcomes and basis
If it exceeds the preset		
threshold, restart	OK $\longrightarrow$	Remove the decoy particles from S'_A to recover S_A
		Measure S_A to obtain K_A
		Compute $K_{AB} = K_A \oplus K_B$

Table 2 The code for basis and polarizations in BB84 protocol

Polarization		
Basis	Bit	
	0	1
+	↕	↔
×	↙	↘

must be a secure channel between Alice and Bob, which ensures the confidentiality of K_B. In this case, Alice can simply make use of the secure channel to transfer K_A.

• *It is not a general key agreement scheme*. We find that K_B has no relation to the confidentiality of the final agreed key $K_{AB} = K_A \oplus K_B$ because K_B is universally accessible. Actually, it is just a key transfer scheme, not a key agreement scheme. As for the differences between key transfer and key agreement, we refer to [3]. More precisely, we want to stress that the scheme is a quantum encryption [2], which can be directly used to encrypt the classical message K_A.

• *There is short of a code for Bob to extract bits from the measured results*. In the end, Bob has to measure the sequence S_A in order to extract the encoded key K_A. These measurements are not deterministic, otherwise the adversary can figure out K_A by man-in-middle attack. We want to stress that a classical signal state, s, can be uniquely represented as a bit, i.e., $s \rightarrow \{0, 1\}$. A quantum signal state qs, however, should be compounded with the measuring basis B so as to be represented as a bit, i.e., $(qs, B) \rightarrow \{0, 1\}$. The strength of BB84 [1] just comes from the bilingual code (Table 2), and that an unknown polarization cannot be deterministically measured by

Table 3 Prototype of Yang et al.'s quantum key agreement scheme

Alice (K_A)		Bob (K_B)
Generate the sequence S_A, and		
insert decoy particles to obtain S'_A	$\xrightarrow[\text{(quantum channel)}]{S'_A}$	
	$\xrightarrow{\text{positions of decoy particles}}$	Measure the decoy particles with the X or Z basis
Compute the error rate	$\xleftarrow[\text{and basis}]{\text{measurement outcomes}}$	Publish the measurement
If it exceeds the preset		outcomes and basis
threshold, restart	$\xrightarrow{\text{OK}}$	Remove the decoy particles from S'_A to recover S_A
		Measure S_A to obtain K_A
Compute	$\xleftarrow[\text{(authenticated classical channel)}]{K_B}$	Announce K_B, and compute
$K_{AB} = K_A \oplus K_B$		$K_{AB} = K_A \oplus K_B$

the adversary, even by the intended receiver, Bob. But the scheme has forgotten to specify such a code.

• *The phrase of authenticated classical channel is misunderstood*. In the classical cryptography, an authenticated channel can be used to authenticate either the transferred message or the identities of sender and receiver. To construct an authenticated channel, it is usual to make use of message authentication code (MAC) or public key encryption. But for a quantum cryptographic scheme, it always assumes that the current public key encryption based on mathematical intractability is insecure. Thus, one needs to use MAC to construct the authenticated classical channel in quantum key agreement schemes. This is a PARADOX, because MAC requires that the sender and receiver share a same password. Clearly, there does not exist such a shared password in the quantum key agreement scheme. That is to say, Alice and Bob need to use other methods, for instance, voice or video communication, to authenticate each other.

• *The claim that the security against passive attack from the outside eavesdropper is not sound*. It wrote:

> In the proposed protocol, Alice's key K_A is transmitted via the quantum channel while K_B is announced by Bob via the authenticated classical channel. If K_A is kept secret and K_B is generated independently, an outside attacker is unable to derive K_{AB} where the security is ensured by the one-time pad.

Apparently, it argues that the confidentiality of K_{AB} is ensured by the *one-time pad*. The claim is false, because K_B which is universally accessible cannot be viewed as one-time secret key.

In fact, the prototype of Yang et al.'s scheme can be depicted as below (see Table 3). The parameter, K_B, has no relation to the subsequent operations, such as Alice's computation of the error rate, Bob's measuring of the decoy particles and publishing

of the measurement outcomes and basis. It is only used to combine the key $K_{AB} = K_A \oplus K_B$. As we stressed before, the parameter K_B is public. So, the true confidentiality results from that whether Bob can remove the decoy particles from S'_A to recover the original sequence S_A, after Alice discloses the positions of decoy particles in S'_A.

4 Conclusion

We show that the Yang et al.'s quantum key agreement scheme is flawed, and some popular phrases in the classical cryptography have been unconcernedly used. We hope this note could correct some misunderstandings about such quantum key agreement schemes.

Acknowledgements We are grateful to the reviewers for their valuable suggestions.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Bennett, C., Brassard, G.: Quantum cryptography, public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984)
2. Liu, L., Cao, Z., Markowitch, O.: On the fundamental difference between encryption and key establishment. Int. J. Electron. Inf. Eng. **11**(2), 99–105 (2019)
3. Menezes, A., Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
4. Yang, Y., et al.: New quantum key agreement protocols based on Bell states. Quantum Inf. Process. **18**(10), 322 (2019)