Remarks on Some Quantum Cryptographic Schemes

Zhengjun Cao

Département d'informatique, Université Libre de Bruxelles. zhencao@ulb.ac.be

Abstract We remark that the schemes [PhysRevLett.98.020503, PhysRevA.74.012315, PhysRevA.71.022321, PhysRevA.72.012304, PhysRevA.69.052307, PhysRevA.59.1829] are not secret sharing schemes as claimed.

Keywords. quantum key establishment, quantum secret sharing, BB84 scheme

1 Introduction

Key establishment is a process whereby a shared secret becomes available to two or more parties. The idea of secret sharing is to start with a secret, and divide it into pieces called shares which are distributed amongst users such that the pooled shares of specific subsets of users allow reconstruction of the original secret. In this note, we remark that the schemes [PhysRevLett.98.020503, PhysRevA.74.012315, PhysRevA.71.022321, PhysRevA.72.012304, PhysRevA.69.052307, PhysRevA.59.1829] are key establishment schemes instead of secret sharing schemes as claimed. In fact, these key establishment models are somewhat different from that of BB84 [1].

2 Differences between key establishment and secret sharing

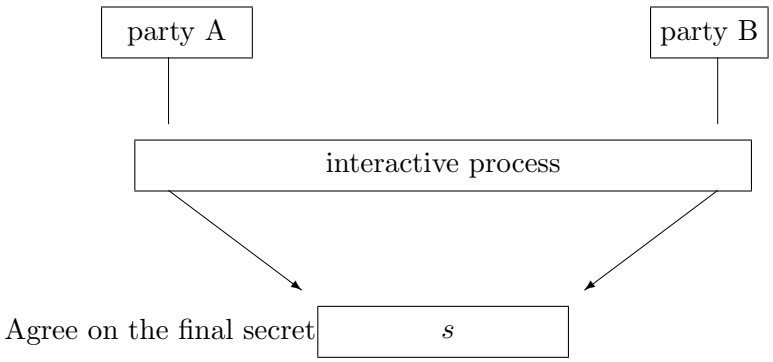
2.1 Key establishment

In classical scenario, the terms key establishment, key distribution, key exchange and key agreement are confusably used. Roughly speaking, all of them indicate that users establish a fresh secret key. But we should point out that these terms are different strictly from the term, secret sharing.

Key establishment [7] is a process whereby a shared secret becomes available to two or more parties, for subsequent cryptographic use. Key establishment may be broadly subdivided into key transport and key agreement. A key transport protocol is a key establishment technique where one party creates or otherwise obtains a secret value, and securely transfers it to the other(s). A key agreement protocol is a key establishment technique in which a shared secret

is derived by two (or more) parties as a function of information contributed by, or associated with, each of these, such that no party can predetermine the resulting value.

G1: a general model for key establishment



In quantum scenario, the term quantum key establishment is seldom mentioned. In contrast, the term quantum key distribution (QKD) is popular with researchers because of the BB84 protocol [1]. The purpose of the QKD system is to use the two channels and a small portion of the already shared key to generate new key portion, larger than the one just used. The initial key only needs to be large enough to allow for the first generation sequence, typically authenticating two messages, one from Alice to Bob and one in the other direction. This will enable the key to grow somewhat, and will allow for further runs, in which the key will grow even more. In general, a QKD scheme consists of the following:

1) Raw key generation: Use the quantum channel to transmit a bit sequence, shared between Alice and Bob but equal only in a portion of the positions.

2) Sifting: Remove most of the bits that do not match by comparing parameters of each use of the quantum channel. A smaller "sifted" key is obtained which is equal for Alice and Bob in a considerably larger portion.

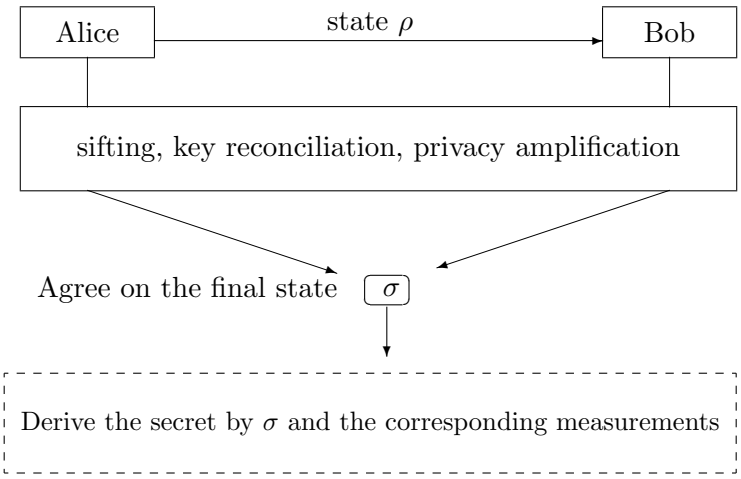
3) Key reconciliation: Perform error correction on the sifted key and estimate the error rate to detect whether Eve was listening on the quantum channel, either with a few sacrificed bits from the sifted key. If the error rate is above a predetermined bound, Alice and Bob conclude that Eve has been listening and the round must be aborted.

4) Privacy amplification: If the noise is lower than the predetermined bound, Eve may still have been listening but in that case she has opted to only extract very little information. In this case, Alice and Bob can perform "privacy amplification" to lower Eve's information even further, sacrificing a few bits of their candidate key in the process.

5) Authentication: The step is to authenticate the messages sent from Alice to Bob and from Bob to Alice on the classical channel, to make sure Eve has not modified these messages.

The QKD model can be graphically illustrated as following.

G2: QKD model



We should point out that:

1. A quantum state does not naturally imply a secret key. For instance, the superposition $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ can be interpreted as either bit 0 or bit 1, if it is measured with respect to the classical base $\{|0\rangle, |1\rangle\}$.

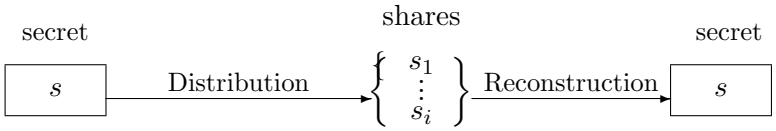
2. Although the QKD model contains the process of quantum state distribution and the process of quantum state reconstruction, the reconstructed state is not identical to the original state because of sifting.

3. The final secret key is fresh because of the privacy amplification.

2.2 Secret sharing

A secret sharing scheme is related to key establishment. The original motivation for secret sharing was the following. To safeguard cryptographic keys from loss, it is desirable to create backup copies. The greater the number of copies made, the greater the risk of security exposure; the smaller the number, the greater the risk that all are lost. The idea of secret sharing is to start with a secret, and divide it into pieces called shares which are distributed amongst users such that the pooled shares of specific subsets of users allow reconstruction of the original secret.

G3: The model for secret sharing



Remark 1 Notice that the difference between a secret sharing scheme and a key establishment scheme is that whether there is an original secret key which has to be reconstructed.

Remark 2 Intuitively, designing a secret sharing scheme is more difficult than designing a key establishment scheme. As for this point, we refer to Shamir's secret sharing [8] and Diffie-Hellman key exchange/agreement [2].

3 Some quantum cryptographic schemes are not secret sharing as claimed

In 2007, S. Gaertner et al [PhysRevLett.98.020503] claimed that they have presented the first experimental demonstration of four-party quantum secret sharing via four-photon entanglement. The GKBW scheme [4] involves the state distribution and state reconstruction processes. But the resulting secret key is fresh. There is no an original key which has to be reconstructed. That is to say, the scheme is not a secret sharing scheme as it claimed. Naturally, it is a key establishment. Precisely speaking, it is a variation of BB84 scheme. The party A consists of any user from the four users. The party B consists of the other three users. Likewise, the schemes [PhysRevA.74.012315, PhysRevA.71.022321, PhysRevA.72.012304, PhysRevA.69.052307, PhysRevA.59.1829] are not secret sharing schemes as claimed. They are key establishment schemes. To clarify this point, we investigate the protocol [PhysRevLett.98.020503].

The scheme works as follows. Alice, Bob, Claire, and David share each a photon from the following four-photon polarization-entangled state [10]

$$|\Psi\rangle = \frac{1}{2\sqrt{3}}[2|HHVV\rangle - |HVHV\rangle - |HVVH\rangle - |VHHV\rangle - |VHVH\rangle + 2|VVHH\rangle]_{abcd}$$

where H and V denotes horizontal and vertical polarization of photons in the four spatial modes a, b, c, and d. In the following, we assume that Alice is the dealer. Each party chooses randomly between two complementary measurement bases. To transfer the measurement results into a key sequence, each participant identifies his result either with a bit value of 0 or 1. The measurements will be repeated until they have established a raw key of desired length. For key sifting, each participant announces publicly whenever he has registered a photon and which measurement basis he has used, but not the results. After key sifting, all participants have to

check for external eavesdropping. To finally obtain a common secure key, they have to perform key reconciliation and privacy amplification.

Comparing the GKBW scheme with BB84, we find the scheme is indeed a variation of BB84. In the variation, the party A consists of Alice. The party B consists of Bob, Claire, and David. The involved state is four-photon entanglement. Obviously, the resulting secret key is fresh.

In the following Table 1, we list some variations of BB84. It will be helpful to clarify the difference between key establishment and secret sharing.

Table 1: key establishment models different from BB84

scheme	party A	party B	involved quantum state
PhysRevA.59.1829	Alice	Bob, Charlie	3-GHZ
PhysRevA.69.052307	Alice	$n-1$ participants	n-GHZ
PhysRevA.71.022321	Alice	Bob, Charlie	qutrit
PhysRevA.72.012304	m members	n members	qubit
PhysRevA.74.012315	Alice	Bob, Charlie	high-dimensional entanglement
PhysRevLett.98.020503	Alice	Bob, Charlie, David	four-photon entanglement

4 Conclusion

In this note, we clarify that some quantum cryptographic schemes are not secret sharing as claimed. We also point out that they are indeed some variations of BB84.

References

[1] C. Bennet, G. Brassard; Quantum Cryptography: Public key distribution and coin tossing, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore India, December, pp. 175-179 (1984)

[2] W. Diffie, M. E. Hellman; New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, pp. 644-654 (1976)

[3] D. Greenberger, M. Horne, A. Zeilinger; in Bell's Theorem, Quantum Theory, and Conceptions of Universe, edited by M. Kaftos (Kluwer Academic, Dordrecht,1989); D. Greenberger, M. Horne, A. Shimony, A. Zeilinger; Am. J. Phys. 58, 1131 (1990)

[4] S. Gaertner, C. Kurtsiefer, M. Bourennane, H. Weinfurter; Experimental Demonstration of Four-Party Quantum Secret Sharing, PhysRevLett.98.020503 (2007)

[5] M. Hillery, V. Bužek, A. Berthiaume; Quantum secret sharing, PhysRevA.59.1829 (1999)

[6] LY Hsu, CM Li; Quantum secret sharing using product states, PhysRevA.71.022321 (2005)

[7] A. Menezes, P. Oorschot, S. Vanstone; Handbook of applied cryptography, pp.490-527 (1996)

[8] A. Shamir; How to share a secret; Comm. ACM, 22 (11), pp. 612-613 (1979)

[9] H. Takesue, K. Inoue; Quantum secret sharing based on modulated high-dimensional time-bin entanglement, PhysRevA.74.012315 (2006)

[10] H. Weinfurter, M. Zukowski; Four-photon entanglement from down-conversion, PhysRevA.64.010102 (2001)

[11] L. Xiao, GL Long, FG Deng, JW Pan; Efficient multiparty quantum-secret-sharing schemes, PhysRevA.69.052307 (2004)

[12] FL Yan, T. Gao; Quantum secret sharing between multiparty and multiparty without entanglement, PhysRevA.72.012304 (2005)