Cryptanalysis of efficient multiparty quantum secret sharing based on a novel structure and single qubits

Xiao-Qiu Cai  
Luoyang Normal University

Zi-Fan Liu  
Luoyang Normal University

Shuang Li  
Luoyang Normal University

Tian-Yin Wang  
wangtianyin79@163.com

Luoyang Normal University

Research Article

Keywords: quantum cryptography, quantum secret sharing, collusion attack

Posted Date: December 6th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3692842/v1

License: Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.
Cryptanalysis of efficient multiparty quantum secret sharing based on a novel structure and single qubits

Xiao-qiu Cai¹, Zi-fan Liu¹,², Shuang Li¹,² and Tian-yin Wang¹,²*

¹Correspondence: wangtianyin79@163.com
²School of Mathematical Science, Luoyang Normal University, Luoyang, China
Full list of author information is available at the end of the article

Abstract
Quantum secret sharing is a basic quantum cryptographic primitive, which has a lot of applications in information security and privacy preservation. An efficient multiparty quantum secret sharing protocol [EPJ Quantum Technology 2023 10: 29] based on a novel structure and single qubits was reported recently. In this paper, we give a cryptanalysis of this protocol and show that it cannot satisfy the security requirement for secret sharing because an unauthorized set of agents can gain access to some information on the dealer’s secret by a special collusion attack. Furthermore, we put forward an effective way to deal with the security problem.

Keywords: quantum cryptography; quantum secret sharing; collusion attack

1 Introduction
In 1979, Shamir [1] and Blakely [2] independently introduced the concept of \((k, n)\) threshold secret sharing scheme respectively, which allowed a secret \(s\) to be split into \(n\) shares such that \(s\) can be easily reconstructed from any \(k\) shares, but less than \(k\) shares can reveal no information on the secret \(s\). Owing to the special property, secret sharing was used to construct robust key management, secure multiparty computation or other cryptographic schemes that can function securely and reliably even when misfortunes destroy most of the shares and security breaches expose all but one of the remaining shares [3, 4, 5].

In the last decades, the principles of quantum mechanics supplied many interesting cryptographic applications such as quantum key distribution, quantum secure direct communication (QSDC), quantum digital signature, and quantum secret sharing (QSS) [6, 7]. In contrast to classical secret sharing, the security of QSS is based on the fundamental principles of quantum mechanics rather than mathematical difficult problems, which makes it secure against any opponent even if he/she has infinite computing resources. On account of the security advantage, QSS has attracted much attention and many proposals have been reported both in theoretical and experimental aspects [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] since the first proposal with Greenberger-Horne-Zeilinger state was given by Hillery et al [19].

Cryptographic design and cryptanalysis are two inherent directions, which are opposite to but stimulate each other. Both of them are indispensable to the development of cryptography. This is also the case for quantum cryptography. Nevertheless,
it is very complicated to analyze the security of QSS because multiple participants are involved and some may be not honest [20, 21, 22].

In order to achieve an excellent balance between security and performance, an efficient multiparty QSS protocol based on a novel structure and single qubits (named KTYC-protocol hereafter) was reported recently [23], which excluded some deficiency of traditional loop QSS schemes because each agent can interact with the dealer independently by an independent secure communication tunnel based on QSDC. In this paper, we analyze the security of KTYC-protocol and give a new collision attack, whereby an unauthorized set of agents can get some information on the dealer’s secret. Furthermore, the proportion that the unauthorized set can extract information on the secret will be close to 1 with the increase of the agents’ number in the unauthorized set. Finally, we propose a possible way to improve the KTYC-protocol’s security.

2 The KTYC-protocol
In this section, let us give a brief description of KTYC-protocol. Assume that the dealer Alice has a secret $s$ whose length is $S$, and she wants the secret $s$ to be shared among $N$ agents: $P_1, P_2, \ldots, P_N$. This protocol can be described as follows [23].

Step 1. Every agent $P_i$ ($i = 1, 2, \ldots, N$) prepares $t$ qubits $\otimes_{j=1}^{t} |\varphi_{ij}\rangle$, and each qubit $|\varphi_{ij}\rangle$ is randomly chosen from the set \{\(0\), \(1\), \(+\), \(\)\} for $i = 1, 2, \ldots, N$ and $j = 1, 2, \ldots, t$, where $t = \lceil \frac{S}{N} \rceil$, 
\(+\) = \(\frac{1}{\sqrt{2}} (0 + 1)\), 
\(-\) = \(\frac{1}{\sqrt{2}} (0 - 1)\), and \(\otimes\) denotes the direct product of qubits. Then they send their respective quantum sequences to Alice after inserting several decoy qubits [24, 25].

Step 2. When receiving the quantum sequences, Alice checks the channel by the decoy qubits. Specifically, Alice randomly chooses sufficient qubits and requires all the agents to publish the basis and states of these qubits. Then she uses the same basis to measure and compare the results. If the error rate is higher than the threshold, she requests that the sequence be resent until it passes the channel checking.

Step 3. Alice joins these sequences together and reorders qubits. Then she encodes the secret $s$ into the sequence by using $I$ and $Y$ operations according to her message “0” and “1”, respectively, and divides it into $N$ sequences, where $I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $Y = |1\rangle\langle 0| - |0\rangle\langle 1| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Subsequently, she sends these sequences back to all agents after inserting decoy qubits [24, 25].

Step 4. After all agents have received the sequences, Alice publishes the positions and states of the decoy qubits. All agents check the channel with these decoy qubits inserted by Alice. If the error rate is lower than the threshold, Alice publishes the order of the qubits; otherwise, the communication is terminated and restarted via a different channel.

Step 5. All agents cooperate to recover the secret $s$ by exchanging their information on original quantum states.

3 The cryptanalysis of KTYC-protocol
As we know, the security of QSS requires that just an authorized set of agents can recover the secret $s$ distributed by the dealer, but any unauthorized set of agents
can learn no information on it [19, 20, 21, 22]. However, here we show that an unauthorized set can gain access to some information on the secret $s$ in the KTYC-protocol. Furthermore, the information on the secret $s$ that an unauthorized set can obtain will increase in proportion to the number’s square of agents in the unauthorized set. The detailed analysis is given as follows.

From Section 2, it can be seen that the KTYC-protocol is a $(N, N)$ threshold QSS protocol in fact. Therefore, there is only one authorized set of agents, i.e., \{P_1, P_2, \ldots, P_N\}, who can recover the secret $s$ if all the $N$ agents cooperate with each other in Step 5. As mentioned in [23], in contrast to the traditional loop QSS schemes based on QSDC, the KTYC-protocol is based on a new structure that each agent can communicate with the dealer by an independent quantum secure direct communication path. This design makes all the $N$ agents adopt the same privileges in this protocol, but it also gives a good chance for dishonest agents to gain access to the information on the secret $s$, which can be shown in Theorem 1.

**Theorem 1.** An unauthorized set can gain access to about $\frac{d^2}{N}$ bits of the dealer’s secret $s$ if they collude with each other in the KTYC-protocol, where $d$ ($d < N$) is the number of agents in the unauthorized set.

Proof. In Step 3, when the dealer Alice receives all the $N$ agents’ quantum sequences $\otimes_{j=1}^t |\varphi\rangle_j^1$, $\otimes_{j=1}^t |\varphi\rangle_j^2$, \ldots, $\otimes_{j=1}^t |\varphi\rangle_j^N$, she joins them together and encodes the secret $s$ into the quantum sequence. Then she divides it into $N$ sequences and sends these sequences back to $N$ agents. Clearly, each agent will receive a quantum sequence including $t$ qubits from Alice, of which about $\frac{t}{N}$ qubits are prepared by himself/herself in Step 1 according to the principles of probability. For these qubits, when Alice publishes the order of the qubits in Step 4, the agent can choose the right basis to measure them and then deduce Alice’s encoding operations because he/she knows their initial states. Therefore, any agent can gain access to about $\frac{t}{N}$ bits of the secret $s$, which means that Theorem 1 holds for $d = 1$.

For $d = 2$, i.e., there are two agents in the unauthorized set. In this case, each of them will receive a quantum sequence including $t$ qubits from Alice, of which about $\frac{2}{N}$ qubits are prepared by themself in Step 1 according to the principles of probability. Therefore, they can gain access to about

$$\frac{2t}{N} + \frac{2t}{N} = \frac{4t}{N} = \frac{2^2t}{N}$$

bits of the secret $s$.

For $d = 3$, i.e., there are three agents in the unauthorized set. In this case, each of them will receive a quantum sequence including $t$ qubits from Alice, of which about $\frac{3}{N}$ qubits are prepared by themself in Step 1 according to the principles of
probability. Therefore, they can gain access to about 
\[
\frac{3t}{N} + \frac{3t}{N} + \frac{3t}{N} = \frac{9t}{N} = \frac{3^2t}{N}
\]
bits of the secret \(s\).

For \(d = 4\) to \(N - 1\), it can be gotten that the unauthorized set can gain access to about \(\frac{d^2t}{N}\) bits of the secret \(s\) by simple analysis.

In conclusion, when there are \(d\) (\(d < N\)) agents in the unauthorized set, they can gain access to about \(\frac{d^2t}{N}\) bits of the secret \(s\). The proof of Theorem 1 is completed.

\[\text{Figure 1} \quad \text{The relation between the number (d) of agents in an unauthorized set and the bits (}\frac{d^2t}{N}\text{) of the secret } s \text{ they can get. Here } N = 10, t = 7 \text{ and } S = 70.\]

From Theorem 1, it can be seen that the information on the secret \(s\) that an unauthorized set can obtain will increase in proportion to the number’s square of agents in the unauthorized set, which is shown in Fig. 1. Furthermore, the proportion \(\frac{d^2t}{N}\) that the unauthorized set can extract information on the secret \(s\) is close to 1 with the increase of the agents’ number in the unauthorized set, which is shown in Fig. 2.

So far, we have given a cryptanalysis of the KTYC-protocol, which shows that this protocol is not secure in the sense that it does not satisfy the security requirement for QSS.
Figure 2 The relation between the number \((d)\) of agents in an unauthorized set and the proportion \((\frac{d^2}{N^2})\) that they can extract information on the secret \(s\). Here \(N = 10\), \(t = 7\) and \(S = 70\).

4 Suggestion for improvement

From Section 3, it can be seen that the success of the proposed collusion attack is for that the KTYC-protocol is based on a novel structure, which makes other agents have no effect on the dealer’s secret bits if the encoded qubits are not prepared by themselves. Therefore, in order to deal with the security leak, every agent must hold a share on each bit of the dealer’s secret \(s\), which can be realized in two ways. One is that every agent perform an encryption on each encoded qubit, but this will change the structure of the KTYC-protocol. The other way is that the dealer preprocesses the secret \(s\) to be shared in advance. Specifically, in Step 3, the dealer randomly prepares \(N\) random numbers \(s_1, s_2, \ldots, s_N\), where

\[
s_1 + s_2 + \cdots + s_N = s. \tag{3}
\]

Then the dealer encodes \(s_1, s_2, \ldots, s_N\) into the qubit sequences \(\otimes_{j=1}^{t-1} |\psi\rangle_j^1\), \(\otimes_{j=1}^{t} |\psi\rangle_j^2\), \(\ldots, \otimes_{j=1}^{t} |\psi\rangle_j^{N}\), respectively. After that, the dealer performs the same actions as that in Step 3 except that the encoding operations are not performed any longer.

It is evident that all \(N\) agents have equally influence on each bit of the dealer’s secret \(s\), which means \(s\) can be easily reconstructed by the only authorized set \(\{P_1, P_2, \ldots, P_N\}\), but any unauthorized set can reveal no information on the secret \(s\) in the improved version.

5 Conclusion

To sum up, we give a cryptanalysis of the KTYC-protocol and present a collusion attack. Using this attack, an unauthorized set of agents can gain access to some information on the dealer’s secret. Furthermore, the information on the dealer’s
secret that the unauthorized set can obtain increases in proportion to the number’s square of agents, and the proportion that the unauthorized set can extract information on the dealer’s secret is close to 1 with the increase of the agents’ number in the unauthorized set. Finally, we analyze the reason for the security leak and propose an effective way to improve the KTYC-protocol’s security. We hope this work shed some light on the development of QSS.

**Abbreviations**

QSS, Quantum Secret Sharing; QSDC, quantum secure direct communication.

**Acknowledgements**

**Declarations**

**Ethical Approval and Consent to participate**

Not applicable.

**Consent for publication**

Not applicable.

**Availability of supporting data**

Not applicable.

**Competing interests**

The authors declare that they have no competing interests.

**Funding**

This work was supported by the National Natural Science Foundation of China (Grant Nos. 62272208, 62172196, 61902166), and the Natural Science Foundation of Henan Province, China (Grant No. 212300410062).

**Authors’ contributions**

X.Q. Cai gave the cryptanalysis, Z.F. Liu proposed the way to deal the security problem, X.Q. Cai and T.Y. Wang wrote the main manuscript text, and S. Li prepared figure 1 and figure 2. All authors reviewed the manuscript.

**Author details**

1. School of Mathematical Science, Luoyang Normal University, Luoyang, China.
2. School of Mathematics and Information Science, Henan Normal University, Xinxiang, China.

**References**