The Journal of Systems and Software 83 (2010) 1801–1804

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Multi-party covert communication with steganography and quantum secret sharing

Xin Liao [a,*], Qiao-yan Wen [a], Ying Sun [a], Jie Zhang [b]

[a] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China

ARTICLE INFO

Article history:
Received 19 January 2010
Received in revised form 21 April 2010
Accepted 24 April 2010
Available online 15 June 2010

Keywords:
Multi-party covert communication
Steganography
Quantum secret sharing

ABSTRACT

In this paper, we address the "multi-party covert communication", a stronger notion of security than standard secure multi-party communication. Multi-party covert communication guarantees that the process of it cannot be observed. We propose a scheme for steganographic communication based on a channel hidden within quantum secret sharing (QSS). According to our knowledge nobody has ever raised the scheme, providing us the motivation for this work. To an outside observer, participants will engage in a typical instance of QSS, just like the others. But when the session is over, covert multi-party communication has already been done. Further analysis shows that the amount of hidden information one can acquire is 0, even if either an outside observer guesses the covert communication is carrying on or a dishonest participant is eavesdropping.

1. Motivation

Suppose Alice, the leader of two spies, wants to assign an important and secret mission to two spies, Bob and Charlie. Instead of assigning the whole mission to any individual, Alice has better to distribute the mission in such a way that no one alone has access to it, while Bob and Charlie can reconstruct it cooperatively. All of them want to conceal the communication, and the presence of the mission goes unnoticed by others. How can they carry out such a communication?

We call the above simple scenario "the spies' problem". In fact, it is a special case of multi-party covert communication (MCC), which is required to meet the following challenges:

- *Cooperativity*: secrets are distributed among a group of participants, each allocated a share of secrets. Secrets can only be reconstructed under the circumstances that all the shares are combined together, and each participant barely knows his own part.
- *Covertness*: MCC would have good visual/statistical imperceptibility, and the presence has to be unnoticed by an outside observer.
- *Security*: an attacker should acquire hidden information as little as possible, even if he guesses the covert communication is underway.
- *Scalability*: many participants in different places can covertly complete this communication, and the computational complexity does not increase obviously after adding one into the original.

Steganography is primarily concerned for military or commercial utilization and presents less risk because the existence of secret data is concealed (Petitcolas et al., 1999; Wang and Wang, 2004). The primary contribution of this paper is to introduce a new application of steganograhy, and to show a way realizing MCC. The idea of using steganography and quantum secret sharing in multi-party covert communication in this paper is recommendable.

Can multi-party covert communication be achieved by trivial composition of classical secret sharing with steganography?

No. One steganographically encodes all messages of classical secret sharing, leading to a scheme in which no outside observer can determine whether it is running. But all classical cryptosystems except for one-time pad are based on computational complexity assumptions, and the security is conditional (Vernam, 1926; Shannon, 1949). If an attacker guesses the covert communication is underway, and the threat of computing power to classical cryptosystems increases gradually, the amount of acquired hidden information will not be negligible anymore. Furthermore, how to determine whether an eavesdropper is active during the communication is another problem. Recent advances in steganalysis have also made conventional steganography much more detectable (Ker, 2005; Pevnu and Fridrich, 2005; Goljan et al., 2006; Ker, 2007).

The representation of classical information by quantum states is ideally suited for solving these above problems. Quantum states cannot be copied, and any attempt to obtain information from

* Corresponding author.
E-mail address: liaoxinbupt@gmail.com (X. Liao).

0164-1212/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2010.04.076

the original source always results in a detectable disturbance, so participants can establish evidence that an eavesdropper is active, i.e., they can detect an eavesdropper's presence. Recently, Martin (2007a,b), Martin presented an interesting perspective for steganographic communication with quantum key distribution (Bennett and Brassard, 1984; Bennett et al., 1992). The amount of acquired hidden information is very small even if an attacker guesses the covert communication is taking place. In this paper we propose a multi-party covert communication scheme by elegantly integrating steganography into quantum secret sharing (QSS) (Karlsson et al., 1999; Hillery et al., 1999; Guo and Guo, 2003; Yang and Wen, 2008; Hao et al., 2010). Since only a few modifications are made to the original QSS scheme, the taking place of covert communication cannot be observed. The cover object of our scheme is a current QSS rather than digital media such as images, audio and video, so it is secure against the current detection attack. Further analysis shows that the amount of hidden information one can acquire is 0, even if either an outside observer guesses the covert communication is underway or a dishonest participant eavesdrops.

The remainder of this paper is organized as follows. In Section 2, quantum information (Nielsen and Chuang, 2000; Xu et al., 2009; Wang and Song, 2009) and Guo et al.'s QSS scheme (Guo and Guo, 2003) are introduced along with their interesting features. In Section 3, we propose a multi-party covert communication scheme, where it takes full advantage of two different mechanisms: steganography and QSS, then analyze its security. Conclusions are drawn in the last section.

2. Preliminaries

2.1. Quantum information

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept: the quantum bit (qubit for short). Just like a classical bit has a state (either 0 or 1), a qubit also has a state. Two possible states for a qubit are $|0\rangle$ and $|1\rangle$, which correspond to the states 0 and 1 for a classical bit. A qubit can exist in a continuum of state between $|0\rangle$ and $|1\rangle$ until it is measured, such as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

where α and β are two complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$.

When a qubit is measured with a orthogonal basis, it only gives "0" or "1" as the measurement result. An observer can specify what they want to measure by specifying a basis. Two examples of basis are: the computation basis $Z = \{|0\rangle, |1\rangle\}$ and the Hadamard rotated basis $X = \{|+\rangle, |-\rangle\}$. They are the only bases we care about in this paper. $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ and $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$ correspond to the states 0 and 1 for a classical bit.

When we measure a state described by the qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the Z basis, we get either the result $|0\rangle$, with probability $|\alpha|^2$, or the result $|1\rangle$, with probability $|\beta|^2$. Table 1 summarizes the measurement results of the states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ in the Z basis and X basis, respectively. Throughout the paper, capital letters denote qubits and lowercase letters denote classical bits. $\oplus$ represents the XOR operation.

2.2. Literature review

In this subsection, we briefly describe Guo et al.'s QSS scheme, consisting of the following steps:

(1) Alice generates two random $2n$-bit strings $l = (l_1, l_2, \cdots, l_{2n})$ and $a = (a_1, a_2, \cdots, a_{2n})$. For each bit of l and a, she creates qubits B_i and C_i in the Z basis (if $l_i = 0$) or X basis (if $l_i = 1$), where $b_i \oplus c_i = a_i$. Table 2 summarizes the coding qubits in the corresponding basis. For example, if $l_i = 1$ and $a_i = 0$, Alice prepares either $B_i = C_i = |+\rangle$ ($b_i = c_i = 0$) or $B_i = C_i = |-\rangle$ ($b_i = c_i = 1$) each with probability 1/2. But she knows exactly which pair of qubits she prepares. She sends $2n$-qubit strings $B = (B_1, B_2, \cdots, B_{2n})$ and $C = (C_1, C_2, \cdots, C_{2n})$ to Bob and Charlie, respectively.
(2) When both Bob and Charlie announce that they have received their strings, Alice announces l. Bob and Charlie measure each qubit in the Z basis or X basis according to the corresponding bit value of l.
(3) Alice randomly selects n check bits in a. Bob and Charlie are required to announce the measurement results of their corresponding check qubits in B and C.
(4) If Alice finds the number of agreed values is unacceptably few, she aborts this run and restarts from step 1. Otherwise, she continues to the next step.
(5) They perform information reconciliation and privacy amplification to generate three m-bit keys k_a, k_b and k_c from the remaining n bits. Alice, Bob and Charlie can obtain k_a, k_b and k_c separately, where $k_a = k_b \oplus k_c$.

Table 1
The measurement results of the states in the different basis.

States	Z Basis	X Basis
$\|0\rangle$	0	0 with probability 1/2, 1 with probability 1/2
$\|1\rangle$	1	0 with probability 1/2, 1 with probability 1/2
$\|+\rangle$	0 with probability 1/2, 1 with probability 1/2	0
$\|-\rangle$	0 with probability 1/2, 1 with probability 1/2	1

3. Our proposed scheme

3.1. A novel multi-party covert communication scheme

In this subsection, we present a novel multi-party covert communication scheme by elegantly integrating steganography into Guo et al.'s QSS. Every run except the first could covertly multi-party communicate 1-bit secret. Before the covert communication takes place, they agree on two integers d ($1 \le d \le n$) and $r \in \{0, 1\}$ in advance. They don't covertly communicate secret bits in the first run. In the j-th ($j \ge 2$) run, Alice uses m-bit key $k_a = (k_0, k_1, \cdots, k_{m-1})$ ($k_i \in \{0,1\}$) generated in the previous run to update d and r:

$$r = k_{m-1} \tag{2}$$

$$d = \left(\sum_{i=0}^{m-2} k_i \times 2^i \bmod n\right) + 1 \tag{3}$$

We make a few modifications to Guo et al.'s QSS, so an outside observer cannot be aware of the happening of covert communication.

Table 2
The coding qubits in the corresponding basis.

l	0		1	
a	0	1	0	1
bc	00 11	01 10	00 11	10 01
BC	$\|0\rangle\|0\rangle$ $\|1\rangle\|1\rangle$	$\|0\rangle\|1\rangle$ $\|1\rangle\|0\rangle$	$\|+\rangle\|+\rangle$ $\|-\rangle\|-\rangle$	$\|-\rangle\|+\rangle$ $\|+\rangle\|-\rangle$