Information Sciences 000 (2018) 1–12

Contents lists available at ScienceDirect

Information Sciences

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

Game theoretic security of quantum bit commitment

Lu Zhou[a], Xin Sun[b,*], Chunhua Su[a], Zhe Liu[c], Kim-Kwang Raymond Choo[d]

[a] Division of Computer Science, University of Aizu, Japan
[b] Institute of Logic and Cognition, Sun Yat-sen University, China
[c] Nanjing University of Aeronautics and Astronautics, China
[d] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA

ARTICLE INFO

Article history:
Received 16 August 2017
Revised 3 March 2018
Accepted 18 March 2018
Available online xxx

Keywords:
Quantum bit commitment
Game theoretic security
Commitment game
Categorical quantum mechanics

ABSTRACT

Due to the threat posed by quantum computing, there has been an increasingly focus on designing secure and efficient quantum-based and post-quantum cryptographic protocols. In this paper, we study and propose a quantum bit commitment (QBC) protocol inspired by the framework of categorical quantum mechanics. We show that our protocol is more secure and simpler than most existing cheat-sensitive QBC protocols. Then, we introduce the notion of game theoretic security, and demonstrate that such a notion is less demanding than unconditional security, yet stricter than cheat-sensitive. We show that our protocol is game theoretic secure for many commitment games. Being game theoretic secure opens the door of applying our protocol to game theory. Specifically, we show that our protocol can be used to implement equilibrium in commitment games. Finally, we run experiments on the IBM quantum computer to demonstrate the practicability of our protocol.

1. Introduction

Bit commitment, used in a wide range of cryptographic protocols (e.g. zero-knowledge proof, multiparty secure computation, and oblivious transfer), consists of two phases, namely: commit and opening. In the commit phase, the sender Alice chooses a bit $b \in \{0, 1\}$, which she wishes to commit to the receiver Bob, and thus presents Bob some evidence about b. The committed bit cannot be known by Bob prior to the opening phase. Later, in the opening phase, Alice announces some information for reconstructing b. Bob then reconstructs a bit b' using Alice's evidence and announcement. Generally, bit commitment is required to satisfy the following properties:

1. Correctness: It should always be that $b' = b$ if both Alice and Bob execute the protocol honestly.
2. Concealing: Before the opening phase, Bob cannot know the committed bit.
3. Binding: After the commit phase, Alice cannot change the committed bit.

1.1. Related works and challenging issues

The first quantum bit commitment (QBC) protocol is proposed by Bennett and Brassard in 1984 [4]. A QBC protocol is unconditionally secure if any cheating can be detected with a probability arbitrarily close to 1. Here, Alice's cheating means that she changes the committed bit after the commit phase, while Bob's cheating means that he learns the committed bit

* Corresponding author at: Department of Philosophy, No. 135, Xigangxi Road, Guangzhou, 510275, China.
E-mail address: xin.sun.logic@gmail.com (X. Sun).

https://doi.org/10.1016/j.ins.2018.03.046
0020-0255/

before the opening phase. A number of QBC protocols have been designed to achieve unconditional security, such as those of Brassard and Crépeau [5] and Brassard et al. [6]. However, according to the Mayers-Lo-Chau (MLC) no-go theorem [19,20], unconditionally secure QBC can never be achieved in principle.

Although unconditionaly secure QBC is impossible, several QBC protocols, which satisfy some other notions of security, have been proposed, such as cheat sensitive quantum bit commitment (CSQBC) protocols [7,13,17,21] and relativistic QBC protocols [1,16]. In CSQBC protocols, the probability for detecting cheating is merely required to be non-zero. With this less stringent security requirement, many insecure QBC protocols can be regarded as secure CSQBC protocols. Indeed, cheat-sensitive is a rather weak notion of security such that many CSQBC protocols are still not very useful.

While unconditional security is impossible and cheat sensitive is too weak, game theoretic security appears as an alternative notion of security. Game theoretic security, formulated by Halpern and Teague [12], have been applied in the study of cryptographic protocols [2,11,15]. The game theoretic security of classic bit commitment protocols, for example, has been explored by Higo et al. [15]. They constructed a game from a bit commitment protocol to determine whether the protocol is game theoretic secure when Nash equilibrium is played.

1.2. Our contributions and organization of this paper

The contribution of this paper is both technical and conceptual. On the technical side, we propose a protocol which is more secure and simpler than all existing CSQBC protocols [7,13,17,21] that we are aware of. Moreover, only Bell state entanglement is used in our protocol, which makes our protocol implementable by the current technology.

On the conceptual side, we propose game theoretic security for quantum bit commitment, which is a security notion between unconditional security and cheat sensitive. While Nash equilibrium plays a central role in Higo et al.'s notion of game theoretic security [15], we use *strong Stackelberg equilibrium* to characterize game theoretic security.

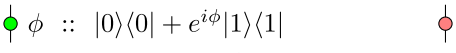
Unlike Nash equilibrium (i.e. a solution concept for games where players make their moves simultaneously), Stackelberg equilibrium is a solution concept for games with sequential moves. A typically simple game with sequential moves is the commitment game [10], which is also known as a leader-follower game. In a commitment game, the leader moves first by playing a pure or mixed strategy, then the follower plays a pure strategy. A Stackelberg equilibrium of a commitment game is a pair of pure strategies such that no player can unilaterally benefit by deviating from his/her strategy to other pure strategies. A strong Stackelberg equilibrium [22] is a pair of mixed and pure strategies such that the leader cannot unilaterally benefit by deviating from his/her mixed strategy to another mixed strategy and the follower cannot unilaterally benefit by deviating from his/her pure strategy to another pure strategy.

We define the game theoretic security of QBC protocols in the setting of commitment games. The leader plays a mixed strategy by making commitments using a QBC protocol, then the follower plays a pure strategy and opens the leader's commitment. Roughly speaking, a QBC protocol is game theoretic secure for a given commitment game if a strong Stackelberg equilibrium will be played by two players using the QBC protocol. Our protocol is game theoretic secure with respect to most commitment games. Being game theoretic secure opens the door of applying our protocol to game theory. As a case study and application, we show that our protocol can be use to implement strong Stackelberg equilibrium in many commitment games.

This paper is structured as follows. Background materials is presented in Section 2. Then, we present the proposed QBC protocol in Section 3 and its game theoretic security in Section 4. In Section 5 we run experiments on the IBM Q quantum computer to demonstrate the practicability of our protocol with the current technology. We evaluate our work by comparison with existing protocols in Section 6 and conclude this paper in Section 7.

2. Background knowledge

We assume the readers are familiar with the basic knowledge of quantum computation, and briefly review categorical quantum mechanics and the ZX-calculus in this section. The ZX-calculus is a graphical language of categorical quantum mechanics introduced by Coecke and Duncan [8,9]. We mainly use the single-qubit fragment of the ZX-calculus in this paper. A single-qubit quantum operator is represented in the ZX-calculus by a diagram which contains exactly two wires connected to a node:



where the phases ϕ and θ are real numbers. A green node with phase ϕ is called a $Z(\phi)$ diagram while a red node with phase θ is called a $X(\theta)$ diagram. The diagrams are read from bottom to top. The bottom wire indicates the input and the top wire indicates the output. Quantum gates can be expressed by diagrams in the ZX-calculus. For example, the I and X gates can be represented by $Z(0)$ and $X(\pi)$ diagrams, respectively. Indeed,

$$Z(0) = |0\rangle\langle 0| + e^{i0}|1\rangle\langle 1| = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix}[1,0] + \begin{bmatrix} 0 \\ 1 \end{bmatrix}[0,1]$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Please cite this article as: L. Zhou et al., Game theoretic security of quantum bit commitment, Information Sciences (2018), https://doi.org/10.1016/j.ins.2018.03.046