Game-Theoretic Security of Commitment Protocols under a Realistic Cost Model

Tsuyoshi Komatsubara and Yoshifumi Manabe
Department of Computer Science, Faculty of Informatics, Kogakuin University
Shinjuku, Tokyo, 163-8677 Japan. Email: manabe@cc.kogakuin.ac.jp

***Abstract*—This paper considers game-theoretic security of bit commitment protocols under a realistic cost model. Higo et. al (IWSEC 2013) proved equivalence of game-theoretic security and cryptographic security of bit commitment protocols under an ideal cost model. Their model assumes that there is no cost for communication and computation. Under a realistic model that cost for communication and computation is non-negligible, this paper shows that conventional bit commitment protocols are not game-theoretically secure, and abort detection property is necessary for bit commitment protocols to achieve game-theoretic security.**

***Keywords*-cryptographic protocols, bit commitment, game theory, security definition**

I. Introduction

Consider the following simple guess game between Alice and Bob using a bit commitment protocol.

1) Alice: "I have a bit $b \in \{0, 1\}$. I'll pay \$1,000 to you if you correctly guess the bit. You pay \$1,000 to me if your guess is wrong."
2) Alice and Bob execute the commit phase of a bit commitment protocol and Bob obtains commitment string c of bit b.
3) Bob: "I guess 0 !" ($b' = 0$)
4) Alice and Bob execute the open phase of the bit commitment protocol and Bob obtains b.
5) Bob wins if $b = b'$.

Now suppose that $b = 0$. In the case, Alice has no incentive to execute the open phase (step 4) only to prove that Alice lost the game. The computation and communication for the open phase have some costs, thus Alice might prefer to abort at step 4, if Alice does not want to pay the cost for the open phase. Though the computation and communication cost might be very small for each game instance, if Alice is a company and many instances of the game are played between Alice and a large number of users, the total cost of decommitment can be large, thus the abort strategy might be a reasonable decision for Alice. How the problem happens and how it is avoided? In the theory of cryptography, we model that the cost is negligible and do not consider such cases, but when we apply the theory to real world problems, we must consider these issues.

A simple fix seems to be that Bob sends a committed guess to Alice at step 3. This modified protocol does not solve the problem either because the decommitemnts of b and b' cannot be perfectly executed in parallel [1]. If the decommitment of b finishes first, Bob aborts the decommitment of b' when he knows that he lost the game.

This type of problem occurs only in commitment protocols because commitment protocols have both of the following two characteristics: (1)It is a mutli-phase protocol and (2) A party(the sender) obtains no new information in the second phase (the open phase).

Many protocols such as encryption/decryption, oblivious transfer, secret sharing, and so on are single-phase protocols, that is, each party joins the protocol in a single phase (As for an encryption/decryption, the time of decryption might be far after the time of the encryption. But each party's execution is not divided into multiple phases. As for a secret sharing, receiving a share is just a passive execution(each party does nothing). Each party's strategy exists only in the phase of collecting shares). Since the protocol consists of two phases, the environmental situation for the parties differs between the two phases (If nothing changes for any of the parties, there is no need to execute the protocol in two phases). As shown in the example, the sender might want to execute the protocol in the commit phase, but might not in the open phase.

In addition, for the protocols other than the commitment, the party that executes the protocol gains some new information by the execution. The sender of the commitment protocol knows no new information in the open phase thus an abort in the phase is sometimes a reasonable strategy.

Thus the questions to be discussed in this paper are: (1) Are commitment protocols really secure under the realistic cost models? (2) If the commitment protocols are not secure, how they can be fixed?

Many works have been done about the game theoretic analysis of cryptographic protocols (for example, [2]). Most of them deal rational secret sharing [3], [4]. Some of them considers general two party protocols [5], oblivious transfer [6], and bit commitment [7]. About the assumption of the analysis of bit commitment protocols, Asharov et. al [5] considers a fail-stop model for the parties. Higo et. al [7] considers a malicious model, but the cost of computation and communication for executing the protocol is ignored. This paper discusses under the malicious model for the parties and assumes that the cost for computation and communication is not negligible.

This paper first gives a new definition for game-theoretical security of bit commitment protocols under a realistic cost

model. Then, we show that usual(conventional) cryptographically secure bit commitment protocols are not game-theoretically secure under the model. Next, we show that the ability of detecting and proving the sender's abort is necessary for game-theoretic security.

II. Preliminaries

We say a function $\nu : \mathbb{N} \to \mathbb{R}$ is negligible if for any polynomial p, there exists $N \in \mathbb{N}$ such that for any $k > N$, it holds that $\nu(k) < 1/p(k)$. A negligible function is denoted as $negl(\cdot)$. We denote by $a \prec b$ or $b \succ a$ for $a(k), b(k) \in \mathbb{R}$, if $a(k) < b(k) - \epsilon(k)$ for some non-negligible function $\epsilon(k) > 0$. We denote by $a \approx b$ if $a(k) - b(k) \leq negl(k)$.

A probabilistic polynomial time algorithm is denoted as a PPT. In this paper, all parties use PPT algorithms in the security parameter k. For two algorithms A and B, denote the view of A (all information accessible by A) during an interaction with B by $\mathsf{view}_A(B)$, and the output of A after the interaction with B by $\mathsf{out}_A(B)$.

Next, we show the definition of bit commitment protocols in cryptography.

Definition 1 (Bit commitment [8], [9]): A bit commitment protocol $\mathsf{Com}(k)$ is a tuple of interactive PPT algorithms in the security parameter k, denoted by $\mathsf{Com}(k) = ((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$.

The commit phase is an interaction between $S_C^{(k)}$ and $R_C^{(k)}$, where $S_C^{(k)}$ receives a bit $b \in \{0,1\}$ as an input. The output of $S_C^{(k)}(b)$ is the commitment string c and a private output d for $S_O^{(k)}$. The information for decommitment is included in d. Without loss of generality, let c be the transcript of the interaction between $S_C^{(k)}(b)$ and $R_C^{(k)}$, and let d be $\mathsf{view}_{S_C^{(k)}(b)}(R_C^{(k)})$.

The open phase is an interaction between $S_O^{(k)}$ and $R_O^{(k)}$, where $S_O^{(k)}$'s input is tuple (b', c, d) and $R_O^{(k)}$'s input is c. Input d and c are decided by the commit phase. Note that for an incorrect execution the input bit b' might be $b' \neq b$, that is, a malicious sender tries to decommit to b'. After the interaction, $R_O^{(k)}$ outputs 1 if the receiver accepts, and 0 otherwise.

The conventional cryptographic security is shown below. In section III, we show a new cryptographic security, strong-security under a realistic cost model.

Definition 2 (Conventional cryptographic security [8], [9]): A commitment protocol $\mathsf{Com}(k) = ((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is cryptographically secure if it satisfies the following three properties.

- (**Correctness**) For any $b \in \{0,1\}$, it holds that $Pr[\mathsf{out}_{R_O^{(k)}(c)}(S_O^{(k)}(b,c,d)) = 1] \geq 1 - negl(k)$, where c is the transcript between $S_C^{(k)}(b)$ and $R_C^{(k)}$, and $d = \mathsf{view}_{S_C^{(k)}(b)}(R_C^{(k)})$.
- (**Hiding property**) For any $b \in \{0,1\}$, PPT cheating receiver $R_C^{*(k)}$, and PPT algorithm(distingusher) $D^{(k)}$, it holds that $|Pr[D^{(k)}(\mathsf{view}_{R_C^{*(k)}}(S_C^{(k)}(b))) = b] - 1/2| \leq negl(k)$.
- (**Binding property**) For any $b \in \{0,1\}$, PPT cheating sender $(S_C^{*(k)}, S_O^{*(k)})$, it holds that $Pr[\mathsf{out}_{R_O^{(k)}(c^*)}(S_O^{*(k)}(0,c^*,d^*)) = \mathsf{out}_{R_O^{(k)}(c^*)}(S_O^{*(k)}(1,c^*,d^*)) = 1] \leq negl(k)$, where c^* is the transcript of the interaction between $S_C^{*(k)}(b)$ and $R_C^{(k)}$ and $d^* = \mathsf{view}_{S_C^{*(k)}(b)}(R_C^{(k)})$.

In game theory, each player has a set of strategy. Since each player is assumed to be a polynomially bounded player, game-theoretic definition also reflects the assumption.

Definition 3 (Computational game): A computational game is a sequence $G^{(k)} = (n, A_i^{(k)}(i = 1, \ldots, n), U_i^{(k)}(i = 1, \ldots, n))$, where n is the number of players,
$\forall k \in \mathbb{N}, A_i^{(k)}$ is the set of actions taken by player i,
$U_i^{(k)} : A_1^{(k)} \times A_2^{(k)} \times \cdots \times A_n^{(k)} \to \mathbb{R}$ is the utility function of player i.
Note that $G^{(k)}$ is known to every player in advance.

A strategy of a player is a plan that specifies the action chosen by the player for every history of the game. For the commitment protocols, the players first execute the commit phase. In the open phase, each player knows the result of the players' actions taken in the commit phase and then decides the action in the open phase. Thus a strategy is a function whose input is the description of a game and a history of the game and whose output is an action.

One of the most commonly discussed solution concept of a game is a Nash equilibrium [10], [11]. Since each player is PPT, computational Nash equilibrium is discussed in this paper.

Definition 4 (Computational Nash equilibrium):
A tuple of strategies $(p_1, p_2, \ldots, p_n)$ is an ϵ-computational Nash equilibrium in a computational game $G^{(k)}$ if $\forall i (1 \leq i \leq n)$, $\forall p_i' \in PPT$, $\forall k \in \mathbb{N}$, $U_i^{(k)}(p_1, \ldots, p_{i-1}, p_i, p_{i+1}, \ldots, p_n) \geq$
$U_i^{(k)}(p_1, \ldots, p_{i-1}, p_i', p_{i+1}, \ldots, p_n) - \epsilon(k)$.
That is, when a tuple of strategy is a computational Nash equilibrium, no player has incentive to change its strategy.

III. New game-theoretic definition

This section gives a new game-theoretic security definition of commitment protocols. Our definition of utility functions considers the cost for commitment protocols. As written in the introduction, S might intentionally abort in the open phase because of some reason. Under the realistic model that computation and communication cost for bit commitment protocols is not negligible, S can obtain more utility by abort because of lowering the cost. The only way to prevent S's abort seems to be the R's detect and punishment, for example, forcing to pay the money or reputation that S is dishonest. In either case, the proof that S aborted is necessary to avoid false punishment. Thus proof must be

able to be verified by anyone. Therefore, in order for a commitment protocol to be secure under the realistic cost model, the ability to detect and prove S's abort is necessary for R. This section gives a new definition of game-theoretic security and cryptographic security.

First, we give a definition of commitment protocol with abort detection property and the strong-security of bit commitment protocols.

Definition 5 (Bit commitment with abort detection): A bit commitment protocol $\mathsf{Com}(k)$ is a tuple of interactive PPT algorithms, denoted by $\mathsf{Com}(k) = ((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$.

The commit phase and the open phase are the same as the one in Definition 1.

After the interaction, $R_O^{(k)}$ outputs 1 if R accepts, 0 if R rejects, and $\mathbb{P}$(a proof of S's abort) if S aborts in the open phase.

The difference is the proof of S's abort in the open phase. $\mathbb{P}$ can be verified by everyone. One of the realistic realization of the above protocol is usage of a public bulletin board. S writes the commitment string c to the bulletin board. In the open phase, S writes the decommitment information d^* to the bulletin board. Everyone can verify the correctness of the decommiment using d^* and c. If S aborts, no message is written to the bulletin board and anyone can verify that S aborted. Note that the punishment mechanism in the proof is outside of the discussion in this paper. We assume that there is some punishment mechanism using $\mathbb{P}$.

Definition 6 (Cryptographic strong-security): A commitment protocol $\mathsf{Com}(k) = ((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is cryptographically strong-secure if it satisfies correctness, hiding property, binding property in Def. 2, and the following abort detection property.

- (**Abort detection property**) For any $b \in \{0,1\}$ and cheating sender $(S_C^{*(k)}, S_O^{*(k)})$, if $S_O^{*(k)}$ aborts $Pr[\mathsf{out}_{R_O^{(k)}(c^*)}(S_O^{*(k)}(b, c^*, d^*)) = \mathbb{P}] \geq 1 - negl(k)$, where c^* is the transcript of the interaction between $S_C^{*(k)}(b)$ and $R_C^{(k)}$, $d^* = \mathsf{view}_{S_C^{*(k)}(b)}(R_C^{(k)})$, and $\mathbb{P}$ is a valid proof that S aborted in the open phase.
  For any $b \in \{0,1\}$ and cheating receiver $R_O^{*(k)}$, if the sender is correct, $Pr[\mathsf{out}_{R_O^{*(k)}(c)}(S_O^{(k)}(b, c, d)) = \mathbb{P}] \leq negl(k)$, where c is the transcript of the interaction between $S_C^{(k)}(b)$ and $R_C^{(k)}$, $d = \mathsf{view}_{S_C^{(k)}(b)}(R_C^{(k)})$, and $\mathbb{P}$ is a cheating proof that S aborted in the open phase.

Next, we propose new game-theoretic security. Under the realistic cost model, the sender S has the following three preferences.

- SL-1 S does not prefer R to know the committed bit b before executing the open phase.
- SL-2 On executing the open phase, S prefers to be able to choose a bit to be opened.
- SL-3 S prefers that S's intentional abort in the open phase is not detected and proved by R.
- SL-4 S prefers that R cannot give a false proof that S is aborted when S correctly executes the protocol.

R's preference is as follows.

- RL-1 R prefers to know the committed bit b before executing the open phase.
- RL-2 R does not prefer S to change the bit to be opened in the open phase.
- RL-3 R prefers to open the committed bit b correctly in the open phase unless the protocol was aborted.
- RL-4 R prefers to be able to detect and prove S's intentional abort.
- RL-5 R prefers to be able to give a false proof that S aborted even if S is correct.

SL-3 and SL-4 are newly added to the preferences in [7]. The meaning of SL-3 is that if R cannot detect S's abort, S can abort in the open phase and spend a lower cost. SL-4 means that if R can give a false proof, S obtains some punishment using the false proof. For the receiver, RL-4 and RL-5 are newly added to the preferences in [7]. The meaning of RL-4 is that in the guess game, R needs to be able to detect and prove S's intentional abort in the open phase. The meaning of RL-5 is that R obtains more utility if R gives a false punishment to S. RL-4 and RL-5 supposes that there is some mechanism to punish S. Without such a mechanism, there is no way for R to effectively use the (false) proof of S's abort, thus RL-4 and RL-5 are not satisfied for R. The actual mechanism to punish S is outside of this paper.

Note that RL-3 means the utility of a correct decommitment and the utility of R's intentional abort are the same. In some cases, R might prefer R's abort to a correct decommitment, for example, after the commit phase, the committed bit is informed to R from someone else (other than S). Since decommitment needs R's computation and communication cost, under a realistic cost model, R prefers abort in the open phase. If R prefers abort, there is no way for S to prevent R's abort. This definition allows R's abort.

Definition 7 (New bit commitment game): For PPT algorithms $D^{(k)}$, $S_C^{'(k)}$, $S_O^{'(k)}$, $R_C^{'(k)}$, and, $R_O^{'(k)}$, the two-phase game $\Gamma^{Com(k)}((S_C^{'(k)}, S_O^{'(k)}), (R_C^{'(k)}, R_O^{'(k)}))$ is executed as follows.

1. S selects PPT $S_C^{'(k)}$ and R selects $R_C^{'(k)}$ simultaneously.
2. Choose a bit $b \in \{0,1\}$ randomly and set $\mathsf{guess} = \mathsf{amb} = \mathsf{cor} = \mathsf{sabt} = \mathsf{rabt} = \mathsf{dsabt} = 0$.
3. Observe an interaction between $S_C^{'(k)}(b)$ and $R_C^{'(k)}$, and let c be the transcript during the interaction. Set $\mathsf{sabt} = 1$ if S aborts and $\mathsf{rabt} = 1$ if R aborts. Let $d = \mathsf{view}_{S_C^{'(k)}(b)}(R_C^{'(k)})$.
4. S selects $S_O^{'(k)}$ using d. R simultaneously selects $R_O^{'(k)}$ using c.
5. Set $\mathsf{guess} = 1$ if $b = D^{(k)}(\mathsf{view}_{R_C^{'(k)}}(S_C^{'(k)}(b)))$.
6. Observe an interaction between $S_O^{'(k)}(b, c, d)$ and

$R_O^{'(k)}(c)$. Set $\mathsf{sabt} = 1$ if S aborts and $\mathsf{rabt} = 1$ if R aborts.

7 Observe an interaction between $S_O^{'(k)}(1-b,c,d)$ and $R_O^{'(k)}(c)$. Set $\mathsf{rabt} = 1$ if R aborts.

8 Set $\mathsf{amb} = 1$ if $\mathsf{out}_{R_O^{'(k)}(c)}(S_O^{'(k)}(0,c,d)) = \mathsf{out}_{R_O^{'(k)}(c)}(S_O^{'(k)}(1,c,d)) = 1$. Set $\mathsf{cor} = 1$ if $\mathsf{out}_{R_O^{'(k)}(c)}(S_O^{'(k)}(b,c,d)) = 1$. Set $\mathsf{dsabt} = 1$ if $\mathsf{out}_{R_O^{'(k)}(c)}(S_O^{'(k)}(b,c,d)) = \mathbb{P}$, where $\mathbb{P}$ is a valid proof that S aborted.

The tuple $(\mathsf{guess}, \mathsf{amb}, \mathsf{cor}, \mathsf{sabt}, \mathsf{dsabt}, \mathsf{rabt})$ is the outcome of the game. The meaning is as follows. After the commit phase, R tries to know the committed bit b before the open phase using $D^{(k)}$. If $D^{(k)}$ succeeds, set $\mathsf{guess} = 1$, otherwise, $\mathsf{guess} = 0$. Then, S tries to open to b and $1-b$. If both of these two opens succeed, set $\mathsf{amb} = 1$, otherwise, $\mathsf{amb} = 0$. If open to b succeeds, set $\mathsf{cor} = 1$, otherwise $\mathsf{cor} = 0$. If S (R) aborts during the execution, set $\mathsf{sabt} = 1$ ($\mathsf{rabt} = 1$). $\mathsf{dsabt} = 1$ means that $R_O^{(k)}$ outputs a proof that S aborts in the open phase (it does not mean S really aborted). Note that S's abort in $S_O^{'(k)}(1-b,c,d)$ is not considered, because executing $S_O^{'(k)}(1-b,c,d)$ is based on the will that S tries to decommit to incorrect value $1-b$, thus S generally does not abort by himself. The main difference between the definition in [7] is refinement of abort in [7] to sabt, dsabt, and rabt. In [7], the abort in S and R are equally treated. As written above, we need to treat them differently and introduce sabt and rabt. In addition, we need to indicate whether the valid proof is obtained or not and dsabt is added.

Note that the bit commitment game is a two-phase game, that is, after the commit phase is finished, each player can change its strategy for the open phase depending on the information obtained in the commit phase.

Next, we formalize our new preferences as new utility functions.

Definition 8 (New utility function): For a bit commitment protocol $\mathsf{Com}(k)$, let $(\mathsf{guess}, \mathsf{amb}, \mathsf{cor}, \mathsf{sabt}, \mathsf{dsabt}, \mathsf{rabt})$ be the random variables representing the outcome of $\Gamma^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$.

For PPT algorithms $S_C^{'(k)}$ and $S_O^{'(k)}$, let $(\mathsf{guess}', \mathsf{amb}', \mathsf{cor}', \mathsf{sabt}', \mathsf{dsabt}', \mathsf{rabt}')$ be the random variables representing the outcome of $\Gamma^{Com(k)}((S_C^{'(k)}, S_O^{'(k)}), (R_C^{(k)}, R_O^{(k)}))$.

The utility function $U_S^{Com(k)}$ for S satisfies $U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) > U_S^{Com(k)}((S_C^{'(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ if one of the following conditions holds.

S-1 $|Pr[\mathsf{guess} = 1] - 1/2| \prec |Pr[\mathsf{guess}' = 1] - 1/2|$.

S-2 $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}' = 1]$ and $Pr[\mathsf{amb} = 1] \succ Pr[\mathsf{amb}' = 1]$

S-3 $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}' = 1]$, $Pr[\mathsf{amb} = 1] \approx Pr[\mathsf{amb}' = 1]$, and $Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] \succ Pr[\mathsf{sabt}' = 1 \wedge \mathsf{dsabt}' = 0]$.

S-4 $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}' = 1]$, $Pr[\mathsf{amb} = 1] \approx Pr[\mathsf{amb}' = 1]$, $Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] \approx Pr[\mathsf{sabt}' = 1 \wedge \mathsf{dsabt}' = 0]$, and $Pr[\mathsf{sabt} = 0 \wedge \mathsf{dsabt} = 1] \succ Pr[\mathsf{sabt}' = 0 \wedge \mathsf{dsabt}' = 1]$.

For PPT algorithms $R_C^{'(k)}$ and $R_O^{'(k)}$, let $(\mathsf{guess}', \mathsf{amb}', \mathsf{cor}', \mathsf{sabt}', \mathsf{dsabt}', \mathsf{rabt}')$ be the random variables representing the outcome of $\Gamma^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{'(k)}, R_O^{'(k)}))$. The utility function $U_R^{Com(k)}$ for R satisfies $U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) > U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{'(k)}, R_O^{(k)}))$ if one of the following conditions holds.

R-1 $|Pr[\mathsf{guess} = 1] - 1/2| \succ |Pr[\mathsf{guess}' = 1] - 1/2|$.

R-2 $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}' = 1]$ and $Pr[\mathsf{amb} = 1] \prec Pr[\mathsf{amb}' = 1]$

R-3 $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}' = 1]$, $Pr[\mathsf{amb} = 1] \approx Pr[\mathsf{amb}' = 1]$, and $Pr[\mathsf{sabt} = 1 \vee \mathsf{rabt} = 1 \vee \mathsf{cor} = 1] \succ Pr[\mathsf{sabt}' = 1 \vee \mathsf{rabt}' = 1 \vee \mathsf{cor}' = 1]$.

R-4 $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}' = 1]$, $Pr[\mathsf{amb} = 1] \approx Pr[\mathsf{amb}' = 1]$, $Pr[\mathsf{sabt} = 1 \vee \mathsf{rabt} = 1 \vee \mathsf{cor} = 1] \approx Pr[\mathsf{sabt}' = 1 \vee \mathsf{rabt}' = 1 \vee \mathsf{cor}' = 1]$, and $Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] \prec Pr[\mathsf{sabt}' = 1 \wedge \mathsf{dsabt}' = 0]$.

R-5 $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}' = 1]$, $Pr[\mathsf{amb} = 1] \approx Pr[\mathsf{amb}' = 1]$, $Pr[\mathsf{sabt} = 1 \vee \mathsf{rabt} = 1 \vee \mathsf{cor} = 1] \approx Pr[\mathsf{sabt}' = 1 \vee \mathsf{rabt}' = 1 \vee \mathsf{cor}' = 1]$, $Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] \approx Pr[\mathsf{sabt}' = 1 \wedge \mathsf{dsabt}' = 0]$, and $Pr[\mathsf{sabt} = 0 \wedge \mathsf{dsabt} = 1] \prec Pr[\mathsf{sabt}' = 0 \wedge \mathsf{dsabt}' = 1]$

S-3, S-4, R-4, and R-5 are newly added to represent preference SL-3, SL-4, RL-4, and RL-5, respectively.

Definition 9 (New game-theoretic security): Let $\mathsf{Com}(k)$ be a bit commitment protocol. $\mathsf{Com}(k)$ is game-theoretically secure if the tuple of the strategies $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is in a computational Nash equilibrium for the utility function in Def. 8.

IV. Equivalence between the security notions

First, we show that the usual (conventional) bit commitment protocols are not game-theoretically secure under the realistic cost model.

Theorem 1: Not every cryptographically secure bit commitment protocol $\mathsf{Com}(k)$ is game-theoretically secure.

(Proof) Sender S changes the strategy from $(S_C^{(k)}, S_O^{(k)})$ to $(S_C^{''(k)}, S_O^{''(k)}) = (S_C^{(k)}, S_O^{abort(k)})$, that is, S always aborts in the open phase. Thus $Pr[\mathsf{sabt}'' = 1] = 1$ and $Pr[\mathsf{sabt} = 1] \approx 0$ are satisfied. Since $\mathsf{Com}(k)$ is cryptographically secure, $|Pr[\mathsf{guess} = 1] - 1/2| \approx 0$ and $Pr[\mathsf{amb} = 1] \approx 0$.

Since $S_C^{''(k)} = S_C^{(k)}$ and $S_O^{''(k)}$ is abort, $|Pr[\mathsf{guess}'' = 1] - 1/2| \approx 0$ and $Pr[\mathsf{amb}'' = 1] \approx 0$ hold. Thus, $Pr[\mathsf{guess} = 1] \approx Pr[\mathsf{guess}'' = 1]$ and $Pr[\mathsf{amb} = 1] \approx Pr[\mathsf{amb}'' = 1]$ hold.

In conventional cryptographically secure bit commitment protocols, R cannot perfectly detect the sender's abort.

R cannot distinguish the sender's intentional abort and a failure of the communication link between S and R. Thus, $Pr[\mathsf{sabt}'' = 1 \wedge \mathsf{dsabt}'' = 0] \succ 0$ is satisfied. Therefore, $Pr[\mathsf{sabt}'' = 1 \wedge \mathsf{dsabt}'' = 0] \succ Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsbt} = 0]$ and S-3 is satisfied. Thus, S obtains more utility by changing the strategy from $(S_C^{(k)}, S_O^{(k)})$ to $(S_C^{''(k)}, S_O^{''(k)})$. □

In order to show the theorem holds for realistic situations, let us consider the following example. Let u be S's utility by opening the bit correctly and c be the cost of correctly executing $S_O^{(k)}$. The cost of $S_O^{abort(k)}$ is 0. Let us suppose that R can give some punishment $x(< 0)$ to S when R can prove that S aborts. $U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) = u - c$ and $U_S^{Com(k)}((S_C^{(k)}, S_O^{abort(k)}), (R_C^{(k)}, R_O^{(k)})) = x \cdot Pr[\mathsf{dsabt}'' = 1] - 0$. S obtains more utility by abort if $x \cdot Pr[\mathsf{dsabt}'' = 1] > u - c$. The values of u, c, and x depend on the financial value of the committed bit, computation and communication environment, and so on. For the case of the above guess game, $u = 0$ when S knows that she lost the game. If R cannot detect and prove that S aborts, $Pr[\mathsf{dsabt}'' = 1] = 0$ and $x \cdot Pr[\mathsf{dsabt}'' = 1] > u - c$ hold and S obtains more utility by the abort.

In order to prevent abort, some mechanism is necessary to either (1) give some rewards from R to S for correct decommitment by S or (2) give some punishment to S for aborting. Let us first discuss case (1). If R pays S's cost for the computation and communication for opening, S might honestly execute the opening phase. However, this intuition does not hold for the guess game shown in the introduction. Let the cost for opening by S be c and the reward of correctly executing opening be r. When S loses, S needs to pay \$1,000 to R. Thus the utility of correctly executing opening is $-\$1,000 - c + r$ and aborting is 0, if R cannot prove S's abort. Thus S honestly executes opening when S lost the game only if $r \geq \$1,000 + c$. If $r \geq \$1,000 + c$, R gains nothing even when R wins the game. Thus, giving reward is not a realistic solution.

Therefore, the only way to prevent aborting is giving punishment from to S after aborting. In order to give a punishment from R to S, it is necessary for R to be able to detect S's abort and prove that S really aborted to everyone. Without the proof, the other parties cannot understand that S really aborted. In addition, it is necessary for R not to be able to give a false proof that S aborted when S correctly executes opening.

Now, we show that the strong cryptographic security and our new game-theoretic security are equivalent.

Theorem 2: Bit commitment protocol $\mathsf{Com}(k)$ is game-theoretically secure if and only if it is cryptographically strong-secure.

The following two lemmas prove the main theorem.

Lemma 1: If bit commitment protocol $\mathsf{Com}(k)$ is cryptographically strong-secure, then it is game-theoretically secure.

(Proof) We assume that $\mathsf{Com}(k) = ((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not game-theoretically secure and show that it is not cryptographically strong-secure. Since $\mathsf{Com}(k)$ is not game-theoretically secure, one of the followings hold.

(Case 1) For some PPT $S_C^{''(k)}, S_O^{''(k)}$, $U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) < U_S^{Com(k)}((S_C^{''(k)}, S_O^{''(k)}), (R_C^{(k)}, R_O^{(k)}))$ holds.

(Case 2) For some PPT $R_C^{''(k)}, R_O^{''(k)}$, $U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) < U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{''(k)}, R_O^{''(k)}))$ holds.

First consider Case 1. From Def. 8, at least one of S-1, S-2, S-3, or S-4 is satisfied.

Let us assume that S-1 is satisfied. $|Pr[\mathsf{guess} = 1] - 1/2| \succ |Pr[\mathsf{guess}'' = 1] - 1/2|$, thus changing the strategy from $S_C^{(k)}$ to $S_C^{''(k)}$ decreases the possibility for R to guess committed bit b. It means that $|Pr[\mathsf{guess} = 1] - 1/2| \succ 0$. Thus, R can guess the committed bit b using some PPT $D^{(k)}$ when S and R use $S_C^{(k)}$ and $R_C^{(k)}$. Therefore, $\mathsf{Com}(k)$ does not satisfy hiding property.

Next let us assume that S-2 is satisfied. Since $Pr[\mathsf{amb} = 1] \prec Pr[\mathsf{amb}'' = 1]$, if S changes the strategy from $(S_C^{(k)}, S_O^{(k)})$ to $(S_C^{''(k)}, S_O^{''(k)})$, the possibility that S can open the committed bit to 0 and 1 increases. Therefore, $\mathsf{Com}(k)$ does not satisfy binding property.

Next, let us assume that S-3 is satisfied. Since $Pr[\mathsf{sabt}'' = 1 \wedge \mathsf{dsabt}'' = 0] \succ Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0]$, if S changes the strategy from $(S_C^{(k)}, S_O^{(k)})$ to $(S_C^{''(k)}, S_O^{''(k)})$, the possibility that R can detect S's abort decreases. Thus, $\mathsf{Com}(k)$ does not satisfy abort detection property.

Next, let us assume that S-4 is satisfied. Since $Pr[\mathsf{sabt} = 0 \wedge \mathsf{dsabt} = 1] \succ Pr[\mathsf{sabt}' = 0 \wedge \mathsf{dsabt}' = 1]$, $Pr[\mathsf{sabt} = 0 \wedge \mathsf{dsabt} = 1] \succ 0$. Thus R can give a false proof that S aborted even if S executes correctly. Therefore, $\mathsf{Com}(k)$ does not satisfy abort detection property.

Next, consider Case 2. From Def. 8, at least one of R-1, R-2, R-3, R-4, or R-5 is satisfied.

First let us assume that R-1 is satisfied. Since

$$|Pr[\mathsf{guess}'' = 1] - 1/2| \succ |Pr[\mathsf{guess} = 1] - 1/2|,$$

$$|Pr[\mathsf{guess}'' = 1] - 1/2| \succ 0$$

holds for $((S_C^{(k)}, S_O^{(k)}), (R_C^{''(k)}, R_O^{''(k)}))$. Thus, $\mathsf{Com}(k)$ does not satisfy hiding property.

Next let us assume that R-2 is satisfied. Since

$$Pr[\mathsf{amb}'' = 1] \prec Pr[\mathsf{amb} = 1],$$

$$Pr[\mathsf{amb} = 1] \succ 0.$$

This means that $\mathsf{Com}(k)$ does not satisfy binding property.

Next let us assume that R-3 is satisfied. Since

$$Pr[\mathsf{sabt}'' = 1 \vee \mathsf{rabt}'' = 1 \vee \mathsf{cor}'' = 1] \succ$$

$$Pr[\mathsf{sabt} = 1 \vee \mathsf{rabt} = 1 \vee \mathsf{cor} = 1],$$

$$Pr[\mathsf{sabt} = 1 \vee \mathsf{rabt} = 1 \vee \mathsf{cor} = 1] \prec 1$$

holds. Thus,

$$Pr[\mathsf{sabt} = 0 \wedge \mathsf{rabt} = 0] \succ 0$$

and

$$Pr[\mathsf{cor} = 1 | \mathsf{sabt} = 0 \wedge \mathsf{rabt} = 0] \prec 1.$$

This means that $\mathsf{Com}(k)$ does not satisfy correctness.

Next let us assume that R-4 is satisfied. Since

$$Pr[\mathsf{sabt}'' = 1 \wedge \mathsf{dsabt}'' = 0] \prec Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0],$$

$$Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] \succ 0$$

holds. Thus, when S aborts in the open phase, R cannot detect and prove S's abort. This means that $\mathsf{Com}(k)$ does not satisfy abort detection property.

Next let us assume that R-5 is satisfied. Since

$$Pr[\mathsf{sabt} = 0 \wedge \mathsf{dsabt} = 1] \prec Pr[\mathsf{sabt}'' = 0 \wedge \mathsf{dsabt}'' = 1],$$

$$Pr[\mathsf{sabt}'' = 0 \wedge \mathsf{dsabt}'' = 1] \succ 0$$

holds. Thus, even if S honestly executes, R can give a proof that S aborted. This means that $\mathsf{Com}(k)$ does not satisfy abort detection property.

In any case, $\mathsf{Com}(k)$ is not cryptographically strong-secure. □

Lemma 2: If bit commitment protocol $\mathsf{Com}(k)$ is game-theoretically secure, then it is cryptographically strong-secure.

(Proof) We assume that $\mathsf{Com}(k) = ((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not cryptographically strong-secure and show that it is not game-theoretically secure. Since $\mathsf{Com}(k)$ is not cryptographically strong-secure, one of the followings hold.

- Case 1 $\mathsf{Com}(k)$ does not satisfy correctness.
- Case 2 $\mathsf{Com}(k)$ satisfies correctness but does not satisfy hiding property.
- Case 3 $\mathsf{Com}(k)$ satisfies correctness and hiding property, but does not satisfy hiding property for some $R_C^{'(k)} \neq R_C^{(k)}$.
- Case 4 $\mathsf{Com}(k)$ satisfies correctness and hiding property but does not satisfy binding property.
- Case 5 $\mathsf{Com}(k)$ satisfies correctness, hiding property and binding property, but does not satisfy binding property for some $(S_C^{''(k)}, S_O^{''(k)})$, where $S_C^{''(k)} \neq S_C^{(k)}$.
- Case 6 $\mathsf{Com}(k)$ satisfies correctness, hiding property and binding property but does not satisfy abort detection property.
- Case 7 $\mathsf{Com}(k)$ satisfies correctness, hiding property, binding property, and abort detection property but does not satisfy abort detection property for some $S_C^{''(k)} \neq S_C^{(k)}$.
- Case 8 $\mathsf{Com}(k)$ satisfies correctness, hiding property, binding property, abort detection property, but does not satisfy false abort detection impossibility property for some $(R_C^{''(k)}, R_O^{''(k)}) \neq (R_C^{(k)}, R_O^{(k)})$.

We denote the outcome of the game $\Gamma^{Com}(k)((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ by $(\mathsf{guess}, \mathsf{amb}, \mathsf{cor}, \mathsf{sabt}, \mathsf{dsabt}, \mathsf{rabt})$.

First let us assume that Case 1 is satisfied. Even if both parties correctly execute the protocol, the probability that R cannot open the committed bit is non-negligible. That is, for some bit $b \in \{0, 1\}$, it holds that

$$Pr[\mathsf{cor} = 1] \prec 1.$$

Let $(R_C^{abort(k)}, R_O^{abort(k)})$ be a tuple of strategies such that R aborts just after the beginning of the protocol. We denote the outcome of the game $\Gamma^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{abort(k)}, R_O^{abort(k)}))$ by $(\mathsf{guess}'', \mathsf{amb}'', \mathsf{cor}'', \mathsf{sabt}'', \mathsf{dsabt}'', \mathsf{rabt}'')$. The following equalities are obtained.

$$Pr[\mathsf{sabt} = 1] = Pr[\mathsf{sabt}'' = 1] = 0$$

$$Pr[\mathsf{cor} = 1] \prec 1$$

$$Pr[\mathsf{cor}'' = 1] = 0$$

$$Pr[\mathsf{rabt} = 1] = 0$$

$$Pr[\mathsf{rabt}'' = 1] = 1$$

Thus,

$$Pr[\mathsf{sabt}'' = 1 \vee \mathsf{rabt}'' = 1 \vee \mathsf{cor}'' = 1] \succ$$

$$Pr[\mathsf{sabt} = 1 \vee \mathsf{rabt} = 1 \vee \mathsf{cor} = 1]$$

and

$$U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$

$$U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{abort(k)}, R_O^{abort(k)}))$$

holds from R-3, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium.

(Case 2): R can break the hiding property with the honest strategy $R_C^{(k)}$. For some PPT distinguisher $D^{(k)}$, It holds that $Pr[D^{(k)}(\mathsf{view}_{R_C^{(k)}}(S_C^{(k)}(b))) = b] \succ 1/2$. Let $(S_C^{abort(k)}, S_O^{abort(k)})$ be a tuple of strategies of abort the commitment just after starting the protocol, that is, the sender does not execute the commitment at all.

We denote the outcome of the game $\Gamma^{Com(k)}((S_C^{abort(k)}, S_O^{abort(k)}), (R_C^{(k)}, R_O^{(k)}))$ by $(\mathsf{guess}'', \mathsf{amb}'', \mathsf{cor}'', \mathsf{sabt}'', \mathsf{dsabt}'', \mathsf{rabt}'')$.

It holds that

$$|Pr[\mathsf{guess} = 1] - 1/2| \succ |Pr[\mathsf{guess}'' = 1] - 1/2| = 0.$$

Thus,

$$U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$

$$U_S^{Com(k)}((S_C^{abort(k)}, S_O^{abort(k)}), (R_C^{(k)}, R_O^{(k)}))$$

holds from S-1, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium.

(Case 3) R cannot break the hiding property with honest strategy $R_C^{(k)}$ but with some strategy $R_C^{''(k)} \neq R_C^{(k)}$. That is, for some PPT distinguisher $D^{(k)}$, it holds that

$$Pr[D^{(k)}(\mathsf{view}_{R_C^{''(k)}}(S_C^{(k)}(b))) = b] \succ$$

$$Pr[D^{(k)}(\mathsf{view}_{R_C^{(k)}}(S_C^{(k)}(b))) = b] \approx 1/2.$$

Let $R_O^{abort(k)}$ be a strategy such that R aborts in the open phase.

We denote the outcome of the game $\Gamma^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{''(k)}, R_O^{abort(k)}))$ by $(\mathsf{guess''}, \mathsf{amb''}, \mathsf{cor''}, \mathsf{sabt''}, \mathsf{dsabt''}, \mathsf{rabt''})$.

We obtain

$$|Pr[\mathsf{guess''} = 1] - 1/2| \succ |Pr[\mathsf{guess} = 1] - 1/2| \approx 0.$$

Thus,

$$U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$

$$U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{''(k)}, R_O^{abort(k)}))$$

holds from R-1, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium.

(Case 4) S can break the binding property with $(S_C^{(k)}, S_O^{(k)})$. That is, for some $b \in \{0, 1\}$, it holds that

$$Pr[\mathsf{out}_{R_O^{(k)}(c)}(S_O^{(k)}(0, c, d)) =$$

$$\mathsf{out}_{R_O^{(k)}(c)}(S_O^{(k)}(1, c, d)) = 1] \succ 0,$$

where c is the transcript between $S_C^{(k)}(b)$ and $R_C^{(k)}$, and $d = \mathsf{view}_{S_C^{(k)}(b)}(R_C^{(k)}))$. Let $(R_C^{abort(k)}, R_O^{abort(k)})$ be a tuple of strategies of abort.

We denote the outcome of the game $\Gamma^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{abort(k)}, R_O^{abort(k)}))$ by $(\mathsf{guess''}, \mathsf{amb''}, \mathsf{cor''}, \mathsf{sabt''}, \mathsf{dsabt''}, \mathsf{rabt''})$.

We obtain

$$|Pr[\mathsf{guess} = 1] - 1/2| \approx |Pr[\mathsf{guess''} = 1] - 1/2| = 0,$$

$$Pr[\mathsf{amb} = 1] \succ Pr[\mathsf{amb''} = 1] = 0.$$

Thus,

$$U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$

$$U_R^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{abort(k)}, R_O^{abort(k)}))$$

holds from R-2, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium.

(Case 5) S can break the binding property with some strategy $(S_C^{''(k)}, S_O^{''(k)}) \neq (S_C^{(k)}, S_O^{(k)})$. That is, for some $b \in \{0, 1\}$, it holds that

$$Pr[\mathsf{out}_{R_O^{(k)}(c')}(S_O^{''(k)}(0, c', d')) =$$

$$\mathsf{out}_{R_O^{(k)}(c')}(S_O^{''(k)}(1, c', d')) = 1] \succ 0,$$

where c' is the transcript between $S_C^{''(k)}(b)$ and $R_C^{(k)}$, and $d' = \mathsf{view}_{S_C^{''(k)}(b)}(R_C^{(k)}))$.

We denote the outcome of the game $\Gamma^{Com(k)}((S_C^{''(k)}, S_O^{''(k)}), (R_C^{(k)}, R_O^{(k)}))$ by $(\mathsf{guess''}, \mathsf{amb''}, \mathsf{cor''}, \mathsf{sabt''}, \mathsf{dsabt''}, \mathsf{rabt''})$.

If hiding property is simultaneously broken by $(S_C^{''(k)}, S_O^{''(k)})$, R aborts in the open phase and S just breaks hiding property by himself. It is not a cryptographically valid attack to a bit commitment protocol for S. Thus this case is not considered and we assume that

$$|Pr[\mathsf{guess} = 1] - 1/2| \approx |Pr[\mathsf{guess''} = 1] - 1/2| \approx 0.$$

The following equation is obtained from the assumption.

$$Pr[\mathsf{amb''} = 1] \succ Pr[\mathsf{amb} = 1] \approx 0.$$

Thus,

$$U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$

$$U_S^{Com(k)}((S_C^{''(k)}, S_O^{''(k)}), (R_C^{(k)}, R_O^{(k)}))$$

holds from S-2, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium.

(Case 6) Even if S aborts in the open phase, R cannot correctly detect and prove the abort.

Let $S_O^{abort(k)}$ be sender's abort strategy in the open phase.

We denote the outcome of the game $\Gamma^{Com(k)}((S_C^{(k)}, S_O^{abort(k)}), (R_C^{(k)}, R_O^{(k)}))$ by $(\mathsf{guess''}, \mathsf{amb''}, \mathsf{cor''}, \mathsf{sabt''}, \mathsf{dsabt''}, \mathsf{rabt''})$.

For a correct execution, $Pr[\mathsf{sabt} = 1] = 0$, thus $Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] = 0$. Since R cannot perfectly detect S's abort, $Pr[\mathsf{sabt''} = 1 \wedge \mathsf{dsabt''} = 0] \succ 0$.

We obtain the following equations.

$$|Pr[\mathsf{guess''} = 1] - 1/2| \approx |Pr[\mathsf{guess} = 1] - 1/2|$$

$$Pr[\mathsf{amb''} = 1] \approx Pr[\mathsf{amb} = 1]$$

Thus,

$$U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$

$$U_S^{Com(k)}((S_C^{(k)}, S_O^{abort(k)}), (R_C^{(k)}, R_O^{(k)}))$$

holds from S-3, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium.

(Case 7) R cannot detect sender's abort for $S_C^{''(k)} \neq S_C^{(k)}$. Let $S_O^{abort(k)}$ be sender's abort strategy in the open phase.

We denote the outcome of the game $\Gamma^{Com(k)}((S_C^{''(k)}, S_O^{abort(k)}), (R_C^{(k)}, R_O^{(k)}))$ by $(\mathsf{guess''}, \mathsf{amb''}, \mathsf{cor''}, \mathsf{sabt''}, \mathsf{dsabt''}, \mathsf{rabt''})$.

We assume that hiding property and binding property are satisfied with $S_C^{''(k)}$, because breaking hiding property is not a cryptographically valid attack for S(as in Case 5) and

breaking binding property is already considered in Case 5. Thus,

$$|Pr[\mathsf{guess}'' = 1] - 1/2| \approx |Pr[\mathsf{guess} = 1] - 1/2|$$

$$Pr[\mathsf{amb}'' = 1] \approx Pr[\mathsf{amb} = 1]$$

are satisfied. For a correct execution, $Pr[\mathsf{sabt} = 1] = 0$, thus

$$Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] = 0.$$

Since the receiver cannot perfectly detect sender's abort,

$$Pr[\mathsf{sabt}'' = 1 \wedge \mathsf{dsabt}'' = 0] \succ 0.$$

Thus,

$$U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$
$$U_S^{Com(k)}((S_C^{''(k)}, S_O^{abort(k)}), (R_C^{(k)}, R_O^{(k)}))$$

holds from S-3, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium.

(Case 8) R can give a false proof that S aborts even if S executes correctly for some strategy $(R_C^{''(k)}, R_O^{''(k)}) \neq (R_C^{(k)}, R_O^{(k)})$. We assume that hiding property and binding property are satisfied with $(R_C^{''(k)}, R_O^{''(k)})$, because breaking binding property is not a cryptographically valid attack for R and breaking hiding property is already discussed in Case 3. Thus,

$$|Pr[\mathsf{guess}'' = 1] - 1/2| \approx |Pr[\mathsf{guess} = 1] - 1/2|$$

$$Pr[\mathsf{amb}'' = 1] \approx Pr[\mathsf{amb} = 1]$$

are satisfied. Since R does not abort,

$$Pr[\mathsf{sabt} = 1 \vee \mathsf{rabt} = 1 \vee \mathsf{cor} = 1] \approx$$
$$Pr[\mathsf{sabt}'' = 1 \vee \mathsf{rabt}'' = 1 \vee \mathsf{cor}'' = 1]$$

is satisfied. Since S does not abort,

$$Pr[\mathsf{sabt} = 1 \wedge \mathsf{dsabt} = 0] \approx Pr[\mathsf{sabt}'' = 1 \wedge \mathsf{dsabt}'' = 0]$$

is satisfied. For a correct execution,

$$Pr[\mathsf{sabt} = 0] = 0,$$

thus

$$Pr[\mathsf{sabt} = 0 \wedge \mathsf{dsabt} = 1] = 0.$$

Since R can give a false proof,

$$Pr[\mathsf{sabt}'' = 0 \wedge \mathsf{dsabt}'' = 1] \succ 0.$$

Thus,

$$U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)})) <$$
$$U_S^{Com(k)}((S_C^{(k)}, S_O^{(k)}), (R_C^{''(k)}, R_O^{''(k)}))$$

holds from R-5, that is, $((S_C^{(k)}, S_O^{(k)}), (R_C^{(k)}, R_O^{(k)}))$ is not a Nash equilibrium. □

V. Conclusion

Under a realistic model that cost for communication and computation is non-negligible, this paper showed that conventional bit commitment protocols are not game-theoretically secure, and abort detection property is necessary for bit commitment protocols to achieve game-theoretic security. Further study includes considering game-theoretical security of other important cryptographic protocols.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number 26330019.

References

[1] S. Even and Y. Yacobi, "Relations among public key signature systems," Technical Report 175, Technion, Haifa, Israel, Tech. Rep., 1980.

[2] J. Katz, "Bridging game theory and cryptography: Recent results and future directions," in *Theory of Cryptography*. Springer, 2008, pp. 251–272.

[3] J. Halpern and V. Teague, "Rational secret sharing and multiparty computation," in *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*. ACM, 2004, pp. 623–632.

[4] S. D. Gordon and J. Katz, "Rational secret sharing, revisited," in *Security and Cryptography for Networks*. Springer, 2006, pp. 229–241.

[5] G. Asharov, R. Canetti, and C. Hazay, "Towards a game theoretic view of secure computation," in *Advances in Cryptology–EUROCRYPT 2011*. Springer, 2011, pp. 426–445.

[6] H. Higo, K. Tanaka, A. Yamada, and K. Yasunaga, "A game-theoretic perspective on oblivious transfer," in *Information Security and Privacy*. Springer, 2012, pp. 29–42.

[7] H. Higo, K. Tanaka, and K. Yasunaga, "Game-theoretic security for bit commitment." in *IWSEC*. Springer, 2013, pp. 303–318.

[8] K.-M. Chung, F.-H. Liu, C.-J. Lu, and B.-Y. Yang, "Efficient string-commitment from weak bit-commitment," in *Advances in Cryptology-ASIACRYPT 2010*. Springer, 2010, pp. 268–282.

[9] O. Goldreich, *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge university press, 2001, vol. 1.

[10] D. Fudenberg and J. Tirole, *Game Theory*, ser. MIT Press Books. The MIT Press, December 1991, vol. 1, no. 0262061414.

[11] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic game theory*. Cambridge University Press, 2007.