Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 85 (2006)

Using Quantum Oblivious Transfer for Cheat Sensitive Quantum Bit Commitment

Andreas Jakoby[1], **Maciej Liśkiewicz**[1], and **Aleksander Mądry**[2]

[1] Institut für Theoretische Informatik, Universität zu Lübeck, Germany

[2] Institute of Computer Science, University of Wrocław, Poland

Abstract

We investigate two-party cryptographic protocols, called cheat sensitive protocols, which guarantee that if one party cheats then the other has good probability of detecting the mistrustful party. We give quantum protocols for two basic cryptographic primitives: bit commitment and one-out-of-two oblivious transfer ($\binom{2}{1}$-OT), and prove that they are cheat sensitive. For the quantum bit commitment scheme we show that if a cheating gives ε advantage i.e. information about the committed bit then the committer can detect the cheating with a probability $\Omega(\varepsilon^2)$; If the committer cheats trying to change his mind during the revealing phase then the probability of detecting the cheating is greater than some fixed constant $\lambda > 0$. This improves the probabilities of cheating detections shown by Hardy and Kent [Phys.Rev.Lett.'04], as well as the scheme by Aharonov et al. [Proc. STOC'00] who presented a protocol that is sensitive against cheating by one party, but not both parties at the same time. Our cheat sensitive quantum $\binom{2}{1}$-OT protocol guarantees that if cheating gives any mistrustful party ε advantage then the other party can detect the cheating with a probability $\Omega(\varepsilon^2)$.

The heart of the both cheat-sensitive protocols is a weakened version of quantum $\binom{2}{1}$-OT which we call *susceptible* quantum $\binom{2}{1}$-OT. In this version, similarly as in the standard definition, Alice has initially secret bits a_0, a_1 and Bob has a secret selection bit i and if both parties are honest they solve the $\binom{2}{1}$-OT problem fulfilling the standard security requirements. However, if Alice is dishonest and she gains some information about the secret selection bit then the probability that Bob computes the correct value is proportionally small. Moreover, if Bob is dishonest and he learns something about both bits, then he is not able to gain full information about one of them.

ISSN 1433-8092

1 Introduction

In bit commitment protocol Bob commits a bit b to Alice in such a way that Alice learns nothing (in an information theoretic sense) about b during this phase and later on, at the revealing time, Bob cannot change his mind. It is well known that unconditionally secure bit commitment is impossible even when the parties use quantum communication protocols ([10, 11]). Thus, much effort has been focused on schemes using some weakened security assumptions.

In a weak variant of quantum bit commitment, introduced independently by Aharonov et al. [2] and Hardy and Kent [8], the protocol should guarantee that if one party cheats then the other has good probability of detecting the mistrustful party. Speaking more precisely, we require that if Bob changes his mind during the revealing phase then Alice detects the cheating with a positive probability (we call this property *binding*) and if Alice learns information about the committed bit before the revealing time then Bob discovers the leakage of information with positive probability (*sealing* property).

In [8] Hardy and Kent give protocol that is simultaneously sealing and binding and prove that if Alice (Bob) uses a strategy giving $\varepsilon > 0$ advantage then Bob (Alice, resp.) can detect the cheating with a probability strictly greater then 0. The authors do not analyze, however, the quantitative dependence of the probability on ε. In [2] Aharonov et al. present a similar protocol to that proposed in [8] such that after depositing phase either Alice or Bob challenges the other party and (1) when Alice asks Bob to reveal b and Bob influences the value with advantage ε then she detects the cheating with probability $\Omega(\varepsilon^2)$ and (2) when Bob challenges Alice to return the depositing qubit and Alice predicts b with advantage ε then Bob detects the cheating with probability $\Omega(\varepsilon^2)$. Thus the protocol is either binding or sealing, but not simultaneously both (the authors therefore call the protocol a quantum bit escrow). Aharonov et al. left open whether simultaneous binding and sealing can be achieved.

In our paper we give the first, up to our knowledge, QBC scheme that is simultaneously binding and sealing such that if Alice's cheating gives ε advantage then Bob can detect the cheating with a probability which is $\Omega(\varepsilon^2)$. If Bob cheats (anyhow) then Alice's probability of detecting the cheating is greater than some fixed constant $\lambda > 0$, i.e. when Bob decides to set the value b to 0 or to 1 and in the revealing time wants to change his mind then for any strategy Bob uses the probability that Alice detects this attack is greater than λ.

In the one-out-of-two oblivious transfer problem ($\binom{2}{1}$-OT, for short) Alice has initially two secret bits a_0, a_1 and Bob has a secret selection bit i. The aim of a $\binom{2}{1}$-OT protocol is disclosing the selected bit a_i to Bob, in such a way that Bob gains no further information about the other bit and Alice learns nothing at all. The problem has been proposed by Even et al. [7], as a generalization of Rabin's notion for oblivious transfer [12]. Oblivious transfer is a primitive of central importance particularly in secure two-party and multi-party computations. It is well known ([9, 4]) that $\binom{2}{1}$-OT can be used as a basic component to construct protocols solving more sophisticated tasks of secure computations such as two-party oblivious circuit evaluation. Several secure OT protocols has been proposed in the literature [3, 5, 6] however, even in quantum world, there exists no unconditionally secure protocol for $\binom{2}{1}$-OT (see e.g. [11]). In our paper we construct an $\binom{2}{1}$-OT scheme such that if one party cheats then the other has good probability of detecting the cheater.

The core of the both cheat-sensitive protocols is a version of quantum $\binom{2}{1}$-OT which we call *susceptible* quantum $\binom{2}{1}$-OT. Similarly as in the standard definition, in a susceptible $\binom{2}{1}$-OT protocol Alice has initially secret bits a_0, a_1 and Bob has a secret selection bit i and if both parties are honest[1] they solve the $\binom{2}{1}$-OT problem fulfilling the standard requirements. However if Alice is dishonest and she gains some information about the secret selection bit then the probability that Bob computes the correct value is proportionally decreased. Moreover, if Bob is dishonest he can learn about both bits, but if he does so then he is not able to gain full information about one of them.

In the paper we present a susceptible $\binom{2}{1}$-OT protocol which, speaking informally (precise definitions will be given in Section 3), fulfills the following properties.

- If both Alice having initially bits a_0, a_1 and Bob having bit i are honest then Bob learns the selected bit a_i, but he gains no further information about the other bit and Alice learns nothing.
- If Bob is honest and has a bit i and Alice learns i with advantage ε then for all $a_0, a_1 \in \{0,1\}$ the probability that Bob computes the correct value a_i, when the protocol completes, is at most $1 - \Omega(\varepsilon^2)$.
- If Alice is honest and has bits a_0, a_1 then for every $i \in \{0,1\}$ it is true that if Bob can predict the value a_{1-i} with advantage ε then the probability that Bob learns correctly a_i is at most $1 - \Omega(\varepsilon^2)$.

The protocol can be used e.g. by the mistrustful parties for which computing the correct result of $\binom{2}{1}$-OT is much more preferential than gaining addition information. In this paper we show, however, an application of the protocol for parties who may be not interested in computing the correct value at all. A key property of the protocol, which will be used for detecting a cheating, is that when the protocol is finished then the probability that a dishonest party constructs input values which are consistent with the result and the given input of the other party is proportionally small. Let us consider the following bit commitment protocol, where $v := OT((a_0, a_1), i)$ means, for short, that Alice having initially a_0, a_1 and Bob knowing i perform the susceptible $\binom{2}{1}$-OT protocol and when the protocol completes Bob knows the result v.

Protocol 1 (Cheat Sensitive QBC) *B commits bit b;*

- **Depositing Phase**
  1. *A chooses randomly bits a_0, a_1, a_2, a_3; B chooses randomly bits $\hat{b}$ and c;*
  2. *A and B compute*
     $v_0 := OT((a_0, a_1), \hat{b});\ v_1 := OT((a_2, a_3), b)$ *if* $c = 0$ *or*
     $v_0 := OT((a_0, a_1), b);\ v_1 := OT((a_2, a_3), \hat{b})$ *if* $c = 1$.
  3. *B reveals c.*
- **Revealing Phase** *B reveals b;*
  ○ *Binding test: B sends to A v_{1-c}; A rejects when $v_{1-c} \neq OT((a_{2-2c}, a_{3-2c}), b)$.*
  ○ *Sealing test: A sends to B a_{2c}, a_{2c+1}; B rejects when $v_c \neq OT((a_{2c}, a_{2c+1}), \hat{b})$.*

One of the main results of this paper says that using our susceptible $\binom{2}{1}$-OT protocol, the bit commitment protocol above fulfills simultaneously the binding and sealing property.

As a second application we give a cheat sensitive protocol for the $\binom{2}{1}$-OT function:

Protocol 2 (Cheat Sensitive QOT) Input *A: $m_0, m_1 \in \{0,1\}$, B: $b \in \{0,1\}$;* Result *B: m_b.*

1. **Quantum Phase** *A chooses randomly bits a_0, a_1 and B chooses randomly bit i; then A and B compute $v := OT((a_0, a_1), i)$;*

[1] We say that a party is honest if it never deviates from the given protocol.

2. **Test Phase** *A chooses randomly bit* `A_tests` *and B chooses randomly bit* `B_tests`*;*
   A and B exchange the values `A_tests` *and* `B_tests`*: A sends first and B sends next;*
   Go to the Computation Phase when nobody wants to test i.e. if `A_tests` $=$ `B_tests` $= 0$*;*
   If `A_tests` $= 1$ *then B sends v, i to A;*
   If `A_tests` $= 0 \ \wedge$ `B_tests` $= 1$ *then A sends a_0, a_1 to B;*
   If $v \neq OT((a_0, a_1), i)$ the parties reject and otherwise go to the Quantum Phase.

3. **Computation Phase** *B sends $c := i \oplus b$ to A. Then A sends $a_0 \oplus m_c, a_1 \oplus m_{1 \oplus c}$ to B and B computes $v \oplus a_c \oplus m_b = m_b$.*

We prove that using the susceptible $\binom{2}{1}$-OT protocol as a black-box, the protocol above has the following properties: (1) if both Alice and Bob are honest then the protocol fulfills the standard security requirements for $\binom{2}{1}$-OT; (2) if Alice learns b with advantage ε then Bob detects cheating with probability $\Omega(\varepsilon^2)$, and (3) if Bob learns about m_0, m_1 with advantages $\varepsilon_0, \varepsilon_1$, resp. then Alice detects cheating with probability $\Omega(\varepsilon^2)$, where $\varepsilon = \min\{\varepsilon_0, \varepsilon_1\}$.
The paper is organized as follows. In Section 2 some basic quantum preliminaries are given. In Section 3 we define formally properties of a susceptible $\binom{2}{1}$-OT protocol and prove that the given scheme fulfills the properties. Section 4 gives formal definition of binding and sealing and proves that Protocol 1 is simultaneously binding and sealing. In Section 5 we will introduce the notion of cheat sensitive QOT and analyze Protocol 2.

2 Preliminaries

The model of two-party computation we use in this paper is essentially the same as defined in [2]. We assume that the reader is already familiar with basics of quantum cryptography (see [2] for an exemplary summary of results that will be used in the following).
Let $|0\rangle$,$|1\rangle$ be an encoding of classical bits in our computational (perpendicular) basis. Let $|0_\times\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $|1_\times\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ be an encoding of classical bits in diagonal basis. By R_α, $\alpha \in \{0, \frac{1}{2}, 1\}$, we denote the unitary operation of rotation by an angle of $\alpha \cdot \pi/2$. More formally:

$$R_\alpha := \begin{pmatrix} \cos(\alpha \cdot \frac{\pi}{2}) & \sin(\alpha \cdot \frac{\pi}{2}) \\ -\sin(\alpha \cdot \frac{\pi}{2}) & \cos(\alpha \cdot \frac{\pi}{2}) \end{pmatrix}$$

We should note that this operation allows us to exchange between the bit encoding in perpendicular and in diagonal basis. Moreover, by applying R_1 we can flip the value of the bit encoded in any of those two bases.
For a mixed quantum state ρ and a measurement $\mathcal{O}$ on ρ, let $\rho^{\mathcal{O}}$ denote the classical distribution on the possible results obtained by measuring ρ according to $\mathcal{O}$, i.e. $\rho^{\mathcal{O}}$ is some distribution $p_1, \ldots, p_t$ where p_i denotes the probability that we get result i. We use L_1-norm to measure distance between two probability distributions $p = (p_1, \ldots, p_t)$ and $q = (q_1, \ldots, q_t)$ over the same domain: $|p - q|_1 = \frac{1}{2}\sum_{i=1}^{t} |p_i - q_i|$.
Let $||A||_t = \mathrm{tr}(\sqrt{A^\dagger A})$, where $\mathrm{tr}(A)$ denotes trace of matrix A. A fundamental theorem gives us a bound on L_1-norm for the probability distributions on the measurement results:

Theorem 1 (see [1]) *Let ρ_0, ρ_1 be two density matrices on the same Hilbert space $\mathcal{H}$. Then for any generalized measurement $\mathcal{O}$ $|\rho_0^{\mathcal{O}} - \rho_1^{\mathcal{O}}|_1 \leq \frac{1}{2}||\rho_0 - \rho_1||_t$. This bound is tight and the orthogonal measurement $\mathcal{O}$ that projects a state on the eigenvectors of $\rho_0 - \rho_1$ achieves it.*

A well-known result states that if $|\phi_1\rangle$, $|\phi_2\rangle$ are pure states, then $||\ |\phi_1\rangle\langle\phi_1| - |\phi_2\rangle\langle\phi_2|\ ||_t = 2\sqrt{1 - |\langle\phi_1|\phi_2\rangle|^2}$.

Lemma 1 *Suppose Bob has a bit b s.t.* $\Pr[b=0]=1/2$ *and let Alice generate a state with two quantum registers. Assume she sends the second register to Bob, then Bob depending on b makes some transformation on his part and sends the result back to Alice. Denote by ρ_0 density matrix of the resulting state for $b=0$ and by ρ_1 density matrix of the state for $b=1$. Then for any measurement $\mathcal{O}$ Alice makes and a value v Alice learns we have* $\Pr_{b\in_R\{0,1\}}[v=b] \ \le\ 1/2+\frac{|\rho_0^{\mathcal{O}}-\rho_1^{\mathcal{O}}|_1}{2}$.

The proof of this lemma follows by some straight forward calculations and will be skipped in this extended abstract. We will use some obvious variations of this lemma to bound the advantage of Alice resp. Bob in what will follow.

3 Susceptible Oblivious Transfer

In this section we give the formal definition of the susceptible $\binom{2}{1}$-OT protocol and then present a protocol for this problem[2].

Definition 1 *We say that a two-party quantum protocol between Alice and Bob is a (δ,ε)-susceptible $\binom{2}{1}$-OT protocol if the following requirements hold.*

- *If both Alice depositing initially bits a_0, a_1 and Bob having bit i are honest then Bob learns the selected bit a_i but in such a way that he gains no further information about the other bit and Alice learns nothing.*
- *Whenever Bob is honest and has a selection bit i, with* $\Pr[i=0]=1/2$, *then for every strategy used by Alice, every value i' Alice learns about i and for any value a' Bob learns at the end of the computation it holds that for all* $a_0, a_1 \in \{0,1\}$
$$\textit{if } \Pr_{i\in_R\{0,1\}}[i'=i]\ge 1/2+\delta \quad \textit{then } \Pr_{i\in_R\{0,1\}}[a'=a_i]\le 1-\varepsilon.$$
- *Whenever Alice is honest and deposits bits a_0, a_1, with* $\Pr[a_i=0]=1/2$, *then for every strategy used by Bob, all values a'_0, a'_1 Bob learns about a_0, a_1, resp. it holds that for all* $i\in\{0,1\}$ *if* $\Pr_{a_0,a_1\in_R\{0,1\}}[a'_{1-i}=a_{1-i}]\ge 1/2+\delta$ *then* $\Pr_{a_0,a_1\in_R\{0,1\}}[a'_i=a_i]\le 1-\varepsilon$.

Protocol 3 (Susceptible QOT) Input $A: a_0, a_1\in\{0,1\}, B: i\in\{0,1\}$; Output $B: a_i$.
1. *A chooses randomly $\alpha\in_R\{0,\frac{1}{2}\}$ and $h\in_R\{0,1\}$ and sends to B:*
$$R_\alpha|a_1\oplus h\rangle\otimes R_\alpha|a_0\oplus h\rangle$$
2. *B receives $|\Phi_1\rangle\otimes|\Phi_0\rangle$, chooses randomly $\beta\in_R\{0,1\}$ and sends $R_\beta|\Phi_i\rangle$ back to A.*
3. *A receives $|\Phi\rangle$, computes $R_\alpha^{-1}|\Phi\rangle$, measures the state in computational basis obtaining the result n and sends $m=n\oplus h$ to B.*
4. *B receives m and computes $a_i=m\oplus\beta$.*

Here, as usually, $\oplus$ denotes xor. To see that this protocol computes $\binom{2}{1}$-OT correctly if both parties are honest we remind that the operator $R_\alpha R_\beta$ commutes with R_α^{-1} (this is not true in general, although it is true in 2D) and that R_β is (up to a phase) a NOT-gate conditioned on β. We will now focus on the question whether Protocol 3 still retains security if we use it against malicious parties. The following theorem follows from Lemma 2 and 3 which will be proven in the remaining part of this section:

Theorem 2 *Protocol 3 is $(O(\sqrt[2]{\varepsilon}),\varepsilon)$-susceptible $\binom{2}{1}$-OT protocol.*

[2] The requirements of the susceptible oblivious transfer given in Definition 1 *may seem* to contradict each other if one follows the Lo and Chau's argument not carefully enough [10]. For additional remarks see Section A in the Appendix.

3.1 Malicious Alice

Lemma 2 *Let Alice and Bob perform Protocol 3 and assume Bob is honest and deposits a bit i, with* $\Pr[i=0]=1/2$. *Then for every strategy used by Alice, every value i' Alice learns about i and for any value a' Bob learns at the end of the computation it holds that for all $a_0, a_1 \in \{0,1\}$ if* $\Pr_{i \in_R \{0,1\}}[a' = a_i] \geq 1 - \varepsilon$ *then* $\Pr_{i \in_R \{0,1\}}[i' = i] \leq 1/2 + 16\sqrt{\varepsilon}$.

Proof: Any cheating strategy $\mathcal{A}$ of Alice can be described as preparing some state $|\Phi\rangle = \sum_{x \in \{0,1\}^2} |v_x, x\rangle$, sending the two rightmost qubits to Bob and perform some measurement $\{H_0, H_1, H_2, H_3\}$ on this what she gets back after Bob's round, where H_0,H_1,H_2, H_3 are four pairwise orthogonal subspaces being a division of whole Hilbert space that comes into play, such that, for $l, k = 0, 1$, if our measurement indicates the outcome corresponding to H_{2k+l} then it reflects Alice's belief that $i = l$ and that the message $m = k$ should be sent to Bob.
Assume now, that $a_0 \oplus a_1 = 0$. We should note that in this case $m \oplus a_0 = \beta$. So Alice, in order to ensure the correct result of the protocol, has to indicate the value of β. Let $|S\rangle = |v_{00}, 00\rangle + |v_{11}, 11\rangle$, $|A\rangle = |v_{01}, 01\rangle + |v_{10}, 10\rangle$. That is, $|S\rangle$ is a part of the state that is symmetric with respect to qubits being sent to Bob and $|A\rangle$ is the rest being anti-symmetric. Let $\rho_{a,b}$ be a density matrix of Alice's system after Bob's round, corresponding to $i = a$ and $\beta = b$. After some calculations we get:

$$\begin{array}{rcl}
\rho_{0,0} & = & \sum_{x=(x_1,x_2)\in\{0,1\}^2} |v_x x_1\rangle\langle v_x x_1| \\
& & +|v_{00}0\rangle\langle v_{10}1| + |v_{10}1\rangle\langle v_{00}0| + |v_{11}1\rangle\langle v_{01}0| + |v_{01}0\rangle\langle v_{11}1| \\
\rho_{0,1} & = & \sum_{x=(x_1,x_2)\in\{0,1\}^2} |v_x \overline{x_1}\rangle\langle v_x \overline{x_1}| \\
& & -|v_{00}1\rangle\langle v_{10}0| - |v_{10}0\rangle\langle v_{00}1| - |v_{11}0\rangle\langle v_{01}1| - |v_{01}1\rangle\langle v_{11}0| \\
\rho_{1,0} & = & \sum_{x=(x_1,x_2)\in\{0,1\}^2} |v_x x_2\rangle\langle v_x x_2| \\
& & +|v_{00}0\rangle\langle v_{01}1| + |v_{01}1\rangle\langle v_{00}0| + |v_{11}1\rangle\langle v_{10}0| + |v_{10}0\rangle\langle v_{11}1| \\
\rho_{1,1} & = & \sum_{x=(x_1,x_2)\in\{0,1\}^2} |v_x \overline{x_2}\rangle\langle v_x \overline{x_2}| \\
& & -|v_{00}1\rangle\langle v_{01}0| - |v_{01}0\rangle\langle v_{00}1| - |v_{11}0\rangle\langle v_{10}1| - |v_{10}1\rangle\langle v_{11}0| \; .
\end{array}$$

where $\overline{x_t}$ means flipping bit x_t, i.e. $\overline{x_t} = 1 - x_t$.
We look first onto possibilities of Alice's dishonest behaviour. In order to cheat, Alice has to distinguish between density matrices $\gamma_l = \frac{1}{2}\rho_{l,0} + \frac{1}{2}\rho_{l,1}$, where γ_l corresponds to $i = l$. By examination of the difference of those matrices we get after some calculations that:

$$\gamma_0 - \gamma_1 = \frac{1}{2}|V_S 0\rangle\langle V_A 1| + \frac{1}{2}|V_A 1\rangle\langle V_S 0| - \frac{1}{2}|V_S 1\rangle\langle V_A 0| - \frac{1}{2}|V_A 0\rangle\langle V_S 1|$$

where $|V_S\rangle = |v_{00}\rangle + |v_{11}\rangle$ and $|V_A\rangle = |v_{10}\rangle - |v_{01}\rangle$. We can easily adapt Lemma 1 to show that the advantage δ of Alice is at most $\sum_{l=0}^{3} \sigma_l$ where

$$\begin{array}{rcl}
\sigma_l \; = \; |\mathrm{tr}(H_l(\gamma_0 - \gamma_1)H_l{}^\dagger)| & \leq & \sum_{j\in\{0,1\}} \frac{1}{2}|tr(H_l(|V_S(j-1)\rangle\langle V_A j| + |V_A j\rangle\langle V_S(j-1)|)H_l{}^\dagger)| \\
& \leq & \sum_{j\in\{0,1\}}(|\langle O_j^l|V_A j\rangle| \cdot |\langle V_S(1-j)|O_j^l\rangle|) \\
& \leq & \sum_{j\in\{0,1\}} |\langle O_j^l|V_A j\rangle|
\end{array}$$

and $|O_j^l\rangle$ is an orthogonal, normalized projection of $|V_A j\rangle$ onto subspace H_l. The second inequality is true because we have $\mathrm{tr}(H_l|V_A j\rangle\langle\psi|H_l{}^\dagger) = \langle O_j^l|V_A j\rangle\langle\psi|O_j^l\rangle$ for every state $|\psi\rangle$.
Let j_l be the index for which $|\langle O_{j_l}^l|V_A j_l\rangle| \geq |\langle O_{1-j_l}^l|V_A(1-j_l)\rangle|$. Clearly, $\sigma_l \leq 2|\langle O_{j_l}^l|V_A j_l\rangle|$. Moreover, we assume that $\sigma_0 + \sigma_1 \geq \sigma_2 + \sigma_3$. If this is not the case we could satisfy this condition by altering the strategy $\mathcal{A}$ of Alice (by appropriate rotation of her basis) in such a way that the definitions of H_k and H_{k+2} would swap leaving everything else unchanged.

We look now on the probability of obtaining the correct result by Alice. The probability p_0 of Alice getting outcome $\beta = 0$ in case of $\beta = 1$ is at least

$$\begin{aligned} p_0 \geq \tfrac{1}{2}\langle O^0_{j_0}|\rho_{0,1}|O^0_{j_0}\rangle + \tfrac{1}{2}\langle O^0_{j_0}|\rho_{1,1}|O^0_{j_0}\rangle = \\ \tfrac{1}{2}|\langle O^0_{j_0}|v_{00}1\rangle - \langle O^0_{j_0}|v_{01}0\rangle|^2 + \tfrac{1}{2}|\langle O^0_{j_0}|v_{00}1\rangle - \langle O^0_{j_0}|v_{10}0\rangle|^2 \\ +\tfrac{1}{2}|\langle O^0_{j_0}|v_{11}0\rangle - \langle O^0_{j_0}|v_{01}1\rangle|^2 + \tfrac{1}{2}|\langle O^0_{j_0}|v_{11}0\rangle - \langle O^0_{j_0}|v_{10}1\rangle|^2 \ . \end{aligned}$$

So, by inequality $|a-b|^2 + |a-c|^2 \geq \frac{1}{2}|b-c|^2$ we get that

$$\begin{aligned} p_0 \ &\geq \ \tfrac{1}{4}|\langle O^0_{j_0}|v_{01}0\rangle - \langle O^0_{j_0}|v_{10}0\rangle|^2 + \tfrac{1}{4}|\langle O^0_{j_0}|v_{01}1\rangle - \langle O^0_{j_0}|v_{10}1\rangle|^2 \\ &= \ \tfrac{1}{4}|\langle O^0_{j_0}|V_A0\rangle|^2 + \tfrac{1}{4}|\langle O^0_{j_0}|V_A1\rangle|^2 \ \geq \ \tfrac{1}{16}\sigma_0^2. \end{aligned}$$

Similar calculation of the probability p_1 of getting outcome $\beta = 1$ in case of $\beta = 0$ yields that the probability of computing wrong result is at least

$$\Pr[\beta' \neq \beta] = \Pr[\beta \oplus m \neq a_i] \geq \frac{1}{16}(\sigma_0^2 + \sigma_1^2) \geq \frac{1}{256}(\sum_{l=0}^{3} \sigma_l)^2.$$

Hence, the lemma holds for the case $a_0 \oplus a_1 = 0$.

Since in case of $a_0 \oplus a_1 = 1$ the reasoning is completely analogous - we exchange only the roles of $|V_S\rangle$ and $|V_A\rangle$ and Alice has to know the value of $\beta \oplus i$ in order to give the correct answer to Bob, the proof is concluded. ■

To see that quadratical bound imposed by the above lemma can be met, consider $|\Phi\rangle = \sqrt{1-\varepsilon}|000\rangle + \sqrt{\varepsilon}|110\rangle$. Intuitively, we label the symmetric and anti-symmetric part of $|\Phi\rangle$ with 0 and 1. Let $H_2 = |01\rangle\langle 01|$, $H_3 = 0$. One can easily calculate that

$$\rho_{0,0} = (1-\varepsilon)|00\rangle\langle 00| + \sqrt{\varepsilon(1-\varepsilon)}(|00\rangle\langle 11| + |11\rangle\langle 00|) + \varepsilon|11\rangle\langle 11|$$

$$\rho_{1,0} = (1-\varepsilon)|00\rangle\langle 00| + \varepsilon|10\rangle\langle 10|$$

and therefore $||\rho_{0,0} - \rho_{1,0}||_t \geq \sqrt{\varepsilon(1-\varepsilon)} - 2\varepsilon$. So, by Theoren 1 there exists a measurement $\{H_0, H_1\}$ allowing us to distinguish between those two density matrices with $\sqrt{\varepsilon(1-\varepsilon)} - 2\varepsilon$ accuracy and moreover $H_2, H_3 \perp H_0, H_1$ since $\mathrm{tr}(H_2\rho_{0,0}H_2^\dagger) = \mathrm{tr}(H_2\rho_{1,0}H_2^\dagger) = 0$. Now, let $M = \{H_0, H_1, H_2, H_3\}$ be Alice's measurement. To cheat, we use the following strategy $\mathcal{A}$ corresponding to her input $a_0 = a_1 = 0$. Alice sends $|\Phi\rangle$ to Bob, after receiving the qubit back she applies the measurement M. If the outcome is H_2 then she answers $a_0 \oplus \beta = 1$ to Bob and sets $i' = 0$ with probability $\frac{1}{2}$, in the other case she sends $a_0 \oplus \beta = 0$ to Bob and according to the outcome being 0 or 1 she sets $i' = 0$ ($i' = 1$).

To see that this strategy gives correct result with probability greater than $1 - \varepsilon$ we should note that probability of outcome H_2 in case of $\beta = 0$ is 0 and in case of $\beta = 1$ is $1 - \varepsilon$. Therefore, since $\beta = 0$ with probability $\frac{1}{2}$, our advantage in determining the input of Bob is greater than $\frac{1}{2}\sqrt{\varepsilon} - \frac{3}{2}\varepsilon$.

Remark 1 The need for the property provided by Lemma 2 was motivated primary by a scenario in which, like in private computations, the involved parties try to gain knowledge about the inputs of the other parties but attempting to compute the correct value. Use of Protocol 3 for cheat sensitive computations needs, however, a stronger property which says that for any dishonest Alice if the protocol is finished then she is not able to determine values $\tilde{a}_0, \tilde{a}_1$ which are consistent with Bob's input i and the value a' he decides at the end of the protocol. To this aim we will use the following stronger version of the lemma: *for i, i', and a' as in the lemma it holds that if $\Pr_{i \in_R \{0,1\}}[i' = i] \geq 1/2 + 16\sqrt{\varepsilon}$ then for all values $\tilde{a}_0, \tilde{a}_1$ which Alice determine after the protocol is finished it is true that $\Pr_{i \in_R \{0,1\}}[a' = \tilde{a}_i] \leq 1 - \varepsilon$.*

To see that the stronger version of Lemma 2 holds, we should note that from the lemma it follows immediately that for all $a_0, a_1 \in \{0,1\}$ if $\Pr_{i \in_R \{0,1\}}[i' = i] \geq 1/2 + 16\sqrt{\varepsilon}$ then $\varepsilon \leq \Pr_{i \in_R \{0,1\}}[a' = a_i] \leq 1 - \varepsilon$. In fact, if for any Alice's strategy $\Pr_{i \in_R \{0,1\}}[a' = a_i] < \varepsilon$ for some input a_0, a_1 then Alice can modify this strategy for the input a_0, a_1 in such a way that in the last round she sends to Bob $1 - m$ instead of m. This leads, however, to a contradiction since for the modified strategy and the input a_0, a_1 it holds that $\Pr_{i \in_R \{0,1\}}[a' = a_i] > 1 - \varepsilon$. Thus assuming Alice's advantage is greater than $16\sqrt{\varepsilon}$ we get that for any value $\tilde{a}$ Alice can determine, both $\varepsilon \leq \Pr_{i \in_R \{0,1\}}[a' = \tilde{a}] \leq 1 - \varepsilon$ and $\varepsilon \leq \Pr_{i \in_R \{0,1\}}[a' \neq \tilde{a}] \leq 1 - \varepsilon$ are true.

3.2 Malicious Bob

Now, we analyze Bob's possibility of cheating.

Lemma 3 *Let Alice and Bob perform Protocol 3. Assume Alice is honest and deposits bits a_0, a_1, with $\Pr[a_i = 0] = 1/2$. Then for every strategy used by Bob and all values a'_0, a'_1 which Bob learns about a_0, a_1, it holds that: for all $i \in \{0,1\}$*

$$\textit{if } \Pr_{a_0, a_1 \in_R \{0,1\}}[a'_i = a_i] \geq 1 - \varepsilon^2 \quad \textit{then } \Pr_{a_0, a_1 \in_R \{0,1\}}[a'_{1-i} = a_{1-i}] \leq 1/2 + 16\sqrt{2}\varepsilon.$$

Proof: Consider some malicious strategy $\mathcal{B}$ of Bob. Wlog we may assume that the probability of $a'_0 = a_0$ is greater than the probability of $a'_1 = a_1$. Our aim is to show that

$$\text{if } \Pr_{a_0, a_1 \in_R \{0,1\}}[a'_0 \neq a_0] \leq \varepsilon^2 \quad \text{then } \Pr_{a_0, a_1 \in_R \{0,1\}}[a'_1 = a_1] \leq 1/2 + 16\sqrt{2}\varepsilon.$$

Strategy $\mathcal{B}$ can be think of as a two step process. First a unitary transformation U is acting on $|\Phi_{a_0,a_1,h}\rangle = |v\rangle \otimes R_\alpha |a_1 \oplus h\rangle \otimes R_\alpha |a_0 \oplus h\rangle$, where v is an ancillary state[3]. Next the last qubit of $U(|\Phi_{a_0,a_1,h}\rangle)$ is sent to Alice[4], she performs step 3 on these qubit and sends the classical bit m back to Bob. Upon receiving m, Bob executes the second part of his attack: he performs some arbitrary measurement $\{H_0, H_1, H_2, H_3\}$, where H_0 (H_1) corresponds to Bob's belief that $a_0 = 0, a_1 = 0$ (resp. $a_0 = 0, a_1 = 1$) and H_2 (H_3) corresponds to $a_0 = 1$ and $a_1 = 0$ (resp. $a_0 = 1$ and $a_1 = 1$). In other words, outcome corresponding to H_{2l+k} implies $a'_0 = l$ and $a'_1 = k$.

The unitary transformation U can be described by a set of vectors $\{V_k^{l,j}\}$ such that $U(|v\rangle \otimes |l, j\rangle) = |V_0^{l,j}\rangle \otimes |0\rangle + |V_1^{l,j}\rangle \otimes |1\rangle$. Or alternatively in diagonal basis, by a set of vectors $\{W_k^{l,j}\}$ such that $U(|v\rangle \otimes |l_\times, j_\times\rangle) = |W_0^{l,j}\rangle \otimes |0_\times\rangle + |W_1^{l,j}\rangle \otimes |1_\times\rangle$.

We present now, an intuitive, brief summary of the proof. Informally, we can think of U as about some kind of disturbance of the qubit $R_\alpha |a_0 \oplus h\rangle$ being sent back to Alice. First, we will show that in order to cheat Bob's U has to accumulate after Step 2, till the end of the protocol, some information about the value of $a_0 \oplus h$ hidden in this qubit. On the other hand, to get the proper result i.e. the value of a_0, this qubit's actual information about encoded value has to be disturbed at the smallest possible degree. That implies for Bob a necessity of some sort of cloning that qubit, which turns out to impose the desired bounds on possible cheating. We show this by first reducing the task of cloning to one where no additional hint in the form of $R_\alpha |a_1 \oplus h\rangle$ is provided and then an analysis of this simplified process. Therefore, the proof indicates that the hardness of cheating the protocol is contained in the necessity of cloning, which gives us a sort of quantitative non-cloning theorem. Although, it seems to

[3] Note that this does not restrict Bob's power. Particularly, when Bob tries to make a measurement in the first step then using standard techniques we can move this measurement to the second step.

[4] We can assume wlog that the last qubit is sent since U is arbitrary.

concern only our particular implementation of the protocol, we believe that this scenario is useful enough to be of independent interests.

We analyze first Bob's information gain about a_1. Wlog we may assume that Bob can distinguish better between two values of a_1 if $a_0 = 0$. That is

$$\Pr_{a_1 \in_R \{0,1\}}[a_1' = a_1 | a_0 = 0] \geq \Pr_{a_1 \in_R \{0,1\}}[a_1' = a_1 | a_0 = 1].$$

Let now $\rho_{j,k,l}$ be a density matrix of the system before Bob's final measurement, corresponding to $\alpha = j \cdot \frac{1}{2}$, $h = k$, $a_1 = l$ and $a_0 = 0$. The advantage δ of Bob in this case (i.e. δ such that $\Pr[a_1' = a_1 \mid a_0 = 0] = 1/2 + \delta$) can be estimated by Lemma 1 by Bob's ability to distinguish between the following density matrices:

$$\begin{array}{ll} \frac{1}{4}(\rho_{0,0,0} + \rho_{1,0,0} + \rho_{0,1,0} + \rho_{1,1,0}) & \text{(case } a_1 = 0\text{), and} \\ \frac{1}{4}(\rho_{0,0,1} + \rho_{1,0,1} + \rho_{0,1,1} + \rho_{1,1,1}) & \text{(case } a_1 = 1\text{).} \end{array}$$

Using the triangle inequality we get that for the measurement $\mathcal{O}$ performed by Bob

$$\delta \leq \frac{1}{8}(|\rho^{\mathcal{O}}_{0,0,0} - \rho^{\mathcal{O}}_{0,1,1}|_1 + |\rho^{\mathcal{O}}_{1,1,0} - \rho^{\mathcal{O}}_{1,0,1}|_1 + |\rho^{\mathcal{O}}_{0,1,0} - \rho^{\mathcal{O}}_{0,0,1}|_1 + |\rho^{\mathcal{O}}_{1,0,0} - \rho^{\mathcal{O}}_{1,1,1}|_1). \qquad (1)$$

Each component corresponds to different values of α and $h \oplus a_1$. And each component is symmetric to the other in such a way that there exists a straight-forward local transformation for Bob (i.e. appropriate rotation of the computational basis on one or both qubits) which transform any of above components onto another. So, we can assume wlog that the advantage in distinguishing between $\rho_{0,0,0}$ and $\rho_{0,1,1}$ $\delta_0 = |\rho^{\mathcal{O}}_{0,0,0} - \rho^{\mathcal{O}}_{0,1,1}|_1$ is the maximum component in the right-hand side of the inequality (1) and therefore we have $\delta \leq \frac{1}{2}\delta_0$. Let, for short, $\gamma_0 = \rho_{0,0,0}$ and $\gamma_1 = \rho_{0,1,1}$. One can easily calculate that

$$\begin{array}{rcll} \gamma_0 & = & |0\rangle\langle 0| \otimes |V_0^{00}\rangle\langle V_0^{00}| + |1\rangle\langle 1| \otimes |V_1^{00}\rangle\langle V_1^{00}| & (2) \\ \gamma_1 & = & |0\rangle\langle 0| \otimes |V_1^{01}\rangle\langle V_1^{01}| + |1\rangle\langle 1| \otimes |V_0^{01}\rangle\langle V_0^{01}|. & (3) \end{array}$$

As we can see to each value of m in above density matrices corresponds a pair of vectors which are critical for Bob's cheating. I.e. the better they can be distinguishable by his measurement the greater is his advantage. But, as we will see later, this fact introduces perturbation of the indication of the value of a_0.

First, we take a look on the measurements H_0, H_1 performed by Bob. Let us define σ_{2m+p} for $p, m \in \{0,1\}$ as follows

$$\sigma_{2m+p} = \begin{cases} |\mathrm{tr}(H_p|0V_p^{0p}\rangle\langle 0V_p^{0p}|H_p^\dagger) - \mathrm{tr}(H_p|0V_{1-p}^{0(1-p)}\rangle\langle 0V_{1-p}^{0(1-p)}|H_p^\dagger)| & \text{if } m = 0, \\ |\mathrm{tr}(H_p|1V_{1-p}^{0p}\rangle\langle 1V_{1-p}^{0p}|H_p^\dagger) - \mathrm{tr}(H_p|1V_p^{0(1-p)}\rangle\langle 1V_p^{0(1-p)}|H_p^\dagger)| & \text{if } m = 1. \end{cases}$$

Let for $m = 0$, $p_0 \in \{0,1\}$ be such that $\sigma_{p_0} \geq \sigma_{1-p_0}$ and similarly, for $m = 1$ let $p_1 \in \{0,1\}$ be such that $\sigma_{2+p_1} \geq \sigma_{2+(1-p_1)}$. Then we get

$$\begin{array}{rcl} |\gamma_0^{\mathcal{O}} - \gamma_1^{\mathcal{O}}|_1 & = & \sum_{t=0}^3 |\mathrm{tr}(H_t\gamma_0 H_t^\dagger) - \mathrm{tr}(H_t\gamma_1 H_t^\dagger)| \\ & \leq & 2(\sigma_{p_0} + \sigma_{2+p_1}) + \sum_{t=2}^3 |\mathrm{tr}(H_t\gamma_0 H_t^\dagger) - \mathrm{tr}(H_t\gamma_1 H_t^\dagger)|. \end{array}$$

We should see first that the second term in the above sum corresponds to advantage in distinguishing between two values of a_1 by measurement H_2, H_3 in case of $a_0 = 0$. But those subspaces reflect Bob's belief that $a_0 = 1$. Therefore, we have that

$$\sum_{t=2}^3 |\mathrm{tr}(H_t\gamma_0 H_t^\dagger) - \mathrm{tr}(H_t\gamma_1 H_t^\dagger)| \leq \Pr_{a_0, a_1 \in_R \{0,1\}}[a_0' \neq a_0 | a_0 = 0].$$

So, we can neglect this term because it is of the order of the square of the advantage (if not then our lemma would be proved). Hence we get: $\frac{\delta_0}{2} \leq \sigma_{p_0} + \sigma_{2+p_1}$.
Now, we define projection O_m as follows. For $m = 0$ let O_0 be the normalized orthogonal projection of $|0V_{p_0}^{0p_0}\rangle$ onto the subspace H_{p_0} if

$$\mathrm{tr}(H_{p_0}|0V_{p_0}^{0p_0}\rangle\langle 0V_{p_0}^{0p_0}|H_{p_0}^{\dagger}) \;\geq\; \mathrm{tr}(H_{p_0}|0V_{1-p_0}^{0(1-p_0)}\rangle\langle 0V_{1-p_0}^{0(1-p_0)}|H_{p_0}^{\dagger}).$$

Otherwise, let O_0 be the normalized orthogonal projection of $|0V_{1-p_0}^{0(1-p_0)}\rangle$ onto H_{p_0}. Analogously, we define O_1 as a normalized orthogonal projection of $|1V_{1-p_1}^{0p_1}\rangle$ onto the subspace H_{p_1} if

$$\mathrm{tr}(H_{p_1}|1V_{1-p_1}^{0p_1}\rangle\langle 1V_{1-p_1}^{0p}|H_{p_1}^{\dagger}) \;\geq\; \mathrm{tr}(H_{p_1}|1V_{p_1}^{0(1-p_1)}\rangle\langle 1V_{p_1}^{0(1-p_1)}|H_{p_1}^{\dagger})$$

else O_1 is a normalized orthogonal projection of $|1V_{p_1}^{0(1-p_1)}\rangle$ onto H_{p_1}. Hence we get

$$\sigma_{p_0} \leq ||\langle 0V_{p_0}^{0p_0}|O_0\rangle|^2 - |\langle 0V_{1-p_0}^{0(1-p_0)}|O_0\rangle|^2|, \quad \sigma_{2+p_1} \leq ||\langle 1V_{1-p_1}^{0p_1}|O_1\rangle|^2 - |\langle 1V_{p_1}^{0(1-p_1)}|O_1\rangle|^2|.$$

We would like now to investigate the probability of obtaining the correct result. Recall that $\Pr[a_1 = 0] = \frac{1}{2}$. We should first note that the density matrices corresponding to initial configuration of the second qubit $R_\alpha|a_1 \oplus h\rangle$ is now exactly $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ even if we know h and α. So, from the point of view of the protocol those two configurations are indistinguishable. Therefore, we can substitute the second qubit from the initial configuration with a random bit r encoded in perpendicular basis and the probability of obtaining proper result is unchanged. We analyze the probability of computing the correct result in case of $r = 0$. Note, that the vectors $\{V_k^{0,j}\}_{k,j}$ still describe U, but vectors $\{W_k^{0j}\}_{k,j}$ are different, defined by U acting now on initial configuration $|v\rangle \otimes |0\rangle \otimes R_\alpha|j\rangle$, with $\alpha = \frac{1}{2}$. We investigate the correspondence between $\{V_k^{0j}\}_{k,j}$ and the new vectors. For $j = 0$ we have:

$$\begin{aligned} U(|v00_\times\rangle) &= \tfrac{1}{\sqrt{2}}U(|v00\rangle - |v01\rangle) \;=\; \tfrac{1}{\sqrt{2}}(V_0^{00}|0\rangle + V_1^{00}|1\rangle - V_0^{01}|0\rangle - V_1^{01}|1\rangle) \\ &= \tfrac{1}{2}((V_0^{00} - V_1^{00} - V_0^{01} + V_1^{01})|0_\times\rangle + (V_0^{00} + V_1^{00} - V_0^{01} - V_1^{01})|1_\times\rangle)). \end{aligned}$$

Similarly, for $j = 1$ we have:

$$\begin{aligned} U(|v01_\times\rangle) &= \tfrac{1}{\sqrt{2}}U(|v00\rangle + |v01\rangle) \;=\; \tfrac{1}{\sqrt{2}}(V_0^{00}|0\rangle + V_1^{00}|1\rangle + V_0^{01}|0\rangle + V_1^{01}|1\rangle) \\ &= \tfrac{1}{2}((V_0^{00} - V_1^{00} + V_0^{01} - V_1^{01})|0_\times\rangle + (V_0^{00} + V_1^{00} + V_0^{01} + V_1^{01})|1_\times\rangle)). \end{aligned}$$

Thus, let us denote these vectors by

$$\widetilde{W}_0^{00} = \frac{1}{2}((V_0^{00} + V_1^{01}) - (V_0^{01} + V_1^{00})), \qquad \widetilde{W}_1^{00} = \frac{1}{2}((V_0^{00} - V_1^{01}) - (V_0^{01} - V_1^{00})),$$
$$\widetilde{W}_0^{01} = \frac{1}{2}((V_0^{00} - V_1^{01}) + (V_0^{01} - V_1^{00})), \qquad \widetilde{W}_1^{01} = \frac{1}{2}((V_0^{00} + V_1^{01}) + (V_0^{01} + V_1^{00})).$$

In order to obtain the correct result Bob has to distinguish between the density matrices corresponding to two values of a_0. In particular, he has to distinguish between density matrices γ_0', γ_1' corresponding to two possible values of a_0 knowing that $m = 0$. These density matrices are:

$$\gamma_0' \;=\; \frac{1}{4}|0\rangle\langle 0| \otimes (|V_0^{00}\rangle\langle V_0^{00}| + |V_1^{01}\rangle\langle V_1^{01}| + |\widetilde{W}_0^{00}\rangle\langle\widetilde{W}_0^{00}| + |\widetilde{W}_1^{01}\rangle\langle\widetilde{W}_1^{01}|), \tag{4}$$

$$\gamma_1' \;=\; \frac{1}{4}|0\rangle\langle 0| \otimes (|V_0^{01}\rangle\langle V_0^{01}| + |V_1^{00}\rangle\langle V_1^{00}| + |\widetilde{W}_0^{01}\rangle\langle\widetilde{W}_0^{01}| + |\widetilde{W}_1^{00}\rangle\langle\widetilde{W}_1^{00}|). \tag{5}$$

Now, the probability of failure i.e. the probability that in case of $m = 0$ Bob's measurement indicates that $a_0 = 0$ if in fact it is $a_0 = 1$, is at least

$$\mathrm{tr}(H_{p_0}\gamma_1' H_{p_0}^\dagger) \geq \mathrm{tr}(|O_0\rangle\langle O_0|\gamma_1') = \frac{1}{4}(|\langle 0V_0^{01}|O_0\rangle|^2+|\langle 0V_1^{00}|O_0\rangle|^2+|\langle 0\widetilde{W}_0^{01}|O_0\rangle|^2+|\langle 0\widetilde{W}_1^{00}|O_0\rangle|^2).$$

But since the fact that

$$\widetilde{W}_0^{01} = \frac{1}{2}((V_0^{00} - V_1^{01}) + (V_0^{01} - V_1^{00})), \qquad \widetilde{W}_1^{00} = \frac{1}{2}((V_0^{00} - V_1^{01}) - (V_0^{01} - V_1^{00})),$$

and the parallelogram law ($|a+b|^2 + |a-b|^2 = 2|a|^2 + 2|b|^2$), we have that this probability is at least

$$\begin{aligned} &\tfrac{1}{4}(|\langle 0\widetilde{W}_0^{01}|O_0\rangle|^2 + |\langle 0\widetilde{W}_1^{00}|O_0\rangle|^2) \geq \tfrac{1}{8}|\langle 0V_0^{00}|O_0\rangle - \langle 0V_1^{01}|O_0\rangle|^2 \\ &\geq \tfrac{1}{32}(|\langle 0V_0^{00}|O_0\rangle| - |\langle 0V_1^{01}|O_0\rangle|)^2(|\langle 0V_0^{00}|O_0\rangle| + |\langle 0V_1^{01}|O_0\rangle|)^2 \\ &\qquad \geq \tfrac{1}{32}(|\langle 0V_0^{00}|O_0\rangle|^2 - |\langle 0V_1^{01}|O_0\rangle|^2)^2 \geq \tfrac{\sigma_{p_0}^2}{32}. \end{aligned}$$

Similarly we analyze density matrices γ_0'', γ_1'' corresponding to two possible values of a_0 knowing that $m = 1$. These density matrices are equal to resp. γ_1' and γ_0' after changing $|0\rangle\langle 0|$ to $|1\rangle\langle 1|$. Now, by repeating completely analogous estimation of failure's probability with usage of vectors $|V_0^{01}\rangle$, $|V_1^{00}\rangle$, $|\widetilde{W}_0^{00}\rangle$ and $|\widetilde{W}_1^{01}\rangle$, we get that this probability is at least $\frac{\sigma_{2+p_1}^2}{32}$. Therefore, since the vectors involved in imposing failure in both cases are distinct, we conclude that $\Pr_{a_1 \in_R \{0,1\}}[a_0' \neq a_0 | r = 0] \geq \frac{\sigma_{p_0}^2 + \sigma_{2+p_1}^2}{32}$. Hence we have

$$\begin{aligned} \Pr_{a_1 \in_R \{0,1\}}[a_0' \neq a_0] = \tfrac{1}{2}\Pr_{a_1 \in_R \{0,1\}}[a_0' \neq a_0 | r = 0] + \tfrac{1}{2}\Pr_{a_1 \in_R \{0,1\}}[a_0' \neq a_0 | r = 1] \\ \geq \tfrac{\sigma_{p_0}^2 + \sigma_{2+p_1}^2}{64} \geq \tfrac{\delta^2}{128} \end{aligned}$$

and the lemma is proved.

Finally, it is worth mentioning that the value of m doesn't need to be correlated in any way with value of a_i. That is, Bob by using entanglement (for instance, straightforward use of Bell states) can make the value of m independent of a_i and still acquire perfect knowledge about a_i. He uses simple error-correction to know whether $m = a_i$ or $m = 1 - a_i$. His problems with determining whether flip has occurred, start only when he wants additionally to accumulate some information about the value of $a_i \oplus h$. ∎

To see that this quadratical bound can be achieved consider the following cheating strategy. Let U^* be such that $U^*(|v\rangle \otimes |l, j\rangle) = |v_j\rangle \otimes |l, j\rangle$. So, $|V_j^{l,j}\rangle = |v_j\rangle \otimes |l\rangle$ and $|V_{1-j}^{l,j}\rangle = 0$. Moreover, let $\langle v_0|v_1\rangle = \sqrt{1-\varepsilon}$. As we can see, usage of U^* accumulates some information about value of $j = a_0 \oplus h$ by marking it with two non-parallel (therefore possible to distinguish) vectors in Bob's system. We do now the following. We use U^* on $|v\rangle \otimes R_\alpha |a_1 \oplus h\rangle \oplus R_\alpha |a_0 \oplus h\rangle$ and send the last qubit to Alice. When we get the message m which is exactly a_0 with probability[5] of order $1 - \varepsilon$, we make an optimal measurement to distinguish between v_0 and v_1. By Theorem 1 this optimal measurement has advantage of order $\sqrt{\varepsilon}$. So, after getting the outcome j', we know that $\Pr[j' = a_0 \oplus h] \geq \frac{1}{2} + \Omega(\sqrt{\varepsilon})$ and we can simply compute the value of $h' = m \oplus j'$. Having such knowledge about the value of h' we can distinguish between values of a_1 encoded in the second qubit $R_\alpha |a_1 \oplus h\rangle$ with the advantage proportional to $\Omega(\sqrt{\varepsilon})$.

[5] This can be easily computed - the perturbation arises when $\alpha = \frac{1}{2}$.

4 Cheat Sensitive Quantum Bit Commitment

We recall first a formal definition of the binding and sealing property of a quantum bit commitment. We follow here the definition by Aharonov et al. [2]. Let us start with the binding property. Assume Alice follows the bit commitment protocol and Bob is arbitrarily. During the depositing phase Bob and Alice compute in some rounds a super-position $|\psi_{AB}\rangle$ with two quantum registers: one kept by Bob and one by Alice. After a communication phase Bob either uses a strategy trying to convince Alice to 0 or a strategy to convince Alice to 1. Depending on the results of the computations Alice decides to one of the values $v_A \in \{0, 1, err\}$; In case $v_A = err$, she rejects the protocol. Let p_i be the probability that Alice decides $v_A = i$, and p_{err} be the probability that Alice decides $v_A = err$, when Bob uses strategy 0. Analogously, denote the probabilities q_0, q_1, q_{err} for Bob's strategy 1. A protocol is (δ, ε)-***binding*** if whenever Alice is honest, for any Bob's strategy it is true: if $p_{err}, q_{err} \leq \varepsilon$ then $|p_0 - q_0|, |p_1 - q_1| \leq \delta$.

Now, a bit commitment protocol is (δ, ε)-*sealing*, if whenever Bob is honest and deposits a bit b s.t. $\Pr[b = 0] = 1/2$ then for any Alice's strategy and a value b' Alice learns, it holds that: if $\Pr_{b \in_R \{0,1\}}[\textit{Bob detects error}] \leq \varepsilon$ then $\Pr_{b \in_R \{0,1\}}[b' = b] \leq 1/2 + \delta$. The probability is taken over b chosen uniformly from $\{0, 1\}$ and the protocol.

Theorem 3 *Using Protocol 3 as a black-box for computing OT, Protocol 1 is* $(16\sqrt{\varepsilon}, \varepsilon)$-*sealing. Moreover, there exists a constant* $\lambda > 0$ *such that for all strategies Bob uses it holds* $\max\{p_{err}, q_{err}\} > \lambda$*, where* p_{err} (q_{err}) *denotes the probability that Alice decides error when Bob uses strategy for* 0 (1 *resp.). So, whenever Bob wants to cheat then it will be detected by Alice with constant probability.*

Proof: We will show first the sealing property. Thus, assume Bob is honest and Alice performing Protocol 1 uses an arbitrary strategy to gain knowledge about b. Denote the strategy by $\mathcal{BC}$. Let v_0, v_1 be the values Bob computes in the Depositing Phase. Moreover let a_0, a_1 denote bits which Alice determines and sends to Bob in the Revealing Phase. Then

$$\Pr[\textit{Bob detects error}] \;=\; \Pr[v_0 \neq a_{\hat{b}} \wedge c = 0] + \Pr[v_1 \neq a_{\hat{b}} \wedge c = 1] \tag{6}$$

where the probability is taken over $b, \hat{b}, c$ chosen uniformly and over the Protocol 1 when Alice uses strategy $\mathcal{BC}$.

Now let us consider, for a moment, that Alice and Bob compute the OT function using Protocol 3. We assume Bob is honest and has initially a bit i. Consider the following Alice's strategy to gain knowledge about i, which we will denote as $\mathcal{OT}$ (see Figure 4).

At the beginning Alice chooses randomly bits $\tilde{b}$ and $\tilde{c}$. If $\tilde{c} = 0$ then using strategy $\mathcal{BC}$ Alice first performs the execution of the OT protocol with Bob on input i and next she performs the second execution of the protocol for OT with an artificial party C, where C simulates an honest Bob on input $\tilde{b}$. Otherwise i.e. if $\tilde{c} = 1$, we switch the order of the both execution, i.e. Alice performs first the protocol for OT with C and next executes the OT protocol with Bob on input i.

Let v be the value which Bob determines in this scenario and let i' be the value Alice learns about i. We should note that strategies $\mathcal{OT}$ and $\mathcal{BC}$ are equivalent in the following sense: Assume Bob's input is i, Alice uses strategy $\mathcal{OT}$ performing Protocol 3, and let $\rho_i^{\mathcal{OT}}$ denote a density matrix of a mixed state in Alice's hands when the protocol is finished. Similarly, for Bob's input $\hat{b}$ and assuming that Alice uses strategy $\mathcal{BC}$ executing Protocol 1, let $\rho_{\hat{b}}^{\mathcal{BC}}$ denote a density matrix of a mixed state in Alice's hands when Bob has revealed b in the Revealing

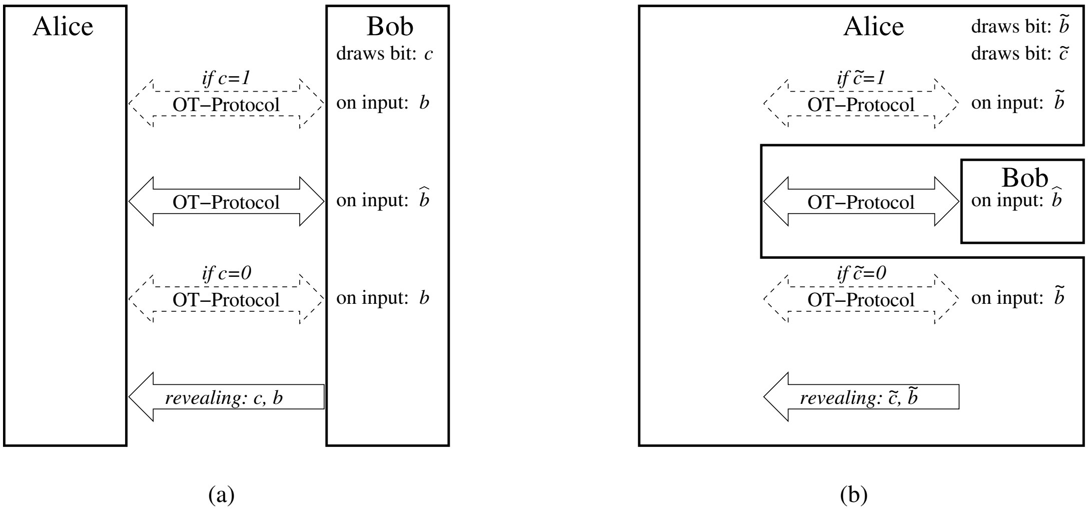

Figure 1: (a) Alice's strategy $\mathcal{BC}$ when performing Protocol 1 after the binding test but before the sealing test; (b) Alice's strategy $\mathcal{OT}$ for Protocol 3 on Bob's input $i = \hat{b}$.
Assuming that $\Pr[b = 0] = 1/2$, if $\rho^{\mathcal{BC}}_{\hat{b}}$ denotes the state of Alice's system at the end of scenario (a) and if $\rho^{\mathcal{OT}}_{\hat{b}}$ is the state of Alice's system at the end of scenario (b) then $\rho^{\mathcal{BC}}_{\hat{b}} = \rho^{\mathcal{OT}}_{\hat{b}}$.

Phase. Then we have $\rho^{\mathcal{OT}}_0 = \rho^{\mathcal{BC}}_0$ and $\rho^{\mathcal{OT}}_1 = \rho^{\mathcal{BC}}_1$. Assume Bob performs Protocol 3 on input $i = \hat{b}$. Hence we get that for the values a_0, a_1 which Alice determines in the Revealing Phase of Protocol 1 it holds that

$$\Pr_{\mathcal{OT}}[v \neq a_{\hat{b}}] \quad = \quad \Pr[v_0 \neq a_{\hat{b}} \wedge c = 0] + \Pr[v_1 \neq a_{\hat{b}} \wedge c = 1],$$

where the left-hand side probability is taken over Protocol 3 with Alice's strategy $\mathcal{OT}$ and the probabilities on the right-hand sides are taken over Protocol 1 with Alice's strategy $\mathcal{BC}$. Note that the left-hand side probability does not concern an event that the computed value v is (not) correct for some given Alice and Bob's inputs. Using strategy $\mathcal{OT}$ on the inputs, Alice may be not interested in computing the correct value at all. The left-hand side gives the probability that if Protocol 3 with Alice's strategy $\mathcal{OT}$ is finished then the particular values a_0, a_1 are *not* consistent with Bob's input and the value v he decides at the end of the protocol. Thus from (6) we obtain that: $\Pr_{\mathcal{OT}}[v \neq a_{\hat{b}}] = \Pr[\mathit{Bob\ detects\ error}]$.
Now, assume that when Alice is using strategy $\mathcal{BC}$ Bob detects in the sealing test an error with probability at most ε. Hence, $\Pr_{\mathcal{OT}}[v \neq a_{\hat{b}}] \leq \varepsilon$ and using Lemma 2, or speaking more precisely its stronger version as stated in Remark 1, we get $\Pr_{\mathcal{OT}}[\hat{b}' = \hat{b}] \leq 1/2 + 16\sqrt{\varepsilon}$, where $\hat{b}'$ is the value Alice learns about $\hat{b}$. Thus, for any value $\hat{b}'$ which Alice learns about $\hat{b}$ when performing Protocol 1 it holds that

$$\Pr[\hat{b}' = \hat{b}] \leq 1/2 + 16\sqrt{\varepsilon}, \tag{7}$$

where the probability is taken over Protocol 1 when strategy $\mathcal{BC}$ is used. Hence, Alice's advantage about $\hat{b}$ is at most $16\sqrt{\varepsilon}$. Note, however, that our aim is to show a bound on Alice's advantage about b and not about the value $\hat{b}$. In fact, performing Protocol 1 Alice may be not interested in learning the value $\hat{b}$ at all. One of the key properties of Protocol 1 is that Alice's maximum advantage about b is closely related to the maximum advantage she can get about $\hat{b}$. Particularly, the maximum advantage about b when $c = 1$ is the same as the maximum advantage about $\hat{b}$ in case $c = 0$. Analogously, Alice can learn b when $c = 0$ with the same advantage as she can learn $\hat{b}$ if $c = 1$. Speaking formally, the following property holds.

Let $\rho_{x,y}$ be a density matrix of Alice's part of the system corresponding to $c = x$ and $b = y$ when Step 2 is finished, but before Bob reveals c in Step 3. Similarly let $\hat{\rho}_{x,y}$ be Alice's part of the system at this point corresponding to $c = x$ and $\hat{b} = y$. Then for all $y \in \{0, 1\}$ we have $\rho_{0,y} = \hat{\rho}_{1,y}$ and $\rho_{1,y} = \hat{\rho}_{0,y}$.

Now assume that when the Depositing Phase is finished Alice makes measurements to learn value b: she uses $\mathcal{O}'$ when $c = 0$ and $\mathcal{O}''$ if $c = 1$. Let b' denote the value Alice learns about b when measurement $\mathcal{O}'$ is used and let b'' be the value Alice learns about b when she uses $\mathcal{O}''$. Then by Lemma 1 we can bound the probability that Alice learns bit b correctly as follows:

$$\begin{array}{rcl} \Pr[b' = b \wedge c = 0] + \Pr[b'' = b \wedge c = 1] & \leq & 1/2 + \frac{|\rho_{0,0}^{\mathcal{O}'} - \rho_{0,1}^{\mathcal{O}'}|_1}{4} + \frac{|\rho_{1,0}^{\mathcal{O}''} - \rho_{1,1}^{\mathcal{O}''}|_1}{4} \\ & = & 1/2 + \frac{|\hat{\rho}_{1,0}^{\mathcal{O}'} - \hat{\rho}_{1,1}^{\mathcal{O}'}|_1}{4} + \frac{|\hat{\rho}_{0,0}^{\mathcal{O}''} - \hat{\rho}_{0,1}^{\mathcal{O}''}|_1}{4}. \end{array}$$

Thus, using measurements $\mathcal{O}'$ and $\mathcal{O}''$ Alice can learn the correct value $\hat{b}$ with advantage at most $\frac{|\hat{\rho}_{1,0}^{\mathcal{O}'} - \hat{\rho}_{1,1}^{\mathcal{O}'}|_1}{4} + \frac{|\hat{\rho}_{0,0}^{\mathcal{O}''} - \hat{\rho}_{0,1}^{\mathcal{O}''}|_1}{4}$. Since this bound is tight, by (7) we get that it is at most $16\sqrt{\varepsilon}$ what completes the proof for the sealing property.

In case of binding, we first notice that the following claim is true.

Claim 1 *Assume Alice and Bob perform sequentially two executions of Protocol 3. Suppose Alice chooses randomly bits a_0, a_1, a_2, a_3 and performs honestly both the first execution with input a_0, a_1 and the second execution with input a_2, a_3. Then for every strategy $\mathcal{S}$ used by Bob and all values a'_0, a'_1, a'_2, a'_3 which Bob learns about a_0, a_1, a_2, a_3, resp., it holds that*

$$\textit{for all } i \in \{0,1\} \quad \textit{if} \Pr[a'_i = a_i] \geq 1 - \varepsilon^2 \quad \textit{then} \Pr[a'_{1-i} = a_{1-i}] \leq 1/2 + 16\sqrt{2}\varepsilon, \textit{ and}$$
$$\textit{for all } j \in \{0,1\} \quad \textit{if} \Pr[a'_{2+j} = a_{2+j}] \geq 1 - \varepsilon^2 \quad \textit{then} \Pr[a'_{3-j} = a_{3-j}] \leq 1/2 + 16\sqrt{2}\varepsilon,$$

where the probabilities are taken over a_0, a_1, a_2, a_3 chosen uniformly from $\{0, 1\}$ and the above scheme.

Proof: To show that the claim holds, we construct two strategies $\mathcal{B}_0$ and $\mathcal{B}_1$ for Bob performing Protocol 3 with Alice on input m_0, m_1. In both strategies Bob initially chooses random bits r_0, r_1 and then uses strategy $\mathcal{B}$ as follows: In $\mathcal{B}_0$ he executes $\mathcal{B}$ performing first the execution of the Protocol 3 with Alice on input m_0, m_1 and then the second (artificial) execution of the OT protocol with his subprocess C that simulates an honest Alice on input r_0, r_1. In $\mathcal{B}_1$ Bob follows $\mathcal{B}$ performing first the execution of the Protocol 3 with C on input r_0, r_1 and next the execution with Alice on input m_0, m_1.

Let m'_0, m'_1 be the values which Bob learns about m_0, m_1 using strategy $\mathcal{B}_0$ and let m''_0, m''_1 denote the values which Bob learns about m_0, m_1 using strategy $\mathcal{B}_1$. Then for all $i \in \{0, 1\}$ we have $\Pr_{\mathcal{B}_0}[m'_i = m_i] = \Pr[a'_i = a_i]$ and similarly for all $j \in \{0, 1\}$ it holds $\Pr_{\mathcal{B}_1}[m''_j = m_j] = \Pr[a'_{2+j} = a_{2+j}]$, where the left-hand side probabilities are taken over strategy $\mathcal{B}_0$, resp. $\mathcal{B}_1$ and the right-hand side corresponds to strategy $\mathcal{B}$. To see this, note that when the computations are finished, density matrices of quantum states in Bob's hands for strategy $\mathcal{B}$ on a_0, a_1 and for strategy $\mathcal{B}_0$ on $m_0 = a_0, m_1 = a_1$ are equal to each other and that an analogous property holds for $\mathcal{B}$ and $\mathcal{B}_1$. Thus, using Lemma 3 for strategy $\mathcal{B}_0$ and next for strategy $\mathcal{B}_1$ we get the claim. ∎

So, let a'_0, a'_1, a'_2, a'_3 be the values which Bob learns about Alice's input a_0, a_1, a_2, a_3 performing Protocol 1 and assume Bob has revealed value c and b. Let $\ell := 2 - 2c$. Then by the claim we have that for all $i \in \{0,1\}$ if $\Pr[a'_{\ell+i} = a_{\ell+i}] \geq 1 - \varepsilon^2$ then $\Pr[a'_{\ell+1-i} = a_{\ell+1-i}] \leq 1/2 + 16\sqrt{2}\varepsilon$. Thus by examination of the above bounds it follows that for some constant $\lambda > 0$

$$\max\{\Pr[a'_\ell \neq a_\ell], \Pr[a'_{\ell+1} \neq a_{\ell+1}]\} > \lambda.$$

This completes the proof of binding property since, using the notation given in the definition of this property, we have $p_{err} = \Pr[a'_\ell \neq a_\ell]$, $p_0 = \Pr[a'_\ell = a_\ell]$, and $p_1 = 0$. Similarly $q_{err} = \Pr[a'_{\ell+1} \neq a_{\ell+1}]$, $q_0 = 0$, and $q_1 = \Pr[a'_{\ell+1} = a_{\ell+1}]$.

∎

5 Computing Oblivious Transfer Cheat Sensitively

In this section we give the formal definition of the cheat sensitive $\binom{2}{1}$-OT computation.

Definition 2 *In a cheat sensitive $\binom{2}{1}$-OT quantum protocol Alice and Bob communicate with each other and finally Alice decides on a value $v_A \in \{\text{correct, error}\}$ and Bob decides on $v_B \in \{0, 1, \text{error}\}$. We say that the protocol is (δ, ε)-cheat sensitive if at the end of the computation the following requirements hold.*

- *If both Alice depositing initially bits a_0, a_1 and Bob having bit i are honest then Bob learns[6] the selected bit a_i in such a way that he gains no further information about the other bit and Alice decides on the value $v_A = \text{correct}$ and learns nothing else.*
- *Whenever Bob is honest and has a selection bit i, with $\Pr[i = 0] = 1/2$, then for every strategy used by Alice and every value i' Alice learns about i it holds that*

  $$\textit{if } \Pr_{i \in_R \{0,1\}}[i' = i] \geq 1/2 + \delta \quad \textit{then } \Pr_{i \in_R \{0,1\}}[\textit{Bob decides } v_B = \text{error}] \geq \varepsilon.$$

- *Whenever Alice is honest and deposits bits a_0, a_1, with $\Pr[a_i = 0] = 1/2$, then for every strategy used by Bob, all values a'_0, a'_1 Bob learns about a_0, a_1 it holds that if $\Pr_{a_0,a_1 \in_R \{0,1\}}[(a'_0, a'_1) = (a_0, a_1)] \geq 1/2 + \delta$ then $\Pr_{a_0,a_1 \in_R \{0,1\}}[\textit{Alice decides } v_A = \text{error}] \geq \varepsilon$.*

Remark 2 *In the previous version of this paper we have used the following alternative definition of sensitiveness with respect to a malicious Bob:* Whenever Alice is honest and deposits bits a_0, a_1, with $\Pr[a_i = 0] = 1/2$, then for every strategy used by Bob, all values a'_0, a'_1 Bob learns about a_0, a_1, resp., with advantages $\Pr_{a_0,a_1 \in_R \{0,1\}}[a'_i = a_i] = 1/2 + \delta_i$ it holds that if $\min\{\delta_0, \delta_1\} \geq \delta$ and $\max\{\delta_0, \delta_1\} \geq 1/2 - \delta/2$ then $\Pr_{a_0,a_1 \in_R \{0,1\}}[\text{Alice decides } v_A = \textit{error}] \geq \varepsilon$. *It seems, however, that Definition 2 determines sensitiveness with respect to a cheating Bob in more natural and elegant way. Moreover, note that if $\min\{\delta_0, \delta_1\} \geq \delta$ and $\max\{\delta_0, \delta_1\} \geq 1/2 - \delta/2$ then we get:*

$$\begin{aligned} \Pr[(a'_0, a'_1) = (a_0, a_1)] &= 1 - \Pr[a'_0 \neq a_0 \vee a'_1 \neq a_1] \\ &\geq 1 - \Pr[a'_0 \neq a_0] - \Pr[a'_1 \neq a_1] \ \geq \ 1/2 + \delta/2. \end{aligned}$$

Thus, the current definition is stronger (modulo a small constant factor) than the previous one.

[6] Speaking formally, we assume Bob learns a_i with probability 1.

Theorem 4 *Using Protocol 3 as a black-box for computing OT, Protocol 2 is $(16\sqrt{\varepsilon},\varepsilon)$-cheat sensitive.*

Proof: Note first that if both Alice and Bob are honest then the Computation Phase is performed with probability 1 after constant expected number of Quantum Phases and Alice and Bob compute $\binom{2}{1}$-OT fulfilling the standard security requirements.
Now assume Bob is honest and has a selection bit b with $\Pr[b=0]=1/2$ and Alice performing Protocol 2 uses an arbitrary strategy to gain knowledge about b. Denote Alice's strategy as $\mathcal{OT}$. Let $\rho_{\ell,i}$ be a density matrix of a mixed state in Alice's hands when the Quantum Phase of the ℓ-th iteration is completed, for some $\ell \geq 1$, and (a) performing the protocol Alice has used strategy $\mathcal{OT}$ and (b) during the ℓ-th iteration Bob has chosen bit i.
Next consider, for a moment, that Alice and Bob perform the susceptible $\binom{2}{1}$-OT Protocol 3 and define for a dishonest Alice the following strategy $\mathcal{OT}_\ell$: Initially, Alice chooses randomly bits $i_1, i_2, \ldots, i_{\ell-1}$ and then she performs $\ell-1$ executions of the Protocol 3 with an artificial party C, such that for $k=1,2,\ldots,\ell-1$, C simulates the k-th execution with an honest Bob on input i_k. Next Alice executes Protocol 3 with Bob on input i. Let $\hat{\rho}_{\ell,i}$ be Alice's part of the state when the computation is finished, Alice has used strategy $\mathcal{OT}_\ell$, and Bob's input bit is i. Then we have that for every $i \in \{0,1\}$

$$\hat{\rho}_{\ell,i} = \rho_{\ell,i}. \tag{8}$$

Moreover, using Remark 1 we get that for the probabilities taken over Protocol 3 and strategy $\mathcal{OT}_\ell$ it holds

$$\text{if } \Pr_{\mathcal{OT}_\ell}[i'=i] \geq 1/2+\delta \text{ then } \Pr_{\mathcal{OT}_\ell}[v \neq \tilde{a}_i] \geq \tfrac{\delta^2}{256}, \tag{9}$$

for all values $\tilde{a}_0, \tilde{a}_1$ which Alice determines after the protocol is finished. Here, i' denotes the value Alice learn about i and v is the value computed by Bob.
Now we come back to Protocol 2. Assume that $\Pr[\textit{Alice learns b correctly}] \geq 1/2+16\sqrt{\varepsilon}$, where the probability is taken over the protocol and strategy $\mathcal{OT}$. Denote by i_ℓ the bit Bob chooses initially in the ℓ-th iteration. Analogously, let c_ℓ and v_ℓ refer to bits involved during the ℓ-th iteration, i.e. let c_ℓ denote the bit send by Bob to Alice and let v_ℓ be the value computed by the party performing the cheating test during this iteration. Moreover, let $\texttt{A\_tests}_\ell$ and $\texttt{B\_tests}_\ell$ be value chosen during the ℓ-th iteration and let b'_ℓ be the value Alice learns about b when the ℓ-th iteration is completed and the parties decide to execute the Computation Phase (i.e. when $\texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0$). Then we have

$$\begin{aligned}\Pr[\textit{Alice learns b correctly}] &= \textstyle\sum_\ell p_\ell \cdot \Pr[b'_\ell = b \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0] \\ &= \textstyle\sum_\ell p_\ell \cdot (1/2+\delta_\ell) \;\geq\; 1/2+16\sqrt{\varepsilon},\end{aligned}$$

where $p_\ell = \Pr[\texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0]$ denotes the probability that during the ℓ-th iteration both values $\texttt{A\_tests}$ and $\texttt{B\_tests}$ are equal to 0, i.e. the probability that nobody wants to test during this iteration. Moreover the value δ_ℓ stands for Alice's advantage to learn b correctly in the Computation Phase executed after ℓ iterations. Note that the last inequality above implies that $\sum_\ell p_\ell \cdot \delta_\ell \geq 16\sqrt{\varepsilon}$. A very important feature of the protocol is that if q_ℓ denotes the probability $\Pr[\texttt{A\_tests}_\ell = 0 \wedge \texttt{B\_tests}_\ell = 1]$ then $q_\ell = p_\ell$.
Denote by $i'_\ell = b'_\ell \oplus c_\ell$. Hence the probabilities $\Pr[b'_\ell = b \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0]$ and $\Pr[i'_\ell = i_\ell \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0]$ are equal to each other. Now, our aim is to give a relationship between this probability and the probability that Alice learns Bob's input correctly when performing Protocol 3 with strategy $\mathcal{OT}_\ell$. So, assume Alice and Bob execute Protocol 3 and Alice uses strategy $\mathcal{OT}_\ell$. Moreover, assume that when the protocol is finished,

Alice still simulates strategy $\mathcal{OT}$ to gain knowledge about Bob's input bit $i = i_\ell$. Hence by the property (8) we get that

$$\Pr_{\mathcal{OT}_\ell}[i' = i] \;=\; \Pr[b'_\ell = b \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0] \;=\; 1/2 + \delta_\ell$$

and using (9) we can conclude that $\Pr_{\mathcal{OT}_\ell}[v \neq \tilde{a}_i] \geq \frac{\delta_\ell^2}{256}$ for all values $\tilde{a}_0, \tilde{a}_1$ which Alice determines. Thus, particularly for $\tilde{a}_0 = a_{\ell,0}$ and $\tilde{a}_1 = a_{\ell,1}$, where $a_{\ell,0}, a_{\ell,1}$ denote the values decided by Alice in the Test Phase during the ℓ-th iteration of Protocol 2, it holds

$$\Pr_{\mathcal{OT}_\ell}[v \neq a_{\ell,i}] \geq \frac{\delta_\ell^2}{256},$$

too. Hence, using again the property (8) we obtain that

$$\Pr[v_\ell \neq a_{\ell,i_\ell} \mid \texttt{A\_tests}_\ell = 0 \wedge \texttt{B\_tests}_\ell = 1] \;=\; \Pr_{\mathcal{OT}_\ell}[v \neq a_{\ell,i_\ell}] \;\geq\; \frac{\delta_\ell^2}{256},$$

and finally we can estimate the probability that Bob detects an error as follows:

$$\begin{aligned}\Pr[\textit{Bob detects error}] &= \textstyle\sum_\ell q_\ell \cdot \Pr[v_\ell \neq a_{\ell,i_\ell} \mid \texttt{A\_tests}_\ell = 0 \wedge \texttt{B\_tests}_\ell = 1] \\ &\geq \textstyle\sum_\ell p_\ell \cdot \frac{\delta_\ell^2}{256} \\ &\geq \frac{1}{256}(\textstyle\sum_\ell p_\ell \cdot \delta_\ell)^2 \;\geq\; \varepsilon.\end{aligned}$$

The last but one inequality is obtained using Jensen's inequality[7]. This completes the proof that the protocol is $(16\sqrt{\varepsilon}, \varepsilon)$-cheat sensitive according to Alice.

Now assume Alice is honest and Bob using an arbitrary strategy tries to gain knowledge about Alice's input bits m_0, m_1 when performing Protocol 2. Denote Bob's strategy as $\mathcal{OT}$ and assume that Alice's input bits m_0, m_1 are chosen independently and uniformly. Let ρ_{ℓ,a_0,a_1} be a density matrix of Bob's part of the state when the Quantum Phase of the ℓ-th iteration is completed and (a) during the ℓ-th iteration Alice has chosen $a_0, a_1 \in \{0,1\}$, and (b) performing the protocol Bob has used strategy $\mathcal{OT}$.

Similarly as in the previous case consider, for a moment, that Alice and Bob perform the susceptible $\binom{2}{1}$-OT Protocol 3. For a dishonest Bob we define the following strategy $\mathcal{OT}_\ell$: Initially, Bob chooses randomly bits $a_{1,0}, a_{1,1}, a_{2,0}, a_{2,1}, \ldots, a_{\ell-1,0}, a_{\ell-1,1}$. Then he performs $\ell - 1$ executions of the Protocol 3 with an artificial party C, such that for $k = 1, 2, \ldots, \ell - 1$, C simulates the k-th execution with an honest Alice on input $a_{k,0}, a_{k,1}$. Assume Alice and Bob execute Protocol 3. Let $\hat{\rho}_{\ell,a_0,a_1}$ be Bob's part of the state when the computation is finished, Bob has used strategy $\mathcal{OT}_\ell$, and Alice's input bit is a_0, a_1. Then we have that for all $a_0, a_1 \in \{0,1\}$

$$\hat{\rho}_{\ell,a_0,a_1} = \rho_{\ell,a_0,a_1}. \tag{10}$$

We use next the following modification of Lemma 3: If Alice and Bob perform Protocol 3 and the honest Alice deposits bits a_0, a_1 then for every strategy used by Bob, for all values a'_0, a'_1 which Bob learns about a_0, a_1 and for any value i' which Bob determines when the protocol is completed it holds that:

$$\text{if } \Pr_{a_0,a_1 \in_R \{0,1\}}[a'_{i'} = a_{i'}] \geq 1 - \delta^2 \;\text{ then } \Pr_{a_0,a_1 \in_R \{0,1\}}[a'_{1-i'} = a_{1-i'}] \leq 1/2 + 16\sqrt{2}\delta.$$

Note that, while the implication in Lemma 3 concerns *fixed* values of selection bit, the implication above involve values which are determined by Bob when the protocol is finished. For

[7] Note that $\sum_\ell p_\ell$ may be less than 1. However, $p_1, p_2, p_3, \ldots$ can be extended to a probability distribution by defining, for the value $\delta_0 = 0$, the probability $p_0 = 1 - \sum_\ell p_\ell$.

example, if (a dishonest) Bob chooses initially selection Bit i such that $\Pr[i = 0] = 1/2$ and then he performs Protocol 3 on the chosen input i, then we have that the both probabilities $\Pr_{a_0,a_1 \in_R \{0,1\}}[a'_0 = a_0]$ and $\Pr_{a_0,a_1 \in_R \{0,1\}}[a'_1 = a_1]$ are equal to $\frac{1}{2}(1+1/2) = 3/4$ but the probability $\Pr_{a_0,a_1 \in_R \{0,1\}}[a'_{i'} = a_{i'}] = 1$. It is easy to see, that the proof of Lemma 3 works for the modified version, too. Thus for strategy $\mathcal{OT}_\ell$ it holds that

$$\text{if } \Pr_{\mathcal{OT}_\ell}[a'_{i'} = a_{i'}] \geq 1 - \delta^2 \text{ then } \Pr_{\mathcal{OT}_\ell}[a'_{1-i'} = a_{1-i'}] \leq 1/2 + 16\sqrt{2}\delta. \tag{11}$$

Now, come back to Protocol 2 and assume that $\Pr[\textit{Bob learns } (m_0, m_1) \textit{ correctly}] \geq 1/2 + 16\sqrt{\varepsilon}$, where the probability is taken over the protocol and strategy $\mathcal{OT}$. Denote by $a_{0,\ell}, a_{1,\ell}$ the bits Alice chooses initially in the ℓ-th iteration. Analogously, let c_ℓ denote the bit send by Bob to Alice during the ℓ-th iteration and let $z_0 := a_{0,\ell} \oplus m_{c_\ell}, z_1 := a_{1,\ell} \oplus m_{1-c_\ell}$ denote the bits Alice send to Bob. Moreover, let $\texttt{A\_tests}_\ell$ and $\texttt{B\_tests}_\ell$ be value chosen during the ℓ-th iteration and let $m'_{0,\ell}, m'_{1,\ell}$ be the values Bob learns about m_0, m_1 when the ℓ-th iteration is completed and the parties decide to execute the Computation Phase. Then we have

$$\begin{aligned} &\Pr[\textit{Bob learns } (m_0, m_1) \textit{ correctly}] \\ &\qquad = \textstyle\sum_\ell \; p_\ell \cdot \Pr[(m'_{0,\ell}, m'_{1,\ell}) = (m_0, m_1) \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0] \\ &\qquad \geq 1/2 + 16\sqrt{2\varepsilon}, \end{aligned}$$

where, as in the previous case, $p_\ell = \Pr[\texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0]$. Define $q_\ell = \Pr[\texttt{A\_tests}_\ell = 1]$. Then it holds

$$q_\ell \;=\; \Pr[\texttt{A\_tests}_\ell = 0] \;\geq\; \Pr[\texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0] \;=\; p_\ell.$$

Next, denote by $a'_{\ell,0} = z_0 \oplus m'_{c_\ell}$ and $a'_{\ell,1} = z_1 \oplus m'_{1-c_\ell}$. Since the probabilities $\Pr[(m'_{0,\ell}, m'_{1,\ell}) = (m_0, m_1) \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0]$ and $\Pr[(a'_{0,\ell}, a'_{1,\ell}) = (a_{0,\ell}, a_{1,\ell}) \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0]$ are equal to each other we obtain

$$\textstyle\sum_\ell \; p_\ell \cdot \Pr[a'_{\ell,0} = a_{\ell,0} \wedge a'_{\ell,1} = a_{\ell,1} \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0] \;\geq\; 1/2 + 16\sqrt{2\varepsilon}. \tag{12}$$

Let us consider now the case $\texttt{A\_tests}_\ell = 1$. Let i'_ℓ be the value which Bob determines when the Quantum Phase of the ℓ-th iteration is completed and Alice tests Bob. Wlog we assume

$$\Pr[a'_{\ell,i'_\ell} = a_{\ell,i'_\ell} \mid \texttt{A\_tests}_\ell = 1] \;\geq\; \Pr[a'_{\ell,1-i'_\ell} = a_{\ell,1-i'_\ell} \mid \texttt{A\_tests}_\ell = 1]$$

and define δ_ℓ such that $\Pr[a'_{\ell,1-i'_\ell} = a_{\ell,1-i'_\ell} \mid \texttt{A\_tests}_\ell = 1] = 1/2 + \delta_\ell$. Wlog we can assume that the probability $\Pr[a'_{\ell,1-i'_\ell} = a_{\ell,1-i'_\ell} \mid \texttt{A\_tests}_\ell = 1]$ is not less than $\Pr[a'_{\ell,1-i'_\ell} = a_{\ell,1-i'_\ell} \mid \texttt{A\_tests}_\ell = \texttt{B\_tests}_\ell = 0]$. Hence using the inequality (12) one can conclude

$$\textstyle\sum_\ell \; p_\ell \cdot \Pr[a'_{1-i'_\ell,\ell} = a_{1-i'_\ell,\ell} \mid \texttt{A\_tests}_\ell = 1] \geq 1/2 + 16\sqrt{2\varepsilon}.$$

Thus, we have $\sum_\ell \; p_\ell \cdot (1/2 + \delta_\ell) \geq 1/2 + 16\sqrt{2\varepsilon}$ and therefore one can obtain the following inequality:

$$\textstyle\sum_\ell \; p_\ell \cdot \delta_\ell \geq 16\sqrt{2\varepsilon}. \tag{13}$$

Now, by property (10) we get

$$\Pr_{\mathcal{OT}_\ell}[a'_{1-i'_\ell} = a_{1-i'_\ell}] \;=\; \Pr[a'_{\ell,1-i'_\ell} = a_{\ell,1-i'_\ell} \mid \texttt{A\_tests}_\ell = 1] \;=\; 1/2 + \delta_\ell$$

and using (11) we can conclude that $\Pr_{\mathcal{OT}_\ell}[a'_{i'} \neq a_{i'}] \geq \frac{\delta_\ell^2}{512}$. Hence, using again property (10) we obtain that

$$\Pr[a'_{\ell,i'_\ell} \neq a_{\ell,i'_\ell} \mid \texttt{A\_tests}_\ell = 1] \;=\; \Pr_{\mathcal{OT}_\ell}[a'_{i'} \neq a_{i'}] \;\geq\; \frac{\delta_\ell^2}{512}$$

and finally we can estimate the probability that Alice detects en error as follows:

$$\begin{aligned} \Pr[\textit{Alice detects error}] \;&\geq\; \textstyle\sum_\ell q_\ell \cdot \Pr[a'_{\ell,i'_\ell} \neq a_{\ell,i'_\ell} \mid \texttt{A\_tests}_\ell = 1] \\ &\geq\; \textstyle\sum_\ell p_\ell \cdot \frac{\delta_\ell^2}{512} \\ &\geq\; \textstyle\frac{1}{512}(\sum_\ell p_\ell \cdot \delta_\ell)^2 \;\geq\; \varepsilon. \end{aligned}$$

The last but one inequality follows from Jensen's inequality. This completes the proof that the protocol is $(16\sqrt{2\varepsilon}, \varepsilon)$-cheat sensitive according to Bob. ∎

6 Concluding Remark

In this paper a weak variant of quantum bit commitment is investigated. We give quantum bit commitment scheme that is simultaneously binding and sealing and we show that if a malicious Alice gains some information about the committed bit b then Bob detects this with a probability $\Omega(\varepsilon^2)$. When Bob cheats then Alice's probability of detecting the cheating is greater than a constant $\lambda > 0$. Using our bounds we get that the value $\lambda \approx 0.0005$, which is very small from practical point of view (but theoretically optimal). So, an interesting task would be to improve the constant.
Furthermore, we have shown that *bit*-$\binom{2}{1}$-OT can be computed cheat sensitively. An interesting task would be to find a cheat sensitive protocol for *string*-$\binom{2}{1}$-OT. Unfortunately, our techniques does not seem to be directly applicable in this case, mainly due to possible bit correlation in string-$\binom{2}{1}$-OT. Existence of such cheat sensitive *string*-$\binom{2}{1}$-OT would also open the possibility of cheat sensitive computation of an arbitrary function by applying the method of Kilian [9].

References

[1] D. Aharonov, A. Kitaev, and N. Nisan, *Quantum circuits with mixed states*, STOC, 1998, 20-30.

[2] D. Aharonov, A. Ta-Shma, U. Vazirani, A. Yao, *Quantum bit escrow*, STOC, 2000, pp. 705-714.

[3] C. Bennet, G. Brassard, C. Crépau, and M.-H. Skubiszewska, *Practical quantum oblivious transfer*, CRYPTO, 1992, pp. 351–366.

[4] G. Brassard, C. Crépau, and J.-M. Robert, *Information Theoretic Reductions Among Disclosure Problems*, FOCS, 1986, pp. 168–173.

[5] C. Crépeau, *Quantum oblivious transfer*, J.of Modern Optics, vol. 41 no. 12, 1994, pp. 2445–2454.

[6] C. Crépeau and J. Kilian, *Achieving oblivious transfer using weakened security assumptions,* in Proc. FOCS 1988, pp. 42-52.

[7] S. Even, O. Goldreich, and A. Lempel, *A randomized protocol for signing contracts,* Comm. ACM, vol. 28, 1985, 637-647.

[8] L. Hardy and A. Kent, *Cheat Sensitive Quantum Bit Commitment*, Phys. Rev. Lett. 92, 157901 (2004)

[9] J. Kilian, *Founding cryptography on oblivious transfer,* STOC, 1988, pp. 20–31.

[10] H.K. Lo and H.F. Chau, *Why Quantum Bit Commitment and Ideal Quantum Coin Tossing are Impossible*, Physica D 120, 1998, pp. 177–187.

[11] D. Mayers, *Unconditionally Secure Quantum Bit Commitment is Impossible*, Physical Review Letters 78, 1997, pp. 3414–3417. Phys. Rev. Lett. 85, 2000, pp. 441–444.

[12] M.O. Rabin, *How to exchange secrets by oblivious transfer,* Tech. Memo TR-81, Aiken Computation Laboratory, 1981.

Appendix

A Additional Remarks Concerning the Definition 1 and the Protocol 3

The requirements of the susceptible oblivious transfer given in Definition 1 may seem to contradict each other. For example, at first glance it seems that the first and the last requirement of Definition 1 cannot be achieved simultaneously when honest Alice and dishonest Bob use Protocol 3. As proposed by a reader of a previous version of this paper, this may be argued as follows. But, as we will show below, the reasoning is wrong.

($*$) Consider the purified version of Protocol 3, where each player creates a uniform superposition whenever they are supposed to toss a random coin. Assume that Alice and Bob run the protocol as follows. Alice is honest and Bob replaces his input i with an equal superposition of 0 and 1. Now consider the final joint state between Alice and Bob. Assume that neither party makes any measurement during the protocol, so that the final state is a pure state. In particular, any coin tosses are simulated by creating superpositions. Now, from Alice's point of view, Bob is running the protocol on a random input i. In the honest case her part of the state is the same, regardless of whether $i = 0$ or $i = 1$. So Alice's part of the state is the same when Bob uses a superposition of 0 and 1 (Bob's part of the state may be different). Let ψ_i be the state when Bob runs the protocol with input i, and let ψ be the state when he runs it with an equal superposition of 0 and 1. Hence $\mathrm{tr}_B(\psi_i) = \mathrm{tr}_B(\psi)$. So, there is a unitary transformation U_i acting on Bob's part alone such that $(I \otimes U_i)\psi = \psi_i$. So Bob may apply U_0, then figure out bit a_0. Since he learns this bit with probability 1, the state is not disturbed. He can undo his operations and repeat to learn a_1.

Now, we explain why the reasoning ($*$) is wrong. Consider the purified version of Protocol 3. Then the (pure) state of the whole system after Step 2 looks as follows:

$$|r\rangle|\phi_0\rangle|\theta_0\rangle|s_0\rangle + |r\rangle|\phi_1\rangle|\theta_1\rangle|s_1\rangle$$

where the first two registers are in Alice's hands and the last two registers in Bob's hands, the first register is used to purify Alice's coin tosses, $|\phi_i\rangle|\theta_i\rangle$ is the state when Bob runs the protocol with input i and finally the last register is used by Bob to make the superposition. Step 3 transforms the state to:

$$|r\rangle|m_0\rangle|\theta_0\rangle|s_0\rangle + |r\rangle|m_1\rangle|\theta_1\rangle|s_1\rangle \tag{14}$$

where m_i depends, as in the protocol, on Bob's input. Now, if Alice would send to Bob the second register, i.e. the *qubit* describing m_i, then the reasoning above works. But, Alice sends to Bob the *bit*: either m_0 or m_1, and not a superposition entangled with the rest of the system. So, in fact, the analysis ($*$) does not correspond to Protocol 3.

Remark If one wants to move the final measurement to Step 4 using a purification, as is done in the analysis ($*$), then one has to 'put' the result of Alice's measurement made in Step 3 into Alice's part of the pure state (the analysis makes an error overlooking this) i.e. the system after Step 2 is: $|r\rangle|0\rangle|\phi_0\rangle|\theta_0\rangle|s_0\rangle + |r\rangle|1\rangle|\phi_1\rangle|\theta_1\rangle|s_1\rangle$ and the final state of the system (before the final measurement) looks as follows:

$$|r\rangle|m_0\rangle|m_0\rangle|\theta_0\rangle|s_0\rangle + |r\rangle|m_1\rangle|m_1\rangle|\theta_1\rangle|s_1\rangle$$

where the first two registers are in Alice's hands and the rest in Bob's, and according to the protocol, $R_\alpha^{-1}|\phi_i\rangle = |m_i \oplus h\rangle$, where $m_i \oplus h$ is just a classical bit that we xor with h at the end of Step 3. The second register is used to purify the state after the measurement in Step 3 and it corresponds to the outcome of the measurement. Note that any purification that leads to a state in which A does not know the result of this measurement means a change of our protocol! Now, using the notation as in analysis $(*)$, if ψ_i is the final state when B runs the protocol with input i, and ψ the state when he runs it with an equal superposition of 0 and 1 (in our analysis $\psi =$(14)) then we have for an appropriate Alice's input: $0 = m_0 \neq m_1 = 1$, hence $\mathrm{tr}_B(\psi) = 1/2 \sum_i |r\rangle\langle r||i\rangle\langle i|$, and $\mathrm{tr}_B(\psi_i) = |r\rangle\langle r||i\rangle\langle i|$. Thus $\mathrm{tr}_B(\psi_i) \neq \mathrm{tr}_B(\psi)$ in general, what contradicts the assumption in $(*)$.