Susceptible Two-Party Quantum Computations

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

[1] Institute of Theoretical Computer Science, University of Lübeck, Germany
liskiewi@tcs.uni-luebeck.de
[2] Massachusetts Institute of Technology, Cambridge, MA, USA
madry@mit.edu

Abstract. In secure two-party function evaluation Alice holding initially a secret input x and Bob having a secret input y communicate to determine a prescribed function $f(x, y)$ in such a way that after the computation Bob learns $f(x, y)$ but nothing more about x other than he could deduce from y and $f(x, y)$ alone, and Alice learns nothing. Unconditionally secure function evaluation is known to be essentially impossible even in the quantum world. In this paper we introduce a new, weakened, model for security in two-party quantum computations. In our model – we call it susceptible function computation – if one party learns something about the input of the other one with advantage ε then the probability that the correct value $f(x, y)$ is computed, when the protocol completes, is at most $1 - \delta(\varepsilon)$, for some function δ of ε. Thus, this model allows to measure the trade-off between the advantage of a dishonest party and the error induced by its attack. Furthermore, we present a protocol for computing the one-out-of-two oblivious transfer function that achieves a quadratic trade-off i.e. $\delta = \Omega(\varepsilon^2)$.

1 Introduction

In two-party computation, Alice holding initially a private (i.e., secret) input $x \in \{0,1\}^n$ and Bob having a private input $y \in \{0,1\}^m$ communicate to determine a given function $f(x, y) \in \{0,1\}^p$. In the standard *one-sided* setting the computation is secure if the, possible malicious, parties with unbounded computing power perform a communication protocol in such a way that (1) at the end of an honest execution of the protocol Bob learns the value $f(x, y)$ unambiguously (2) no matter what Bob does he cannot learn anything more about x other than what follows from the values of y and $f(x, y)$, and (3) no matter what Alice does, she learns nothing.

In [6] Beimel, Malkin, and Micali have given a combinatorial characterization of all securely computable functions in classical setting. It is proved there that f can be computed securely if and only if there do not exist inputs x_0, x_1, y_0, y_1 such that $f(x_0, y_0) = f(x_1, y_0)$ and $f(x_0, y_1) \neq f(x_1, y_1)$. Unfortunately, almost all useful functions fail to satisfy this criterion.

⋆ Part of this work was done during the stay of the first author at the University of Freiburg, Germany.

⋆⋆ On leave from Instytut Informatyki, Uniwersytet Wrocławski, Poland.

R. Safavi-Naini (Ed.): ICITS 2008, LNCS 5155, pp. 121–136, 2008.

An important example of a function that cannot be computed in such way is the one-out-of-two oblivious transfer function $\mathtt{OT}$ defined as follows: let Alice hold initially two secret bits a_0, a_1 and let Bob have a secret selection bit i. Then we define $\mathtt{OT}((a_0, a_1), i) = a_i$. The problem has been proposed in [16,15,12] as a generalization of Rabin's notion for oblivious transfer [22]. Oblivious transfer is a primitive of central importance particularly in secure two-party and multi-party computations. It is well known ([18,9]) that $\mathtt{OT}$ can be used as a basic component to construct protocols solving more sophisticated tasks of secure computations such as two-party oblivious circuit evaluation.

The impossibility of (unconditionally) secure function computations in the *classical* setting rises a question whether, and if so - in which way, *quantum* cryptography can ensure the security. Indeed, much interest has been devoted to develop quantum two-party protocols [3,4,8,14,13,10,7,23], some of which were claimed to be unconditionally secure [10,7,23]. However, in his paper [21] Lo proved that such (unconditionally) secure computations of all non-trivial functions are impossible even in quantum setting. As a corollary, a possibility of a secure quantum computation of the one-out-of-two oblivious transfer function $\mathtt{OT}$ is ruled out.

Moreover, Lo [21] generalized his impossibility result to non-ideal protocols, being ones that may violate the security constraints (1)-(3) slightly. In his 'non-ideal' model the requirements are relaxed as follows:

(1′) The density matrix that Bob has at the end of the protocol can be slightly different from an eigenstate of the measurement operator that he is supposed to use (thus, the correctness with probability 1 is not guaranteed any more, even if parties follow the protocol honestly).
(2′) There is allowed a small probability of Alice's distinguishing between different Bob's inputs.
(3′) There is allowed also a small probability of Bob's distinguishing between different Alice's inputs.

So, intuitively, the result of Lo states that there is no quantum protocol for computing any non-trivial function such that its correctness is high and the information leakage is small.

In this paper we consider a slightly different relaxation of ideal case of the security requirements for the one-sided two-party computation. Our model, we call it *susceptible function computation*, requires the constraint (1) (i.e. an honest execution of the protocol computes $f(x, y)$ correctly) but it allows, even huge information gain by a cheater. However, it requires that if the leakage is big then the probability that Bob computes the correct value $f(x, y)$ is proportionally small. In other words (precise definition will be given in Section 2), for a function $\delta(\cdot)$ we require that for all inputs x and y

(a) If both parties follow the protocol then at the end of the computation Bob learns the value $f(x, y)$ unambiguously.

(b) If Alice learns y with advantage ε then the probability that Bob computes the correct value $f(x, y)$ at the end of the protocol, is at most $1 - \delta(\varepsilon)$, for some function δ of ε.
(c) If Bob with advantage ε learns about x more than what follows from the values of y and $f(x, y)$ then the probability that Bob is able to compute correctly the value $f(x, y)$ is at most $1 - \delta(\varepsilon)$.

Particularly, if both Alice and Bob honestly perform a $\delta(\varepsilon)$-susceptible protocol, for an appropriate function δ, then Bob learns the value $f(x, y)$ correctly and he gains no additional information about x and Alice learns nothing about y. Note, that in our model Bob cannot get full knowledge about x; otherwise he would be able to compute $f(x, y)$ correctly, what contradicts requirement (c).

Intuitively, our model investigates the security of two-party computations when, for some external reasons, the correct computation of $f(x, y)$ is desired by both parties that are, nevertheless, curious to acquire additional knowledge about the input of the other party. To get this additional information a cheating party may arbitrarily deviate from the protocol.[1] But, the key feature of our model is that it imposes a trade-off between the addition knowledge that a cheating party can infer and the correctness of the value $f(x, y)$ computed by Bob. Particularly, if for given Alice's input x and Bob's input y the parties need to compute the correct value $f(x, y)$ with probability 1 then for any strategy used by a cheating party he or she is not able to gain any additional information. However, if for some external reasons, it is sufficient that the protocol may compute the correct value with probability (at least) $1 - \varepsilon$ then a cheater may get some (limited) additional information, and the amount of information is bounded by $\delta(\varepsilon)$.

The main result of this paper states that for the `OT` function there exists a susceptible protocol with $\delta(\varepsilon) = \Omega(\varepsilon^2)$. Hence, we show that a non-trivial function can be computed $\Omega(\varepsilon^2)$-susceptible. That is, we give an `OT` protocol which, speaking informally (precise definitions are presented 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 input bits $a_0, a_1 \in \{0, 1\}$ 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 input bit $i \in \{0, 1\}$ 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 $1 - \Omega(\varepsilon^2)$.

Such a model of function evaluation is new and there exists no *classical* counterpart of such susceptible two-party computations. This follows from a

[1] This is in contrast to honest-but-curious model, where parties have to follow the protocol faithfully.

combinatorial characterization of functions securely computable in the honest-but-curious model given by Beaver [5] and Kushilevitz [20] as well as from the characterization theorem of privately computable functions in a weak sense by Chor and Kushilevitz [11].

Though these papers study the so called *two-sided* setting, in which both parties learn the result of the function when the protocol is completed, we can apply them for the one-sided model for slightly modified functions: we replace the original function $f(x, y)$ by $r \oplus f(x, y)$ where r is an additional Bob's input and $\oplus$ denotes the bitwise xor-function. Now, using this modification one can conclude from [5,20] that if a classical (one-sided) protocol computes $\mathtt{OT}$ correctly with probability 1 then its information leakage is strictly greater than 0.

Moreover, from [11] we get that if a classical protocol computes $\mathtt{OT}$ correctly with probability $1 - \varepsilon$, then one of the parties can learn something about the input of the other one with advantage at least $\frac{1}{2} - \varepsilon$. The characterization from [11] holds for honest-but-curious players, but we can apply it also to the malicious setting: we just make the malicious party to use the honest-but-curious strategy to cheat. Thus, the theorem by Chor and Kushilevitz can also be used to analyze even malicious attacks. Clearly, the above assertions invalidate existence of any susceptible two-party protocols in classical setting.

Comparison to Previous Work. For secure two-party computations two models are considered in the literature. In the first one, the *honest-but-curious* model, we assume that the players never deviate from the given protocol but try to acquire knowledge about the input of the other player only by observing the communication. In the second setting, the *malicious* model, Alice or Bob may arbitrarily deviate from the protocol to defeat the security constraints. Moreover, depending on the computational power of the players we distinguish between computationally security and information theoretically security. In the first case we assume that any player is computationally bounded and in the second case we do not restrict the computational power of the players.

Recall, that in the classical malicious model, only few (trivial) functions can be computed securely in the information theoretic setting ([6]). The similar holds also for the honest-but-curious model. This follows from the characterization by Beaver [5] and Kushilevitz [20]. In [19] Klauck shows that in the honest-but-curious model quantum computations do not help. He proves that every function that can be computed securely using a quantum protocol can also be computed securely by a deterministic protocol.[2] On the other hand, he shows that allowing a small leakage, quantum communication allows us to compute Boolean functions which are not securely computable in the classical honest-but-curious model.

As we already mentioned, [21] proved that for quantum protocols in malicious setting it is impossible to compute securely any non-trivial function. In the light of this fact, Hardy and Kent [17] and independently Aharonov et al. [2], have introduced the notion of cheat sensitive protocols which, instead of unconditional

[2] In the literature one calls secure computations in the honest-but-curious model also private computations.

security, give only a guarantee that if one party cheats then the other has a proportional probability of detecting the mistrustful party. The result of Aharonov et al. [2] presents a protocol for quantum bit commitment they call it quantum bit escrow that ensures that whenever one party cheats with advantage ε then, at the end of the protocol, there exists a test that can be performed by the other party that detects the cheating with probability $\Omega(\varepsilon^2)$. However, the drawback of this protocol is that only one party can perform the test i.e. only one party can check whether the other cheated, and there is no mechanism that would allow fair resolving of this conflict. The authors state finding a protocol without this drawback as an open problem. Also the protocol presented by Hardy and Kent [17] is a weak variant of cheat sensitive quantim bit commitment in the sense that either Alice or Bob can detect a cheating party with non-zero probability. >From this perspective, our result can be seen as a cheat sensitive protocol for oblivious transfer (which subsumes bit commitment) with $\Omega(\varepsilon^2)$ trade-off, provided there is some way of allowing the party to test whether Bob computed correct value. Unfortunately, since we do not know how to implement such mechanism, the open problem is still unsettled.

2 Preliminaries

We assume that the reader is already familiar with the basics of quantum cryptography (see [2] for a description of the model and results that will be helpful). The model of quantum two-party computation we use in this paper is essentially the same as defined in [2].

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 $\mathcal{O} = \{O_j\}_j$, i.e. $\rho^{\mathcal{O}}$ is some distribution $p_1, \ldots, p_t$ where p_j denotes the probability that we get result j and O_j are projections on the orthonormal subspaces corresponding to j. 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 $\{1, 2, \ldots, t\}$: $|p - q|_1 = \frac{1}{2} \sum_{i=1}^{t} |p_i - q_i|$.

In the following we investigate one sided two party quantum protocols $F = (A, B)$, i.e. let x denote the input of Alice and y denote the input of Bob then at the end of the protocol Bob knows the result $F(x, y)$ of the protocol. By purification we can assume that each protocol consists of two phases. In the first phase, called quantum phase, both parties perform only unitary transformations on the quantum states. In the second phase both parties only perform a measurement and maybe some computations on classical bits.

We say that a quantum protocol $F = (A, B)$ for computing the function f is $\delta(\varepsilon)$-susceptible with respect to Alice, if for every strategy A' used by Alice the protocol $F' = (A', B)$ fulfills the following condition: *Let $\rho_A^{x,y}$ denote a reduced density matrix in Alice's hand at the end of the quantum phase of Alice and let $\mathcal{O}$ be the measurement of y by Alice. Then for all x and y it is true: if for some*

y' with $y \neq y'$ it holds that $|(\rho_A^{x,y})^{\mathcal{O}} - (\rho_A^{x,y'})^{\mathcal{O}}|_1 \geq \varepsilon$ then the probability that Bob computes the correct value of $f(x,y)$ is at most $1-\delta(\varepsilon)$, i.e. $\Pr[F'(x,y) = f(x,y)] \leq 1-\delta(\varepsilon)$.

We say that $F = (A,B)$ is $\delta(\varepsilon)$-susceptible with respect to Bob, if for every strategy B' used by Bob the protocol $F' = (A,B')$ fulfills the following condition: *Let $\rho_B^{x,y}$ denote a reduced density matrix in Bob's hand at the end of the quantum phase of Bob and let $\mathcal{O}$ be the measurement of x by Bob. Then for all y and for all x it is true: if for some $x' \neq x$ with $f(x,y) = f(x',y)$ it holds that $|(\rho_B^{x,y})^{\mathcal{O}} - (\rho_B^{x',y})^{\mathcal{O}}|_1 \geq \varepsilon$ then the probability that Bob computes the correct value of $f(x,y)$ is at most $1-\delta(\varepsilon)$.*

Both probabilities are taken over the random inputs of all the parties.

Definition 1. *Let $\delta(\varepsilon)$ be a function in ε. A quantum protocol F for computing f is $\delta(\varepsilon)$-susceptible if the following conditions hold:*

1. *If both parties follow F then Bob computes f correctly, i.e.* $\Pr[F(x,y) = f(x,y)] = 1$ *for all x and y,*
2. *F is $\delta(\varepsilon)$-susceptible with respect to Alice, and*
3. *F is $\delta(\varepsilon)$-susceptible with respect to Bob.*

We recall that we are interested in unconditional security, so in particular the above definition does not restrict the computational power of adversaries.

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.

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 $||\ |\phi_1\rangle\langle\phi_1| - |\phi_2\rangle\langle\phi_2|\ ||_t = 2\sqrt{1 - |\langle\phi_1|\phi_2\rangle|^2}$.

3 $\Omega(\varepsilon^2)$-Susceptible Oblivious Transfer

In this section we present a $\Omega(\varepsilon^2)$-susceptible protocol for OT.

Protocol 1 (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 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 two dimensions) and that R_β is (up to a phase) a NOT-gate conditioned on β. We will now focus on the question whether Protocol 1 still retains security if we use it against malicious parties. The following theorem follows from Lemma 1 and 2 which will be proven in the remaining part of this section:

Theorem 2. *Protocol 1 is a* $\Omega(\varepsilon^2)$*-susceptible protocol for* OT.

3.1 Malicious Alice

Lemma 1. *Let Alice and Bob perform Protocol 1 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* a' *Bob learns at the end of the computation it holds that for all* $a_0, a_1 \in \{0,1\}$ *and for any generalized measurement* $\mathcal{O}$

$$\text{if } |(\rho_A^0)^{\mathcal{O}} - (\rho_A^1)^{\mathcal{O}}|_1 \geq \varepsilon \text{ then } \Pr_{i \in_R \{0,1\}}[a' = a_i] \leq 1 - c_A \cdot \varepsilon^2 \ .$$

where ρ_A^j *denotes a reduced density matrix in Alice hand at the end of the protocol if Bob's input bit is given by* $i := j$ *and* $c_A > 0$ *is a constant independent of Alice's strategy.*

Proof: Any cheating strategy $\mathcal{A}$ of Alice corresponding to her input a_0, a_1 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 performing some measurement $\mathcal{O} = \{H_0, H_1, H_2, H_3\}$ 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. We emphasis that we allow Alice's strategy to depend on her input.

The outline of the proof is the following. We first bond the fact that $\mathcal{A}$ achieves some advantage ε to a certain relation between $\mathcal{H}$ and $|\Phi\rangle$. Then we show that this relation implies at least $c_A \cdot \varepsilon^2$ of noise in the value of a' computed by Bob.

We first consider the case when $a_0 \oplus a_1 = 0$. Clearly, in this case $m \oplus a_0 = m \oplus a_1 = \beta$. So if Alice manages to compute m that is correct i.e. $a' = m \oplus \beta = a_i$ then she also knows the value of β. Thus, we can compute the probability of $\mathcal{A}$ computing the correct result, by computing the the probability that she can indicate the value of β correctly.

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:

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

where $\overline{x_t}$ means flipping bit x_t, i.e. $\overline{x_t} = 1 - x_t$.

We look first onto Alice's advantage that she can achieve. In order to cheat, Alice has to distinguish between two density matrices $\gamma_l = \frac{1}{2}\rho_{l,0} + \frac{1}{2}\rho_{l,1}$ for $l \in \{0,1\}$, 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 $|V_A\rangle = |v_{10}\rangle - |v_{01}\rangle$. One can easily show that the advantage $\varepsilon := |(\rho_A^0)^{\mathcal{O}} - (\rho_A^1)^{\mathcal{O}}|_1$ of Alice is at most $\sum_{l=0}^{3} \sigma_l$ where

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

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 $|\langle O_{j_l}^l|V_A j_l\rangle| \ge |\langle O_{1-j_l}^l|V_A(1-j_l)\rangle|$. Clearly, $\sigma_l \le 2|\langle O_{j_l}^l|V_A j_l\rangle|$. Moreover, we assume that $\sigma_0 + \sigma_1 \ge \sigma_2 + \sigma_3$. 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 that convinces her that $\beta = 0$ in case when actually $\beta = 1$ 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

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

Similar calculation of the probability p_1 of getting outcome convincing Alice that $\beta = 1$ when actually $\beta = 0$ yields that the probability of computing wrong result is at least

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

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 $\beta \oplus i$, instead of β in order to give the correct answer to Bob, the proof is concluded. ∎

In fact, the above lemma is asymptotically tight since we can design a strategy of Alice which allows her to meet the quadratical bound imposed by the above lemma. To see this, consider $|\Phi\rangle = \sqrt{1-\Delta}|000\rangle + \sqrt{\Delta}|110\rangle$. 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

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

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

and therefore $||\rho_{0,0} - \rho_{1,0}||_t \geq \sqrt{\Delta(1-\Delta)} - 2\Delta$. So, by Theorem 1 there exists a measurement $\{H_0, H_1\}$ allowing us to distinguish between those two density matrices with $\sqrt{\Delta(1-\Delta)} - 2\Delta$ 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 the last two qubits of $|\Phi\rangle$ to Bob, after receiving the qubit back she applies the measurement M. If the outcome is H_2 then she answers $m = a_0 \oplus \beta = 1$ to Bob and sets $i' = 0$ with probability $\frac{1}{2}$, in the other

case she sends $m = a_0 \oplus \beta = 0$ 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 $1 - \frac{\Delta}{2}$ we should note that probability of outcome H_2 in case of $\beta = 0$ is 0 and in case of $\beta = 1$ is $1 - \Delta$. On the other hand, since $\beta = 0$ with probability $\frac{1}{2}$, Alice's advantage in determining the input of Bob is greater than $\frac{1}{2}\sqrt{\Delta} - \frac{3}{2}\Delta$. So, by setting $\varepsilon = \frac{1}{2}\sqrt{\Delta} - \frac{3}{2}\Delta$, we get that the presented strategy proves that the Protocol 1 cannot be $\delta(\varepsilon)$ susceptible for $\delta(\varepsilon) \geq 2\varepsilon^2$.

3.2 Malicious Bob

Now, we analyze Bob's possibility of cheating. Our goal is to show:

Lemma 2. *Let Alice and Bob perform Protocol 1. Assume Alice is honest and deposits bits a_0, a_1, with $\Pr[a_0 = 0] = \Pr[a_1 = 0] = 1/2$. Let i denote Bob's input bit. Then for every strategy $\mathcal{B}$ used by Bob and any value a'_i computed by Bob it holds that for $i = 0$*

$$\text{if } |(\rho_B^{a_0 a_1, 0})^{\mathcal{O}} - (\rho_B^{a_0 \overline{a}_1, 0})^{\mathcal{O}}|_1 \geq \varepsilon \text{ then } \Pr_{a_0, a_1 \in_R \{0,1\}}[a'_0 = a_0] \leq 1 - c_B \varepsilon^2$$

and for $i = 1$

$$\text{if } |(\rho_B^{a_0 a_1, 1})^{\mathcal{O}} - (\rho_B^{\overline{a}_0 a_1, 1})^{\mathcal{O}}|_1 \leq \varepsilon \text{ then } \Pr_{a_0, a_1 \in_R \{0,1\}}[a'_1 = a_1] \geq 1 - c_B \varepsilon^2.$$

where $\rho_B^{a_0 a_1, i}$ denotes a reduced density matrix in Bob's hand at the end of the protocol and $c_B > 0$ is a constant independent of Bob's strategy.

Proof: Consider some malicious strategy $\mathcal{B}$ of Bob. Wlog we may assume that $i = 0$ - the case of $i = 1$ is completely symmetric. In the following we skip the superscript i, i.e. let $\rho_B^{a_0 a_1}$ denote $\rho_B^{a_0 a_1, i}$, for short. Our aim is to show that

$$\text{if } |(\rho_B^{a_0 a_1})^{\mathcal{O}} - (\rho_B^{\overline{a}_0 a_1})^{\mathcal{O}}|_1 \leq \varepsilon \text{ then } \Pr_{a_0, a_1 \in_R \{0,1\}}[a' \neq a_0] \leq c_B \varepsilon^2.$$

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 of Protocol 1 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 $\mathcal{O} = \{H_0, H_1, H_2, H_3\}$, where outcome corresponding to subspace H_{2l+k} implies Bob's believe that $a'_0 = l$ 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 $U(|v\rangle \otimes |l_\times, j_\times\rangle) = |W_0^{l,j}\rangle \otimes |0_\times\rangle + |W_1^{l,j}\rangle \otimes |1_\times\rangle$.

[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.

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 (which is sent back to Alice) has to still contain actual information about encoded value being disturbed at the smallest possible degree. That implies for Bob a necessity of some sort of partial cloning of 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 we analyze this simplified process. In this way, this proof gives us a sort of quantitative non-cloning theorem. Although, it seems to 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 advantage i.e. his 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

$$|(\rho_B^{00})^{\mathcal{O}} - (\rho_B^{01})^{\mathcal{O}}|_1 \quad \geq \quad |(\rho_B^{10})^{\mathcal{O}} - (\rho_B^{11})^{\mathcal{O}}|_1 \ .$$

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 $\varepsilon = |(\rho_B^{00})^{\mathcal{O}} - (\rho_B^{01})^{\mathcal{O}}|_1$ of Bob in this case can be estimated by Bob's ability to distinguish between the following density matrices:

$$\begin{aligned} &\tfrac{1}{4}(\rho_{0,0,0} + \rho_{1,0,0} + \rho_{0,1,0} + \rho_{1,1,0}) \quad \text{(case } a_1 = 0\text{), and} \\ &\tfrac{1}{4}(\rho_{0,0,1} + \rho_{1,0,1} + \rho_{0,1,1} + \rho_{1,1,1}) \quad \text{(case } a_1 = 1\text{).} \end{aligned}$$

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

$$\varepsilon \leq \frac{1}{8}(|\rho_{0,0,0}^{\mathcal{O}} - \rho_{0,1,1}^{\mathcal{O}}|_1 + |\rho_{1,1,0}^{\mathcal{O}} - \rho_{1,0,1}^{\mathcal{O}}|_1 + |\rho_{0,1,0}^{\mathcal{O}} - \rho_{0,0,1}^{\mathcal{O}}|_1 + |\rho_{1,0,0}^{\mathcal{O}} - \rho_{1,1,1}^{\mathcal{O}}|_1). \quad (1)$$

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 $\rho_{0,1,1}$, $\varepsilon_0 = |\rho_{0,0,0}^{\mathcal{O}} - \rho_{0,1,1}^{\mathcal{O}}|_1$ is the maximum component in the right-hand side of the inequality (1) and therefore we have $\varepsilon \leq \frac{1}{2}\varepsilon_0$. Let, for short, $\gamma_0 = \rho_{0,0,0}$ and $\gamma_1 = \rho_{0,1,1}$. One can easily calculate that

$$\gamma_0 = |0\rangle\langle 0| \otimes |V_0^{00}\rangle\langle V_0^{00}| + |1\rangle\langle 1| \otimes |V_1^{00}\rangle\langle V_1^{00}| \quad (2)$$

$$\gamma_1 = |0\rangle\langle 0| \otimes |V_1^{01}\rangle\langle V_1^{01}| + |1\rangle\langle 1| \otimes |V_0^{01}\rangle\langle V_0^{01}|. \quad (3)$$

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

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

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

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

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). We get: $\frac{\varepsilon_0}{2} \leq \sigma_{p_0} + \sigma_{2+p_1}$.

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

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

We proceed now, to investigation of the probability of obtaining the correct result i.e. the correct value of a_0. Recall that $\mathrm{Pr}[a_1 = 0] = \frac{1}{2}$ so 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, as perceived by Bob, those two density matrices are indistinguishable. Therefore, we can substitute the second qubit from the initial configuration with a density matrix $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ of a random bit r

encoded in perpendicular basis and the probability of obtaining proper result is unchanged.

We analyze now 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, they are 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

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

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:

$$\gamma_0' = \frac{1}{4}|0\rangle\langle 0| \otimes (|V_0^{00}\rangle\langle V_0^{00}| + |V_1^{01}\rangle\langle V_1^{01}| + |\widetilde{W}_0^{00}\rangle\langle\widetilde{W}_0^{00}| + |\widetilde{W}_1^{01}\rangle\langle\widetilde{W}_1^{01}|), \quad (4)$$
$$\gamma_1' = \frac{1}{4}|0\rangle\langle 0| \otimes (|V_0^{01}\rangle\langle V_0^{01}| + |V_1^{00}\rangle\langle V_1^{00}| + |\widetilde{W}_0^{01}\rangle\langle\widetilde{W}_0^{01}| + |\widetilde{W}_1^{00}\rangle\langle\widetilde{W}_1^{00}|). \quad (5)$$

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

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

But since the fact that $\widetilde{W}_0^{01} = \frac{1}{2}((V_0^{00} - V_1^{01}) + (V_0^{01} - V_1^{00}))$, $\widetilde{W}_1^{00} = \frac{1}{2}((V_0^{00} - V_1^{01}) - (V_0^{01} - V_1^{00}))$, and the parallelogram law ($|a+b|^2 + |a-b|^2 = 2|a|^2 + 2|b|^2$), we have that this probability is at least

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

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

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

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 $a_i \oplus h$. ∎

Once again, it turns out that the quadratic susceptibility is asymptotically optimal. To see that this quadratical bound imposed by the above lemma 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 $\langle v_0 | v_1\rangle = \sqrt{1 - \Delta}$. 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 $1 - \Delta$, we make an optimal measurement to distinguish between v_0 and v_1. By Theorem 1 this optimal measurement has advantage of order $\sqrt{\Delta}$. So, after getting the outcome j', we know that $\Pr[j' = a_0 \oplus h] \geq \frac{1}{2} + \Omega(\sqrt{\Delta})$ 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 $\Omega(\sqrt{\Delta})$. So, our claim follows.

4 Concluding Remark

In this paper we have presented a $\Omega(\varepsilon^2)$-susceptible protocol for OT. An interesting question is whether we can find $\delta(\varepsilon)$-susceptible protocols for other non-trivial functions and a reasonable δ and whether there exists a combinatorial characterization for such functions.

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

The next natural question to ask is whether there exists a $\delta(\varepsilon)$-susceptible protocol for $\mathtt{OT}$ such that $\delta(\varepsilon)$ is asymptotically greater than $\Omega(\varepsilon^2)$. In fact, looking at the quadratic trade-off of the expression $|| \; |\phi_1\rangle\langle\phi_1| - |\phi_2\rangle\langle\phi_2| \; ||_t$ in the case of $\langle\phi_1|\phi_2\rangle = 1 - \varepsilon$ and the case of $\langle\phi_1|\phi_2\rangle = \varepsilon$ might suggest that the quadratic trade-off (which similarly arises in [2]) is inherent for all non-trivial susceptible computable functions.

It is also interesting to know, whether our protocol could be transformed into one that does not need external reasons to make the correct computation of $\mathtt{OT}((a_1, a_2), i)$ desirable for both parties i.e. a protocol in which failure to compute $\mathtt{OT}((a_1, a_2), i)$ correctly would immediately lead to detection of cheating.

Finally, even if our protocol is very simple - thus may be relatively easy to implement - the constants hidden in $\Omega(\varepsilon^2)$ are rather impractical. Thus, trying to come up with a different protocol with better constants or some way of amplifying the trade-off of our protocol can be worthwhile.

References

1. Aharonov, D., Kitaev, A., Nisan, N.: Quantum circuits with mixed states. In: Proc. STOC 1998, pp. 20–30 (1998)
2. Aharonov, D., Ta-Shma, A., Vazirani, U., Yao, A.: Quantum bit escrow. In: Proc. STOC 2000, pp. 705–714 (2000)
3. Ardehali, M.: A perfectly secure quantum bit commitment protocol, Los Alamos preprint archive quant-ph/9505019
4. Ardehali, M.: A simple quantum oblivious transfer protocols, Los Alamos preprint archive quant-ph/9512026
5. Beaver, D.: Perfect Privacy for Two Party Protocols, Technical Report TR-11-89, Harvard University (1989)
6. Beimel, A., Malkin, T., Micali, S.: The All-or-Nothing Nature of Two-Party Secure Computation. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 80–97. Springer, Heidelberg (1999)
7. Bennet, C., Brassard, G., Crépau, C., Skubiszewska, M.-H.: Practical quantum oblivious transfer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 351–366. Springer, Heidelberg (1992)
8. Brassard, G., Crépau, C.: Quantum bit commitment and coin tossing protocols. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 49–61. Springer, Heidelberg (1991)
9. Brassard, G., Crépau, C., Robert, J.-M.: Information Theoretic Reductions Among Disclosure Problems. In: Proc. FOCS, pp. 168–173 (1986)
10. Brassard, G., Crépau, C., Jozsa, R., Langlois, D.: A quantum bit commitment scheme provably unbreakable by both parties. In: Proc. FOCS, pp. 362–371 (1993)
11. Chor, B., Kushilevitz, E.: A Zero-One Law for Boolean Privacy. SIAM Journal on Discrete Mathematics 4(1), 36–47 (1991)
12. Crépeau, C.: Equivalence between two flavors of oblivious transfers. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 350–354. Springer, Heidelberg (1988)
13. Crépeau, C.: Quantum oblivious transfer. Journal of Modern Optics 41(12), 2445–2454 (1994)
14. Crépeau, C., Salvail, L.: Quantum Oblivious Mutual Identification. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 133–146. Springer, Heidelberg (1995)

15. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Comm. ACM 28, 637–647 (1985)
16. Fischer, M.J., Micali, S., Rackoff, C.: A secure protocol for the oblivious transfer. In: Proc. EUROCRYPT 1984 (1984); Printed version in J. of Cryptology, 9(3), 191-195 (1996)
17. Hardy, L., Kent, A.: Cheat Sensitive Quantum Bit Commitment. Phys. Rev. Lett. 92, 157901 (2004)
18. Kilian, J.: Founding cryptography on oblivious transfer. In: Proc. STOC, pp. 20–31 (1988)
19. Klauck, H.: Quantum and approximate privacy. Theory of Computing Systems 37(1), 221–246 (2004)
20. Kushilevitz, E.: Privacy and Communication Complexity. SIAM J. on Disc. Math. 5(2), 273–284 (1992)
21. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A 56, 1154–1162 (1997)
22. Rabin, M.O.: How to exchange secrets by oblivious transfer, Tech. Memo TR-81, Aiken Computation Laboratory (1981)
23. Yao, A.C.: Security of quantum protocols against coherent measurements. In: Proc. STOC, pp. 67–75 (1995)