Quantum Bit Escrow

Dorit Aharonov *
University of California
Berkeley, CA 94720
doria@cs.berkeley.edu

Amnon Ta-Shma †
University of California
Berkeley, CA 94720
amnon@cs.berkeley.edu

Umesh V. Vazirani ‡
University of California
Berkeley, CA 94720
vazirani@cs.berkeley.edu

Andrew C. Yao §
Princeton University
Princeton, NJ 08544
yao@cs.princeton.edu

ABSTRACT

Unconditionally secure bit commitment and coin flipping are known to be impossible in the classical world. Bit commitment is known to be impossible also in the quantum world. We introduce a related new primitive - *quantum bit escrow*. In this primitive Alice commits to a bit b to Bob. The commitment is *binding* in the sense that if Alice is asked to reveal the bit, Alice can not bias her commitment without having a good probability of being detected cheating. The commitment is *sealing* in the sense that if Bob learns information about the encoded bit, then if later on he is asked to prove he was playing honestly, he is detected cheating with a good probability. Rigorously proving the correctness of quantum cryptographic protocols has proved to be a difficult task. We develop techniques to prove quantitative statements about the binding and sealing properties of the quantum bit escrow protocol.

A related primitive we construct is a quantum biased coin flipping protocol where no player can control the game, i.e., even an all-powerful cheating player must lose with some constant probability, which stands in sharp contrast to the classical world where such protocols are impossible.

*This research was supported in part by a U.C. president's postdoctoral fellowship and NSF Grant CCR-9800024.

†Supported in part by David Zuckerman's David and Lucile Packard Fellowship for Science and Engineering and NSF NYI Grant No. CCR-9457799.

‡This research was supported in part by NSF Grant CCR-9800024, and a JSEP grant.

§This research was supported in part by DARPA and NSF under CCR-9627819, by NSF under CCR-9820855, and by a Visiting Professorship sponsored by the Research Miller Institute at Berkeley.

General Terms

Quantum cryptography, Quantum coin tossing, Quantum bit commitment

1. INTRODUCTION

We start with an informal definition of a (very) weak variant of bit commitment. In this variant there is first a commitment stage in which Alice commits a bit b to Bob. Later on there is a reveal stage in which Alice reveals the bit and Bob proves he played honestly. The protocol should be binding in the sense that if Alice changes her mind at revealing time then Bob has a good probability of catching her cheating, and sealing in the sense that if Bob learns information about the committed bit then Alice has a good probability of catching him cheating. Thus, the fundamental (and only) difference between this primitive and bit commitment is that in bit commitment Bob can not learn from the encoding any information about b, while in the weak primitive Bob can learn a lot of information about the encoded bit, but if he does so Alice catches him cheating with a good probability.

DEFINITION 1. *(Weak bit commitment) A weak bit commitment protocol is a quantum communication protocol between Alice and Bob which consists of two stages, the depositing stage and the revealing stage, and a final classical declaration stage at which both Alice and Bob each declare "accept" or "reject". The following requirements should hold.*

- *If both Alice and Bob are honest, then at depositing stage Alice decides on a bit, b. She then communicates with Bob, where Alice's protocol depends on b. At revealing stage Alice and Bob communicate, and during this stage Alice reveals to Bob the deposited bit b. Both Alice and Bob accept.*
- *(Binding) If Alice tries to change her mind about the value of b, then there is non zero probability that an honest Bob would reject.*
- *(Sealing) If Bob attempts to learn information about the deposited bit b, then there is non zero probability that an honest Alice would reject.*

Later on, we will give more formal definitions of "Alice changing her mind" and "Bob learning information", and

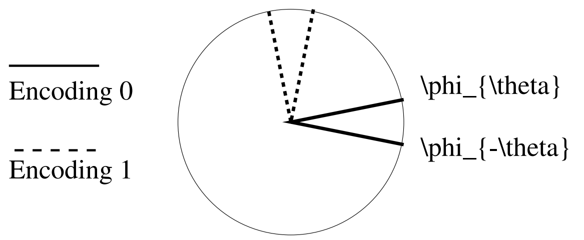

Figure 1: $\phi_{b,x}$

we will quantify the degree to which a protocol is binding or sealing.
Now, consider the following protocol:

PROTOCOL 1. *(Bit Escrow) For an angle* $\alpha \in [-\pi, \pi]$ *define* $\phi_\alpha = \cos(\alpha)|0\rangle + \sin(\alpha)|1\rangle$. *Let,*

$$\phi_{b,x} = \begin{cases} \phi_{-\theta} & b=0, x=0 \\ \phi_{\theta} & b=0, x=1 \\ \phi_{\frac{\pi}{2}-\theta} & b=1, x=0 \\ \phi_{\frac{\pi}{2}+\theta} & b=1, x=1 \end{cases}$$

for some fixed angle $\theta \leq \frac{\pi}{8}$, *say,* $\theta = \frac{\pi}{8}$. *See Figure 1.*
To deposit bit b, *Alice picks a random* $x \in \{0,1\}$, *and sends* $\phi_{b,x}$ *to Bob. Later on, one of the following two challenges is issued:*

- *Either Alice is asked to reveal the deposited bit, and then Alice sends the classical bits* b *and* x *to Bob* [1]. *Bob measures* ϕ *according to the basis* $\{\phi_{0,x}, \phi_{1,x}\}$ *and verifies that the result of the measurement is* $\phi_{b,x}$.
- *Or Bob is asked to return the deposited qubit, he returns a qubit* q, *and Alice measures it in the* $\{\phi_{0,x}, \phi_{1,x}\}$ *basis and verifies that it is* $\phi_{b,x}$.

We rigorously define and prove:

THEOREM 1. *Protocol 1 has the following properties:*

- *The deposited qubit does not reveal, in an information theoretic sense, all the information about the deposited bit* b.
- *(Binding) When Bob asks Alice to reveal the classical bit* b *that she deposited, if Alice influences the value of* b *with advantage* ϵ *then she is detected cheating with probability* $\Omega(\epsilon^2)$.
- *(Sealing) When Alice challenges Bob to return the deposited qubit, then if Bob can predict* b *with advantage* ϵ *then he is detected cheating with probability* $\Omega(\epsilon^2)$.

Protocol 1 and Theorem 1 do not achieve the goal set in definition 1 of weak bit commitment. Definition 1 asks for a protocol that is both binding and sealing, i.e., a commitment s.t. if either player cheats he is detected cheating with a good probability. Protocol 1 and Theorem 1 only give a commitment that is either binding (if Alice has to reveal) or sealing (if Bob has to return the qubit), but not simultaneously both. We therefore call this protocol a *bit escrow* protocol. The question of achieving simultaneous binding and sealing i.e. a weak bit commitment protocol, is left open. This question was addressed in [3], who independently defined the binding and sealing properties, and we discuss it in section 1.2.
We describe soon how to use the first two properties in Theorem 1 to get a biased coin flipping protocol with a constant bias.

1.1 Quantum Coin flipping

Alice and Bob are going through a divorce. They want to decide by a coin flip over the phone who is going to keep the car. The problem is that they do not trust each other any more.

DEFINITION 2. *(Classical coin flipping) [2] A coin flipping protocol with* δ *bias is one where Alice and Bob communicate and finally decide on a value* $c \in \{0,1\}$ *s.t. if at least one of the players is honest then for any strategy of the dishonest player* $Prob(c=0) \in [\frac{1}{2}-\delta, \frac{1}{2}+\delta]$.

Classical coin flipping can be implemented either by a trusted party or by assuming players with limited computational power and some cryptographic assumptions. However, if the players have unlimited computational power then no coin flipping protocol is possible in a classical world. This is because any protocol represents a two player game, and therefore game theory tells us that there is a player with an always winning strategy.
By contrast, in the quantum setting coin flipping (without computational assumptions) is not a priori ruled out. This is because any attempt by a player to measure extra information by deviating from the protocol can disturb the quantum state, and therefore be detected by the other player. This leads Lo and Chau[5] and later Mayers *et. al.*[7] to consider quantum coin flipping. There are several ways to define quantum coin flipping when cheaters can be detected. We define:

DEFINITION 3. *(quantum coin flipping) A quantum coin flipping protocol with bias* δ *is one where Alice and Bob communicate and finally each decides on a value* $c \in \{0,1,err\}$. *Let* c_A *(*c_B*) denote Alice's (Bob's) result. We require:*

- *If both players are honest then* c_A *always equals* c_B, $Prob(c_A = err) = 0$, *and* 0 *and* 1 *have equal probability:* $Prob(c_A = 0) = Prob(c_A = 1) = \frac{1}{2}$.
- *If one of the players is honest and the other is not, then for any strategy of the dishonest player, the honest player's result* c *satisfies for any* $b \in \{0,1\}$:

$$Prob(c = b) \leq \frac{1}{2} + \delta$$

Lo and Chau [5] showed that there is no quantum coin flipping protocol with 0 bias, under a certain restriction ("ideal coin flipping".) Mayers et al [7] generalized their proof to the general 0 bias case. Lo and Chau leave open the question whether non-exact protocols exist. Mayers et al [7] suggest a quantum coin flipping protocol that is based on a biased-coin protocol that is repeated many times. Mayers et al prove that it works well against some strong, natural

[1] This means that when Bob gets the qubit q_b that is supposed to carry a classical value for b, Bob measures q_b first in the $\{|0\rangle, |1\rangle\}$ basis. We carry this convention throughout the paper.

attacks. However, no general proof is given or claimed for the coin-flipping protocol or the biased-coin sub-protocol.
We give a simple protocol for quantum biased coin flipping, with constant bias. It is a modification of protocol 1:

PROTOCOL 2. *(A biased coin flipping protocol)*

- *Alice picks $b, x \in_R \{0,1\}$ and sends Bob $\phi_{b,x}$. We set $\theta = \frac{\pi}{8}$.*
- *Bob chooses $b' \in_R \{0,1\}$ and sends it to Alice.*
- *Alice sends Bob b and x. Bob checks against the qubit she sent in the first step. The result of the game is $r = err$ if Alice is caught cheating and $r = b \oplus b'$ otherwise.*

Based on the properties of protocol 1 we can prove that no player can fully control the game:

THEOREM 2. *Protocol 2 has $\delta \leq 0.42$ bias.*

i.e., no player can force his result with probability greater than 0.92. We note that while our protocol is resilient against all powerful malicious quantum players, it requires only simple single qubit operations from the honest player. An intriguing question is whether quantum coin flipping protocols are possible for arbitrarily low biases.

1.2 Weak Bit Commitment?

Hardy and Kent [3] (see Section 1.3) noticed that Protocol 1 can be used to give a weak bit commitment protocol if Alice and Bob can access a random independent coin flip. This is done as follows: at revealing time Alice first reveals the bit b, and then they receive a random independent coin flip. If the coin is 0, Bob is challenged to convince Alice that he hasn't been cheating, and if the coin flip turns out to be 1, then Alice is challenged. This is still correct if the coin flip is biased, as long as both probabilities for 0 and for 1 are constant.
Since we already have a biased coin flipping protocol, we might consider using this biased coin flipping protocol combined with the bit escrow protocol to give a weak bit commitment protocol. Consider the following protocol (see Figure 2):

PROTOCOL 3. *To deposit bit b, Alice picks a random $x \in \{0,1\}$, and sends $\phi = \phi_{b,x}$ to Bob. To reveal the bit, Alice sends b to Bob. Then a biased-coin flipping protocol (Protocol 2) is played.*

- *If Alice loses she is asked to reveal x and Bob measures ϕ according to the basis $\{\phi_{0,x}, \phi_{1,x}\}$ and verifies that the result of the measurement is $\phi_{b,x}$.*
- *If Bob loses he is asked to return the deposited qubit q, and Alice measures it in the $\{\phi_{0,x}, \phi_{1,x}\}$ basis and verifies that it is $\phi_{b,x}$.*

It is left as an open question whether this protocol, or perhaps a protocol which uses a different coin flipping procedure, is actually a weak bit commitment protocol. The main difficulty in proving or disproving such a result is the issue of independence between the coin flipping protocol and the bit escrow protocol. In other words, one has to prove that the cheater cannot use entanglement to correlate the events of being detected cheating in the bit-escrow protocol and winning the biased coin flipping protocol, in such a way that the cheater is never challenged when he (or she) has positive probability of being detected.

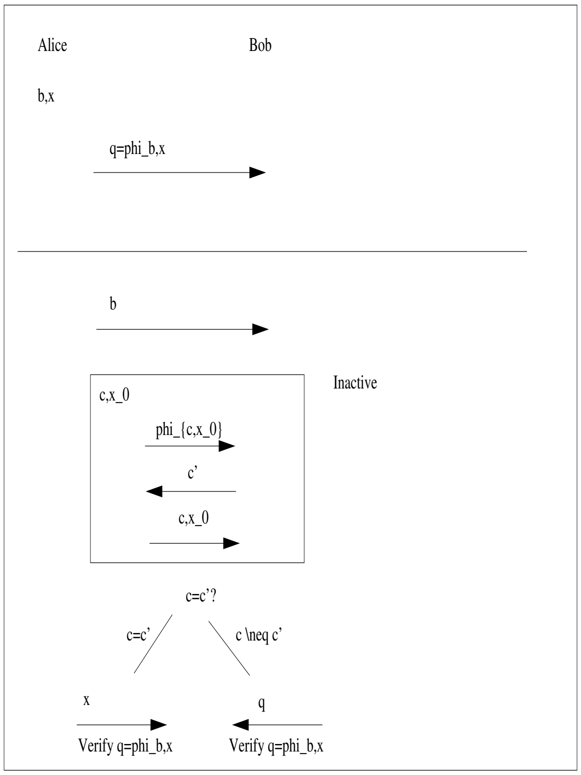

Figure 2: *Protocol 3*

It is our hope that our techniques could be extended to give weak bit commitment with $\Omega(\epsilon^c)$ binding and sealing for some constant c. Our results also show that Protocol 3 cannot be more than $\Omega(\epsilon^2)$ sealing or binding. It might be interesting to find a protocol that does better, or prove that such a protocol does not exist. It seems that a weak bit commitment protocol with better than quadratic security parameters can be used repeatedly to give a secure coin flipping protocol with unbounded bias.

1.3 Related Work

Some of the work presented here was independently done by Hardy and Kent [3]. They independently defined the binding and sealing properties and the weak bit commitment primitive (giving it different names). The protocol they analyze is similar in structure to protocol 3. Hardy and Kent's result asserts that a protocol similar to Protocol 3 is simultaneously sealing and binding. I.e., if Alice (Bob) uses a strategy that gives her (him) ϵ advantage, then Alice (Bob) is detected cheating with some probability which is strictly greater than 0 (they do not analyze the dependence of the detection probability on ϵ). However, no proof is given regarding the security against a cheater who tries to correlate the two parts of the protocol to his (or her) advantage.

2. PRELIMINARIES

The model. Let $\{e_1, \ldots, e_{2^n}\}$ be an orthonormal basis for $\mathbb{C}^n$, and let $|i\rangle = |i_1, \ldots, i_n\rangle$ be the vector e_i. A pure state

over n qubits is a vector $v \in \mathbb{C}^{2^n}$ of norm 1. Any pure state $|v\rangle$ can be expressed as $|v\rangle = \Sigma_i a_i |i\rangle$, with $\Sigma_i |a_i|^2 = 1$. A mixed state is a classical distribution over pure states, $\{p_i, \phi_i\}$, where $0 \le p_i \le 1$, $\Sigma_i p_i = 1$ and ϕ_i is a pure state, and the interpretation we give it is that the system is with probability p_i in the pure state ϕ_i. A quantum system is, in general, in a mixed state. The system Alice builds in the first stage of Protocol 2 is in a mixed state that is with probability $\frac{1}{4}$ in some pure state $\phi_{b,x}$.
A quantum system can undergo two basic operations: unitary evolution and measurement.

Unitary evolution : If a unitary transformation $U : \mathbb{C}^{2^n} \mapsto \mathbb{C}^{2^n}$ is applied to a pure state ϕ, then the new state of the system is the pure state $U\phi$. If U is applied to the mixture $\{p_i, \phi_i\}$ then the new state of the system is the mixture $\{p_i, U\phi_i\}$. The interpretation we give it is that with probability p_i the system was in the pure state ϕ_i hence it is now in the pure state $U\phi_i$.

Orthogonal Measurements : An orthogonal measurement is a decomposition of the system into orthogonal subspaces. More formally, suppose the system is in a super position $\phi \in \mathbb{C}^{2^n}$. Suppose $\mathcal{H}_1, \ldots, \mathcal{H}_k$ are orthogonal subspaces, and $\mathbb{C}^{2^n} = \mathcal{H}_1 \oplus \ldots \oplus \mathcal{H}_k$. A measurement of ϕ according to the decomposition $\mathcal{H}_1, \ldots, \mathcal{H}_k$, will get result i (or $\mathcal{H}_i$) with probability $q_i = |\Pi_{\mathcal{H}_i}|\phi\rangle|^2$ where $\Pi_{\mathcal{H}_i}$ is the projection on subspace $\mathcal{H}_i$, and then the state will collapse to $\frac{1}{\sqrt{q_i}}\Pi_{\mathcal{H}_i}|\phi\rangle$. In other words, ϕ falls into the subspace $\mathcal{H}_i$ with probability which is the length of the projection squared, and the new vector is the normalized projected vector. An orthogonal measurement can be represented using an Hermitian matrix M whose eigenspaces are the subspaces $\mathcal{H}_i$. A measurement of a mixture is the mixture of the measurements of the pure states.

Given a system ρ on $\mathbb{C}^{2^n}$, one can use an ancilla, say $|0, \ldots, 0\rangle \in \mathbb{C}^{2^m}$, apply a unitary transformation $U : \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^m} \mapsto \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^m}$, and then an orthogonal measurement on $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^m}$. It turns out that this is the most general measurement possible. There are several equivalent ways to formulate this so called 'generalized measurement', and we refer the interested reader to [8].

The Density Matrix. The density matrix of a pure state $|\phi\rangle$ is the matrix $|\phi\rangle\langle\phi|$, where $\langle\phi| = ((\phi)^t)^*$ is the conjugate transpose of ϕ. For example, the density matrix of $\phi_{0,0}$ is

$$|\phi_{-\theta}\rangle\langle\phi_{-\theta}| = \begin{pmatrix} \cos^2(\theta) & -\cos(\theta)\sin(\theta) \\ -\cos(\theta)\sin(\theta) & \sin^2(\theta) \end{pmatrix}$$

The density matrix of a mixed state $\{p_i, \phi_i\}$ is $\Sigma_i p_i |\phi_i\rangle\langle\phi_i|$. All density matrices are Hermitian, positive semi-definite and have trace 1. If a unitary matrix U operates on the system, it transforms the density matrix ρ to $U\rho U^\dagger$. A measurement M operating on a system whose density matrix is ρ results in an expected outcome $Trace(M\rho)$.

Distinguishing Between Density Matrices. Given a quantum system ρ and a generalized measurement $\mathcal{O}$ on it, let $\rho^{\mathcal{O}}$ denote the classical distribution on the possible results that we get by measuring ρ according to $\mathcal{O}$. i.e., it is some classical distribution $p_1, \ldots, p_k$ where we get result i with probability p_i. Given two different mixed states, we can ask how well one can distinguish between the two mixtures. We need a measure for the distance between two classical distributions and we choose the l_1 norm:

DEFINITION 4. *Let $p_1, \ldots, p_k$ and $q_1, \ldots, q_k$ be two probability distributions over $\{1, \ldots, k\}$. Then $|p - q|_1 = \Sigma_i |p_i - q_i|$.*

A fundamental theorem about distinguishing density matrices[1] tells us:

THEOREM 3. *[1] Let ρ_1, ρ_2 be two density matrices on the same space $\mathcal{H}$. Then for any generalized measurement $\mathcal{O}$*

$$|\rho_1^{\mathcal{O}} - \rho_2^{\mathcal{O}}|_1 \le Trace(\sqrt{A^\dagger A})$$

where $A = \rho_1 - \rho_2$. Furthermore, the bound is tight, and the orthogonal measurement $\mathcal{O}$ that projects a state on the eigenvectors of $\rho_1 - \rho_2$ achieves this bound.

Theorem 3 shows that the density matrix captures all the accessible information that a quantum state contains. If two different mixtures have the same density matrix (which is quite possible) then physically they are two different systems, but practically (and from a computational point of view) they are indistinguishable.
The quantity $Trace(\sqrt{A^\dagger A})$ is of independent interest. If we define $||A||_t = Trace(\sqrt{A^\dagger A})$ then $||\cdot||_t$ defines a norm, and has some additional properties such as $||A \otimes B||_t = ||A||_t \cdot ||B||_t$, $||A||_t = 1$ for any density matrix A and $||AB||_t, ||BA||_t \le ||A||_t \cdot ||B||_t$. If ϕ_1, ϕ_2 are two pure states, and ρ_i is the reduced density matrix of ϕ_i, then $||\rho_0 - \rho_1||_t = 2\sqrt{1 - |\langle\phi_1|\phi_2\rangle|^2}$. See [1] for more details.

Locality. We now turn to the local view of a subsystem. Suppose we are in a mixed state ρ over $k + m$ qubits, where Alice holds the first k qubits A and Bob holds the last m qubits B. Assume that Alice applies a generalized measurement $\mathcal{O}$ on her qubits A. This induces a new density matrix $\rho_B^{\mathcal{O}}$ on B. E.g., if Alice and Bob were in the super position $\phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ over two qubits and Alice measured the second qubit according to the basis $\{|0\rangle, |1\rangle\}$, then Bob is with probability $\frac{1}{2}$ in the super position $|0\rangle$ and with probability $\frac{1}{2}$ in $|1\rangle$, hence $\rho_B^{\mathcal{O}} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$. A fundamental fact from physics, which can also be proven rigorously, tells us that in fact $\rho_B^{\mathcal{O}}$ does not depend on $\mathcal{O}$, but only on the original matrix ρ. We thus denote it by $\rho|_B$, and call it the density matrix ρ reduced onto the subsystem B. Alternatively, we say that the rest of the system is *traced out.* The physical interpretation of the above result is that a player is guaranteed locality, i.e., a player Bob who holds a subsystem B knows that the results he gets from measurements he applies on B do not depend on the way the system outside B evolves. It is also some kind of commitment. If Alice sends Bob k qubits that have reduced density matrix ρ_B, then whatever Alice later does can not change this reduced density matrix.

Purification. A density matrix on a Hilbert space A can always be viewed as a reduced density matrix of a pure state on a larger Hilbert space, a process which is called "purification". A pure state $|\phi\rangle_{A,B}$ is a purification of the density matrix ρ_A if the reduced density matrix of $|\phi\rangle\langle\phi|_{A,B}$ to the Hilbert space A is ρ. The most straight forward way to purify a density matrix $\rho = \sum_i w_i|\phi_i\rangle\langle\phi_i|$ is by the state $|\phi\rangle = \sum_i \sqrt{w_i}|i\rangle \otimes |\phi_i\rangle$.

Fidelity.
The fidelity is a way to measure distances between density matrices, which is an alternative to the trace metric. Given two density matrices ρ_0, ρ_1 on the same Hilbert space A the fidelity is defined [4] to be:

$$f(\rho_0, \rho_1) = \sup |\langle\phi_0|\phi_1\rangle|^2 \tag{1}$$

where the supremum is taken over all purifications $|\phi_0\rangle$ of ρ_0 and $|\phi_1\rangle$ of ρ_1 to the same dimensional Hilbert space. We note here a few important properties which can easily be proven:

1. $0 \le f(\rho_0, \rho_1) \le 1$
2. $f(\rho_0, \rho_1) = 1 \iff \rho_0 = \rho_1$
3. For ρ_0 which is a pure state, i.e. $\rho_0 = |\phi_0\rangle\langle\phi_0|$, we have
$$f(\rho_0, \rho_1) = \langle\phi_0|\rho_1|\phi_0\rangle.$$

Note that the fidelity increases as the distance between two density matrices decreases. It is also not too difficult to see that the supremum is always achieved, i.e. we can replace the supremum by a maximum; See [4] for more details.

Entanglement. Suppose Alice holds a register A, Bob holds B, and the system is in a pure state ψ_{AB}. If we look at Bob's system alone then we might see a mixed state, and as we said before, Alice can not change the reduced density matrix of Bob by local operations on her side. On the other hand Alice might gain different aspects of knowledge on the actual result that Bob gets.

Example 1. $\psi_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. *If Alice measures in the $\{|0\rangle, |1\rangle\}$ basis, then Bob's system is with probability half in the state $|0\rangle$, and with probability half in the state $|1\rangle$, and the register A reflects the result Bob gets, i.e., Alice knows whether Bob gets a zero or a one. Now, ψ_{AB} can also be represented as $\frac{1}{\sqrt{2}}(|+,+\rangle + |-,-\rangle)$ where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Alice can measure the register A in the $\{|+\rangle, |-\rangle\}$ basis. Now Bob's system is with probability $\frac{1}{2}$ in the state $|+\rangle$, and with probability half in the state $|-\rangle$, and the register A reflects the result Bob gets, i.e., Alice knows whether Bob gets $|+\rangle$ or $|-\rangle$. Notice that Bob's reduced density matrix is the same in both cases.*

An important Theorem by Mayers [6] and independently Lo and Chau [5] states:

Theorem 4. *Suppose the reduced density matrix of B is the same in ϕ_{AB} and ψ_{AB}. Then Alice can move from ϕ_{AB} to ψ_{AB} by applying a* local *transformation on her side.*

I.e., even though Alice can not change Bob's reduced density matrix, she can determine how to "open" the mixture, and do so in a way that gives her full knowledge of Bob's result.

3. THE BINDING PROPERTY

In Protocol 1 Alice sends a qubit to Bob (we call it a "deposit" step) and later on she tells Bob how to "open" the qubit (the "reveal" step) which also determines the value that is supposed to be in the qubit. Such a protocol is worthless unless the deposit step is "binding" Alice to a pre-determined value. We first define the binding property in a general way. We then analyze how binding Protocol 1 is. Suppose we have a two step protocol:

Deposit : Alice prepares a super-position ψ_{AB} with two quantum registers A and B. Alice sends the second register B to Bob.

Reveal : Alice and Bob communicate. Bob follows the protocol and Alice is arbitrary. If Alice wants to create a bias towards 0 she uses one strategy, and if she wants a bias towards 1 she uses a different strategy. Bob decides on a result $r_B \in \{0, 1, err\}$.

Let us denote by p_0 the probability that Alice claims the result is 0 in the zero strategy, by p_1 the probability that Alice claims the result is 1 in the zero strategy, and by p_{err} the probability that Bob decides the answer is $r_B = err$ when Alice uses the zero strategy. We similarly define q_0, q_1, q_{err} for the one strategy.

Definition 5. *((ϵ, γ) binding) A protocol is (ϵ, γ) binding, if whenever Bob is honest, for any strategy Alice uses, if $p_{err}, q_{err} \le \epsilon$ then $|p_0 - q_0|, |p_1 - q_1| \le \gamma$.*

3.1 Protocol 1 is quadratically binding

Theorem 5. *Protocol 1 is $(\epsilon, \gamma = \frac{2\sqrt{\epsilon}}{\cos(2\theta)})$ binding.*

Proof. (of Theorem 5). At deposit time Alice sends Bob one qubit B, which might be entangled with the qubits A that Alice holds. Let us denote the reduced density matrix of B by ρ. At revealing time, Alice may choose whether she wants to bias the result towards 0, in which case she applies the generalized measurement M_0, or towards 1 in which case she applies M_1. The measurements M_0 and M_1 do not change the reduced density matrix ρ of Bob, but rather give different ways to realize ρ as a mixture of pure-states, and give Alice information about the value that Bob actually gets to see in this mixture.
Now, we even go further and give Alice complete freedom to choose the way she realizes the reduced density matrix ρ of Bob as a mixture, and we give her the knowledge of Bob's value for free. Let us say that when Alice applies M_0, the reduced density matrix ρ is realized as the mixture $\{p_i, \phi_i\}$, and when Alice applies M_1 the reduced density matrix ρ is realized as the mixture $\{p'_i, \phi'_i\}$.
Now, let us focus on the zero strategy. Say Alice realizes ρ as $\{p_i, \phi_i\}$. When the i'th event happens, Alice's strategy tells her to send some two qubits q_b, q_x to Bob, that are supposed to hold classical $0,1$ values for b and x. Bob then measures q_b and q_x in the $\{|0\rangle, |1\rangle\}$ basis. Now, if one of q_b, q_x is not a classical bit, then Alice can measure it herself in the $\{|0\rangle, |1\rangle\}$ basis, and get a mixture over classical bits. Furthermore, we can push all the probabilistic decisions into the mixture $\{p_i, \phi_i\}$. Thus, w.l.o.g, we can assume Alice's answers q_b and q_x are classical bits that are determined by the event i. Let us denote by u_i the vector ϕ_{b_i, x_i} where b_i, x_i

are Alice's answers when event i occurs. W.l.o.g we may assume $u_i \in \{\phi_{b,x}\}$, otherwise we know Bob immediately rejects.
The probability Bob discovers that Alice is cheating is then $1 - |\langle\phi_i|u_i\rangle|^2$ and the overall probability Bob detects Alice is cheating is

$$p_{err} = \Sigma_i p_i (1 - |\langle\phi_i|u_i\rangle|^2)$$

Let us define the density matrix $\rho_0 = \Sigma_i p_i |u_i\rangle\langle u_i|$.

CLAIM 6. $||\rho - \rho_0||_t \leq 2\sqrt{p_{err}}$.

PROOF. $|||\phi_i\rangle\langle\phi_i| - |u_i\rangle\langle u_i|||_t = 2\sqrt{1 - |\langle\phi_i|u_i\rangle|^2}$. Therefore

$$\begin{aligned} ||\rho - \rho_0||_t &= ||\Sigma_i p_i|\phi_i\rangle\langle\phi_i| - \Sigma_i p_i|u_i\rangle\langle u_i|\ ||_t \\ &\leq \Sigma_i p_i|||\phi_i\rangle\langle\phi_i| - |u_i\rangle\langle u_i|\ ||_t \\ &= 2\Sigma_i p_i\sqrt{1 - |\langle\phi_i|u_i\rangle|^2} \end{aligned}$$

Now, by Cauchy-Schwartz inequality,

$$\begin{aligned} \Sigma_i p_i \sqrt{1 - |\langle\phi_i|u_i\rangle|^2} &= \Sigma_i \sqrt{p_i}\sqrt{p_i(1 - |\langle\phi_i|u_i\rangle|^2)} \\ &\leq \sqrt{\Sigma_i p_i}\sqrt{\Sigma_i p_i(1 - |\langle\phi_i|u_i\rangle|^2)} \\ &= \sqrt{p_{err}} \end{aligned}$$

and the claim follows. □

Similarly, if Alice tries to bias the result towards 1, B ends up in the mixture $\{p'_i, \phi'_i\}$, and when ϕ'_i occurs Alice sends b', x' to Bob that correspond to a vector $u'_i \in \{\phi_{b,x}\}$. We define ρ_1 to be the reduced density matrix $\rho_1 = \Sigma_i p'_i|u'_i\rangle\langle u'_i|$. As before, $||\rho - \rho_1||_t \leq 2\sqrt{q_{err}}$. Hence, $||\rho_0 - \rho_1||_t \leq 2(\sqrt{p_{err}} + \sqrt{q_{err}})$.
To conclude the proof, we establish the following claim:

CLAIM 7. *Let ρ_0 and ρ_1 be density matrices corresponding to mixtures over $\{\phi_{b,x}\}$. Let p_0 be the probability of $\phi_{0,0}$ or $\phi_{0,1}$ in the first mixture, and $p_1 = 1 - p_0$ be the probability of $\phi_{1,0}$ or $\phi_{1,1}$. Similarly let q_0 and q_1 be the corresponding quantities for the second mixture. Then $||\rho_0 - \rho_1||_t \geq 2 \cdot |p_0 - q_0| \cos 2\theta$.*

PROOF. We show that we can distinguish the mixtures with probability at least $|p_0 - q_0| \cos 2\theta$ when we measure them according to the basis $\{|0\rangle, |1\rangle\}$. If we do the measurement on a qubit whose state is the reduced density matrix ρ_0 we get the $|0\rangle$ answer with probability $p_0 \cos^2(\theta) + p_1 \sin^2(\theta)$, while if we do the measurement on a qubit whose state is the reduced density matrix ρ_1 we get the $|0\rangle$ answer with probability $q_0 \cos^2(\theta) + q_1 \sin^2(\theta)$. The difference is $|p_0 \cos^2(\theta) + p_1 \sin^2(\theta) - (q_0 \cos^2(\theta) + q_1 \sin^2(\theta))| = |p_0 - q_0|(\cos^2(\theta) - \sin^2(\theta))$, where we used $p_1 - q_1 = (1 - p_0) - (1 - q_0) = q_0 - p_0$. Altogether we get $||\rho_0 - \rho_1||_t \geq 2 \cdot |p_0 - q_0|(\cos^2(\theta) - \sin^2(\theta))$ as desired. □

Putting it together:

$$2 \cdot \cos(2\theta) \cdot |p_0 - q_0| \leq ||\rho_1 - \rho_1||_t \leq 2(\sqrt{p_{err}} + \sqrt{q_{err}}) \leq 4\sqrt{\epsilon}$$

I.e., $|p_0 - q_0| \leq \frac{2\sqrt{\epsilon}}{\cos(2\theta)}$.

3.2 A Quadratic Strategy for Alice

We now show that Alice has a quadratic strategy for Protocol 1, and thus Theorem 5 is essentially tight. In fact, we show the quadratic bound for a more general family of protocols. Let ρ_0, ρ_1 be two density matrices of the same dimension, ρ_0 can be realized as the mixture $\{p_i^0, |\alpha_i^0\rangle\}$, and ρ_1 as $\{p_i^1, |\alpha_i^1\rangle\}$. To encode b, honest Alice picks $|\alpha_i^b\rangle$ with probability p_i and sends it to Bob. At revealing time Alice sends b and i to Bob, and Bob tests whether Alice is cheating by projecting his state on $|\alpha_i^b\rangle$.

THEOREM 8. *Let f be the fidelity $f(\rho_0, \rho_1)$. For any $0 \leq \alpha \leq \pi/4$ there exists a strategy for Alice with advantage $\sqrt{f} sin(2\alpha)/2$ and probability of detection at most $\frac{(1-f)sin^2(\alpha)}{2}$.*

On first reading of the next proof the reader might want to check the proof in the simpler case where ρ_0 and ρ_1 represent pure states, i.e., $\rho_b = |\psi_b\rangle\langle\psi_b|$.

PROOF. We first represent the strategy of a honest Alice in quantum language. Consider two maximally parallel purifications $|\psi_0\rangle$ and $|\psi_1\rangle$ of ρ_0 and ρ_1, where ρ_0 and ρ_1 are density matrices of the register B, and the purifications are states on a larger Hilbert space $A \otimes B$. By [4], $|\langle\psi_0|\psi_1\rangle|^2 = f(\rho_0, \rho_1)$. At preparation time, Alice prepares the state

$$|\beta\rangle = \frac{1}{\sqrt{2}}(|0, \psi_0\rangle + |1, \psi_1\rangle)$$

on $A \otimes B$ and one extra qubit C. Alice then sends the register B to Bob. At revealing time, Alice measures the qubit C in the $|0\rangle, |1\rangle$ basis, to get a bit b. The state of registers A, B is now $|\psi_b\rangle$. Alice then applies a unitary transformation U_b on register A, which rotates her state $|\psi_b\rangle$ to the state

$$|\psi'_b\rangle = \sum_j \sqrt{p_j^b}|j\rangle_A|\alpha_j^b\rangle_B$$

This is possible by Theorem 4. After applying U_b, Alice measures register A in the computational basis and sends Bob the bit b and the outcome of the second measurement, j. This strategy is similar to the honest strategy, except for that Alice does not know what bit and state is sent until revealing time.
We can also assume w.l.o.g. that the maximally parallel purifications satisfy that $\langle\psi_0|\psi_1\rangle$ is real and positive. This can be assumed since otherwise we could multiply $|\psi_0\rangle$ by an overall phase without changing the reduced density matrix and the absolute value of the inner product.
To cheat, Alice creates the encoding $|\beta\rangle_{CAB}$ and sends register B to Bob. Alice's one strategy is also as described above. The zero strategy, on the other hand, is a slight modification of the honest strategy. At revealing time, Alice measures the control qubit C in the $\{|\phi_\alpha\rangle, |\phi_\alpha^\perp\rangle\}$ basis, where

$$\begin{aligned} |\phi_\alpha\rangle &= c|0\rangle + s|1\rangle, \\ |\phi_\alpha^\perp\rangle &= -s|0\rangle + c|1\rangle, \end{aligned} \tag{2}$$

and $s = \sin(\alpha)$, $c = \cos(\alpha)$. If the outcome is a projection on $|\phi_\alpha\rangle$ Alice sends $b = 0$ and proceeds according to the $b = 0$ honest protocol, i.e. applies U_0 to register A, measures in the computational basis and sends the result to Bob. If the outcome is a projection on $|\phi_\alpha^\perp\rangle$, Alice proceeds according to the $b=1$ honest protocol. Let us now compute Alice's advantage and Alice's probability of getting caught cheating. We can express $|\beta\rangle$ as:

$$\begin{aligned}|\beta\rangle &= \frac{1}{\sqrt{2}}(c|\phi_\alpha,\psi_0\rangle - s|\phi_\alpha^\perp,\psi_0\rangle) + \\ &\quad \frac{1}{\sqrt{2}}(s|\phi_\alpha,\psi_1\rangle + c|\phi_\alpha^\perp,\psi_1\rangle).\end{aligned}$$

Hence, the probability Alice sends $b=0$ in the zero strategy is $\frac{1}{2}|c\psi_0+s\psi_1|^2 = \frac{1}{2}(c^2+s^2+2cs\langle\psi_0|\psi_1\rangle) = \frac{1}{2}(1+2cs\sqrt{f})$. We conclude:

CLAIM 9. *Alice's advantage is* $\frac{\sqrt{f}\sin(2\alpha)}{2}$.

We now prove that the detection probability is at most $(1-f)s^2$. The state of $A\otimes B$ conditioned that the first measurement yields $|\phi_\alpha\rangle$ can be written as $\frac{1}{\sqrt{Pr(b=0)}}\frac{1}{\sqrt{2}}(c|\psi_0\rangle + s|\psi_1\rangle)$ where $Pr(b=0)$ is the probability Alice sends $b=0$ in the zero strategy. The above state can be written as

$$\frac{1}{\sqrt{Pr(b=0)}}\frac{1}{\sqrt{2}}(c+\sqrt{f}s)|\psi_0\rangle + \sqrt{1-f}s|\psi_0^\perp\rangle$$

The rest of the protocol involves Alice's rotation of the state by U_0, then Alice's measurement of the register A and Bob's measurement of the register B. The entire process can be treated as a generalized measurement on this state, where this measurement is a projection onto one of two subspaces, the "cheating Alice" and the "Honest Alice" subspaces. We know that $|\psi_0\rangle$ lies entirely in the honest Alice subspace, and thus the probability that Alice is caught, conditioned that C was projected on ϕ_α, is at most $\frac{1}{Pr(b=0)}\frac{1}{2}(1-f)s^2$. In the same way, when we condition on a projection on $\phi_\alpha^\perp$, Alice's state can be written as $\frac{1}{\sqrt{Pr(b=1)}}\frac{1}{\sqrt{2}}((c-\sqrt{f}s)|\psi_1\rangle - \sqrt{1-f}s|\psi_1^\perp\rangle)$. which gives a probability of detection which is at most $\frac{1}{Pr(b=1)}\frac{1}{2}(1-f)s^2$. Adding the conditional probabilities together we get that the detection probability is at most $\frac{(1-f)s^2}{2}$. □

4. THE SEALING PROPERTY

DEFINITION 6. *((ϵ,p) sealing) A bit escrow protocol is (ϵ,p) sealing, if whenever Alice is honest and deposits a bit b s.t. $Prob(b=0)=\frac{1}{2}$, for any strategy Bob uses and a value c Bob learns, it holds that either*

- $\Pr_{b\in_R\{0,1\},protocol}\ (c=b) \le \frac{1}{2}+\epsilon$, *or*
- $\Pr_{b\in_R\{0,1\},protocol}\ (r_A = err) \ge p$

The probability is taken over b taken uniformly from $\{0,1\}$ and the protocol.

We show here that protocol 1 is quadratically sealing. This means that whatever Bob does, he will always be detected cheating with probability which is at least the square of his advantage. Later, we show that this is tight.

4.1 Protocol 1 is Quadratically Sealing

THEOREM 10. *Protocol 1 is $(\epsilon = O(\frac{\sqrt{p}}{\sin(2\theta)}),p)$ sealing.*

PROOF. We first describe a general scenario. Alice is honest and sends $|\phi_{b,x}\rangle_A$ to Bob. Bob has an ancilla $|0\rangle_C$. Bob applies some unitary transformation U acting on the registers A and C. Let us denote

$$|\alpha_{b,x}\rangle = U(|\phi_{b,x},0\rangle_{AC})$$

Bob then sends register A to Alice, and keeps register C to himself. We want to show that if C contains much information about b then Alice detects Bob cheating with a good probability.
We can express $\alpha_{b,x}$ as a superposition,

$$|\alpha_{b,x}\rangle = |\phi_{b,x},w_{b,x}\rangle + |\phi_{\neg b,x},w'_{b,x}\rangle \quad (3)$$

where we have used the basis $|\phi_{b,x}\rangle$, $|\phi_{\neg b,x}\rangle$, for A. In this representation, the probability p Bob is caught cheating is:

$$p = \frac{1}{4}\sum_{b,x}||w'_{b,x}||^2 \quad (4)$$

which in particular implies that $||w'_{b,x}|| \le 2\sqrt{p}$.
We now want to express Bob's advantage. Let ρ_0 (ρ_1) be the reduced density matrix of the register B conditioned on the event that $b=0$ ($b=1$). Then,

$$\rho_b = \sum_x Pr(x)(|w_{b,x}\rangle\langle w_{b,x}| + |w'_{b,x}\rangle\langle w'_{b,x}|) \quad (5)$$

Bob's advantage is at most the trace distance between ρ_0 and ρ_1, and we want to bound it from above. Triangle inequality gives: $||\rho_0-\rho_1||_t \le \frac{1}{2}(\ |||w_{0,0}\rangle\langle w_{0,0}| - |w_{1,1}\rangle\langle w_{1,1}|||_t + |||w_{0,1}\rangle\langle w_{0,1}| - |w_{1,0}\rangle\langle w_{1,0}|||_t + \sum_{b,x}|||w'_{b,x}\rangle\langle w'_{b,x}|||_t\ )$.
As the trace norm of two pure states a and b is $2\sqrt{1-|\langle a|b\rangle|^2}$, and using Equation 4, we get:

$$\begin{aligned}||\rho_0-\rho_1||_t &\le \sqrt{1-|\langle w_{0,0}|w_{1,1}\rangle|^2} + \\ &\quad \sqrt{1-|\langle w_{0,1}|w_{1,0}\rangle|^2} + 2p\end{aligned}$$

We now claim;

LEMMA 11. *$|\langle w_{0,0}|w_{1,1}\rangle|$, $|\langle w_{0,1}|w_{1,0}\rangle| \ge 1 - O(ctg^2(2\theta)+4)p$.*

Thus, altogether, $||\rho_0-\rho_1||_t \le O(ctg(2\theta)\sqrt{p})$ which completes the proof. □

We now turn to the proof of Lemma 11.

PROOF. (of Lemma).
We will prove that all the unprimed w vectors lie in one bunch of small width, using the unitarity of U. The unitarity of U implies that $\langle\phi_{b,x}|\phi_{b',x'}\rangle = \langle\alpha_{b,x}|\alpha_{b',x'}\rangle$. We can express $\alpha_{b,x}$ as in Equation 3. We get:

$$\begin{aligned}\langle\phi_{b,x}|\phi_{b',x'}\rangle &= \langle\phi_{b,x}|\phi_{b',x'}\rangle\langle w_{b,x}|w_{b',x'}\rangle + \\ &\quad \langle\phi_{b,x}|\phi_{\neg b',x'}\rangle\langle w_{b,x}|w'_{b',x'}\rangle + \\ &\quad \langle\phi_{\neg b,x}|\phi_{b',x'}\rangle\langle w'_{b,x}|w_{b',x'}\rangle + \\ &\quad \langle\phi_{\neg b,x}|\phi_{\neg b',x'}\rangle\langle w'_{b,x}|w'_{b',x'}\rangle\end{aligned}$$

Substituting the values b,x,b',x' for actual values, and noticing that $|\langle w'_{b,x}|w'_{b',x'}\rangle| \le 4p$, we in particular get the following equations:

$$\begin{aligned}\langle w_{b,x}|w_{b,x}\rangle &=_{4p} 1 & (6)\\ \langle w_{0,0}|w'_{1,0}\rangle + \langle w'_{0,0}|w_{1,0}\rangle &= 0 & (7)\\ \langle w_{0,1}|w'_{1,1}\rangle + \langle w'_{0,1}|w_{1,1}\rangle &= 0 & (8)\end{aligned}$$

$$\begin{aligned}\langle w_{1,0}|w'_{1,1}\rangle - \langle w'_{1,0}|w_{1,1}\rangle &=_{4cp/s} \frac{c}{s}(1-\langle w_{1,0}|w_{1,1}\rangle) & (9)\\ \langle w_{0,1}|w'_{1,0}\rangle + \langle w'_{0,1}|w_{1,0}\rangle &=_{4sp/c} \frac{s}{c}(1-\langle w_{0,1}|w_{1,0}\rangle) & (10)\\ -\langle w_{0,0}|w'_{1,1}\rangle - \langle w'_{0,0}|w_{1,1}\rangle &=_{4sp/c} \frac{s}{c}(1-\langle w_{0,0}|w_{1,1}\rangle) & (11)\\ \langle w'_{0,0}|w_{0,1}\rangle - \langle w_{0,0}|w'_{0,1}\rangle &=_{4cp/s} \frac{c}{s}(1-\langle w_{0,0}|w_{0,1}\rangle) & (12)\end{aligned}$$

where $c = \cos(2\theta)$, $s = \sin(2\theta)$ and we write $x =_q y$ if $|x - y| \leq q$. A partial result can already be derived from what we have so far. By equation 4, we note that the length of the primed w vectors is at most $2\sqrt{p}$. Inserting this to equations 10 and 11, we get that $|\langle w_{0,0}|w_{1,1}\rangle|$ and similarly $|\langle w_{0,1}|w_{1,0}\rangle|$ are close to 1 up to terms of order $\sqrt{p}$. This is a weaker than the result which we want to achieve in lemma 11, which is closeness to 1 up to order p terms. If we stop here, the closeness of the unprimed w vectors up to order $\sqrt{p}$ implies that Bob's information is at most of the order of $\sqrt[4]{p}$. Note, however, that so far all we have used is unitarity, and we have not used the particular properties of the set of vectors we use in the protocol. In the rest of the proof, we will use the symmetry in protocol 1 to improve on this partial result, and to show that Bob's information is at most of the order of $\sqrt{p}$. Basically, the symmetry which we will use is the fact that the vectors in the protocol can be paired into orthogonal vectors.

We proceed as follows. The idea is to express equations 9-12 as inequalities involving only the distances between two w vectors, $||w_{b,x} - w_{b',x'}||$ and then to solve the set of the four inequalities to give an upper bound on the pairwise distances. This will imply a bound on the inner products, $\langle w_{b,x}|w_{b',x'}\rangle$, by the following connection:

Claim 12. $1 - Re(\langle w_{b,x}|w_{b',x'}\rangle) \geq \frac{||w_{b,x}-w_{b',x'}||^2}{2}$.

where $Re(z)$ denotes the real part of the complex number z.

Proof. $||w_{b,x} - w_{b',x'}||^2 = \langle w_{b,x} - w_{b',x'}|w_{b,x} - w_{b',x'}\rangle \leq 2 - 2Re(\langle w_{b,x}|w_{b',x'}\rangle)$. □

We denote:

$$\begin{aligned}a &= ||w_{0,0} - w_{0,1}||\\ b &= ||w_{0,0} - w_{1,1}||\\ c &= ||w_{0,1} - w_{1,0}||\\ d &= ||w_{1,0} - w_{1,1}||\end{aligned}$$

Let LHS (RHS) be the sum of the left (right) hand side of the last four equations.

Claim 13. $Re(RHS) \geq \frac{c}{2s}(a^2 + d^2) + \frac{s}{2c}(b^2 + c^2)$.

Proof.

$$\begin{aligned}Re(RHS) &= \frac{c}{s}(2 - Re(\langle w_{0,0}|w_{0,1}\rangle) - Re(\langle w_{1,0}|w_{1,1}\rangle))\\ &+ \frac{s}{c}(2 - Re(\langle w_{0,0}|w_{1,1}\rangle) - Re(\langle w_{0,1}|w_{1,0}\rangle))\end{aligned}$$

and now we can apply claim 12. □

Expressing the left hand side of the equations in terms of a, b, c and d might look a bit more complicated, and this is where we invoke the symmetric properties of the protocol, namely equations 7 and 8.

Claim 14. $Re(LHS) \leq 4\sqrt{p}(a + b + c + d)$

Proof. We first look at the LHS of Equation 11 + Equation 12. By adding $\langle w_{0,1}|w'_{1,1}\rangle + \langle w'_{0,1}|w_{1,1}\rangle = 0$ (due to Equation 8) and by using the fact that $Re(\langle\alpha|\beta\rangle) = Re(\langle\beta|\alpha\rangle)$ we get that the LHS of these two equations contributes $Re(\langle w'_{0,0}|w_{0,1} - w_{1,1}) + Re(\langle w'_{0,1}|w_{1,1} - w_{0,0}) + Re(\langle w'_{1,1}|w_{0,1} - w_{0,0}) \leq 2\sqrt{p}(c + d) + 2\sqrt{p}b + 2\sqrt{p}a$.
Similarly, the LHS of Equation 9 +Equation 10 is $Re(\langle w'_{1,0}|w_{0,1} - w_{1,1}) + Re(\langle w'_{0,1}|w_{1,0} - w_{1,1}) + Re(\langle w'_{1,1}|w_{1,0} - w_{0,1}) \leq 2\sqrt{p}(a + b + d + c)$.
Altogether, $Re(LHS) \leq 4\sqrt{p}(a + b + c + d)$. □

Combining Claims 14 and 13 with our knowledge that $Re(RHS) \leq Re(LHS) + \frac{8cp}{s} + \frac{8sp}{c}$ we get:

$$\frac{c}{2s}(a^2 + d^2) + \frac{s}{2c}(b^2 + c^2) \leq$$
$$4\sqrt{p}(a + b + c + d) + \frac{8cp}{s} + \frac{8sp}{c}$$

We want to show that a, b, c, d are all of the order of $\sqrt{p}$. Define $\Delta = a + b + c + d$. For $0 \leq \theta \leq \frac{\pi}{8}$, $ctg(2\theta) \geq tg(2\theta)$. Since all terms in the left hand side are positive, we have for each of a, b, c, d an upper bound in terms of Δ:

$$a^2, b^2, c^2, d^2 \leq \frac{8\Delta\sqrt{p}}{s/c} + 16p(1 + (\frac{c}{s})^2)$$

Thus, $\Delta = a + b + c + d \leq 4\sqrt{\frac{8\Delta\sqrt{p}c}{s} + \frac{16p}{s^2}}$.
Solving the quadratic equation

$$\Delta^2 - \frac{2^7\sqrt{p}c}{s}\Delta - \frac{2^8 p}{s^2} \leq 0$$

for Δ we get

$$\Delta \leq 132 \cdot \sqrt{p} \cdot ctg(2\theta)$$

Finally,

$$\begin{aligned}|\langle w_{0,0}|w_{1,1}\rangle| &\geq |Re(\langle w_{0,0}|w_{1,1}\rangle)|\\ &= \frac{||w_{0,0}||^2 + ||w_{1,1}||^2 - b^2}{2}\\ &\geq \frac{2 - b^2 - 8p}{2}\\ &\geq 1 - (2^{15}ctg^2(2\theta) + 4)p\end{aligned}$$

where the third inequality is true due to equation 6. Similarly, we have the same lower bound for $|\langle w_{0,1}|w_{1,0}\rangle|$, which implies lemma 11.

Thus, our bit escrow protocol gives quadratic sealing.

Remark 1. *Protocol 1 is sealing even if we modify it a little bit, as follows: at* revealing *time Alice first reveals b and then Bob returns the qubit q. In other words, if Bob has learned ϵ information about b after the deposit stage, then even if later on he gets to know b, he cannot avoid being detected with probability $\Omega(\epsilon^2)$. To see this, we use linearity. If Bob has a strategy which gives him detection probability p in the modified protocol, then w.l.o.g. his strategy is to apply the identity if $b = 0$ and some unitary operation U if $b = 1$.*

However, since the $b=1, x=0$ and $b=1, x=1$ cases are linear combinations of the $b=0, x=0$ and $b=0, x=1$ cases, one can show that if Bob's probability for detection is p in the $b=0$ case, then it is also $O(p)$ in the $b=1$ case, and therefore Bob does not have to apply U in the first place. This means that if he has a cheating strategy for the modified protocol, then he also has a cheating strategy with about the same parameters for protocol 1, and so by Theorem 10 the modified protocol is also quadratically secure.

REMARK 2. *One might suspect that this quadratic gap will always be the case for any reasonable set of vectors for Alice. This is not correct. If Alice only uses $\phi_{0,1}$ and $\phi_{1,0}$, then Bob has a strategy which gives him $\sqrt[4]{p}$ advantage. We will not elaborate on this in this paper.*

4.2 A Quadratic Strategy for Bob

THEOREM 15. *Let ρ_0, ρ_1 be two density matrices of the same dimension, such that $\|\rho_0 - \rho_1\|_t = t$. Consider the following protocol. Alice tosses a random bit b. She chooses a pure state from the mixture ρ_b, and sends it to Bob. Then Bob returns to Alice the state, and Alice projects it on the original state to test whether Bob has manipulated it. We claim that for any $1 \geq p \geq 0$, there is a strategy for Bob such that he learns b with advantage $t\sqrt{p}$, and his probability of detection is at most $\frac{1}{2}(1-\sqrt{1-p})$, which is $\Theta(p)$ for small p.*

proof: Alice prepares an encoding ψ_b of $b \in \{0,1\}$ in register B, and sends register B to Bob. Let ρ_b be the reduced density matrix of ψ_b to register B. We denote $t = ||\rho_0 - \rho_1||_t$. By Theorem 3 we know that if Bob is interested in learning information about b, and is not concerned with being detected cheating, the best he can do is a measurement according to the eigenvalue basis of $\rho_0 - \rho_1$. Given, any $0 \leq p \leq 1$ we modify this strategy to a strategy where the detection probability is at most p, and yet, Bob gets much information.
Let us consider more precisely Bob's best strategy for learning b if he is not concerned with being caught. Let $\{e_1, \ldots, e_K\}$ be the eigenvector basis of $\rho_0 - \rho_1$. Let V^+ (V^-) be the set of eigenvectors e with non-negative (negative) eigenvalues. The measurement M is defined by the Hermitian matrix for which V^+ is an eigenspace of eigenvalue 0 and V^- is an eigenspace of eigenvalue 1. By Theorem 3

$$|Trace(\rho_0 M) - Trace(\rho_1 M)| = \frac{t}{2} \qquad (13)$$

To apply a weak form of the measurement M, Bob takes a one qubit ancilla C. He applies a unitary transformation U on the received message and the ancilla, as follows:

$$U|e,0\rangle = \begin{cases} |e,0\rangle & \text{If } e \in V^+ \\ |e\rangle \otimes |v\rangle & \text{If } e \in V^- \end{cases}$$

where $|v\rangle = \sqrt{1-p}|0\rangle + \sqrt{p}|1\rangle$ and U is completed to a unitary transformation. After applying U Bob returns register B to Alice, and keeps the ancilla C for himself. Notice that the special case $p=1$ is equivalent to the measurement M.

LEMMA 16. $||U\rho_0|_C - U\rho_1|_C||_t = t\sqrt{p}$.

PROOF. We will show

CLAIM 17.

$$\begin{aligned} U\rho_0|_C &= Trace(\rho_0 M)|0\rangle\langle 0| + (1 - Trace(\rho_0 M))|v\rangle\langle v| \\ U\rho_1|_C &= Trace(\rho_1 M)|0\rangle\langle 0| + (1 - Trace(\rho_1 M))|v\rangle\langle v| \end{aligned}$$

Thus, $U\rho_0|_C - U\rho_1|_C = (Trace(\rho_0 M) - Trace(\rho_1 M))(|0\rangle\langle 0| - |v\rangle\langle v|) = \pm \frac{t}{2}(|0\rangle\langle 0| - |v\rangle\langle v|)$, where the last equality is due to Equation 13. Since, $|||0\rangle\langle 0| - |v\rangle\langle v|||_t = 2\sqrt{1 - \langle 0|v\rangle|^2} = 2\sqrt{p}$ we get $||U\rho_0|_C - U\rho_1|_C||_t = t\sqrt{p}$ as desired. □

We now prove Claim 17.

PROOF. (of Claim 17). We express $\rho_0 = \sum_j w_j |\alpha_j\rangle\langle\alpha_j|$, where α_j is a pure state.We further express each α_j in the eigenbasis $\{e_i\}$:

$$|\alpha_j\rangle = \sum_{i+} a_{ij}^+ |e_i^+\rangle + \sum_{i-} a_{ij}^- |e_i^-\rangle$$

Applying U, this state is taken to:

$$U|\alpha_j, 0\rangle = \sum_{i+} a_{ij}^+ |e_i^+\rangle|0\rangle + \sum_{i-} a_{ij}^- |e_i^-\rangle|v\rangle$$

The reduced density matrix to the register C, in case of event $|\alpha_j\rangle$ is:

$$\textstyle\sum_{i+} |a_{ij}^+|^2 |0\rangle\langle 0| + \sum_{i-} |a_{ij}^-|^2 |v\rangle\langle v|$$

and altogether, $U\rho_0|_C = \sum_j w_j (\sum_{i+} |a_{ij}^+|^2)|0\rangle\langle 0| +$
$\sum_j w_j (\sum_{i-} |a_{ij}^-|^2)|v\rangle\langle v|$. To complete the proof we just notice that $\sum_j w_j(\sum_{i+} |a_{ij}^+|^2) = Trace(\rho_0 M)$. The proof for $U\rho_0|_C$ is similar. □

We now analyze the error detection probability.

LEMMA 18. $Prob(err) \leq \frac{1}{2}(1 - \sqrt{1-p})$

PROOF. Say Alice sent Bob the state $|w\rangle$. We can express it as $|w\rangle = a|w^+\rangle + b|w^-\rangle$ where $|w^+\rangle \in Span(V^+)$ and $|w^-\rangle \in Span(V^-)$. Bob applies U on w and gets

$$\begin{aligned} U|w\rangle &= a|w^+, 0\rangle + b|w^-, v\rangle \\ &= a|w^+, 0\rangle + \sqrt{1-p}\,b|w^-, 0\rangle + \sqrt{p}\,b|w^-, 1\rangle \end{aligned}$$

Therefore, if we measure the last qubit, then with probability pb^2 we end up in $|w^-\rangle$ and with probability $1 - pb^2$ we end up in $a|w^+\rangle + \sqrt{1-p}\,b|w^-\rangle$ normalized. Thus the density matrix of $U|w\rangle$ after tracing out the last qubit is:

$$\rho = \begin{pmatrix} |a|^2 & b\bar{a}\sqrt{1-p} \\ \bar{b}a\sqrt{1-p} & |b|^2 \end{pmatrix}$$

To find out the probability for Alice not to detect Bob cheating, we calculate $\langle w|\rho|w\rangle$. We get:

$$\begin{aligned} Pr(\neg Err) &= |a|^4 + 2|ab|^2\sqrt{1-p} + |b|^4 \\ &= 1 - 2|ab|^2(1 - \sqrt{1-p}) \end{aligned}$$

The probability of Alice detecting an error is thus $2|ab|^2(1 - \sqrt{1-p}) \leq \frac{1}{2}(1 - \sqrt{1-p})$. □

REMARK 3. *The average of $|ab|$ can tend to 0.5, even when t tends to 0. This can be seen by taking ρ_0 to be composed of two states which are the basis states $|0\rangle$ and $|1\rangle$ rotated by θ towards each other, whereas ρ_1 is the mixture of the basis states rotated by θ outwards. As θ tends to 0, t tends to 0, but $|ab|$ tend to 0.5.*

5. PROOF OF THEOREM 2

We show that no cheater can control the game.

When Bob cheats :

Suppose Alice is honest and Bob is arbitrary. Let us look at the mixture that Alice generates at the first step of Protocol 2. Let $\rho_{b=0}$ be the density matrix in the case $b=0$, and $\rho_{b=1}$ in the case $b=1$. Then $||\rho_{b=0}-\rho_{b=1}||_t = 2\cos(2\theta)$. It follows from Theorem 3 that whatever Bob does, the probability that $b'=b$ and Bob wins is at most $\Pr(b'=b) \leq \frac{1}{2}+\frac{\cos(2\theta)}{2} = \cos^2(\theta)$ which for $\theta=\frac{\pi}{8}$ is at most 0.86.

When Alice cheats :

Now, suppose Bob is honest and Alice is arbitrary. $Prob(\text{Alice wins }) = x$, which is at most $\frac{p_0+q_1}{2}$, whereas the probability that Alice loses is at least $\frac{p_1+q_0}{2}$. The difference $|x-(1-x)|$ is at most $\frac{p_0-q_0+q_1-p_1}{2} \leq \frac{|p_0-q_0|+|p_1-q_1|}{2} = |p_0-q_0|$, i.e., $x \leq \frac{1+|p_0-q_0|}{2}$.

Also, $\frac{p_{err}+q_{err}}{2} \leq 1-x$, as whenever Alice is caught cheating she loses. This implies that $\sqrt{p_{err}}+\sqrt{q_{err}} \leq 2\sqrt{1-x}$ as the maximum is obtained when $p_{err} = q_{err} = 1-x$.

Finally, from the proof of Theorem 5 we have $|p_0 - q_0| \leq \frac{\sqrt{p_{err}}+\sqrt{q_{err}}}{cos(2\theta)}$. Putting it all together we get:

$$\begin{aligned} x &\leq \frac{1+|p_0-q_0|}{2} \\ &\leq \frac{1}{2}+\frac{\sqrt{p_{err}}+\sqrt{q_{err}}}{2cos(2\theta)} \\ &\leq \frac{1}{2}+\frac{\sqrt{1-x}}{\cos(2\theta)} \end{aligned}$$

For $\theta=\frac{\pi}{8}$ we get the quadratic equation $4x^2+4x-7 \leq 0$. Solving it we get $x \leq \frac{\sqrt{8}-1}{2} \leq 0.9143$.

6. REFERENCES

[1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC-98)*, pages 20–30, New York, May 23–26 1998. ACM Press.

[2] Manuel Blum. Coin flipping by telephone: A protocol for solving impossible problems. In Allen Gersho, editor, *Advances in Cryptology: A Report on CRYPTO 81*, pages 11–15. Department of Electrical and Computer Engineering, U. C. Santa Barbara, 24–26 August 1981.

[3] Lucien Hardy and Adrian Kent. Cheat sensitive quantum bit commitment. Technical report, quant-ph/9911043, 1999.

[4] R. Jozsa. fidelity. *J. Mod. Optics*, 41, 1994.

[5] H. Lo and H. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, 120:177–187, 1998. See also quant-ph/9711065.

[6] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, 1997.

[7] D. Mayers, L. Salvail, and Y. Chiba-Kohno. Unconditionally secure quantum coin tossing. Technical report, quant-ph/9904078, 1999.

[8] J. Preskill. Lecture notes. http://www.theory.caltech.edu/people/preskill/ph229/.