Strong connections between quantum encodings, non-locality and quantum cryptography

Jamie Sikora, André Chailloux, Iordanis Kerenidis

Strong connections between quantum encodings, non-locality and quantum cryptography

Jamie Sikora,[1] André Chailloux,[2] and Iordanis Kerenidis[1,3]

[1] *Laboratoire d'Informatique Algorithmique: Fondements et Applications, CNRS - Université Paris Diderot, France.*
[2] *INRIA Paris-Roquencourt, SECRET Project-Team, France.*
[3] *Centre for Quantum Technologies, National University of Singapore, Singapore.*

(Dated: April 3, 2014)

Encoding information in quantum systems can offer surprising advantages but at the same time there are limitations that arise from the fact that measuring an observable may disturb the state of the quantum system. In our work, we provide an in-depth analysis of a simple question: What happens when we perform two measurements sequentially on the same quantum system? This question touches upon some fundamental properties of quantum mechanics, namely the uncertainty principle and the complementarity of quantum measurements. Our results have interesting consequences, for example they can provide a simple proof of the optimal quantum strategy in the famous Clauser-Horne-Shimony-Holt game. Moreover, we show that the way information is encoded in quantum systems can provide a different perspective in understanding other fundamental aspects of quantum information, like non-locality and quantum cryptography. We prove some strong equivalences between these notions and provide a number of applications in all areas.

Quantum information studies how information is encoded in quantum systems and how it can be observed through measurements. On one hand, the exponential number of amplitudes that describe the state of a quantum system can be used in order to encode a vast amount of classical information into the state of a quantum system. Hence, we can use quantum information to resolve many distributed tasks much more efficiently than with classical information [1–3]. On the other hand, quantum information does not always offer advantages, since every time an observer measures a quantum system its state may collapse and information may become irretrievable. For example, Holevo's theorem [4], asserts that one quantum bit can be used to transmit only one bit of classical information and no more.

The intricate interplay between encoding information in quantum systems and measurement interference is at the heart of some fundamental results in quantum information, from Bell inequalities [5] to quantum key distribution [6]. Our goal is to deepen our understanding of the connections between quantum encodings, non-locality, and quantum cryptography and provide new insight on the power and limitations of quantum information, by looking at it through these various lenses.

This paper links three seemingly unrelated concepts in quantum information (encodings, non-local games, and cryptographic primitives) via properties of sequential non-commuting measurements. The technical part of this paper examines quantum encodings and bounds the success of sequentially measuring an encoding of two bits (or strings) to learn their XOR. We then show how these bounds can be used to study not only encodings, but non-local games and cryptographic tasks as well. The conceptual part of this paper discusses how the applications we consider are all equivalent in some sense. When viewing each as extracting information from a quantum encoding, we are able to preserve the three notions: (1) hiding the XOR in the encoding, (2) providing perfect security in the cryptographic task, and (3) satisfying the non-signaling principle in the non-local game.

In addition to providing philosophical insights towards each of these quantum tasks, we combine the technical and conceptual tools in this paper to give applications in all areas.

QUANTUM ENCODINGS AND COMPLEMENTARITY OF MEASUREMENTS

One of the fundamental postulates of quantum mechanics is Heisenberg's uncertainty principle which shows that it is impossible to perfectly ascertain the momentum and position of a particle. More precisely, entropic uncertainty relations provide explicit bounds on the entropy of the outcome distributions of the different measurements. For example, if we consider two measurements in the computational and Hadamard bases, then no matter the state of the quantum system, there is always some entropy in at least one of the outcome distributions, hence the measurement outcomes cannot be perfectly predicted simultaneously.

Another important notion, which is more closely related to quantum encodings, is the complementarity of quantum measurements. Complementarity analyzes what happens to the outcome distributions of measurements when performed sequentially on the same system. We say that two measurements are perfectly complementary, if after having performed the first measurement, no more information can be extracted by performing the second measurement on the post-measured state. This is, for example, the case with a Hadamard and a computational basis measurement, or any measurement after a

complete projective measurement. On the other hand, they are non-complementary if after measuring with one, the outcome distribution of the second is unaffected.

We make the connection of complementarity and quantum encodings clearer by considering the following scenario: Let us consider two different observables that take binary values $x_0 \in \{0,1\}$ and $x_1 \in \{0,1\}$ according to some known distribution. Assume that given one copy of a quantum system (of any dimension) in state ρ_{x_0,x_1}, i.e., a quantum encoding of the bits x_0, x_1, there exists a quantum measurement, i.e., a decoding procedure, that correctly measures x_0 with probability p_0 and a different measurement that correctly measures x_1 with probability p_1. We would like to analyze these probabilities and more specifically the *average decoding probability* $(p_0 + p_1)/2$.

Uncertainty relations show that when the measurements are "incompatible" the average decoding probability cannot be too large. For example, for the computational and Hadamard bases one can show this probability is always at most $\cos^2(\pi/8)$. There are many cases where we do not know the different measurement operators, only the probabilities they succeed. For example, one may not know the measurements used in an implicit strategy in a cryptographic protocol or quantum non-local game where the only defining property of the strategy is the success probability. Could we still provide some interesting bound on the average decoding probability that would hold independent of the measurement operators, possibly by relating it to some other property of the quantum encoding?

We provide such bounds by relating the average decoding probability to the decoding probability of some other function $f(x_0, x_1)$ of the bits. Classically, it is straightforward to relate the probability of decoding $f(x_0, x_1)$ to the probabilities of decoding each bit x_i; in the quantum world, this task is delicate. Suppose we want to compute the XOR of the two bits (i.e., compute whether the two bits have the same value or not), and for this we perform the measurement for each bit x_i in sequence. Once the first bit is decoded, the post-measured state is an eigenstate of the first operator, hence the probability of then correctly decoding the second bit may have changed.

Much of the previous literature about measuring the post-measured state concerns ideas surrounding Heisenburg's uncertainty principle (see, for example, [7] and the references therein). In a setting more related to this paper, post-measurement information has been used for state discrimination [8, 9]. This is useful for cryptography in the bounded-storage model [10] and the noisy-storage model [11, 12].

LEARNING RELATIONS

Our first contribution is an analysis of the process of sequentially performing two measurements on the same quantum state: Let $|\psi\rangle$ be a pure state and $\{C, 1-C\}$, $\{D, 1-D\}$ be two projective measurements such that $\cos^2(\alpha) := \|C|\psi\rangle\|_2^2 \geq \frac{1}{2}$ and $\cos^2(\beta) := \|D|\psi\rangle\|_2^2 \geq \frac{1}{2}$, where C and D correspond to correctly measuring. Through geometric arguments, we bound the probability that both measurements succeed (give the correct guess) or both fail (give the incorrect guess) as:

$$\cos^2(\alpha-\beta) \geq \|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \geq \cos^2(\alpha+\beta). \quad (1)$$

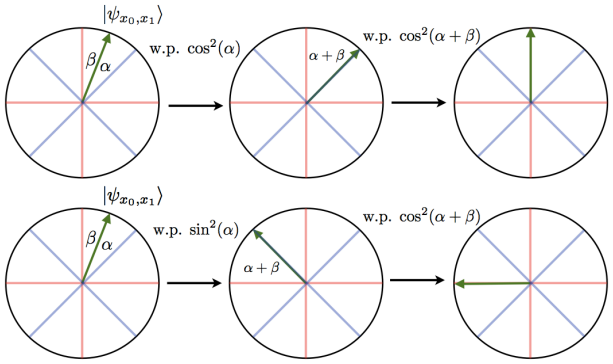

FIG. 1: (Color online) Simple scenario for the lower bound in Equation (1): Two-outcome projective measurements on a pure state in two dimensions. By successive measurements, one can learn the XOR by learning both bits correctly or by learning both bits incorrectly. This occurs with probability $\cos^2(\alpha)\cos^2(\alpha+\beta) + \sin^2(\alpha)\cos^2(\alpha+\beta) = \cos^2(\alpha+\beta)$.

In the language of quantum encodings, we can use (1) to provide the following learning relation for bits, and extend it to strings. (The proof of Equation (1) and Theorem 1, below, can be found in the appendix.)

Theorem 1. *For any quantum encoding of bits x_0 and x_1,* $\Pr[\text{learning } x_0 \oplus x_1] \geq (2c-1)^2$, *where we define* $c := \frac{1}{2}\Pr[\text{learning } x_0] + \frac{1}{2}\Pr[\text{learning } x_1]$. *For $x_0, x_1 \in \{0,1\}^n$, if $c \geq 1/2$, then we have* $\Pr[\text{learning } x_0 \oplus x_1] \geq \Pr[\text{learning } (x_0, x_1)] \geq c(2c-1)^2$.

The probability of learning a bit (or a bit string) is the maximum over all quantum measurements of correctly measuring the bit (or bit string). Theorem 1 shows that, independent of the measurements, the average probability of correctly measuring two observables cannot be very large unless at the same time the probability of correctly measuring both or none of the observables is large as well. A similar result has been obtained for a restricted class of encodings, those based on *hyperbits* [13].

We can now define a measure of complementarity Γ, as the difference between the probability of decoding the XOR of the two bits and the probability had the measurements been non-complementary. By Equation (1),

$$
\begin{aligned}
|\Gamma| &= \Big| \|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \\
&- \|C|\psi\rangle\|_2^2 \|D|\psi\rangle\|_2^2 - \|(1-C)|\psi\rangle\|_2^2 \|(1-D)|\psi\rangle\|_2^2 \Big| \\
&\leq \frac{1}{2}\sin(2\beta)\sin(2\alpha). \qquad (2)
\end{aligned}
$$

Note Γ is zero for non-complementary measurements and our bound can be saturated, e.g., when $C = D$ we have $\Gamma = \frac{1}{2}\sin(2\beta)\sin(2\alpha)$, and for $C = 1 - D$ we have $\Gamma = -\frac{1}{2}\sin(2\beta)\sin(2\alpha)$.

THE CLAUSER-HORNE-SHIMONY-HOLT GAME AS A QUANTUM ENCODING

Non-locality is a fundamental property of quantum information. Here, two space-like separated parties, Alice and Bob, initially share some resource and do not communicate further. We study the joint probability distributions of measurement outcomes that can arise when Alice and Bob perform measurements locally. Bell inequalities provide bounds on the possible distributions when the initial resource is classical and we are interested in the maximum violation when Alice and Bob share quantum entanglement.

One can describe Bell inequalities as games between Alice and Bob. For example, in the Clauser-Horne-Shimony-Holt (CHSH) game [14], Alice receives a random $x \in \{0,1\}$ and outputs $a \in \{0,1\}$ and Bob receives a random $y \in \{0,1\}$ and outputs $b \in \{0,1\}$. The quantum value of the game, $\omega^*(\text{CHSH})$, is the maximum probability that $a \oplus b = yx$ over all initial states and all measurement operators. There is a quantum strategy to win this game with probability $\cos^2(\pi/8)$; moreover, Tsirelson's bound shows this value is optimal [15].

Recently, non-locality has been studied from the point of view of information. The goal is to understand quantum mechanics through information principles: for example, why is there a quantum strategy for the CHSH game with probability exactly $\cos^2(\pi/8)$ and not more? *Information causality*, one such postulate about information transmission, asserts that any theory that abides to it must comply with Tsirelson's bound for the CHSH game [16]. To make the connection between non-locality and quantum information more clear, let us see how we can recast the CHSH game as a quantum encoding: Once Alice receives x and measures a, Bob's post-measurement state can be seen as an encoding of a and x. When $y = 0$, Bob needs to output a and when $y = 1$, he needs to output $a \oplus x$. Hence, we can write the value as $\omega^*(\text{CHSH}) = \frac{1}{2}(\Pr[\text{Bob learns } a] + \Pr[\text{Bob learns } a \oplus x])$. Note that the non-signaling condition of CHSH implies the probability of Bob guessing Alice's input x is $1/2$ or equivalently the probability of learning the XOR of a and $a \oplus x$ is $1/2$ (in this case, we say that the encoding "hides" the XOR). With this perspective, Theorem 1 provides an alternative proof of Tsirelson's bound, since solving the inequality $(2\omega^*(\text{CHSH}) - 1)^2 \leq 1/2$ gives $\omega^*(\text{CHSH}) \leq \cos^2(\pi/8)$.

LEARNING RELATIONS AND OBLIVIOUS TRANSFER

Another area where quantum information has had great impact is cryptography. The properties of quantum information, for example, the uncertainty principle, enable secure key distribution protocols [6], however, when the two parties do not trust each other, there are only partial advantages. For example, quantum protocols for coin flipping or bit commitment can only restrict cheating to a probability of $1/\sqrt{2}$ or 0.739, respectively [17–19]. We wish to relate the ability to perform cryptographic primitives to non-locality and quantum encodings.

We look at *oblivious transfer* (OT), defined below.

Definition 1 (Imperfect oblivious transfer)**.** *A quantum oblivious transfer protocol with correctness p, denoted here as OT_p, is an interactive protocol with no inputs, between Alice and Bob such that:*

- *Alice outputs two independent, uniformly random bits (z_0, z_1) or Abort and Bob outputs uniformly random bit b and another bit w or Abort.*
- *If Alice and Bob are honest, $w = z_b$ with probability p.*
- *Alice and Bob can abort only if cheating is detected.*
- *If $p = 1$ we say the protocol is* perfect*.*

Ideally at the end of the protocol, Bob should only learn the value of z_b and Alice should remain oblivious to which bit Bob learned [20, 21]*.*

We also examine quantum oblivious *string* transfer protocols with correctness p, denoted here as OT_p^n which is defined analogously to an imperfect oblivious transfer protocol except z_0 and z_1 are n-bit strings.

Oblivious transfer is the most important task in providing security between distrustful parties, since any complex operation can be rendered secure using secure oblivious transfer [22]. Using Theorem 1, we prove a series of new results for oblivious transfer [32]. First, we extend the oblivious transfer bounds in [23] to oblivious string transfer, and show that in any protocol, either Alice can learn Bob's index or Bob can learn both of Alice's strings with probability at least 58.52% (proof in the appendix). Second, we consider the case when cheating Bob wants to learn the XOR of Alice's bits. Note that most definitions enforce that Bob gets no information about Alice's other bit (instead of the XOR of her bits). Classically, the two definitions are equivalent [24]. Quantumly, we use the XOR definition that relates directly to the CHSH game (discussed in the next section).

Theorem 2. *For any* OT_p *protocol, we have* $p \leq \Pr[\text{Alice learns b}]\left(\sqrt{\Pr[\text{Bob learns } z_0 \oplus z_1]} + 1\right)$.

Proof. We show how to use oblivious transfer to construct a *coin flipping* protocol. A quantum coin flipping protocol with correctness p, denoted CF_p, is an interactive protocol with no inputs, between Alice and Bob such that:

- The protocol is aborted with probability $1-p$ when Alice and Bob are honest.
- If the protocol is not aborted, then they both output a randomly generated bit c.

We say that the coin flipping protocol has cheating probabilities A_{CF} and B_{CF} where

- $A_{\mathrm{CF}} := \max_{c\in\{0,1\}} \Pr[\text{Bob accepts outcome } c]$,
- $B_{\mathrm{CF}} := \max_{c\in\{0,1\}} \Pr[\text{Alice accepts outcome } c]$.

The coin flipping protocol is as follows.

1. Alice and Bob perform the OT_p protocol so they have outputs (z_0, z_1) and (b, w) respectively.
2. If no one aborted, then Alice sends randomly chosen $d \in_R \{0,1\}$ to Bob.
3. Bob sends b and w to Alice.
4. If z_b from Bob is inconsistent with Alice's bits then Alice aborts. Otherwise, they both output $c = b \oplus d$.

We see that when Alice and Bob are honest, Alice aborts in this protocol with probability $1-p$, since p is the probability that Bob receives the correct bit in the OT_p protocol. If Alice does not abort, the outcome of the coin flipping protocol is random.

Cheating Alice: Let A_{OT} denote the probability Alice can learn b in the OT_p protocol (without Bob aborting) and let A_{CF} denote the probability Alice can force honest Bob to accept a desired outcome in the coin flipping protocol. It is straightforward to see that $A_{\mathrm{OT}} = A_{\mathrm{CF}}$.

Cheating Bob: Let B_{OT} denote the probability Bob can learn $z_0 \oplus z_1$ in the OT_p protocol (without Alice aborting) and let B_{CF} denote the probability Bob can force honest Alice to accept a desired outcome in the coin flipping protocol. Using our XOR learning relation for bits, and an analysis similar to the one in [23], we can show that $\frac{\sqrt{B_{\mathrm{OT}}}+1}{2} \geq B_{\mathrm{CF}}$. Kitaev's lower bound for coin flipping [17] states that

$$A_{\mathrm{CF}} B_{\mathrm{CF}} \geq \Pr[\text{Alice and Bob honestly output 0}]$$

for any quantum coin flipping protocol. In the case of the coin flipping protocol above, we have that Alice and Bob both output either bit with probability $p/2$ (since the protocol is aborted with probability $1-p$). Therefore, we have $A_{\mathrm{OT}}\frac{\sqrt{B_{\mathrm{OT}}}+1}{2} \geq A_{\mathrm{CF}}B_{\mathrm{CF}} \geq \frac{p}{2}$ implying $A_{\mathrm{OT}}\left(\sqrt{B_{\mathrm{OT}}}+1\right) \geq p$, proving Theorem 2. □

Notice that for secure protocols with $\Pr[\text{Alice learns b}] = \frac{1}{2}$ and $\Pr[\text{Bob learns } z_0 \oplus z_1] = \frac{1}{2}$, we have $p \leq \cos^2(\pi/8)$, which shows that the secure oblivious transfer protocol in [25] is optimal. Last, by relating oblivious transfer and bit commitment protocols [23], we prove that in any OT protocol with $p = 1$, Alice can learn Bob's index or Bob can learn the XOR of Alice's bits with probability at least 59.9% (proof in the appendix).

EQUIVALENCES BETWEEN CHSH-TYPE GAMES, SECURE OBLIVIOUS TRANSFER AND QUANTUM ENCODINGS

So far, we have used Theorem 1 to provide results about the CHSH game and oblivious transfer. We now show that these applications are deeply connected and can be extended to more intricate non-local games and oblivious transfer variants. Such non-local games are important since knowing their Bell inequality violations brings us that much closer to understanding the true power of quantum entanglement and the hope of characterizing it as a resource via the right information postulate(s).

We now consider *secure* OT_p^n protocols where Alice can obtain no information about Bob's index b (without him aborting) and Bob can obtain no information about $z_0 \oplus z_1$ (without Alice aborting).

We also consider the following generalization of the CHSH game.

Definition 2 (CHSH_n game)**.** *The* CHSH_n game *is a game between Alice and Bob where:*

- *Alice and Bob are allowed to create and share an entangled state* $|\psi\rangle$ *before the game starts. Once the game starts, there is no further communication between Alice and Bob.*
- *Alice receives a random string* $x \in \{0,1\}^n$ *and Bob receives a random bit* $y \in \{0,1\}$.
- *Alice outputs* $a \in \{0,1\}^n$ *and Bob outputs* $b \in \{0,1\}^n$.
- *Alice and Bob win if* $a_i \oplus b_i = y\,x_i$, *for all* $i \in \{1,\ldots,n\}$.

The value of the game, $\omega^*(\mathrm{CHSH}_n)$*, is the maximum probability which Alice and Bob can win.*

The CHSH game is the special case when $n = 1$ (we omit the subscript 1 in this case).

A relationship between learning probabilities and quantum games is pointed out in [26], where they show

that in any physical theory, the amount of non-locality and uncertainty of the theory are tightly linked. In our equivalences, we strengthen the quantum connection by conserving the notions of security / non-signaling / hidden XOR and we deal with the interactivity of oblivious transfer protocols.

Theorem 3. *The following four statements are equivalent for every $n \in \mathbb{N}$:*

1. *There is a quantum encoding of $x_0, x_1 \in \{0,1\}^n$ that hides the XOR and $\frac{1}{2}\sum_{c\in\{0,1\}} \Pr[\text{learn } x_c] = p$.*
2. *There is a secure, non-interactive OT_p^n protocol.*
3. *There is a secure OT_p^n protocol.*
4. *There is a strategy for winning the game CHSH_n with probability p.*

Proof. We provide four reductions.

(1. $\implies$ 2.). Let $\{\rho_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ be a set of quantum states and $\{\pi_{x_0,x_1} : x_0, x_1 \in \{0,1\}^n\}$ be a probability distribution satisfying the properties of statement 1 of Theorem 3. Alice chooses x_0, x_1 with probability π_{x_0,x_1} and sends ρ_{x_0,x_1} to Bob. Alice outputs $(z_0, z_1) := ((1-a)x_0 + ax_1 + d_1, (1-a)x_1 + ax_0 + d_2)$, for random choices of $a \in \{0,1\}$ and $d_1, d_2 \in \{0,1\}^n$ that she sends to Bob. The first bit randomizes the success probabilities for Bob (so he has an equal probability of learning z_0 and z_1) and the d_1, d_2 bit strings ensure that Alice's outcomes are random. Bob picks a random bit b and measures to learn z_b depending on a, d_1, d_2. In particular, the probability of learning z_b for $b \in \{0,1\}$ is equal to the average decoding probability of x_0 and x_1, hence equal to p. Note that $z_0 \oplus z_1 = x_0 \oplus x_1 \oplus d_1 \oplus d_2$ is hidden from Bob and Alice cannot learn b (since Bob does not send any message), thus this protocol is secure.

(2. $\implies$ 4.). Suppose there is a secure, non-interactive OT_p^n protocol. Without loss of generality [33], Alice and Bob's joint state from the non-interactive OT_p^n protocol is $1/2^n \sum_{z_0,z_1\in\{0,1\}^n} |z_0, z_1\rangle\langle z_0, z_1| \otimes \rho_{z_0,z_1}$, for some ρ_{z_0,z_1} in Bob's space $\mathcal{B}$. Since Alice has no information about b, Bob can use ρ_{z_0,z_1} and measurements $\{M^0_{z_0}\}_{z_0\in\{0,1\}^n}$, $\{M^1_{z_1}\}_{z_1\in\{0,1\}^n}$ to learn the value of Alice's first and second string, respectively, with $\Pr[\text{Bob learns } z_0] = \Pr[\text{Bob learns } z_1] = p$. Consider some purification $|\psi_{z_0,z_1}\rangle \in \mathcal{A}\otimes\mathcal{B}$ of ρ_{z_0,z_1} where $\mathcal{A}$ is controlled by Alice. Let

$$|\Omega\rangle := \frac{1}{2^n} \sum_{z_0,z_1\in\{0,1\}^n} |z_0 \oplus z_1\rangle_{\mathcal{A}_1} |z_0\rangle_{\mathcal{A}_2} |z_1\rangle_{\mathcal{A}_3} |\psi_{z_0,z_1}\rangle_{\mathcal{AB}},$$

$|\Omega_x\rangle$ to be the post-measured state assuming Alice measured $\mathcal{A}_1$ to get x, and $\rho_x := \mathrm{Tr}_{\mathcal{A}_2\mathcal{A}_3\mathcal{A}} |\Omega_x\rangle\langle\Omega_x|$ to be Bob's state. We have $\rho_x = \rho_0$, $\forall x \in \{0,1\}^n$, since Bob has no information about $z_0 \oplus z_1$. By Uhlmann's theorem, for all $x \in \{0,1\}^n$, there exists unitary U_x on $\mathcal{A}_2 \otimes \mathcal{A}_3 \otimes \mathcal{A}$ with $(U_x \otimes I_{\mathcal{B}})|\Omega_0\rangle = |\Omega_x\rangle$. We define the CHSH_n strategy:

1. Alice and Bob share the state $|\Omega_0\rangle$ and receive random $x \in \{0,1\}^n$ and $y \in \{0,1\}$, respectively.
2. Alice applies (U_x) such that Alice and Bob share the state $|\Omega_x\rangle$. She measures the space $\mathcal{A}_2$ in the computational basis to get her outcome a.
3. Bob applies the measurement $\{M^y_b\}_{b\in\{0,1\}^n}$ on his space $\mathcal{B}$ to determine his outcome b.

Conditioned on Alice receiving x and outputting a, Bob has the state $\mathrm{Tr}_{\mathcal{A}}|\psi_{a,x\oplus a}\rangle\langle\psi_{a,x\oplus a}| = \rho_{a,x\oplus a}$. If Bob gets $y = 0$, he must output $b = a$. If Bob gets $y = 1$, he must output $b = a \oplus x$. The probability they win the CHSH_n game with this strategy is hence equal to p.

(3. $\implies$ 1.). Let $|\Omega\rangle_{\mathcal{AB}}$ be the final joint state of the OT_p^n protocol for honest Alice and Bob. Suppose Alice measures to learn (z_0, z_1) which are distributed uniformly. Let ρ_{z_0,z_1} be Bob's post-measured state. Then, $\{\rho_{z_0,z_1} : z_0, z_1\}$ and π being the uniform distribution satisfy the hidden XOR condition, since Alice does not abort (both parties are honest), and the protocol is secure. We now describe a procedure to decode each z_c, for $c \in \{0,1\}$, with probability p.

We may assume Bob measures his part of the state $|\Omega\rangle_{\mathcal{AB}}$ (instead of decoding ρ_{z_0,z_1}) since it does not matter if Alice measures before or after Bob. Suppose $|\Omega_b\rangle_{\mathcal{AB}}$ is the post-measured joint state when Bob partially measures $|\Omega\rangle_{\mathcal{AB}}$ to obtain his index b. Since Bob will not abort and the protocol is secure, we know b is hidden from Alice. Again, by Uhlmann's theorem, Bob can transform $|\Omega_0\rangle$ to $|\Omega_1\rangle$ and vice versa via a unitary acting on $\mathcal{B}$. Hence Bob can measure $|\Omega\rangle_{\mathcal{AB}}$ to learn b, collapse the state to $|\Omega_b\rangle$ and then apply the unitary mapping $|\Omega_b\rangle$ to $|\Omega_c\rangle$. He then uses the decoding procedure of the OT_p^n protocol to learn z_c with probability p.

(4. $\implies$ 1.). Let $|\Omega\rangle_{\mathcal{AB}}$ be the state that Alice and Bob share before receiving x and y in a CHSH_n game strategy that succeeds with probability p. Suppose Alice measures to learn a (conditioned on x). Let $\rho_{a,x}$ be Bob's post-measured state which occurs with probability $\pi_{a,x}$. We define the necessary states and probabilities by relabelling $a \to x_0$ and $x \oplus a \to x_1$. Then, Bob has no information about $x_0 \oplus x_1 = a \oplus (x \oplus a) = x$ from non-signaling, and the average decoding probability for x_0 and x_1 is p.

Since trivially (2. $\implies$ 3.), we conclude the proof of Theorem 3. □

We can also prove an equivalence between quantum encodings of n pairs of bits that hide the XOR of each pair and the n-fold repetitions of CHSH and OT, defined

below.

Definition 3 (n-fold repetition of oblivious transfer)**.** *A quantum n-fold repetition of oblivious transfer protocol with correctness p, denoted here as $\mathrm{OT}_p^{\otimes n}$, with cheating probabilities $A_{\mathrm{OT}^{\otimes n}}$ and $B_{\mathrm{OT}^{\otimes n}}$, is defined analogously to an imperfect oblivious string transfer protocol except b is an n-bit string (so z_b takes values from each of Alice's strings according to b). We say an $\mathrm{OT}_p^{\otimes n}$ protocol is secure if Alice can gain no information about the string b (without Bob aborting) and if Bob can gain no information about the string $z_0 \oplus z_1$ (without Alice aborting).*

Definition 4 (n-fold repetition of CHSH)**.** *An n-fold repetition of* CHSH*, denoted $\mathrm{CHSH}^{\otimes n}$, is a game between Alice and Bob where:*

- *Alice and Bob are allowed to create and share an entangled state $|\psi\rangle$ before the game starts. Once the game starts, there is no further communication between Alice and Bob.*
- *Alice receives a random $x \in \{0,1\}^n$ and Bob receives a random $y \in \{0,1\}^n$.*
- *Alice outputs $a \in \{0,1\}^n$ and Bob outputs $b \in \{0,1\}^n$.*
- *Alice and Bob win if $a_i \oplus b_i = x_i \cdot y_i$, for all $i \in \{1, \ldots, n\}$.*

The value of the game, $\omega^*(\mathrm{CHSH}^{\otimes n})$, is the maximum probability which Alice and Bob can win.

Theorem 4. *The following four statements are equivalent for every $n \in \mathbb{N}$:*

1. *There is an encoding of $x_0, x_1 \in \{0,1\}^n$ that hides the XOR and $\frac{1}{2^n}\sum_{c\in\{0,1\}^n} \Pr[\text{learn } x_c] = p$, where $x_c \in \{0,1\}^n$ is defined as $(x_c)_i := (x_{c_i})_i$.*
2. *There is a secure, non-interactive $\mathrm{OT}_p^{\otimes n}$ protocol.*
3. *There is a secure $\mathrm{OT}_p^{\otimes n}$ protocol.*
4. *There is a strategy for winning the game $\mathrm{CHSH}^{\otimes n}$ with probability p.*

APPLICATIONS OF EQUIVALENCES

Our equivalences provide new ways of looking at nonlocal games and cryptographic primitives, through the lens of quantum encodings. Apart from conceptual tools, we can use the equivalences to prove a number of results in all areas.

First, using Theorem 1 for encodings that hide the XOR with $n = 1$ and Theorem 4, we have an alternative proof of the optimality of Tsirelson's bound, $\omega^*(\mathrm{CHSH}) \leq \cos^2(\pi/8)$.

Using Theorem 1 for encodings that hide the XOR and Theorem 3, we provide a new upper bound on the value of CHSH_n, $\omega^*(\mathrm{CHSH}_n) \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}$. It is an interesting open question to compute the exact quantum value of this game, especially since it is a simple generalization of the CHSH game for which the quantum value is not known to be implied by information causality.

There is an alternative way of upper bounding the value of this game numerically using semidefinite programming (SDP) [27]. We provide below the values for small n. We see that the SDP relaxation gives a tighter bound than ours for $n \leq 3$, but the numerical results suggest that our bound outperforms the SDP bound for larger values of n.

Value	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$
Lower Bound	0.750	0.625	0.562	0.531	0.515
Conjectured Value	0.853	0.750	0.676	0.625	0.588
SDP Relaxation	0.853	0.780	0.743	0.725	0.716
Our Bound	1	0.853	0.750	0.676	0.625

The table above also includes our conjectured optimal value, below.

Conjecture 1. $\forall n \in \mathbb{N}$, $\omega^*(\mathrm{CHSH}_n) = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2^n}}$.

Similarly, for secure OT_p^n, we have $p \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}$ (again, for $n = 1$, we can get the optimal $p \leq \cos^2(\pi/8)$).

Second, by Theorem 4 and the perfect parallel repetition property of CHSH [28], i.e., the fact that if Alice and Bob play n games in parallel, the probability of winning all games is exactly $(\cos^2(\pi/8))^n$, we have for any secure $\mathrm{OT}_p^{\otimes n}$ protocol, $p \leq (\cos^2(\pi/8))^n$, which is attainable by using n secure $\mathrm{OT}_{\cos^2(\pi/8)}$ protocols. In other words, secure oblivious transfer admits perfect parallel repetition.

ROBUSTNESS OF EQUIVALENCES

Similar results can also be obtained in the case of a *weighted average decoding probability* defined as $q\Pr[\text{learning } x_0] + (1-q)\Pr[\text{learning } x_1]$, for $q \in [0,1]$. When the XOR is hidden, and $q = 1/2$, Theorem 1 shows that the above quantity is at most $\cos^2(\pi/8)$. A similar analysis shows that for any q, this value is at most

$$\frac{1}{2} + \frac{1}{2}\sqrt{q^2 + (1-q)^2}. \tag{3}$$

It is also interesting to see that such a learning relation is related to the CHSH game where Bob gets input $y = 0$ with probability q and input $y = 1$ with probability $1 - q$ while Alice still gets a uniform input. Using a similar method than in Theorem 3, we can show that this game has value at most $\frac{1}{2} + \frac{1}{2}\sqrt{q^2 + (1-q)^2}$. We can show the optimality of this bound using the semidefinite programming characterization of the bias of XOR games in [28].

DISCUSSION

We have provided new relations between the average decoding probability of two bits (or strings) and the probability of decoding their XOR. Moreover, we have shown precise equivalences between quantum encodings, CHSH-type games, and oblivious transfer, showing that non-locality and cryptographic primitives are often two facets of the same quantum mechanical behaviour. Last, we used our equivalences to prove new results for non-local games and oblivious transfer protocols.

As we have mentioned, it is an open question to compute the quantum value of the game CHSH_n through semidefinite programming or by proving stronger learning relations. Moreover, we would like to find an information postulate that implies that any theory that abides to it must win this game with exactly the quantum value (similar to information causality for the case of CHSH).

[1] R. Raz, in *Proc. 31st Annual ACM Symposium on Theory of Computing* (ACM, 1999), pp. 358–367.
[2] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[3] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, SIAM J. Comput. **38**, 1695 (2008).
[4] A. Holevo, Problemy Peredachi Informatsii **9**, 3 (1973).
[5] J. Bell, Physics **1**, 195 (1964).
[6] C. Bennett and G. Brassard, in *IEEE Inter. Conf. on Computer Systems and Signal Processing* (1984).
[7] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).
[8] M. Ballester, S. Wehner, and A. Winter, IEEE Trans. on Information Theory **54**, 4183 (2008).
[9] D. Gopal and S. Wehner, Phys. Rev. A **82**, 022326 (2010).
[10] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, SIAM J. Comput. **37**, 1865 (2008), ISSN 0097-5397.
[11] S. Wehner, C. Schaffner, and B. Terhal, Phys. Rev. Lett. **100**, 220502 (2008).
[12] C. Schaffner, Phys. Rev. A **82**, 032308 (2010).
[13] M. Pawlowski and A. Winter, Phys. Rev. A **85**, 022331 (2012).
[14] J. Clauser, M. Horne, A. Shimony, and R. Holt, Physical Review Letters **23**, 880 (1969).
[15] B. Tsirelson, Journal of Soviet Mathematics **36**, 557 (1987).
[16] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski, Nature **461**, 1101 (2009).
[17] A. Kitaev, *Presentation at the 6th workshop on quantum information processing (QIP 2003)* (2002).
[18] A. Chailloux and I. Kerenidis, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (2009), vol. 0, pp. 527–533, ISSN 0272-5428.
[19] A. Chailloux and I. Kerenidis, in *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science* (2011), vol. 0, pp. 354–362, ISSN 0272-5428.
[20] S. Wiesner, SIGACT News **15**, 78 (1983).
[21] M. Rabin, in *Technical Report TR-81, Aiken Computation Laboratory, Harvard University* (1981).
[22] J. Kilian, in *STOC '88: Proceedings of the 20th ACM symposium on Theory of computing* (1988), pp. 20–31.
[23] A. Chailloux, I. Kerenidis, and J. Sikora, Quantum Information and Computation **13**, 158 (2013).
[24] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Advances in Cryptology - CRYPTO 2006* (2006), pp. 427–444.
[25] C. Bennett, G. Brassard, S. Breidbard, and S. Wiesner, in *Advances in Cryptology CRYPTO 1982* (1983), pp. 267–275.
[26] J. Oppenheim and S. Wehner, Science **330:6007**, 1072 (2010).
[27] J. Kempe, O. Regev, and B. Toner, SIAM Journal on Computing **39**, 3207 (2010).
[28] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay, Computational Complexity **17**, 282 (2008).
[29] H.-K. Lo, Phys. Rev. A **56**, 1154 (1997).
[30] N. Gisin, S. Popescu, V. Scarani, S. Wolf, and J. Wullschleger, in *IEEE Information Theory Workshop (ITW)* (2006), pp. 24–26.
[31] M. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, 2000).
[32] We use a non-composable definition of security which makes our impossibility results even stronger.
[33] For our purposes, we can assume Alice discards her quantum state except for the registers containing z_0 and z_1.

Appendix

Proof of Equation (1) and Theorem 1

Recall Equation (1) reproduced below,

$$\cos^2(\alpha-\beta) \geq \|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \geq \cos^2(\alpha+\beta).$$

We first prove the lower bound. Define the following states:

$$|X\rangle := \frac{C|\psi\rangle}{\|C|\psi\rangle\|_2}, \quad |X'\rangle := \frac{(I-C)|\psi\rangle}{\|(I-C)|\psi\rangle\|_2},$$

$$|Y\rangle := \frac{D|\psi\rangle}{\|D|\psi\rangle\|_2}, \quad |Y'\rangle := \frac{(I-D)|\psi\rangle}{\|(I-D)|\psi\rangle\|_2}.$$

We can write $|\psi\rangle$ as
$|\psi\rangle = \cos(\alpha)|X\rangle + \sin(\alpha)|X'\rangle = \cos(\beta)|Y\rangle + \sin(\beta)|Y'\rangle$.
Since $|X\rangle$ is an eigenvector of C, we can write $C = |X\rangle\langle X| + \Pi_C$ and similarly we can write $I - C = |X'\rangle\langle X'| + \Pi_{C'}$, such that

$$\begin{aligned}\langle \Pi_C, |X\rangle\langle X| \rangle &= \langle \Pi_{C'}, |X\rangle\langle X| \rangle \\ &= \langle \Pi_C, |X'\rangle\langle X'| \rangle \\ &= \langle \Pi_{C'}, |X'\rangle\langle X'| \rangle \\ &= 0.\end{aligned}$$

We now write $|Y\rangle = \gamma_0|X\rangle + \gamma_1|X'\rangle + \gamma_2|Z\rangle$, where $\||Z\rangle\|_2 = 1$, $\langle X|Z\rangle = \langle X'|Z\rangle = 0$, and $|\gamma_0| = \sqrt{x_0}$, $|\gamma_1| = \sqrt{x_1}$, and $|\gamma_2| = \sqrt{x_2}$ for some $x_0, x_1, x_2 \in [0,1]$. Using this expression for $|Y\rangle$, we have

$$\begin{aligned}\|CD|\psi\rangle\|_2^2 &= \cos^2(\beta)\,\|C|Y\rangle\|_2^2 \\ &= \cos^2(\beta)\left(x_0 + x_2\,\|\Pi_C|Z\rangle\|_2^2\right).\end{aligned}$$

Since $|\psi\rangle = \cos(\alpha)|X\rangle + \sin(\alpha)|X'\rangle = \cos(\beta)|Y\rangle + \sin(\beta)|Y'\rangle$, we can write $|Y'\rangle = \gamma_0'|X\rangle + \gamma_1'|X'\rangle + \gamma_2'|Z\rangle$, with $|\gamma_0'| = \sqrt{x_0'}$, $|\gamma_1'| = \sqrt{x_1'}$, and $|\gamma_2'| = \sqrt{x_2'}$ for some $x_0', x_1', x_2' \in [0,1]$. Using this expression for $|Y'\rangle$, we have

$$\begin{aligned}\|(1-C)(1-D)|\psi\rangle\|_2^2 &= \sin^2(\beta)\,\|(1-C)|Y'\rangle\|_2^2 \\ &= \sin^2(\beta)\left(x_1' + x_2'\,\|\Pi_{C'}|Z\rangle\|^2\right).\end{aligned}$$

Notice that

$$1 = \|C|Z\rangle\|_2^2 + \|(I-C)|Z\rangle\|_2^2 = \|\Pi_C|Z\rangle\|_2^2 + \|\Pi_{C'}|Z\rangle\|_2^2.$$

We define $A := \|\Pi_C|Z\rangle\|_2^2 = 1 - \|\Pi_{C'}|Z\rangle\|_2^2$. This yields

$$\begin{aligned}&\|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \\ =\;& \cos^2(\beta)\left(x_0 + x_2\,\|\Pi_C|Z\rangle\|_2^2\right) \\ &+ \sin^2(\beta)\left(x_1' + x_2'\,\|\Pi_{C'}|Z\rangle\|_2^2\right) \\ =\;& \cos^2(\beta)\,(x_0 + x_2 A) + \sin^2(\beta)\,(x_1' + x_2'(1-A)) \\ =\;& \cos^2(\beta)x_0 + \sin^2(\beta)\,(x_1' + x_2') \\ &+ A\left(\cos^2(\beta)x_2 - \sin^2(\beta)x_2'\right) \\ =\;& \cos^2(\beta)x_0 + \sin^2(\beta)\,(1 - x_0') \\ &+ A\left(\cos^2(\beta)x_2 - \sin^2(\beta)x_2'\right). \qquad (4)\end{aligned}$$

Define $A(\rho,\sigma) := \arccos F(\rho,\sigma)$ to be the angle between two states ρ and σ, which is a metric (see p. 413 in [31]). Since $\langle Y|Y'\rangle = 0$, we have

$$A(|Y'\rangle, |X\rangle) \geq \pi/2 - A(|X\rangle, |Y\rangle).$$

This implies that

$$\begin{aligned}\sqrt{x_0'} &= \cos\left(\arccos|\langle Y'|X\rangle|\right) \\ &\leq \cos\left(\pi/2 - \arccos\sqrt{x_0}\right) \\ &= \sin\left(\arccos\sqrt{x_0}\right) \\ &= \sqrt{1-x_0}.\end{aligned}$$

This yields $x_0' \leq 1 - x_0$. In addition, notice that $\langle\psi|Z\rangle = 0$, which implies that

$$\begin{aligned}&\langle Z|\left(\cos(\beta)|Y\rangle + \sin(\beta)|Y'\rangle\right) = 0 \\ \iff\;& \cos^2(\beta)|\langle Z|Y\rangle|^2 = \sin^2(\beta)|\langle Z|Y'\rangle|^2 \\ \iff\;& \cos^2(\beta)x_2 = \sin^2(\beta)x_2'.\end{aligned}$$

This gives us the bound,

$$\|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \geq x_0. \qquad (5)$$

To conclude, we have

$$\begin{aligned}\arccos(\sqrt{x_0}) &= A(|X\rangle, |Y\rangle) \\ &\leq A(|X\rangle, |\psi\rangle) + A(|\psi\rangle, |Y\rangle) \\ &\leq \alpha + \beta,\end{aligned}$$

yielding $x_0 \geq \cos^2(\alpha+\beta)$ which concludes the proof of the lower bound.

For the upper bound, we have $x_0' \leq 1 - x_0$ and $\cos^2(\beta)x_2 = \sin^2(\beta)x_2'$, hence,

$$\|CD|\psi\rangle\|_2^2 + \|(1-C)(1-D)|\psi\rangle\|_2^2 \leq 1 - x_0',$$

from (4). We now show $1 - x_0' \leq \cos^2(\beta - \alpha)$. Since $\sqrt{x_0'} = |\langle Y'|X\rangle|$, we have

$$\begin{aligned}\arccos\left(\sqrt{x_0'}\right) &= A(|Y'\rangle, |X\rangle) \\ &\leq A(|X\rangle, |\psi\rangle) + A(|Y'\rangle, |\psi\rangle) \\ &= \pi/2 - (\beta - \alpha).\end{aligned}$$

so $\sqrt{x_0'} \geq \cos(\pi/2 - (\beta-\alpha)) = \sin(\beta-\alpha)$ implying $1 - x_0' \leq \cos^2(\beta-\alpha)$, as desired. □

Proof of Theorem 1. The proof of the first statement in the theorem relies on the following decoding strategy: First, we apply the decoding procedure for learning the first bit and then we apply the second decoding procedure on the post-measurement state. The probability of decoding the XOR is the probability that both decoding procedures succeed (give correct guesses for each bit) or they both fail (give incorrect guesses for each bit).

We prove the theorem using the following (equivalent) setting. We suppose two parties, Alice and Bob, share a joint pure state $|\Omega\rangle_{\mathcal{AB}}$ such that Alice performs a projective measurement $M = \{M_{x_0,x_1}\}_{x_0,x_1\in\{0,1\}}$ on $\mathcal{A}$ to determine x_0 and x_1 and the post-measured state is Bob's encoding of x_0 and x_1. Let p_i be the maximum probability that Bob can learn bit x_i, for $i \in \{0,1\}$. We note that without loss of generality, Bob can perform a projective measurement to guess the value of x_i with maximum probability [31]. Let $P = \{P_0, P_1\}$ be Bob's projective measurement that allows him to guess x_0 with probability $p_0 = \cos^2(\alpha) \geq \frac{1}{2}$ and $Q = \{Q_0, Q_1\}$ be Bob's projective measurement that allows him to guess x_1 with probability $p_1 = \cos^2(\beta) \geq \frac{1}{2}$ (these measurements are on $\mathcal{B}$ only). Consider the following projections (on $\mathcal{A}\otimes\mathcal{B}$):

$$C = \sum_{x_0,x_1} M_{x_0,x_1}\otimes P_{x_0} \quad \text{and} \quad D = \sum_{x_0,x_1} M_{x_0,x_1}\otimes Q_{x_1}.$$

C (resp. D) is the projection on the subspace where Bob guesses correctly x_0 (resp. x_1) after applying P (resp. Q). Consider the strategy where Bob applies the two measurements P and Q one after the other to learn (x_0, x_1), from which he can calculate $x_0 \oplus x_1$. If both

guesses are correct or if both guesses are incorrect then his guess for $x_0 \oplus x_1$ is correct.

Let Bob perform the following projective measurement to learn both bits:

$$R = \{R_{x_0,x_1} := Q_{x_1} P_{x_0} Q_{x_1}\}_{x_0,x_1 \in \{0,1\}}.$$

The measurement where Bob guesses both bits correctly when applying R is

$$E = \sum_{x_0,x_1} M_{x_0,x_1} \otimes R_{x_0,x_1} = DCD,$$

with outcome probability $\langle\Omega|E|\Omega\rangle = \|CD|\Omega\rangle\|_2^2$. The measurement where Bob guesses both bits incorrectly when applying R is

$$F = \sum_{x_0,x_1} M_{x_0,x_1} \otimes R_{\bar{x_0},\bar{x_1}} = (I-D)(I-C)(I-D).$$

The probability of this measurement outcome is $\langle\Omega|F|\Omega\rangle = \|(I-C)(I-D)|\Omega\rangle\|_2^2$. With this strategy, Bob can guess $x_0 \oplus x_1$ with probability

$$||CD|\Omega\rangle||_2^2 + ||(I-C)(I-D)|\Omega\rangle||_2^2 \geq \cos^2(\alpha+\beta)$$

by (1). Note that

$$c := \frac{p_0+p_1}{2} = \frac{\cos^2(\alpha)+\cos^2(\beta)}{2} \geq \frac{1}{2}$$

and for such values of α, β, we have $\cos(\alpha+\beta) \geq \cos^2(\alpha) + \cos^2(\beta) - 1$. Therefore,

$$\Pr[\text{Bob can learn } x_0 \oplus x_1] \geq \cos^2(\alpha+\beta) \geq (2c-1)^2.$$

For the second statement, ideally, we would like to extend our proof approach from bits to strings, but unfortunately this statement is not true anymore if x_0 and x_1 are strings. Instead, the analysis in [23] can be generalized to strings to show

$$\Pr[\text{learning } (x_0,x_1)] \geq \left(\frac{\cos^2(\alpha)+\cos^2(\beta)}{2}\right)\cos^2(\alpha+\beta).$$

If $c \geq 1/2$, then by the same reasoning as above, we have $\Pr[\text{learning } (x_0,x_1)] \geq c(2c-1)^2$. The statement about the XOR follows directly from the above statement. □

Proofs of the security bounds for oblivious transfer protocols

We now provide proofs of the lower bounds of 59.9% and 58.52% for any oblivious transfer and oblivious string transfer protocol, respectively, with $p = 1$, by relating them to bit commitment. A quantum bit commitment protocol, denoted BC, is an interactive protocol with no inputs, between Alice and Bob, with two phases:

- Commit phase: Bob chooses a random b and interacts with Alice to commit to b.
- Reveal phase: Alice and Bob interact to reveal b to Alice.
- If the parties are honest, Alice accepts the value of b.

We say that the bit commitment protocol has cheating probabilities A_{BC} and B_{BC} where

- $B_{\text{BC}} := \max\left\{\sum_{b\in\{0,1\}} \frac{1}{2}\Pr[\text{Alice accepts outcome } b]\right\}$,
- $A_{\text{BC}} := \Pr[\text{Alice can learn } b \text{ after commit phase}]$.

We present a bit commitment protocol based on oblivious string transfer [23].

1. Commit phase: Alice and Bob perform the OT_1^n protocol such that Alice gets the output $(z_0,z_1) \in \{0,1\}^n \times \{0,1\}^n$ and Bob gets the output $(b,w) \in \{0,1\} \times \{0,1\}^n$. Here, b is the committed bit.
2. Reveal phase: If no one aborted, then Bob sends (b,w) to Alice.
3. If (b,w) from Bob is inconsistent with (z_0,z_1) then Alice aborts. Otherwise, she accepts b as the committed bit.

Let A_{OT^n} denote the probability Alice can learn b in the OT_1^n protocol without Bob aborting. Clearly we have $A_{\text{OT}^n} = A_{\text{BC}}$.

Let B_{OT^n} denote the probability Bob can learn $z_0 \oplus z_1$ in the OT_1^n protocol without Alice aborting. Notice that Bob must send (c, z_c) if he wants to reveal c in the BC protocol. Therefore, by letting q be the probability the OT_p^n is not aborted by Alice using Bob's optimal bit commitment strategy, we have $B_{\text{BC}} = qc$, where

$$c = \frac{1}{2}\sum_{b\in\{0,1\}} \Pr[\text{Bob learns } z_b | \text{Alice did not abort } \text{OT}_1^n].$$

From Theorem 1, we know that Bob has a strategy to learn (z_0,z_1) with probability,

$$B_{\text{OT}^n} \geq qc(2c-1)^2,$$

noting that $B_{\text{BC}} \geq 1/2 \implies c \geq 1/2$.

We now use the lower bound for bit commitment [19], which states that there is a parameter $t \in [0,1]$ such that

$$B_{\text{BC}} \geq \left(1 - \left(1 - \frac{1}{\sqrt{2}}\right)t\right)^2 \quad \text{and} \quad A_{\text{BC}} \geq \frac{1}{2} + \frac{t}{2}.$$

The above bound yields the lower bound $\max\{A_{\text{OT}^n}, B_{\text{OT}^n}\} \geq 0.5852$, which is independent of n. If $n = 1$, we can use the stronger bound in Theorem 1 to get

$$B_{\text{OT}} \geq q(2c-1)^2,$$

improving the lower bound to the desired value $\max\{A_{\text{OT}}, B_{\text{OT}}\} \geq 0.599$. □