Cryptography in a quantum world
Wehner, S.D.C.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Chapter 9

Interactive Proof Systems

As we saw in the past chapters, two spatially separated parties, Alice and Bob, can use entanglement to obtain correlations that are impossible to achieve classically, without any additional communication. However, there do exist classical systems whose strength, or security, indeed depends crucially on the fact that specific parties cannot communicate during the course of the protocol. How are such systems affected by the presence of entanglement? Can Alice and Bob use their shared entanglement to gain a significant advantage? Here, we study interactive proof systems which are a specific case of such a classical system. Surprisingly, it turns out that the space-like separation is lost altogether and we can simulate two classical parties with just a single quantum one.

9.1 Introduction

9.1.1 Classical interactive proof systems

Before getting to the heart of the matter, we first need to take a closer look at interactive proof systems. Classical interactive proof systems have received considerable attention [BFL91, BOGKW88, CCL90, Fei91, LS91, FL92] since their introduction by Babai [Bab85] and Goldwasser, Micali and Rackoff [GMR89] in 1985. An interactive proof system takes the form of a protocol of one or more rounds between two parties, a verifier and a prover. Whereas the prover is computationally unbounded, the verifier is limited to probabilistic polynomial time. Both the prover and the verifier have access to a common input string $x$. The goal of the prover is to convince the verifier that $x$ belongs to a pre-specified language $L$. The verifier’s aim, on the other hand, is to determine whether the prover’s claim is indeed valid. In each round, the verifier sends a polynomial (in $x$) size query to the prover, who returns a polynomial size answer. At the end of the protocol, the verifier decides to accept, and conclude $x \in L$, or reject based on the messages exchanged and his own private randomness. A language
has an interactive proof if there exists a verifier \( V \) and a prover \( P \) such that: If \( x \in L \), the prover can always convince \( V \) to accept. If \( x \notin L \), no strategy of the prover can convince \( V \) to accept with non-negligible probability. IP denotes the class of languages having an interactive proof system. Watrous [Wat99] first considered the notion of quantum interactive proof systems. Here, the prover has unbounded quantum computational power whereas the verifier is restricted to quantum polynomial time. In addition, the two parties can now exchange quantum messages. QIP is the class of languages having a quantum interactive proof system. Classically, it is known that \( IP = PSPACE \) [Sha92, She92], where PSPACE is the class of languages decidable using only polynomial space. For the quantum case, it has been shown that \( PSPACE \subseteq QIP \subseteq EXP \) [Wat99, KW00]. If, in addition, the verifier is given polynomial size quantum advice, the resulting class \( QIP^{qpoly} \) contains all languages [Raz05]. Let \( QIP(k) \) denote the class where the prover and verifier are restricted to exchanging \( k \) messages. It is known that \( QIP = QIP(3) \) [KW00] and \( QIP(1) \subseteq PP \) [Vya03, MW05], where PP is the class of all problems solvable by a probabilistic machine in polynomial time. We refer to [MW05] for an overview of the extensive work done on QIP(1), also known as QMA. Very little is known about \( QIP(2) \) and its relation to either PP or PSPACE.

In multiple-prover interactive proof systems the verifier can interact with multiple, computationally unbounded provers. Before the protocol starts, the provers are allowed to agree on a joint strategy, however they can no longer communicate during the execution of the protocol. Let MIP denote the class of languages having a multiple-prover interactive proof system. Here, we are especially interested in two-prover interactive proof systems as introduced by Ben-Or, Goldwasser, Kilian and Widgerson [BOGKW88]. Babai, Fortnow and Lund [BFL91], and Feige and Lovász [FL92] have shown that a language is in NEXP if and only if it has a two-prover one-round proof system, i.e., \( \text{MIP}[2] = \text{NEXP} \). Feige and Lovász have also shown that a system using more than two provers is thus no more powerful than a system with only two provers, i.e., \( \text{MIP}[2] \subseteq \text{MIP} \). Let \( \oplus \text{MIP}[2] \) denote the restricted class where the verifier’s output is a function of the XOR of two binary answers. Even for such a system \( \oplus \text{MIP}[2] = \text{NEXP} \), for certain soundness and completeness parameters [CHTW04a]. Classical multiple-prover interactive proof systems are thus more powerful than classical proof systems based on a single prover, assuming \( PSPACE \neq \text{NEXP} \).

### 9.1.2 Quantum multi-prover interactive proof systems

Given the advent of quantum computing, one can also consider quantum interactive proof systems with multiple provers. These can be grouped into two categories: First, one can consider provers and a verifier that are quantum themselves and can exchange quantum messages. Kobayashi and Matsumoto have considered such quantum multiple-prover interactive proof systems which form
an extension of quantum single prover interactive proof systems as described above. Let QMIP denote the resulting class. In particular, they showed that QMIP = NEXP if the provers do not share quantum entanglement [KM03]. If the provers share at most polynomially many entangled qubits the resulting class is contained in NEXP [KM03].

Secondly, one can consider proof systems where all communication remains classical, but the provers can share any entangled state as part of their strategy on which they are allowed to perform arbitrary measurements. Cleve, Høyer, Toner and Watrous [CHTW04a] have raised the question whether a classical two-prover system is weakened in such a setting. We write MIP\(^{\ast}\) if the provers share entanglement. The authors provide a number of examples which demonstrate that the soundness condition of a classical proof system can be compromised, i.e. the interactive proof system is weakened, when entanglement is used. In their paper, it is proved that \(\oplus\text{MIP}[2] \subseteq \text{NEXP}\). Later, the same authors also showed that \(\oplus\text{MIP}[2] \subseteq \text{EXP}\) using semidefinite programming [CHTW04b]. Entanglement thus clearly weakens an interactive proof system, assuming EXP \(\neq\) NEXP.

Intuitively, entanglement allows the provers to coordinate their answers, even though they cannot use it to communicate. By measuring the shared entangled state the provers can generate correlations which they can use to deceive the verifier. Tsirelson [Tsi80, Tsi87] has shown that even quantum mechanics limits the strength of such correlations, as we saw in Chapter 6. Recall that Popescu and Rohrlich [PR94, PR96, PR97] have raised the question why nature imposes such limits. To this end, they constructed a toy-theory based on non-local boxes [PR94, vD00], which are hypothetical “machines” generating correlations stronger than possible in nature. In their full generalization, non-local boxes can give rise to any type of correlation as long as they cannot be used to signal. Preda [Pre05] showed that sharing non-local boxes allows two provers to coordinate their answers perfectly and obtained \(\oplus\text{MIP}_{\text{NL}} = \text{PSPACE}\), where we write \(\oplus\text{MIP}_{\text{NL}}\) to indicate that the two provers share non-local boxes.

Kitaev and Watrous [KW00] mention that it is unlikely that a single-prover quantum interactive proof system can simulate multiple classical provers, because then from QIP \(\subseteq\) EXP and MIP = NEXP it follows that EXP = NEXP.

Surprisingly, it turns out that when the provers are allowed to share entanglement it can be possible to simulate two such classical provers by one quantum prover. This indicates that entanglement among provers truly leads to a weaker proof system. In particular, we show that a two-prover one-round interactive proof system where the verifier computes the XOR of two binary answers and the provers are allowed to share an arbitrary entangled state, can be simulated by a single quantum interactive proof system with two messages: \(\oplus\text{MIP}[2] \subseteq \text{QIP}(2)\). Since very little is known about QIP(2) so far [KW00], we hope that our result may help shed some light on its relation to PP or PSPACE. Our result also leads to a proof that \(\oplus\text{MIP}[2] \subseteq \text{EXP}\).
9.2 Proof systems and non-local games

9.2.1 Non-local games

For our proof, it is necessary to link interactive proof systems to non-local games, as we described in Chapter 6.2.3. Since we consider only two parties, we omit unnecessary indices and use separate letters to refer to the sets of possible questions and answers. We briefly recap our setup, summarized in Figure 9.1: Let $S$, $T$, $A$ and $B$ be finite sets, and $\pi$ a probability distribution on $S \times T$. Let $V$ be a predicate on $S \times T \times A \times B$. Then $G = G(V, \pi)$ is the following two-person cooperative game\footnote{Players 1 and 2 collaborate against the verifier}:

A pair of questions $(s, t) \in S \times T$ is chosen at random according to the probability distribution $\pi$. Then $s$ is sent to player 1, henceforth called Alice, and $t$ to player 2, which we call Bob. Upon receiving $s$, Alice has to reply with an answer $a \in A$. Likewise, Bob has to reply to question $t$ with an answer $b \in B$. They win if $V(s, t, a, b) = 1$ and lose otherwise. Alice and Bob may agree on any kind of strategy beforehand, but they are no longer allowed to communicate once they have received questions $s$ and $t$. The value $\omega(G)$ of a game $G$ is the maximum probability that Alice and Bob win the game. We write $V(a, b|s, t)$ instead of $V(s, t, a, b)$ to emphasize the fact that $a$ and $b$ are answers given questions $s$ and $t$.

Here, we are particularly interested in non-local games. Alice and Bob are allowed to share an arbitrary entangled state $|\Psi\rangle$ to help them win the game. Let $\mathcal{H}^A$ and $\mathcal{H}^B$ denote the Hilbert spaces of Alice and Bob respectively. The state $|\Psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$ is part of the quantum strategy that Alice and Bob can agree on beforehand. This means that for each game, Alice and Bob can choose a specific $|\Psi\rangle$ to maximize their chance of success. In addition, Alice and Bob can agree on quantum measurements. For each $s \in S$, Alice has a projective measurement described by $\{X^a_s | a \in A\}$ on $\mathcal{H}^A$. For each $t \in T$, Bob has a projective measurement described by $\{Y^b_t | b \in B\}$ on $\mathcal{H}^B$. For questions $(s, t) \in S \times T$, Alice performs the measurement corresponding to $s$ on her part of $|\Psi\rangle$ which gives her outcome $a$. Likewise, Bob performs the measurement corresponding to $t$ on his part of $|\Psi\rangle$ with outcome $b$. Both send their outcome, $a$ and $b$, back to the verifier. The probability that Alice and Bob answer $(a, b) \in A \times B$ is then given by

$$\langle \Psi | X^a_s \otimes Y^b_t | \Psi \rangle.$$ 

The probability that Alice and Bob win the game is now given by

$$\Pr[\text{Alice and Bob win}] = \sum_{s, t} \pi(s, t) \sum_{a, b} V(a, b|s, t) \langle \Psi | X^a_s \otimes Y^b_t | \Psi \rangle.$$ (9.1)

The quantum value $\omega_q(G)$ of a game $G$ is the maximum probability over all possible quantum strategies that Alice and Bob win. Recall that XOR game is
a game where the value of $V$ only depends on $c = a \oplus b$ and not on $a$ and $b$ independently. For XOR games we write $V(c|s,t)$ instead of $V(a,b|s,t)$. Here, we are only interested in the case that $a \in \{0, 1\}$ and $b \in \{0, 1\}$ and XOR games. Alice and Bob’s measurements are then described by $\{X^0_s, X^1_s\}$ for $s \in S$ and $\{Y^0_t, Y^1_t\}$ for $t \in T$ respectively. Note that $X^0_s + X^1_s = I$ and $Y^0_t + Y^1_t = I$ and thus these measurements can be expressed in the form of observables $X_s$ and $Y_t$ with eigenvalues $\pm 1$: $X_s = X^0_s - X^1_s$ and $Y_t = Y^0_t - Y^1_t$. Recall from Chapter 6.3.2 that Tsirelson [Tsi80, Tsi87] has shown that for any $|\Psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$ there exists real unit vectors $x_s, y_t \in \mathbb{R}^N$ with $N = |S| + |T|$ such that $\langle \Psi | X_s \otimes Y_t | \Psi \rangle = \langle x_s | y_t \rangle$. It is then easy to see from Eq. (9.1) that for XOR games we can express the maximum winning probability as

$$\omega_q(G) = \max_{x_s, y_t} \frac{1}{2} \sum_{s,t} \pi(s,t) \sum_c V(c|s,t) (1 + (-1)^c \langle x_s | y_t \rangle),$$  

where the maximization is taken over all unit vectors $x_s, y_t \in \mathbb{R}^N$.

### 9.2.2 Multiple classical provers

It is well known [CHTW04a, FL92], that two-prover one-round interactive proof systems with classical communication can be modeled as (non-local) games. Here,
Alice and Bob take the role of the two provers. The verifier now poses questions \( s \) and \( t \), and evaluates the resulting answers. A proof system associates with each string \( x \) a game \( G_x \), where \( \omega(G_x) \) determines the probability that the verifier accepts (and thus concludes \( x \in L \)). The string \( x \), and thus the nature of the game \( G_x \) is known to both the verifier and the provers. Ideally, for all \( x \in L \) the value of \( \omega(G_x) \) is close to one, and for \( x \notin L \) the value of \( \omega(G_x) \) is close to zero.

It is possible to extend the game model for MIP\([2]\) to use a randomized predicate for the acceptance predicate \( V \). This corresponds to \( V \) taking an extra input string chosen at random by the verifier. However, known applications of MIP\([2]\) proof systems do not require this extension [Fei95]. Our argument in Section 9.3 can easily be extended to deal with randomized predicates. Since \( V \) is not a randomized predicate in [CHTW04a], we follow this approach.

We concentrate on proof systems involving two provers, one round of communication, and single-bit answers. The provers are computationally unbounded, but limited by the laws of quantum physics. However, the verifier is probabilistic polynomial time bounded. As defined by Cleve, Høyer, Toner and Watrous [CHTW04a],

9.2.1. Definition. For \( 0 \leq s < c \leq 1 \), let \( \oplus \text{MIP}_{c,s}[2] \) denote the class of all languages \( L \) recognized by a classical two-prover interactive proof system of the following form:

- They operate in one round, each prover sends a single bit in response to the verifier’s question, and the verifier’s decision is a function of the parity of those two bits.
- If \( x \in L \) then there exists a strategy for the provers for which the probability that the verifier accepts is at least \( c \) (the completeness probability).
- If \( x \notin L \) then, whatever strategy the two provers follow, the probability that the verifier accepts is at most \( s \) (the soundness probability).

9.2.2. Definition. For \( 0 \leq s < c \leq 1 \), let \( \oplus \text{MIP}^*_{c,s}[2] \) denote the class corresponding to a modified version of the previous definition: all communication remains classical, but the provers may share prior quantum entanglement, which may depend on \( x \), and perform quantum measurements.

We generally omit indices \( c, s \), unless they are explicitly relevant.

In Chapter 7, we discussed how to find the optimal strategies for XOR-games. In particular, we saw that we can determine the optimal value of \( \omega_q(G_x) \) in time exponential in \( \min(|S|, |T|) \) using semidefinite programming. This implies immediately that \( \oplus \text{MIP}^* \subseteq \text{EXP} \), as was shown by Cleve, Hoyer, Toner and Watrous [CHTW04a] during their presentation at CCC’04. Here, we show something stronger, namely that \( \oplus \text{MIP}^* \subseteq \text{QIP}(2) \).
9.3. Simulating two classical provers with one quantum prover

9.2.3 A single quantum prover

Instead of two classical provers, we can also consider a system consisting of a single quantum prover $P_q$ and a quantum polynomial time verifier $V_q$ as defined by Watrous [Wat99]. Again, the quantum prover $P_q$ is computationally unbounded, however, he is limited by the laws of quantum physics. The verifier and the prover can communicate over a quantum channel. In this thesis, we are only interested in one round quantum interactive proof systems: the verifier sends a single quantum message to the prover, who responds with a quantum answer. We here express the definition of QIP(2) [Wat99] in a form similar to the definition of $\oplus \text{MIP}^*$:

9.2.3. Definition. Let $\text{QIP}(2,c,s)$ denote the class of all languages $L$ recognized by a quantum one-prover one-round interactive proof system of the following form:

- If $x \in L$ then there exists a strategy for the quantum prover for which the probability that the verifier accepts is at least $c$.
- If $x \notin L$ then, whatever strategy the quantum prover follows, the probability that the quantum verifier accepts is at most $s$.

9.3 Simulating two classical provers with one quantum prover

We now show that an interactive proof system where the verifier bases his decision only on the XOR of two binary answers is in fact no more powerful than a system based on a single quantum prover. The main idea behind our proof is to combine two classical queries into one quantum query, and thereby simulate the classical proof system with a single quantum prover. Similar techniques have been used to prove results about classical locally decodable codes [KW03, WdW05]. Recall that the two provers can use an arbitrary entangled state as part of their strategy.

For our proof we make use of the fact that we can write the optimal value of the game as in Eq. (9.2).

9.3.1. Theorem. For all $s$ and $c$ such that $0 \leq s < c \leq 1$, $\oplus \text{MIP}^*_{c,s}[2] \subseteq \text{QIP}(2,c,s)$.

Proof. Let $L \in \oplus \text{MIP}^*_{c,s}[2]$ and let $V_e$ be a verifier witnessing this fact. Let $P_e^1$ (Alice) and $P_e^2$ (Bob) denote the two provers sharing entanglement. Fix an input string $x$. As mentioned above, interactive proof systems can be modeled as games indexed by the string $x$. It is therefore sufficient to show that there exists a verifier $V_q$ and a quantum prover $P_q$, such that $\omega_{\text{sim}}(G_x) = \omega_q(G_x)$, where $\omega_{\text{sim}}(G_x)$ is the value of the simulated game.
Let $s,t$ be the questions that $V_e$ sends to the two provers $P_1$ and $P_2$ in the original game. The new verifier $V_q$ now constructs the following state in $V \otimes M$

$$|\Phi_{init}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_v |0\rangle_M + |1\rangle_v |1\rangle_M),$$

and sends register $M$ to the single quantum prover $P_q$.

We first consider the honest strategy of the prover. Let $a$ and $b$ denote the answers of the two classical provers to questions $s$ and $t$ respectively. The quantum prover now transforms the state to

$$|\Phi_{honest}\rangle = \frac{1}{\sqrt{2}} ((-1)^a |0\rangle_v |s\rangle_M + (-1)^b |1\rangle_v |t\rangle_M),$$

and returns register $M$ back to the verifier. The verifier $V_q$ now performs a measurement on $V \otimes M$ described by the following projectors

$$P_0 = |\Psi^+_{st}\rangle \langle \Psi^+_{st}| \otimes I$$
$$P_1 = |\Psi^-_{st}\rangle \langle \Psi^-_{st}| \otimes I$$
$$P_{reject} = I - P_0 - P_1,$$

where $|\Psi^\pm_{st}\rangle = (|0\rangle_v |s\rangle_M \pm |1\rangle_v |t\rangle_M)/\sqrt{2}$. If he obtains outcome “reject”, he immediately aborts and concludes that the quantum prover is cheating. If he obtains outcome $m \in \{0,1\}$, the verifier concludes that $c = a \oplus b = m$. Note that $Pr[m = a \oplus b | s,t] = \langle \Phi_{honest}|P_{a \oplus b}|\Phi_{honest}\rangle = 1$, so the verifier can reconstruct the answer perfectly.

We now consider the case of a dishonest prover. In order to convince the verifier, the prover applies a transformation on $M \otimes P$ and send register $M$ back to the verifier. We show that for any such transformation the value of the resulting game is at most $\omega_q(G_e)$: Note that the state of the total system in $V \otimes M \otimes P$ can now be described as

$$|\Phi_{dish}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_v |\phi_s\rangle + |1\rangle_v |\phi_t\rangle)$$

where $|\phi_s\rangle = \sum_{u \in S'} |u\rangle_v |\alpha_u^s\rangle$ and $|\phi_t\rangle = \sum_{v \in S' \cup T'} |v\rangle_v |\beta_v^t\rangle$ with $S' = \{0s | s \in S\}$ and $T' = \{1t | t \in T\}$. Any transformation employed by the prover can be described this way. We now have that

$$Pr[m = 0 | s,t] = \langle \Phi_{dish}|P_0|\Phi_{dish}\rangle = \frac{1}{4} (\langle \alpha_s^* |\alpha_s^s\rangle + \langle \beta_t^i |\beta_t^i\rangle) + \frac{1}{2} \Re(\langle \alpha_s^* |\beta_t^i\rangle)$$

$$Pr[m = 1 | s,t] = \langle \Phi_{dish}|P_1|\Phi_{dish}\rangle = \frac{1}{4} (\langle \alpha_s^* |\alpha_s^s\rangle + \langle \beta_t^i |\beta_t^i\rangle) - \frac{1}{2} \Re(\langle \alpha_s^* |\beta_t^i\rangle)$$

The probability that the prover wins is given by

$$Pr[Prover\ wins] = \sum_{s,t} \pi(s,t) \sum_{c \in \{0,1\}} V(c | s,t) Pr[m = c | s,t].$$
9.3. Simulating two classical provers with one quantum prover

The prover will try to maximize his chance of success by maximizing $\Pr[m = 0|s, t]$ or $\Pr[m = 1|s, t]$. We can therefore restrict ourselves to considering real unit vectors for which $\langle \alpha_s^s | \alpha_s^s \rangle = 1$ and $\langle \beta_t^t | \beta_t^t \rangle = 1$, as the dimension of our vectors is directly determined by their number. Hence, we may also assume that $|\alpha_s^s\rangle = 0$ iff $s \neq s'$ and $|\beta_t^t\rangle = 0$ iff $t \neq t'$: any other strategy can lead to rejection and thus to a lower probability of success. By substituting into Eqs. (9.3) and (9.4), it follows that the probability that the quantum prover wins the game (when he avoids rejection) is

$$\frac{1}{2} \sum_{s, t, c} \pi(s, t) V(c|s, t)(1 + (-1)^c \langle \alpha_s^s | \beta_t^t \rangle).$$

(9.5)

In order to convince the verifier, the prover’s goal is to choose real vectors $|\alpha_s^s\rangle$ and $|\beta_t^t\rangle$ which maximize Eq. (9.5). Since in $|\phi_s\rangle$ and $|\phi_t\rangle$ we sum over $|S'| + |T'| = |S| + |T|$ elements respectively, the dimension of $P$ need not exceed $N = |S| + |T|$. Thus, it is sufficient to restrict the maximization to vectors in $\mathbb{R}^{|S| + |T|}$. Given Eq. (9.5), we thus have

$$\omega_{sim}(G_x) = \max_{\alpha_s^s, |\beta_t^t\rangle} \frac{1}{2} \sum_{s, t, c} \pi(s, t) V(c|s, t)(1 + (-1)^c \langle \alpha_s^s | \beta_t^t \rangle),$$

where the maximization is taken over vectors $\{\alpha_s^s \in \mathbb{R}^N : s \in S\}$, and $\{\beta_t^t \in \mathbb{R}^N : t \in T\}$. However, we know from Eq. (9.2) that

$$\omega_q(G_x) = \max_{x_s, y_t} \frac{1}{2} \sum_{s, t, c} \pi(s, t) V(c|s, t)(1 + (-1)^c \langle x_s|y_t \rangle)$$

where the maximization is taken over unit vectors $\{x_s \in \mathbb{R}^N : s \in S\}$ and $\{y_t \in \mathbb{R}^N : t \in T\}$. We thus have

$$\omega_{sim}(G_x) = \omega_q(G_x)$$

which completes our proof.

9.3.2. Corollary. For all $s$ and $c$ such that $0 \leq s < c \leq 1$, $\oplus\text{MIP}^*_c[2] \subseteq \text{EXP}$.

Proof. This follows directly from Theorem 9.3.1 and the result that $\text{QIP}(2) \subseteq \text{EXP}$ [KW00].
9.4 Conclusion

As we have shown, the strength of classical systems can be weakened considerably in the presence of entanglement. In our example above, we showed that the systems can be weakened so much that all space-like separation is lost: we saw that two classical parties with entanglement are as powerful as a single quantum party.

It would be interesting to show that this result also holds for a proof system where the verifier is not restricted to computing the XOR of both answers, but some other Boolean function. However, the approach based on vectors from Tsirelson’s results does not work for binary games. Whereas it is easy to construct a single quantum query which allows the verifier to compute an arbitrary function of the two binary answers with some advantage, it thus remains unclear how the value of the resulting game is related to the value of a binary game. Furthermore, mere classical tricks trying to obtain the value of a binary function from XOR itself seem to confer extra cheating power to the provers.

Examples of non-local games with longer answers [CHTW04a], such as the Kochen-Specker or the Magic Square game, seem to make it even easier for the provers to cheat by taking advantage of their entangled state. Furthermore, existing proofs that MIP = NEXP break down if the provers share entanglement. It is therefore an open question whether MIP* = NEXP or, MIP* ⊆ EXP.

As described, non-locality experiments between two space-like separated observers, Alice and Bob, can be cast in the form of non-local games. For example, the experiment based on the well known CHSH inequality [CHSH69], is a non-local game with binary answers of which the verifier computes the XOR [CHTW04a]. Our result implies that this non-local game can be simulated in superposition by a single prover/observer: Any strategy that Alice and Bob might employ in the non-local game can be mirrored by the single prover in the constructed “superposition game”, and also vice versa, due to Tsirelson’s constructions [Tsi80, Tsi87] mentioned earlier. This means that the “superposition game” corresponding to the non-local CHSH game is in fact limited by Tsirelson’s inequality [Tsi80], even though it itself has no non-local character. Whereas this may be purely coincidental, it would be interesting to know its physical interpretation, if any. Perhaps it may be interesting to ask whether Tsirelson-type inequalities have any consequences on local computations in general, beyond the scope of these very limited games.