Rigidity for Monogamy-Of-Entanglement Games

Anne Broadbent
Department of Mathematics and Statistics, University of Ottawa, Canada

Eric Culf
Department of Mathematics and Statistics, University of Ottawa, Canada

Abstract

In a monogamy-of-entanglement (MoE) game, two players who do not communicate try to simultaneously guess a referee’s measurement outcome on a shared quantum state they prepared. We study the prototypical example of a game where the referee measures in either the computational or Hadamard basis and informs the players of her choice.

We show that this game satisfies a rigidity property similar to what is known for some nonlocal games. That is, in order to win optimally, the players’ strategy must be of a specific form, namely a convex combination of four unentangled optimal strategies generated by the Breidbart state. We extend this to show that strategies that win near-optimally must also be near an optimal state of this form. We also show rigidity for multiple copies of the game played in parallel.

We give three applications: (1) We construct for the first time a weak string erasure (WSE) scheme where the security does not rely on limitations on the parties’ hardware. Instead, we add a prover, which enables security via the rigidity of this MoE game. (2) We show that the WSE scheme can be used to achieve bit commitment in a model where it is impossible classically. (3) We achieve everlasting-secure randomness expansion in the model of trusted but leaky measurement and untrusted preparation and measurements by two isolated devices, while relying only on the temporary assumption of pseudorandom functions. This achieves randomness expansion without the need for shared entanglement.

2012 ACM Subject Classification Theory of computation → Quantum computation theory; Theory of computation → Cryptographic primitives; Security and privacy → Mathematical foundations of cryptography

Keywords and phrases Rigidity, Self-Testing Monogamy-of-Entanglement Games, Bit Commitment, Randomness Expansion

Digital Object Identifier 10.4230/LIPIcs.ITCS.2023.28

Related Version Full Version: https://arxiv.org/abs/2111.08081

Funding Funded by the Air Force Office of Scientific Research under award number FA9550-20-1-0375, Canada’s NFRF and NSERC, an Ontario ERA, and the University of Ottawa’s Research Chairs program.

Acknowledgements We would like to thank Arthur Mehta for introducing us to sum-of-squares decompositions, and Sébastien Lord for many insightful discussions.

1 Introduction

Monogamy-of-entanglement (MoE) games provide an intuitive way to understand the strength of quantum multipartite correlations. Such games pit two cooperating players, usually named Bob and Charlie, against an honest referee, Alice. The players try, without communicating, to simultaneously guess the outcome of Alice’s measurement on a quantum state provided by the players and with which they may share entanglement freely. Interestingly, any one of the players can always correctly guess the result of any projective measurement Alice makes, by providing her with one register of a maximally entangled state, whereas two players are prohibited from simultaneously doing as well since tripartite correlations of the shared state are weaker.
The quintessential MoE game is the original example introduced by Tomamichel, Fehr, Kaniewski, and Wehner [35]. In this game, Alice’s space consists of a single qubit and she measures either in the computational or the Hadamard basis with equal probability to get a one-bit answer. As shown there, Bob and Charlie can win with probability at most $\cos^2 \frac{\pi}{8} \approx 0.85$. The TFKW game has a particularly simple optimal strategy: Bob and Charlie share no entanglement; they just send Alice a pure Breidbart state $|\beta\rangle \propto |0\rangle + |+\rangle$, and always guess 0 for the measurement outcome. Due to the symmetries of Alice’s measurement bases under the Pauli operators, there are 4 optimal entangled strategies: the Wiesner-Breidbart states $|\beta\rangle, X|\beta\rangle, Z|\beta\rangle, XZ|\beta\rangle$, illustrated in Figure 1. But the question remains: are these all the possible optimal strategies or are there optimal strategies where the players use entanglement? This question is tantamount to asking about the rigidity of the TFKW game.

The idea of rigidity, first formally introduced by Mayers and Yao [24], is that certain games can be used to “self-test” quantum states: if such a game is won with high enough probability, then the self-test property tells us that the players must hold some quantum state, up to local isometry. Up until now, the study of rigidity has been limited to nonlocal games. This area of study grew around the CHSH game, introduced by Clauser, Horne, Shimony, and Holt [8], was known, even before rigidity was formalised, to self-test a maximally-entangled state on two qubits [36]. This result was later extended to be robust [25] and to hold under parallel repetition [9]. Rigidity of nonlocal games has found many applications [17,31].

Our main contribution is to prove the first rigidity result for a monogamy-of-entanglement game:

▶ Main Theorem (informal). The state of any optimal strategy for the TFKW game is given as a convex combination of the entangled optimal states $|\beta\rangle, X|\beta\rangle, Z|\beta\rangle, XZ|\beta\rangle$. This is robust and extends to multiple rounds played in parallel.

Here, by convex combination, we mean a superposition of separable states where the components on Alice’s register are the Wiesner-Breidbart states and the components on Bob and Charlie’s register are simultaneously distinguishable by a measurement. A similar notion of rigidity holds for some nonlocal games [22]. This requirement on optimal strategies of the TFKW game forces Bob and Charlie to not use any of their shared entanglement while playing.

For applications, it is often necessary to extend the rigidity result to be robust and to the scenario where games are played in parallel, because playing the game once gives no information on the winning probability. What can be done to remedy this is to play many rounds at the same time to build up statistics about the win rate. This requires the result to be robust – a guarantee that the state is near-optimal if the winning probability is near-optimal. Also, the result needs to hold for games played in parallel, to ensure that there is no way entanglement helps in winning multiple games optimally.

Application: Weak string erasure and bit commitment

We construct for the first time a weak string erasure (WSE) scheme that is secure against adversaries with unrestricted quantum systems. WSE is a cryptographic primitive introduced by König, Wehner, and Wullschleger [19] that allows the sharing of partial information between mistrustful parties, a sender Alice and a receiver Bob. WSE implies both bit commitment and oblivious transfer. Since these are information-theoretically impossible in both the classical and quantum plain model [7,21,23], additional assumptions are necessary to be able to realise WSE. In [19], they use a noisy-storage model to limit the amount of storage a dishonest party can access.
In our model, we introduce a third party, a prover Charlie in full collusion with Bob but isolated from him. Under the assumption of a public broadcast from Alice to Bob and Charlie, we exploit the rigidity of the TFKW game to arrive at a secure scheme for WSE, which requires no entanglement and may be run in one round – it can be realised as a relativistic prepare-and-measure scheme.

Two-prover bit commitment was studied before in the classical context [3], where it was shown that separating the sender into two isolated parties can be used to ensure the binding property (see also [13]). In contrast, the WSE that we achieve implies, using [19], a bit commitment with two isolated receivers and a single sender. To the best of our knowledge, this is the first such scheme; furthermore, we show that, with classical communication only, our model reduces to the single-receiver model, so we have identified a new qualitative advantage for quantum communication in cryptography.

**Application: Everlasting randomness expansion**

Randomness is a precious resource for computation and cryptography. Pseudorandom generators are functions that produce large amounts of randomness from a small random seed, but the quality of this randomness is inherently based on a computational assumption, e.g. one-way functions. Thus, given sufficient computational power or time, an adversary can eventually break the scheme.

Quantum entanglement has long been known to provide an advantage in creating unconditionally secure randomness [1, 11]. Due to the randomness inherent in quantum mechanics, verifying that two isolated parties violate a Bell inequality provides intrinsic, fresh randomness, which can be used to yield exponential randomness expansion [38]. Further, using the rigidity of the CHSH game, it is possible to guarantee that the randomness is secure against side information, providing arbitrarily large randomness expansion [12]. The technical difficulty with these schemes is that they require entanglement between isolated parties, which remains difficult to generate in sufficient quantities.

Here, we give a protocol where entanglement between isolated parties is not required in order to expand randomness, using the rigidity of TFKW. To allow Alice to start with only a small random seed, the questions she asks are pseudorandom rather than uniformly random, requiring a computational assumption to hold during the interaction of the protocol, after which the output randomness becomes nearly identical to uniform, providing everlasting security [33, 37]. By verifying a near-optimal strategy, Alice extracts randomness using her knowledge of the state. Furthermore, we note that in our model, all of the measurement settings Alice uses can be leaked as she measures, without compromising the security or uniformity of the randomness.
1.1 Summary of Techniques

In this section, we summarise the techniques used to show our results. First, we mention our interpretation of MoE games, and then go through the general method we follow to prove rigidity of the TFKW game and apply it to achieve weak string erasure and everlasting randomness expansion.

Monogamy-of-entanglement games

We give an expression of a two-answer MoE game, such as the TFKW game, in terms of a game polynomial where the variables are Bob and Charlie’s observables. In this way, we may study the strategies of a game by studying the positivity of this operator-valued polynomial. This technique expands upon one that has been used previously to study nonlocal games [14].

Rigidity

We present a sum-of-squares (SOS) decomposition of the game polynomial for the TFKW game. The state $|\psi\rangle$ of any optimal strategy is an eigenspace of the game polynomial in terms of the observables of that strategy, which provides a selection of relations for the observables. There are two types of relations that come out: one allows to exchange Bob and Charlie’s observables and the other gives that $|\psi\rangle$ is an eigenvector of a particular sum of observables. In particular, these imply that either of the players’ observables must commute with respect to the state, generating a $|\psi\rangle$-representation of $Z_2^2$. As such, we invoke the Gowers-Hatami theorem as in [39] to locally dilate the players’ space isometrically and transform this into a bona fide representation. These observables are simultaneously diagonalisable, so the dilated shared space can be decomposed as a direct sum of orthogonal subspaces on which they act as scalars. Returning to the relations from the SOS decomposition using the dilated observables allows us to constrain where the shared state lives in this orthogonal sum and show that the components on Alice’s space must take the form $X^{s_0}Z^{s_1}|\beta\rangle$.

We then build on this technique to show the rigidity in the robust case. Here, however, since the winning probability is assumed to be some $\varepsilon > 0$ smaller than optimal, the value of each of the terms in the SOS decomposition are not zero when acting on the state, but rather in $O(\varepsilon)$. Nevertheless, we can use the relations to get an approximate representation, which we dilate similarly with Gowers-Hatami. This cannot give that the state is exactly a convex combination as above, but rather that its projection onto the unwanted subspaces is small, giving that this is $O(\sqrt{\varepsilon})$ close to an optimal state.

The most general rigidity result we prove is the robust case of the parallel repetition of TFKW games. To generalise the exact-case method, we use a technique of [9] to extract sufficiently many strategies for TFKW that win near-optimally. Proceeding by showing a relation between the near-optimal strategies on each qubit, we get that the state is $O(n^3\sqrt{\varepsilon})$ away from an optimal state given by a convex combination of tensor product of states $X^{s_0}Z^{s_1}|\beta\rangle$.

Finally, we adapt a technique of [31] to be able to pass from winning statistics Alice may observe when playing TFKW games in parallel to a guarantee on the winning probability of a large subset of the games. Knowing upper bounds on the winning probability of each of the games, we can couple independent Bernoulli random variables to each game, and use Hoeffding’s inequality to show that there is but a low probability that the players win most games while the winning probability for too many of them is more than $\varepsilon$ away from optimal.
Weak string erasure

We construct a WSE scheme whose security is based upon the rigidity of the TFKW game. The receiver Bob prepares a state $\rho_{ABC}$ shared between Alice, Bob, and Charlie, where Alice holds $N \in \text{poly}(n)$ qubits. In the honest case, this has the form of an optimal state for the parallel-repeated TFKW game, which Alice verifies by playing the game on $N - n$ of her qubits. On the remaining $n$ qubits, however, she measures in a random Wiesner-Breidbart basis, i.e. either the basis $|\beta\rangle_X Z|\beta\rangle$ or the basis $Z|\beta\rangle_X |\beta\rangle$. Informing Bob which basis she chose for these $n$ qubits, he may guess on average half of the bits and have no information about the rest. This provides security against a dishonest Bob. For security against a dishonest Alice, we note that the rigidity still gives Bob the freedom to choose the Wiesner-Breidbart state on the register he gives to Alice. It can be seen from Figure 1 that these states constitute a pair of mutually-unbiased bases. Therefore, if Bob chooses the state randomly, this eliminates Alice’s chance of guessing which bits he knows. The isolation requirement between Bob and Charlie is necessary to prevent an attack where they jointly share a maximally entangled state with Alice and then can always measure each bit in the correct basis. The requirement that Alice broadcast publicly which $n$ bits are used to generate the output string is to prevent an attack where she asks Bob and Charlie to play the TFKW game on different bits, and uses Charlie’s replies to extract information about Bob’s prepared conjugate-coding basis.

Everlasting Randomness Expansion

We use the rigidity of the TFKW game, as well as a computational assumption on the existence of pseudorandom generators, to construct a randomness expansion scheme that is everlasting, in the sense that the output randomness is guaranteed to be near-uniform in trace norm, as long as the computational assumption is not broken during the execution of the protocol. As in the previous protocol, Alice interacts with a pair of adversaries, Bob and Charlie, and they play the TFKW game on $N - n$ of the qubits. However, rather than choosing the locations and questions for the TFKW game rounds uniformly at random, she chooses them by sampling the output of a pseudorandom generator, given a random seed. Bob and Charlie, who are assumed to be computationally bounded, have only a negligible probability of distinguishing this from the uniformly random case, and thus this check has only a negligibly small probability of failure. Alice measures each of the remaining $n$ qubits in the basis $|0\rangle_\Theta, |1\rangle_\Theta$ that diagonalises the Pauli $Y$ operator. Since this basis is mutually unbiased with both of the Wiesner-Breidbart bases, the outcome is nearly uniformly random, and neither Bob nor Charlie have information on what this outcome is, as long as they stay isolated.

Further Related Work

The study of monogamy-of-entanglement games is a burgeoning field in quantum information, with several applications to cryptography. Johnston, Mittal, Russo, and Watrous [18] adapted the overlap technique of [35] to show that all MoE games with two questions can be won using an unentangled strategy and satisfy perfect parallel repetition, and gave a generalisation of the NPA hierarchy [27] that can be used on MoE games. Broadbent and Lord [6] used the TFKW game to study uncloneable encryption in the quantum random oracle model. Most recently, Coladangelo, Liu, Liu, and Zhandry [10] defined a new MoE game of a slightly different style where Bob and Charlie try to guess different strings, for which an upper
bound on the winning probability was shown by Culf and Vidick [15] using overlaps. In [10], they use this game along with some computational assumptions to construct schemes for uncloneable decryption and copy-protection of pseudorandom functions.

Our randomness expansion scheme may be contrasted with the work of Brakerski, Chris-tiano, Mahadev, Vazirani, and Vidick [4], where they also use a short-term computational assumption to achieve everlasting randomness expansion. They use the learning with errors (LWE) assumption to construct noisy trapdoor claw-free functions, to verify that an untrusted quantum device approximately prepares states in the Hadamard basis. This protocol does not require a communication assumption or a trusted measurement, but it requires a particular computational assumption and a full fault-tolerant quantum computer in the honest case. Less demanding models, where some aspects of the devices are trusted, have also been considered. In a semi-device-independent model, it is assumed that the dimensions of the devices’ Hilbert spaces are constrained [30]. Randomness expansion schemes in this model do not require entanglement, but make use of strong assumptions on the devices: a finite distribution of states and measurements, and no entanglement with another system [20]. There are also more asymmetric models, like quantum steering, where one of the devices may be completely trusted while the other is untrusted [5].

1.2 Outline

In Section 2 we present the notation and technical facts from the theories of quantum information, probability, and approximate representation of finite groups that we use throughout the paper. Next, in Section 3, we formally define the concept of a monogamy-of-entanglement game and present different ways of understanding the winning probabilities of strategies for these games. In Section 4, we prove rigidity for the TFKW game. Our most general rigidity results are given by Theorem 18 and Theorem 21. Lastly, in Section 5 we apply the rigidity result to construct a weak string erasure scheme, which we relate to a construction of bit commitment; and combine it with a computational assumption to construct a everlasting randomness expansion scheme.

2 Preliminaries

In this section, we go over the basic technical facts needed in the remainder of the paper. First, in Section 2.1, we introduce the general notation we use, which is largely standard. Next, in Section 2.2, we go over the basic objects from quantum information theory we need, including the definitions and properties of some important states and operators on the space of a qubit we see throughout. In Section 2.3, we touch on some notation and results from probability theory. Finally, in Section 2.4, we recall some results from the representation theory of finite groups and its generalisation to approximate representations. We also prove that operators we encounter later generate approximate representations.

2.1 Notation

A Hilbert space is a \( \mathbb{C} \)-vector space with an inner product that is complete as a metric space. Here, we only consider finite-dimensional Hilbert spaces so the completeness is always guaranteed. As is customary, we use Dirac bra-ket notation. For a one-dimensional Hilbert space, we write \( |v\rangle \) to mean \( \text{span}_{\mathbb{C}}\{|v\rangle\} \) when there is little chance of confusion.
Let $H$ and $K$ be Hilbert spaces. We denote the space of all linear operators $H \rightarrow K$ as $\mathcal{L}(H,K)$, and write $\mathcal{L}(H) := \mathcal{L}(H,H)$. We denote the set of these operators $\mathcal{P}(H)$ and often write $P \geq 0$ to mean $P \in \mathcal{P}(H)$. The set of isometries is $\mathcal{U}(H,K)$ and the set of unitaries is $\mathcal{U}(H) = \mathcal{U}(H,H)$. Operators $A, B \in \mathcal{L}(H)$ are said to commute if $AB = BA$ and anticommute if $AB = -BA$. The commutator of two operators is $[A, B] = AB - BA$.

We consider the natural numbers to be $\mathbb{N} = \{1, 2, 3, \ldots\}$, and for $n \in \mathbb{N}$ write the subset $[n] = \{1, \ldots, n\} \subseteq \mathbb{N}$. We see elements of the vector space $\mathbb{Z}_2^n$ for $n \in \mathbb{N}$ as bit strings, so we write them as a concatenation $x = x_1 x_2 \ldots x_n$. We define, for $i \in [n]$, $1^i \in \mathbb{Z}_2^n$ as the bit string that is 1 in position $i$ and 0 elsewhere. Analogously, for a subset $I \subseteq [n]$, write $x_I = x_{i_1} x_{i_2} \ldots x_{i_k}$ for $I = \{i_1, \ldots, i_k\}$ with $i_1 < i_2 < \ldots < i_k$; and $1^I \in \mathbb{Z}_2^n$ the string that is 1 at indices in $I$ and 0 elsewhere.

### 2.2 Quantum Information

The classical states of a system are represented by a finite set $H$ called a register. The pure quantum states are represented by superpositions of elements of the register, so vectors with norm 1 in the Hilbert space $H = \text{span}_{\mathbb{C}} \{|h\rangle : h \in H\} \cong \mathbb{C}^{|H|}$, where the spanning set is an orthonormal basis. More generally, a quantum state may be seen as a mixed state, which is represented as a density operator, a positive, trace-one operator. We write this set $\mathcal{D}(H)$ of density operators. Every mixed state may be purified by appending some auxiliary register.

We call a state classical if it is diagonal in the canonical basis of $H$ – it corresponds exactly to a probability distribution on $H$.

A quantum measurement is represented by a positive operator-valued measurement (POVM), which is a map $P : X \rightarrow \mathcal{P}(H)$, $x \mapsto P_x$ where $X$ is the (finite) set of possible measurement outcomes and $\sum_x P_x = \mathbb{1}_H$. The probability of measuring outcome $x$ given a state $\rho \in \mathcal{D}(H)$ is given by Born’s rule as $\text{Tr}(P_x \rho)$. Again, any measurement may be purified by adding auxiliary registers, to a projector-valued measurement (PVM), which is a measurement where the $P_x$ are orthogonal projectors $P_x P_y = \delta_{x,y} P_x$.

Given two registers $H$ and $K$, the corresponding joint quantum system is given by the tensor product Hilbert space $H \otimes K$. If necessary, we (perhaps inconsistently) add the name of the register as a subscript onto a state/operator to distinguish which register it acts on/belongs to. A state $|\psi\rangle \in H \otimes K$ is separable if it can be written as a pure tensor of the form $|\psi\rangle = |v\rangle_H \otimes |w\rangle_K$. Otherwise, the state is entangled. An operation is local if it acts as a pure tensor. The partial trace of a register $H$ is the linear map $\text{Tr}_H : \mathcal{L}(H \otimes K) \rightarrow \mathcal{L}(K)$ defined on pure tensors as $\text{Tr}_H(A \otimes B) = \text{Tr}(A)B$ (and extended linearly), corresponding to making a measurement on the space $H$ and then forgetting the result. For a state $\rho_{HK} \in \mathcal{D}(H \otimes K)$, we write the state on $H$ as $\rho_H = \text{Tr}_K(\rho_{HK})$.

The Euclidean norm $\|\langle v | v \rangle\| = \sqrt{\langle v | v \rangle}$ gives the appropriate distance metric between pure states. For mixed states, we use the trace distance $d_\text{tr}(\rho, \sigma) = \|\rho - \sigma\|_\text{tr} = \frac{1}{2} \text{Tr}[\rho - \sigma]$, where the absolute value of an operator is $|L| = \sqrt{L^* L}$. For other operators, we use the operator norm $\|L\| = \sup \{\|L|v\| : \langle v | v \rangle = 1\}$.

An important system is the bit $Q = \mathbb{Z}_2 = \{0, 1\}$, and its corresponding Hilbert space, the qubit $Q \cong \mathbb{C}^2$. The basis $\{|0\rangle, |1\rangle\}$ is the computational basis and the basis $\{|+\rangle, |\rangle\rangle\}$ where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\rangle\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is the Hadamard basis. The Hadamard operator is the Hermitian unitary $H : Q \rightarrow Q$ that maps the computational basis to the Hadamard basis, which is expressed in either basis as $H = \frac{1}{\sqrt{2}}[|+\rangle \langle 1| - |1\rangle \langle +|]$. In the computational basis, the Pauli operators are $Z = [1_2^0, 0_2^1], X = [0_2^1, 1_2^0], Y = [0_2^i, 1_2^{-i}]$. It is direct to check that $Z$ and $X$ anticommute, and that the Hadamard diagonalises $X$, so that $X = HZH$. We define the Breidbart operator $6 : Q \rightarrow Q$ as the Hermitian unitary that diagonalises...
H, so \( H = 6Z6 \) and in the computational basis \( \delta = \left[ \begin{array}{c} \cos \frac{\pi}{3} \\ \sin \frac{\pi}{3} \\ -\cos \frac{\pi}{3} \\ -\sin \frac{\pi}{3} \end{array} \right] \); and the Breidbart state \( |\beta\rangle = 6|0\rangle \). Important relations that follow from the definition are \( H|\beta\rangle = |\beta\rangle \), \( Z|\beta\rangle = 6|\rangle \), \( X|\beta\rangle = 6|\rangle \), and \( XX|\beta\rangle = 6|1\rangle \). Finally, we define the conjugate-coding/Wiesner/BB84 states on \( n \in \mathbb{N} \) qubits for \( x, \theta \in \mathbb{Z}_2^n \) as \( |x^\theta\rangle = H^\theta|x\rangle = H^\theta_1|x_1\rangle \otimes \cdots \otimes H^\theta_n|x_n\rangle \in \mathbb{Q}^{2^n} \); and we also call the states \( 6^{2n}|x^\theta\rangle \) the Wiesner-Breidbart states.

More details are given in any of the many resources for quantum information, such as [28,40].

2.3 Probability

Any probability distribution on a finite set \( X \) may be represented by a function \( \pi : X \to [0,1] \) such that \( \sum_{x \in X} \pi(x) = 1 \). Then, the probability of an event \( S \subseteq X \) is \( \text{Pr}(S) = \sum_{x \in S} \pi(x) \). For any function \( f : X \to V \), \( V \) is a \( \mathbb{C} \)-vector space, we write the expectation value with respect to this distribution as \( \mathbb{E}_{x \sim \pi} f(x) = \sum_{x \in X} \pi(x) f(x) \). We distinguish the uniform probability distribution \( u : X \to [0,1] \), which is \( u(x) = \frac{1}{|X|} \); and we write \( E_{x \in X} \) to mean \( \mathbb{E}_{x \sim \pi} \). Any probability distribution \( \pi \) on \( X \) can be represented as a classical state \( \mu_\pi = \mathbb{E}_{x \sim \pi} |x\rangle \langle x| \in D(X) \), where we write in particular the maximally mixed state as the classical state of the uniform distribution \( \mu_X := \mu_u \). For a random variable \( \Gamma \), we use the same notation \( \mathbb{E}_{x \sim \pi} \) to denote \( x \) sampled from the image of \( \Gamma \) with respect to its distribution. If \( \Gamma \) has image in a vector space, we write its expectation as \( \mathbb{E}_{x \sim \pi} x = \mathbb{E} \Gamma \). An important bound we make use of is Hoeffding’s inequality. Let \( \Gamma_1, \ldots, \Gamma_n \) be independent random variables with image in \([0,1]\), and write their sum \( \Gamma = \Gamma_1 + \ldots + \Gamma_n \). The inequality states that for any \( t \geq 0 \), \( \text{Pr}(\Gamma - \mathbb{E} \Gamma \geq t) \leq e^{-2t^2 \pi} \).

2.4 Exact and Approximate Representation Theory

Throughout this section, let \( G \) be a finite group. A unitary representation of \( G \) over \( \mathbb{C} \) is a group homomorphism \( \gamma : G \to \mathcal{U}(V) \), where \( V \) is a finite-dimensional \( \mathbb{C} \)-vector space. Let \( \text{Irr}(G) \) be a set of representatives for the isomorphism classes of the irreducible representations; \( \text{Irr}(G) \) has finitely many elements and the sum \( \sum_{\gamma \in \text{Irr}(G)} d_{\gamma} \text{Tr}(\gamma(g)) = |G|\delta_{g,1} \), where \( d_{\gamma} \) is the dimension of the representation \( \gamma \). The only irreducible representations of an Abelian group are 1-dimensional. The important example we see in this paper is \( \mathbb{Z}_2^n \) under addition. The irreducible representations are indexed by the elements \( s \in \mathbb{Z}_2^n \), and they take the form \( \gamma_s(x) = (-1)^{xs} \), where \( x \cdot s = x_1s_1 + x_2s_2 + \ldots + x_ns_n \). Complete explanations are available from many perspectives, such as [32,41]. We now go into rather more detail about the theory of approximate representations, which hinges on a result of Gowers and Hatami [16].

**Definition 1.** Let \( V \) and \( W \) be Hilbert spaces and let \( |\psi\rangle \in V \otimes W \). For \( \varepsilon \geq 0 \), an \((\varepsilon,|\psi\rangle)\)-representation of \( G \) is a map \( f : G \to \mathcal{U}(V) \) such that, for every \( y \in G \),

\[
\mathbb{E}_{x \in G} \| f(x)f(y) - f(xy) |\psi\rangle \|^2 \leq \varepsilon^2.
\]

(1)

The following theorem characterises how close an approximate representation is to a true representation. Note that it has a slightly different form from how they were presented in previous work [14,39]. The proof is given in the full version and is almost identical to the proof of [39].

**Theorem 2** (Gowers-Hatami). Let \( f : G \to \mathcal{U}(V) \) be a \((\varepsilon,|\psi\rangle)\)-representation. Then, there exists a Hilbert space \( V' \), an isometry \( V' \to V \), and a representation \( g : G \to \mathcal{U}(V) \) such that, for any \( x \in G \), \( \| (Vf(x) - g(x)V)|\psi\rangle \| \leq \varepsilon \).
Later, we naturally come across approximate representations of $Z_n^2$. These representations are induced by approximate commutation relations of the generators. To show they are in fact approximate representations, we need to relate approximate commutation of the generators to approximate commutation of all the elements. The proofs of these results are provided in the full version. First, we tackle the case that needs no extra assumptions, $G = Z_2^2$.

Lemma 3. Let $V$ and $W$ be Hilbert spaces, let $|\psi\rangle \in V \otimes W$, and let $U_0, U_1 \in \mathcal{U}(V)$ be self-inverse such that $\|[[U_0, U_1]|\psi\rangle\| \leq \delta$, for some $\delta \geq 0$. Then, the function $f : Z_2^2 \rightarrow \mathcal{U}(V)$ defined by $f(00) = I$, $f(01) = U_0$, $f(10) = U_1$, and $f(11) = U_0U_1$ is an $(\delta\sqrt{2}, |\psi\rangle)$-representation of $Z_2^2$.

Extending a result of this form to $Z_n^2$ for $n > 2$ requires another condition on the unitaries, in order to be able to use the commutation with respect to $|\psi\rangle$ even when there are operators sitting between the state and the unitaries. To do this, we impose an additional relation, arising from our sum-of-squares decomposition, which allows to swap operators onto another register while incurring only a small error.

Lemma 4. Let $V, W$ be Hilbert spaces, let $|\psi\rangle \in V \otimes W$, and let $U_1,...,U_n, V_1,...,V_n \in \mathcal{U}(V)$ be a collection of self-inverse unitaries such that $\|[[U_i, U_j]|\psi\rangle\| \leq \delta$, $\|U_i|\psi\rangle - V_i|\psi\rangle\| \leq \epsilon$, and $[U_i, V_j] = 0$ for some $\delta, \epsilon \geq 0$. Then, the map $f : Z_2^2 \rightarrow \mathcal{U}(V)$ defined as $f(x) = U^x := U_1^{x_1} \cdots U_n^{x_n}$, is an $(n^2(3\epsilon + \delta), |\psi\rangle)$-representation of $Z_2^2$.

### 3 Monogamy-of-Entanglement Games

In this section, we formally introduce the concept of a MoE game. In Section 3.1, we define MoE games and how to play them, and introduce the game from [35] we study in this paper. In Section 3.2, we introduce a different way to look at winning a game, and use this to get an algebraic approach, adapted from a technique for nonlocal games [2], to upper bounding the winning probability.

![Figure 2](image_url) Scenario of a monogamy-of-entanglement game. Note that Alice’s measurements, though not included in the diagram, are fixed by the description of the game.

#### 3.1 Definitions

Informally, a monogamy-of-entanglement (MoE) game is a game played by three quantum parties: a trusted referee, Alice, against two collaborating adversaries, Bob and Charlie, who may agree on a strategy but do not communicate while the game is in play. Such a game is played as follows:

1. The adversaries prepare a quantum state $\rho_{ABC}$ shared between the three players. After this, they may no longer communicate.
2. Alice chooses a measurement to make on her space and provides Bob and Charlie the information about what measurement she chose.
3. Alice measures, and Bob and Charlie both try to guess her outcome using their parts of the state.
4. The adversaries win the game if they simultaneously guessed Alice’s outcome correctly.

The setup for a generic MoE game is given in Figure 2. Note that if there were only one adversary, they would always be able to guess Alice’s measurement (as long as it is projective) by sharing a maximally entangled state. However, this is not in general true for MoE games because there is no maximal tripartite entanglement. We can define such a game more formally as follows.

Definition 5. An monogamy-of-entanglement (MoE) game is a tuple $G = (\Theta, Y, A, \pi, A)$, where

- $\Theta$ is a finite set representing the possible questions;
- $Y$ is a finite set representing the possible answers;
- $A$ is the complex Hilbert space that Alice holds;
- $\pi : \Theta \to [0, 1]$ is a function representing the probability that Alice chooses each question;
- $A : \Theta \times Y \to \mathcal{P}(A)$, $(\theta, y) \mapsto A^\theta_y$ is a function where, for each $\theta$, $A^\theta : Y \to \mathcal{P}(A)$ is a POVM.

The strategies Bob and Charlie may use are constrained only by the laws of quantum mechanics. There are other classes of strategies based on other resource theories [18] that are not studied here.

Definition 6. A quantum strategy for an MoE game $G = (\Theta, Y, A, \pi, A)$ is a tuple $S = (B, C, B, C, \rho)$, where

- $B$ and $C$ are the complex Hilbert spaces that Bob and Charlie hold, respectively;
- $B$ and $C$ are Bob and Charlie’s quantum measurements, so positive operator-valued functions $B : \Theta \times Y \to \mathcal{P}(B)$, $(\theta, y) \mapsto B^\theta_y$ and $C : \Theta \times Y \to \mathcal{P}(C)$, $(\theta, y) \mapsto C^\theta_y$, such that $B^\theta$ and $C^\theta$ are POVMs.
- and $\rho \in \mathcal{D}(A \otimes B \otimes C)$ is a shared quantum state.

Definition 7. The winning probability of a strategy $S$ for a game $G$ is

$$w_G(S) = \sum_{\theta \sim \pi, y \in Y} \text{Tr}[(A^\theta_y \otimes B^\theta_y \otimes C^\theta_y)\rho].$$

The optimal winning probability of the game is the supremum over strategies $w_G = \sup_S w_G(S)$.

Note that there is no a strategy that wins with probability $w_G$ if the set of winning probabilities is not closed. The MoE game we study here is the original game of this kind introduced in [35], where they find that the winning probability of the TFKW game is about 0.85.

Definition 8. The TFKW game is the MoE game $\text{TFKW} = (\mathbb{Z}_2, \mathbb{Z}_2, Q, u, A)$, where $u(\theta) = \frac{1}{2}$ is the uniform distribution and $A^\theta_y = |y^\theta\rangle\langle y^\theta|$. 

Theorem 9 ([35]). $w_{\text{TFKW}} = \cos^2(\frac{\pi}{8}) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$.

The canonical strategy for this game is unentangled, i.e. Bob and Charlie share no entanglement: they simply provide Alice with the Breidbart state $|\beta\rangle$ and always guess outcome 0. Note that there are optimal strategies using any of the single-qubit Wiesner-Breidbart states due to the symmetries of Alice’s measurement operators. The behaviour of these strategies is given in Table 1.
Table 1 Answers $y$ for the unentangled optimal strategies of the TFKW game. Bob and Charlie reply with the same answer, depending on both $\theta$ and the Wiesner-Breidbart state they chose.

| State          | $\theta = 0$ | $\theta = 1$ |
|----------------|--------------|--------------|
| $|\beta\rangle$ | 0            | 0            |
| $Z|\beta\rangle$ | 0            | 1            |
| $X|\beta\rangle$ | 1            | 0            |
| $XZ|\beta\rangle$ | 1            | 1            |

A result of [35] gives that a strategy for an MoE game may be assumed to be pure, i.e. the shared state is pure and Bob and Charlie’s measurements are projective.

Theorem 10 ([35]). A strategy $\mathcal{S} = (\mathcal{B}, \mathcal{C}, B, C, \rho)$ for an MoE game $\mathcal{G}$ may be purified to a pure strategy $\tilde{\mathcal{S}} = (\tilde{\mathcal{B}}, \tilde{\mathcal{C}}, \tilde{B}, \tilde{C}, \tilde{\rho})$, where $\tilde{B}$ and $\tilde{C}$ are projective and $\tilde{\rho} = |\psi\rangle\langle\psi|$ is pure, that wins with the same probability.

We called a strategy purified if it is pure as in the above lemma, but there additionally exists an auxiliary register $R$ to which none of the players have access, such that $|\psi\rangle \in A \otimes B \otimes C \otimes R$. In this way, we may reach the state of any general strategy simply by tracing out this independent.

One way to construct new MoE games is using parallel repetition. Given an MoE game $\mathcal{G}$, a parallel repetition is the game where $n$ copies of $\mathcal{G}$ is played some fixed number of times $n$ simultaneously. To win the parallel repetition, the adversaries must win all $n$ copies of $\mathcal{G}$.

Definition 11. Let $\mathcal{G} = (\Theta, Y, A, \pi, A)$ be an MoE game and let $n \in \mathbb{N}$. The $n$-fold parallel repetition of $\mathcal{G}$ is the MoE game $\mathcal{G}^n = (\Theta^n, Y^n, A^n, \pi^n, A^n)$ for $\pi^n(\theta_1, \ldots, \theta_n) = \pi(\theta_1) \cdots \pi(\theta_n)$ and $(A^n)^{(\theta_1, \ldots, \theta_n)} = A^n_{\theta_1} \otimes \cdots \otimes A^n_{\theta_n}$.

For convenience, we write in general $A^n = A_1 \otimes \cdots \otimes A_n$ where $A_i = A$, to distinguish terms in different positions. The major result of [35] is that they show that the adversaries cannot do better at the parallel-repeated TFKW game than by just playing a separate optimal strategy of the single game on each copy. This leads to an exponentially-decreasing bound on the winning probability.

We use a different notion of winning probability here. Instead of considering the probability of winning all the games at once, we consider the probability for each game using the same strategy.

Definition 12. Let $\mathcal{G} = (\Theta, Y, A, \pi, A)$ be an MoE game, let $i \in [n]$, and $\mathcal{S} = (\mathcal{B}, \mathcal{C}, B, C, \rho)$ be a strategy for $\mathcal{G}^n$. Then, the $i$-th winning probability of $\mathcal{G}^n$ is

$$w^i_{\mathcal{G}^n}(\mathcal{S}) = \frac{1}{\theta^{-\pi^n}} \sum_{y \in Y^n} \text{Tr}[[A^n_{\theta,i} \otimes B^n_{y,i} \otimes C^n_{y,i}]\rho],$$

(3)

where $A^n_{y,i} = \sum_{x_i = y} A^n_{x_i}$ and $B^n_{y,i} = \sum_{x_i = y} B^n_{x_i}$ with analogous definition for $C^n_{y,i}$.

Due to the tensor product structure of $A^n$, $A^n_{y,i}$ depends only on the $i$-th element of $\theta$. Explicitly, $A^n_{y,i} = I_1 \otimes \cdots \otimes I_{i-1} \otimes A^n_{y,i} \otimes I_{i+1} \cdots \otimes I_n$. The operators $B^n_{y,i}$ and $C^n_{y,i}$ depend in general on all the elements of $\theta$. Nevertheless, some important properties of the $A^n_{y,i}$ still hold: if the adversaries’ measurements are projective, the operators commute for the same value of $\theta$, i.e. $[B^n_{y,i,1}, B^n_{y,i,j}] = 0$, and satisfy the product relation $B^n_y = B^n_{y,1}B^n_{y,2} \cdots B^n_{y,n}$; these hold identically for the $C^n_{y,i}$. 
3.2 Observables, Bias, and Positivity

In this section, we work with a two-answer MoE game, so we identify Y with \( \mathbb{Z}_2 \): \( \mathcal{G} = (\Theta, \mathbb{Z}_2, A, \pi, A) \). As is done for nonlocal games \([14]\), we express the winning probability in terms of observables.

► **Definition 13.** Let \( P : \mathbb{Z}_2 \to \mathcal{P}(\mathcal{H}) \) be a POVM. Then, the observable of \( P \) is \( \mathcal{F} = P_0 - P_1 \).

The observable characterises the measurement as \( P_y = \frac{1}{2}(I + (-1)^y\mathcal{F}) \); and \( \mathcal{F} \) is unitary if and only if \( P \) is a POVM. In the context of an MoE game, we write the observables \( A_\theta = A \mathcal{F} \) for simplicity. It is a direct calculation to express the winning probability in terms of the observables:

\[
\mathcal{w}_\mathcal{G}(\mathcal{S}) = \frac{1}{4} \sum_{\theta \in \pi} \text{Tr}[(A_\theta \otimes (B_\theta \otimes I_C + I_B \otimes C_\theta) + I_A \otimes (I_{BC} + B_\theta \otimes C_\theta))\rho].
\]  

(4)

As in the case of a nonlocal game, we study the bias of a strategy to quantify how much it differs from a random but coordinated guess: it is a value in \([-2, 2]\) and is 0 if the winning probability is \( \frac{1}{2} \).

► **Definition 14.** The bias of a strategy \( \mathcal{S} \) for an MoE game \( \mathcal{G} \) is

\[
\mathcal{b}_\mathcal{G}(\mathcal{S}) = 4\mathcal{w}_\mathcal{G}(\mathcal{S}) - 2 = \frac{1}{4} \sum_{\theta \in \pi} \text{Tr}[(A_\theta \otimes (B_\theta \otimes I_C + I_B \otimes C_\theta) - I_A \otimes (I_{BC} - B_\theta \otimes C_\theta))\rho].
\]  

(5)

The optimal bias of the game is \( \mathcal{b}_\mathcal{G} = \sup_\Theta \mathcal{b}_\mathcal{G}(\mathcal{S}) \).

The optimal bias of the TFKW game is \( \mathcal{b}_{\text{TFKW}} = \sqrt{2} \). To simplify, we define \( b_0 = B_0 \otimes I_C \), \( c_0 = I_B \otimes C_0 \), and omit identity operators. Then, \( \mathcal{b}_\mathcal{G}(\mathcal{S}) = \frac{1}{2} \sum_{\theta \in \pi} \text{Tr}[(A_\theta \otimes (b_\theta + c_\theta) - 1 \otimes (1 - b_\theta c_\theta))\rho]. \) For any strategy, we call \( \sum_{\theta \in \Theta} \pi(\theta)(A_\theta \otimes (b_\theta + c_\theta) - 1 \otimes (1 - b_\theta c_\theta)) \) the game polynomial. For the TFKW game, the observables are Pauli operators \( A_0 = Z \) and \( A_1 = X \), giving game polynomial

\[
\frac{1}{2}(Z \otimes (b_0 + c_0) + X \otimes (b_1 + c_1) - 1 \otimes (1 - b_0 c_0) - 1 \otimes (1 - b_1 c_1)).
\]  

(6)

A simple but powerful observation is that a value \( \beta \in \mathbb{R} \) upper bounds the bias \( \beta \geq \mathcal{b}_\mathcal{G}(\mathcal{S}) \) if

\[
\beta - \frac{1}{2} \sum_{\theta \in \pi} (A_\theta \otimes (b_\theta + c_\theta) - 1 \otimes (1 - b_\theta c_\theta)) \geq 0
\]  

(7)

as operators. By considering the eigenvalues, the smallest value of \( \beta \) for which this always holds is the optimal bias \( \mathcal{b}_\mathcal{G} \). Conversely, checking whether Equation (7) holds for some fixed \( \beta \) shows \( \beta \geq \mathcal{b}_\mathcal{G} \).

This provides a way to upper bound the winning probability of an MoE game via a positivity argument. Formally, we consider whether a polynomial in a certain noncommutative algebra is positive under the matrix representations of the algebra. In language like \([29]\), we consider the semi-pre-C*-algebra \( \mathcal{L}(A)|\mathbb{F}_2^\mathcal{G}| \times \mathbb{F}_2^\mathcal{G} \), where \( \mathbb{F}_n^k \) is the free group with \( n \) generators of order \( k \). The first copy of \( \mathbb{F}_2^\mathcal{G} \) gives Bob’s observables, since they are self-inverse. Similarly, the second corresponds to Charlie’s observables, in Cartesian product since they commute with Bob’s. The algebra is then the matrix algebra over the group algebra \( \mathbb{C}[\mathbb{F}_2^\mathcal{G}| \times \mathbb{F}_2^\mathcal{G}] \), extending the scalars to contain Alice’s observables. An element \( P \) corresponding to the game polynomial belongs to this algebra, and a unitary representation where the free groups are in tensor product is a strategy.
As in [29], one way to approach positivity is with a sum-of-squares (SOS) argument. That is, if \( \beta - P \) (cf. Equation (7)) decomposes as a sum of Hermitian squares \( \sum_i S_i^\dagger S_i \), then it is positive under any representation as a Hermitian square is always a positive matrix. In fact, an SOS decomposition must exist for all \( \beta > b_G \) [29]. We use an SOS decomposition with \( \beta = b_G \) for the TFKW game.

4 Rigidity of the TFKW Game

In this section, we prove that the TFKW game is rigid. In Section 4.1, we give an SOS decomposition for the game polynomial. In Sections 4.2 and 4.3, we show rigidity for one round in the optimal then the nearly optimal cases. In Section 4.4, we extend this to games played in parallel. The main rigidity result is Theorem 18. Finally, in Section 4.5, we relate the winning statistics to the rigidity.

4.1 Sum-of-Squares Decomposition

Let \( P \) be game polynomial for TFKW. Then, \( b_{\text{TFKW}} - P = \sqrt{2} - P \) decomposes as the SOS

\[
\frac{1}{4\sqrt{2}} \left( (Z \otimes b_0 + X \otimes c_1 - \sqrt{2})^2 + (Z \otimes c_0 + X \otimes b_1 - \sqrt{2})^2 \right) + \frac{1}{4} \left( (b_0 - c_0)^2 + (b_1 - c_1)^2 \right). \tag{8}
\]

The form of the SOS takes inspiration from the one used to prove Tsirelson’s bound for the CHSH game [2,14]. First, it directly implies that \( \sqrt{2} \) upper bounds the bias of TFKW, giving an alternate proof of the winning probability to that of [35]. Conversely, an optimal state must be in the 0 eigenspace of this operator, and therefore it must be in the 0 eigenspace of each of the squared terms.

4.2 Exact Rigidity

Before dealing with the more involved robust and eventually parallel-repeated rigidity, we can get intuition from working with the exact case, where the strategy wins with exactly optimal probability.

\[\textbf{Theorem 15 (exact rigidity).} \text{ Let } S = (B,C,B,C, |\psi\rangle\langle\psi|) \text{ be a purified strategy for TFKW. If this strategy is optimal, then there exist Hilbert spaces } B', C' \text{ and isometries } V : B \to B' \text{ and } W : C \to C' \text{ such that we have a decomposition of the state}
\]

\[
(V \otimes W)|\psi\rangle = \sum_{s \in \mathbb{Z}_2 \times \mathbb{Z}_2} X^m Z^n |\beta\rangle \otimes |\psi_s\rangle, \tag{9}
\]

where the supports of the \( |\psi_s\rangle \in B' \otimes C' \otimes R \) on both \( B' \) and \( C' \) are orthogonal; and there exist commuting operators \( B_y \in \mathcal{U}(B') \) and \( C_y \in \mathcal{U}(C) \) such that

\[
VB_y|\psi\rangle = B_y'V|\psi\rangle, \\
WC_y|\psi\rangle = C_y'W|\psi\rangle, \tag{10}
\]

\[
B_y'|\psi_s\rangle = C_y'|\psi_s\rangle = (-1)^s|\psi_s\rangle. \tag{11}
\]

It is a direct to see that these strategies win optimally. Intuitively, what the players must do to win optimally is agree on a Wiesner-Breidhart state, seen in Figure 1, to give Alice, which they can do without communicating using the simultaneous distinguishability, and then guess accordingly.
28:14 Rigidity for MoE Games

Proof. Letting $P$ be the game polynomial (Equation (6)), we know $\langle \psi | \sqrt{2} - P | \psi \rangle = 0$. Then, each of the terms in the SOS (Equation (8)) is positive so they must all be zero, giving four relations \((Z \odot b_0 + X \odot c_1) | \psi \rangle = \sqrt{2} | \psi \rangle\), \((Z \odot c_0 + X \odot b_1) | \psi \rangle = \sqrt{2} | \psi \rangle\), \(b_0 | \psi \rangle = c_0 | \psi \rangle\), and \(b_1 | \psi \rangle = c_1 | \psi \rangle\). These imply a relation with only Alice and Bob’s observables, \((Z \odot b_0 + X \odot b_1) | \psi \rangle = \sqrt{2} | \psi \rangle\). Squaring, \(2 | \psi \rangle = (Z \odot b_0 + X \odot b_1)^2 | \psi \rangle = 2 | \psi \rangle + 2Z X \odot [b_0, b_1] | \psi \rangle\), so the commutator \([b_0, b_1] | \psi \rangle = 0\), that is \(b_0 \) and \(b_1 \) commute with respect to \(| \psi \rangle\). Thus, the group generated by \(B_0 \) and \(B_1 \) is a \((0, | \psi \rangle)\)-representation of \(Z^2\). By the Gowers-Hatami theorem (Theorem 2), there exists an isometry \(V : B \rightarrow B'\) and a representation \(g : Z^2 \rightarrow U(B')\) such that \(V f(x) | \psi \rangle = g(x) V | \psi \rangle\). Defining \(B'_0 = g(01)\) and \(B'_1 = g(10)\), these are commuting unitaries such that \(V B_0 | \psi \rangle = B'_0 V | \psi \rangle\). Further, as \(g \) is a representation, the dilated space decomposes as a direct sum of irreducible representations \(B' = \bigoplus_{s \in Z^2} B_s\), such that the operators act as \(B'_0 = \sum_{s \in Z^2} (-1)^s 1_{B,s}\). Following an identical line of reasoning for Charlie’s observables, there exists an isometry \(W : C \rightarrow C'\) and commuting unitaries \(C'_0, C'_1 \in U(C')\) such that \(W C_0 | \psi \rangle = C'_0 W | \psi \rangle\), and the space decomposes as \(C' = \bigoplus_{s \in Z^2} C_s\) so that \(C'_0 = \sum_{s \in Z^2} (-1)^s 1_{C,s}\). Defining the dilated state \(| \psi' \rangle = (V \otimes W) | \psi \rangle\), we have that the relations extend to the dilated spaces as

\[
\begin{align*}
(Z \otimes B'_0 + X \otimes B'_1) | \psi' \rangle &= \sqrt{2} | \psi' \rangle \\
B'_0 | \psi' \rangle &= C'_0 | \psi' \rangle \\
B'_1 | \psi' \rangle &= C'_1 | \psi' \rangle.
\end{align*}
\]

Now, since \(| \psi' \rangle \in A \otimes B' \otimes C' \otimes R = \bigoplus_{s, s' \in Z^2} A \otimes B_s \otimes C_{s'} \otimes R\), we can decompose it accordingly as \(| \psi' \rangle = \sum_{s, s' \in Z^2} | v_{s, s'} \rangle\). Then, Equation (13) gives that \(\sum_{s, s' \in Z^2} (-1)^{s_0} | v_{s, s'} \rangle = \sum_{s, s' \in Z^2} (-1)^{s'} | v_{s, s'} \rangle\), so \(v_{s, s'} = 0\) if \(s_0 \neq s'_0\). Doing the same with Equation (14) gives that \(v_{s, s'} = 0\) if \(s \neq s'\). The decomposition of the spaces means that \((Z \otimes B_0 + X \otimes B_1) \otimes 1_{C,R} = \sum_{s, s' \in Z^2} ((-1)^s Z + (-1)^s X) \otimes 1_{B,s} \otimes 1_{C,R}\); and Equation (12) says that \(| \psi' \rangle\) must belong to the \(\sqrt{2}\)-eigenspace of this operator. Since \((-1)^s Z + (-1)^s X = \sqrt{2} X^{s_0} Z^{s_1} H Z^{s_1} X^{s_0}\), the \(\sqrt{2}\)-eigenspace is simply the span of \(X^{s_0} Z^{s_1} | \beta \rangle\). Thus, \(| \psi' \rangle \in \bigoplus_{s, s' \in Z^2} X^{s_0} Z^{s_1} | \beta \rangle \otimes B_s \otimes C_{s'} \otimes R\).

Taking the intersection of the spaces \(| \psi' \rangle\) belongs to, \(| \psi' \rangle \in \bigoplus_{s \in Z^2} X^{s_0} Z^{s_1} | \beta \rangle \otimes B_s \otimes C_s \otimes R\), which gives the result.

4.3 Robust Rigidity

Now, we move on to the study of the robust rigidity, where the winning probability is slightly below optimal. We can approach the proof as in the exact case, while keeping track of the error.

**Theorem 16** (robust rigidity). Let \(S = (B, C, B', C, | \psi \rangle | \psi \rangle^\dagger\) be a purified strategy for TFKW that wins with probability \(w_{TFKW}(S) \geq \cos^2 \frac{\pi}{8} - \varepsilon\) for some \(\varepsilon \geq 0\). Then there exists a constant \(K = 110\) and isometries \(V : B \rightarrow B'\) and \(W : C \rightarrow C'\) such that the distance between quantum states

\[
\left\| (V \otimes W) | \psi \rangle - \sum_{s \in Z^2} X^{s_0} Z^{s_1} | \beta \rangle \otimes | \psi_s \rangle \right\| \leq K \sqrt{\varepsilon},
\]

\[
(16)
\]
where the $|\psi_a\rangle \in B' \otimes C' \otimes R$ have orthogonal supports on both $B'$ and $C$; and there exists a constant $L = 18$, and commuting observables $B'_0 \in \mathcal{U}(B')$ and $C'_0 \in \mathcal{U}(C)$ such that

\begin{align}
&\|VB'_0|\psi\rangle - B'_0V|\psi\rangle\| \leq L \sqrt{\varepsilon} \\
&\|WCG'_0|\psi\rangle - C'_0W|\psi\rangle\| \leq L \sqrt{\varepsilon},
\end{align}

(17)

\begin{align}
&|B'_0|\psi_a\rangle = C'_0|\psi_a\rangle = (-1)^a|\psi_a\rangle.
\end{align}

(18)

As seen for the CHSH game in [31], the $O(\sqrt{\varepsilon})$-dependence of this upper bound is in fact necessary, though it may be possible to improve the constants: if we take an unentangled optimal strategy for TFKW and perturb by a vector of length $\delta$, the winning probability decreases $O(\delta^2)$.

**Proof.** By hypothesis, the bias $b_{\text{TFKW}}(S) \geq \sqrt{2 - 4\varepsilon}$, so $\langle \sqrt{2 - P}|\psi\rangle \leq 4\varepsilon$. Using the SOS,

\begin{align}
16\sqrt{2\varepsilon} \geq \langle \psi| (Z \otimes b_0 + X \otimes c_1 - \sqrt{2})^2 |\psi\rangle + \langle \psi| (Z \otimes c_0 + X \otimes b_1 - \sqrt{2})^2 |\psi\rangle \\
+ \sqrt{2}\left(\langle \psi| (b_0 - c_0)^2 |\psi\rangle + \langle \psi| (b_1 - c_1)^2 |\psi\rangle\right).
\end{align}

(19)

We have $8\sqrt{2\varepsilon} \geq \min\left\{ \langle \psi| (Z \otimes b_0 + X \otimes c_1 - \sqrt{2})^2 |\psi\rangle, \langle \psi| (Z \otimes c_0 + X \otimes b_1 - \sqrt{2})^2 |\psi\rangle \right\}$ and $16\varepsilon \geq \langle \psi| (b_0 - c_0)^2 |\psi\rangle$, since each term is positive. These the Euclidean norm conditions

\begin{align}
2(8)^{1/4} \sqrt{\varepsilon} \geq \min\left\{ \left\| (Z \otimes b_0 + X \otimes c_1 - \sqrt{2}) |\psi\rangle \right\|, \left\| (Z \otimes c_0 + X \otimes b_1 - \sqrt{2}) |\psi\rangle \right\| \right\}
\end{align}

(20)

\begin{align}
4\sqrt{\varepsilon} \geq \left\| (b_0 - c_0) |\psi\rangle \right\|.
\end{align}

(21)

Using Equation (21) in Equation (20), we get

\begin{align}
\left\| (Z \otimes b_0 + X \otimes b_1 - \sqrt{2}) |\psi\rangle \right\| \leq \left\| (Z \otimes b_0 + X \otimes c_1 - \sqrt{2}) |\psi\rangle \right\| + \left\| X \otimes (b_1 - c_1) |\psi\rangle \right\|,
\end{align}

(22)

\begin{align}
\left\| (Z \otimes b_0 + X \otimes b_1 - \sqrt{2}) |\psi\rangle \right\| \leq \left\| (Z \otimes c_0 + X \otimes b_1 - \sqrt{2}) |\psi\rangle \right\| + \left\| X \otimes (b_0 - c_0) |\psi\rangle \right\|,
\end{align}

(23)

which gives $\left\| (Z \otimes b_0 + X \otimes b_1 - \sqrt{2}) |\psi\rangle \right\| \leq 2(2 + 8^{1/4}) \sqrt{\varepsilon}$. Noting $X \otimes [b_0, b_1] = (Z \otimes b_0 + X \otimes b_1)^2 - 2 = (Z \otimes b_0 + X \otimes b_1 + \sqrt{2})(Z \otimes b_0 + X \otimes b_1 - \sqrt{2})$, we have that

\begin{align}
\left\| [b_0, b_1] |\psi\rangle \right\| = \left\| ZX \otimes [b_0, b_1] |\psi\rangle \right\| \leq \left\| ZX \otimes X \otimes b_1 + \sqrt{2} \right\| \left\| (Z \otimes b_0 + X \otimes b_1 - \sqrt{2}) |\psi\rangle \right\|
\leq 2(2 + \sqrt{2})(2 + 8^{1/4}) \sqrt{\varepsilon},
\end{align}

(24)

that is, Bob’s operators almost commute with respect to $|\psi\rangle$. We use Lemma 3 with $U_0 = B_0$ and $U_1 = B_1$ to generate a $\langle \sqrt{2(2 + \sqrt{2})(2 + 8^{1/4}) \sqrt{\varepsilon)}, |\psi\rangle \rangle$-representation $f$ of $Z^2_2$. By Gowers-Hatami, there exists an isometry $V : B \rightarrow B'$ to some Hilbert space and a representation $g : Z^2_2 \rightarrow U(\mathcal{B}')$ such that $\| (Vf(x) - g(x)V)|\psi\rangle \| \leq \sqrt{2}(2 + \sqrt{2})(2 + 8^{1/4}) \sqrt{\varepsilon}$. Defining $B'_0 = g(01)$ and $B'_1 = g(10)$, they are commuting observables such that $\| (VB'_0 - B'_0V)|\psi\rangle \| \leq \sqrt{2}(2 + \sqrt{2})(2 + 8^{1/4}) \sqrt{\varepsilon}$; and since $g$ is a representation, there exists an orthogonal decomposition $B' = \bigoplus_{s \in Z^2_2} B_s$ where $B'_0 = \sum_{s \in Z^2_2} (-1)^s B_s$. In the same way, $C'_0 = \bigoplus_{s \in Z^2_2} C_s$ and $C'_0 = \sum_{s \in Z^2_2} (-1)^s C_s$, and there exists an isometry $W : C \rightarrow C'$ such that $\| (WC'_0 - C'_0W)|\psi\rangle \| \leq \sqrt{2}(2 + \sqrt{2})(2 + 8^{1/4}) \sqrt{\varepsilon}$. Defining $|\psi'\rangle = (V \otimes W)|\psi\rangle$, we can extend Equation (20) and Equation (21) to the dilated spaces as

\begin{align}
\left\| (Z \otimes B'_0 + X \otimes B'_1 - \sqrt{2}) |\psi'\rangle \right\| \leq 2(2 + 2\sqrt{2})(2 + 8^{1/4}) \sqrt{\varepsilon},
\end{align}

(25)

\begin{align}
\left\| B'_0|\psi'\rangle - C'_0|\psi'\rangle \right\| \leq 4(1 + \sqrt{2})(2 + 8^{1/4} + 1) \sqrt{\varepsilon}.
\end{align}

(26)
Rigidity for MoE Games

From the decomposition of Bob and Charlie’s spaces, $A \otimes B' \otimes C' \otimes R = \bigoplus_{s,s' \in \mathbb{Z}_2} A \otimes B_s \otimes C_s' \otimes R$, thus the state decomposes accordingly as $|\psi\rangle = \sum_{s,s' \in \mathbb{Z}_2} |v_{s,s'}\rangle$. Using this in Equation (26) gives $4((1 + \sqrt{2})(2 + 8^{1/4}) + 1)\sqrt{\varepsilon} \geq \|\sum_{s,s' \in \mathbb{Z}_2} ((-1)^{s} - (-1)^{s'})|v_{s,s'}\rangle\| = 2\|\sum_{s \neq s'} |v_{s,s'}\rangle\|$.

We write $|v_0\rangle = \sum_{s} |v_{s,s}\rangle$ and $|v_1\rangle = \sum_{s \neq s'} |v_{s,s'}\rangle$, so that $|\psi\rangle = |v_0\rangle + |v_1\rangle$ and $\|v_1\|| \leq \|\sum_{s \neq s'} |v_{s,s'}\rangle\| + \|\sum_{s \neq s'} |v_{s,s'}\rangle\| \leq 4((1 + \sqrt{2})(2 + 8^{1/4}) + 1)\sqrt{\varepsilon}$. Writing $|\beta_s\rangle = X^{s'} Z Z^1 |\beta_s\rangle$, we can decompose $Z \otimes B_0^s + X \otimes B_1^s - \sqrt{\varepsilon} = \sum_{s} ((-1)^{s}Z + (-1)^{s}X - \sqrt{\varepsilon}) \otimes I_{B,s} = 2\sqrt{\varepsilon} \sum_{s} (|\beta_s\rangle (\beta_s - I) \otimes I_{B,s})$. Also, define the projection $|v_{s}\rangle = \sum_{s} (|\beta_s\rangle (\beta_s \otimes I)) |v_{s,s}\rangle$, so that Equation (25) implies

$$\|\|\psi\rangle - |v_{s}\rangle\|| \leq \left\|\sum_{s' \neq s} (|\beta_s\rangle (\beta_s - I)|v_{s,s'}\rangle\right\| + \left\|\sum_{s \neq s'} (|\beta_s\rangle (\beta_s \otimes I)) |v_{s,s'}\rangle\right\| \leq (6 + \frac{\varepsilon}{2}) (2 + 8^{1/4}) + 4\sqrt{\varepsilon}. \quad (27)$$

Note that although $|v_{s}\rangle$ is not necessarily normalised, it must be subnormalised and the above implies that $\left\|\sum_{s' \neq s} (|\beta_s\rangle (\beta_s - I)|v_{s,s'}\rangle\right\| = \left\|\sum_{s \neq s'} (|\beta_s\rangle (\beta_s \otimes I)) |v_{s,s'}\rangle\right\| \leq \left\|\|\psi\rangle - \|v_{s}\rangle\|| \leq (6 + \frac{\varepsilon}{2}) (2 + 8^{1/4}) + 4\sqrt{\varepsilon}$. Defining $|\phi\rangle = \sum_{s' \neq s} (|\beta_s\rangle \otimes |v_{s,s}\rangle)$, we have by construction that $|\phi\rangle = \sum_{s} (|\beta_s\rangle \otimes |v_{s,s}\rangle) \in B_s \otimes C_s \otimes R$, so simultaneously distinguishable by Bob and Charlie. Thus, to complete the proof,

$$\|\|\psi\rangle - |\phi\rangle\|| \leq \|\|\psi\rangle - |v_{s}\rangle\|| + \|v_{s}\rangle - |\phi\rangle\|| \leq 2(6 + \frac{\varepsilon}{2}) (2 + 8^{1/4}) + 4\sqrt{\varepsilon}. \quad \blacksquare$$

4.4 Parallel-Repeated Robust Rigidity

Now, we consider the robust rigidity of the parallel-repeated game. In the full version, we first consider the exact parallel case, but for conciseness, we skip this here. First, we need a lemma that relates the operators of any two strategies that share the same state.

Lemma 17. Let $^0\mathcal{S}$ and $^1\mathcal{S}$ be purified strategies for $TFKW$ that both win with probability $w_{TFKW}(^0\mathcal{S}) \geq \cos^2\left(\frac{\pi}{2}\right) - \delta$ for some $\delta \geq 0$. If we suppose their shared states are equal, $|\psi\rangle = |^0\psi\rangle = |^1\psi\rangle$, then there is a constant $Q = 6300$ such that for every $\theta \in \mathbb{Z}_2$,

$$\|{^0B_0}|\psi\rangle - {^1B_0}|\psi\rangle\| \leq Q\sqrt{\delta}$$
$$\|{^0C_0}|\psi\rangle - {^1C_0}|\psi\rangle\| \leq Q\sqrt{\delta}. \quad (28)$$

Proof. For each strategy, we use Theorem 16 where we may assume that the isometries are equal, since their images have equal dimension. Then, there exist $K, L \geq 0$; Hilbert spaces with two decompositions $B' = \bigoplus_{s \in \mathbb{Z}_2} B_s$ and $C' = \bigoplus_{s \in \mathbb{Z}_2} C_s'$; isometries $V : B \rightarrow B'$ and $W : C \rightarrow C'$; and vectors $|\psi_i\rangle \in B'_s \otimes C'_s \otimes R$ such that $\||V \otimes W||\psi\rangle - \sum_{s \in \mathbb{Z}_2} |\beta_s\rangle \otimes |\psi'_s\rangle\|| \leq K\sqrt{\delta}$. Further, for each $\theta \in \mathbb{Z}_2$, there exist unitary observables $^1B'_\theta \in \mathcal{U}(B')$ and $^1C'_\theta \in \mathcal{U}(C')$ such that

$$\left\||^1B'_\theta|\psi\rangle - (^1B'_\theta|\psi\rangle)\right\| \leq L\sqrt{\delta}, \quad \left\||W \otimes C'_\theta - (W \otimes C'_\theta)|\psi\rangle\right\| \leq L\sqrt{\delta},$$
$$|^1C'_\theta|\psi\rangle = (W \otimes C'_\theta)|\psi\rangle = (-1)^{s'}|\psi'_s\rangle, \quad [^1B'_\theta, ^1B'_{\theta}] = 0, \quad [^1C'_\theta, ^1C'_{\theta}] = 0. \quad (29)$$

First, utilising the triangle inequality, the distance between the two rigidity decompositions is $\||\sum_{s \in \mathbb{Z}_2} |\beta_s\rangle \otimes |\psi'_s\rangle - \sum_{s \in \mathbb{Z}_2} |\beta_s\rangle \otimes |\psi'_s\rangle\|| \leq 2K\sqrt{\delta}$. Expanding $A$ in the basis $\{|\beta_{00}\rangle, |\beta_{11}\rangle\}$,

$$\left\||^1B'_0|\psi_{00}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{01}\rangle + |^1\psi_{01}\rangle)\right\| - \left\||^1B'_0|\psi_{00}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{01}\rangle + |^1\psi_{01}\rangle)\right\| \leq 2K\sqrt{\delta}$$
$$\left\||^1B'_1|\psi_{11}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{00}\rangle - |^1\psi_{00}\rangle)\right\| - \left\||^1B'_1|\psi_{11}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{00}\rangle - |^1\psi_{00}\rangle)\right\| \leq 2K\sqrt{\delta}. \quad (30)$$

$$\left\||^1C'_0|\psi_{00}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{01}\rangle + |^1\psi_{01}\rangle)\right\| - \left\||^1C'_0|\psi_{00}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{01}\rangle + |^1\psi_{01}\rangle)\right\| \leq 2K\sqrt{\delta}$$
$$\left\||^1C'_1|\psi_{11}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{00}\rangle - |^1\psi_{00}\rangle)\right\| - \left\||^1C'_1|\psi_{11}\rangle + \frac{1}{\sqrt{2}}(|^1\psi_{00}\rangle - |^1\psi_{00}\rangle)\right\| \leq 2K\sqrt{\delta}. \quad (31)$$
We use projectors $i\Pi_\varepsilon^B = iB_0^iB_0^{i+1}$, $i\Pi_\varepsilon^C = iC_0^iC_0^{i+1}$. These are norm 1 so acting by $\Pi_\varepsilon^B \otimes \Pi_\varepsilon^C$ on Equation (31) gives $\|i\Pi_\varepsilon^B|\psi_i\rangle\| \leq 2K\sqrt{\delta}$, $\|i\Pi_\varepsilon^B|\psi_0\rangle\| \leq 2\sqrt{2K}\sqrt{\delta}$. Acting by $\Pi_\varepsilon^{B_0}$ on Equation (30) gives $\|\psi_0\rangle - i\Pi_\varepsilon^{B_0}|\psi_0\rangle\| \leq 6K\sqrt{\delta}$. This holds for other values of $s$, so

$$\|\psi_0\rangle - |\psi_i\rangle\| \leq \|\psi_0\rangle - i\Pi_\varepsilon^B|\psi_0\rangle\| + \sum_{s \neq 0} \|i\Pi_\varepsilon^B|\psi_0\rangle\| \leq 4(2 + \sqrt{2})K\sqrt{\delta}. \quad (32)$$

The same thing holds in the same way for the other values of $s$ in the ket. Then

$$\|\Pi_\varepsilon^{B_0} - i\Pi_\varepsilon^{B_0}\| = \|\Pi_\varepsilon^{B_0} - i\Pi_\varepsilon^{B_0}\| \leq \|\Pi_\varepsilon^{B_0} - i\Pi_\varepsilon^{B_0}(V \otimes W)|\psi_i\rangle\| + 2L\sqrt{\delta}
\leq \|\Pi_\varepsilon^{B_0} \sum_{a \in 2^2} |\beta_a\rangle \otimes |\psi_a\rangle - i\Pi_\varepsilon^{B_0} \sum_{a \in 2^2} |\beta_a\rangle \otimes |\psi_a\rangle\| + 2K\sqrt{\delta} + 2L\sqrt{\delta}
= \|\sum_{a \in 2^2} (-1)^a |\beta_a\rangle \otimes (|\psi_a\rangle - |\psi_a\rangle)| + 2K\sqrt{\delta} + 2L\sqrt{\delta} \leq 20000(K + L)\sqrt{\delta} \quad (33)$$

We can do the same with Charlie’s observables.

**Theorem 18 (robust parallel-repeated rigidity).** Let $n \in \mathbb{N}$ and let $S = (B, C, B, C, \rho = |\psi\rangle\langle\psi|)$ be a purified strategy for $\text{TPR}^\rho$. Suppose that for some $\varepsilon \geq 0$, for each $i \in [n]$, the $i$-th game wins with probability $w_{\text{TPR}}(S) \geq cos^2 \frac{\pi}{4} - \varepsilon$. Then, there exists a constant $K = 320 000 + o(1)$, Hilbert spaces $B'$ and $C'$, and isometries $V : B \rightarrow B'$ and $W : C \rightarrow C'$ such that the distance between quantum states

$$\|\Pi_\varepsilon^{B_0} - i\Pi_\varepsilon^{B_0}\| = \|\Pi_\varepsilon^{B_0} - i\Pi_\varepsilon^{B_0}\| \leq \|\Pi_\varepsilon^{B_0} - i\Pi_\varepsilon^{B_0}(V \otimes W)|\psi_i\rangle\| + 2L\sqrt{\delta}
\leq \|\Pi_\varepsilon^{B_0} \sum_{a \in 2^2} |\beta_a\rangle \otimes |\psi_a\rangle - i\Pi_\varepsilon^{B_0} \sum_{a \in 2^2} |\beta_a\rangle \otimes |\psi_a\rangle\| + 2K\sqrt{\delta} + 2L\sqrt{\delta}
= \|\sum_{a \in 2^2} (-1)^a |\beta_a\rangle \otimes (|\psi_a\rangle - |\psi_a\rangle)| + 2K\sqrt{\delta} + 2L\sqrt{\delta} \leq 20000(K + L)\sqrt{\delta} \quad (33)$$

for at least one value of $\varphi$ for each $i$.

The $i$-th strategies $\varphi^i$ is $(B, C, \varphi^iB, \varphi^iC, \rho)$ where $\varphi^iB_0 = B_0^iB_0^{i+1}$ and $\varphi^iC_0 = C_{0,0}^i$. for the game where $A_0^i = (A^i)^{0,1}_y$. We make use of the fact that the $i$-th winning probability is $w_{\text{TPR}}(S) = \mathbb{E}_{\varphi_i = 0} w_{\text{TPR}}(\varphi^iS)$. However, since this is not optimal, showing that the $\varphi^iS$ win near-optimally is an obstacle. To get past this, we adapt a technique of [9]. It guarantees that there is a “good set” of strategies which wins nearly as well, and the set is large enough to continue the proof.

**Proof.** Define $\varepsilon_{\varphi, i} \geq 0$ such that $w_{\text{TPR}}(\varphi^iS) = cos^2 \frac{\pi}{4} - \varepsilon_{\varphi, i}$. Then, we have that, for each $i$, $\varepsilon_{\varphi, i} \geq \mathbb{E}_{\varphi_i = 0} \varepsilon_{\varphi, i}$. We want enough terms where $\varepsilon_{\varphi, i}$ is not much larger than $\varepsilon$. To do so, let the set of good values of $\varphi$ be $G_i = \{ \varphi \in \mathbb{Z}^2 : \varphi_i = 0 |\varepsilon_{\varphi, i} \leq \varepsilon \}$. As in [9], we claim $|G_i| \geq 2^{n-i} - 2^{n-i} + 1$. In fact, suppose $|G_i| < 2^{n-i} - 2^{n-i} + 1$. Then, there are at least $2^{n-i}$ values of $\varphi$ where $\varepsilon_{\varphi, i} > \varepsilon$. But $\varepsilon \geq \frac{1}{2\sqrt{3}} \sum_{\varphi \in G_i} \varepsilon_{\varphi, i} > \frac{1}{2\sqrt{3}} 2^{n-i} 2^2 = \frac{1}{2} \frac{1}{2} 2^{n-i} 2^{n-i} > \frac{1}{2} \varepsilon > \varepsilon$, which is a contradiction. Now, as a single game, for $\varphi \in G_i$, the SOS implies $\|\Pi_\varepsilon^{B_0} - i\Pi_\varepsilon^{B_0}\| \leq 4\sqrt{3}\sqrt{\varepsilon}$. We get commutation of $\varphi^iB_0$ and $\varphi^iB_1$ with respect to $|\psi\rangle$
\[ \| [\psi^i B_\theta, \psi^{i'} B_\rho] |\psi\rangle \| \leq 2\sqrt{5}(2 + \sqrt{2})(2 + 8^{1/4})\sqrt{\varepsilon} =: K_0\sqrt{\varepsilon}. \]  

(37)

Now, we need commutation between operators for different values of \(i\). Let \(i \neq i' \in [n]\), \(\theta, \theta' \in \mathbb{Z}_2\) and \(\varphi, \varphi' \in \mathbb{Z}_2^2\) such that \(\varphi_i = \varphi'_{i'} = 0\). By the pigeonhole principle, there exists a \(\chi \in (G_i + \theta \mathbb{1}) \cap (G_{i'} + \theta' \mathbb{1})\), so using Lemma 17 with \(\delta = 5\varepsilon\), there exists \(Q \geq 0\) such that

\[ \| (\psi^i B_\theta - \chi^{i+\theta \mathbb{1}} B_\rho) |\psi\rangle \| \leq \sqrt{5}Q\sqrt{\varepsilon} \quad \| (\psi^{i'} B_{\theta'} - \chi^{i'+\theta' \mathbb{1}} B_{\rho'}) |\psi\rangle \| \leq \sqrt{5}Q\sqrt{\varepsilon}, \]  

and identically for Charlie’s observables. Thus, knowing \(\| [\chi^{i+\theta \mathbb{1}} B_\theta, \chi^{i'+\theta' \mathbb{1}} B_{\theta'}] |\psi\rangle \| \leq K_0\sqrt{\varepsilon},\)

\[ \| [\psi^{i B_\theta}, \psi^{i' B_{\theta'}}] |\psi\rangle \| \leq \| (\psi^i B_\theta \otimes \psi^{i'} B_{\theta'} - \psi^{i',i} C_{\theta'} \otimes \psi^i C_{\theta}) |\psi\rangle \| + 8\sqrt{5}\sqrt{\varepsilon} \]

\[ \leq \| (\chi^{i+\theta \mathbb{1}} B_\theta \otimes \chi^{i'+\theta' \mathbb{1}} C_{\theta'} - \chi^{i'+\theta' \mathbb{1}} B_{\theta'} \otimes \chi^{i+\theta \mathbb{1}} C_{\theta}) |\psi\rangle \| \]

\[ + (4\sqrt{5}Q + 8\sqrt{5})\sqrt{\varepsilon} \leq (4\sqrt{5}(Q + 4) + K_0)\sqrt{\varepsilon}. \]  

(39)

For each \(i\), pick some \(\varphi \in G_i\) to define \(i B_\theta := \psi^i B_\theta\), so \(\| [i B_\theta, i' B_{\theta'}] |\psi\rangle \| \leq (4\sqrt{5}(Q + 4) + K_0)\sqrt{\varepsilon}\). Then, Lemma 4 with \(U_0 = i B_\theta\), \(V_0 = C\theta\), \(\varepsilon = 4\sqrt{5}\sqrt{\varepsilon}\), and \(\delta = (4\sqrt{5}(Q + 4) + K_0)\sqrt{\varepsilon}\) generates \((L_n)^2\sqrt{\varepsilon}, |\psi\rangle\)-representation of \((\mathbb{Z}_2^n)^{\mathbb{Z}_2}\) for \(L = 4\sqrt{5}(Q + 4) + K_0\). The same holds for Charlie.

This lets us use the Gowers-Hatami theorem again. There exist Hilbert spaces with decompositions \(B' = \bigoplus_{t \in \mathbb{Z}_2} B_t\) and \(C' = \bigoplus_{t \in \mathbb{Z}_2} C_t\); isometries \(V : B \to B'\) and \(W : C \to C'\); and observables \(\chi^{i B_\theta} = \sum_{t \in \mathbb{Z}_2} (-1)^{t \varphi_{i,t}} 1_{B_t} \in U(B')\) and \(\chi^{i' C_\theta} = \sum_{t \in \mathbb{Z}_2} (-1)^{t \varphi'_{i',t}} 1_{C_t} \in U(C')\) such that

\[ \| (V^i B_\theta - i B_\theta V)|\psi\rangle \| = L_n^2\sqrt{\varepsilon} \quad \| (W^i C_\theta - i C_\theta W)|\psi\rangle \| = L_n^2\sqrt{\varepsilon}. \]  

(40)

Let \(|\psi\rangle = (V \otimes W)|\psi\rangle\). We can put these observables back into the original inequalities to get

\[ \| (Z_i \otimes B_0' + X_i \otimes (B_1' - \sqrt{2})|\psi\rangle \| \leq (2L_n^2 + 2\sqrt{5}(2 + 8^{1/4}))\sqrt{\varepsilon} \]  

(41)

\[ \| (B_0' - C_0')|\psi\rangle \| \leq (2L_n^2 + 4\sqrt{5})\sqrt{\varepsilon}. \]  

(42)

Since the quantum state \(|\psi\rangle\) \(\in \bigoplus_{t,t' \in \mathbb{Z}_2} \bigoplus_{\mathbb{Z}_2} A_1 \otimes \cdots \otimes A_n \otimes B_t \otimes C_{t'} \otimes \mathbb{R}\), we can write it as

\[ |\psi\rangle = \sum_{t,t' \in \mathbb{Z}_2} |v_{t,t'}\rangle. \]

Using \(Z_i \otimes B_0' + X_i \otimes B_1' - \sqrt{2} = 2\sqrt{2} \sum_{t} (|\beta_{t,i}\rangle |\beta_{t,1}\rangle - 1) \otimes 1_{B_t}\) and defining \(|v_{\beta,i}\rangle = \sum_{t \in \mathbb{Z}_2} (|\beta_{t,i}\rangle |\beta_{t,1}\rangle \cdots |\beta_{t,n}\rangle |v_{t,t'}\rangle\), we have

\[ \| |\psi\rangle - |v_{\beta,i}\rangle \| \leq \frac{1}{\sqrt{2}} \sum_{t=1}^{n-1} \| (Z_i \otimes B_0' + X_i \otimes B_1' - \sqrt{2})|\psi\rangle \| \leq \frac{1}{\sqrt{2}}(L_n^2 + \sqrt{5}(2 + 8^{1/4}))\sqrt{\varepsilon}. \]  

(43)

Equation (42) implies \(2L_n^2 + 4\sqrt{5})\sqrt{\varepsilon} \geq \sum_{t,t'} \| (\Omega_{t,t'}) |v_{t,t'}\rangle \| \]

\[ = \| \sum_{t \neq t'} |v_{t,t'}\rangle \| \]. Writing \(|\psi\rangle = |v_0\rangle + |v_1\rangle\) where \(|v_0\rangle = \sum_{t \in \mathbb{Z}_2} |v_{t,t'}\rangle\) and \(|v_1\rangle = \sum_{t \neq t'} |v_{t,t'}\rangle\). Then,

\[ \| |v_1\rangle \|^2 = \sum_{t \neq t'} \langle v_{t,t'} | v_{t,t'} \rangle \leq \sum_{\theta} \sum_{t \neq t'} \sum_{i \neq i'} \langle v_{t,t'} | v_{t,t'} \rangle \leq 2n \left[ \left( L_n^2 + 2\sqrt{5}\right) \sqrt{\varepsilon} \right]^2. \]  

(44)
Now, let $|v_β⟩ = \sum_{i∈(2\mathbb{Z})^n} |β_1⟩(|β_1⟩⊗⋯⊗|β_n⟩)_{i,ε}$, then $||v_β⟩ - |v_β,n⟩|| ≤ ||v_β⟩||$, so $||v_β⟩ - |v_β⟩|| ≤ ||v_β⟩ - |v_β,n⟩|| + ||v_β,n⟩ - |v_β⟩|| ≤ \left(\frac{n}{\sqrt{2}}(Ln^2 + \sqrt{5}(2 + 8^{1/4})) + 2\sqrt{2n}(Ln^2 + 2\sqrt{5})\right)\sqrt{ε}$. To normalise $|v_β⟩$, let $|φ⟩ = \frac{|v_β⟩}{||v_β⟩||}$, giving $||v_β⟩ - |φ⟩|| ≤ 2||v_β⟩ - |v_β⟩|| ≤ \sqrt{2}\left[n(Ln^2 + \sqrt{5}(2 + 8^{1/4})) + 2\sqrt{2n}(Ln^2 + 2\sqrt{5})\right]\sqrt{ε}$.

We can generalise this result slightly to a general strategy, using the properties of purified strategies

**Corollary 19.** Let $n ∈ \mathbb{N}$ and let $S = (B, C, B, C, ρ)$ be an arbitrary strategy for $\text{TFKW}$. Suppose that for some $ε ≥ 0$, for each $i ∈ [n]$, the $i$-th game wins with probability $w_{\text{TFKW}}^i(S) ≥ \cos^2 \frac{π}{8} − ε$. Then there exists a constant $K ≥ 0$ and isometries $V : B → B'$ and $W : C → C'$ such that

$$||V ⊗ W)ρ(V ⊗ W)^\dagger - Tr[R(|φ⟩⟨φ|)]||_{Tr} ≤ Kn^3\sqrt{ε},$$

where $R$ is an auxiliary register such that $|φ⟩ = \sum_{i∈(2\mathbb{Z})^n} X^{1i}Z^{t1i}|β⟩⊗⋯⊗X^{1o}Z^{t0i}|β⟩⊗|ψ⟩$ for some vectors $|ψ⟩ ∈ B' ⊗ C ⊗ R$ with orthogonal supports on both $B'$ and $C'$.

To prove Corollary 19 we use the relation between the Euclidean and trace distances (see full version), trace out $R$, and use the fact that measurement purification is isometric (Theorem 10).

### 4.5 Observed Statistics

In any self-testing scenario, the referee cannot actually query the winning probability of the adversaries’ strategy. To get around this, she may play many rounds of the game in parallel and use the winning statistics to approximate their winning probability. The information Alice receives might not be meaningful as the players’ strategies need not be independent for the different rounds of the game. A technique of [31] allows us to get around this.

**Lemma 20.** Let $0 < ε, η < 1$ and let $δ ∈ \mathbb{R}$ such that $δ ≤ ηε$. Let $S$ be a strategy for $\text{TFKW}$. Let $E ⊆ \{0, \ldots, n\}$ be the set of rounds $i$ such that $w_{\text{TFKW}}^i(S) ≥ \cos^2 \frac{π}{8} − ε$, and let $W ∈ \{0, \ldots, n\}$ be the number of rounds the adversaries win. Then, if $|E| < (1 − η)n$,

$$Pr(W \geq (\cos^2 \frac{π}{8} − δ)n) ≤ e^{−2n(ηε − δ)^2}.$$  \hspace{1cm} (46)

We use this in contrapositive. That is, except with small probability, if the adversaries win at least $(\cos^2 \frac{π}{8} − δ)n$ games, then at least $(1 − η)n$ of them win near-optimally. This result is analogous to a similar result for sequentially repeated games in [31]; a proof is given in the full version.

In view of applications, we give in Theorem 21 a version of Corollary 19 where Alice has less information about the winning probabilities of the strategy. Rather than assuming that she knows that they win each round near-optimally, we assume that Alice only knows with high probability that each round wins near-optimally. Then, we ascertain the behaviour of the shared state in expectation. This will allow us to directly apply the result of Lemma 20 to get conclusions about the state.

**Theorem 21.** Let $n ∈ \mathbb{N}$ and let $S = (B, C, B, C, ρ)$ be a strategy for $\text{TFKW}$. Suppose that for some $ε, η ∈ [0, 1]$, for each $i ∈ [n]$, there is a probability $1 − η$ that the $i$-th game wins with probability $w_{\text{TFKW}}^i(S) ≥ \cos^2 \frac{π}{8} − ε$. Then, there exists a constant $K ≥ 0$, Hilbert spaces
and rigid quantum states. We write the \textit{ccq} state with the classical part duplicated as 
\[(V ⊗ W)ρ(V ⊗ W)^† + \text{Tr}_R(\langle φ | φ \rangle) \leq K\|H\|^3 \sqrt{ε} \leq Kn^3 \sqrt{ε}.\] (47)

Let \(σ = |β⟩⟨β|_{A_L} \otimes \text{Tr}_{A_L R}(|φ⟩⟨φ|).\) Then, \(σ\) has the form we want and \(\|\text{Tr}_R(|φ⟩⟨φ|) - σ\| \leq n - |H|,\) giving that \(E[\|\text{Tr}_R(|φ⟩⟨φ|) - σ\|] \leq n - \sum_i H_i = nη.\) The triangle inequality gives the result.

We give an example of the results of this section by considering an explicit choice of parameters.

\textbf{Example 22.} Fix some large \(n \in \mathbb{N}\). Take \(ε = n^{-8}, \eta = n^{-2},\) and \(δ = \frac{1}{n} n^{-10} .\) Suppose Alice plays \(N = n^{21}\) rounds of the TFKW game in parallel with Bob and Charlie, and that the players are able to win at least \(cos^2 \frac{π}{8} N - \frac{1}{n} n^{11}\) of them. Then Lemma 20 implies that, other than with probability \(e^{-c} n^{-\frac{8}{ε}}\), there are at least \((1 - n^{-2})N\) rounds that win with probability \(\omega_{TFKW}(S) \geq cos^2 \frac{π}{8} - n^{-8}\). Then Alice can check the rigidity on \(n\) rounds chosen uniformly at random: call this register \(A'.\) Due to the uniform randomness, each of the \(n\) has probability \(1 - n^{-2}\) of being within \(n^{-8}\) of optimal. Then, we can use the rigidity of Theorem 21 to say that there exists a constant \(K \geq 0,\) Hilbert spaces \(B'\) and \(C',\) and isometries \(V : B \to B'\) and \(W : C \to C'\) such that the expected value of the distance between quantum states \(E[\|V ⊗ W)\rho(V ⊗ W)^† - \text{Tr}_R(\langle φ | φ \rangle)\|] \leq \frac{K + 1}{n},\)

where \(|φ⟩ = \sum_{i \in \{0,1\}^n} X^{i_1} X^{i_2} |β⟩ \otimes \cdots \otimes X^{i_{n-1}} X^{i_n} |β⟩ \otimes |φ⟩\) for some auxiliary register \(R\) and \(|i⟩_{BCR} ∈ B' ⊗ C' ⊗ R\) with orthogonal supports on both \(B'\) and \(C'.\)

\section{Applications}

In this section, we present applications of our rigidity result. In Section 5.1, we introduce further definitions we will need. In Section 5.2, we construct a three-party weak string erasure scheme and in Section 5.3, we discuss its implications for bit commitment. In Section 5.4, we construct an everlasting randomness expansion protocol in a model closely following the model for MoE games.

\subsection{Preliminaries and Notation}

A \textit{classical-quantum state} (cq) is a state \(φ_{XH}\) that takes the form 
\[ρ_{XH} = \sum_{x ∈ X} p_x |x⟩⟨x|_X ⊗ ρ_{H}^x ∈ D(X ⊗ H),\] where \(p_x ≥ 0, \sum p_x = 1,\) and the \(ρ_{H}^x ∈ D(H)\) are quantum states. We write the cq state with the classical part duplicated as 
\[ρ_{XXH} ∈ D(X ⊗ X ⊗ H).\] If a quantum register decomposes as a product \(H = H_1 × \cdots × H_n,\) for any set \(i = \{i_1, \ldots, i_k\} ⊆ [n]\) with \(i_1 < \cdots < i_k\) and state \(ρ_H ∈ D(H),\) write 
\[ρ_{Hi_1,\ldots,i_k} = ρ_{Hi_1} ⊗ \cdots ⊗ ρ_{Hi_k} ∈ D(H_1 ⊗ \cdots ⊗ H_n).\] For a cq state \(ρ_{HI} ∈ D(I ⊗ H),\) write \(ρ_{IH_i} = \sum_{i \in I} p_i |i⟩⟨i|_I ⊗ ρ_{H_i} ∈ D(\bigoplus_{i ∈ I} |i⟩ ⊗ H_i) ⊆ D(I ⊗ H).\)
The conditional min-entropy is $H_{\text{min}}(H|K)_{\rho} = -\lg \inf \{ \Tr(\sigma K) | P(\rho) \leq I_H \otimes \sigma K, \sigma K \in P(K) \}$. If $\rho$ is classical on $H$, $2^{-H_{\text{min}}(H|K)_{\rho}}$ is the probability of guessing $H$ knowing $K$. For $\varepsilon > 0$, $H_{\text{min}}^\varepsilon(H|K)_{\rho} = \sup \{ H_{\text{min}}(H|K), \sigma \in P(H \otimes K), \| \rho - \sigma \|_\Tr \leq \Tr(\rho)\varepsilon, \Tr(\sigma) \leq \Tr(\rho) \}$, is the robust version of this entropy, called the smooth min-entropy. For more information, see [34].

Generally, the evolution of a quantum system is given by a quantum channel, which is represented by a completely positive trace-preserving (CPTP) map. The partial trace provides an example. Write the basis diagonalising Pauli $Y$ as $|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. Write $\neg 1(n)$ for the set of negligible functions in $n$, those $f$ such that $p(n)f(n) \to 0$ for all polynomials $p$; abusing notation, we also use $\neg 1(n)$ to represent an element of the set.

### 5.2 Weak String Erasure

Weak string erasure (WSE) is a fundamental cryptographic primitive, introduced in [19]. A WSE protocol provides a sender Alice with a random string $x \in \mathbb{Z}_2^n$ and a receiver Bob with a string $\hat{x} \in \mathbb{Z}_2^n$ and a subset $\epsilon \subseteq [n]$ such that $|\epsilon|$ is on average $n/2$, such that $x_i = \hat{x}_i$. Security for such a scheme consists of Alice not knowing $\epsilon$, while Bob does not know the substring $x_{\epsilon^c}$.

**Definition 23 ([19]).** A $(n, \lambda, \varepsilon)$-weak string erasure (WSE) scheme is a protocol between two parties, Alice and Bob, that creates a state $\rho_{XAI\hat{X}B}$, where $X, I, \hat{X}$ are classical registers such that $X = \mathbb{Z}_2^n$ holds string $x$, $\hat{X} = \mathbb{Z}_2^n$ holds Bob’s guess of $x$, and $I = P([n])$ holds $\epsilon$; and $A$ and $B$ are optional quantum registers corresponding to Alice and Bob’s remaining quantum states. The scheme must satisfy correctness, and security for both Alice and Bob:

- **Correctness:** If both Alice and Bob are honest then $\rho_{X\hat{X}I} = \rho_{X\hat{X}I}$ and $\rho_{XI} = \mu_X \otimes \mu_I$.
- **Security for Alice:** If Alice is honest $H_{\text{min}}^\varepsilon(X|B)_{\rho} \geq \lambda n$.
- **Security for Bob:** If Bob is honest, $\rho_{AI} = \rho_A \otimes \mu_I$ in the event that Alice does not abort.

We say that a protocol is a $(n, \lambda, \varepsilon)$-WSE scheme that fails with probability $p$ if any one of the three conditions does not hold with probability at most $p$. However, as it implies bit commitment, WSE is not information-theoretically possible in the plain model. We use a new model with an additional dishonest prover, Charlie, who colludes with the receiver, and with restrictions on the communication.

**Definition 24.** A WSE scheme in the three-party model consists of a sender, Alice, a receiver, Bob, and a prover, Charlie. It satisfies the following:

- Charlie is dishonest if and only if Bob is dishonest.
- Alice communicates by publicly broadcasting.
- Bob and Charlie are isolated from each other once Alice starts broadcasting.

In this model, the state takes the form $\rho_{XAI\hat{X}BC}$, where $C$ is the register held by Charlie. If he is dishonest, he should not be able to get more information than his collaborator, Bob. Thus, we require that security for Alice from Definition 23 is satisfied with respect to either Bob or Charlie.

---

1 In [42], the consider oblivious transfer in a three-party model with much stronger assumptions, where an untrusted third party prepares states for Alice and Bob, the third party produces each state identically and independently, Alice and Bob cooperate to verify the states before running the protocol, and the third party does not collude with them.
Definition 25. A \((n, \lambda, \varepsilon)\)-WSE scheme in the three-party model is a protocol that produces a shared state \(\rho_{XAI}^{\hat{X}BC}\) such that

- **Two-party WSE:** \(\rho_{XAI}^{\hat{X}B}\), the state with Charlie’s register traced out, satisfies Definition 23.

- **Symmetric security for Alice:** If Alice is honest \(H_{\min}(X|C) \geq \lambda n\).

For our protocol, an honest sender exploits the rigidity of the TFKW game to achieve security. Note that Charlie must remain isolated from Bob for it to stay secure. Bob’s security is because Alice must broadcast, so Bob and Charlie receive the same TFKW game questions even if she is dishonest.

Protocol 26 (three-party weak string erasure).

1. Bob prepares the shared state \(\mathcal{N}^{\otimes N} |x\varphi\rangle_A \otimes |x\varphi\rangle_B \otimes |x\varphi\rangle_C\) for \(x, \varphi \in \mathbb{Z}_2^N\) chosen uniformly at random. Bob and Charlie are then no longer allowed to communicate.
2. Alice chooses a set of \(n\) indices \(J \subseteq [N]\) and a string \(\theta \in \mathbb{Z}_2^N\) uniformly at random. She measures each of her qubits \(1 \leq i \leq N\) in basis \(\{|0_{\theta}^i\rangle, |1_{\theta}^i\rangle\}\) if \(i \notin J\) and in basis \(\{b|0_{\theta}^i\rangle, b|1_{\theta}^i\rangle\}\) if \(i \in J\). This produces a string \(y \in \mathbb{Z}_2^N\) that she keeps; and she broadcasts \(J\) and \(\theta\).
3. Bob and Charlie, without communicating, each measure their subspaces to get strings corresponding to their optimal guess at the TFKW game on \(J^c\), \(y^B = y^C = x + 1^J \wedge \theta \wedge \varphi \in \mathbb{Z}_2^N\), and they then send \(y^B_J\) and \(y^C_J\), respectively, to Alice.
4. Alice checks if her string everywhere but the index set, \(y_J^c\), matches \(y^B_J\) and \(y^C_J\) simultaneously on at least \((\cos^2 \frac{\pi}{8} - \delta)N\) bits. If it does not, she aborts.
5. Alice takes as output \(y_J\), and Bob takes as output the set \(\iota(\theta, \varphi) \subseteq J\) where the bits of \(\theta\) and \(\varphi\) match, and the string \(y^B_J\).

In Figure 3, we give a setup for our WSE scheme, where we see that the single round of communication makes it possible to devise a way to run the protocol relativistically. Also, it requires no quantum storage to run honestly. Alice samples \(\theta\) and \(J\) before Bob prepares the state, measures her register as she is receiving it, and only after reveal \(\theta\) and \(J\). Since her measurements are local, this has the same effect as if she waited until Bob and Charlie finish communicating to measure.

It is a direct computation to see that the scheme is correct. A proof is given in the full version.
Theorem 27. Let $K$ be the constant from Theorem 21. For $N, n \in \mathbb{N}$ and $\varepsilon, \eta, \delta \in (0, 1)$ with $\varepsilon > \delta$, Protocol 26 is a $(n, \lg(\frac{1}{n}), K n^3 \sqrt{\varepsilon} + n \eta)$-WSE scheme failing with probability $e^{-2N(\varepsilon - \delta)^2}$.

Proof. First, we show security for Bob. Bob, as he is honest, prepares the shared state $\rho_{ABC} = \mathbb{E}_{x, \varphi} G^{\otimes N} |x, \varphi\rangle_{A} G^{\otimes N} \otimes |x, \varphi\rangle_{B} \otimes |x, \varphi\rangle_{C}$. Alice must send some $J$ and $\theta$ to Bob and Charlie and get $y, \theta, J$ by a channel $\Phi : \mathcal{L}(A) \to \mathcal{L}(Y \otimes A')$, $\rho_{Y'ABC} = \mathbb{E}_{x, \varphi} \sum_{y, \theta, J} |y\theta J\rangle_{Y} \langle y\theta J|_{Y} \otimes |y\theta J\rangle_{Y} \Phi(G^{\otimes N} |x, \varphi\rangle_{A} G^{\otimes N} |y\theta J\rangle_{Y} \otimes |x, \varphi\rangle_{B} \otimes |x, \varphi\rangle_{C}$. Bob provides Alice with $y^B_j = x_j + \theta_j$, $\land \varphi_j$, and Charlie with the same. Bob produces $\iota(\theta, \varphi)$ so the state is $\rho_{Y' A' YX} = \mathbb{E}_{x, \varphi} \sum_{y, \theta, J} |y\theta J\rangle_{Y} \langle y\theta J|_{Y} \otimes |y\theta J\rangle_{Y} \Phi(G^{\otimes N} |x, \varphi\rangle_{A} G^{\otimes N} |y\theta J\rangle_{Y} \otimes |\iota(\theta, \varphi)\rangle_{I} \otimes |x_j\rangle_{X} \otimes \rho_{C}^{|x_j, \varphi_j\rangle}$.

If Alice does not abort, for her to guess $\iota$, she needs to guess $\varphi_j$. Since she has no information on $x_j$, she does no better than uniformly random:

$$\rho_{Y' A'} = \mathbb{E}_{x, \varphi} \sum_{y, \theta, J} |y\theta J\rangle_{Y} \langle y\theta J|_{Y} \otimes |y\theta J\rangle_{Y} \Phi(G^{\otimes N} |x, \varphi\rangle_{A} G^{\otimes N} |y\theta J\rangle_{Y} \otimes |\iota(\theta, \varphi)\rangle_{I} = \rho_{Y' A'} \otimes \mu_I,$$

which implies that any action Alice does locally gives rise to an uncorrelated final state $\rho_{A'I} = \rho_A \otimes \mu_I$.

Now, we study security for Alice. We show that $H_{K \sqrt{\varepsilon} + n \eta}(X|B)_\rho \geq -\ln(\frac{3}{4}) n$. Bob may produce any shared state $\rho_{ABC}$. The next three steps consist of playing $N - n$ TFKW games in parallel and verifying the rigidity condition. Therefore, if Alice does not abort, then by Lemma 20 and Theorem 21 there exists $K \geq 0$, isometries $V : B \to B'$ and $W : C \to C'$, an auxiliary register $R$, and a state $|\phi\rangle = \sum_{x, \varphi} G^{\otimes n} |x, \varphi\rangle_{BCR}$ where the $|x, \varphi\rangle_{BCR} \in B' \otimes C' \otimes \mathbb{R}$ have orthogonal support on $B'$ and $C'$ such that $\mathbb{E}_{x, \varphi} \| |(V \otimes W)\rho_{ABC}(V \otimes W)^\dagger - \text{Tr}_R(|\phi\rangle\langle\phi|)\|_{\text{Tr}} \leq K n^3 \sqrt{\varepsilon} + n \eta$, with probability $1 - e^{-2N(\varepsilon - \delta)^2}$. Let $\sigma_{A'BC} = \text{Tr}_R(|\phi\rangle\langle\phi|)$ and we study first what happens if the shared state is $\sigma$. Since Bob and Charlie may not communicate, we trace out Charlie’s state. By the orthogonality from the rigidity theorem, $\sigma_{A'\Theta B} = \mathbb{E}_{x, \varphi} \sum_{x, \varphi} G^{\otimes n} |x, \varphi\rangle_{X} \otimes |\theta\rangle_{\Theta} \otimes \text{Tr}_{CR}(|x, \varphi\rangle_{X} |x, \varphi\rangle_{B})$. Alice’s measurement gives her $X$ and makes the state

$$\sigma_{X \Theta B} = \mathbb{E}_{x, \varphi} \sum_{y, \theta} |y\rangle \langle y| \otimes |\theta\rangle_{\Theta} \otimes \text{Tr}_{CR}(|x, \varphi\rangle_{X} |x, \varphi\rangle_{B}).$$

Noting that Bob’s register is uncorrelated with part of Alice’s register $X_{(\theta, \varphi)_R}$, that gives that Bob’s probability of guessing any bit in that register is $\frac{1}{2}$. So, Bob’s probability of guessing $X$ is $\left(\frac{1}{2}\right)^n$, giving min-entropy $H_{\min}(X|B)_\sigma \geq -\lg(\frac{3}{4}) n$, where $B$ is Bob’s register including $\Theta$. Now we relate this to the smooth min-entropy of $\rho$. Since $V \otimes W$ is an isometry, $H_{\min}(X|B)_\rho = H_{\min}(X|B)_{\rho(V \otimes W)^\dagger} \geq H_{\min}(X|B)_\sigma \geq -\lg(\frac{3}{4}) n$. Note that this holds in the same way for Charlie, so he cannot extract any more information that Bob can if he is dishonest.
5.3 Bit Commitment from WSE

Bit commitment (BC) is a cryptographic primitive where a sender, Alice, sends an encoded bit (or more generally a bit string) to a receiver, Bob, and may choose to reveal it at a later time. Accordingly, a scheme for BC consists of a commit protocol and a reveal protocol. The scheme should be hiding – Bob is unable to learn the bit until Alice chooses to reveal it – and binding – Alice must reveal the same bit that she originally chose. We define such a scheme in essentially the same way as in [19].

Definition 28. A \((\ell, \epsilon)\)-randomised bit string commitment (RBC) scheme is a pair of protocols between two parties Alice and Bob: a protocol commit that creates a state \(\rho_{YAB}\) and a protocol reveal that creates from this a state \(\rho_{YA\hat{Y}FB}\). Here, \(Y = \mathbb{Z}_2^\ell\) holds Alice’s committed string; \(\hat{Y} = \mathbb{Z}_2^\ell\) holds the string Alice reveals; \(F = \mathbb{Z}_2\) indicates whether Bob accepts (1) or rejects (0) the reveal; and \(A, A', B, B'\) are additional quantum registers for Alice and Bob, respectively. The scheme must be correct, \(\epsilon\)-hiding, and \(\epsilon\)-binding:

- **Correctness:** If Alice and Bob are honest, for \(\sigma_Y = \mu_Y \otimes |1\rangle\langle 1|\), \(\|\rho_{Y\hat{Y}F} - \sigma_{Y\hat{Y}F}\|_{\text{Tr}} \leq \epsilon\).
- **\(\epsilon\)-hiding:** If Alice is honest, \(\|\rho_{YB} - \mu_Y \otimes \rho_B\| \leq \epsilon\).
- **\(\epsilon\)-binding:** If Bob is honest, there exists a state \(\sigma_{YAB}\) where \(\|\rho_{YAB} - \sigma_{YAB}\|_{\text{Tr}} \leq \epsilon\) such that, applying reveal to it to get \(\sigma_{YA\hat{Y}FB}\), \(Pr[Y \neq \hat{Y} \land F = 1] \leq \epsilon\).

We say this scheme fails with probability \(p\) if any one of these conditions does not hold with probability at most \(p\). In [19], they provide a construction of a \((\lambda n - (n - k) - d, 2\epsilon + 2^{-d/2})\)-RBC scheme using an \((n, \lambda, \epsilon)\)-WSE scheme and an \((n, k, d)\)-linear code. Our WSE scheme Protocol 26 gives RBC in a two-receiver model where Alice is a sender who broadcasts, and Bob and Charlie are isolated colluding receivers. As for WSE, we only require that Bob be able to read the revealed string.

Corollary 29. Let \(K, N, n, \epsilon, \eta, \delta\) be constants that satisfy Theorem 27, and fix an \((n, k, d)\)-linear code. Then, for \(\ell = (\log \frac{2}{3})n - (n - k) - d\) and \(\omega = 2Kn^3\sqrt{\epsilon} + 2\eta + 2^{-d/2}\), in the two-receiver model, there exists a \((\ell, \omega)\)-RBC scheme that fails with probability \(e^{-2N(\omega - \delta)^2}\).

5.4 Everlasting Randomness Expansion

The creation of fresh randomness is important for many computational and cryptographic tasks; quantum procedures should be useful for this, as they are probabilistic. A major theoretical hurdle is the difficulty of characterising the behaviour of an untrusted quantum device. Major methods to achieve this require durable entanglement, which can be an impractical requirement. In our contribution, we instead make the assumption of a trusted measurement and a standard computational assumption. First, we formalise this model, based on the structure of an MoE game.

Definition 30. The MoE model for randomness expansion consists of three quantum parties: a trusted verifier Alice, who interacts with two untrusted provers, Bob and Charlie. The model satisfies
Bob and Charlie are able to prepare a tripartite shared state but then are isolated.

- Alice can make trusted measurements on her register, which are leaky in the sense that Bob and Charlie can learn the measurement bases.

**Definition 31.** A \((s(n), \varepsilon)\)-local randomness expander is a protocol in the MoE model, where, given a uniformly random seed in \(S = \mathbb{Z}_2^{s(n)}\), Alice, Bob, and Charlie construct a quantum state \(\rho_{YSB}\), where \(Y = \mathbb{Z}_2^n\) and \(S\) are classical registers that Alice holds and \(B\) and \(C\) are potentially quantum registers that Bob and Charlie hold, respectively, such that

\[
\|\rho_{YSB} - \mu_Y \otimes \mu_S \otimes \rho_B\|_{Tr} \leq \varepsilon \quad \|\rho_{YSB} - \mu_Y \otimes \mu_S \otimes \rho_C\|_{Tr} \leq \varepsilon,
\]

if Alice does not abort during the execution. As before, we say this scheme fails with probability \(p\) if these conditions do not hold with probability at most \(p\).

In this definition, Alice’s output is always approximately uniformly random, and we get the additional guarantee that Bob and Charlie cannot guess the output using their side information if they remain isolated. However, we do not constrain their ability to guess the output if they interact. The main computational tool we will be making use of is the idea of a pseudorandom generator.

**Definition 32.** An algorithm \(Q : \mathbb{Z}_2^s \rightarrow \mathbb{Z}_2^s\) is quantum polynomial time (QPT) if there exists a Turing machine \(T\) such that, for each \(n \in \mathbb{N}\), \(T(n)\) outputs in polynomial time the description of a quantum circuit that, on input \(x \in \mathbb{Z}_2^n\), outputs \(Q(x)\).

**Definition 33.** A family of functions \(G_n : \mathbb{Z}_2^{s(n)} \rightarrow \mathbb{Z}_2^n\) is a pseudorandom generator (PRG) if, for uniform random variables \(\Gamma\) in \(\mathbb{Z}_2^{s(n)}\) and \(\Delta\) in \(\mathbb{Z}_2^n\), and for every QPT algorithm \(Q : \mathbb{Z}_2^s \rightarrow \mathbb{Z}_2\), \(|\Pr[Q(G_n(\Gamma)) = 1] - \Pr[Q(\Delta) = 1]| \leq \text{negl}(n)\). The input is the seed and \(s(n)\) is the seed length.

Because of brute force attacks against \(G_n\), \(s(n) \in O(\log n)\) is a strict lower bound on the seed length. Thus, we cannot hope for exponential randomness expansion with this method, but we can nevertheless expect large polynomial or even superpolynomial expansion. Against computational adversaries, rigidity extends to the TFKW game with pseudorandom questions. This is discussed in detail in the full version. Keeping this in mind, we present the randomness expansion protocol.

**Protocol 34 (randomness expansion).**

1. Alice samples \((t, u) \in \mathbb{Z}_2^{s(N) + \beta}([\log(n)])\) uniformly at random. She computes \(\theta = G_N(t)\) and \(J = G_{[\log(n)]}(u)\), where she interprets \(J\) as a subset of \([N]\) of cardinality \(n\).
2. Bob and Charlie prepare a shared state \(\rho_{ABC}\) and then are isolated.
3. Alice measures each of her qubits \(i \in [N]\) in basis \(\{|0^\theta_i\}, |1^\theta_i\}\) if \(i \notin J\) and in basis \(\{0_\theta, 1_\theta\}\) if \(i \in J\). This produces a string \(y \in \mathbb{Z}_2^N\) that she keeps.
4. Alice sends Bob and Charlie the key \(\theta\) and \(J\). Bob and Charlie each reply with a guess of \(y\), \(y^B\) and \(y^C\) respectively.
5. Alice verifies that they win the TFKW game \(y_i = y^B_i = y^C_i\) for at least \((\cos^2(\frac{\pi}{8}) - \delta)N\) of the \(i \in [N] \setminus J\), and then, if she accepts, takes \(y_J\) to be her output.

The protocol is similar to Protocol 26 since it also makes use of rigidity; the main differences are that Alice samples questions and test qubits pseudorandomly and always measures in the same basis, mutually unbiased with all of the Breidbart states to give a
uniformly random result. Also, Alice shares θ and J immediately after measuring, so they have full information about her measurement bases, so the measurement can be seen as leaky. Bob and Charlie may provide randomness without entanglement by preparing the Breidbart state |β⟩⊗N and guessing 0 on all the TFKW game rounds.

Theorem 35. Let K be the constant from Theorem 21, ε, η, δ ∈ (0, 1) such that ηε > δ, and N ∈ poly(n). Assuming the existence of a pseudorandom generator, $G_n : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{2n}$, Protocol 34 is a (s(N) + s(lg(N))) ; 2Kn^3\sqrt{\varepsilon} + 2n\eta + negl(n))-local randomness expander in the MoE model with QPT provers, that fails with probability $e^{-2N(\eta\varepsilon-\delta)^2} + negl(n)$.

Proof. Write $b = \lfloor \log(N_n) \rfloor$. Let $U, V, W$ be random variables, where $U$ is the number of rounds Bob and Charlie win, $V$ is the number of rounds they would have won if Alice chose $J$ uniformly random (among the subsets of $[N]$ with cardinality $n$), and $W$ is the number of rounds they would have won if Alice chose both $J$ and $\theta$ uniformly random. Take $Q(\theta, J)$ to be the QPT algorithm computed by steps 2-5 of Protocol 34, outputting 1 if Alice accepts the verification of the TFKW games and else 0. Then, taking $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ to be uniform random variables in $\mathbb{Z}_2^n$, $\mathbb{Z}_2^2$, and $\mathbb{Z}_2^2$, we know that $Pr[Q(\Gamma_1, \Gamma_2) = 1] = Pr[U \geq (\cos^2(\varepsilon_\theta) - \delta)|N]$, $Pr[Q(\Gamma_1, \Delta_1) = 1] = Pr[V \geq (\cos^2(\varepsilon_J) - \delta)|N]$, and $Pr[Q(\Delta_1, \Delta_2) = 1] = Pr[W \geq (\cos^2(\varepsilon_J) - \delta)|N]$. Giving $Pr[U \geq (\cos^2(\varepsilon_\theta) - \delta)|N] - Pr[V \geq (\cos^2(\varepsilon_J) - \delta)|N] \leq |Pr[U \geq (\cos^2(\varepsilon_\theta) - \delta)|N] - Pr[V \geq (\cos^2(\varepsilon_J) - \delta)|N]| \leq negl(n)$, as $N \in poly(n)$ and $b \in O(n\log(n))$. Now, using Lemma 20 as in Theorem 27, if less than $(1 - \eta)N$ of the rounds have winning probability greater than $\cos^2(\varepsilon_\theta) - \varepsilon$, then $Pr[W \geq (\cos^2(\varepsilon_J) - \delta)] \leq e^{-2N(\eta\varepsilon-\delta)^2}$. By the above, $Pr[U \geq (\cos^2(\varepsilon_\theta) - \delta)] \leq e^{-2N(\eta\varepsilon-\delta)^2} + negl(n)$. If we select $n$ rounds uniformly random, each of the rounds has probability 1 - η of winning with probability greater than $\cos^2(\varepsilon_\theta) - \varepsilon$. We claim that Bob and Charlie have a negligible probability of distinguishing the real case and the uniform case.

Let $E \subseteq [N]$ be the set of rounds that win with probability greater than $\cos^2(\varepsilon_\theta) - \varepsilon$, and write $J = \{j_1(J), \ldots, j_n(J)\}$, where $j_i(J) < \ldots < j_n(J)$. Then, for each $i \in [n]$, using their strategy to play TFKW a polynomial number of times, there is a QPT algorithm that, on input $J$, outputs whether $j_i(J) \in E$ correctly with probability $1 - negl(n)$. Using pseudorandomness, we know $Pr[j_i(G_1(G_2)] \in E) - Pr[j_i(G_2) \in E)] \in negl(n)$. As $Pr[j_i(\Delta_2)] \in E \geq 1 - \eta$, each of the rounds chosen pseudorandomly has probability at least 1 - $\eta - negl(n)$ of having winning probability greater than $\cos^2(\varepsilon_\theta) - \varepsilon$. So, by Theorem 21 there exists a constant $K \geq 0$, isometries $V : \mathbb{B} \rightarrow \mathbb{B}'$ and $W : \mathbb{C} \rightarrow \mathbb{C}'$, an auxiliary register $R$, and a state $|\phi\rangle = \sum_{x, \varphi \in \mathbb{Z}_2^2} \beta^{\alpha}(x, \varphi) \otimes |x, \varphi_B, \varphi_C \rangle$ where the $|x, \varphi_B, \varphi_C \rangle \in \mathbb{B}' \otimes \mathbb{C}' \otimes \mathbb{R}$ have orthogonal support on both $\mathbb{B}'$ and $\mathbb{C}'$ such that $\mathbb{E}_{J \leftarrow G_1(G_2)} \left\| (V \otimes W)\rho_{A, BC} (V \otimes W)^\dagger - Tr_R(|\phi\rangle \langle \phi|) \right\|_{TV} \leq Kn^3\sqrt{\varepsilon} + n\eta + negl(n).$ (51)

Let $\sigma_{YB} = Tr_Y(|\phi\rangle \langle \phi|)$. If Alice measures her register in the basis $\{ |y\rangle \}_y \in \mathbb{Z}_2^n$, she gets $\sigma_{YB} = \sum_{y,x,\varphi \in \mathbb{Z}_2^2} \langle y_x|G \otimes T|y_x\rangle \otimes Tr_C(|x, \varphi \rangle \langle x, \varphi|) = \sum_{y,x,\varphi \in \mathbb{Z}_2^2} \frac{1}{\sqrt{n}} |y\rangle\langle y| \otimes Tr_C(|x, \varphi \rangle \langle x, \varphi|)$. So, following the protocol, Alice measures $\alpha_j$ of $\rho$ in this basis, giving $\mathbb{E}_{J \leftarrow G_1(G_2)} \left\| V \rho V^\dagger - \mu_Y \sigma_{YB} \right\|_{TV} \leq Kn^3\sqrt{\varepsilon} + n\eta + negl(n)$. Acting with the trace non-increasing channel $\rho \rightarrow V^\dagger \rho V$, $\mathbb{E}_{J \leftarrow G_1(G_2)} \left\| V \rho V^\dagger - \mu_Y \sigma_{YB} \right\|_{TV} \leq Kn^3\sqrt{\varepsilon} + n\eta + negl(n)$, where in particular, $\mathbb{E}_{J \leftarrow G_1(G_2)} \left\| \rho_B - V^\dagger \sigma_{B} V \right\|_{TV} \leq Kn^3\sqrt{\varepsilon} + n\eta + negl(n)$, so, using the triangle inequality, $\mathbb{E}_{J \leftarrow G_1(G_2)} \left\| \rho_B - \mu_Y \rho_B \right\|_{TV} \leq 2Kn^3\sqrt{\varepsilon} + 2n\eta + negl(n)$. Let $S$ be a classical register holding the seed, and let $I = G_b(S)$ be the register that holds $J$. Then,
\[ \| \rho_{YSB} - \mu_Y \otimes \mu_S \otimes \rho_B \|_{\text{Tr}} \leq \| \mathbb{E}_{t \in \mathbb{Z}_2} |t\rangle\langle t|_S \otimes |G_b(t)\rangle\langle G_b(t)|_Y \otimes \left( \rho_{G_b(t)B} - \mu_Y \otimes \rho_B \right) \|_{\text{Tr}} \]
\[ = \mathbb{E}_{t \in \mathbb{Z}_2} \| \rho_{G_b(t)B} - \mu_Y \otimes \rho_B \|_{\text{Tr}} \leq 2Kn^3 \sqrt{\epsilon} + 2n\eta + \text{negl}(n) \] (52)

The same proof holds for \( \rho_{YS} \).

References

1. Antonio Acín and Lluís Masanes. Certified randomness in quantum physics. *Nature*, 540:213–219, December 2016. doi:10.1038/nature20119.
2. Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Physical Review A*, 91(5), 2015. doi:10.1103/physreva.91.052111.
3. Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Widgerson. Multi-prover interactive proofs: how to remove intractability assumptions. In *20th Annual ACM Symposium on Theory of Computing—STOC 1988*, pages 113–131, 1988. doi:10.1145/62212.62223.
4. Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In *59th Annual Symposium on Foundations of Computer Science—FOCS 2018*, pages 320–331, 2018. doi:10.1109/FOCS.2018.00038.
5. Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, January 2012. doi:10.1103/PhysRevA.85.010301.
6. Anne Broadbent and Sébastien Lord. Uncloneable quantum encryption via oracles. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography—TQC 2020*, pages 4:1–4:22, 2020. doi:10.4230/LIPIcs.TQC.2020.4.
7. Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1):351–382, 2016. doi:10.1007/s10623-015-0157-4.
8. John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969. doi:10.1103/PhysRevLett.23.880.
9. Andrea Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Information & Computation*, 17(9-10):831–865, 2017. doi:10.5555/3179561.3179567.
10. Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to uncloneable cryptography. In *Advances in Cryptology—CRYPTO 2021*, pages 556–584, 2021. doi:10.1007/978-3-030-84242-0_20.
11. Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, UK, 2006. arXiv:0911.3814.
12. Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *46th Annual ACM Symposium on Theory of Computing—STOC 2014*, pages 427–436, 2014. doi:10.1145/2591796.2591873.
13. Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. In *Advances in Cryptology—ASIACRYPT 2011*, pages 407–430, 2011. doi:10.1007/978-3-642-25385-0_22.
14. David Cui, Arthur Mehta, Hammoon Mousavi, and Seyed Sajjad Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. *Quantum*, 4:346, 2020. doi:10.22331/q-2020-10-21-346.
Rigidity for MoE Games

15 Eric Culf and Thomas Vidick. A monogamy-of-entanglement game for subspace coset states. Quantum, 6:791, September 2022. doi:10.22331/q-2022-09-01-791.

16 W T Gowers and O Hatami. Inverse and stability theorems for approximate representations of finite groups. Sbornik: Mathematics, 208(12):1784–1817, 2017. doi:10.1070/sm8872.

17 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. Communications of the ACM, 64(11):131–138, 2021. doi:10.1145/3485628.

18 Nathaniel Johnston, Rajat Mittal, Vincent Russo, and John Watrous. Extended non-local games and monogamy-of-entanglement games. Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 472(2189):20160003, 2016. doi:10.1098/rspa.2016.0003.

19 Robert König, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. IEEE Transactions on Information Theory, 58(3):1962–1984, 2012. doi:10.1109/TIT.2011.2177772.

20 Hong-Wei Li, Zhen-Qiang Yin, Yu-Chun Wu, Xu-Bo Zou, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Semi-device-independent random-number expansion without entanglement. Phys. Rev. A, 84:034301, September 2011. doi:10.1103/PhysRevA.84.034301.

21 Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? Physical Review Letters, 78(17):3410–3413, 1997. doi:10.1103/PhysRevLett.78.3410.

22 Laura Mančinska, Thor Gabelgaard Nielsen, and Jitendra Prakash. Glued magic games self-test maximally entangled states, 2021. Available at https://arxiv.org/abs/2105.10658. arXiv:2105.10658.

23 Dominic Mayers. The trouble with quantum bit commitment, 1996. arXiv:9603015.

24 Dominic Mayers and Andrew Yao. Self testing quantum apparatus. Quantum Information & Computation, 4(4):273–286, 2004. URL: http://dl.acm.org/citation.cfm?id=2011827.2011830.

25 M. McKague, T. H. Yang, and V. Scarani. Robust self-testing of the singlet. Journal of Physics A, 45(45):455304, 2012. doi:10.1088/1751-8113/45/45/455304.

26 Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In 49th Annual ACM Symposium on Theory of Computing—STOC 2017, pages 1003–1015, 2017. doi:10.1145/3055399.3055468.

27 Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New Journal of Physics, 10(7):073013, 2008. doi:10.1088/1367-2630/10/7/073013.

28 Michael A. Nielsen and Issac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000.

29 Narutaka Ozawa. About the Connes Embedding Conjecture—Algebraic approaches—, 2013. Available at https://arxiv.org/abs/1212.1700. arXiv:1212.1700.

30 Marcin Pawłowski and Nicolas Brunner. Semi-device-independent security of one-way quantum key distribution. Physical Review A, 84:010302, July 2011. doi:10.1103/PhysRevA.84.010302.

31 Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. Nature, 496:456–460, 2013. doi:10.1038/nature12035.

32 Jean-Pierre. Serre. Linear representations of finite groups. Graduate texts in mathematics ; 042. Springer-Verlag, New York, 1977.

33 Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. The case for quantum key distribution. In Quantum Communication and Quantum Networking, volume 36, pages 283–296, 2010. doi:10.1007/978-3-642-11731-2_35.

34 Marco. Tomamichel. Quantum Information Processing with Finite Resources Mathematical Foundations. SpringerBriefs in Mathematical Physics, 5. Springer International Publishing, Cham, 2016.

35 Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. New Journal of Physics, 15(10):103002, 2013. doi:10.1088/1367-2630/15/10/103002.
B. S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8:329–345, 1993.

Dominique Unruh. Everlasting multi-party computation. In *Advances in Cryptology—CRYPTO 2013*, pages 380–397, 2013. doi:10.1007/978-3-642-40084-1_22.

Umesh V. Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *44th Annual ACM Symposium on Theory of Computing—STOC 2012*, pages 61–76, 2012. doi:10.1145/2213977.2213984.

Thomas Vidick. Expository note based on [NV17]. 2018. URL: http://users.cms.caltech.edu/~vidick/notes/pauli_braiding_1.pdf.

John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 1st edition, 2018.

Steven H. Weintraub. *Representation theory of finite groups: algebra and arithmetic*. Graduate studies in mathematics, v. 59. American Mathematical Society, Providence, R.I, 2003.

Yu-Guang Yang, Peng Xu, Ju Tian, and Hua Zhang. Quantum oblivious transfer with an untrusted third party. *Optik*, 125(18):5409–5413, 2014. doi:10.1016/j.ijleo.2014.06.023.