

Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices

Carl A. Miller and Yaoyun Shi

Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48109, USA
carlmi, shiyy@umich.edu

August 1, 2016

Abstract

Randomness is a vital resource for modern day information processing, especially for cryptography. A wide range of applications critically rely on abundant, high quality random numbers generated securely. Here we show how to expand a random seed at an exponential rate without trusting the underlying quantum devices. Our approach is secure against the most general adversaries, and has the following new features: cryptographic level of security, tolerating a constant level of imprecision in the devices, requiring only a unit size quantum memory per device component for the honest implementation, and allowing a large natural class of constructions for the protocol. In conjunct with a recent work by Chung, Shi and Wu, it also leads to robust unbounded expansion using just 2 multi-part devices. When adapted for distributing cryptographic keys, our method achieves, for the first time, exponential expansion combined with cryptographic security and noise tolerance. The proof proceeds by showing that the Rényi divergence of the outputs of the protocol (for a specific bounding operator) decreases linearly as the protocol iterates. At the heart of the proof are a new uncertainty principle on quantum measurements, and a method for simulating trusted measurements with untrusted devices.

Contents

1	Background and Summary of Results	3
1.1	The Problem and Its Motivations	3
1.2	Related Problems	5
1.3	Overview of Our Results	5
1.4	Related Works	6
1.5	Technical Statements	7
1.6	Numerical Results	11
2	Overview of Proofs	12
2.1	Quantum Rényi Entropies	12
2.2	Partially Trusted Measurement Simulation	13
2.3	An Induction Proof With a Weighted Measure of Randomness	13
2.4	Quantum Key Distribution	14
3	Preliminaries	14
3.1	Notation	14
3.2	Quantum Rényi Divergence	15
3.3	Quantum Devices	17
4	An Uncertainty Principle	19
5	The Self-Testing Property of Binary Nonlocal XOR Games	20
5.1	Definitions and Basic Results	21
5.2	Decomposition Theorems	24
6	Randomness Expansion with Partially Trusted Measurements	28
6.1	Devices with Trusted Measurements	29
6.2	Devices with Partially Trusted Measurements	29
6.3	Entanglement with a Partially Trusted Measurement Device	32
6.4	Simulation	32
7	The Proof of Security for Partially Trusted Devices	33
7.1	Proof Idea	35
7.2	One-Shot Results	36
7.3	Multi-Shot Results	38
7.4	The Security of Protocol A'	40
8	Randomness Expansion from an Untrusted Device	42
8.1	The Trust Coefficient of a Strong Self-Test	42
8.2	The Security of Protocol R	42
8.3	Example: The GHZ game	45
8.4	Completeness	46
9	Unbounded Expansion	48

10	Untrusted-device Quantum Key Distribution	50
10.1	Definitions	50
10.2	The Protocol R_{kd}	51
10.3	Error Rate	51
10.4	Efficient Information Reconciliation	55
10.5	The Security of Protocol R_{kd}	58
11	Further Directions	59
12	Acknowledgments	60
A	Supplementary Material	60
A.1	The Canonical Form for Two Binary Measurements	60
A.2	Smooth Min-entropy and Renyi Divergence	62
A.3	Variables and Functions Used in Section 7	63
A.4	Mathematical Results	65

1 Background and Summary of Results

1.1 The Problem and Its Motivations

Randomness is an indispensable resource for modern day information processing. Without randomness, there would be no fast randomized algorithms, accurate statistical scientific simulations, fair gaming, or secure cryptography. A wide range of applications rely on methods for generating randomness with high quality and in a large quantity. Consider, for example, all the computers and handheld devices that connect to the Internet using public key cryptography such as RSA and DSA for authentication and encryption, and that use secret key cryptography for secure connections. It is probably conservative to estimate that the number of random bits used each day for cryptography is in the order of trillions.

While randomness seems to be abundant in everyday life, its efficient and secure generation is a difficult problem. A typical random number generator such as the `/dev/random/` generator in Linux kernel, would start with random “seeds”, including the thermal noise of the hardware (e.g. from Intel’s Ivy Bridge processors), system boot time in nanoseconds, user inputs, etc., and apply a deterministic function to produce required random bits. Those methods suffer from at least three fundamental vulnerabilities.

The first is due to the fact that no deterministic procedure can increase randomness. Thus when there is not enough randomness to start with, the output randomness is not sufficient to guarantee security. In particular, if the internal state of the pseudorandom generator is correctly guessed or is exposed for other reasons, the output would become completely predictable to the adversary. The peril of the lack of entropy has been demonstrated repeatedly [Guterman et al., 2006, Ristenpart and Yilek, 2010, Lenstra et al., 2012]. [Heninger et al., 2012] were able to break the DSA secret keys of over 1% of the SSH hosts that they scanned on the Internet, by exploiting the insufficient randomness used to generate the keys.

The second vulnerability is that the security of current pseudorandom generators are not only based on unproven assumptions, such as the hardness of factoring the product of two large primes, but also assume that their adversaries have limited computational capability. Therefore, they will fail necessarily if the hardness assumptions turn out to be completely false, or the ad-

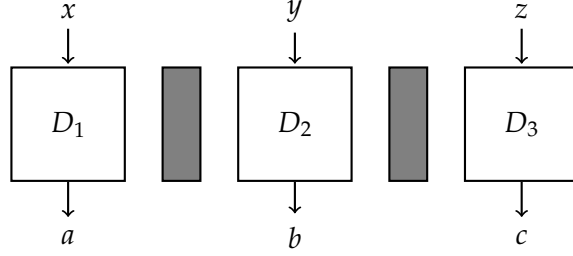


Figure 1: A three-part device playing the GHZ game. Each part D_1 , D_2 , and D_3 , receives a single bit and outputs a single bit. The input (x, y, z) is drawn uniformly from $\{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$. The device wins if $a \oplus b \oplus c = x \vee y \vee z$. No communication among the parts is allowed when the game starts. An optimal classical strategy is for each part to output 1, winning with $3/4$ probability. An optimal quantum strategy is for the three parts to share the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, and for each part to measure σ_x on input 0, and measure σ_y on input 1. This strategy wins with certainty.

versaries gain dramatic increase in computational power, such as through developing quantum computers.

Finally, all those methods rely on trusting the correctness and truthfulness of the generator. The dynamics of market economy leads to a small number of vendors supplying the hardware for random number generation. The demand for platform compatibility results in a small number of generating methods. Thus the risk of the generators containing exploitable vulnerabilities or secret backdoors is necessarily significant. Recent evidence suggest that this is in fact the reality [Perlroth et al., 2013]. Thus for users demanding the highest level of security with the minimum amount of trust, no current solution is satisfactory.

Quantum mechanics postulates true randomness, thus provides a promising approach for mitigating those drawbacks. Applying a sequence of quantum operations can increase entropy even when the operations are applied deterministically, as some quantum operations are inherently unpredictable. Indeed, commercial random number generators based on quantum technology have started to emerge (e.g. by ID Quantique SA). Furthermore, the randomness produced can be unconditionally secure, i.e. without assumptions on the computational power of the adversary.

However, as classical beings, users of quantum random number generators cannot be certain that the quantum device — the quantum state inside and the quantum operations applied — is running according to the specification. How can a classical user ensure that a possibly malicious quantum device is working properly?

Non-local games — games with multiple non-communicating players — provide such a possibility. Consider, for example, the celebrated GHZ game [Greenberger et al., 1989] illustrated in Fig. (1). It is now known ([McKague, 2014], see also [Miller and Shi, 2013]) that any quantum strategy achieving close to the optimal quantum winning probability must be very close to the optimal strategy itself. Consequently, the output of each component is near perfectly random. Intuitively, one needs only to run the game multiple times (using some initial randomness to choose the input string for each round) and if the observed winning average is close to the optimal quantum winning probability, then the output should be sufficiently random. Therefore, the trust on the quantum device can now be replaced by the condition of non-communication between the different components. This condition can be verified through classical means, e.g., by separating the components at a distance so that they do not have time to communicate.

[Colbeck, 2006, Colbeck and Kent, 2011] proposed using nonlocal games as the basis for untrusted-device randomness expansion. Turning the intuition above into rigorous proofs turns out to be rather challenging. Classical security was proved in [Pironio et al., 2010], [Fehr et al., 2013], [Pironio and Massar, 2013], and in the later work [Coudron et al., 2013], which allowed a very broad class of nonlocal games. While useful, classical security does not guard against quantum adversaries, thus is inadequate as quantum computation is becoming a reality. Furthermore, an expansion protocol without quantum security cannot be safely composed with other quantum protocols. [Vazirani and Vidick, 2012] were the first to prove quantum security, using a protocol that expands the initial seed exponentially.

1.2 Related Problems

The randomness expansion problem is closely related to the problem of quantum key distribution (QKD), where two parties at a distance wish to establish a common (random) secret using a public quantum channel. Key distribution is a fundamental cryptographic primitive, and also one of the oldest problems in quantum information [Bennett and Brassard, 1984, Ekert, 1991, Mayers, 2001, Lo and Chau, 1999, Biham et al., 2006, Shor and Preskill, 2000].

Also, untrusted-device randomness expansion is part of the broader area of untrusted-device, or “device-independent,” quantum cryptography. This area of quantum cryptography was pioneered by [Mayers and Yao, 1998]. It was also developed in parallel by other researchers, such as [Barrett et al., 2005], from the perspective of non-locality with inspirations from [Ekert, 1991]. It has now become an important and intensively studied paradigm for understanding the power and limitations of quantum cryptography.

An important related problem in untrusted-device cryptography is *randomness amplification* [Colbeck and Renner, 2012], where one wants to obtain near-perfect randomness from a *weak* random source using untrusted quantum devices (and without any additional randomness). The paper [Chung et al., 2014], which is a companion paper to the present one (with a common author) studies the amplification problem.

1.3 Overview of Our Results

In this work, we analyze a simple exponentially expanding untrusted-device randomness expansion protocol (referred to as the *one-shot protocol*). We give a proof of security against the most general quantum adversaries. More importantly, we accomplish all of the following additional features, none of which has been accomplished by previous works.

The first is *cryptographic security* in the output.¹ The error parameters are not only exponentially small in the input length, but are also negligible (i.e. smaller than any inverse polynomial function) in the running time of the protocol (which is asymptotically the number of uses of the device.) This is the conventional theoretical requirement for cryptographic level of security — the chance that an adversary can distinguish the protocol output from an ideal uniform distribution is negligible, as measured against the amount of resource used for running the protocol.

Secondly, the protocol is *robust*, i.e. tolerating a constant level of “noise”, or implementation imprecision. Thus any honest implementation that performs below the optimal level by a small constant amount will still pass our test with overwhelming probability. For example, we show that any device which wins the GHZ game with probability at least 0.985 will achieve exponential randomness expansion with probability approaching 1.

¹We thank Kai-Min Chung and Xiaodi Wu for pointing out this feature of our result.

Third, our protocol requires only a *constant size quantum memory* for an honest implementation. In between two rounds of interactions, the different components of the device are allowed to interact arbitrarily. Thus an honest device could establish its entanglement on the fly, and needs only to maintain the entanglement (with a constant level of fidelity) for the duration of a single game. Given the challenge of maintaining coherent quantum states, this feature greatly reduces implementation complexity.²

Fourth, relying on a powerful observation of Chung, Shi and Wu [Chung et al., 2014] — what they call the Equivalence Lemma — we show that one can sequentially compose instances of our one-shot protocol, alternating between two untrusted devices and achieve *unbounded* randomness expansion starting with a fixed length seed. The additively accumulating error parameters remain almost identical to the one-shot errors, since they decrease geometrically.

Finally, our protocol allows a large natural class of games to be used. The class consists of all binary XOR games — games whose inputs and outputs are binary and whose scoring function depends on the inputs and the XOR of the outputs — that are *strongly self-testing*. The latter property says that any quantum strategy that is ϵ -close to optimal in its winning probability must be $O(\sqrt{\epsilon})$ close to a unique optimal strategy in its both its state and its measurements. (We call this “strongly self-testing” because this error relationship is the best possible.) We explored this class previously in [Miller and Shi, 2013]. The class of strong self-tests includes the CHSH game and the GHZ game, two commonly used games in quantum information. Broadening the class of usable games has the benefit of enabling greater design space, as different implementation technologies may favor different games. (For example, the highly accurate topological quantum computing approach using Majorana fermions is known not to be quantum universal [Nayak et al., 2008]. In particular, Deng and Duan [Deng and Duan, 2013] showed that for randomness expansion using Majorana fermions, three qubits are required. Our proof allows the use of Majorana fermions for randomness expansion through the GHZ game.)

We include two applications of our expansion protocols. Our protocol can be used in combination with the randomness amplification results of [Chung et al., 2014] to create a robust, untrusted-device quantum protocol that converts an arbitrary weak random source into near-perfect output randomness of an arbitrary large length. This opens the possibility for unconditionally secure cryptography with the minimum trust on the randomness source and the implementing device. The second application is to adapt our protocol for untrusted-device quantum key distribution, resulting in a robust and secure protocol that requires only a small (polylogarithmic) initial seed.

1.4 Related Works

Prior to our paper, the groundbreaking work of [Vazirani and Vidick, 2012] was the first and only work achieving simultaneous exponential expansion and quantum security. As far as we know from their analysis, their security proof achieves only inverse polynomial security, and thus is not cryptographically secure; it is not noise-tolerant (as it requires perfect behavior on some rounds); and it also does not have the feature of constant-sized quantum memory.

Robust DI-QKD was already achieved with full security in [Vazirani and Vidick, 2014]. (There were also previous non-robust proofs [Barrett et al., 2012, Reichardt et al., 2013] and proofs that require that the number of devices increases with the length of the key, e.g., [Hänggi et al., 2010], [Masanes et al., 2011].) The new feature offered by our QKD result is that our seed is polylogarithmic, while that of [Vazirani and Vidick, 2014] is linear.

²An alternative for achieving the small quantum memory requirement is to introduce an additional device component that is required to function as an entanglement creation and distribution component and cannot receive information from other device components. This model would require a communication restriction throughout the protocol.

The paper [Vazirani and Vidick, 2014] on untrusted-device QKD can be considered as a robust randomness expansion protocol with a *linear* rate of expansion (without the constant memory feature). A natural way to develop [Vazirani and Vidick, 2014] further as an expansion result would be to change the input distribution to one that is non-uniform (so as to require less than a linear seed) and to apply the proof to a more general class of games (such as those of [Coudron et al., 2013]). To our knowledge a formal analysis of these generalizations has not yet been published, and they are a topic for further research.

[Coudron and Yuen, 2014] did contemporaneous work on the problem of unbounded randomness expansion. Their paper was the first to prove that (non-robust) unbounded expansion is possible with a *constant* number of devices. We independently proved that robust expansion is possible with $\log^*(N)$ devices. After we learned of their work we observed that a result with both features — robustness and a constant number of devices — follows by combining results from our work and [Chung et al., 2014]. We discuss this more in the next subsection (see the remarks that follow Corollary 1.6).

1.5 Technical Statements

Our main protocol (Figure 2) is based on [Pironio et al., 2010] and [Coudron et al., 2013]. (Indeed, it is only a slight modification of a protocol from the classical security results of [Coudron et al., 2013] — the main differences are the class of games that we use, and most importantly, that we explicitly allow in-between-rounds quantum communication.) We use the idea from [Pironio et al., 2010] to conserve seed by giving a fixed input to the device on most rounds.

The games we use involve n parties, with $n \geq 2$. Such a game is played by a single *device*, which consists of n *components*, where each component has a classical input/output interface.³ For any game that we use, we let \mathbf{w}_G denote the highest winning probability which can be achieved by a quantum strategy, and let $\mathbf{f}_G = 1 - \mathbf{w}_G$ denote the smallest possible failure probability that can be achieved by a quantum strategy.

We discuss some the concepts necessary to evaluate the security of Protocol R. We measure the amount of randomness produced by the quantum min-entropy $H_{\min}(X|E)$, where X denotes the output of the protocol and E denotes the (possibly quantum) information possessed by an adversary. This quantity is appropriate because it measures the amount of uniformly random bits that can be extracted from X by a randomness extractor (see Chapter 5 of [Renner, 2005]).

Let $y \geq 0$. We will say that a subnormalized classical-quantum state ρ is *y-ideal* if its normalization $\rho/\text{Tr}(\rho)$ has conditional min-entropy greater than or equal to y . (For convenience, we will say that the zero state is *y-ideal* for all y .) Let $\epsilon_s, \epsilon_c, \lambda$ be reals in $[0, 1]$. A randomness expansion protocol is said to have a *yield of y extractable bits* with a *soundness error* ϵ_s if for any device D , and any purifying system E for D , the state of (X, E) corresponding to the “success” event is always within trace distance ϵ_s of a *y-ideal* state. It is said to have a *completeness error* ϵ_c with noise level λ if there exists an implementation, referred to as the “correct” implementation, so that for any implementation which deviates by no more than λ from the correct implementation, the probability of aborting is always $\leq \epsilon_c$. If both the soundness and the completeness errors are $\leq \epsilon$, we simply say the protocol has an error ϵ .

³We note that the literature on this subject has some differences in terminology. Some authors would use the word “device” in the way that we have used the word “component.”

Arguments:

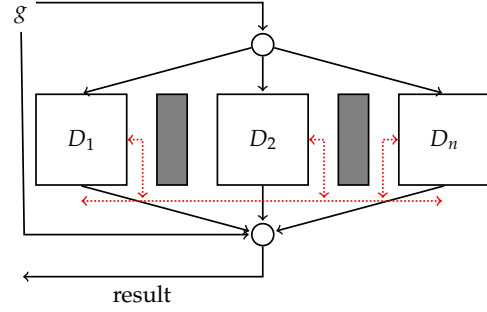
N : a positive integer (the **output length**.)

η : A real $\in (0, \frac{1}{2})$. (The **error tolerance**.)

q : A real $\in (0, 1)$. (The **test probability**.)

G : An n -player nonlocal game that is a **strong self-test** [Miller and Shi, 2013].

D : An untrusted device (with n components) that can play G repeatedly and cannot receive any additional information. In a single use the different components cannot communicate; in between uses, there is no restriction.



A diagram of Protocol R. The dotted red lines denote in-between-round communications.

Protocol R:

1. A bit $g \in \{0, 1\}$ is chosen according to a biased $(1 - q, q)$ distribution.
2. If $g = 1$ ("game round"), then an input string is chosen at random from $\{0, 1\}^n$ (according a probability distribution specified by G) and given to D . Depending on the outputs, a "P" (pass) or an "F" (fail) is recorded according to the rules of the game G .
3. If $g = 0$ ("generation round"), then the input string $00 \dots 0$ is given to the device, and the output of the first component D_1 is determined. If the output of the first component is 0, the event H ("heads") is recorded; otherwise the event T ("tails") is recorded.
4. Steps 1 – 3 are repeated $N - 1$ (more) times.
5. If the total number of failures exceeds $(1 - \mathbf{w}_G + \eta) qN$, the protocol **aborts**. Otherwise, the protocol **succeeds**. If the protocol succeeds, the output consists of an N -length sequence from the alphabet $\{P, F, H, T\}$ representing the outcomes of each round.

Figure 2: The Central Protocol R

Our main result is the following.

Theorem 1.1 (Main Theorem). *For any n -player strong self-test G , and any $\delta > 0$, there exist positive constants q_0, η_0, K, b , such that the following hold when Protocol R is executed with parameters $q \leq q_0$, $\eta \leq \eta_0$.*

1. (Soundness.) *The yield is at least $(1 - \delta)N$ extractable bits with a soundness error $\epsilon_s = K \exp(-bqN)$.*
2. (Completeness.) *For any constant η' , $0 < \eta' < \eta$, the protocol tolerates η' noise level with a completeness error $\epsilon_c = \exp(-(\eta - \eta')^2 qN/3)$.*

The difficult part of this result is the soundness claim, which follows from the results of section 8 (see Corollary 8.7). The completeness claim follows from the Azuma-Hoeffding inequality, and is proved in Proposition 8.13.

Note that the bits g_1, \dots, g_N can be generated by $O(Nh(q))$ uniformly random bits with an error $\exp(-\Omega(qN))$, where h denotes the Shannon entropy function. Therefore, when q is chosen to be small, the protocol needs only $\omega(\log N)$ initial bits and one device to achieve $\Omega(N)$ extractable bits with negligible error.

Corollary 1.2 (One-shot Min-entropy Expansion). *For any real $\omega \in (0, 1)$, setting $q = \Theta(k^\omega / 2^{k^{1-\omega}})$ in Theorem 1.1, Protocol R converts any k uniform bits to $2^{k^{1-\omega}}$ extractable bits with $\exp(-\Omega(k^\omega))$ soundness and completeness errors.*

To obtain near perfect random bits, we apply a quantum-proof strong randomness extractor, in particular one that extracts a source of a linear amount of conditional quantum min-entropy. The parameters of our protocols depend critically on the seed length of such extractors, thus we introduce the following definition.

Definition 1.3 (Seed Length Index). *We call a real ν a seed length index if there exists a quantum-proof strong extractor extracting $\Theta(N)$ bits from a $(N, \Theta(N))$ source with error parameter ϵ using $\log^{1/\nu}(N/\epsilon)$ bits of seed. Denote by μ the supremum of all seed length indices.*

Such extractors exist with $\nu \geq 1/2$, e.g., Trevisan's extractors [Trevisan, 2001] shown to be quantum-proof by De *et al.* [De *et al.*, 2012]. Thus $\mu \geq 1/2$. The definition of soundness error for producing y bits of perfect randomness is the same for producing extractable random bits, except that the ideal C-Q state conditioned on Success is the product state of y perfectly random bits and a quantum state. The following corollary follows directly by composing protocol R and an extractor with ν close to μ .

Corollary 1.4 (One-shot Randomness Expansion). *For any $\omega \in (0, \mu)$, setting $q = \Theta(k^\omega / 2^{k^{\mu-\omega}})$ in Theorem 1.1, Protocol R composed with an appropriate quantum-proof strong extractor converts k bits to $2^{k^{\mu-\omega}}$ uniform bits with soundness and completeness errors $\exp(-\Omega(k^\omega))$.*

The next corollary addresses cryptographic security. (Note: In measuring running time, one round of interaction with the device is considered a unit time.)

Corollary 1.5 (Cryptographic Security). *With the parameters in Corollary 1.4, the running time of the protocol is $T := \Theta(2^{k^{\mu-\omega}})$. Thus for any $\lambda > 1$, setting $\omega = \frac{\lambda}{1+\lambda}\mu$, the errors are $\exp(-\Omega(\log^\lambda T))$, which are negligible in T . That is, the protocol with those parameters achieves cryptographic quality of security (while still exponentially expanding.)*

Once we have near perfect randomness as output, we can use it as the input to another instance of the protocol, thus expanding further with an accumulating error parameter. As the error parameters decrease at an exponential rate, they are dominated by the first set of errors.

Corollary 1.6 (Robust Unbounded Randomness Expansion). *For all integers N and k , and any real $\omega \in (0, \mu)$, k uniformly random bits can be expanded to N output bits with $\exp(-\Omega(k^\omega))$ error under a constant level of noise. The procedure uses $O(\log^* N)$ iterations of Protocol R using $O(\log^* N)$ devices.*

To decrease the number of devices used in unbounded expansion, a possibility (used, e.g., in [Fehr et al., 2013]) is to cross-feed the outputs of two devices (i.e., give the output of one device as the input to another, and then vice versa). But there is an apparent obstacle for proving security for such an approach: once a device produces output, this output is now correlated with the device itself. When this output is fed to a second device to produce new output, one needs to show that the correlation with the first device does not persist. (If it did, then at the third iteration one would be feeding the first device a seed that was correlated with the first device itself, thus causing an insecurity.)

[Coudron and Yuen, 2014] call this the *input security problem*, and solve it by an improved analysis of the Reichardt-Unger-Vazirani protocol [Reichardt et al., 2013]. Under this new analysis, the RUV protocol turns a uniform-to-device input into a globally-uniform output with sufficiently strong parameters. By interleaving the RUV protocol with the exponentially expanding protocol of [Vazirani and Vidick, 2012], they prove non-robust unbounded expansion with 4 two-part devices.

An independent result of [Chung et al., 2014] can be used to address this problem in a different way. The Equivalence Lemma of [Chung et al., 2014] states that if a randomness expansion protocol is secure with a globally random input, then it is also automatically secure with any uniform-to-device input. This means that the correlation of each device with its own output does not cause a problem. Consequently, unbounded expansion with 2 devices can be achieved by cross-feeding *any* secure randomness expansion protocol.

We therefore have the following corollary (which is subsequent to [Coudron and Yuen, 2014], though based on independent techniques). See section 9.

Corollary 1.7 (Robust Unbounded Randomness Expansion with 2 Devices). *The number of (multi-part) devices used in Corollary 1.6 can be reduced to 2.*

To apply our protocol to randomness amplification, we can use the results of [Chung et al., 2014]. The amplification protocol in [Chung et al., 2014] requires having a robust randomness certification procedure to call as a subroutine; for this, we can use Protocol R with $q = \Theta(1)$. The amplification protocol converts a n -bit, min-entropy $\geq k$ weak source to a near perfectly random output of $\Theta(k)$ bits. Then we can concatenate with the protocol of Corollary 1.7 to expand to an arbitrarily long near perfect randomness. (Here the improvement from Corollary 1.6 to Corollary 1.7 implies that the number of devices need not depend on the output length.)

Corollary 1.8 (with [Chung et al., 2014] — Randomness Amplification). *Let $v \in [1/2, \mu]$ be a seed length index. For all sufficiently large integer k , any integer $n = \exp(O(k^{v^2}))$, any real $\epsilon = \exp(-O(k^{v^2}))$, any (n, k) source can be converted to an arbitrarily long near perfect randomness with ϵ soundness and completeness errors under a (universal) constant level of noise. The number of devices used is $2^{O(\log^{1/v}(n/\epsilon))}$, which in particular does not depend on the output length.*

We point out that the number of devices $T = T(n, 1/\epsilon)$ used as a function of the weak source length n and the error parameter ϵ grows super-polynomially (if $\mu < 1$) or polynomially (if

$\mu = 1$). It remains a major open problem if $T(n, 1/\epsilon)$ can be substantially reduced or even be made a universal constant. We stress, however, that the limitation imposed by this function is better interpreted as limiting the achievable error, instead of computational efficiency. This is because, T could still scale efficiently as a function of the *output* length. For example, to output N bits, as long as $\epsilon = \exp(-O(\log^v N))$, the number of devices is still polynomial in N . Therefore, the question of improving T is the question of broadening the application of the combined amplification-expansion protocol to settings requiring inverse-polynomial or even cryptographic quality of error.

Lastly, we state our result on quantum key distribution. Suppose that Alice and Bob would like to establish a shared secret string in an environment where trusted randomness is a scarce resource, and consequently their initial randomness is much shorter than the desired output length. (As with other studies on quantum key distribution (QKD), we will sidestep the authentication issue, assuming that the man-in-the-middle attack is already dealt with.) One way to adapt our randomness expansion protocol for untrusted-device QKD scenario is for Alice to expand her initial randomness, then use the expanded, secure randomness to execute the untrusted device QKD protocol of Vazirani and Vidick [Vazirani and Vidick, 2014]. The end result is an exponentially expanding key distribution protocol. An alternative approach, which is the focus of our new contribution, is to directly adapt our expansion protocol to achieve simultaneously randomness expansion and key distribution (see Protocol R_{kd} in Fig. 7). The benefits of doing so is the reduction of the number of untrusted devices from 2 to 1.

We present the details in section 10 and state our main result on key distribution below. The notion of soundness and completeness errors are similarly defined: the soundness error is the distance of the output distribution to a mixture of aborting and an output randomness of a desired smooth min-entropy, and the completeness error is the probability of aborting for an honest (possibly noisy) implementation.

Corollary 1.9 (Robust Untrusted-Device QKD with Short Seed). *For any strong self-test G , there exist positive constants r, λ, η, q_0 such that for infinitely many positive integers N and any $q \leq q_0$, Protocol R_{kd} (Fig. 7) satisfies the following.*

1. (Soundness.) *The protocol obtains a key of rN extractable bits with a soundness error*

$$\epsilon_s = \exp(-\Omega(qN) + O(1)).$$

2. (Completeness.) *For any constant η' , $0 < \eta' < \eta$, the protocol tolerates η' noise level with a completeness error $\epsilon_c = \exp(-\Omega((\eta - \eta')^2 qN))$.*

The number of initial random bits is $O(Nh(q) + \log N)$, and the time complexity is polynomial in N .

Thus, for example, if we set $q = (\log^2 N)/N$, we can distribute $\Omega(N)$ extractable bits using a seed of size $O(\log^3 N)$, with error terms achieving cryptographic security. Composing this protocol with a quantum-proof randomness extractor that uses a polylogarithmic seed [De et al., 2012] yields untrusted-device QKD from a polylogarithmic seed.

1.6 Numerical Results

The proof methods in the paper are sufficient to give actual numerical bounds for the amount of randomness generated by Protocol R. In subsection 8.3 we offer an example showing how this

is done. If G is a strong self-test, then there is an associated quantity $\mathbf{v}_G > 0$ (called the trust coefficient). Let

$$\pi(y) = 1 - 2y \log\left(\frac{1}{y}\right) - 2(1-y) \log\left(\frac{1}{1-y}\right). \quad (1.1)$$

We show that if $\eta < \mathbf{v}_G/2$, Protocol R produces $\pi(\eta/\mathbf{v}_G)N$ extractable bits per round, modulo error terms (see Corollary 8.5). In particular, a positive rate is achieved provided that $\pi(\eta/\mathbf{v}_G) > 0$, which occurs when $\eta < 0.11 \cdot \mathbf{v}_G$. Subsection 8.3, shows that $\mathbf{v}_{GHZ} \geq 0.14$. Therefore, the GHZ game achieves a positive linear rate provided that $\eta < 0.11 \cdot 0.14 = 0.0154$.

2 Overview of Proofs

While proving classical security of randomness expansion protocols is mainly appropriate applications of Azuma-Hoeffding inequality, proving quantum security is much more challenging. The proof for the Vazirani-Vidick protocol [Vazirani and Vidick, 2012] relies on a characterization of quantum smooth min-entropy based on the quantum-security of Trevisan’s extractors [De et al., 2012]. We take a completely different approach, without any reference to extractors in the main security proof. Below we summarize some of the tools used in our proof, which we are hopeful will find applications elsewhere.

2.1 Quantum Rényi Entropies

We follow previous work [Tomamichel et al., 2009], [Dupuis et al., 2015] and use the Renyi entropy function $H_\alpha(\rho)$ and Renyi divergence function $D_\alpha(\rho\|\sigma)$ to lower bound the number of extractable bits in a classical register with quantum side information. (See subsection 3.2.) Crucially, we use the newer definition of the quantum Renyi divergence function (the “sandwiched” definition) which was introduced in [Jaksic et al., 2010] and developed in [Müller-Lennert et al., 2013], [Wilde et al., 2014].

In [Tomamichel et al., 2009], the authors prove a lower bound on the conditional smooth min-entropy of n identical copies of a bipartite system ρ_{AB} in terms of its relative entropy $H(A|B)_\rho$. They accomplish this by using the Renyi entropy H_α as an intermediate quantity, exploiting inequalities that relate it to both H_{min}^ϵ and H , and then using the additive property of H_α . Our proof incorporates a similar line of reasoning: we prove inductively an upper bound on the Renyi divergence of the outputs of Protocol R (conditioned on the adversary), and then use this to compute a lower bound for the same outputs expressed in terms of smooth min-entropy.

An challenge in our proofs is choosing the right parameter α . If α is too close to 1, the penalty term in the inequality that relates H_α to H_{min}^ϵ will be large enough to make the lower bound on smooth min-entropy useless; but if α is too far from 1, the Renyi entropy is not sensitive enough to detect the effect of rare events, such as the game rounds in Protocol R . The parameter α is therefore adjusted according to parameters in the Protocol R — roughly speaking, it is set so that $\alpha - 1$ is proportional to the parameter q .

Our first original result (Theorem 4.2) is an Renyi entropy uncertainty principle for measurements on an entangled qubit. If QE is a bipartite system where $\dim Q = 2$, let $\{\rho_0, \rho_1\}$ and $\{\rho_+, \rho_-\}$ denote the subnormalized states of E that arise from measuring the computational basis and the Hadamard basis on Q , respectively. Theorem 4.2 expresses uniform constraints (independent of the dimension of E) on the quantities $\text{Tr}[\rho_x^{1+\epsilon}]$. This parallels other known uncertainty relations [Wehner and Winter, 2010]. The proof is based on a known matrix inequality for the $(2 + 2\epsilon)$ -Schatten norm.

2.2 Partially Trusted Measurement Simulation

A key insight which enables our proof is that untrusted devices can be used to simulate *partially* trusted measurements. Let us say that a *device with trusted measurements* F is a single-part input-output device which receives a single bit as an input, and, depending on the value of the bit, performs one of two perfectly anti-commutative binary measurements on a quantum system. The measurements of the device are trusted, but the state is unknown. Now consider another single-part binary device F' which performs as follows (for some real parameters v, h):

1. On input 0, F' performs the same measurement as F .
2. On input 1, one of the following occurs at random:
 - (a) F' performs the same measurement as D (probability = v);
 - (b) F' outputs a perfectly coin flip (probability = h);
 - (c) F' performs an unknown measurement (probability = $1 - v - h$).

The device F' is what we will call a *partially trusted* device (see Definition 6.2 for a formal definition).

Consider the state of the device D after steps 1–3 in Protocol R. Let G_1 be a classical register containing the bit g , and let O_1 be a classical register which we set to be 0 if the output is P or H , and 1 if the output is F or T . We show (sections 5–6) that the joint state of $G_1 O_1$ can be simulated by a partially trusted device D' which accepts G_1 as its input and produces O_1 as its output. (Here, “simulation” means that if either device is prepared with an initial purifying system E , the joint state $EG_1 O_1$ will be the same up to isomorphism regardless of which device was used.)

We define a new protocol (Protocol A' , Figure 4) which is essentially Protocol R with its device replaced by a single-part partially trusted device. Proving the security of Protocol R reduces to proving the security of Protocol A' .

2.3 An Induction Proof With a Weighted Measure of Randomness

The next step is to prove the security of Protocol A' . Let $G = (G_1, \dots, G_N)$ and $O = (O_1, \dots, O_N)$ denote registers containing the input bits and output bits, respectively, from Protocol A' , and let E denote a purifying system for the device in Protocol A' . Let Γ_{EGO}^s denote the subnormalized state of these three systems corresponding to the “success” event (s). Our approach is to prove an upper bound on the (negative) quantity

$$D_\alpha(\Gamma_{EGO}^s \| \Gamma_{EG} \otimes \mathbb{I}_O). \quad (2.1)$$

Another central insight for our proof is the idea of using a weighted measure of randomness. Consider the first-round registers G_1 and O_1 , and E . The bounding operator $\Gamma_{EG_1} \otimes \mathbb{I}_{O_1}$ on $EG_1 O_1$ is equal to

$$(1 - q)\Gamma_E \otimes |00\rangle\langle 00| + (1 - q)\Gamma_E \otimes |01\rangle\langle 01| + (q)\Gamma_E \otimes |10\rangle\langle 10| + (q)\Gamma_E \otimes |11\rangle\langle 11|$$

Let $\lambda > 0$ be a real parameter, and consider the following alternative operator, where we have inserted the factor 2^λ in the fourth summand:

$$\Sigma := (1 - q)\Gamma_E \otimes |00\rangle\langle 00| + (1 - q)\Gamma_E \otimes |01\rangle\langle 01| + (q)\Gamma_E \otimes |10\rangle\langle 10| + (q)2^\lambda \Gamma_E \otimes |11\rangle\langle 11|.$$

The factor 2^λ artificially adds randomness when the event $(g, o) = (1, 1)$ (which corresponds to a game-loss in Protocol R) occurs. Effectively, we lower our expectation for randomness according to how well the device is performing.

Our uncertainty principle for Renyi entropy implies that, for appropriate λ, α , the quantity $D_\alpha(\Gamma_{EG_1O_1} \parallel \Sigma)$ has a uniform upper bound less than zero. This enables an induction proof which shows an upper bound on (2.1).

A version of this argument is carried out in section 7. We deduce a lower bound on the number extractable bits output by Protocol A' . By the reduction discussed above, this implies a lower bound on the number of extractable bits output by Protocol R (see section 8, Corollary 8.4).

2.4 Quantum Key Distribution

Proving quantum distribution requires first showing that when the noise tolerance in Protocol R is set sufficiently low, and the protocol succeeds, then the device must score well not only during game rounds but also during generation rounds. This is accomplished using Azuma's inequality. A consequence is that if two parties possess different subsets of the components of the device D , they can use these devices to construct strings of length N which differ in at most $(1/2 - \lambda)N$ places, where $\lambda > 0$. We then perform efficient information reconciliation on these strings, adapting previous work [Guruswami, 2003], [Smith, 2007].

3 Preliminaries

3.1 Notation

When a sequence is defined, we will use Roman font to refer to individual terms (e.g., h_1, \dots, h_n) and boldface font to refer to the sequence as a whole (e.g., \mathbf{h}). For any bit b , let $\bar{b} = 1 - b$. For any sequence of bits $\mathbf{b} = (b_1, \dots, b_n)$, let $\bar{\mathbf{b}} = (\bar{b}_1, \dots, \bar{b}_n)$.

We write the expression $f(x)^y$ (where f is a function) to mean $(f(x))^y$. Thus, for example, in the expression

$$\text{Tr}[Z]^{1/q} \tag{3.1}$$

the $(1/q)$ th power map is applied after the trace function, not before it.

We write $(\log x)$ to denote the logarithm with base 2, and we write $(\ln x)$ to denote the logarithm with base e . We use $h: [0, 1] \rightarrow \mathbb{R}$ to denote the Shannon entropy function:

$$h(x) = -x \log x - (1 - x) \log(1 - x). \tag{3.2}$$

We will use capital letters (e.g., Q) to denote quantum systems. We use the same letter to denote both the system itself and the complex Hilbert space which represents it. For any finite-dimensional complex Hilbert space Q , let $\mathcal{L}(Q)$ denote the set of linear maps from Q to itself, and let

$$\mathcal{P}(Q) = \{\sigma \in \mathcal{L}(Q) \mid \sigma \geq 0\} \tag{3.3}$$

$$\mathcal{S}(Q) = \{\sigma \in \mathcal{L}(Q) \mid \sigma \geq 0, \text{Tr}(\sigma) \leq 1\} \tag{3.4}$$

$$\mathcal{D}(Q) = \{\sigma \in \mathcal{L}(Q) \mid \sigma \geq 0, \text{Tr}(\sigma) = 1\}. \tag{3.5}$$

These are, respectively, the set of positive semidefinite operators, the set of subnormalized positive semidefinite operators, and the set of density operators.

If $\rho_1: X_1 \rightarrow Y_1$ and $\rho_2: X_2 \rightarrow Y_2$ are two linear operators, then we denote by $\rho_1 \oplus \rho_2$ the operator from $X_1 \oplus X_2$ to $Y_1 \oplus Y_2$ which maps (x_1, x_2) to $(\rho_1(x_1), \rho_2(x_2))$.

If (B, E) is a bipartite system, and ρ is a density operator on $B \otimes E$ representing a classical-quantum state, then we may express ρ as a diagonal-block operator

$$\rho = \begin{bmatrix} \rho_1 & & & & \\ & \rho_2 & & & \\ & & \rho_3 & & \\ & & & \ddots & \\ & & & & \rho_m \end{bmatrix}, \quad (3.6)$$

where ρ_1, \dots, ρ_m denote the subnormalized operators on E corresponding to the basis states of the classical register B . Alternatively, we may express ρ as $\rho = \rho_1 \oplus \rho_2 \oplus \dots \oplus \rho_m$.

For any $\alpha > 0$, and any linear operator X , let $\|X\|_\alpha$ denote the Schatten norm:

$$\|X\|_\alpha = \text{Tr}[(X^*X)^{\alpha/2}]^{1/\alpha}. \quad (3.7)$$

Note that if X is positive semidefinite, this may be written more simply as

$$\|X\|_\alpha = \text{Tr}[X^\alpha]^{1/\alpha}. \quad (3.8)$$

We will often be concerned with the function $Z \mapsto Z^x$, where $x \in [0, 2]$. We note the following mathematical properties.

Proposition 3.1. *Let $\gamma \in [0, 1]$, and let Z, W denote positive semidefinite operators on \mathbb{C}^n .*

- (a) *If $Z \leq W$, then $Z^\gamma \leq W^\gamma$.*
- (b) *If $Z \leq W$ and $X = W - Z$, then*

$$\text{Tr}(X^{1+\gamma}) + \text{Tr}(Z^{1+\gamma}) \leq \text{Tr}(W^{1+\gamma}). \quad (3.9)$$

Proof. Part (a) is given by Theorem 2.6 in [Carlen, 2009]. Part (b) follows from part (a) by the following reasoning:

$$\text{Tr}(W^{1+\gamma}) = \text{Tr}(W \cdot W^\gamma) \quad (3.10)$$

$$= \text{Tr}(X \cdot W^\gamma) + \text{Tr}(Z \cdot W^\gamma) \quad (3.11)$$

$$\geq \text{Tr}(X \cdot X^\gamma) + \text{Tr}(Z \cdot Z^\gamma) \quad (3.12)$$

$$= \text{Tr}(X^{1+\gamma}) + \text{Tr}(Z^{1+\gamma}). \quad (3.13)$$

This completes the proof. □

3.2 Quantum Rényi Divergence

In this subsection we state the definitions of the two primary measures of randomness used in this paper (Renyi divergence and smooth min-entropy) and establish their relationship. We quote the definition of quantum Rényi divergence from [Jaksic et al., 2010], [Müller-Lennert et al., 2013], [Wilde et al., 2014].

Definition 3.2 ([Müller-Lennert et al., 2013]). Let ρ be a density matrix on \mathbb{C}^n . Let σ be a positive semidefinite matrix on \mathbb{C}^n whose support contains the support of ρ . Let $\alpha > 1$ be a real number. Then,

$$d_\alpha(\rho\|\sigma) = \text{Tr} \left[\left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right]^{\frac{1}{\alpha-1}}. \quad (3.14)$$

More generally, for any positive semidefinite matrix ρ' whose support is contained in $\text{Supp } \sigma$, let

$$d_\alpha(\rho'\|\sigma) = \text{Tr} \left[\frac{1}{\text{Tr}[\rho']} \left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho' \sigma^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right]^{\frac{1}{\alpha-1}}. \quad (3.15)$$

Let

$$D_\alpha(\rho'\|\sigma) = \log d_\alpha(\rho'\|\sigma). \quad (3.16)$$

Let AB be a classical quantum system whose state is given by a density operator ρ_{AB} . One way to quantify the amount of randomness in A conditioned on B is via an expression of the form $-D_\alpha(\rho_{AB}\|\mathbb{I}_A \otimes \sigma_B)$, where σ_B is a density operator. (Maximizing over expressions of this form leads to the corresponding notion of conditional Renyi entropy, which will not be used directly in this paper. See Definition 10 in [Müller-Lennert et al., 2013].)

Note that if ρ is a density matrix, then

$$D_\alpha(\rho\|\mathbb{I}) = -\frac{1}{\alpha-1} \log \text{Tr}[\rho^\alpha]. \quad (3.17)$$

For any positive semidefinite operator ρ , let $H_\alpha(\rho) := D_\alpha(\rho\|\mathbb{I})$. This is the unconditional α -Renyi entropy of ρ .

Additionally, we will need a definition of smooth min-entropy. There are multiple definitions of smooth min-entropy that are essentially equivalent. The definition that we will use is not the most up-to-date (see [Tomamichel et al., 2010]) but it is good for our purposes for its simplicity.

Definition 3.3. Let AB be a classical-quantum system, and let ρ_{AB} be a positive semidefinite operator. Let $\epsilon > 0$ be a real number. Then,

$$H_{\min}^\epsilon(A|B)_\rho = \max_{\substack{\rho' \in \mathcal{S}(A \otimes B) \\ \|\rho' - \rho\|_1 \leq \epsilon}} \max_{\substack{\sigma \in P(A) \\ \mathbb{I}_A \otimes \sigma \geq \rho'}} -\log(\text{Tr}(\sigma)). \quad (3.18)$$

The smooth min-entropy measures the number of random bits that can be extracted from a classical source in the presence of quantum information [Renner, 2005]. When it is convenient, we will use the notation $H_{\min}^\epsilon(\rho_{AB}|B)$ instead of $H_{\min}^\epsilon(A|B)_\rho$.

Following [Datta, 2009], let us define the *relative smooth max-entropy* of two operators.

Definition 3.4. Let ρ, σ be positive semidefinite operators on \mathbb{C}^n such that the support of σ contains the support of ρ . Then,

$$D_{\max}(\rho\|\sigma) = \log \min_{\substack{\lambda \in \mathbb{R} \\ \rho \leq \lambda \sigma}} (\lambda). \quad (3.19)$$

For any $\epsilon \geq 0$,

$$D_{\max}^\epsilon(\rho\|\sigma) = \inf_{\substack{\|\rho' - \rho\|_1 \leq \epsilon \\ \rho' \in \mathcal{S}(\mathbb{C}^n)}} D_{\max}(\rho'\|\sigma). \quad (3.20)$$

The quantity D_{max}^ϵ is convenient for computing lower bounds on H_{min}^ϵ . Note that if ψ_B is any density matrix on B ,

$$H_{min}^\epsilon(\rho_{AB}|B) \geq -D_{max}^\epsilon(\rho_{AB} \|\mathbb{I}_A \otimes \psi_B). \quad (3.21)$$

The following proposition and corollary relate smooth min-entropy to Renyi divergence. The proof of the proposition is an easy derivative of proofs of similar results ([Tomamichel et al., 2009], [Dupuis et al., 2015]) and is given in Appendix A.4. The corollary follows easily.

Proposition 3.5. *Let $\alpha \in (1, 2]$. Let ρ be a density operator on a finite-dimensional Hilbert space V , and let $\sigma \in \mathcal{P}(V)$ such that $\text{Supp } \sigma \supseteq \text{Supp } \rho$. Then,*

$$D_{max}^\epsilon(\rho \|\sigma) \leq D_\alpha(\rho \|\sigma) + \frac{2 \log(1/\epsilon) + 1}{\alpha - 1}. \quad (3.22)$$

Additionally, if ρ is a classical-quantum operator on a bipartite state, then there exists a classical-quantum operator ρ' with $\|\rho' - \rho\|_1 \leq \epsilon$ and $\rho' \geq 0$ such that $D_{max}(\rho' \|\sigma)$ satisfies the above bound. \square

Corollary 3.6. *Let AB be a classical-quantum bipartite system, and let ρ_{AB} be a density operator. Let σ_B be a density operator on B whose support contains $\text{Supp } \rho_B$. Let $\epsilon > 0$ and $\alpha \in (1, 2]$ be real numbers. Then, for any $\epsilon > 0$,*

$$H_{min}^\epsilon(A | B)_\rho \geq -D_\alpha(\rho \|\mathbb{I}_A \otimes \sigma_B) - \frac{2 \log(1/\epsilon) + 1}{\alpha - 1}. \quad \square \quad (3.23)$$

3.3 Quantum Devices

Let us formalize some terminology and notation for describing quantum devices. (Our formalism is a variation on that which has appeared in other papers on untrusted devices, such as [Reichardt et al., 2013].)

Definition 3.7. *Let n be a positive integer. A **binary quantum device with n components** $D = (D_1, \dots, D_n)$ consists of the following.*

1. Quantum systems Q_1, \dots, Q_n whose initial state is specified by a density operator,

$$\Phi: (Q_1 \otimes \dots \otimes Q_n) \rightarrow (Q_1 \otimes \dots \otimes Q_n) \quad (3.24)$$

2. For any $k \geq 0$, and any function

$$T: \{0, 1\} \times \{1, 2, \dots, k\} \times \{1, 2, \dots, n\} \rightarrow \{0, 1\} \quad (3.25)$$

a unitary operator

$$U_T: (Q_1 \otimes \dots \otimes Q_n) \rightarrow (Q_1 \otimes \dots \otimes Q_n). \quad (3.26)$$

and a collection of Hermitian operators

$$\left\{ M_{T,j}^{(b)}: Q_j \rightarrow Q_j \right\}_{\substack{b \in \{0,1\} \\ 1 \leq j \leq n}} \quad (3.27)$$

satisfying $\|M_{T,j}^{(b)}\| \leq 1$.

The device D behaves as follows. Suppose that k iterations of the device have already taken place, and suppose that T is such that $T(0, i, j) \in \{0, 1\}$ and $T(1, i, j) \in \{0, 1\}$ represent the input bit and output bit, respectively, for the j th player on the i th round ($i \leq k$). (T is the **transcript function**.) Then,

1. The components D_1, \dots, D_n collectively perform the unitary operation U_T on $Q_1 \otimes \dots \otimes Q_n$.
2. Each component D_j receives its input bit b_j , then applies the binary nondestructive measurement on Q_i given by

$$X \mapsto \left(\sqrt{\frac{\mathbb{I} + M_{T,j}^{(b_j)}}{2}} \right) X \left(\sqrt{\frac{\mathbb{I} + M_{T,j}^{(b_j)}}{2}} \right) \quad (3.28)$$

$$X \mapsto \left(\sqrt{\frac{\mathbb{I} - M_{T,j}^{(b_j)}}{2}} \right) X \left(\sqrt{\frac{\mathbb{I} - M_{T,j}^{(b_j)}}{2}} \right), \quad (3.29)$$

and then outputs the result.

Let us say that one binary quantum device D' **simulates** another binary quantum device D if, for any purifying systems E and E' (for D and D' , respectively), and any input sequence $\mathbf{i}_1, \dots, \mathbf{i}_k \in \{0, 1\}^n$, the joint state of the outputs of D together with E is isomorphic to the joint state of the outputs of D' together with E' on the same input sequence. Similarly, let us say that a protocol X **simulates** another protocol Y if, for any purifying systems E and E' for the quantum devices used by X and Y , respectively, the joint state of E together with the outputs of X is isomorphic to the joint state of E' together with the outputs of Y .

Definition 3.8. Let us say that a binary quantum device D is in **canonical form** if each of its quantum systems Q_j is such that $Q_j = \mathbb{C}^{2^{m_j}}$ for some $m_j \geq 1$, and each measurement operator pair $(M^{(0)}, M^{(1)}) = (M_{T,j}^{(0)}, M_{T,j}^{(1)})$ has the following 2×2 diagonal block form:

$$M^{(0)} = \begin{bmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{bmatrix} \quad M^{(1)} = \begin{bmatrix} 0 & \zeta_1 & & & & \\ \bar{\zeta}_1 & 0 & & & & \\ & & 0 & \zeta_2 & & \\ & & \bar{\zeta}_2 & 0 & & \\ & & & & \ddots & \\ & & & & & 0 & \zeta_{m_j} \\ & & & & & \bar{\zeta}_{m_j} & 0 \end{bmatrix},$$

where the complex numbers ζ_ℓ satisfy

$$|\zeta_\ell| = 1 \text{ and } \text{Im}(\zeta_\ell) \geq 0. \quad (3.30)$$

(Note that the complex numbers ζ_ℓ may be different for each transcript T and each player j .)

When we discuss quantum devices that are in canonical form, we will frequently make use of the isomorphism $\mathbb{C}^{2^m} \cong \mathbb{C}^2 \otimes \mathbb{C}^m$ given by $e_{2k-1} \mapsto e_1 \otimes e_k$, $e_{2k} \mapsto e_2 \otimes e_k$. (Here, e_1, \dots, e_r denote the standard basis vectors for \mathbb{C}^r .)

Proposition 3.9. Any binary quantum device can be simulated by a device that is in canonical form.

Proof. This follows from Theorem A.1 in the appendix. \square

4 An Uncertainty Principle

In this section, we consider the behavior of the map $\rho \mapsto \text{Tr}[\rho^{1+\epsilon}]$ when measurements are applied to a qubit and the operator ρ represents the state of a system that is entangled with the qubit.

We begin by quoting the following theorem, which appears as part of Theorem 5.1 in the paper [Pisier and Xu, 2003].

Theorem 4.1. *Let $X, Y: \mathbb{C}^m \rightarrow \mathbb{C}^n$ be linear operators. Let $p \geq 2$ be a real number, and let $p' = 1/(1 - 1/p)$. Then,*

$$\left[\frac{1}{2} \left(\|X + Y\|_p^p + \|X - Y\|_p^p \right) \right]^{1/p} \leq \left(\|X\|_p^{p'} + \|Y\|_p^{p'} \right)^{1/p'}. \quad \square \quad (4.1)$$

Inequality (4.1) may alternatively be expressed as

$$\left[\left\| \frac{X+Y}{\sqrt{2}} \right\|_p^p + \left\| \frac{X-Y}{\sqrt{2}} \right\|_p^p \right]^{1/p} \leq 2^{1/p-1/2} \left(\|X\|_p^{p'} + \|Y\|_p^{p'} \right)^{1/p'} \quad (4.2)$$

or,

$$\left\| \frac{X+Y}{\sqrt{2}} \right\|_p^p + \left\| \frac{X-Y}{\sqrt{2}} \right\|_p^p \leq 2^{1-p/2} \left(\|X\|_p^{p'} + \|Y\|_p^{p'} \right)^{p/p'}. \quad (4.3)$$

Observe the following: if QW is a bipartite quantum system with $Q = \mathbb{C}^2$ and $\Lambda \in \mathcal{D}(Q \otimes W)$ is a density operator, Λ can be written as

$$\Lambda = \begin{bmatrix} X^*X & X^*Y \\ Y^*X & Y^*Y \end{bmatrix} \quad (4.4)$$

for some $X, Y \in \mathcal{L}(W)$. Then the reduced state of W is

$$\rho := X^*X + Y^*Y \quad (4.5)$$

Additionally, if we let $\{\rho_0, \rho_1\}$ and $\{\rho_+, \rho_-\}$ denote the subnormalized states of W that arise from measurements on Q along the computational and Hadamard bases, respectively, then

$$\rho_0 = X^*X \quad (4.6)$$

$$\rho_1 = Y^*Y \quad (4.7)$$

$$\rho_+ = \left(\frac{X+Y}{\sqrt{2}} \right)^* \left(\frac{X+Y}{\sqrt{2}} \right), \quad (4.8)$$

$$\rho_- = \left(\frac{X-Y}{\sqrt{2}} \right)^* \left(\frac{X-Y}{\sqrt{2}} \right). \quad (4.9)$$

Theorem 4.2. *There exists a continuous function $\Pi: (0, 1] \times [0, 1] \rightarrow \mathbb{R}$ such that the following holds.*

1. *Let V be a quantum system, and let $\rho, \rho_0, \rho_1, \rho_+, \rho_- \in \mathcal{S}(V)$ denote operators arising from measurements of a qubit entangled with V . Let*

$$t = \frac{\text{Tr}(\rho_1^{1+\epsilon})}{\text{Tr}(\rho^{1+\epsilon})}. \quad (4.10)$$

Then, the following inequality always holds:

$$\log \left[\frac{\text{Tr}(\rho_+^{1+\epsilon} + \rho_-^{1+\epsilon})}{\text{Tr}(\rho^{1+\epsilon})} \right] \leq -\epsilon \Pi(\epsilon, t). \quad (4.11)$$

2. The limiting function $\pi(z) := \lim_{(x,y) \rightarrow (0,z)} \Pi(x,y)$ is given by

$$\pi(z) = 1 - 2z \log \left(\frac{1}{z} \right) - 2(1-z) \log \left(\frac{1}{1-z} \right). \quad (4.12)$$

Proof. Express the states ρ_* in terms of operators X and Y as in (4.5–4.9). Applying (4.3) with $p = 2 + 2\epsilon$, and $p' = 1/(1 - 1/p)$ we have the following:

$$\text{Tr}(\rho_+^{1+\epsilon} + \rho_-^{1+\epsilon}) = \left\| \frac{X+Y}{\sqrt{2}} \right\|_{2+2\epsilon}^{2+2\epsilon} + \left\| \frac{X-Y}{\sqrt{2}} \right\|_{2+2\epsilon}^{2+2\epsilon} \quad (4.13)$$

$$\leq 2^{1-p/2} \left(\|X\|_p^{p'} + \|Y\|_p^{p'} \right)^{p/p'} \quad (4.14)$$

$$= 2^{1-p/2} \left[\left(\|X\|_p^p \right)^{p'/p} + \left(\|Y\|_p^p \right)^{p'/p} \right]^{p/p'} \quad (4.15)$$

$$= 2^{-\epsilon} \left[\text{Tr}(\rho_0^{1+\epsilon})^{\frac{1}{1+2\epsilon}} + \text{Tr}(\rho_1^{1+\epsilon})^{\frac{1}{1+2\epsilon}} \right]^{1+2\epsilon} \quad (4.16)$$

Letting

$$s = \frac{\text{Tr}(\rho_0^{1+\epsilon})}{\text{Tr}(\rho^{1+\epsilon})}, \quad (4.17)$$

we have

$$\text{Tr}(\rho_+^{1+\epsilon} + \rho_-^{1+\epsilon}) \leq 2^{-\epsilon} \left[s^{\frac{1}{1+2\epsilon}} + t^{\frac{1}{1+2\epsilon}} \right]^{1+2\epsilon} \text{Tr}(\rho^{1+\epsilon}). \quad (4.18)$$

Since $\text{Tr}(\rho_0^{1+\epsilon}) + \text{Tr}(\rho_1^{1+\epsilon}) \leq \text{Tr}(\rho^{1+\epsilon})$, we have $t + s \leq 1$, and therefore,

$$\text{Tr}(\rho_+^{1+\epsilon} + \rho_-^{1+\epsilon}) \leq 2^{-\epsilon} \left[(1-t)^{\frac{1}{1+2\epsilon}} + t^{\frac{1}{1+2\epsilon}} \right]^{1+2\epsilon} \text{Tr}(\rho^{1+\epsilon}). \quad (4.19)$$

Let

$$\Pi(x,y) = -\frac{1}{x} \log \left\{ 2^{-x} \left[(1-y)^{\frac{1}{1+2x}} + y^{\frac{1}{1+2x}} \right]^{1+2x} \right\}. \quad (4.20)$$

The desired limiting condition follows using L'Hospital's rule. \square

We note that (4.11) can be rewritten as

$$\left(-\frac{1}{\epsilon} \log \text{Tr}(\rho_+^{1+\epsilon} + \rho_-^{1+\epsilon}) \right) - \left(-\frac{1}{\epsilon} \log \text{Tr}(\rho^{1+\epsilon}) \right) \geq \Pi(\epsilon, t). \quad (4.21)$$

The expression on the left side is the difference in $(1+\epsilon)$ -Renyi entropy between the state $\rho_+ \oplus \rho_-$ and the state ρ .

5 The Self-Testing Property of Binary Nonlocal XOR Games

In this section we review some of the known formalism for binary XOR games, and then prove new results.

5.1 Definitions and Basic Results

Definition 5.1. An n -player binary nonlocal XOR game consists of a probability distribution

$$\{p_{\mathbf{i}} \mid \mathbf{i} \in \{0, 1\}^n\} \quad (5.1)$$

on the set $\{0, 1\}^n$, together with an indexed set

$$\{\eta_{\mathbf{i}} \in \{-1, 1\} \mid \mathbf{i} \in \{0, 1\}^n\}. \quad (5.2)$$

Given any indexed sets $\{p_{\mathbf{i}}\}$ and $\{\eta_{\mathbf{i}}\}$ satisfying the above conditions, we can conduct an n -player nonlocal game as follows.

1. A referee chooses a binary vector $\mathbf{c} \in \{0, 1\}^n$ according to the distribution $\{p_{\mathbf{i}}\}$. For each k , he gives the bit c_k as input to the k th player.
2. Each player returns an output bit d_k to the referee.
3. The referee calculates the score, which is given by

$$\eta_{\mathbf{c}} (-1)^{d_1 + d_2 + \dots + d_n}. \quad (5.3)$$

If the score is $+1$, a “pass” has occurred. If the score is -1 , a “failure” has occurred.

We quote some definitions and results from [Miller and Shi, 2013] and [Werner and Wolf, 2001].

Definition 5.2. An *mixed n -player quantum strategy* is a pair

$$\left(\Psi, \{ \{ M_j^{(0)}, M_j^{(1)} \} \}_{j=1}^n \right) \quad (5.4)$$

where Ψ is a density matrix on an n -tensor product space $V_1 \otimes \dots \otimes V_n$ and $M_j^{(i)}$ denotes a linear operator on V_j whose eigenvalues are contained in $\{-1, 1\}$. A *pure n -player quantum strategy* is a pair

$$\left(\psi, \{ \{ M_j^{(0)}, M_j^{(1)} \} \}_{j=1}^n \right) \quad (5.5)$$

which satisfies the same conditions, except that ψ is merely a unit vector on $V_1 \otimes \dots \otimes V_n$. A **qubit strategy** is a pure quantum strategy in which the spaces V_i are equal to \mathbb{C}^2 and the operators $M_j^{(i)}$ are all nonscalar.

The **score** achieved by a quantum strategy at an n -player binary nonlocal XOR game $G = (\{p_{\mathbf{i}}\}, \{\eta_{\mathbf{i}}\})$ is the expected score when the qubit strategy is used to play the game G . This quantity can be expressed as follows. Let \mathbf{M} denote the **scoring operator** for G , which is given by

$$\mathbf{M} = \sum_{\mathbf{i} \in \{0, 1\}^n} p_{\mathbf{i}} \eta_{\mathbf{i}} M_1^{(i_1)} \otimes M_2^{(i_2)} \otimes \dots \otimes M_n^{(i_n)}. \quad (5.6)$$

Then, the score for strategy (5.4) at game G is $\text{Tr}(\mathbf{M}\Psi)$. The score for the pure strategy (5.5) is $\psi^* \mathbf{M} \psi$.

The **optimal score** for a nonlocal game is the highest score that can be achieved at the game by qubit strategies. We denote this quantity by q_G . (As explained in [Miller and Shi, 2013], this is also the highest score that can be achieved by arbitrary quantum strategies.) A game G is a **self-test** if there is only one qubit strategy (modulo local unitary operations on the n tensor components of $(\mathbb{C}^2)^{\otimes n}$) which achieves the optimal score. A game G is **winnable** if $q_G = 1$.

Note that q_G is different from the maximum **passing probability** for quantum strategies, which we denote by w_G . The two are related by $w_G = (1 + q_G)/2$. We will also write f_G for the **minimum failing probability**, which is given by $f_G = 1 - w_G$.

We define functions that are useful for the study of binary XOR games. For any nonlocal game $G = (\{p_i\}, \{\eta_i\})$, define $P_G: \mathbb{C}^n \rightarrow \mathbb{C}$ by

$$P_G(\lambda_1, \dots, \lambda_n) = \sum_{\mathbf{i} \in \{0,1\}^n} p_i \eta_i \lambda_1^{i_1} \lambda_2^{i_2} \dots \lambda_n^{i_n}. \quad (5.7)$$

Define $Z_G: \mathbb{R}^{n+1} \rightarrow \mathbb{R}$ by

$$Z_G(\theta_0, \theta_1, \dots, \theta_n) = \sum_{\mathbf{i} \in \{0,1\}^n} p_i \eta_i \cos \left(\theta_0 + \sum_{k=1}^n i_k \theta_k \right). \quad (5.8)$$

These functions are related by

$$Z_G(\theta_0, \dots, \theta_n) = \operatorname{Re} \left[e^{i\theta_0} P(e^{i\theta_1}, e^{i\theta_2}, \dots, e^{i\theta_n}) \right]. \quad (5.9)$$

$$|P_G(e^{i\theta_1}, \dots, e^{i\theta_n})| = \max_{\theta_0 \in [-\pi, \pi]} Z_G(\theta_0, \dots, \theta_n). \quad (5.10)$$

The functions P_G and Z_G can be used to calculate q_G . This was observed by Werner and Wolf in [Werner and Wolf, 2001]. We sketch a proof here. (For a more detailed proof, see Proposition 1 in [Miller and Shi, 2013].)

Proposition 5.3. *For any nonlocal binary XOR game G , the following equalities hold.*

$$q_G = \max_{|\lambda_1|=\dots=|\lambda_n|=1} |P_G(\lambda_1, \dots, \lambda_n)| \quad (5.11)$$

$$= \max_{\theta_0, \dots, \theta_n \in \mathbb{R}} Z_G(\theta_0, \dots, \theta_n). \quad (5.12)$$

sketch. Let $(\psi, \{M_j^{(i)}\})$ be a qubit strategy for G . By an appropriate choice of basis, we may assume that

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad M_j^{(1)} = \begin{bmatrix} 0 & \zeta_j \\ \bar{\zeta}_j & 0 \end{bmatrix}. \quad (5.13)$$

where $\{\zeta_j\}$ are complex numbers of length 1. The scoring operator \mathbf{M} can be expressed as a reverse diagonal matrix whose entries are

$$\left\{ P_G(\zeta_1^{b_1}, \dots, \zeta_n^{b_n}) \right\}_{(b_1, \dots, b_n) \in \{-1, 1\}^n}. \quad (5.14)$$

The eigenvalues of a reverse diagonal Hermitian matrix whose reverse-diagonal entries are equal to z_1, z_2, \dots, z_{2n} is simply $\pm|z_1|, \pm|z_2|, \dots, \pm|z_n|$. Therefore the operator norm of \mathbf{M} is the maximum absolute value that occurs in (5.14).

The value q_f is the maximum of the operator norm that occurs among all the scoring operators arising from qubit strategies for G . The desired formulas follow. \square

Proposition 5.4. *Let G be a nonlocal binary XOR game. Then, G is a self-test if and only if the following two conditions are satisfied.*

- (A) There is a maximum $(\alpha_0, \dots, \alpha_n)$ for Z_G such that none of $\alpha_1, \dots, \alpha_n$ is a multiple of π .
- (B) Every other maximum of Z_G is congruent modulo 2π to either $(\alpha_0, \dots, \alpha_n)$ or $(-\alpha_0, \dots, -\alpha_n)$.

Proof. See Proposition 2 in [Miller and Shi, 2013]. \square

The following definition will be convenient in later proofs.

Proposition 5.5. *Let G be a nonlocal game which is a self-test. Then, G is **positively aligned** if a maximum for $Z_G(\theta_0, \dots, \theta_n)$ occurs in the region*

$$\{(\theta_0, \dots, \theta_n) \mid 0 < \theta_i < \pi \quad \forall i \geq 1\}. \quad (5.15)$$

For any binary XOR self-test $G = (\{p_i\}, \{\eta_i\})$, we can construct a positively aligned self-test $G' = (\{p'_i\}, \{\eta'_i\})$ by setting $b_1, \dots, b_n \in \{0, 1\}$ so that $b_i = 0$ if Z_G has a maximum with $\theta_i \in (0, \pi)$, and $b_i = 1$ if not, and letting

$$p'_i = p_i \quad (5.16)$$

$$\eta'_i = \eta_{(i+b) \bmod 2}. \quad (5.17)$$

It is easy to see that $q_{G'} = q_G$.

Definition 5.6. *Let $(\psi, \{M_j^{(i)}\})$ and $(\phi, \{N_j^{(i)}\})$ be n -player qubit strategies. Then the **distance** between these two strategies is the quantity*

$$\max \left(\|\psi - \phi\| \cup \left\{ \left\| M_j^{(i)} - N_j^{(i)} \right\| \mid j \in \{1, 2, \dots, n\}, i \in \{0, 1\} \right\} \right). \quad (5.18)$$

(In this formula, the first norm denotes Euclidean distance and second denotes operator norm.) Let G be a self-test. Then, G is a **strong self-test** if there exists a constant K such that any qubit strategy that achieves a score of $q_G - \epsilon$ is within distance $K\sqrt{\epsilon}$ from a qubit strategy that achieves the score q_G .

For any twice differentiable m -variable function $F: \mathbb{R}^m \rightarrow \mathbb{R}$, and any $c = (c_1, \dots, c_m) \in \mathbb{R}^m$, we can define the Hessian matrix for F at c , which is the $m \times m$ matrix formed from the second partial derivatives

$$\frac{\partial^2 F}{\partial x_i \partial x_j}(c_1, \dots, c_m) \quad (5.19)$$

(for $i, j \in \{1, 2, \dots, m\}$).

Proposition 5.7. *Let G be an n -player self-test. Then the following conditions are equivalent.*

1. G is a strong self-test.
2. The function Z_G has nonzero Hessian matrices at all of its maxima.
3. There exists a constant $K > 0$ such that any $(\beta_0, \dots, \beta_n) \in \mathbb{R}^{n+1}$ which satisfies

$$Z_G(\beta_0, \dots, \beta_n) \geq q_G - \epsilon$$

(with $\epsilon \geq 0$) must be within distance $K\sqrt{\epsilon}$ from a maximum of Z_G .

Proof. (1) \iff (2) is Proposition 3 in [Miller and Shi, 2013]. (2) \iff (3) follows from an easy calculus argument. \square

We next prove a proposition and corollary which state consequences of the strong self-testing conditions. These will be the basis for proofs in subsection 5.2.

Proposition 5.8. *Let G be a positively-aligned strong self-test. Let H denote the semicircle $\{e^{i\beta} \mid 0 \leq \beta \leq \pi\} \subseteq \mathbb{C}$. Then, there exists $\alpha \in [-\pi, \pi]$ and $c \geq 0$ such that the set*

$$P_G(H^n) \subseteq \mathbb{C} \quad (5.20)$$

is bounded by the polar curve

$$\begin{aligned} f: [-\pi, \pi] &\rightarrow \mathbb{C} \\ f(\theta) &= (q_G - c(\theta - \alpha)^2)e^{i\theta}. \end{aligned} \quad (5.21)$$

Proof. Since G is positively aligned, we may find a maximum $(\alpha_0, \dots, \alpha_n)$ for Z_G such that $\alpha_1, \dots, \alpha_n \in (0, \pi)$. Choose K according to condition (3) from Proposition 5.7. Let $c = 1/K^2$ and $\alpha = -\alpha_0$.

Suppose, for the sake of contradiction, that there is a point in the set $P_f(H^n)$ which lies outside of (5.21). Then, there exists $\beta_1, \dots, \beta_n \in [0, \pi]$ such that

$$P_f(e^{i\beta_1}, \dots, e^{i\beta_n}) = re^{i\theta} \quad (5.22)$$

(with $\theta \in [-\pi, \pi]$) and

$$r > q_G - c(\theta - \alpha)^2. \quad (5.23)$$

Let $\epsilon = (1/K^2)(\theta - \alpha)^2$. We have

$$Z_G(-\theta, \beta_1, \dots, \beta_n) = r > q_G - c(\theta - \alpha)^2 \quad (5.24)$$

$$= q_G - \epsilon, \quad (5.25)$$

and the distance between $(-\theta, \beta_1, \dots, \beta_n)$ and $(\alpha_0, \dots, \alpha_n)$ is at least $|\theta - \alpha| = K\sqrt{\epsilon}$. (And, it is easy to see that $(-\theta, \beta_1, \dots, \beta_n)$ is not any closer to any of the other maxima of Z_G than it is to $(\alpha_0, \dots, \alpha_n)$.) This contradicts condition (3) of Proposition 5.7. \square

Corollary 5.9. *Let G satisfy the assumptions of Proposition 5.8. Then, there exists a complex number $\gamma \neq 0$ such that for all $\zeta_1, \dots, \zeta_n \in H$,*

$$|P_G(\zeta_1, \dots, \zeta_n) - \gamma| + |\gamma| \leq q_G. \quad (5.26)$$

Proof. Let $R \subseteq \mathbb{C}$ be the region enclosed by the polar curve (5.21). Let $S = \{z \in \mathbb{C} \mid |z| = q_G\}$. We have $S \cap R = \{q_G \cdot e^{i\alpha}\}$. Since the curvature of the curve (5.21) at $e^{i\alpha}$ is strictly greater than $1/q_G$, we can find a circle of radius less than q_G which lies inside of S , which is tangent to S at $q_G \cdot e^{i\alpha}$, and which encloses the region R . Then, if we let γ be the center of this circle, we have $|z - \gamma| + |\gamma| \leq q_G$ for all $z \in R$. The desired inequality follows. \square

5.2 Decomposition Theorems

This subsection proves results on the measurements that are simulated by strong self-tests. For any unit-length complex number ζ , let us write g_ζ for the following modified GHZ state:

$$g_\zeta = \frac{1}{\sqrt{2}} (|00 \dots 0\rangle + \zeta |11 \dots 1\rangle). \quad (5.27)$$

The next theorem uses the canonical form for binary measurements from subsection 3.3. Note that when a collection of four projections $\{P^{(b,c)}\}$ is in canonical form over a space \mathbb{C}^{2^m} , we can naturally express them as operators on $\mathbb{C}^2 \otimes \mathbb{C}^m$ via the isomorphism $\mathbb{C}^{2^m} \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^m$ given by $e_{2k-1} \mapsto e_1 \otimes e_k, e_{2k} \mapsto e_2 \otimes e_k$.

Theorem 5.10. Let $G = (\{p_i\}, \{\eta_i\})$ be a *winnable* n -player self-test which is such that

1. G is positively aligned, and
2. $p_{00\dots 0} > 0$ and $\eta_{00\dots 0} = 1$.

Then, there exists a constant $\delta_G > 0$ such that the following holds. Let $(\Phi, \{M_j^{(i)}\})$ be a quantum strategy whose measurements are in canonical form with underlying space $(\mathbb{C}^2 \otimes W_1) \otimes \dots \otimes (\mathbb{C}^2 \otimes W_n)$. Then the scoring operator \mathbf{M} can be decomposed as

$$\mathbf{M} = \delta_G \mathbf{M}' + (1 - \delta_G) \mathbf{M}'', \quad (5.28)$$

where $\|\mathbf{M}''\| \leq 1$, and

$$\mathbf{M}' = (g_1 g_1^* - g_{-1} g_{-1}^*) \otimes \mathbb{I}_{W_1 \otimes \dots \otimes W_n}. \quad (5.29)$$

Proof. Let

$$T^+ = \left\{ (\theta_0, \dots, \theta_n) \in \mathbb{R}^{n+1} \mid \theta_i > 0 \ \forall i \geq 1 \right\}, \quad (5.30)$$

and

$$T^- = \left\{ (\theta_0, \dots, \theta_n) \in \mathbb{R}^{n+1} \mid \theta_i < 0 \ \forall i \geq 1 \right\}, \quad (5.31)$$

Let q'_G be the maximum value of Z_G that occurs on the set $[-\pi, \pi]^{n+1} \setminus (T^+ \cup T^-)$. By the criteria from Proposition 5.4, this set does not include any of the global maxima for the function Z_G , and so q'_G is strictly smaller than the overall maximum $q_G = 1$. Let

$$\delta_G = \min \{ p_{00\dots 0}, q_G - q'_G \}, \quad (5.32)$$

where $p_{00\dots 0}$ denotes the probability which G associates to the input string $00 \dots 0$.

First let us address the case where $\dim W_j = 1$ for all j . Then

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad (5.33)$$

$$M_j^{(1)} = \begin{bmatrix} 0 & \zeta_j \\ \bar{\zeta}_j & 0 \end{bmatrix}. \quad (5.34)$$

We can compute the scoring operator \mathbf{M} using formula (5.6). When we write this operator as a matrix, using the computational basis for $(\mathbb{C}^2)^{\otimes n}$ in lexicographical order, we obtain a reverse diagonal matrix,

$$\mathbf{M} = \begin{bmatrix} & & & & a_{00\dots 0} \\ & & & a_{00\dots 1} & \\ & & \ddots & & \\ & a_{11\dots 0} & & & \\ a_{11\dots 1} & & & & \end{bmatrix} \quad (5.35)$$

where

$$a_{b_1, \dots, b_n} = P_G(\zeta_1^{(-1)^{b_1}}, \zeta_2^{(-1)^{b_2}}, \dots, \zeta_n^{(-1)^{b_n}}). \quad (5.36)$$

By canonical form, we have $\zeta_j = e^{i\theta_j}$ for some $\theta_j \in [0, \pi]$. Note that can write

$$|a_{b_1, \dots, b_n}| = \max_{\theta_0 \in \mathbb{R}} Z_G(\theta_0, (-1)^{b_1} \theta_1, (-1)^{b_2} \theta_2, \dots, (-1)^{b_n} \theta_n). \quad (5.37)$$

By the definition of q'_G , all of the values $|a_{\mathbf{b}}|$ are bounded by q'_G except possibly $|a_{00\dots 0}|$ and $|a_{11\dots 1}|$, which are both bounded by $q_G = 1$.

We claim that the matrix

$$\mathbf{N} = \begin{bmatrix} & & & & a_{00\dots 0} - \delta_G \\ & & & a_{00\dots 1} & \\ & & \ddots & & \\ & a_{11\dots 0} & & & \\ a_{11\dots 1} - \delta_G & & & & \end{bmatrix} \quad (5.38)$$

which arises from subtracting δ_G from the two corner entries of \mathbf{M} , has operator norm less than or equal to $1 - \delta_G$. Indeed, the operator norm of this Hermitian matrix is the maximum of the absolute values of its entries, and we already know that all of its entries other than its corner entries are bounded by $q'_G \leq 1 - \delta_G$. To show that the absolute values of the corner entries are bounded by $1 - \delta_G$, it suffices to write them out in terms of the parameters of the game G : we have

$$|a_{00\dots 0} - \delta_G| = |P_G(\zeta_1, \dots, \zeta_n) - \delta_G| \quad (5.39)$$

$$= \left| \left(\sum_{\mathbf{i} \in \{0,1\}^n} \eta_{\mathbf{i}} p_{\mathbf{i}} \zeta_1^{i_1} \zeta_2^{i_2} \dots \zeta_n^{i_n} \right) - \delta_G \right| \quad (5.40)$$

$$= \left| (p_0 - \delta_G) + \sum_{\mathbf{i} \neq \mathbf{0}} \eta_{\mathbf{i}} p_{\mathbf{i}} \zeta_1^{i_1} \zeta_2^{i_2} \dots \zeta_n^{i_n} \right| \quad (5.41)$$

$$\leq (p_0 - \delta_G) + \sum_{\mathbf{i} \neq \mathbf{0}} p_{\mathbf{i}} \quad (5.42)$$

$$= 1 - \delta_G, \quad (5.43)$$

and likewise for $(a_{11\dots 1} - \delta_G)$. We conclude that \mathbf{N} has operator norm less than or equal to $1 - \delta_G$. Let $\mathbf{M}'' = \mathbf{N}/(1 - \delta_G)$ and $\mathbf{M}' = (\mathbf{M} - \mathbf{N}')/\delta_G$, and the desired conditions hold.

The proof for the case in which W_1, \dots, W_n are of arbitrary dimension follows by similar reasoning. \square

Theorem 5.11. *Let $G = (\{p_{\mathbf{i}}\}, \{\eta_{\mathbf{i}}\})$ be a strong self-test which is positively aligned. Then, there exist $\delta_G > 0$ and $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ such that the following holds. Let $(\Phi, \{M_j^{(i)}\})$ be a quantum strategy whose measurements are in canonical form with underlying space $(\mathbb{C}^2 \otimes W_1) \otimes \dots \otimes (\mathbb{C}^2 \otimes W_n)$. Then the scoring operator \mathbf{M} can be decomposed as*

$$\mathbf{M} = \delta_G \mathbf{M}' + (q_G - \delta_G) \mathbf{M}'', \quad (5.44)$$

where $\|\mathbf{M}''\| \leq 1$, and

$$\mathbf{M}' = (g_{\alpha} g_{\alpha}^* - g_{-\alpha} g_{-\alpha}^*) \otimes \mathbb{I}_{W_1 \otimes \dots \otimes W_n}. \quad (5.45)$$

Proof. We repeat elements of the proof of Theorem 5.10. It suffices to prove our desired decomposition for the case in which $\dim W_i = 1$ for all i . Let q'_G be the maximum value of Z_G that occurs on the set $[-\pi, \pi]^{n+1} \setminus (T^+ \cup T^-)$ (where T^+ and T^- are defined by (5.30) and (5.31)). Let $\gamma \neq 0$ be the constant that is given by Corollary 5.9, and let

$$\delta_G = \min\{|\gamma|, q_G - q'_G\}. \quad (5.46)$$

We have

$$\mathbf{M} = \begin{bmatrix} & & & & a_{00\dots 0} \\ & & & a_{00\dots 1} & \\ & & \ddots & & \\ & a_{11\dots 0} & & & \\ a_{11\dots 1} & & & & \end{bmatrix} \quad (5.47)$$

where

$$a_{b_1, \dots, b_n} = P_G(\zeta_1^{(-1)^{b_1}}, \zeta_2^{(-1)^{b_2}}, \dots, \zeta_n^{(-1)^{b_n}}). \quad (5.48)$$

for some $\zeta_1, \dots, \zeta_n \in \mathbb{C}$ such that $|\zeta_i| = 1$ and $\text{Im}(\zeta_i) \geq 0$. By Corollary 5.9,

$$|P_G(\zeta_1, \dots, \zeta_n) - \gamma| + |\gamma| \leq q_G, \quad (5.49)$$

and it is easy to see (by the triangle inequality) that for any $c \in [0, 1]$,

$$|P_G(\zeta_1, \dots, \zeta_n) - c\gamma| + |c\gamma| \leq q_G. \quad (5.50)$$

Let

$$\mathbf{N} = \begin{bmatrix} & & & & a_{00\dots 0} - \frac{\delta_G}{|\gamma|} \cdot \gamma \\ & & & a_{00\dots 1} & \\ & & \ddots & & \\ & a_{11\dots 0} & & & \\ a_{11\dots 1} - \frac{\delta_G}{|\gamma|} \cdot \bar{\gamma} & & & & \end{bmatrix} \quad (5.51)$$

The absolute values of the corner entries of this matrix are less than or equal to $q_G - \delta_G$, and the other entries have absolute values less than or equal to $q'_G \leq q_G - \delta_G$. Thus when we set

$$\alpha = \gamma/|\gamma|, \quad (5.52)$$

$$\mathbf{M}' = (g_\alpha g_\alpha^* - g_{-\alpha} g_{-\alpha}^*) \otimes \mathbb{I}_{W_1 \otimes \dots \otimes W_n}, \quad (5.53)$$

$$\mathbf{M}'' = (\mathbf{M} - \delta_G \mathbf{M}') / (q_G - \delta_G), \quad (5.54)$$

the desired result follows. \square

The operator $(g_\alpha g_\alpha^* - g_{-\alpha} g_{-\alpha}^*)$ from the statement of Theorem 5.11 does not describe a projective measurement. It is convenient to have a decomposition theorem involving a projective measurement. This motivates the next result.

We introduce some additional notation. Let

$$\mathbf{b}: \{0, 1, 2, \dots, 2^n - 1\} \rightarrow \{0, 1\}^n \quad (5.55)$$

be the function which maps k to its base-2 representation. For any $\zeta \in \mathbb{C}$ with $|\zeta| = 1$, and any $k \in \{0, 1, 2, \dots, 2^n - 1\}$, let

$$g_{\zeta, k} = \frac{1}{\sqrt{2}} \left(|\mathbf{b}(k)\rangle \langle \mathbf{b}(k)| + \zeta |\overline{\mathbf{b}(k)}\rangle \langle \overline{\mathbf{b}(k)}| \right). \quad (5.56)$$

Theorem 5.12. Let $G = (\{p_i\}, \{\eta_i\})$ be a strong self-test which is positively aligned. Then, there exist $\delta_G > 0$ and $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ such that the following holds. Let $(\Phi, \{M_j^{(i)}\})$ be a quantum strategy whose measurements are in canonical form with underlying space $(\mathbb{C}^2 \otimes W_1) \otimes \dots \otimes (\mathbb{C}^2 \otimes W_n)$. Let $\alpha_0 = \alpha$ and let $\alpha_1, \dots, \alpha_{2^{n-1}-1}$ be any unit-length complex numbers. Then the scoring operator \mathbf{M} can be decomposed as

$$\mathbf{M} = \delta_G \mathbf{M}' + (q_G - \delta_G) \mathbf{M}'', \quad (5.57)$$

where $\|\mathbf{M}''\| \leq 1$, and

$$\mathbf{M}' = \left[\sum_{k=0}^{2^{n-1}-1} (g_{\alpha_k, k} g_{\alpha_k, k}^* - g_{-\alpha_k, k} g_{-\alpha_k, k}^*) \right] \otimes \mathbb{I}_{W_1 \otimes \dots \otimes W_n}. \quad (5.58)$$

Proof. Again it suffices to prove this result for when $\dim W_i = 1$ for all i . Let q'_G be the maximum value of Z_G that occurs on the set $[-\pi, \pi]^{n+1} \setminus (T^+ \cup T^-)$, where T^+ and T^- are defined by (5.30) and (5.31). Let γ be the constant given by Corollary 5.9, let $\alpha = \gamma/|\gamma|$, and let

$$\delta_G = \min\{|\gamma|, (q_G - q'_G)/2\}. \quad (5.59)$$

Write \mathbf{M} as

$$\mathbf{M} = \begin{bmatrix} & & & & a_{00\dots 0} \\ & & & a_{00\dots 1} & \\ & & \ddots & & \\ & a_{11\dots 0} & & & \\ a_{11\dots 1} & & & & \end{bmatrix} \quad (5.60)$$

Let

$$\mathbf{N} = \mathbf{M} - \delta_G \begin{bmatrix} & & & & \alpha_0 \\ & & & \alpha_1 & \\ & & \ddots & & \\ & \alpha_{2^{n-1}-1} & & & \\ \overline{\alpha_1} & & & & \\ \overline{\alpha_0} & & & & \end{bmatrix}, \quad (5.61)$$

The corner entries of \mathbf{N} have absolute value $\leq q_G - \delta_G$ (by Corollary 5.9) and the same holds for the other anti-diagonal entries by the triangle inequality: for any $n \in \{1, 2, \dots, 2^{N-1} - 1\}$,

$$\left| a_{\mathbf{b}(n)} - \delta_G \alpha_n \right| \leq \left| a_{\mathbf{b}(n)} \right| + \delta_G \leq q'_G + (q_G - q'_G)/2 \leq q_G - \delta_G. \quad (5.62)$$

Thus we let $\mathbf{M}''/(q_G - \delta_G)$ and the desired statements hold. \square

6 Randomness Expansion with Partially Trusted Measurements

The goals of this section are to define randomness expansion protocols based on **partially** trusted devices, and then to relate these new protocols to Protocol R.

6.1 Devices with Trusted Measurements

We begin by stating a simple protocol that involves a device with trusted measurements.

Definition 6.1. *A device with trusted measurements consists of the following data.*

1. A single quantum system Q in an initial state Φ .
2. For every pair (\mathbf{i}, \mathbf{o}) of binary strings of equal length, two Hermitian operators $M_{\mathbf{i}, \mathbf{o}}^{(0)}, M_{\mathbf{i}, \mathbf{o}}^{(1)}$ representing the measurements performed on Q when the input and output histories are \mathbf{i} and \mathbf{o} . These operators are assumed to satisfy

$$\left(M_{\mathbf{i}, \mathbf{o}}^{(0)}\right)^2 = \left(M_{\mathbf{i}, \mathbf{o}}^{(1)}\right)^2 = \mathbb{I} \quad (6.1)$$

and

$$M_{\mathbf{i}, \mathbf{o}}^{(0)} M_{\mathbf{i}, \mathbf{o}}^{(1)} = -M_{\mathbf{i}, \mathbf{o}}^{(1)} M_{\mathbf{i}, \mathbf{o}}^{(0)}. \quad (6.2)$$

A trusted measurement device is one whose measurements perfectly anti-commute. A protocol for trusted measurement devices is given in Figure 3. Essentially this protocol is the same as Protocol R, except that we have skipped the process of generating random inputs for the game rounds, and have instead simply used the biased coin flip g itself as input to the device.

6.2 Devices with Partially Trusted Measurements

Definition 6.2. *Let $v \in (0, 1]$ and $h \in [0, 1]$ be real numbers such that $v + h \leq 1$. Then a **partially trusted device with parameters** (v, h) consists of the following data.*

1. A single quantum system Q in an initial state Φ .
2. For every pair (\mathbf{i}, \mathbf{o}) of binary strings of equal length, two Hermitian operators $M_{\mathbf{i}, \mathbf{o}}^{(0)}, M_{\mathbf{i}, \mathbf{o}}^{(1)}$ on Q (representing measurements) that satisfy the following conditions:
 - There exist perfectly anti-commuting measurement pairs $(T_{\mathbf{i}, \mathbf{o}}^{(0)}, T_{\mathbf{i}, \mathbf{o}}^{(1)})$ such that $M_{\mathbf{i}, \mathbf{o}}^{(0)} = T_{\mathbf{i}, \mathbf{o}}^{(0)}$ for all \mathbf{i}, \mathbf{o} , and
 - The operator $M_{\mathbf{i}, \mathbf{o}}^{(1)}$ decomposes as

$$M_{\mathbf{i}, \mathbf{o}}^{(1)} = (v)T_{\mathbf{i}, \mathbf{o}}^{(1)} + (1 - v - h)N_{\mathbf{i}, \mathbf{o}} \quad (6.3)$$

with $\|N_{\mathbf{i}, \mathbf{o}}\| \leq 1$.

The operators $M_{\mathbf{i}, \mathbf{o}}^{(0)}, M_{\mathbf{i}, \mathbf{o}}^{(1)}$ determine the measurements performed by the device on inputs 0 and 1, respectively. Intuitively, a partially trusted device is a device D which always performs a trusted measurement $T^{(0)}$ on input 0, and on input 1, selects one of the three operators $(T^{(1)}, N, 0)$ at random according to the probability distribution $(v, 1 - v - h, h)$.

We will call the parameter v the **trust coefficient**, and we will call h the **coin flip coefficient**. The parameter h measures the extent to which the output of D on input 1 is determined by a fair coin flip. Note that when the input to the device D is 1, then the probability that D gives an output of 1 is necessarily between $h/2$ and $(1 - h/2)$.

Figure 4 gives a randomness expansion protocol for partially trusted devices. It is the same as Protocol A, except that the trusted device has been replaced by a partially trusted device.

Protocol A:

Arguments:

N = positive integer
 $q \in (0, 1)$
 $\eta \in (0, 1/2)$
 D = device with trusted measurements

1. A bit $g \in \{0, 1\}$ is chosen according to a biased $(1 - q, q)$ distribution. The bit g is given to D as input, and an output bit o is recorded.
2. If $g = 1$ and the output given by D is 0, then the event P (“pass”) is recorded. If $g = 1$ and the output is 1, the event F (“fail”) is recorded.
3. If $g = 0$ and the output given by D is 0, then the event H (“heads”) is recorded. If $g = 0$ and the output is 1, the event T (“tails”) is recorded.
4. Steps 1 – 3 are repeated $N - 1$ (more) times. Bit sequences $\mathbf{g} = (g_1, \dots, g_N)$ and $\mathbf{o} = (o_1, \dots, o_N)$ are obtained.
5. If the total number of failures is more than $\eta q N$, the protocol **aborts**. Otherwise, the protocol **succeeds**. If the protocol succeeds, it outputs the bit sequences \mathbf{g} and \mathbf{o} .

Figure 3: A randomness expansion protocol for a trusted measurement device.

Protocol A':*Arguments:*

- v = real number such that $v \in (0, 1]$.
- h = real number such that $h \in [0, 1 - v]$.
- N = positive integer
- $q \in (0, 1)$
- $\eta \in (0, v/2)$
- D = partially trusted device with parameters (v, h) .

1. A bit $g \in \{0, 1\}$ is chosen according to a biased $(1 - q, q)$ distribution. The bit g is given to D as input, and the output bit o is recorded.
2. If $g = 1$ and the output given by D is 0, then the event P ("pass") is recorded. If $g = 1$ and the output is 1, the event F ("fail") is recorded.
3. If $g = 0$ and the output given by D is 0, then the event H ("heads") is recorded. If $g = 0$ and the output is 1, the event T ("tails") is recorded.
4. Steps 1 – 3 are repeated $N - 1$ (more) times. Bit sequences $\mathbf{g} = (g_1, \dots, g_N)$ and $\mathbf{o} = (o_1, \dots, o_N)$ are obtained.
5. If the total number of failures is greater than $(h/2 + \eta)qN$, then the protocol **aborts**. Otherwise, the protocol **succeeds**. If the protocol succeeds, it outputs the bit sequences \mathbf{g} and \mathbf{o} .

Figure 4: A randomness expansion protocol for a partially trusted device.

6.3 Entanglement with a Partially Trusted Measurement Device

Suppose that D is a partially trusted measurement device (see Definition 6.2) with parameters (v, h) . Suppose that E is a quantum system that is entangled with D , and let $\rho = \rho_E$ denote the initial state of E . We will use the following notation: let ρ_+ and ρ_- denote the subnormalized operators which represent the states of E when the input bit is 0 and the output bit is 0 or 1, respectively. Let ρ_P and ρ_F denote the operators which represent an input of 1 and an output of 0 or 1, respectively. Also (using notation from Definition 6.2), let us write ρ_0 and ρ_1 denote the states of E that would occur if the trusted measurement $T^{(1)}$ was applied to Q (instead of the partially trusted measurement $M^{(1)}$). (Note that $T^{(1)}$ is perfectly anticommuting with $M^{(0)}$.)

The following proposition expresses the possible behavior of the system E .

Proposition 6.3. *Let $v \in (0, 1]$ and $h \in [0, 1]$ be such that $v + h \leq 1$. Let D be a partially trusted device with parameters (v, h) , let E be a quantum system that is entangled with D , and let $\rho = \rho_E$. Then,*

$$(h/2)\rho + v\rho_0 \leq \rho_P \leq (1 - h/2)\rho - v\rho_1 \quad (6.4)$$

and

$$(h/2)\rho + v\rho_1 \leq \rho_F \leq (1 - h/2)\rho - v\rho_0. \quad (6.5)$$

Proof. Let N be the measurement operator from the decomposition of $M^{(1)}$ given in Definition 6.2. Let ρ' be the subnormalized operator on E which denotes the state that would be produced if N were applied to Q and the outcome were 0. Clearly, $0 \leq \rho' \leq \rho$. From the decomposition (6.3), ρ_P is a convex combination of the operators ρ_0 , ρ' and $(\rho/2)$:

$$\rho_P = v\rho_0 + (1 - v - h)\rho' + h(\rho/2). \quad (6.6)$$

Since $\rho' \leq \rho$, we have

$$\rho_P \leq v\rho_0 + (1 - v - h)\rho + h(\rho/2) \quad (6.7)$$

$$= v\rho_0 + (1 - v - h/2)\rho \quad (6.8)$$

$$= (1 - h/2)\rho + v(\rho_0 - \rho) \quad (6.9)$$

$$= (1 - h/2)\rho - v\rho_1. \quad (6.10)$$

The other inequalities follow similarly. \square

6.4 Simulation

To any binary XOR game G , we have associated three quantities: q_G , w_G , and f_G . These are respectively the optimal quantum score, optimal quantum winning probability, and least quantum failure probability for G . The quantities are related by $w_G = (1 + q_G)/2$ and $f_G = 1 - w_G$.

Theorem 6.4. *For any n -player strong self-test G which is positively aligned, there exists $\delta_G > 0$ such that the following holds. For any any n -part binary quantum device D , there exists a partially trusted device D' with parameters q_G, δ_G such that Protocol A' (with arguments $\delta_G, 2f_G, N, q, \eta, D'$) simulates Protocol R (with arguments N, η, q, G, D).*

Proof. Choose δ_G according to Theorem 5.12.

Consider the behavior of the device D in the first round. We may assume that the measurements performed by D_1, \dots, D_n are in canonical form. Write the underlying space as $(\mathbb{C}^2 \otimes W_1) \otimes \dots \otimes (\mathbb{C}^2 \otimes W_n)$. If $g = 0$, the measurement performed by D_1 is given by the operator

$$\begin{bmatrix} & & & 1 \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{bmatrix} \otimes \mathbb{I}_{W_1 \otimes \dots \otimes W_n} \quad (6.11)$$

(where the matrix on the left is an operator on $(\mathbb{C}^2)^{\otimes n}$, with the basis taken in lexicographic order as usual).

If $g = 1$ the measurement performed by D is given by the scoring operator \mathbf{M} . Theorem 5.12 guarantees that for some unit-length complex number α , and for any choices of unit-length complex numbers $\alpha_1, \dots, \alpha_{2^{n-1}-1}$, there is a decomposition for \mathbf{M} in the form $\mathbf{M} = \delta_G \mathbf{M}' + (q_G - \delta_G) \mathbf{M}''$ with

$$\mathbf{M}' = \begin{bmatrix} & & & & \alpha \\ & & & \alpha_1 & \\ & & & & \ddots \\ & & & & & \alpha_{2^{n-1}-1} \\ & & & \overline{\alpha_{2^{n-1}-1}} & \\ & & & & \ddots \\ & & & & & \overline{\alpha_1} \\ & & & & & & \overline{\alpha} \end{bmatrix} \otimes \mathbb{I}_{W_1 \otimes \dots \otimes W_n}$$

and $\|\mathbf{M}''\| \leq 1$. To simulate the behavior of D with a partially trusted device, we need only choose $\alpha_1, \dots, \alpha_{2^{n-1}-1}$ so that \mathbf{M}' is perfectly anti-commutative with the operator 6.11. This can be done, for example, by setting $\alpha_1, \alpha_2, \dots, \alpha_{2^{n-2}-1}$ to be equal to α , and $\alpha_{2^{n-2}}, \dots, \alpha_{2^{n-1}-1}$ to be equal to $-\alpha$. Thus the behavior of the device D in the first round of Protocol R can be simulated by a partially trusted device with parameters $(\delta_G, 1 - q_G) = (\delta_G, 2f_G)$. Similar reasoning shows the desired simulation result across all rounds. \square

The following corollary is easy to prove.

Corollary 6.5. *Theorem 6.4 holds true without the assumption that G is positively aligned.* \square

Essentially, the above corollary implies that any security result for Protocol A' can be converted immediately into an identical security result for Protocol R. This will be the basis for our eventual full proof of randomness expansion.

7 The Proof of Security for Partially Trusted Devices

In this section we provide the proof of security for Protocol A' (see Figure 4). Our approach, broadly stated, is as follows: we show the existence of a function $T(v, h, \eta, q, \kappa)$ which provides

$N \in \mathbb{N}$	number of rounds
$q \in (0, 1)$	test probability
$t \in [0, 1]$	failure parameter
$v \in (0, 1]$	trust coefficient
$h \in [0, 1 - v]$	coin flip coefficient
$\eta \in (0, v/2)$	error tolerance
$\kappa \in (0, \infty)$	failure penalty
$r \in (0, 1/(q\kappa)]$	multiplier for Rényi coefficient
$\epsilon \in (0, \sqrt{2}]$	error parameter for smooth min-entropy

Figure 5: Variables used in section 7.

a lower bound on the linear rate of entropy of the protocol. (The variables v, h, η, q are from the protocol, and κ is a positive constant that can be chosen to be arbitrarily small.) The main point of our proofs is that, although T depends on several variables, it does *not* depend on the particular device used in Protocol A' . Thus, we have a uniform security result.

The definition of T is multi-layered and is developed over the course of the section. For the reader's convenience, we have collected all the definitions of the functions that we use, including T , in appendix subsection A.3. The full expression for T is quite complicated, but for our purposes it suffices to calculate the limit $\lim_{(q, \kappa) \rightarrow (0, 0)} T(v, h, \eta, q, \kappa)$, since this will tell us what rate Protocol A' approaches when q is small. This limit will be shown to be equal to $\pi(\eta/v)$, where π denotes the function from Theorem 4.2.

Our proof involves several parameters. For convenience, we include a table here which assigns a name to each parameter (Figure 5.)

To avoid unnecessary repetition, we will use the following conventions in this section.

- Unless otherwise stated, we will assume that the variables from Figure 5 are always restricted to the domains given. (The reader can assume that all unquantified statements are prefaced by, “for all $q \in (0, 1]$, all $\epsilon \in (0, \sqrt{2}]$,” etc.) If we say “ $F(q, \kappa)$ is a real-valued function,” we mean that it is a real valued function on $(0, 1) \times (0, \infty)$. If we say “let $x = \kappa q$,” we mean that x is a real valued function on $(0, 1) \times (0, \infty)$ defined by $x(\kappa, q) = \kappa q$. If the domain of one parameter of a function depends on another variable (as can occur, e.g., for the variable h) we always include the other variable as a parameter of the function.
- When we discuss a single iteration of Protocol A' , will use notation from subsection 6.3: If D is a partially trusted measurement device, and E is a purifying system for D with initial state $\rho = \rho_E$, then $\rho = \rho_H + \rho_T$ and $\rho = \rho_P + \rho_F$ denote the decompositions that occur for a single use of the device on input 0 and 1, respectively. We denote by $\rho_+, \rho_-, \rho_0, \rho_1$ the respective states that would occur if the corresponding fully trusted measurements were used instead. (Note that $\rho_H = \rho_+$ and $\rho_T = \rho_-$.) Let $\bar{\rho}$ denote the operator on $E \oplus E \oplus E \oplus E$ given by

$$\bar{\rho} = (1 - q)\rho_H \oplus (1 - q)\rho_T \oplus q\rho_P \oplus q\rho_F. \quad (7.1)$$

This operator represents the state of E taken together with the input bit and output bit from the first iteration of Protocol A' .

- When we discuss multiple iterations of Protocol A' , we will use the following notation: let G and O denote classical registers which consist of the bit sequences $\mathbf{g} = (g_1, \dots, g_N)$ and

$\mathbf{o} = (o_1, \dots, o_n)$, respectively. We denote basis states for the joint system GO by $|\mathbf{go}\rangle$. We denote the joint state of the system EGO at the conclusion of Protocol A' by Γ_{EGO} .

- If D is a partially trusted measurement device, E is a purifying system, and $\alpha > 0$, then we refer to the quantity

$$\frac{\text{Tr}(\rho_1^\alpha)}{\text{Tr}(\rho^\alpha)} \in [0, 1] \quad (7.2)$$

as the α -**failure parameter** of D . (Note that we used the operator ρ_1 in the above expression, *not* the operator ρ_F . This parameter measures “honest” failures only.)

- Let $\Pi(x, y)$ and $\pi(y)$ denote the functions from Theorem 4.2.

7.1 Proof Idea

Let D be a partially trusted measurement device with parameters v, h , and let E be a purifying system with initial state ρ . Let $\bar{\rho}$ be the operator on $E \oplus E \oplus E \oplus E$ which represents the joint state of E together with the input and output of a single iteration of Protocol A' :

$$\bar{\rho} = (1 - q)\rho_H \oplus (1 - q)\rho_T \oplus q\rho_P \oplus q\rho_F. \quad (7.3)$$

We wish to show that the state $\bar{\rho}$ is more random than the original state ρ . Therefore, we wish to show that the ratio

$$\frac{d_{1+\gamma}(\bar{\rho} \parallel \bar{\sigma})}{d_{1+\gamma}(\rho \parallel \sigma)}, \quad (7.4)$$

for some appropriate $\gamma, \sigma, \bar{\sigma}$, is significantly smaller than 1. For simplicity, we will for the time being take $\sigma = \mathbb{I}$ for the initial bounding operator. (Later in this section we will generalize this choice.)

A natural choice of bounding operator for $\bar{\rho}$ would be

$$(1 - q)\mathbb{I} \oplus (1 - q)\mathbb{I} \oplus q\mathbb{I} \oplus q\mathbb{I}. \quad (7.5)$$

Computing $d_{1+\gamma}(\bar{\rho} \parallel \cdot)$ with this bounding operator would yield

$$\left\{ (1 - q)\text{Tr}[\rho_+^{1+\gamma}] + (1 - q)\text{Tr}[\rho_-^{1+\gamma}] + q\text{Tr}[\rho_P^{1+\gamma}] + q\text{Tr}[\rho_F^{1+\gamma}] \right\}^{1/\gamma} \quad (7.6)$$

Computing this quantity would have the effect, roughly speaking, of measuring the randomness of the output bit of Protocol A' conditioned on E and on the input bit g . However this is not adequate for our purposes, since it treats “passing” rounds the same as “failing” rounds, and does not take into account that the device is only allowed a limited number of failures. (And indeed, this measurement of randomness does not work: if D performs anticommuting measurements on a half of a maximally entangled qubit pair, the divergence quantity $d_{1+\gamma}(\bar{\rho} \parallel \cdot)$ with bounding operator (7.5) is the same as $d_{1+\gamma}(\rho \parallel \mathbb{I})$.)

We will use a slightly different expression to measure the output of Protocol A' . We introduce a single coefficient $2^{-\kappa}$ (with $\kappa > 0$) into the fourth term of the expression:

$$\left\{ (1 - q)\text{Tr}[\rho_+^{1+\gamma}] + (1 - q)\text{Tr}[\rho_-^{1+\gamma}] + q\text{Tr}[\rho_P^{1+\gamma}] + q2^{-\kappa}\text{Tr}[\rho_F^{1+\gamma}] \right\}^{1/\gamma} \quad (7.7)$$

The reason for the introduction of the coefficient $2^{-\kappa}$ is this: in effect, if a game round occurs and the device fails, we lower our expectation for the amount of randomness produced. The quantity (7.7) is equal to $d_{1+\gamma}(\bar{\rho}||\bar{\sigma})$ where

$$\bar{\sigma} = (1-q)\mathbb{I} \oplus (1-q)\mathbb{I} \oplus q\mathbb{I} \oplus q2^{\kappa/\gamma}\mathbb{I}. \quad (7.8)$$

Having chosen the bounding operator $\bar{\sigma}$, we need only to choose the coefficient $\gamma \in (0, 1]$. We will take γ to be of the form $\gamma = rq\kappa$, where $r \in (0, 1/(q\kappa)]$.⁴ (Expressing γ this way enables clean calculations in our proofs.)

The proof proceeds by showing an upper bound on (7.4), then applying induction to get a similar upper bound for N uses of the device, and then applying the relationship between Renyi divergence and smooth min-entropy to get a lower bound on the number of extractable bits produced by Protocol A' .

7.2 One-Shot Results

We begin by proving a one-shot security result under the assumption that some limited information about the device is available.

Proposition 7.1. *There is a continuous real-valued function $\Lambda(v, h, q, \kappa, r, t)$ such that the following conditions hold.*

1. *Let D be a partially trusted measurement device with parameters (v, h) , and let E be a purifying system for D . Let $\gamma = rq\kappa$, and let*

$$\bar{\sigma} = (1-q)\mathbb{I} \oplus (1-q)\mathbb{I} \oplus q\mathbb{I} \oplus q2^{\kappa/\gamma}\mathbb{I}. \quad (7.9)$$

Then,

$$d_{1+\gamma}(\bar{\rho}||\bar{\sigma}) \leq 2^{-\Lambda(v, h, q, \kappa, r, t)} \cdot d_{1+\gamma}(\rho||\mathbb{I}), \quad (7.10)$$

where $t = \text{Tr}(\rho_1^{1+\gamma})/\text{Tr}(\rho^{1+\gamma})$ denotes the $(1+\gamma)$ -failure parameter of D .

2. *The following limit condition is satisfied: for any $t_0 \in [0, 1]$,*

$$\lim_{(q, \kappa, t) \rightarrow (0, 0, t_0)} \Lambda(v, h, q, \kappa, r, t) = \pi(t_0) + \frac{h/2 + vt_0}{r}, \quad (7.11)$$

where π is the function from Theorem 4.2.

Proof. We have

$$d_{1+\gamma}(\bar{\rho}||\bar{\sigma}) = \left\{ (1-q)\text{Tr}[\rho_+^{1+\gamma}] + (1-q)\text{Tr}[\rho_-^{1+\gamma}] + q\text{Tr}[\rho_P^{1+\gamma}] + q2^{-\kappa}\text{Tr}[\rho_F^{1+\gamma}] \right\}^{1/\gamma} \quad (7.12)$$

We will compute a bound on this quantity by grouping the first and second summands together, and then by grouping the third and fourth summands together. Note that by Theorem 4.2, we have

$$\text{Tr}[\rho_+^{1+\gamma}] + \text{Tr}[\rho_-^{1+\gamma}] \leq 2^{-\gamma\Pi(\gamma, t)}\text{Tr}[\rho^{1+\gamma}] \quad (7.13)$$

⁴The reason for this choice of interval for r is that we need $\gamma \leq 1$ for the application of results from section 3.2.

Now consider the sum $\text{Tr}[\rho_P^{1+\gamma}] + 2^{-\kappa}\text{Tr}[\rho_F^{1+\gamma}]$. By superadditivity (see Proposition 3.1),

$$\text{Tr}[\rho_P^{1+\gamma}] + 2^{-\kappa}\text{Tr}[\rho_F^{1+\gamma}] = \text{Tr} \left[2^{-\kappa}(\rho_P^{1+\gamma} + \rho_F^{1+\gamma}) + (1 - 2^{-\kappa})\rho_P^{1+\gamma} \right] \quad (7.14)$$

$$\leq \text{Tr} \left[2^{-\kappa}\rho^{1+\gamma} + (1 - 2^{-\kappa})\rho_P^{1+\gamma} \right]. \quad (7.15)$$

By Proposition 6.3,

$$\text{Tr}[\rho_P^{1+\gamma}] + 2^{-\kappa}\text{Tr}[\rho_F^{1+\gamma}] \leq \text{Tr} \left\{ 2^{-\kappa}\rho^{1+\gamma} + (1 - 2^{-\kappa})[\rho - (h/2)\rho - v\rho_1]^{1+\gamma} \right\}. \quad (7.16)$$

Applying the rule $\text{Tr}[(X - Y)^{1+\gamma}] \leq \text{Tr}[X^{1+\gamma}] - \text{Tr}[Y^{1+\gamma}]$, followed by the fact that $\text{Tr}[\rho_1^{1+\gamma}] = t\text{Tr}[\rho^{1+\gamma}]$, we have the following:

$$\begin{aligned} \text{Tr}[\rho_P^{1+\gamma}] + 2^{-\kappa}\text{Tr}[\rho_F^{1+\gamma}] &\leq \text{Tr} \left\{ 2^{-\kappa}\rho^{1+\gamma} + (1 - 2^{-\kappa})[\rho^{1+\gamma} - (h/2)^{1+\gamma}\rho^{1+\gamma} - v^{1+\gamma}\rho_1^{1+\gamma}] \right\} \\ &= \text{Tr} \left\{ 2^{-\kappa}\rho^{1+\gamma} + (1 - 2^{-\kappa})[\rho^{1+\gamma} - (h/2)^{1+\gamma}\rho^{1+\gamma} - v^{1+\gamma}t\rho^{1+\gamma}] \right\} \\ &= \left\{ 2^{-\kappa} + (1 - 2^{-\kappa})[1 - (h/2)^{1+\gamma} - v^{1+\gamma}t] \right\} \text{Tr}[\rho^{1+\gamma}] \end{aligned} \quad (7.17)$$

$$= \left\{ 1 - (1 - 2^{-\kappa})[(h/2)^{1+\gamma} + v^{1+\gamma}t] \right\} \text{Tr}[\rho^{1+\gamma}]. \quad (7.18)$$

Combining (7.12), (7.13), and (7.18), we find the following: if we set

$$\lambda(v, h, q, \kappa, r, t) = \left((1 - q)2^{-\gamma\Pi(\gamma, t)} + q \left\{ 1 - (1 - 2^{-\kappa})[(h/2)^{1+\gamma} + v^{1+\gamma}t] \right\} \right)^{1/\gamma},$$

then

$$d_{1+\gamma}(\bar{\rho} \parallel \bar{\sigma}) \leq \lambda(v, h, q, \kappa, r, t) \cdot d_{1+\gamma}(\rho \parallel \mathbb{I}). \quad (7.19)$$

Therefore setting $\Lambda = -\log \lambda$ yields (7.10).

It remains for us to evaluate the limiting behavior of Λ as $(q, \kappa, t) \rightarrow (0, 0, t_0)$. We can rewrite the formula for λ as

$$\lambda(v, h, q, \kappa, r, t) = \left(1 + \left\{ (1 - q)(2^{-\gamma\Pi(\gamma, t)} - 1) + q(2^{-\kappa} - 1)[(h/2)^{1+\gamma} + v^{1+\gamma}t] \right\} \right)^{1/\gamma}$$

Applying Proposition A.7 to this expression (with $g = \gamma$, and f equal to the function enclosed by braces), we have

$$\begin{aligned} &\ln \left[\lim_{(q, \kappa, t) \rightarrow (0, 0, t_0)} \lambda(v, h, q, \kappa, r, t) \right] \\ &= \lim_{(q, \kappa, t) \rightarrow (0, 0, t_0)} \left\{ (1 - q) \left(\frac{2^{-\gamma\Pi(\gamma, t)} - 1}{\gamma} \right) + \left(\frac{q(2^{-\kappa} - 1)}{\gamma} \right) [(h/2)^{1+\gamma} + v^{1+\gamma}t] \right\} \\ &= (1)(-\ln 2)\pi(t_0) + (-\ln 2)(r^{-1})[(h/2) + vt_0], \end{aligned}$$

which implies (7.11) as desired. \square

Proposition 7.1 is not sufficient for our ultimate proof of security because it assumes that additional information (beyond the trust parameters v, h) is known about the device D . The next proposition avoids this limitation. (It makes no use of the failure parameters of the device.)

Proposition 7.2. *There is a continuous real-valued function $\Delta(v, h, q, \kappa, r)$ such that the following conditions hold.*

1. *Let D be a partially trusted measurement device with parameters (v, h) , and let E be a purifying system for D . Let $\gamma = rq\kappa$, and let*

$$\bar{\sigma} = (1 - q)\mathbb{I} \oplus (1 - q)\mathbb{I} \oplus q\mathbb{I} \oplus q2^{\kappa/\gamma}\mathbb{I}. \quad (7.20)$$

Then,

$$d_{1+\gamma}(\bar{\rho} \parallel \bar{\sigma}) \leq 2^{-\Delta(v, h, q, \kappa, r)} \cdot d_{1+\gamma}(\rho \parallel \mathbb{I}). \quad (7.21)$$

2. *The following limit condition is satisfied:*

$$\lim_{(q, \kappa) \rightarrow (0, 0)} \Delta(v, h, q, \kappa, r) = \min_{s \in [0, 1]} \left(\pi(s) + \frac{h/2 + vs}{r} \right), \quad (7.22)$$

where π is the function from Theorem 4.2.

Proof. Let Λ be the function from Proposition 7.1, and let

$$\Delta(v, h, q, \kappa, r) = \min_{t \in [0, 1]} \Lambda(v, h, q, \kappa, r, t). \quad (7.23)$$

Clearly, (7.21) holds by Proposition 7.1. Equality (7.22) follows via Proposition A.8. \square

7.3 Multi-Shot Results

The goal of this subsection is to deduce consequences of Proposition 7.2 across multiple iterations. Let Γ_{EGO} denote the joint state of the registers E , G , and O . (Note that Γ is a classical-quantum state with respect to the partition $(GO|E)$.)

The following proposition follows immediately from Proposition 7.2 by induction.

Proposition 7.3. *Let D be a partially trusted measurement device with parameters (v, w) , and let E be a purifying system for D . Let $\gamma = rq\kappa$, and let Φ be the operator on $E \otimes G \otimes O$ given by*

$$\Phi = \mathbb{I}_E \otimes \left(\sum_{\mathbf{g}, \mathbf{o} \in \{0, 1\}^N} (1 - q)^{\sum_i (1 - g_i)} q^{\sum_i g_i} 2^{(\sum_i g_i o_i) / (qr)} |\mathbf{go}\rangle \langle \mathbf{go}| \right). \quad (7.24)$$

Then,

$$D_{1+\gamma}(\Gamma_{EGO} \parallel \Phi) \leq D_{1+\gamma}(\Gamma_E \parallel \mathbb{I}) - N \cdot \Delta(v, h, q, \kappa, r), \quad (7.25)$$

where Δ denotes the function from Proposition 7.2. \square

We note the significance of the exponents in (7.24): the quantity $\sum_{i=1}^N (1 - g_i)$ is the number of generation rounds that occurred in Protocol A', the quantity $\sum_{i=1}^N g_i$ is the number of game rounds, and the quantity $\sum_{i=1}^N g_i o_i$ is the number of times the “failure” event occurred during the protocol.

As stated, Proposition 7.3 is not useful for bounding the randomness of Γ_{EGO} because the quantity $D_{1+\gamma}(\Gamma_E \parallel \mathbb{I})$ could be arbitrarily large. We therefore prove the following alternate version of the proposition. The statement is the same, except that we replace \mathbb{I}_E in (7.24) with Γ_E , and we remove the term $D_{1+\gamma}(\Gamma_E \parallel \mathbb{I})$ from (7.25).

Proposition 7.4. Let D be a partially trusted measurement device with parameters (v, w) , and let E be a purifying system for D . Let $\gamma = rq\kappa$, and let Σ be the operator on $E \otimes G \otimes O$ given by

$$\Sigma = \Gamma_E \otimes \left(\sum_{\mathbf{g}, \mathbf{o} \in \{0,1\}^N} (1-q)^{\sum_i (1-g_i)} q^{\sum_i g_i} 2^{(\sum_i g_i o_i)/(qr)} |\mathbf{go}\rangle \langle \mathbf{go}| \right). \quad (7.26)$$

Then,

$$D_{1+\gamma}(\Gamma_{EGO} \|\Sigma) \leq -N \cdot \Delta(v, h, q, \kappa, r), \quad (7.27)$$

where Δ denotes the function from Proposition 7.2.

Proof. Let $\Gamma = \Gamma_E$. Let (D, E') be the device-environment pair that arises from taking the pair (D, E) and applying the stochastic operation

$$X \mapsto \Gamma^{\frac{-\gamma}{2+2\gamma}} X \Gamma^{\frac{-\gamma}{2+2\gamma}} \quad (7.28)$$

to the system E . The state $\Gamma_{E'}$ of the resulting system E' satisfies

$$\Gamma_{E'} = \frac{\Gamma^{1/(1+\gamma)}}{K}, \quad (7.29)$$

where $K = \text{Tr}(\Gamma^{1/(1+\gamma)})$.

By directly applying the definition of D_α (see Definition 3.2) we can see that certain divergences of Γ_{EGO} and $\Gamma_{E'GO}$ can be computed from one another:

$$D_{1+\gamma}(\Gamma_{E'GO} \|\Phi) = -\frac{1+\gamma}{\gamma} \cdot \log K + D_{1+\gamma}(\Gamma_{EGO} \|\Sigma) \quad (7.30)$$

$$D_{1+\gamma}(\Gamma_{E'} \|\mathbb{I}) = -\frac{1+\gamma}{\gamma} \cdot \log K + D_{1+\gamma}(\Gamma_E \|\Gamma). \quad (7.31)$$

Applying Proposition 7.3 to (D, E') , we find that

$$D_{1+\gamma}(\Gamma_{E'GO} \|\Phi) - D_{1+\gamma}(\Gamma_{E'} \|\mathbb{I}) \leq -N\Delta(v, h, q, \kappa, r). \quad (7.32)$$

By (7.30)–(7.31), the same bound holds when E', Φ, \mathbb{I} are replaced E, Σ, Γ . Since $D_{1+\gamma}(\Gamma_E \|\Gamma) = 0$, the desired inequality is obtained. \square

The following corollary of Proposition 7.4 provides final preparation for the proof of the main result.

Corollary 7.5. Let $\epsilon > 0$. Then, there exists a positive semidefinite operator $\bar{\Gamma}_{EGO}$ which is classical with respect to the systems E and G such that

$$\|\bar{\Gamma}_{EGO} - \Gamma_{EGO}\|_1 \leq \epsilon \quad (7.33)$$

and

$$D_{\max}(\bar{\Gamma}_{EGO} \|\Sigma) \leq -N \cdot \Delta(v, h, q, \kappa, r) + \frac{\log(2/\epsilon^2)}{q\kappa r} \quad (7.34)$$

(where Δ and Σ are as in Proposition 7.2 and Proposition 7.4, respectively).

Proof. This follows from Proposition 3.5. \square

7.4 The Security of Protocol A'

Let s denote the event that Protocol A' succeeds, and let Γ_{EGO}^s denote the corresponding (subnormalized) operator on $E \otimes G \otimes O$.

Proposition 7.6. *There exists a continuous real-valued function $R(v, h, \eta, q, \kappa, r)$ such that the following holds.*

1. Let $\epsilon > 0$. If Protocol A' is executed with parameters (v, h, N, q, η, D) , then

$$H_{min}^\epsilon(\Gamma_{EGO}^s | EG) \geq N \cdot R(v, h, \eta, q, \kappa, r) - \frac{\log(2/\epsilon^2)}{q\kappa r}. \quad (7.35)$$

2. The following equality holds:

$$\lim_{(q, \kappa) \rightarrow (0, 0)} R(v, h, \eta, q, \kappa, r) = \min_{s \in [0, 1]} \left[\pi(s) + \frac{vs - \eta}{r} \right] \quad (7.36)$$

Proof. The “success” event for Protocol A' is defined by the inequality

$$\sum_i g_i o_i \leq (h/2 + \eta)qN. \quad (7.37)$$

Let $S \subseteq G \otimes O$ be the span of the vectors $|\mathbf{go}\rangle$ where (\mathbf{g}, \mathbf{o}) varies over all pairs of sequences satisfying (7.37). For any operator X on $E \otimes G \otimes O$ which is classical-quantum with respect to $(GO|E)$, let X^s denote the restriction of X to $E \otimes S$. Applying this construction to the operators $\Gamma_{EGO}, \bar{\Gamma}_{EGO}$ and Σ from Corollary 7.5, and using the fact that D_{max} and $\|\cdot\|_1$ are monotonically decreasing under restriction to S , we find that

$$D_{max}^\epsilon(\Gamma_{EGO}^s \| \Sigma^s) \leq -N \cdot \Delta(v, h, q, \kappa, r) + \frac{\log(2/\epsilon^2)}{q\kappa r}. \quad (7.38)$$

In order to give a lower bound on the smooth min-entropy of Γ_{EGO}^s , we need to compute its divergence with respect to an operator on $E \otimes G \otimes O$ that is of the form $X \otimes \mathbb{I}_O$, where X is a density matrix. Define a new operator Σ' on $E \otimes G \otimes O$ by

$$\Sigma' = \Gamma_E \otimes \left(\sum_{(\mathbf{g}, \mathbf{o}) \in S} (1 - q)^{\sum_i (1 - g_i)} q^{\sum_i g_i} 2^{(h/2 + \eta)N/r} |\mathbf{go}\rangle \langle \mathbf{go}| \right) \quad (7.39)$$

(recalling that $\gamma = q\kappa r$). Comparing this definition with (7.26) and using the success criterion (7.37), we find that $\Sigma' \geq \Sigma^s$. Therefore, the bound in (7.38) holds also when Σ^s is replaced by Σ' .

When we let Ψ be the operator on $E \otimes G$ defined by

$$\Psi = \Gamma_E \otimes \sum_{\mathbf{g} \in \{0, 1\}^N} (1 - q)^{\sum_i (1 - g_i)} q^{\sum_i g_i} |\mathbf{g}\rangle \langle \mathbf{g}| \quad (7.40)$$

and rewrite Σ' as

$$\Sigma' = 2^{(h/2 + \eta)N/r} (\Psi \otimes \mathbb{I}_O), \quad (7.41)$$

we find (using the rule $D_{\max}^\epsilon(X\|Y) = \log c + D_{\max}^\epsilon(X\|cY)$) that

$$D_{\max}^\epsilon(\Gamma_{\text{EGO}}^s\|\Psi \otimes \mathbb{I}_O) \leq (h/2 + \eta)N/r - N \cdot \Delta(v, h, q, \kappa, r) + \frac{\log(2/\epsilon^2)}{q\kappa r}.$$

Since Ψ is a density matrix, we have

$$H_{\min}^\epsilon(\Gamma_{\text{EGO}}^s \mid EG) \geq -D_{\max}^\epsilon(\Gamma_{\text{EGO}}^s\|\Psi \otimes \mathbb{I}_O). \quad (7.42)$$

Therefore if we let

$$R(v, h, \eta, q, \kappa, r) = -\frac{h/2 + \eta}{r} + \Delta(v, h, q, \kappa, r), \quad (7.43)$$

condition 1 of the theorem is fulfilled. Condition 2 follows easily from the formula for the limit of Δ (7.22). \square

A final improvement can be made on the previous result by optimizing the coefficient r .

Theorem 7.7. *There exist continuous real-valued functions $T(v, h, \eta, q, \kappa)$ and $F(v, h, \eta, q, \kappa)$ such that the following holds.*

1. *If Protocol A' is executed with parameters (v, h, N, q, η, D) , then for any $\epsilon \in (0, \sqrt{2}]$ and $\kappa \in (0, \infty)$,*

$$H_{\min}^\epsilon(\Gamma_{\text{EGO}}^s \mid EG) \geq N \cdot T(v, h, \eta, q, \kappa) - \left(\frac{\log(\sqrt{2}/\epsilon)}{q\kappa} \right) F(v, h, \eta, q, \kappa). \quad (7.44)$$

2. *The following equalities hold, where π denotes the function from Theorem 4.2.*

$$\lim_{(q, \kappa) \rightarrow (0, 0)} T(v, h, \eta, q, \kappa) = \pi(\eta/v), \quad (7.45)$$

$$\lim_{(q, \kappa) \rightarrow (0, 0)} F(v, h, \eta, q, \kappa) = \frac{-2\pi'(\eta/v)}{v}. \quad (7.46)$$

Proof. Let

$$\mathbf{r} = \min \left\{ \frac{v}{-\pi'(\eta/v)}, \frac{1}{q\kappa} \right\}. \quad (7.47)$$

Define the function T by

$$T(v, h, \eta, q, \kappa) = R(v, h, \eta, q, \kappa, \mathbf{r}). \quad (7.48)$$

By substitution into Proposition 7.6, the bound (7.44) will hold when we set F to be equal to $2/(\mathbf{r})$.

To prove (7.45), note that

$$\lim_{(q, \kappa) \rightarrow (0, 0)} T(v, h, \eta, q, \kappa) = \lim_{(q, \kappa) \rightarrow (0, 0)} R \left(v, h, \eta, q, \kappa, \frac{v}{-\pi'(\eta/v)} \right) \quad (7.49)$$

$$= \min_{s \in [0, 1]} \left[\pi(s) - \frac{\pi'(\eta/v)}{v} (vs - \eta) \right] \quad (7.50)$$

$$= \min_{s \in [0, 1]} \left[\pi(s) - \pi'(\eta/v) \left(s - \frac{\eta}{v} \right) \right]. \quad (7.51)$$

The function enclosed by square brackets in (7.51) is a convex function of s (by Theorem 4.2) and its derivative at $s = \eta/v$ is zero. Therefore, a minimum is achieved at $s = \eta/v$, and the expression in (7.51) thus evaluates simply to $\pi(\eta/v)$.

Equality (7.46) is immediate. This completes the proof. \square

8 Randomness Expansion from an Untrusted Device

In this section, we will combine the results of previous sections to prove that randomness expansion from an untrusted device is possible.

8.1 The Trust Coefficient of a Strong Self-Test

Corollary 6.5 proves that if G is a strong self-test, then for some $\delta_G > 0$, the behavior of an untrusted device under G can be simulated by a partially trusted device with parameters $(\delta_G, 2\mathbf{f}_G)$. Let us say that the **trust coefficient** of G is the largest value of δ_G which makes such a simulation possible.

As a consequence of the theory in section 5, we have the following formal definition for the trust coefficient of G .

Definition 8.1. Suppose that G is an n -player binary XOR game. Then the **trust coefficient** of G , denoted \mathbf{v}_G , is the maximum value of $c \geq 0$ such that there exists a Hermitian operator N on $(\mathbb{C}^2)^{\otimes n}$ satisfying the following conditions.

1. The square of N is the identity operator on $(\mathbb{C}^2)^{\otimes n}$.
2. The operator N anticommutes with the operator $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \mathbb{I} \otimes \dots \otimes \mathbb{I}$.
3. For any complex numbers $\zeta_1, \dots, \zeta_n \in \{\zeta \mid |\zeta| = 1, \text{Im}(\zeta) \geq 0\}$, the operator given by

$$M = \begin{bmatrix} & & & a_{00\dots0} \\ & & a_{00\dots1} & \\ & \ddots & & \\ & a_{11\dots0} & & \\ a_{11\dots1} & & & \end{bmatrix}, \quad (8.1)$$

where

$$a_{b_1, \dots, b_n} = P_G(\zeta_1^{(-1)^{b_1}}, \zeta_2^{(-1)^{b_2}}, \dots, \zeta_n^{(-1)^{b_n}}), \quad (8.2)$$

satisfies

$$\|M - cN\| \leq \mathfrak{q}_G - c. \quad (8.3)$$

8.2 The Security of Protocol R

Combining Theorem 7.7, Corollary 6.5, and the definition from the previous subsection, we have the following. As with Protocol A', let us record the outputs of Protocol R as bit sequences $G = (g_1, \dots, g_N)$ and $O = (o_1, \dots, o_N)$, where $o_i = 0$ if the outcome of the i th round is H or P , and $o_i = 1$ otherwise. If E is a purifying system for the device D used in Protocol R, then we denote by Γ_{EGO} the state of E, G , and O , and by Γ_{EGO}^s the subnormalized state corresponding to the “success” event.

Theorem 8.2. *There exists continuous real-valued functions $T(v, h, \eta, q, \kappa)$ and $F(v, h, \eta, q, \kappa)$ (with the domains specified in Figure 5) such that the following statements hold.*

1. Let G be an n -player strong self-test. Let D be an untrusted device with n components, and let E be a purifying system for D . Suppose that Protocol R is executed with parameters N, η, q, G, D . Then, for any $\kappa \in (0, \infty)$ and $\epsilon \in (0, \sqrt{2}]$, the following bound holds.

$$H_{min}^\epsilon(\Gamma_{EGO}^s \mid EG) \geq N \cdot T(\mathbf{v}_G, 2\mathbf{f}_G, \eta, q, \kappa) - \left(\frac{\log(\sqrt{2}/\epsilon)}{q\kappa} \right) F(\mathbf{v}_G, 2\mathbf{f}_G, \eta, q, \kappa), \quad (8.4)$$

2. The following limit conditions are satisfied, where π denotes the function from Theorem 4.2.

$$\lim_{(q,\kappa) \rightarrow (0,0)} T(v, h, \eta, q, \kappa) = \pi(\eta/v), \quad (8.5)$$

$$\lim_{(q,\kappa) \rightarrow (0,0)} F(v, h, \eta, q, \kappa) = \frac{-2\pi'(\eta/v)}{v}. \quad (8.6)$$

The following corollary shows that the linear rate of Protocol R can be lower bounded by the function π from Theorem 4.2.

Corollary 8.3. *Let G be a strong self-test, and let $\eta > 0$ and $\delta > 0$ be real numbers. Then, there exists positive reals b and q_0 such that the following holds. If Protocol R is executed with parameters N, η, q, G, D , where $q \leq q_0$, then*

$$H_{min}^\epsilon(\Gamma_{EGO}^s \mid EG) \geq N \cdot (\pi(\eta/\mathbf{v}_G) - \delta), \quad (8.7)$$

where $\epsilon = \sqrt{2} \cdot 2^{-bqN}$.

Proof. By the limit conditions for T and F , we can find $q_0, \kappa_0 > 0$ sufficiently small and $M > 0$ sufficiently large so that for any $q \in (0, q_0]$ and $\kappa \in (0, \kappa_0]$,

$$T(\mathbf{v}_G, 2\mathbf{f}_G, \eta, q, \kappa) \geq \pi(\eta/\mathbf{v}_G) - \delta/2 \quad (8.8)$$

$$F(\mathbf{v}_G, 2\mathbf{f}_G, \eta, q, \kappa) \leq M. \quad (8.9)$$

Let $b = \delta\kappa_0/(2M)$, and let $\epsilon = \sqrt{2} \cdot 2^{-bqN}$. Then, provided that $q \leq q_0$, the output of Protocol R satisfies

$$\begin{aligned} H_{min}^\epsilon(\Gamma_{EGO}^s \mid EG) &\geq N \cdot T(\mathbf{v}_G, 2\mathbf{f}_G, \eta, q, \kappa_0) - \left(\frac{\log(\sqrt{2}/\epsilon)}{q\kappa_0} \right) F(\mathbf{v}_G, 2\mathbf{f}_G, \eta, q, \kappa_0) \\ &\geq N(\pi(\eta/\mathbf{v}_G) - \delta/2) - \left(\frac{bqN}{q\kappa_0} \right) M \\ &= N(\pi(\eta/\mathbf{v}_G) - \delta/2) - (\delta/2)N, \end{aligned} \quad (8.10)$$

$$= N(\pi(\eta/\mathbf{v}_G) - \delta/2) - (\delta/2)N, \quad (8.11)$$

which simplifies to the desired bound. \square

We will prove some additional corollaries in order to achieve a security result at full strength. First wish to show that the output register O has high min-entropy even when conditioned on the original inputs to the device D . The above corollary takes into account the biased coin flips g_1, \dots, g_N used in the protocol, but it does not take into account the inputs that are given to D during game rounds.

For each $k \in \{1, \dots, N\}$, let I_k denote a classical register consisting of n bits which records the input used at the k th round. Let I be the collection of the all the registers I_1, \dots, I_N .

Corollary 8.4. *Let G be a strong self-test, and let $\eta > 0$ and $\delta > 0$ be real numbers. Then, there exist positive reals b, K , and q_0 such that the following holds. If Protocol R is executed with parameters N, η, q, G, D , where $q \leq q_0$, then*

$$H_{\min}^{\epsilon}(\Gamma_{EGIO}^s \mid EGI) \geq N \cdot (\pi(\eta/\mathbf{v}_G) - \delta), \quad (8.12)$$

where $\epsilon = K \cdot 2^{-bqN}$.

Proof. Let $\delta' = \delta/2$. By Corollary 8.4, we can find b' and q_0 such that whenever Protocol R is executed with $q \leq q_0$,

$$H_{\min}^{\epsilon'}(\Gamma_{EGO}^s \mid EG) \geq N \cdot (\pi(\eta/\mathbf{v}_G) - \delta/2), \quad (8.13)$$

where $\epsilon' = \sqrt{2} \cdot 2^{-b'qN}$. By decreasing q_0 if necessary, we will assume that $q_0 < \delta/(2n)$.

For each $k \in \{1, 2, \dots, \lfloor N\delta/(2n) \rfloor\}$, let \bar{I}_k denote the input string that was given to the device D on the k th game round. If there were fewer than k game rounds, then simply let \bar{I}_k be the sequence $00 \dots 0$. Let \bar{I} denote the collection of the registers $\bar{I}_1, \dots, \bar{I}_{\lfloor N\delta/(2n) \rfloor}$.

Let d denote the event that

$$\sum G_i \leq N\delta/(2n). \quad (8.14)$$

(That is, d denotes the event that the number of game rounds is not more than $N\delta/2$.) By the Azuma-Hoeffding inequality,

$$P(d) \leq e^{-N[\delta/(2n) - q_0]^2/2}. \quad (8.15)$$

Let ϵ be the sum of ϵ' and the quantity on the right of (8.15), and let sd denote the intersection of the event d and the success event s . Observe the following sequence of inequalities, where we first use the fact that the operator Γ_{EGIO}^{sd} can be reconstructed from the operator Γ_{EGIO}^{sd} , and then use the fact that the register \bar{I} consists of $\leq (N\delta/2)$ bits:

$$H_{\min}^{\epsilon}(\Gamma_{EGIO}^s \mid EGI) \geq H_{\min}^{\epsilon'}(\Gamma_{EGIO}^{sd} \mid EGI) \quad (8.16)$$

$$= H_{\min}^{\epsilon'}(\Gamma_{EGIO}^{sd} \mid EG\bar{I}), \quad (8.17)$$

$$\geq H_{\min}^{\epsilon'}(\Gamma_{EGO}^{sd} \mid EG) - N\delta/2 \quad (8.18)$$

$$\geq H_{\min}^{\epsilon'}(\Gamma_{EGO}^s \mid EG) - N\delta/2 \quad (8.19)$$

$$\geq N \cdot (\pi(\eta/\mathbf{v}_G) - \delta). \quad (8.20)$$

We wish to show that ϵ is upper bounded by a decaying exponential function of qN (i.e., a function of the form $J \cdot 2^{-cqN}$, where J and c are positive constants depending only on δ, η , and G). We already know that ϵ' has such an upper bound. The expression on the right side of (8.15) also has such a bound — indeed, it has a bound of the form $J \cdot 2^{-cN}$, which is stronger. Therefore ϵ (which is the sum of the aforementioned quantities) is also bounded by a decaying exponential function. This completes the proof. \square

Finally, we wish to state a result using the language of extractable bits from subsection 1.5. Note that if ρ_{XZ} is a subnormalized classical quantum state of a system (X, Z) that is such that

$$H_{\min}^{\epsilon}(\rho_{XZ} \mid Z) \geq C, \quad (8.21)$$

Then either $\text{Tr}(\rho) \leq 2\epsilon$, in which case ρ is within trace distance 2ϵ of the zero state (which has an infinite number of extractable bits) or $\text{Tr}(\rho) > 2\epsilon$, in which case ρ is within ϵ of a nonzero state ρ' satisfying $H_{\min}(\rho' | Z) \geq C$. In the latter case, since $\text{Tr}(\rho') \geq \text{Tr}(\rho) - \epsilon > \epsilon$, we must have

$$H_{\min}^{\epsilon}(\rho' / \text{Tr}(\rho') | Z) \geq C - \log(1/\epsilon). \quad (8.22)$$

Thus ρ_{XZ} is within trace-distance 2ϵ of a state that has $C - \log(1/\epsilon)$ extractable bits.

The next collary follows easily.

Corollary 8.5. *Let G be a strong self-test, and let $\eta, \delta > 0$ be real numbers. Then, there exist positive reals b, K and q_0 such that the following holds. If Protocol R is executed with parameters N, η, q, G, D with $q \leq q_0$, then it produces*

$$N \cdot (\pi(\eta / \mathbf{v}_G) - \delta) \quad (8.23)$$

extractable bits with soundness error $K \cdot 2^{-bqN}$.

Remark 8.6. *Corollary 8.4 implies that if $\pi(\eta / \mathbf{v}_G) > 0$, then (provided q is sufficiently small) a positive linear rate of output entropy is achieved by Protocol R . Using Theorem 4.2, this means that a positive linear rate is achieved if $\eta < 0.11 \cdot \mathbf{v}_G$. \square*

Recall that $\pi(0) = 1$. The next corollary follows easily from Corollary 8.4.

Corollary 8.7. *Let G be a strong self-test, and let $\delta > 0$ be a real number. Then, there exist positive reals b, K, η and q_0 such that the following holds. If Protocol R is executed with parameters N, η, q, G, D with $q \leq q_0$, then it produces $N \cdot (1 - \delta)$ extractable bits with soundness error $K \cdot 2^{-bqN}$.*

8.3 Example: The GHZ game

Let H denote the 3-player binary XOR game whose polynomial P_H is given by

$$P_H(\zeta_1, \zeta_2, \zeta_3) = \frac{1}{4} (1 - \zeta_1 \zeta_2 - \zeta_2 \zeta_3 - \zeta_1 \zeta_3). \quad (8.24)$$

This is the Greenberger-Horne-Zeilinger (GHZ) game.

Proposition 8.8. *The trust coefficient for the GHZ game H is at least 0.14.*

For the proof of this result we will need the following lemma (which the current authors also used in [Miller and Shi, 2013]):

Lemma 8.9. *Let a, b, c be unit-length complex numbers such that $\text{Im}(a) \geq 0$ and $\text{Im}(b), \text{Im}(c) \leq 0$. Then,*

$$|1 - ab - bc - ca| \leq \frac{\sqrt{2}}{2}. \quad (8.25)$$

Proof. We have

$$-1 + ab + bc + ca = (-1 + bc) + a(b + c). \quad (8.26)$$

The complex number $(b + c)$ lies at an angle of $\pi/2$ (in the counterclockwise direction) from $(-1 + bc)$. Since a has nonnegative imaginary part, the angle formed by $a(b + c)$ and $(-1 + bc)$ must be an obtuse or a right angle. Therefore,

$$|(-1 + bc) + a(b + c)|^2 \leq |-1 + bc|^2 + |a(b + c)|^2 \quad (8.27)$$

$$\leq 4 + 4 \quad (8.28)$$

$$= 8. \quad (8.29)$$

The desired result follows. \square

of Proposition 8.8. We proceed from Definition 8.1. Let N be the reverse-diagonal matrix

$$N = \begin{bmatrix} & & & & & & 1 \\ & & & & & 1 & \\ & & & & -1 & & \\ & & & -1 & & & \\ & & -1 & & & & \\ & -1 & & & & & \\ 1 & & & & & & \end{bmatrix}. \quad (8.30)$$

Clearly, N anticommutes with $\sigma_x \otimes \mathbb{I} \otimes \dots \otimes \mathbb{I}$.

Let $\zeta_1, \zeta_2, \zeta_3$ be unit-length complex numbers with nonnegative imaginary part, and let M be the operator given by (8.1)–(8.2). We wish to show that the operator norm of $M - (0.14)N$ is bounded by $q_H - 0.14 = 0.86$.

Note that

$$\left| \frac{1}{4} (1 - \zeta_1 \zeta_2 - \zeta_2 \zeta_3 - \zeta_1 \zeta_3) - 0.14 \right| = \left| 0.11 - \frac{1}{4} (\zeta_1 \zeta_2 + \zeta_2 \zeta_3 + \zeta_1 \zeta_3) \right| \quad (8.31)$$

$$\leq 0.11 + 0.75 \quad (8.32)$$

$$= 0.86. \quad (8.33)$$

Also, by applying Lemma 8.9,

$$\left| \frac{1}{4} (1 - \zeta_1 \overline{\zeta_2} - \overline{\zeta_2} \zeta_3 - \zeta_1 \overline{\zeta_3}) + 0.14 \right| \leq \left| \frac{1}{4} (1 - \zeta_1 \overline{\zeta_2} - \overline{\zeta_2} \zeta_3 - \zeta_1 \overline{\zeta_3}) \right| + 0.14 \quad (8.34)$$

$$\leq \frac{\sqrt{2}}{2} + 0.14 \quad (8.35)$$

$$\leq 0.86. \quad (8.36)$$

Applying similar arguments shows that every reverse-diagonal entry of $(M - 0.14 \cdot N)$ has absolute value bounded by 0.86. This completes the proof. \square

Remark 8.10. By the above result and Remark 8.6, we have the following. If η is a positive real smaller than 0.0154 ($= 0.11 \cdot 0.14$) and if $q > 0$ is sufficiently small, then executing Protocol R with the GHZ game yields a positive linear rate of entropy. \square

8.4 Completeness

Let D be an n -component binary quantum device. For any $j \geq 1$, we will use the expressions I_j and Y_j to denote the input strings and output strings (each in $\{0, 1\}^n$) for D from the j th iteration.

Definition 8.11. Let G be a strong self-test. For each input string $i = (i^1, \dots, i^n) \in \{0, 1\}^n$, the unique optimal strategy for G (see section 5) determines a distribution on output strings $y \in \{0, 1\}^n$ which we denote by $\{p_i^y \mid y \in \{0, 1\}^n\}$. We will say that D has **noise level** β (for the game G) if, for any $k \geq 1$, and $i_1, \dots, i_k, y_1, \dots, y_{k-1} \in \{0, 1\}^n$ such that

$$\mathbf{P}((Y_1, \dots, Y_{k-1}) = (y_1, \dots, y_{k-1}) \mid (I_1, \dots, I_{k-1}) = (i_1, \dots, i_{k-1})) > 0, \quad (8.37)$$

the conditional distribution

$$\{\mathbf{P}((Y_1, \dots, Y_{k-1}) = (y_1, \dots, y_k) \wedge Y_k = y \mid (I_1, \dots, I_k) = (i_1, \dots, i_k))\}_y \quad (8.38)$$

is within statistical distance (2β) from $\{p_{i_k}^y\}_y$.

Note that an easy argument shows that a device with noise level β must achieve an expected score of at least $\mathbf{w}_G - \beta$.

We now discuss completeness. We will make use of a refined Azuma-Hoeffding inequality [Dembo and Zeitouni, 1997].

Lemma 8.12. *Suppose that S_1, S_2, \dots, S_N is a Martingale with*

$$|S_{i+1} - S_i| \leq 1,$$

and

$$\text{Var}[S_{i+1} - S_i \mid S_1, \dots, S_i] \leq w,$$

for all $i, 1 \leq i \leq N - 1$. Then for any $\epsilon \in (0, 1)$,

$$\mathbb{P}[S_N \geq \epsilon w N] \leq \exp\left(-\epsilon^2 \frac{w}{2} N \left(1 - \frac{1-w}{3} \epsilon\right)\right). \quad (8.39)$$

In particular if $\epsilon \leq 1$, we have

$$\mathbb{P}[S_N \geq \epsilon w N] \leq \exp\left(-\epsilon^2 \frac{w}{3} N\right). \quad (8.40)$$

Proposition 8.13. *Suppose that the device in Protocol R has noise level $\eta' < \eta$. Then the probability of aborting is at most $\exp(-(\eta - \eta')^2 q N / 3)$.*

Proof. Let I_1, \dots, I_N and Y_1, \dots, Y_N be random variables containing the inputs and outputs for Protocol R. Let Z_i be equal to 1 if the game is won on the i th round and 0 otherwise. Let

$$z_i = \mathbf{E}[Z_i \mid I_1, \dots, I_{i-1}, Y_1, \dots, Y_{i-1}]. \quad (8.41)$$

By definition, Protocol R (Fig. 2) aborts when

$$\sum_i g_i(1 - Z_i) \geq (1 - \mathbf{w}_G + \eta)qN. \quad (8.42)$$

By assumption,

$$\sum_i (\mathbf{w}_G - z_i) \leq \eta' N. \quad (8.43)$$

Let

$$R_i = \sum_{k=1}^i g_k(1 - Z_k) - q \sum_{k=1}^i (1 - z_k). \quad (8.44)$$

Then R_1, R_2, \dots is a Martingale with

$$\text{Var}[R_i - R_{i-1} \mid R_1, \dots, R_{i-1}] = q(1 - z_i)[1 - q(1 - z_i)] \leq q, \quad (8.45)$$

thus (8.42) implies that

$$\sum_i g_i(1 - Z_i) - q \sum_i (1 - z_i) \geq \eta q N - q \sum_i (\mathbf{w}_G - z_i) \geq (\eta - \eta') q N. \quad (8.46)$$

Thus by Corollary 10.4, the probability of aborting is $\leq \exp(-(\eta - \eta')^2 q N / 3)$. \square

9 Unbounded Expansion

In this section, we prove a general result, the Composition Lemma (Lemma 9.3 below), that implies Corollary 1.7 straightforwardly. This general result implies that known untrusted-device randomness expansion protocols, including ours, can be composed sequentially with additive errors, even if only two devices are used. The proof will be short, but it is important to define the error parameters appropriately. We use a high-level framework for rigorously reasoning about these protocols, following [Chung et al., 2014]. We only sketch the necessary elements and refer interested readers to [Chung et al., 2014] for a more comprehensive description.

Since we are cross-feeding inputs and outputs between devices, we will use the same syntax for both input and output states. A **protocol state space** \mathcal{H} is a three-part Hilbert space

$$\mathcal{H} = C \otimes D \otimes E, \quad (9.1)$$

where C, D, E are referred to as the **classical**, **device**, and **adversary** subsystems, respectively.⁵ We also represent a protocol space by the triple (C, D, E) .

We call a *subnormalized* classical-quantum-quantum state ρ over \mathcal{H} a **protocol state**. Those states are the accepting (or non-aborting) portion of the normalized states in our protocols. Denote by $\hat{\rho} = \rho / \text{Tr}(\rho)$ the corresponding normalized state. Correspondingly, we allow quantum operations to be trace-non-increasing with the understanding that the missing trace (from the unit) corresponds to rejecting (or aborting).

We call a protocol state ρ_{CDE} **device-uniform**, **adversary-uniform**, or **global-uniform** if in $\hat{\rho}$, C is uniform with respect to D , or E , or DE , respectively. For any $\epsilon \in [0, 2]$, ρ is said to be ϵ -**device-uniform** if there exists a subnormalized device-uniform state $\tilde{\rho}_D$ within ϵ trace-distance to ρ . Similarly define ϵ -adversary-uniform and ϵ -global-uniform.

A **strong untrusted-device (UD) extractor** Π is a procedure which takes as input a classical register X , a device D , and a quantum system E , then performs X -controlled operations on D and E , produces a classical output register Y , and then “aborts” or “succeeds.” For our discussion in this paper, we allow the steps in the procedure to include both classical interaction with the device, and arbitrary device-adversary operations (i.e., quantum operations on the composite system DE). The protocol Π maps protocol states over the input protocol space (X, D, E) to those over the output protocol space (Y, D, XE) (the success states). An **implementation** of the extractor Π is a specification of the initial state of (X, D, E) , and the measurements performed by the device, and the operations used in any device-adversary interactions.

If Π is a strong UD extractor which involves no device-adversary interactions, then an **ideal implementation** for Π is one in which the device is such that it has the same conditional input-output distribution on each use. If an ideal implementation has been specified, we then use the term **noise level** in the same sense as in Definition 8.11: an implementation for Π has noise level η if at each use, the output distribution of the device D on any transcript and any input is within statistical distance η from that of the ideal implementation. The extractor Π has **completeness error** ϵ_c tolerating noise level η if for any implementation having noise level η , the success probability of Π is at least $1 - \epsilon_c$.

Let Π is a strong UD extractor which has no device-adversary interactions. We call ϵ_s a **soundness error** of Π on a set \mathcal{S} of protocol states if for any $\rho \in \mathcal{S}$ and any compatible implementation, $\Pi(\rho)$ is ϵ_s -adversary uniform. We say that on \mathcal{S} , Π has a **adjustment completeness error** $\hat{\epsilon}_c$ tolerating a noise level η , if there exists an ideal implementation, such that for all *normalized* states

⁵If D is a quantum device, then by a small abuse of notation, let us also use the letter D to denote the quantum system inside D .

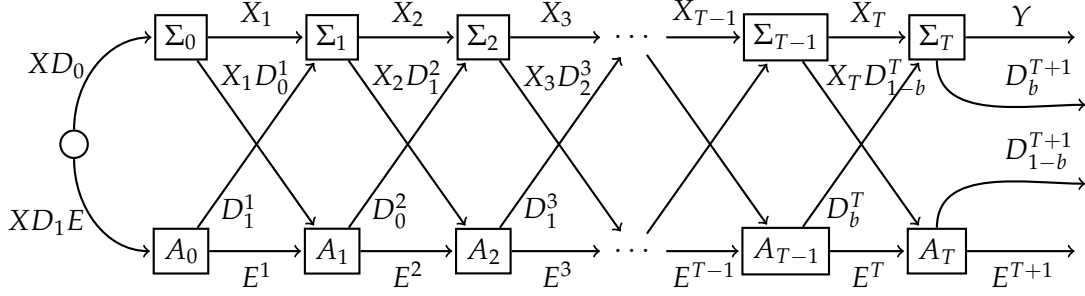


Figure 6: The tensor network representation of a cross-feeding protocol. Superscripts indicate that a (device or adversary) subsystem may change after an operation. Each E^t includes a copy of X_0, \dots, X_{t-1} to be consistent with the definition of strong UD extractors. The subscript $b = T \bmod 2$.

$\rho \in \mathcal{S}$ and all implementations with noise level η , the protocol's final state is within $\hat{\epsilon}_c$ trace distance to a *normalized* adversary-uniform state. This change of completeness error is not substantial: $\hat{\epsilon}_c \leq 2(\epsilon_c + \epsilon_s)$, and $\epsilon_s \leq \hat{\epsilon}_c$.

The Equivalence Lemma of Chung, Shi and Wu [Chung et al., 2014] states the following.

Theorem 9.1 (The Equivalence Lemma [Chung et al., 2014]). *Let Π be a strong UD extractor that has no device-adversary interactions. Then on the set of global-uniform inputs and the set of device-uniform inputs, Π has the same soundness error, adjustment completeness error, and noise tolerating level.*

We now formally define the composition of protocols using two devices. (The earliest mention of this approach that we know of was in [Pironio et al., 2010].)

Definition 9.2. *Let D_0 and D_1 be two untrusted quantum devices and $T \geq 1$ be an integer. A **cross-feeding protocol** Σ using D_0 and D_1 consists of a sequence of strong UD extractors Σ_i , $i = 0, 1, \dots, T$, such that Σ_i uses $D_{i \bmod 2}$ and the output of Σ_i is used as the input to Σ_{i+1} . The input to Σ is the input to Σ_0 , and the output is that of Σ_T .*

*Furthermore, Π is said to use **restorable** devices if, for each i , $1 \leq i \leq T$, between Σ_{i-1} and Σ_{i+1} , there is a device-adversary variable operation A_i on $X_i D_{i+1 \bmod 2} E$, controlled by X_i .*

A cross-feeding protocol is illustrated in Fig. (6). Allowing the device-adversary A_i operations reduces the technical challenges for practical implementations, since in an honest implementation, A_i can be used to replenish the consumed entanglement. While our wording of “two” devices was inspired by a possible implementation of using two physical devices, the inactive device can certainly be replaced by a different physical device, since such replacement is one possible A_i operation. The essence of our two device protocol lies in how communication is restricted: besides forbidding communication between an active device and its external world — which is already required for a single-device protocol — the additional constraint is that after an active device finishes its work, no information is allowed to travel from the device to the inactive device before the latter becomes active. A single device would not satisfy this latter requirement.

Lemma 9.3 (Composition Lemma). *Let Σ be a cross-feeding protocol defined above. Assume that for each i , $0 \leq i \leq T$, Σ_i has a soundness error $\epsilon_{s,i}$, and an adjustment completeness error $\hat{\epsilon}_{c,i}$ tolerating a noise level η (set to be the same for all Σ_i), with respect to device-uniform inputs. Let $\epsilon_s := \sum_{i=0}^T \epsilon_{s,i}$ and $\hat{\epsilon}_c := \sum_{i=0}^T \hat{\epsilon}_{c,i}$. Then Σ on states uniform to D_0 has a soundness error ϵ_s , and an adjustment completeness error $\hat{\epsilon}_c$ tolerating an η level of noise.*

In particular, the above statement holds if each Σ_i has no device-adversary interaction and the parameters $\epsilon_s, \hat{\epsilon}_c, \eta$ are valid on global-uniform inputs.

The soundness proof uses the following two facts, both of which follow directly from the corresponding definitions.

Fact 9.4. Let $b \in \{0, 1\}$ and $\rho = \rho_{YD_b(D_{1-b}E)}$ be adversary-uniform. Then ρ as $\rho_{YD_{1-b}(D_bE)}$ is device-uniform for D_{1-b} . This remains true for $(I \otimes A_{D_bE})\rho$ for any operation A_{D_bE} on D_bE .

Fact 9.5. If Π is a strong UD extractor with an ϵ soundness error, and ρ is δ -device-uniform, $\Pi(\rho)$ is $(\epsilon + \delta)$ -adversary uniform.

Proof. The proof for the device-uniform case follows from a straightforward inductive proof on the following two statements. Denote by $\epsilon_s^i := \sum_{j=0}^i \epsilon_{s,j}$, and $\hat{\epsilon}_c^i := \sum_{j=0}^i \hat{\epsilon}_{c,j}$.

- (Soundness) On any implementation and any initial input uniform to D_0 , for each $i, 0 \leq i \leq T$, the output of Σ_i is ϵ_s^i -adversary-uniform.
- (Completeness) Fix an ideal implementation for each Σ_i to achieve the adjustment completeness error. For any η -deviated implementation, any normalized initial input uniform to D_0 , any $i, 0 \leq i \leq T$, the output of Σ_i is $\hat{\epsilon}_c^i$ -close to a normalized adversary-uniform state.

More specifically, for the soundness argument, the base case holds by applying Fact 9.5 to Σ_0 and the assumption that the input is uniform to D_0 . For the inductive step, by the inductive hypothesis (assuming it holds for $i, 0 \leq i \leq T - 1$) and Fact 9.4, the input to Σ_{i+1} is ϵ_s^i -device uniform. By Fact 9.5, the output is thus ϵ_s^{i+1} -adversary uniform. The proof for the completeness follows from the definition of completeness and triangle inequality.

The global-uniform case follows by applying the Equivalence Lemma 9.1. \square

Corollary 1.7 follows by using our robust protocol in Corollary 1.4.

10 Untrusted-device Quantum Key Distribution

In this section, we shall first formally define what we mean by a key distribution protocol using untrusted quantum devices. We then present Protocol R_{kd} , a natural adaptation of Protocol R for untrusted-device quantum key distribution, then we prove its correctness (Corollary 1.9.)

10.1 Definitions

A **min-entropy untrusted-device key distribution (ME-UD-KD) protocol** Π_{kd} is a communication protocol in the following form between two parties Alice and Bob who have access to distinct components of an untrusted quantum device. Before the protocol starts, they share a string that is uniformly random to the device. They communicate through a public, but authenticated, channel. At each step, both the message they send and the new input to their device components are a deterministic function of the initial randomness, the messages received, and the previous output of their device component. The protocol terminates with a public bit S , indicating if the protocol succeeds or aborts, and Alice and Bob each have a private string: A and \tilde{A} , respectively.

The protocol is said to have a yield M with a **soundness error** ϵ_s if both the following conditions hold.

- (a) the joint state (S, A, E) is ϵ_s -close to a mixture of an aborting state and one where A has M extractable bits, and
- (b) the joint state (S, A, \tilde{A}) is ϵ_s -close to a mixture of an aborting state and one where $A = \tilde{A}$.

The protocol is said to have a completeness error ϵ_c with respect to a non-empty class of untrusted devices $\mathcal{U}_{\text{honest}}$, if for any device in this class, the protocol aborts with probability $\leq \epsilon_c$.

If in the above definition, Condition (a) has “ M extractable bits” replaced by “ M uniformly random bits”, then we call the protocol simply an **untrusted-device key distribution protocol** with those parameters.

10.2 The Protocol R_{kd}

Protocol R_{kd} is an adaptation of Protocol R to the distributed setting and is described in Fig. 7. There are two main steps in the proof for Corollary 1.9. The first is to show that for an appropriate range of the parameters, Protocol R has a soundness and completeness error of $\exp(-\Omega(qN))$ with the ideal state being that A and B differ in at most a $(1/2 - \lambda)$ fraction, for a constant λ . The second step is to construct the Efficient Information Reconciliation Protocol that works on the ideal state and for Bob to correct the differences with some small failure probability. We present those two steps in two separate subsections, which are followed by the proof for the Corollary.

10.3 Error Rate

The completeness error is straightforward, so our focus will be on the soundness error.

Our result applies to a broader class of games than the strong self-tests.

Definition 10.1. Let $f : [0, 1] \rightarrow [0, 1]$ be a strictly increasing concave function with $f(0) = 0$. A game G is said to be **f -self-testing in probability** if there exists an input x_0 such that the following holds: If for any $\theta \in (0, 1)$ and any quantum strategy that wins with probability $(1 - \theta)\mathbf{w}_G$, the game wins on x_0 with probability $\geq (1 - f(\theta))\mathbf{w}_G$.

Theorem 10.2. Let G be a strong self-test. Then there exists a constant $C > 0$ such that G is $C\sqrt{\theta}$ -self-testing in probability.

Proof. Since G is strongly self-testing, there is a unique quantum strategy which achieves the optimal winning probability \mathbf{w}_G (see section 5). Let x_0 be an input string (which occurs with nonzero probability in G) such that, if the optimal strategy is applied on input x_0 , the winning probability is at least \mathbf{w}_G .

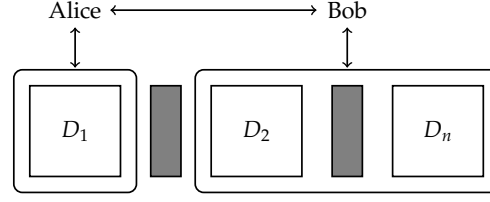
If a given quantum strategy for G achieves a score of $(1 - \theta)\mathbf{w}_G$, then by the strong self-testing property its output distribution on input x_0 is $C_1\sqrt{\theta}$ -close to that of the optimal strategy, for some constant C_1 . The result follows. \square

Consequently all strong self-tests are $O(\sqrt{\theta})$ -self-testing in probability.

We now fix a game G that is f -self-testing in probability for some function f on input $00 \dots 0$. Let w_i , $1 \leq i \leq N$, be the random variable denoting the chance of winning the i th round game under the full input distribution, right after the $(i - 1)$ th round is played. Similarly define w_i^0 by replacing the full input distribution with the input $00 \dots 0$. These random variables may be correlated as the behavior of the i th game may depend on the history of the previous $i - 1$ games. Let W_i be a random variable which is equal to 1 if the game is won on the i th round, and 0 otherwise. Note that the expected value of W_i is equal to w_i if the i th round is a game round, and is equal

Arguments:

G : An n -player nonlocal game that is a **strong self-test** (Definition 5.6). Assume without loss of generality that 0^n is an input on which the winning probability is no less than the average in the optimal quantum strategy.



A diagram of Protocol R_{kd} .

D : An untrusted device (with n components) that can play G repeatedly and cannot receive any additional information. Alice interacts with the first component while Bob interacts the rest of the device. No communication is allowed among the components during Step 1-4 of the protocol. All random bits chosen by Alice and Bob together are assumed to be perfectly random to D .

N : a positive integer (the **output length**.)

λ : A real $\in (0, w_G - 1/2)$. ($1/2 - \lambda$ is the **key error fraction**.)

η : A real $\in (0, \frac{1}{2})$. (The **error tolerance**.)

q : A real $\in (0, 1)$. (The **test probability**.)

Protocol:

1. Repeat the following procedure for N times. Alice and Bob will each produce a raw key, stored as an N -bit binary string A and B , respectively.
 - (a) Alice and Bob choose a bit $g \in \{0, 1\}$ according to a biased $(1 - q, q)$ distribution.
 - (b) If $g = 1$ ("game round"), then Alice and Bob choose an input string at random from $\{0, 1\}^n$ according to the probability distribution specified by G . They give their part(s) of D the corresponding input bit, exchange their output bits and record a "P" (pass) or an "F" (fail) according to the rules of the game G , and store this bit ("P" as 1 and "F" as 0) as their raw key bit for this round.
 - (c) If $g = 0$ ("generation round"), then the input string $00 \dots 0$ is given to the device. Alice sets the raw key bit in A for this round to be her output bit. Bob sets his raw key bit in B to be the unique bit that when XOR'ed with the output bit(s) of his device component(s) would constitute a win for the game. That is, their bits are the same if and only if they win the game.
2. If the total number of failures is more than $(1 - w_G + \eta)qN$, the protocol **aborts**.
3. If not yet aborted, they run an Efficient Information Reconciliation (such as Protocol EIR in Fig. 8) on A and B , the parameters λ and $\epsilon = \exp(-qN)$. Alice's final output is A (unchanged), and Bob's final output \tilde{A} is his output from the information reconciliation protocol.

Figure 7: Protocol R_{kd}

to w_i^0 if the i th round is a generation round. Another useful fact about W_i 's is that when $g_i = 0$, $W_i = 1$ if and only if the i 'th bits of A and B are equal. This follows from the construction of B . Consequently,

$$\sum_i W_i = N - |A + B|. \quad (10.1)$$

Intuitively, if the devices are doing well on the game rounds, they should do well on the randomness generating rounds as well because of self-testing. The following theorem is one way to express this intuition.

Lemma 10.3. *Let G be a strong self-test game that is f -self-testing in probability for some f on input $00 \dots 0$. Consider Protocol R (Fig. 2) using G and an arbitrary $q \in (0, 1)$. For any $\lambda \in (0, \mathbf{w}_G - 1/2)$ and all sufficiently small constant $\eta > 0$, there exist constants $\alpha, \beta > 0$ such that for the events*

$$P := \sum_i g_i(1 - W_i) \leq (1 - \mathbf{w}_G + \eta)qN, \quad (10.2)$$

$$M := \sum_i (1 - g_i)W_i \leq (1/2 + \lambda)(1 - q)N, \quad \text{and}, \quad (10.3)$$

$$E := P \wedge M, \quad (10.4)$$

we have

$$\mathbb{P}[E] \leq \exp(-\alpha qN) + \exp(-\beta N). \quad (10.5)$$

To prove the above lemma, we first derive two concentration results. Consider

$$T_i := \sum_{j=1}^i (g_j(1 - W_j) - q(1 - w_j)). \quad (10.6)$$

Since $E[g_i(1 - W_i) - q(1 - w_i) \mid T_1, \dots, T_{i-1}] = 0$, and

$$\text{Var}[T_i - T_{i-1} \mid T_1, \dots, T_{i-1}] = q(1 - w_i)[1 - q(1 - w_i)] \leq q, \quad (10.7)$$

applying Lemma 8.12, we have

Corollary 10.4. *For any $\epsilon \in (0, 1)$,*

$$\mathbb{P}\left[\sum_i g_i(1 - W_i) - q \sum_i (1 - w_i) \leq -\epsilon qN\right] \leq \exp\left(-\epsilon^2 \frac{q}{3}N\right). \quad (10.8)$$

Consider now

$$S_i := \sum_{j=1}^i ((1 - g_j)W_j - (1 - q)w_j^0). \quad (10.9)$$

Then S_i is a Martingale and

$$\text{Var}[S_i - S_{i-1} \mid S_1, \dots, S_{i-1}] = (1 - q)w_i^0[1 - (1 - q)w_i^0] \leq 1 - q. \quad (10.10)$$

Thus the following Corollary follows from the standard Azuma-Hoeffding bound.

Corollary 10.5. *For any $\epsilon > 0$,*

$$\mathbb{P}\left[\sum_i ((1 - g_0)W_i - (1 - q)w_i^0) \leq -\epsilon(1 - q)N\right] \leq \exp\left(-\frac{\epsilon^2}{3}(1 - q)N\right). \quad (10.11)$$

of Lemma 10.3. Fix an arbitrary $\lambda \in (0, \mathbf{w}_G - 1/2)$. Let $\eta_0 = \eta_0(\lambda), \epsilon_1, \epsilon_2 \in (0, 1)$ be determined later. Fix an arbitrary $\eta \in (0, \eta_0)$. Define the following two events

$$E_1 := \sum_i g_i(1 - W_i) > q \sum_i (1 - w_i) - \epsilon_1 q N, \quad (10.12)$$

$$E_2 := \sum_i (1 - g_i) W_i > (1 - q) \sum_i w_i^0 - \epsilon_2 (1 - q) N. \quad (10.13)$$

Apply Corollaries (10.4) and (10.5) with $\epsilon = \epsilon_1$ and $\epsilon = \epsilon_2$, respectively, we have

$$\mathbb{P}[\bar{E}_1] \leq \exp\left(-\frac{\epsilon_1^2}{3} q N\right), \quad (10.14)$$

$$\mathbb{P}[\bar{E}_2] \leq \exp\left(-\frac{\epsilon_2^2}{3} (1 - q) N\right). \quad (10.15)$$

Then

$$\mathbb{P}[E] \leq \mathbb{P}[\bar{E}_1] + \mathbb{P}[\bar{E}_2] + \mathbb{P}[E \wedge E_1 \wedge E_2] \quad (10.16)$$

$$\leq \exp\left(-\frac{\epsilon_1^2}{3} q N\right) + \exp\left(-\frac{\epsilon_2^2}{3} (1 - q) N\right) + \mathbb{P}[E \wedge E_1 \wedge E_2], \quad (10.17)$$

where the bounds from (10.14, 10.15) are used.

To bound $\mathbb{P}[E \wedge E_1 \wedge E_2]$, denote by

$$\hat{w} := \frac{1}{N} \sum_i w_i / \mathbf{w}_G, \quad \text{and,} \quad \hat{w}^0 := \frac{1}{N} \sum_i w_i^0 / \mathbf{w}_G. \quad (10.18)$$

Event P and E_1 imply

$$1 - \hat{w} < (\eta + \epsilon_1) / \mathbf{w}_G = \eta_0 / \mathbf{w}_G. \quad (10.19)$$

By the assumption that G is f -self-testing in probability and the concavity of f , the above implies

$$1 - \hat{w}^0 < f(\eta_0 / \mathbf{w}_G). \quad (10.20)$$

Meanwhile, Event M and E_2 imply

$$1 - \hat{w}^0 > 1 - \frac{1/2 + \lambda + \epsilon_2}{\mathbf{w}_G}. \quad (10.21)$$

The last two inequalities imply

$$f((\eta + \epsilon_1) / \mathbf{w}_G) > 1 - (1/2 + \lambda + \epsilon_2) / \mathbf{w}_G. \quad (10.22)$$

Since $f(\theta) \rightarrow 0$ when $\theta \rightarrow 0^+$, the LHS of the above inequality $\rightarrow 0$ when $\eta + \epsilon_1 \rightarrow 0$. Note that for any fixed $\lambda < \mathbf{w}_G - 1/2$, RHS > 0 when $\epsilon_2 \rightarrow 0^+$. Following this intuition, we define

$$\eta_0 := \max\{t \in [0, \mathbf{w}_G] : f(t / \mathbf{w}_G) \leq 1 - (1/2 + \lambda) / \mathbf{w}_G\}. \quad (10.23)$$

Now if one sets $\epsilon_1 = \eta_0 - \eta - \epsilon'$ and let $\epsilon', \epsilon_2 \rightarrow 0^+$,

$$\lim_{\epsilon' \rightarrow 0^+} f((\eta + \epsilon_1) / \mathbf{w}_G) = f(\eta_0 / \mathbf{w}_G) \leq 1 - (1/2 + \lambda) / \mathbf{w}_G = \lim_{\epsilon_2 \rightarrow 0^+} 1 - (1/2 + \lambda + \epsilon_2) / \mathbf{w}_G.$$

Thus for some sufficiently small $\epsilon'_0 > 0$ and $\epsilon_2 > 0$, Eqn. 10.22 becomes false, which means that Event $E \wedge E_1 \wedge E_2$ does not occur. Setting

$$\alpha := (\eta_0 - \eta - \epsilon'_0)^2 / 3 \quad \text{and} \quad \beta := \epsilon_2, \quad (10.24)$$

and by Eqn. (10.17),

$$\mathbb{P}[E] \leq \exp(-\alpha q N) + \exp(-\beta N). \quad (10.25)$$

Thus the theorem holds. \square

10.4 Efficient Information Reconciliation

We now arrive at the problem of resolving differences between Alice and Bob's keys. This problem, called *information reconciliation* (IR), has been studied since the early days of quantum cryptography (the earliest works include [Robert, 1985, Bennett et al., 1988]). There are several variations of the problem, for examples, depending on how the differences are quantified and if computationally efficient solutions are sought. The content of this subsection is a synthesis of known results; as such we do not claim any credit of originality. We choose to include it here because of our goals may be different from other sources. Also, efficient constructions of a component (list-decodable codes) known to be useful for IR long ago only became known more recently. The IR protocol presented here follows a well-known framework (e.g., as described in [Smith, 2007]), but will use the latest tools, some known after [Smith, 2007]. Thus, to the best of our knowledge, no other sources have put these known facts together.

We summarize our goals for IR. First, we would like to succeed *whenever* the differences (referred to as errors) are bounded away from the above by $1/2$ -fraction. We hope that the solution is efficient, not just in term of computational complexity, but also, most critically, the bits communicated, as well as the number of shared random bits used. This is because any bit communicated in this stage will be subtracted from the min-entropy guarantee, and that our goal is to achieve secure quantum key distribution with a short seed. We note that in the literature, the issue of computational efficiency and the amount of share randomness were often not considered, or were considered under a different set of assumptions (e.g., [Renner, 2005, Tomamichel and Leverrier, 2015]).

We define a quantity to describe the limit of surviving fraction of min-entropy.

Definition 10.6 (Efficient Information Reconciliation). *Let $\lambda \in (0, 1/2)$, $\epsilon \in (0, 1)$, N , R and M be integers, and T be a function on N , λ and ϵ . An **information reconciliation protocol** with those parameters is a communication protocol between two parties Alice and Bob with the following property. On any N -bit strings A and B , known to Alice and Bob, respectively, they start the protocol with a shared R -bit string, communicate M bits, and finally Bob outputs an N -bit string \tilde{A} . If $A = \tilde{A}$, the protocol succeeds; otherwise it fails. For all A and B of Hamming distance $|A \oplus B| \leq (1/2 - \lambda)N$, the probability of failure is*

$$\mathbb{P}[A \neq \tilde{A}] \leq \epsilon. \quad (10.26)$$

The computation complexity of the protocol is $\leq T$.

*The protocol is said to be **efficient** if for a constant λ , $R = O(\log(N/\epsilon))$, $M \leq (1 - c)N + O(\log(1/\epsilon))$ for some constant $c = c(\lambda)$, and $T = \text{poly}(N, \log(1/\epsilon))$.*

The key ingredient in the protocol is to use binary linear error-correcting codes. When the relative error is $< 1/4$, one can use a uniquely decodable code, as shown by [Bennett et al., 1991]. Otherwise, there is no binary code with a constant rate, by the Plotkin bound. Thus we will have to resort to list-decodable binary linear codes. A folklore approach for pinning down the actual error from the decoded list is to use hashing. Here we use approximate universal hashing. Explicit constructions of all these three tools are known and are summarized below.

Theorem 10.7 (Corollary of Theorem 5 in [Guruswami and Indyk, 2005]). *For any $\lambda \in (0, 1/4)$, there exists a family of binary linear codes with a relative error $1/4 - \lambda$, a rate $\Omega(\lambda^3)$, and linear time complexity for encoding and decoding.*

Theorem 10.8 ([Guruswami and Rudra, 2008] (Theorem 5.3 and Remark 5.2)). *For any $\lambda \in (0, 1/2)$, and for an infinite number of integers $N > 0$, there exists a binary linear code of block length N , relative error $1/2 - \lambda$, rate $\Omega(\lambda^3)$, that can be list-decoded into a list of size $N^{\tilde{O}(\log 1/\lambda^3)}$ with $O(N^{O(1/\lambda^4)})$ encoding and decoding time.*

Definition 10.9 (Approximate Universal Hash Functions). *A set H of functions $h : U \rightarrow V$ is a ϵ -Universal Hash Function (-UHF) family if for all $u, u' \in U, u \neq u'$,*

$$\mathbb{P}_{h \in H}[h(u) = h(u')] \leq \epsilon. \quad (10.27)$$

It is well known that good approximate UHF exists. A standard construction is the following (see, e.g., [Boneh and Shoup, 2015]). Let \mathbb{F}_p be a finite field of size q , $U = \mathbb{F}_q^\ell$, $H = V = \mathbb{F}_p$, where each $k \in H$ is identified with the function h_k

$$h_k : (a_{\ell-1}, a_{\ell-2}, \dots, a_0) \mapsto k^\ell + a_{\ell-1}k^{\ell-1} + \dots + a_1k + a_0. \quad (10.28)$$

Clearly if $(a'_{\ell-1}, a'_{\ell-2}, \dots, a'_0) \neq (a_{\ell-1}, a_{\ell-2}, \dots, a_0)$,

$$\mathbb{P}_{k \in H}[h_k(a'_{\ell-1}, a'_{\ell-2}, \dots, a'_0) = h_k(a_{\ell-1}, a_{\ell-2}, \dots, a_0)] \leq \ell/p. \quad (10.29)$$

Thus H is an ℓ/p -UHF with $|U| = p^\ell$, $|V| = |H| = p$.

We will use an approximate UHF of the following parameters.

Proposition 10.10. *For all sufficiently large integer N and any $\epsilon \geq \frac{1}{4}2^{-N}$, there exists an explicit ϵ -UHF from $\{0, 1\}^N \rightarrow \{0, 1\}^n$ of size 2^n , where $n = \lceil \log(\frac{N}{\epsilon} / \log \frac{N}{\epsilon}) \rceil + 2$.*

Proof. In the construction described above, use the finite field of size 2^n and set $\ell = \lfloor \epsilon 2^n \rfloor$. We need only to check that $n, \ell \geq 1$ and $n\ell \geq N$, which is indeed the case. \square

We are ready to present our protocol for Efficient Information Reconciliation and prove its correctness.

One may note that in the final step of Protocol EIR, Bob could alternatively abort when there is no unique Δ_i such that $h(Y + \Delta_i) = h(X)$. For technical convenience, our definition of Efficient Information Reconciliation does not allow abort. But it can be easily modified to allow aborting, and resulting performance parameters will be similar.

Proposition 10.11. *The Protocol EIR in Fig. 8 is an Efficient Information Reconciliation protocol (Definition 10.6). If $\lambda > 1/4$ and a uniquely decodable code C is used, no randomness is needed and the protocol succeeds with certainty.*

Proof. The length of Alice's message, the correctness of Bob's output, and the computational complexities follow from the properties of the error-correcting code (Theorems 10.7 and 10.8). For the case of $\lambda \leq 1/4$, the length of the shared randomness follows from the property of \mathcal{H} . To analyze the failure probability, first observe that under the assumption that $|X + Y| \leq (1/2 - \lambda)N$, $X + Y = D_i$ for some i . Thus the chance of failure is precisely the existence of $i' \neq i$ such that $h(Y + D_i) = h(Y + D_{i'})$. This probability is no more than $L\epsilon' = \epsilon$, as desired. \square

We remark that for an Efficient Information Reconciliation protocol, there may be a tradeoff between the communication cost and the randomness used. For example, when the error rate $1/2 - \lambda < 1/4$, using a uniquely decodable code from Theorem 10.7 avoids the use of randomness but $c(\lambda) = O((\lambda - 1/4)^3)$. If one uses the list-decodable code from Theorem 10.8, the rate may be higher at the cost of some randomness.

Arguments:

λ : A real constant $\in (0, 1/2]$.

X, Y : Binary strings of length N such that $|X \oplus Y| \leq (1/2 - \lambda)N$.

ϵ : A failure probability. Can be 0 if $\lambda \in (1/4, 1/2]$.

A : The check matrix of an explicitly constructible (i.e. encoding and decoding in polynomial time) binary linear error-correcting code C of length N , relative error $1/2 - \lambda$, and a linear rate $R = R(\lambda)$. The code C is uniquely decodable if $\epsilon = 0$. Such code exists (e.g., [Alon et al., 1992], [Guruswami and Indyk, 2005]) with $R(\lambda) = \Omega((\lambda - 1/4)^3)$. If C is list-decodable code, the list size $L = L(N, \lambda) = N^{O(1)}$. Such a code exists (e.g, with $R(\lambda) = \Omega(\lambda^3)$ as in [Guruswami and Rudra, 2006]).

\mathcal{H} : If C is list-decodable, let $\epsilon' := \epsilon/L$. \mathcal{H} is an explicit ϵ' -UHF from $\{0, 1\}^N$ to $\{0, 1\}^k$ of size 2^k , where $k = \lceil \log(\frac{N}{\epsilon'} / \log \frac{N}{\epsilon'}) \rceil + 2 = \log(1/\epsilon) + O(\log N)$. Such \mathcal{H} exists according to Proposition 10.10.

Protocol:

1. Alice sends Bob $AX \in \{0, 1\}^{(1-R)N}$.
2. If C is uniquely decodable, Bob computes the error syndrome $AY + AX = A(X + Y)$, runs the decoding algorithm to obtain the unique D with $|D| \leq (1/2 - \lambda)N$ and $AD = A(X + Y)$. The protocol terminates with Bob outputting $Y + D$.
3. Otherwise (C is list-decodable with list size L), Bob list-decodes from $A(X + Y)$ to obtain a list $\{\Delta_1, \Delta_2, \dots, \Delta_L\}$, where by the property of C , $X + Y = \Delta_i$, for some i , $1 \leq i \leq L$.
4. Alice and Bob draw a random $h \in \mathcal{H}$, and Alice sends Bob $h(X)$. Bob checks if there exists a unique Δ_i such that $h(Y + \Delta_i) = h(X)$. If yes, Bob outputs $Y + \Delta_i$; otherwise he outputs Y .

Figure 8: Protocol EIR: an Efficient Information Reconciliation protocol

10.5 The Security of Protocol R_{kd}

We are now ready to prove our main result for untrusted-device QKD.

PROOF OF COROLLARY 1.9. We set r_G to be the supremum of reals R such that for some $\lambda < \mathbf{w}_G - 1/2$, there exists an infinite family of explicit list-decodable⁶ binary linear codes of rate R and relative error $1/2 - \lambda$. By using the list-decodable code from Theorem 10.8, $r_G = \Omega((\mathbf{w}_G - 1/2)^3) > 0$.

We will show that any $r < r_G$ can be achieved. The proof for completeness is a standard application of concentration inequalities thus we leave the proof for the interested reader. We shall focus on proving the soundness.

Let $\delta = r_G - r$. Let $\lambda \in (0, \mathbf{w}_G - 1/2)$ be such that there exists an Efficient Information Reconciliation protocol P_{EIR} with $c(\lambda) \geq r_G - \delta/3$. Such λ and P_{EIR} exist by the definition of r_G and Proposition 10.11.

Applying Theorem 1.1 with the δ parameter there set to be $\delta/3$, we get the constants K, b, q_0 and η_0 . Let $\eta \leq \eta_0$ and $q \leq q_0$ so that Theorem 1.1 applies. Further assume that η is small enough so that Lemma 10.3 also applies.

To prove Condition (a) of the soundness definition (subsection 10.1), note that by Theorems 1.1, the SAE -state (where S is the aborting decision bit, and E is the adversary's system) before information reconciliation has $(1 - \delta/3)N$ extractable bits with soundness error $\epsilon'_s := K \exp(-bqN)$. By definition, P_{EIR} communicates $\leq (1 - c(\lambda))N + O(\log 1/\epsilon)$ bits. Thus the yield in A after information reconciliation is at least

$$[(1 - \delta/3) - (1 - c(\lambda))] \cdot N - O(\log 1/\epsilon) \quad (10.30)$$

$$= [c(\lambda) - \delta/3] \cdot N - O(qN) \quad (10.31)$$

$$\geq (r_G - 2\delta/3 - O(q))N. \quad (10.32)$$

If necessary, we lower the upper-bound for q so that in the above, $O(q) \leq \delta/3$. Thus the yield in A is at least $(r_G - \delta)N = rN$. Since P_{EIR} does not abort or change AE , the final state when restricted to SAE remains unchanged, thus is ϵ'_s -close to a mixture of an aborting state and a state where A has rN extractable bits.

To satisfy soundness condition (b) (see subsection 10.1), we now bound the probability of the event E_{\neq} that the protocol does not abort and Alice and Bob's keys (A and \tilde{A}) disagree. That is, with P being the passing event (10.2),

$$E_{\neq} := (P \wedge (A \neq \tilde{A})). \quad (10.33)$$

Recall that A and B are the raw keys before P_{EIR} . Denote by Δ the event that $|A + B| < (1/2 - \lambda)N$. Let C_G be the event that the number of game rounds is $\leq (1/2 + \lambda)qN$. By the Chernoff bound, with $\gamma := \frac{(1/2 - \lambda)^2}{2}$,

$$\mathbb{P}[C_G] \leq \exp(-\gamma qN). \quad (10.34)$$

Let events P, M, E be defined as in Lemma 10.3, which we now apply with the above λ . Note that $(\bar{M} \wedge \bar{C}_G)$ implies Δ , because by construction, the raw key bits for game rounds always agree.

⁶We require that the size of the list is polynomial in the block length.

We now upper-bound $\mathbb{P}[E_{\neq}]$.

$$\mathbb{P}[E_{\neq}] \leq \mathbb{P}[E] + \mathbb{P}[C_G] + \mathbb{P}[E_{\neq} \wedge \bar{E} \wedge \bar{C}_G] \quad (10.35)$$

$$= \mathbb{P}[E] + \mathbb{P}[C_G] + \mathbb{P}[P \wedge (A \neq \tilde{A}) \wedge \bar{C}_G \wedge \bar{M}] \quad (10.36)$$

$$\leq \mathbb{P}[E] + \mathbb{P}[C_G] + \mathbb{P}[(A \neq \tilde{A}) \wedge \Delta] \quad (10.37)$$

$$\leq \mathbb{P}[E] + \mathbb{P}[C_G] + \mathbb{P}[(A \neq \tilde{A})|\Delta]. \quad (10.38)$$

Applying Lemma 10.3, equation (10.34), and definition of Efficient Information Reconciliation, the above is upper-bounded by

$$\exp(-\alpha qN) + \exp(-\beta N) + \exp(-\gamma qN) + \exp(-qN). \quad (10.39)$$

Thus setting $b' := \min\{b, \alpha, \beta, \gamma, 1\}$ and $K' = \max\{K, 5\}$, we have that the soundness error is

$$K' \exp(-b' qN) = \exp(-\Omega(qN) + O(1)), \quad (10.40)$$

thus proving the soundness result.

The number of random bits used in the expansion protocol is $O(Nh(q))$, and the number used in P_{EIR} is $O(\log N/\epsilon)$, where $\epsilon = \exp(-qN)$. This gives a total of $O(Nh(q) + \log N + qN)$ random bits, which is $O(Nh(q) + \log N)$ (or simply $O(Nh(q))$ when $qN = \Omega(1)$).

We leave the claims on the instantiation to the reader. \square

11 Further Directions

A natural goal at this point is to improve the certified rate of Protocol R. This is important for the practical realization of our protocols. By the discussion in section 8, this reduces to two simple questions. First, what techniques are there for computing the trust coefficient v_G of a binary XOR game? Second, is it possible to reprove Theorem 4.2 in such a way that the limiting function $\pi(x)$ becomes larger? A related question is to improve the key rate of Protocol R_{kd} . The “hybrid” technique of Vazirani and Vidick [Vazirani and Vidick, 2014] for mixing the CHSH game with a trivial game with unit quantum winning strategy may extend to general binary XOR games.

It would also be interesting to explore whether Theorem 1.1 could be extended to nonlocal games outside the class of strong self-tests. Such an extension will not only facilitate the realization of those protocols, but also will further identify the essential feature of quantum information enabling those protocols. As the characterization of strong self-tests is critical for our proof, developing a theory of robust self-testing beyond binary XOR games may be useful for our question. It is also conceivable that there exist fairly broad conditions under which a classical security proof, which is typically much easier to establish, automatically imply quantum security. We consider identifying such a wholesale security lifting principle as a major open problem.

A different direction to extend our result is to prove security based on physical principles more general than quantum mechanics, such as non-signaling principle, or information causality [Pawłowski et al., 2009].

Our protocols require some initial perfect randomness to start with. The Chung-Shi-Wu protocol [Chung et al., 2014] relaxes this requirement to an arbitrary min-entropy source and tolerates a universal constant level of noise. However, those were achieved at a great cost on the number of non-communicating devices. Another major open problem is whether our protocol can be modified to handle non-uniform input.

Randomness expansion can be thought of as a “seeded” extractions of randomness from untrusted quantum devices, in the sense of Chung, Shi, and Wu [Chung et al., 2014]. Our one-shot and unbounded expansion results demonstrate a tradeoff between the seed length and the output length different from that in classical extractors. Recall that a classical extractor with output length N and error parameter ϵ requires $\Omega(\log N/\epsilon)$ seed length, while our unbounded expansion protocol can have a fixed seed length (which determines the error parameter). What is the maximum amount of randomness one can extract from a device of a given amount of entanglement (i.e. is the exponential rate optimal for one device)? What can one say about the tradeoff between expansion rate and some proper quantity describing the communication restrictions? Answers to those questions will reveal fundamental features of untrusted quantum devices as a source for randomness extraction, and will hopefully lead to an intuitive understanding of where the randomness comes from.

Yet another important direction forward is to prove security in more complicated composition scenarios than the cross-feeding protocol. As pointed out by [Barrett et al., 2013], a device reused may store previous runs’ information thus potentially may cause security problem in sequentially composed QKD protocols. While such “memory attack” appears not to be a problem for sequential compositions of our randomness expansion protocol, it may for other more complicated compositions. Thus it is desirable to design untrusted-device protocols and prove their security under broader classes of compositions.

12 Acknowledgments

We are indebted to Anne Broadbent, Kai-Min Chung, Roger Colbeck, Brett Hemenway, Adrian Kent, Christopher Portmann, Thomas Vidick, Ilya Volkovich, Xiaodi Wu, and Andrew Yao for useful discussions, and to Michael Ben-Or, Qi Cheng, Venkatesan Guruswami, and Adam Smith for pointers to the literature on error-correcting codes and information reconciliation.

A Supplementary Material

A.1 The Canonical Form for Two Binary Measurements

Theorem A.1. *Let V be a finite dimensional \mathbb{C} -vector space and let X_0, X_1 be Hermitian operators on V satisfying $\|X_0\|, \|X_1\| \leq 1$. Then, there exists a unitary embedding $U: W \rightarrow \mathbb{C}^{2^n}$, $n \geq 1$, and operators Y_0, Y_1 of the form*

$$Y_0 = \begin{bmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & \ddots \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{bmatrix} \quad Y_1 = \begin{bmatrix} 0 & \zeta_1 & & & \\ \overline{\zeta_1} & 0 & & & \\ & & 0 & \zeta_2 & \\ & & \overline{\zeta_2} & 0 & \\ & & & & \ddots \\ & & & & & 0 & \zeta_{m_j} \\ & & & & & \overline{\zeta_{m_j}} & 0 \end{bmatrix} \quad (\text{A.1})$$

with $\|\zeta_k\| = 1$, such that $X_k = U^* Y_k U$ for $k \in \{0, 1\}$.

We prove this theorem by a series of lemmas. Consider the class of all triples (V, X_0, X_1) satisfying the condition from the first sentence of Theorem A.1. Consider the following two conditions on such triples:

(A) The operators X_k satisfy $X_k^2 = \mathbb{I}$.

(B) The vector space V is equal to \mathbb{C}^m , and X_0, X_1 have a uniform diagonal block form:

$$X_k = \begin{bmatrix} B_k^1 & & & & & \\ & B_k^2 & & & & \\ & & \ddots & & & \\ & & & B_k^r & & \\ & & & & b_k^1 & \\ & & & & & b_k^2 \\ & & & & & & \ddots \\ & & & & & & & b_k^s \end{bmatrix}$$

where $2r + s = m$, $b_k^j \in \{-1, +1\}$ and each B_k^j is a 2×2 Hermitian matrix with eigenvalues $+1$ and -1 .

Lemma A.2. Any triple (V, X_0, X_1) satisfying the conditions of Theorem A.1 has a unitary embedding into a triple satisfying condition (A).

Proof. Let $U: V \rightarrow V \oplus V$ be given by $U(v) = v \oplus 0$, and let $\{X'_k \mid k = 0, 1\}$ be the operators on $V \oplus V$ defined by

$$X'_k = \left[\begin{array}{c|c} X_k & \sqrt{\mathbb{I} - X_k^2} \\ \hline \sqrt{\mathbb{I} - X_k^2} & -X_k \end{array} \right]. \quad (\text{A.2})$$

It is easily checked that $(X'_k)^2 = \mathbb{I}$. □

Lemma A.3. Any triple (V, X_0, X_1) satisfying condition (A) has a unitary embedding into a triple satisfying condition (B).

Proof. We can choose an orthonormal basis $\{v_1, \dots, v_{\dim V}\}$ for V such that X_0 has the form

$$X_0 = \left[\begin{array}{c|c} \mathbb{I}_n & 0 \\ \hline 0 & -\mathbb{I}_m \end{array} \right]. \quad (\text{A.3})$$

where \mathbb{I}_r denotes the $r \times r$ identity matrix. By an appropriate unitary transformation of V that respects this block structure, we obtain another orthonormal basis $\{v'_1, \dots, v'_{\dim v}\}$ such that X_0 and X_1 have the form

$$X_0 = \left[\begin{array}{c|c} \mathbb{I}_n & 0 \\ \hline 0 & -\mathbb{I}_m \end{array} \right] \quad \text{and} \quad X_1 = \left[\begin{array}{c|c} A & D \\ \hline D^* & C \end{array} \right], \quad (\text{A.4})$$

where A and C are diagonal matrices. The condition $X_1^2 = \mathbb{I}$ implies that $A^2 + DD^* = \mathbb{I}$ and $D^*D + C^2 = \mathbb{I}$. Since both DD^* and D^*D are diagonal, D is diagonal. Reordering the bases yields the desired form. □

Lemma A.4. Any triple (V, X_0, X_1) satisfying condition (B) has a unitary embedding into a triple of the form (A.1).

Proof. It suffices to prove the lemma for the case where X_0, X_1 are both scalars, and the case where X_0, X_1 are each 2×2 Hermitian matrices with eigenvalues $+1$ and -1 . The first case is easy and is left to the reader. For the second case, we can find an orthonormal basis $\{v_1, v_2\}$ for \mathbb{C}^2 under which $X_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, and then find a basis of the form $\{(\cos \theta)v_1 + i(\sin \theta)v_2, (\cos \theta)v_2 + i(\sin \theta)v_1\}$ with $z \in \mathbb{C}, |z| = 1$ under which X_1 is an antidiagonal matrix. \square

This completes the proof of Theorem A.1.

A.2 Smooth Min-entropy and Renyi Divergence

This subsection provides supporting proofs for section 3.2.

Proposition A.5. *Let $\alpha \in (1, 2]$. Let ρ be a density operator on a finite-dimensional Hilbert space V , and let σ be a positive semidefinite operator on V such that $\text{Supp } \sigma \supseteq \text{Supp } \rho$. Then, there exists a positive semidefinite operator ρ' such that $\rho' \leq \sigma$ and*

$$\log \|\rho - \rho'\|_1 \leq \frac{\alpha - 1}{2} \cdot D_\alpha(\rho \| \sigma) + \frac{1}{2} \quad (\text{A.5})$$

Proof. Our proof is based on the proof of Lemma 19 in [Dupuis et al., 2015] (which, in turn, is based on [Tomamichel et al., 2009]). For any Hermitian operator H , let P_H^+ denote projection on the subspace spanned by the positive eigenvectors of H , and let $\text{Tr}^+(H) = \text{Tr}(P_H^+ H P_H^+)$. Let

$$\delta = \text{Tr}^+(\rho - \sigma). \quad (\text{A.6})$$

Note that, by the construction from the proof of Lemma 15 in [Tomamichel et al., 2009], there must exist a subnormalized operator ρ' such that $\rho' \leq \sigma$ and $\|\rho' - \rho\|_1 \leq \sqrt{2\delta}$.

Let $P = P_{\rho - \sigma}^+$, and let P^\perp denote the complement of P . Note that by applying the data processing inequality for D_α (see Theorem 5 in [Müller-Lennert et al., 2013]) to the quantum operation $X \mapsto |0\rangle\langle 0| \otimes PXP + |1\rangle\langle 1| \otimes P^\perp X P^\perp$, we have

$$D_\alpha(\rho \| \sigma) \geq \frac{1}{\alpha - 1} \log \left(\text{Tr} \left[\left((P\sigma P)^{\frac{1-\alpha}{2\alpha}} (P\rho P) (P\sigma P)^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right. \right. \quad (\text{A.7})$$

$$\left. + \left((P^\perp(\sigma)P^\perp)^{\frac{1-\alpha}{2\alpha}} (P^\perp \rho P^\perp) (P^\perp \sigma P^\perp)^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right] \right) \quad (\text{A.8})$$

$$\geq \frac{1}{\alpha - 1} \log \left(\text{Tr} \left[\left((P\sigma P)^{\frac{1-\alpha}{2\alpha}} (P\rho P) (P\sigma P)^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right] \right) \quad (\text{A.9})$$

Let $\bar{\sigma} = P\sigma P$ and $\bar{\rho} = P\rho P$. We have the following.

$$D_\alpha(\rho \| \sigma) \geq \frac{1}{\alpha - 1} \log \left(\text{Tr} \left[\left(\bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \bar{\rho} \bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \right) \left(\bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \bar{\rho} \bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \right] \right) \quad (\text{A.10})$$

Note that $\bar{\rho} \geq \bar{\sigma}$ by construction, and $Z \mapsto Z^{\alpha-1}$ is a monotone function (see part (a) of Proposition 3.1). Therefore we have the following.

$$D_\alpha(\rho \| \sigma) \geq \frac{1}{\alpha - 1} \log \left(\text{Tr} \left[\left(\bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \bar{\rho} \bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \right) \left(\bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \bar{\sigma} \bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \right] \right) \quad (\text{A.11})$$

$$\geq \frac{1}{\alpha - 1} \log \left(\text{Tr} \left[\left(\bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \bar{\rho} \bar{\sigma}^{\frac{1-\alpha}{2\alpha}} \right) \bar{\sigma}^{\frac{\alpha-1}{\alpha}} \right] \right) \quad (\text{A.12})$$

$$\geq \frac{1}{\alpha - 1} \log (\text{Tr} [\bar{\rho}]) \quad (\text{A.13})$$

$$\geq \frac{1}{\alpha - 1} \log \delta \quad (\text{A.14})$$

where in the last line we used the fact that $\text{Tr}(\bar{\rho}) \geq \text{Tr}(\bar{\rho} - \bar{\sigma}) = \delta$. Let ρ' be a positive semidefinite operator satisfying $\rho' \leq \sigma$ and $\|\rho' - \rho\|_1 \leq \sqrt{2\delta}$. Then we have

$$D_\alpha(\rho\|\sigma) \geq \frac{1}{\alpha-1} \log \left(\|\rho' - \rho\|_1^2 / 2 \right), \quad (\text{A.15})$$

which implies the desired result. \square

Proposition A.6. *Suppose that in Proposition A.5, V is the state space of a bipartite quantum system AB , and ρ, σ are classical-quantum operators.⁷ Then, there exists an operator ρ' satisfying the conditions of Proposition A.5 such that ρ' itself is a classical-quantum operator.*

Proof. This is an easy consequence of the construction for ρ' (from the proof of Lemma 15 in [Tomamichel et al., 2009]) which was used in the proof of Proposition A.5. \square

of Proposition 3.5. Let λ be the quantity on the right side of inequality (3.22). We have

$$D_\alpha(\rho\|2^{-\lambda}\sigma) = \frac{2 \log \epsilon - 1}{\alpha - 1}. \quad (\text{A.16})$$

By Proposition A.5, we can find a positive semidefinite operator $\rho' \leq 2^{-\lambda}\sigma$ such that

$$\|\rho' - \rho\|_1 \leq \epsilon. \quad (\text{A.17})$$

The result follows from the definition of D_{\max}^ϵ . \square

A.3 Variables and Functions Used in Section 7

In this subsection we collect together the variables in functions that are used in the proof of security for Protocol A' . We include also the assertions about the limits of the functions. (This is intended just for the reader's convenience — all these statements are included in the body of the paper.)

Variables:

$N \in \mathbb{N}$	number of rounds
$q \in (0, 1)$	test probability
$t \in [0, 1]$	failure parameter
$v \in (0, 1]$	trust coefficient
$h \in [0, 1 - v]$	coin flip coefficient
$\eta \in (0, v/2)$	error tolerance
$\kappa \in (0, \infty)$	failure penalty
$r \in (0, 1/(q\kappa)]$	multiplier for Rényi coefficient
$\epsilon \in (0, \sqrt{2}]$	error parameter for smooth min-entropy

Functions:

Note that the functions $\gamma(q, \kappa, r)$ and $\mathbf{r}(v, \eta, q, \kappa)$ defined below are written simply as γ and \mathbf{r} .

⁷That is, A is a classical register and ρ, σ have the form $\rho = \sum_i |a_i\rangle \langle a_i| \otimes \rho_i$ and $\sigma = \sum_i |a_i\rangle \langle a_i| \otimes \sigma_i$ where $\{a_1, \dots, a_n\}$ is a standard basis for A .

$$\gamma(q, \kappa, r) := q\kappa r$$

$$\lim_{(q, \kappa) \rightarrow (0, 0)} \gamma(q, \kappa, r) = 0$$

$$\Pi(\gamma, t) := -\frac{1}{\gamma} \log \left\{ 2^{-\gamma} \left[(1-t)^{\frac{1}{1+2\gamma}} + t^{\frac{1}{1+2\gamma}} \right]^{1+2\gamma} \right\}$$

$$\pi(t) := 1 - 2t \log \left(\frac{1}{t} \right) - 2(1-t) \log \left(\frac{1}{1-t} \right)$$

$$\lim_{(q, \kappa, t) \rightarrow (0, 0, t_0)} \Pi(\gamma, t) = \pi(t_0)$$

$$\lambda(v, h, q, \kappa, r, t) := \left((1-q)2^{-\gamma\Pi(\gamma, t)} + q \left\{ 1 - (1-2^{-\kappa})[(h/2)^{1+\gamma} + v^{1+\gamma}t] \right\} \right)^{1/\gamma}$$

$$\Lambda(v, h, q, \kappa, r, t) := -\log(\lambda(v, h, q, \kappa, r, t))$$

$$\lim_{(q, \kappa, t) \rightarrow (0, 0, t_0)} \Lambda(v, h, q, \kappa, r, t) = \pi(t_0) + \frac{h/2 + vt_0}{r}$$

$$\Delta(v, h, q, \kappa, r) := \min_{s \in [0, 1]} \Lambda(v, h, q, \kappa, r, s)$$

$$\lim_{(q, \kappa) \rightarrow (0, 0)} \Delta(v, h, q, \kappa, r) = \min_{s \in [0, 1]} \left(\pi(s) + \frac{h/2 + vs}{r} \right)$$

$$R(v, h, \eta, q, \kappa, r) := -\frac{h/2 + \eta}{r} + \Delta(v, h, q, \kappa, r)$$

$$\lim_{(q, \kappa) \rightarrow (0, 0)} R(v, h, \eta, q, \kappa, r) = \min_{s \in [0, 1]} \left[\pi(s) + \frac{vs - \eta}{r} \right]$$

$$\mathbf{r}(v, \eta, q, \kappa) := \min \left\{ \frac{v}{-\pi'(\eta/v)}, \frac{1}{q\kappa} \right\}$$

$$\lim_{(q, \kappa) \rightarrow (0, 0)} \mathbf{r}(v, \eta, q, \kappa) = \frac{v}{-\pi'(\eta/v)}$$

$$T(v, h, \eta, q, \kappa) := R(v, h, \eta, q, \kappa, \mathbf{r})$$

$$\lim_{(q, \kappa) \rightarrow (0, 0)} T(v, h, \eta, q, \kappa) = \pi(\eta/v)$$

$$F(v, h, \eta, q, \kappa) := \frac{2}{\mathbf{r}}$$

$$\lim_{(q, \kappa) \rightarrow (0, 0)} F(v, h, \eta, q, \kappa) = \frac{-2\pi'(\eta/v)}{v}$$

A.4 Mathematical Results

Proposition A.7. Let $U \subseteq \mathbb{R}^n$, let $\mathbf{z} \in \mathbb{R}^n$ be an element in the closure of U , and let f, g be continuous functions from U to \mathbb{R} . Suppose that

$$\lim_{\mathbf{x} \rightarrow \mathbf{z}} f(\mathbf{x}) = 0 \tag{A.18}$$

and

$$\lim_{\mathbf{x} \rightarrow \mathbf{z}} \frac{f(\mathbf{x})}{g(\mathbf{x})} = c. \tag{A.19}$$

Then,

$$\lim_{\mathbf{x} \rightarrow \mathbf{z}} (1 + f(\mathbf{x}))^{1/g(\mathbf{x})} = e^c. \tag{A.20}$$

Proof. This can be proved easily by taking the natural logarithm of both sides of (A.20). \square

Proposition A.8. Let $U \subseteq \mathbb{R}^n$ and $V \subseteq \mathbb{R}^m$, and assume that V is **compact**. Let $f: U \times V \rightarrow \mathbb{R}$ be a continuous function. Let $\mathbf{z} \in \mathbb{R}^n$ be an element in the closure of U , and assume that $\lim_{(\mathbf{x}, \mathbf{y}) \rightarrow (\mathbf{z}, \mathbf{y}_0)} f(\mathbf{x}, \mathbf{y})$ exists for every $\mathbf{y}_0 \in V$. Then,

$$\lim_{\mathbf{x} \rightarrow \mathbf{z}} \min_{\mathbf{y} \in V} f(\mathbf{x}, \mathbf{y}) = \min_{\mathbf{y} \in V} \lim_{\mathbf{x} \rightarrow \mathbf{z}} f(\mathbf{x}, \mathbf{y}). \quad (\text{A.21})$$

Proof. By assumption, there exists a continuous extension of f to $(U \cup \{\mathbf{z}\}) \times V$. Denote this extension by \bar{f} . Let $h(\mathbf{x}, \mathbf{y}) = \bar{f}(\mathbf{x}, \mathbf{y}) - \bar{f}(\mathbf{z}, \mathbf{y})$.

Let $\delta > 0$. For any $\mathbf{y} \in V$, since $h(\mathbf{z}, \mathbf{y}) = 0$ and h is continuous at (\mathbf{z}, \mathbf{y}) , we can find an $\epsilon_{\mathbf{y}} > 0$ such that the values of h on the cylinder

$$\{(\mathbf{x}, \mathbf{y}') \mid |\mathbf{x} - \mathbf{z}| < \epsilon_{\mathbf{y}}, |\mathbf{y}' - \mathbf{y}| < \epsilon_{\mathbf{y}}\} \quad (\text{A.22})$$

are confined to $[-\delta, \delta]$. Since V is compact, we can choose a finite set $S \subseteq V$ such that the $\epsilon_{\mathbf{y}}$ -cylinders for $\mathbf{y} \in S$ cover V . Letting $\epsilon = \min_{\mathbf{y} \in S} \epsilon_{\mathbf{y}}$, we find that the values of h on the ϵ -neighborhood of V are confined to $[-\delta, \delta]$. Therefore, the minimum of $f(\mathbf{x}, \mathbf{y})$ on the ϵ -neighborhood of V is within δ of $\min_{\mathbf{y} \in V} \bar{f}(\mathbf{z}, \mathbf{y})$. The desired equality (A.21) follows. \square

References

- [Alon et al., 1992] Alon, N., Bruck, J., Naor, J., Naor, M., and Roth, R. M. (1992). Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38(2):509–516.
- [Barrett et al., 2012] Barrett, J., Colbeck, R., and Kent, A. (2012). Unconditionally secure device-independent quantum key distribution with only two devices. *Phys. Rev. A*, 86:062326.
- [Barrett et al., 2013] Barrett, J., Colbeck, R., and Kent, A. (2013). Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 110:010503.
- [Barrett et al., 2005] Barrett, J., Hardy, L., and Kent, A. (2005). No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503.
- [Bennett and Brassard, 1984] Bennett, C. and Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing*, 11:175–179.
- [Bennett et al., 1991] Bennett, C. H., Brassard, G., Crépeau, C., and Skubiszewska, M.-H. (1991). Practical quantum oblivious transfer. In Feigenbaum, J., editor, *Advances in Cryptology—CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer-Verlag, 1992.
- [Bennett et al., 1988] Bennett, C. H., Brassard, G., and Robert, J.-M. (1988). Privacy amplification by public discussion. *SIAM journal on Computing*, 17(2):210–229.
- [Biham et al., 2006] Biham, E., Boyer, M., Boykin, P. O., Mor, T., and Roychowdhury, V. (2006). A proof of the security of quantum key distribution. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(4):381–439.

- [Boneh and Shoup, 2015] Boneh, D. and Shoup, V. (2015). *A Graduate Course in Applied Cryptography*. Available at https://crypto.stanford.edu/~dabo/cryptobook/draft_0_2.pdf.
- [Carlen, 2009] Carlen, E. A. (2009). Trace inequalities and quantum entropy: An introductory course. In Sims, R. and Ueltschi, D., editors, *Entropy and the Quantum*, volume 529 of *Contemporary Mathematics*, pages 73–140.
- [Chung et al., 2014] Chung, K.-M., Wu, X., and Shi, Y. (2014). Physical randomness extractors. arXiv:1402.4797v3.
- [Colbeck, 2006] Colbeck, R. (2006). *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge.
- [Colbeck and Kent, 2011] Colbeck, R. and Kent, A. (2011). Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305.
- [Colbeck and Renner, 2012] Colbeck, R. and Renner, R. (2012). Free randomness can be amplified. *Nature Physics*, 8:450–454.
- [Coudron et al., 2013] Coudron, M., Vidick, T., and Yuen, H. (2013). Robust randomness amplifiers: Upper and lower bounds. In Raghavendra, P., Raskhodnikova, S., Jansen, K., and Rolim, J. D. P., editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, volume 8096 of *Lecture Notes in Computer Science*, pages 468–483. Springer.
- [Coudron and Yuen, 2014] Coudron, M. and Yuen, H. (2014). Infinite randomness expansion with a constant number of devices. *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC '14)*, pages 427–436.
- [Datta, 2009] Datta, N. (2009). Min- and max- relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826.
- [De et al., 2012] De, A., Portmann, C., Vidick, T., and Renner, R. (2012). Trevisan’s extractor in the presence of quantum side information. *SIAM J. Comput.*, 41(4):915–940.
- [Dembo and Zeitouni, 1997] Dembo, A. and Zeitouni, O. (1997). *Large Deviations Techniques and Applications*. Springer, 2nd edition.
- [Deng and Duan, 2013] Deng, D.-L. and Duan, L.-M. (2013). Fault-tolerant quantum random-number generator certified by majorana fermions. *Phys. Rev. A*, 88:012323.
- [Dupuis et al., 2015] Dupuis, F., Fawzi, O., and Wehner, S. (2015). Entanglement sampling and applications. *IEEE Transactions on Information Theory*, 61(2):1093–1112.
- [Ekert, 1991] Ekert, A. K. (1991). Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.*, 67:661–663.
- [Fehr et al., 2013] Fehr, S., Gelles, R., and Schaffner, C. (2013). Security and composability of randomness expansion from Bell inequalities. *Phys. Rev. A*, 87:012335.
- [Greenberger et al., 1989] Greenberger, D., Horne, M., and Zeilinger, A. (1989). Going beyond Bell’s theorem. In Kafatos, M., editor, *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, pages 69 – 72. Kluwer, Dordrecht.

- [Guruswami, 2003] Guruswami, V. (2003). List decoding with side information. In *IEEE Conference on Computational Complexity*, page 300. IEEE Computer Society.
- [Guruswami and Indyk, 2005] Guruswami, V. and Indyk, P. (2005). Linear-time encodable/decodable codes with near-optimal rate. *IEEE Transactions on Information Theory*, 51(10):3393–3400.
- [Guruswami and Rudra, 2006] Guruswami, V. and Rudra, A. (2006). Explicit capacity-achieving list-decodable codes. In Kleinberg, J. M., editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 1–10. ACM.
- [Guruswami and Rudra, 2008] Guruswami, V. and Rudra, A. (2008). Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150.
- [Guterman et al., 2006] Guterman, Z., Pinkas, B., and Reinman, T. (2006). Analysis of the linux random number generator. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy, SP '06*, pages 371–385, Washington, DC, USA. IEEE Computer Society.
- [Hänggi et al., 2010] Hänggi, E., Renner, R., and Wolf, S. (2010). Efficient device-independent quantum key distribution. In *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 216–234. See also: Quantum cryptography based solely on Bell’s theorem, arXiv:0911.4171.
- [Heninger et al., 2012] Heninger, N., Durumeric, Z., Wustrow, E., and Halderman, J. A. (2012). Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Security Symposium*.
- [Jaksic et al., 2010] Jaksic, V., Ogata, Y., Pautrat, Y., and Pillet, C.-A. (2010). Entropic fluctuations in quantum statistical mechanics. an introduction. *Quantum Theory from Small to Large Scales: Lecture Notes of the Les Houches Summer School*, 95.
- [Lenstra et al., 2012] Lenstra, A. K., Hughes, J. P., Augier, M., Bos, J. W., Kleinjung, T., and Wachter, C. (2012). Ron was wrong, Whit is right. *IACR Cryptology ePrint Archive*, 2012:64.
- [Lo and Chau, 1999] Lo, H.-K. and Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056.
- [Masanes et al., 2011] Masanes, L., Pironio, S., and Acin, A. (2011). Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2(238).
- [Mayers, 2001] Mayers, D. (2001). Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406.
- [Mayers and Yao, 1998] Mayers, D. and Yao, A. (1998). Quantum cryptography with imperfect apparatus. In *Proc. 39th FOCS*, pages 503–509.
- [McKague, 2014] McKague, M. (2014). *Theory of Quantum Computation, Communication, and Cryptography: 6th Conference, TQC 2011, Madrid, Spain, May 24-26, 2011, Revised Selected Papers*, chapter Self-Testing Graph States, pages 104–120. Springer Berlin Heidelberg, Berlin, Heidelberg.

- [Miller and Shi, 2013] Miller, C. A. and Shi, Y. (2013). Optimal robust self-testing by binary non-local XOR games. In Severini, S. and Brandão, F. G. S. L., editors, *8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2013, May 21-23, 2013, Guelph, Canada*, volume 22 of *LIPICs*, pages 254–262. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. Full version: arXiv:1207.1819v4.
- [Müller-Lennert et al., 2013] Müller-Lennert, M., Dupuis, F., Szehr, O., Fehr, S., and Tomamichel, M. (2013). On quantum Rényi entropies: a new generalization and some properties. *Journal of Mathematical Physics*, 54:122203.
- [Nayak et al., 2008] Nayak, C., Simon, S. H., Stern, A., Freedman, M., and Das Sarma, S. (2008). Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys.*, 80:1083–1159.
- [Pawłowski et al., 2009] Pawłowski, M., Paterek, T., Kaszlikowski, D., Scarani, V., Winter, A., and Żukowski, M. (2009). Information causality as a physical principle. *Nature*, 461:1101–1104.
- [Perlroth et al., 2013] Perlroth, N., Larson, J., and Shane, S. (2013). N.S.A. able to foil basic safeguards of privacy on web. *The New York Times*, September 5.
- [Pironio et al., 2010] Pironio, S., Acín, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D. N., Maunz, P., Olmschenk, S., Hayes, D., Luo, L., Manning, T. A., and Monroe, C. (2010). Random numbers certified by Bell’s theorem. *Nature*, 464:1021–1024.
- [Pironio and Massar, 2013] Pironio, S. and Massar, S. (2013). Security of practical private randomness generation. *Phys. Rev. A*, 87:012336.
- [Pisier and Xu, 2003] Pisier, G. and Xu, Q. (2003). Non-commutative L^p -spaces. In *Handbook of the geometry of Banach spaces, Vol. 2*, pages 1459–1517. North-Holland, Amsterdam.
- [Reichardt et al., 2013] Reichardt, B. W., Unger, F., and Vazirani, U. (2013). Classical command of quantum systems. *Nature*, 496:456–460.
- [Renner, 2005] Renner, R. (2005). *Security of Quantum Key Distribution*. PhD thesis, ETH. arXiv:0512258.
- [Ristenpart and Yilek, 2010] Ristenpart, T. and Yilek, S. (2010). When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. In *NDSS. The Internet Society*.
- [Robert, 1985] Robert, J.-M. (1985). Détection et correction d’erreurs en cryptographie. Master’s thesis, Université de Montréal.
- [Shor and Preskill, 2000] Shor, P. W. and Preskill, J. (2000). Simple proof of security of BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444.
- [Smith, 2007] Smith, A. (2007). Scrambling adversarial errors using few random bits, optimal information reconciliation, and better private codes. In Bansal, N., Pruhs, K., and Stein, C., editors, *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2007, New Orleans, Louisiana, USA, January 7-9, 2007*, pages 395–404. SIAM.
- [Tomamichel et al., 2009] Tomamichel, M., Colbeck, R., and Renner, R. (2009). A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55(12):5840–5847.

- [Tomamichel et al., 2010] Tomamichel, M., Colbeck, R., and Renner, R. (2010). Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56:4674–4681.
- [Tomamichel and Leverrier, 2015] Tomamichel, M. and Leverrier, A. (2015). A rigorous and complete proof of finite key security of quantum key distribution. arXiv:1506.08458.
- [Trevisan, 2001] Trevisan, L. (2001). Extractors and pseudorandom generators. *J. ACM*, 48(4):860–879.
- [Vazirani and Vidick, 2014] Vazirani, U. and Vidick, T. (2014). Fully device independent quantum key distribution. *Physical Review Letters*, 113(140501).
- [Vazirani and Vidick, 2012] Vazirani, U. V. and Vidick, T. (2012). Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In Karloff, H. J. and Pitassi, T., editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 61–76. ACM.
- [Wehner and Winter, 2010] Wehner, S. and Winter, A. (2010). Entropic uncertainty relations—a survey. *New Journal of Physics*, 12(025009).
- [Werner and Wolf, 2001] Werner, R. F. and Wolf, M. M. (2001). All-multipartite Bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64(3):32112.
- [Wilde et al., 2014] Wilde, M. M., Winter, A., and Yang, D. (2014). Strong converse for the classical capacity of entanglement-breaking and hadamard channels via a sandwiched rényi relative entropy. *Communications in Mathematical Physics*, 331(2):593–622.