On the Communication Complexity of Correlation and Entanglement Distillation

Ke Yang

May 4th, 2004

School of Computer Science
Computer Science Department
Carnegie Mellon University
Pittsburgh, PA

Thesis Committee

Steven Rudich (chair)
Avrim Blum
Robert Griffiths
Andris Ambainis (IAS, Princeton)

Submitted in partial fulfillment of the requirements for the Degree of Doctor of Philosophy

Abstract

One of the recurring themes in information theory and quantum information theory is correlation corruption and correlation recover. Correlation corruption refers to the situation where Alice and Bob share information that is not perfectly correlated (or perfectly entangled, if they share quantum information). Correlation corruption arises in many natural situations, including transmitting information through a noisy channel, measuring a noisy signal source, quantum decoherence, and adversarial distortion. Correlation recovery refers to the action Alice and Bob takes to "restore" the correlation/entanglement by agreeing on some perfectly correlated/entangled information.

Traditionally correlation repair is done via a preventive strategy, namely error correction. Using this strategy, Alice encodes her information using an error correcting code or a quantum error correcting code before sending it through a noisy channel to Bob, who then decodes and recovers the original information. Error correcting codes and quantum error correcting codes are extremely useful objects in information theory with numerous applications in many other areas of science and technology. They are well studied and well understood. However they have limitations. We shall show that some assumptions used by error correction are not sound in many scenarios and make the preventive strategy unsuitable.

We study the alternative strategy of correlation repair, known as the reparative strategy. Using this strategy, Alice and Bob start by sharing imperfectly correlated (raw) information, and then engage in a protocol to "distill" the correlation/entanglement via communication. We call these protocols (classical) correlation distillation protocols and (quantum) entanglement distillation protocols. We show that such a reparative strategy can be as efficient as the preventive strategy. Furthermore, the reparative strategy is more flexible, in that it doesn't have the limitations suffered by error correction. We also point out that in particular, quantum entanglement distillation protocols play a very important role in quantum information theory. Despite the significance of these protocols, they have received much less attention than error correcting codes and are much less well understood.

We focus on the communication complexity of the correlation and entanglement distillation protocols. In designing error correcting codes, efficiency is one of the main concerns. One wants to construct an error correcting code with the least possible redundancy while being able to withhold the highest rate of noise. In correlation and entanglement distillation protocols, the efficiency is measured by the amount the communication between Alice and Bob, and thus it is important to design protocols with minimal amount of communication. Our study is concerned with the minimal amount the communication needed for distillation.

We present a number of results concerning communication complexity for protocols over various noise models, which are mathematically models for different types of correlation corruption. These results span both classical and quantum information theory, and have connections to other areas of computer science, including cryptography and computational complexity.

Chapter 1

Introduction

We introduce the notion of correlation distillation and entanglement distillation and discuss the motivations, as well as related work.

1.1 Correlation Corruption and Correlation Repair

Information theory, since its inception in 1948 by Claude Shannon in his groundbreaking paper [81], has developed into a rich field of research, with applications in a broad spectrum of areas, including electrical engineering, computer science, statistics, and physics. From the 1970s, as researchers start to understand quantum mechanics, the field of quantum information theory emerged as a natural extension to the classical information theory. Exciting (and sometimes confusing) results are discovered, like the EPR paradox (that two quantum states can be space-separated yet entangled, such that their measurements will be correlated), the non-cloning theorem (that quantum information cannot be duplicated), and the teleportation (that Alice and transmit an unknown quantum state to Bob by sending 2 classical bits). Not only did quantum information theory contribute to the development of quantum mechanics, it also found applications in "traditional" areas, such as cryptography.

One of the most recurring themes in information theory is *correlation corruption* and *correlation recovery*. Correlation corruption refers to the situation where Alice and Bob share some information which is not perfectly "correlated". Classically this means that with positive probability, Alice's bits doesn't agree with Bob's. Quantum mechanically, this means that Alice's quantum state isn't perfectly entangled with Bob's quantum state. Researchers have striven to understand the nature of correlation corruption and model it mathematically; we call them *noise models*. On the other hand, correlation recovery refers to the action Alice and Bob take to "restore" the correlation (or entanglement) to the maximum. Naturally, the goal is to **perform correlation repair, using as little resource as possible**.

We discuss some situations where the theme of correlation corruption and correlation recovery occurs naturally.

1.1.1 Information Transmission

Perhaps the most well-known problem in information theory is to transmit information through a noisy channel. In fact, it was considered in Shannon's original paper [81] and was one of the most important motivations for information theory. When Alice sends information to Bob through a *noisy channel*, the channel will "distort" the information. More concretely, suppose Alice sends classical bits to Bob, a classical noisy channel may flip some of the bits (a bit "0" will become "1", and a bit "1" will become "0"), or erase some of the bits (a bit becomes "$\perp$", which is a special symbol indicating the loss of the bit); suppose Alice sends qubits to Bob, a quantum noisy channel may apply a "bit-flip" (normally denoted by X) which switches $|0\rangle$ and $|1\rangle$, a "phase-shift" (normally denoted by Z), which keeps $|0\rangle$ unchanged but changes $|1\rangle$ to $-|1\rangle$, or a bit-flip composed with a phase-shift (normally denoted by Y). If Alice keeps a copy of the information she sends to Bob, then the noisy channel will The noisy channel can certainly corrupt the correlation between Alice and Bob. A large part of information theory is to understand the nature of these noisy channels and devise mechanisms to fight the noise, namely, to perform correlation recovery.

1.1.2 Random Beacons

A random beacon is an entity that broadcasts uncorrelated unbiased random bits. The concept of random beacons were first introduced in 1983 by Rabin [73], who showed how they can be used to solve problems in cryptography. Bennett, DiVincenzo, and Linsker [25] proposed to use a random beacon to authenticate video recording. Maurer [59], Aumann and Rabin [6], and Ding [32] proposed to use a random beacon of extremely high rate to build information-theoretically secure cryptographic primitives, e.g., key exchange, encryption, and oblivious transfer. von Ahn et. al. [2] discusses various applications of random beacons, including verifiable lotteries and proof of ignorance.

There are many proposals to construct a *public, verifiable* random beacon, among them are the ones that use the signals from a cosmic source [2, 62]. In these proposals, Alice (as the beacon owner) and Bob (as a verifier) both point a radio telescope to some extraterrestrial objects, e.g. pulsars, and then measure the signal from them, which presumably contains enough amount of randomness. However, it is inevitable that Alice and Bob have discrepancy in their results, due to measurement errors. Nevertheless, Alice and Bob still wish to agree on some common random bits, or, in other words, to recover the correlation between them. Notice that the random bits they wish to agree on are not necessarily the "raw data" from the measurement. Alice and Bob are free to apply any transformation to their measurement results.

1.1.3 Distilling EPR Pairs

An EPR pair, or an Einstein-Podolsky-Rosen pair [34], is a qubit pair in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ shared by two parties, with one party (Alice) holding one quantum bit and the other party (Bob) holding the second bit. EPR pairs are maximally entangled states and play a very important role in quantum information theory. Using an EPR pair, Alice and Bob can perform quantum teleportation. By performing only local operations and classical communication (often abbreviated as "LOCC"), Alice can "transport" a qubit to Bob, who could be miles away from Alice [17]. So EPR pairs, along with a classical communication channel, effectively constitute a quantum channel. Conversely, "superdense coding" is possible with EPR pairs: if Alice and Bob share an EPR pair, then Alice can transport two classical bits to Bob by just sending one qubit [28]. Therefore, it is quite desirable for Alice and Bob to pre-manufacture a large number of EPR pairs and store them. In this way, they only need to maintain a classical channel between them, which is much more economical than a quantum channel, to transmit quantum information.

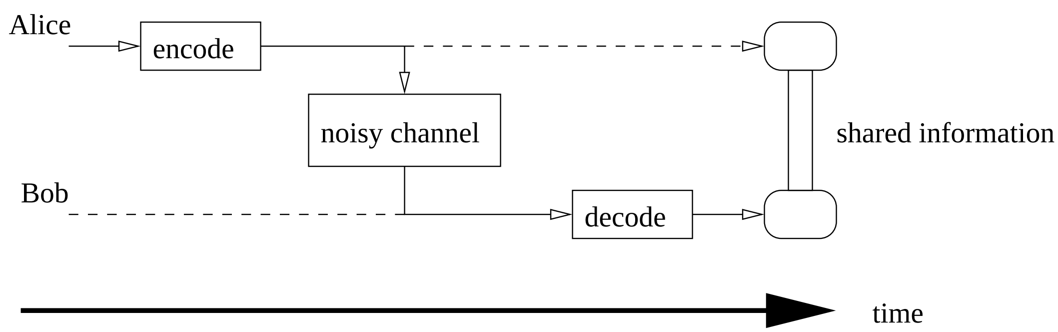
However, it is very hard to store qubits; qubits can easily become entangled with environment and *decohere*. Moreover, the decoherence happen continuously with time, which is hard to prevent with current technology. This poses a serious problem to teleportation, since teleportation needs perfect EPR pairs, and if EPR pairs cannot be stored almost perfectly, teleportation would not be useful. Therefore, Alice and Bob need to "distill" almost perfect EPR pairs from the noise ones, or, in other words, to "recover" the entanglement.

1.1.4 Quantum Key Distribution

Consider the quantum key distribution protocols by Bennett and Brassard [15], and by Bennett [12], where Alice randomly produces a sequence of qubits and send them to Bob, who then measures them. If Alice keeps a copy of the qubits she sends to Bob, then Alice and Bob will share a number of perfectly entangled states. Next, Alice and Bob can exchange information to agree on some random bits, which then can be used as their shared key. However, Eve, the eavesdropper, might intercept some of the qubits Alice sent and distort them. This distortion caused by Eve will result in imperfectly entangled states between Alice and Bob. Therefore, they need to recover from the imperfect entanglement and agree on almost perfectly entangled states, or EPR pairs.

1.2 Error Correction: the Preventive Strategy

The most popular strategy to correlation repair is though the means of Error Correcting Codes (ECCs) and Quantum Error Correcting Codes (QECCs). Consider the situation of transmitting information through a noisy channel. Alice can *encode* her information using an *error correcting code*, or a *quantum error correcting code* into a *code-word*, before sending it to Bob. Then Bob can *decode* the noisy code-word and recover the information. See Figure 1.1. We call this the "preventive" strategy, since preventive measures are taken before the corruption takes place.



Alice encodes the information before sending it through a noisy channel, after which Bob decodes.

Figure 1.1: Preventive strategy for correlation repair

Error correcting codes and quantum error correcting codes have long been central objects of study in the field of information theory, and they have received tremendous amount of attention. More over, not only are they extremely useful in information theory, they also found numerous applications in other fields, including combinatorics, cryptography, and computational complexity. However, they have their limitations.

Timing Constraint

First of all, there is the *timing constraint*. Error correction codes only works where Alice can encode the information *before* the noise takes place, which is not always possible. Consider the random beacon where Alice and Bob measure the noisy signals from a pulsar. In this case, it is impossible to encode the signal from the pulsar and error correction becomes totally useless.

Assumptions on Noise Model

Moreover, almost all research work on error correcting codes focus on a relatively limited noise model, which we call the *identical independent distortion (IID)*. In this model, the information is transmitted in units (e.g. bits or qubits) through a noisy channel, which applies a "distortion" process to each of the units independently. Examples of the deformation process include "flip a bit with probability ϵ" (which corresponds to the Binary Symmetric Channel), "change a bit to $\perp$ with probability ϵ" (which corresponds to the Erasure Channel), and "replace a qubit by a a completely mixed state with probability ϵ" (which corresponds to the Depolarization Channel). Two important assumptions in the IID model is that: 1) the deformation processes are identical to each unit; 2) the processes are independent. These two assumptions greatly simplify the problem of error correction, since the Law of the Large Numbers can be used. One can thus separate the so-called "typical error syndromes" from the "atypical" ones, and only focus on the typical syndromes. However, it is not always realistic to assume the IID model. This is best illustrated by the case of quantum key distribution protocols. Recall in this situation, Eve may intercept some qubits sent by Alice and cause distortion. Notice Eve is adversarial in nature and there is no reason to assume the the noise she causes is IID. Therefore, quantum error correction is not suitable in this case.

As a comment, we point out that Shor and Preskill [83] in fact used a particular class of quantum error correcting codes (known as CSS codes) in the analysis of security of the BB84 protocol. In particular, they showed that this class of QECCs, which were originally designed to work in a so-called "bounded corrupt" noise model, work in the so-called "fidelity" noise model as well, which is an adversarial model and is suitable for the quantum key distribution protocol. However, this appears to be a coincidence, and there is no evidence that any QECC designed for a non-adversarial model will automatically work for an adversarial one.

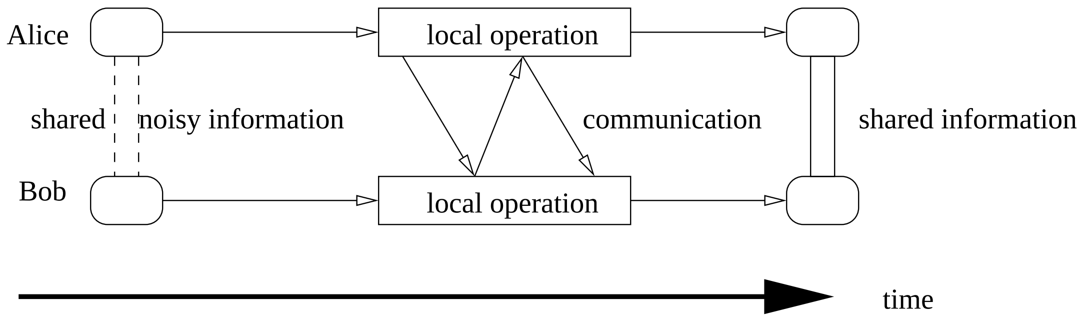
Assumptions on Noise Rate

Finally, error correcting assumes that the *noise rate* is known at the time of encoding, so that an appropriate encoding scheme with appropriate amount of redundancy can be designed. Notice that the noise rate has to be determined before the noise actually takes place, and therefore one often has to *guess* the rate. If the guess is too high, then too much redundancy would be added and bandwidth wasted; if the guess is too low, then too little redundancy may cause the loss of information. Furthermore, there are situations where there simply isn't a fixed noise rate. Take the decohering EPR pairs as an example. The decoherence happens continuously with time, and thus the noise rate is varying with time (more precisely, increases with time). In this case, it is rather inefficient and inflexible to use an quantum error correcting code of a fixed rate.

1.3 Correlation Distillation: the Reparative Strategy

Correlation Distillation Protocols (CDPs) and Entanglement Distillation Protocols (EDPs) provide an alternative strategy for correlation repair. In this strategy, Alice and Bob start by sharing imperfectly consistent information, and then "distill" near-perfect information via communication and local operations. See Figure 1.2. If it is the classical information Alice and Bob are to distill, we call the process a "correlation distillation protocol"; if it is the quantum information, we call it an "entanglement distillation protocol". Overall, we call it the "reparative strategy".

As a technical note, we always assume that the communication in the protocols is classical and noise-free. It is a standard assumption that only classical communication is allowed in quantum entanglement distillation protocols, since quantum communication is considerably more expensive.



Alice and Bob start by sharing noisy information. They then perform local operation and communication to boost correlation.

Figure 1.2: Reparative strategy for correlation repair

These protocols that only involve local operations and classical communications are called "LOCC protocols", standing for "Local Operation Classical Communication". The assumption of noise-free communication can be justified in the following ways. First, the amount of communication is normally much smaller than the amount of the information Alice and Bob share, and thus they can afford to protect their communication either using a communication channel of higher quality or using error correcting of high redundancy. Second, much of the study in this thesis focus on the question of how much information Alice and Bob need to exchange in order to perform correlation/entanglement distillation, and the assumption of noiseless communication greatly simplifies the analysis. Finally, in the case of entanglement distillation, classical communication is used to distill quantum entanglement, and it is reasonable to assume a noise-free classical channel while the quantum channel might be noisy.

Correlation distillation protocols and entanglement distillation protocols solve some problems with error correcting codes and quantum error correcting codes. First, since the distillation takes place after the noise, there is no timing constraint for correlation/entanglement distillation. Therefore, CDPs are suitable for situations like random beacons. Furthermore, since Alice and Bob perform distillation only after the noise, they can measure the noise rate first, and then choose the appropriate distillation protocol. This is more flexible and some times more desirable than error correction, which needs to guess the noise rate (for example, in the case of decohering EPR pairs). In fact, as we shall exhibit later in the thesis, there exist situations (both in classical and in quantum) where error correction almost completely fails while it is still possible to do correlation distillation. See Section **??**. Finally, as we shall discuss later, CDP/EDPs admit a broader range of noise models, and in particular, noise models that are not identical independent distortion. In particular, while QECCs are not appropriate for quantum key distribution protocols, where the noise model is adversarial, EDPs turned out to be the perfect solution, as pointed out by Lo and Chau [56] and Shor and Preskill [83] (they used the term "entanglement purification protocols" for EDPs). [1]

Besides the "practical" advantages of EDPs, they have great theoretical importance in quantum information theory. Quantum entanglement plays a crucial role. Researchers have striven to understand entanglement, and in particular, ways to measure the amount the entanglement as a physical resource. Among various proposals is the concept of *distillable entanglement*[24]. For aquantum state ρ, its distillable entanglement is defined to be asymptotically the ratio of the amount of EPR

[1] In fact, Shor and Preskill used CSS codes, which are a special class of quantum error correcting codes, in their proof. See the discussion before.

pairs that can be produced by the optimal EDP from n copies of state ρ over n, as n increases. Clearly, the study of entanglement distillation protocols is closely related to that of entanglement.

If we compare the two approaches to information agreement, ECC/QECC and CDP/EDP, perhaps the most salient difference between them is that ECC/QECCs are algorithms performed by a single party (Alice for encoding and Bob for decoding), while CDP/EDP are two-party protocols that involve communication. In designing ECC/QECCs, *overhead* is one of the main concerns and the goal is to design ECC/QECCs with as low as possible overhead that can withstand an as high as possible noise rate. For CDP/EDPs, the overhead is the amount of communication between Alice and Bob, i.e., the number of bits exchanged between them. Therefore, the *communication complexity* of CDP/EDPs is one of their most important parameters.

1.4 Our Contributions

In this thesis, we study the communication complexity of correlation and entanglement distillation protocols. Since CDP/EDPs are protocols, they are more complicated objects than ECC/QECCs. For example, with protocols, one might want to distinguish *one-way* communication, where only Alice sends information to Bob, who never sends anything back, from *two-way* communications, where Alice and Bob exchange bits. A protocol can be *deterministic*, where both Alice and Bob are deterministic, *randomized*, where Alice and Bob can have their own supply of random bits, or *randomized public-coin*, where Alice and Bob share a common random source.[2] It is the focus of this thesis to study various type of CDP/EDPs over a large range of noise models.

We briefly summarize a collection of results of the study.

1. **A Relation Between ECC/QECCs and CDP/EDPs**

   We relate a large class of error correcting codes and quantum error correcting codes to correlation distillation protocols and entanglement distillation protocols. More precisely, we point out that every linear ECC corresponds to a CDP over the same noise model with the same overhead, and every stabilizer QECC corresponds to an EDP over the same noise model with the same overhead.

2. **An Impossibility Result for Non-Interactive Correlation Distillation**

   We show a general impossible result for non-interactive correlation distillation over a number of natural noise models. We also show how this result is related to various research areas, including random beacon and information reconciliation.

3. **A Positive Result on One-bit Correlation Distillation**

   We present a positive result where Alice and Bob, but exchanging one bit of information, can perform correlation repair, which were impossible without communication. This shows that even the minimal amount of communication can help in correlation repair.

4. **An Impossibility Result of Non-Interactive Entanglement Distillation**

   We show several impossibility results for non-interactive entanglement distillation, where Alice and Bob wish to produce near-EPR pairs without communication. These are the first results in the area of communication complexity of EDPs, and they provide the first step in understanding entanglement distillation protocols.

[2] We are using the notations from Kushilevitz and Nisan [51].

5. **An Impossibility Result of EDPs over the Entanglement Noise Model**

   We prove an impossibility result on entanglement distillation over the so-called "entanglement noise model". We show that it is impossible to distill EPR pairs from an arbitrarily entangled quantum state. We show how this result is related to classical randomness extractors.

6. **A Complete Characterization of EDPs over the Fidelity Noise Model**

   We completely characterize the communication complexity of entanglement distillation protocols over the so-called "fidelity noise model". We present a protocol that distills near-perfect EPR pairs very efficiently, and prove such a protocol is in fact optimal (up to an additive constant). We also show how this noise model is related to other areas of quantum information theory, including purity-testing protocols [22] and quantum key-distribution protocols [56, 83].

These results appear in the following publications.

1. A. Ambainis, A. Smith, K. Yang.
   Extracting Quantum Entanglement (General Entanglement Purification Protocols).
   Appeared in the *IEEE Conference of Computational Complexity (CCC 2002)*, Montréal, Quebéc, Canada, pp. 103-112, 2002.

2. K. Yang.
   On the (Im)possibility of Non-interactive Correlation Distillation.
   Appeared in the *Latin American Theoretical INformatics (LATIN 2004)*, Buenos Aires, Argentina, 2004.

3. A. Ambainis and K. Yang.
   Towards the Classical Communication Complexity of Entanglement Distillation Protocols with Incomplete Information.
   To appear in the *19th Aunnual IEEE Conference of Computational Complexity (CCC 2004)*, Amherst, MA.

1.5 Related Work

We discuss some related work on correlation distillation and communication complexity.

1.5.1 Error Correction

As we discussed before, error correction is closely related to correlation distillation protocols. Error correction is the preventive strategy for correlation recover, and correlation distillation is the reparative strategy.

Not only are error correcting codes extremely useful in information theory, they also found numerous applications in other fields, including combinatorics, cryptography, and computational complexity.

Error correction has received tremendous amount of attention. Regarding its sheer volume, it is impossible to give an (even remotely) comprehensive list of the literature on this topic. I only list a few of them. Shannon [81] is the first one to consider the problem of error correction, and his paper marked the beginning of the field of information theory. Blahut [11] has a wonderful book completely dedicated to error correcting codes with abound resources. Sudan [85] has a very nice survey on ECCs that is more designed to audiences in computational complexity. Shor [82] and Steane [84] are the first to study quantum error correcting codes and to actually construct them. Gottesman's thesis [35] is a great source for the theory behind quantum error correcting codes with many results. Nielsen and Chuang's book [68] also gives a nice description on both classical and quantum error correction.

1.5.2 Two-party Coin-flipping

Two-party coin-flipping is a classical problem in cryptography, where Alice and Bob wish to establish some commonly agreed random bits by communication. Blum [9] is the first to study the setting where Alice and Bob initially don't share any information and one of them could be cheating. He suggested protocols that are secure against a computationally-limited adversary, based on number-theoretical assumptions. Following Blum's work, Lindell [53] studied the parallel version of the problem under the same setting. Barak [14] consider the two-party coin-tossing resistant to the man in the middle attack. On the other hand, researchers have studied quantum coin-flipping, where Alice and Bob exchange quantum information and agree on a classical bit. For results in this area, see [55, 61, 1, 4, 87, 52]. Classical two-party coin-flipping is a special version of correlation distillation protocols with the assumption that: 1) the players don't share any a priori information; 2) they are polynomial-time bounded; and 3) they don't necessarily collaborate and are liable to cheating. As a result, the protocols for two-party coin-flipping rely on Cryptographic assumptions and the communication complexity is higher than the number of coin flips they agreed on. Quantum two-party coin-flipping, however, does not fit into the thesis, since it requires a quantum channel between Alice and Bob.

1.5.3 Information Reconciliation

Information reconciliation is an extensively studied notion [16, 60, 26, 29, 30] with applications in quantum cryptography and information-theoretical cryptography. In this setting, Alice and Bob each possesses a sequence of random bits that agree "most of the time". Here the "agreement" between Alice's bits (denoted by A) and Bob's bits (denoted by B) is described by the mutual information $I(A;B)$. Moreover, Eve, the eavesdropper, also possess some information (denoted by Z) about the bits held by Alice and Bob, which is quantified by the mutual information $I(Z;AB)$. Alice and Bob wish to "reconcile" their information (namely, to agree on some random information) by communicating in public channel (which is noiseless but readable by Eve). Their goal is to agree on a common random string U with very high probability, while making sure that Eve gains little information from U. In terms of the entropy, let C be the communication between Alice and Bob, then we should have $H(U|AC) \approx 0$, $H(U|BC) \approx 0$, and $I(U;ZC) \approx 0$. Information reconciliation and correlation distillation operate in similar model: Alice and Bob share noisy information, and then communicate to agree on something with higher correlation. However, the primary concern for information reconciliation is the *privacy*, i.e., that Eve gains little information about the information agreed upon, while this thesis focus on the communication complexity.

1.5.4 Random Beacons

A random beacon is an entity that broadcasts uncorrelated unbiased random bits in real time. The concept of random beacons were first introduced in 1983 by Rabin [73], who showed how they can be used to solve problems in cryptography. Bennett, DiVincenzo, and Linsker [25] proposed to use a random beacon to authenticate video recording. Maurer [59], Aumann and Rabin [6], and

Ding [32] proposed to use a random beacon of extremely high rate to build information-theoretically secure cryptographic primitives, e.g., key exchange, encryption, and oblivious transfer. Von Ahn et. al. [2] discusses various applications of random beacons, including verifiable lotteries and proof of ignorance. There are many proposals to construct a *public, verifiable* random beacon, among them are the ones that use the signals from a cosmic source [2, 62]. In these proposals, Alice (as the beacon owner) and Bob (as a verifier) both point a radio telescope to some extraterrestrial objects, like pulsars, and then measure the signal from them, which presumably contains enough amount of randomness. It is inevitable that Alice and Bob have discrepancy in their results, due to measurement errors. Nevertheless, Alice and Bob still wish to agree on some common random bits. Notice that the random bits they wish to agree on are not necessarily the "raw data" from the measurement; Alice and Bob are free to apply any transformation to their measurement results. The research on random beacons is still ongoing, and is divided into 2 directions. Along one direction, the problem is exactly as in correlation distillation, where Alice and Bob wish to resolve the discrepancy with minimal (preferably zero) amount of communication; along the other direction, no communication is allowed (which normally will always induce some disagreement), and the goal is to design a mechanism that prevents *cheating*, where the beacon owner maliciously modify its measurement data in order to affect the random bits it outputs.

1.5.5 Quantum Entanglement Distillation

As we mentioned before, quantum entanglement distillation protocols are two-party protocols involving only local (quantum) operation and classical communication. These protocols generally takes some entangled bipartite states as input and output near-perfect EPR pairs. The process of entanglement distillation was also known as "entanglement concentration" or "entanglement purification". Quantum entanglement distillation protocols fall into the category of refreshing correlation distillation protocols, since Alice and Bob try to output "fresh" EPR pairs.

There have been a lot of research efforts on studying entanglement distillation protocols [20, 21, 24, 42, 43, 74, 75, 76, 7]. Different "noise" models on the imperfect EPR pairs are presented and studied.

To our knowledge, Bennett, Bernstein, Popescu, and Schumacher are the first to consider the problem of producing EPR pairs from "less entangled" states. In their seminal paper [20], they gave a protocol that converts many identical copies of pure state $|\phi\rangle = (\cos\theta|01\rangle + \sin\theta|10\rangle)$ to perfect EPR pairs. They call this process "entanglement concentration". In the same year, Bennett, Brassard, Popescu, Schumacher, Smolin, and Wootters [21] studied the problem of "extracting" near-perfect EPR pairs from identical copies of mixed entangled states. This is the first time that the notion "entanglement purification protocols" was presented, which were renamed to "entanglement distillation protocols" later. They also pointed out that EDPs can be used to send quantum information through a noisy channel. Later, Bennett, DiVincenzo, Smolin and Wootters [24] improved the efficiency of the protocols in [21] and proved a result that closely related EDPs to quantum error correcting codes, which is an alternative means to transmit quantum information reliably through a noisy channel. Horodecki, Horodecki, and Horodecki [41, 44] and Rains [74, 75, 76] gave various asymptotic bounds on distillable entanglement for arbitrary entangled states. They considered the situation where n identical copies of a state are given as input to an LOCC protocol, which then outputs m EPR pairs. They studied the asymptotic behavior of m/n as n approaches infinity. Researchers also studied EDPs for a single copy of an arbitrary pure state, see Vidal [89], Jonathan and Plenio [48], Hardy [40], and Vidal, Jonathan, and Nielsen [90]. Much of the work was built on the result of majorization by Nielsen [66], who is the first one that studied conditions under which one pure state can be transformed into another one by LOCC.

From another direction, researchers have studied EDPs with *incomplete information*, where Alice and Bob don't know the exact state they share. The state is in a mixed state, or is prepared adversarially. In this case we cannot hope that Alice and Bob would act optimally. However, there still exist protocols that do reasonably well. Bennett *et. al* [21, 24] studied the model where Bob's share in the EPR pairs underwent a noisy channel, resulting in a mixed state. They showed that their protocol would "distill" near-perfect EPR pairs even when Alice and Bob don't have the complete knowledge of the shared state. Under another circumstance, "purity-testing protocols" were studied implicitly by Lo and Chau [56], Shor and Preskill [83], and later explicitly by Barnum, Crépeau, Gottesman, Smith, and Tapp [22]. Purity-testing protocols are LOCC protocols that approximately distinguish the state of perfect EPR pairs from the rest states. Ambainis, Smith, and Yang [7] pointed out that purity-testing protocols are indeed EDPs where Alice and Bob only know the *fidelity* of the state they share. Using constructions from [22], Ambainis, Smith and Yang constructed a "Random Hash" protocol that produces $(n - s)$ EPR pairs of conditional fidelity at least $1 - 2^{-s}/(1 - \epsilon)$ on any n qubit-pair input state of fidelity $1 - \epsilon$. Their protocol would fail with probability ϵ, and the conditional fidelity of its output is the fidelity *conditioned on* the protocol not failing.

Many of previous work assume that Alice and Bob have the complete information about the state they share, and thus they can act *optimally*. The main focus of the majority of the previous work is the *yield* of the protocols, i.e., the question "how many EPR pairs can be extracted from the input state, using *unlimited* classical communication?" Lately, there has been work that start to study the communication complexity of EDPs, started by Lo and Popsecu [57] and followed by Ambainis and Yang [8]. Here the question is "how many bits need to be exchanged in order to distill n EPR pairs?" In the thesis, I will continue this line of research on the communication complexity of EDPs with the focus on the situation where Alice and Bob have *incomplete* information about their shared states.

1.5.6 Communication Complexity

Classical communication complexity studies the minimal amount of classical information (normally measured in bits) needed to be transmitted between multiple parties in order to collectively perform certain computation. The results are typically information theoretical, and don't rely on any unproven assumptions. The field of communication complexity was pioneered by Yao [93], and now is a very rich field in theoretical computer science, and has found applications in many areas, like network analysis, VLSI design, data structure, and computational complexity. The readers are referred to [51] for a nice introduction and tutorial.

Quantum communication complexity mostly studies the minimal amount of quantum information (normally measured in qubits) needed to be exchanged in order to perform some (classical or quantum) task. This field is also first studied by Yao [94], and now it is becoming one of the main topics in quantum information theory. It is a very successful area, and numerous results have emerged. In fact, most known lower bounds in quantum computation can be regarded as communication complexity results. We refer the readers to [13] for a nice survey, and [18, 49, 50, 77] for some important techniques and results.

Despite the numerous results emerging from classical and quantum communication complexity, another class of problem, namely the *classical* communication complexity for *quantum* protocols, has being largely ignored until very recently. This class of problem is concerned with the minimal number of classical bits needed to be communicated to perform certain quantum tasks. An example is the classical communication complexity for EDPs: one may ask "how many bits do Alice and Bob need to exchange in order to distill n EPR pairs?" One reason that not many researchers pay too much attention to this problem might be the conception that classical communication is "cheap" compared to quantum communication, and thus one can assume they are free. However, as pointed by Lo and Popescu [57], there are situations where classical communication can not be justifiably ignored. One example is the super-dense coding [28]: Alice and Bob can use n qubits to transmit $2n$ bits of classical information, if they previously share n EPR pairs. Nevertheless, if it takes more than n bits of classical communication to distill the n EPR pairs, it would totally destroy the purpose of super-dense coding. Furthermore, in the study of LOCC protocols over quantum states, no quantum communication takes place, and it is therefore interesting to study the classical communication complexity of these (quantum) protocols.

The history of classical communication complexity for quantum protocols can probably traced back to the seminal paper by Bennett and Wienser [28], which discussed teleportation and constructed a protocol that uses $2n$ classical bits to transmit n qubits. However, this topic was largely overlooked until by Lo and Popescu [57] and Lo [54]. Lo and Popescu [57] discussed the classical communication complexity of various protocols by Bennett et. al. [20]. They observed that the "entanglement concentration protocol" in [20] doesn't require any classical communication. However, the "entanglement dilution protocol", which transforms m EPR pairs into n copies of less entangled qubit pairs, requires $O(n)$ bits of classical communication. Lo and Popescu then constructed a new dilution protocol that only uses $O(\sqrt{n})$ bits of communication. This protocol was proven to be asymptotically optimal independently by Hayden and Winter [46], and Harrow and Lo [45], who proved matching lower bounds for general entanglement dilution protocols. Lo [54] studied the communication complexity for Alice and Bob to jointly *prepare* many copies of arbitrary (known) pure states, and proved an non-trivial upper bound.

All the previous results focus on a relatively simple situation, where the input are identical copies of a known pure state, and only the asymptotic results are known. In the thesis work, I propose to study the communication complexity of EDPs with *incomplete information*. In this setting, Alice and Bob don't have the complete knowledge about the input state they share. Rather, the input state is a mixed state, or is adversarially prepared. I also propose to study the *precise* communication complexity of EDPs, rather than their *asymptotic* behavior. In fact, we try to answer questions of the following fashion: "On this particular input state class, how many bits of classical communication are needed in order to just output a *single* EPR pair with certain quality?"

Bibliography

[1] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao. Quantum bit escrow. In *STOC 2002*, pp. 705–714.

[2] L. von Ahn, M. Blum, N. Hopper, J. Langford, and K. Yang. Beacon Bits. *manuscript, in preparation*, 2002.

[3] N. Alon, U. Maurer, and A. Wigderson. private communication.

[4] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. In *STOC 2001.*

[5] A. Ambainis. private communication.

[6] Y. Aumann and M.O. Rabin. Information Theoretically Secure Communication in the Limited Storage Space Model. in *Crypto 99*:65-79, 1999.

[7] A. Ambainis, A. Smith, and K. Yang. Extracting Quantum Entanglement (General Entanglement Purification Protocols). in the *IEEE Conference of Computational Complexity (CCC 2002).* pp. 103-112, 2002.

[8] A. Ambainis and K. Yang. Towards the Classical Communication Complexity of Entanglement Distillation Protocols with Incomplete Information. To appear in the *19th Aunnual IEEE Conference of Computational Complexity (CCC 2004)*, Amherst, MA. Also available at *LANL eprint* `quant-ph/0207090`.

[9] M. Blum, Coin flipping by phone. In *IEEE Spring COMPCOM*, pp. 133–137, February 1982.

[10] M. Blum. Independent unbiased coin flips from a correlated biased source: a finite state Markov chain. In *FOCS 1984*, pp. 425–433, 1984.

[11] R. E. Blahut, Theory and Practice of Error Control Codes. *Addison-Wesley*, 1983.

[12] C. Bennett. Quantum cryptography using any two nonorthogonal states. IN *Phys. Rec. Lett.*, 68(21):3121–3124, 1992.

[13] G. Brassard, Quantum Communication Complexity (a survey). Available at *LANL eprint* `quant-ph/0101005`.

[14] B. Barak. Constant-Round Coin-Tossing With a Man in the Middle or Realizing the Shared Random String Model. To appear in *FOCS* 2002.

[15] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceeding of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, Bangalore, India, December 1984.

[16] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental Quantum Cryptography. In *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[17] C. H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. In *Phys. Rev. Lett.*, **70**, 1895 (1993).

[18] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum Lower Bounds by Polynomials. In *39th IEEE Symposium on Foundations of Computer Science (FOCS'98)*, pp.352-361, also available at *LANL eprint* `quant-ph/9802049`. Journal version in *Journal of the ACM*, 48(4):778-797, 2001.

[19] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor. Quantum computing without entanglement. *manuscript*, 2002.

[20] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. In *Phys. Rev. A*, vol. 53, No. 4, April 1996.

[21] C. H. Bennett, H. J. Bernstein, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. In *Phys. Rev. Lett.*, vol. 76, page 722, 1996.

[22] H. Barnum, C. Crépeau, D. Gottesman, A. Smith and A. Tapp. Authentication of Quantum Messages. To appear in *FOCS 2002*, also available at *LANL eprint* `quant-ph/0205128`.

[23] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of Very Noisy Mixed States and Implications for NMR Quantum Computing. In *Phys. Rev. Lett.*, **83**, 1054 (1999).

[24] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. In *Phys. Rev. A*, vol. 54, No. 5, November 1996.

[25] C. H. Bennett, D. P. DiVincenzo, and R, Linsker. Digital recording system with time-bracketed authentication by on-line challenges and method for authenticating recordings. *US patent* 5764769 (1998).

[26] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology — EUROCRYPT '93*, LNCS 765, pp. 410–423, 1994.

[27] C. H. Bennett and J. A. Smolin. Trust enhancement by multiple random beacons. In *LANL eprint* `http://xxx.lanl.gov/abs/cs.CR/0201003` (2002).

[28] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. In *Phys. Rev. Lett.* **69**, 2881 (1992).

[29] C. Cachin and U. Maurer. Linking Information Reconciliation and Privacy Amplification. In *Journal of Cryptology*, vol. 10, no. 2, pp. 97-110, 1997.

[30] C. Cachin and U.Maurer. Unconditional Security Against Memory-Bounded Adversaries. In *Advances in Cryptology - CRYPTO '97*, LNCS 1294, pp. 292–306, 1997.

[31] T. M. Cover and J. A. Thomas. Elements of Information Theory. *John Wiley and Sons*, 1991.

[32] Y. Z. Ding. Oblivious Transfer in the Bounded Storage Model. In *Advances in Cryptology — CRYPTO 2001*, LNCS 2139, pages 155 – 177, 2001.

[33] S. Dziembowski and U. Maurer. Tight Security Proofs for the Bounded-Storage Model. In *STOC* 2002.

[34] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? In *Phys. Rev.* **47**, 777 (1935), also reprinted in *Quantum Theory and Measurement*, edited by J. A. Wheeler and W. Z. Zurek, Princeton University Press, 1983.

[35] D. Gottesman. Stabilizer codes and quantum error correction. *Ph.D. thesis, Caltech*, also available at *LANL eprint* `quant-ph/9705052`.

[36] D. Gottesman. *Private Communication*, 2001.

[37] V. Guruswami. List decoding of error-correcting codes. *Ph.D. thesis*, MIT, 2001.

[38] V. Guruswami. List Decoding with Side Information. In *IEEE Conference on Computational Complexity*, 2003.

[39] O. Goldreich. The Foundations of Cryptography - Volume 1, *Cambridge University Press*, 2001.

[40] L. Hardy. Method of areas for manipulating the entanglement properties of one copy of a two-particle pure entangled state. In *Phys. Rev. A*, **60**, 1912 (1999). also available at *LNAL erint* `quant-ph/9903001`.

[41] M. Horodecki, P. Horodecki, and R. Horodecki. Distillability of Inseparable Quantum Systems. In `quant-ph/9607009`.

[42] M. Horodecki, P. Horodecki. Reduction criterion of separability and limits for a class of protocols of entanglement distillation. In *LANL eprint* `quant-ph/9708015`.

[43] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a "bound" entanglement in nature? in *LANL eprint* `quant-ph/9801069`.

[44] M. Horodecki, P. Horodecki, and R. Horodecki. Asymptotic entanglement manipulations can be genuinely irreversible. In *Phys. Rev. Lett.*, 84:4260–4263, 2000. See errata at *LANL e-print* `quant-ph/9912076`.

[45] A. Harrow and H. K. Lo. A tight lower bound on the classical communication cost of entanglement dilution. In *LANL eprint* `quant-ph/0204096`.

[46] P. Hayden and A. Winter. On the communication cost of entanglement transformations. In *LANL eprint* `quant-ph/0204092`.

[47] R. Jozsa and N. Linden. On the role of entanglement in quantum computational speed-up. Available at *LANL e-print* `quant-ph/0201143`.

[48] D. Jonathan and M. Plenio. Minimal conditions for local pure-state entanglement manipulation. In *Phys. Rev. Lett.* **83**, 1455 (1999), also available at *LANL eprint* `quant-ph/9903054`.

[49] H. Klauk. One-way communication complexity and the Nečiporuk lower bound on formula size. available at *LANL eprint* `http://xxx.lanl.gov/abs/cs.CC/0111062`, conference versions at ISAAC '97, Complexity '98, STOC '00.

[50] H. Klauk. Lower Bounds for quantum communication complexity. In the *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS'01)*, 2001. Also available at *LANL eprint* `quant-ph/0106160`.

[51] E. Kushilevitz and N. Nisan. Communication Complexity. *Cambridge University Press*, 1997.

[52] B. Leslau. Attacks on symmetric quantum coin-tossing protocols. In *LANL eprint* `quant-ph/0104075`.

[53] Y. Lindell. Parallel Coin-Tossing and Constant-Round Secure Two-Party Computation. In *Advances in Cryptology — CRYPTO 2001*, LNCS 2139, pages 171 – 189, 2000.

[54] H. K. Lo. Classical communication cost in distributed quantum information processing — a generalization of quantum communication complexity. In *LANL eprint* `quant-ph/9912009`.

[55] H. K. Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. In *Physica D*, 120:177–187, 1998.

[56] H. K. Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution Over Arbitrary Long Distances. In *Science* **283**, 2050-2056 (1999), also available at *LANL eprint* `quant-ph/9803006`.

[57] H. K. Lo and S. Popescu. The classical communication cost of entanglement manipulation: Is entanglement an inter-convertible resource? In *Phys. Rev. Lett.*, **83**, pp. 1459 – 1462, 1999, also available at *LANL eprint* `quant-ph/9902045`.

[58] P. Lancaster and M. Tismenetsky. The theory of matrices, second edition, with applications. Academic Press, 1985.

[59] U. M. Maurer. Conditionally-perfect secrecy and a provably secure randomized cipher. In *Journal of Cryptology,* 5:53-66, 1992.

[60] U. M. Maurer. Secret key agreement by public discussion from common information. In *IEEE Transactions on Information Theory*, vol 39, pp. 733–742, May 1993.

[61] D. Mayers, L. Salvail, and Y. Chiba-Kohno. Unconditionally secure quantum coin-tossing. In *LANL eprint* `9904078`.

[62] E. Mossel and R. O'Donnell. Coin Flipping from a Cosmic Source: On Error Correction of Truly Random Bits. *manuscript.*

[63] R. Motwani and P. Raghavan. Randomized algorithms. *Cambridge University Press*, 1995.

[64] M. Naor, A. Orlitsky, and P. Shor. Three results on interactive communication. In *IEEE Transactions on Information Theory*, 39:1608–1615, 1993.

[65] J. von Neumann, Various techniques used in connection with random digits. In *Notes by G. E. Forsythe, National Bureau of Standards*, 1952, vol. 12, pages 36-38.

[66] M. Nielsen. Conditions for a Class of Entanglement Transformations. In *Phys. Rev. Lett.*, **83** (2), pp 436–439 (1999), also available at *LANL eprint* `quant/ph/9811053`.

[67] M. Nielsen. Probability Distributions Consistent with a Mixed State. Available at *LANL eprint* `quant/ph/9909020`.

[68] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. *Cambridge University Press*, 2000.

[69] N. Nisan and A. Ta-Shma. Extracting randomness: a survey and new constructions. In *JCSS* 58(1): pp. 148–173, 1999.

[70] N. Nisan and D. Zuckerman. Randomness is linear in space. In *JCSS* 52(1): pp. 43–52, 1996. A preliminary version under the name "More deterministic simulation in logspace" appeared in *STOC 1993*, pp. 235–244, 1993.

[71] A. Orlitsky. Worst-case interactive communication I: Two messages are almost optimal. In *IEEE Transactions on Information Theory*, 36(5):1111–1126, 1990.

[72] A. Peres. Quantum theory: concepts and methods. *Kluwer Academic*, 1993.

[73] M. Rabin. Transaction Protection by Beacons. In *Journal of Computer and System Sciences*, 27(2):256-267, October 1983.

[74] E. M. Rains. A rigorous treatment of distillable entanglement. In *LANL eprint* `quant-ph/9809078`.

[75] E. M. Rains. An improved bound on distillable entanglement. In *LANL eprint* `quant-ph/9809082`.

[76] E. M. Rains. A semidefinite program for distillable entanglement. In *LANL eprint* `quant-ph/0008047`.

[77] A. Razborov. Quantum Communication Complexity of Symmetric Predicates. (Russian). To appear in *Izvestia of the Russian Academy of Science, mathematics*, No 6, 2002. English version available at *LANL eprint* `quant-ph/0204025`.

[78] O. Reingold, R. Shaltiel and A. Wigderson. Extracting randomness via repeated condensing. In *FOCS 2000*, pp. 22–31, 2000.

[79] M. Santha and U. V. Vazirani. Generating quasi-random sequences from slightly-random sources. In *FOCS 1984*, pp. 434–440, 1984.

[80] R. Shaltiel. Recent developments in extractors. Available at `http://www.wisdom.weizmann.ac.il/~ronens/papers/survey.ps`.

[81] C. Shannon. A Mathematical Theory of Communication. In *Bell Sys. Tech. Journal*, 27:379–423, 623–656, 1948.

[82] P. Shor. Scheme for Reducing Deconherence in Quantum Memory. In *Phys. Rev. A* **52**, 2493 (1995).

[83] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum key Distribution Protocol. In *Phys. Rev. Lett.* 85 (2000) 441-444, also available at *LANL eptin* `quant-ph/0003004`.

[84] A. M. Steane. Error Eorrecting Codes in Quantum Theory. In *Phys. Rev. Lett.* **77**, 793 (1996).

[85] M. Sudan. Coding theory: Tutorial & Survey. In *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, pages 36-53, 2001.

[86] M. Sudan. Algorithmic Introduction to Coding Theory. Course note available at `http://theory.lcs.mit.edu/ madhu/FT01/`.

[87] R. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. In *Phys. Rev. A*, 65:012310, 2002.

[88] A. Ta-Shma, C. Umans, D. Zuckerman. Loss-less condensers, unbalanced expanders and extractors. In *Proceedings of STOC'01*, pp. 143-152.

[89] G. Vidal. Entanglement of pure states for a single copy. In *Phys. Rev. Lett.* 83 (1999) 1046-1049, also available at *LNAL eprint* `quant-ph/9902033`.

[90] G. Vidal, D. Jonathan, and M. Nielsen. Approximation transformations and tobust manipulation of bipartite pure state entanglement. In *Phys. Rev. A* **62**, 012304 (2000), also available at *LANL epint* `quant-ph/9910099`.

[91] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model In *Phys. Rev. A* **(**40), 4277 (1989).

[92] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. In *Nature*, **299**, 802 (1982).

[93] A. Yao. Some Complexity Questions Related to Cistributed Computing. In *Proceedings of the 11th ACM Symposium on Theory of Computing (STOC'79)*, pp. 209–213, 1979.

[94] A. Yao. Quantum Circuit Complexity. In *Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, (FOCS'93)*, pp. 351–361, 1993.

[95] K. Yang. On the (im)possibility of non-interactive correlation distillation. *Manuscript*, 2002.