On the Communication Complexity of Correlation and Entanglement Distillation — a Thesis Propsal

Ke Yang

February 25, 2003

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.

I propose to 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.

My thesis will 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. My study concerns the minimal amount the communication needed for distillation.

I will present a number of known 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. I propose to continue the project of understanding communication complexity of correlation/entanglement distillation as my thesis work.

Contents

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 [78], 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, one wishes 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 [78] 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 Beacon

A random beacon is an entity that broadcasts uncorrelated unbiased random bits. The concept of random beacons were first introduced in 1983 by Rabin [70], 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 [58], 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, 61]. 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.

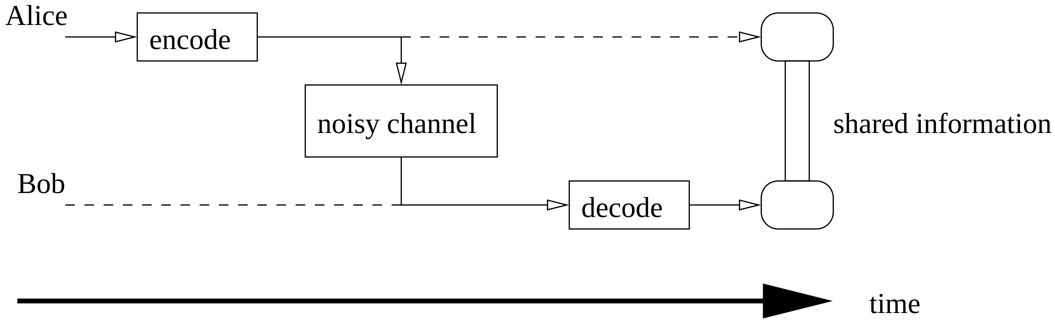
However, it is very hard to store qubits; qubits can easily become entangled with environment and *decohere*. Moreover, the decoherence happen continuously with time, which is hard to prevent with current technology. This poses a serious problem to teleportation, since teleportation needs perfect EPR 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. 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: 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.

Assumption 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.

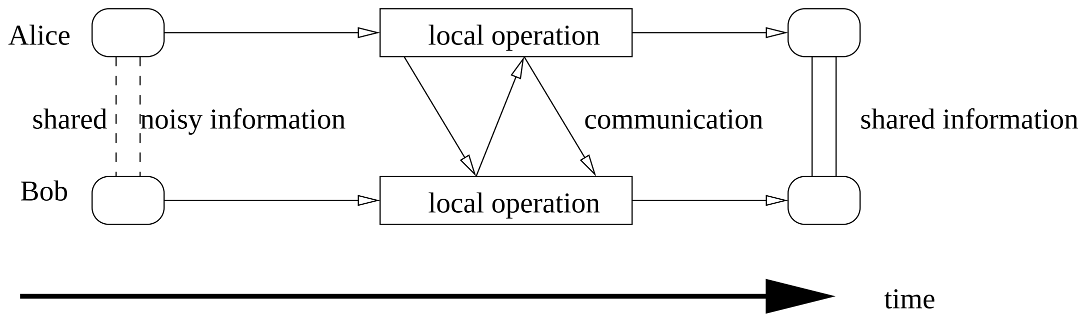
One can thus separate the so-called "typical error syndromes" from the "atypical" ones, and only focus on the typical syndromes. However, it is not always realistic to assume the IID model. This is best illustrated by the case of quantum key distribution protocols. Recall in this situation, Eve may intercept 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 [80] 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.

Assumption 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/Entanglement Distillation: the Post-Corruption 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 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".



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

Figure 2: Reparative strategy for correlation repair

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 entanglement distillation protocols, since quantum communication is considerably more expensive. 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, many 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). 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 [55] and Shor and Preskill [80] (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 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] 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.

1.4 A Brief Summary of Results

I propose to 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.

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 [55, 80].

[2] We are using the notations from Kushilevitz and Nisan [50].

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 [78] 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 [82] has a very nice survey on ECCs that is more designed to audiences in computational complexity. Shor [79] and Steane [81] 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 [66] 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 [52] 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 [54, 60, 1, 4, 83, 51]. 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, 59, 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 [70], 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 [58], 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, 61]. 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, 41, 42, 71, 72, 73, 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 [40, 43] and Rains [71, 72, 73] 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 [85], Jonathan and Plenio [47], Hardy [39], and Vidal, Jonathan, and Nielsen [86]. Much of the work was built on the result of majorization by Nielsen [64], 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 [55], Shor and Preskill [80], 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 [56] 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 [89], 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 [50] 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 [90], 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, 48, 49, 74] 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 [56], 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 [56] and Lo [53]. Lo and Popescu [56] 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 [45], and Harrow and Lo [44], who proved matching lower bounds for general entanglement dilution protocols. Lo [53] 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?"

2 Quantum Mechanics and Quantum Information Theory

We introduce the notions and concepts in quantum mechanics and quantum information theory.

2.1 Quantum Mechanics

We briefly summarize the laws and conventions in quantum mechanics used in this thesis. This summary is by no means complete and we refer the reader to Peres [69] and Nielsen and Chuang [66] for a more comprehensive treatise.

2.2 The Quantum States and the Dirac Notation

A quantum system is described in a *Hilbert space*, i.e., a linear space with a well-defined inner product. In this thesis we only consider Hilbert spaces of finite dimension. We use $\mathcal{H}_N$ to denote a Hilbert space of dimension N. A *pure state* is described by a unit (column) vector in a Hilbert space and is normally denoted in the so-called *Dirac notation* as $|\,\phi\rangle$. A *qubit* is a two-state quantum system, and is also the smallest quantum state possible. A general qubit can be written as $|\,\phi\rangle = \alpha|\,0\rangle + \beta|\,1\rangle$, where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. We can view this general state $|\,\phi\rangle$ as a *superposition* of the two basis states $|\,0\rangle$ and $|\,1\rangle$. In general, a a system of n qubits is described in a Hilbert space of dimension 2^n, which can be conveniently viewed as a tensor product of n two-state subspaces, i.e., $\mathcal{H}_{2^n} = \mathcal{H}_2 \otimes \mathcal{H}_s \otimes \cdots \otimes \mathcal{H}_2$. We always assume the existence of a fixed, canonical *computational basis* in an N-dimensional Hilbert space, denoted as $\{|\,0\rangle, |\,1\rangle, ..., |\,N-1\rangle\}$, and a general pure state can be written as $|\,\phi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |\,x\rangle$, where $\sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1$. Again, it is in general a superposition of 2^n basis states.

A "bra" is a unit row vector, defined as $\langle\phi\,| = (|\,\phi\rangle)^\dagger$, where $x^\dagger$ denotes the operation of applying transpose followed by the complex conjugate to x. For pure states $|\,\phi\rangle$ and $|\,\psi\rangle$, their inner product can be conveniently written as $(|\,\phi\rangle, |\,\psi\rangle) = \langle\phi\,|\cdot|\,\psi\rangle = \langle\phi\,|\,\psi\rangle$.

An *outer product* of two pure states $|\,\phi\rangle$ and $|\,\psi\rangle$ is a matrix defined as $|\phi\rangle\langle\psi| = |\,\phi\rangle \cdot \langle\psi\,|$.

The outer product and the inner product are conveniently related by the trace of a matrix.

$$\mathrm{Tr}(|\phi\rangle\langle\psi|) = \langle\psi\,|\,\phi\rangle \tag{1}$$

2.2.1 The Density Matrix and Mixed States

An alternative way to describe a pure state $|\,\phi\rangle$ is by its outer product with itself, $|\phi\rangle\langle\phi|$. This is known as the *density matrix* notation, and $|\phi\rangle\langle\phi|$ is the density matrix representing state $|\,\phi\rangle$. One advantage for the density matrix notation is that it can conveniently represent *mixed states.* A mixed state emerges when we don't have the complete information about a quantum system but only partial knowledge represented as a probabilistic distribution. More precisely, a mixed state is a probabilistic ensemble (mixture) of pure states. In Dirac notation, one writes a mixed state as $\{p_i, |\,\phi_i\rangle\}$, which means this state is in state $|\,\phi_i\rangle$ with probability p_i. Naturally, we have that $\sum_i p_i = 1$. In the density matrix notation, such a state is simply represented as

$$\rho = \sum_i p_i \cdot |\phi_i\rangle\langle\phi_i|. \tag{2}$$

It is easy to see that all density matrices are positive operators (i.e., they are Hermitians and all their eigenvalues are non-negative) and have trace 1. In fact, one can define a density matrix as one that is positive and have trace 1. Notice any such matrix can be written in the form of Eq. (2) by spectral decomposition.

Notice that there might exist two very different ensembles of pure states that yield the same density matrix. For example, consider an ensemble A which is state $|0\rangle$ with probability 0.5, and state $|1\rangle$ with probability 0.5. Its density matrix is $\rho_A = 0.5 \cdot |0\rangle\langle 0| + 0.5 \cdot |1\rangle\langle 1| = I/2$. Consider another ensemble B that is state $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ with probability 0.5 and state $|\phi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ with probability 0.5. It density matrix is $\rho_B = 0.5 \cdot |\phi_+\rangle\langle\phi_+| + 0.5 \cdot |\phi_-\rangle\langle\phi_-| = I/2$. So these two ensembles have the same density matrix, although they are formed very differently. However, the law of quantum mechanics says, that all the information one can obtain from a quantum system can be derived from its density matrix. Therefore, if two systems have identical density matrices, then there is no way to distinguish them. So the two ensembles A and B describe the same quantum system.

When studying a large quantum system, some times it is convenient to focus on a smaller "subsystem" within the large system. One can derive the *reduced density matrix* for the subsystem from the density matrix of the large system. Suppose the smaller system is in a Hilbert space $\mathcal{H}_A$ and the large system is in a Hilbert space $\mathcal{H}_{AB}$ with density matrix ρ. Then the density matrix ρ_A for the subsystem can be obtained by "tracing out" the system B, denoted by $\rho_A = \mathrm{Tr}_B(\rho)$. Here Tr_B is a linear operator defined as

$$\mathrm{Tr}_A(|a_0\rangle\langle a_1|^A \otimes |b_0\rangle\langle b_1|^B) = \langle b_0 \mid b_1\rangle \cdot |a_0\rangle\langle a_1| \tag{3}$$

Here we use superscript to denote the subsystem a state is in: $|a_0\rangle\langle a_1|^A$ is a state in subsystem A and $|b_0\rangle\langle b_1|^B$ is a state in subsystem B. It is possible that ρ is a pure state in the large quantum system AB, while the local density matrix ρ_A corresponds to a mixed state. In this case we say that state A and state B are *entangled*. Entanglement is one of the most important features in quantum mechanics and quantum information theory.

2.2.2 Quantum Operations

There are two types of operations that can be applied to a quantum system, namely unitary operations and measurements.

A unitary operation is a linear operator. For a quantum system of dimension N, such a linear operator can be naturally described as an $N \times N$ matrix U that maps a pure state $|\phi\rangle$ to $U|\phi\rangle$, and (equivalently) a mixed state ρ to $U\rho U^\dagger$. Such a matrix is *unitary*, if and only if $UU^\dagger = I$. The law of quantum mechanics dictates that all unitary operations are allowed. Some of the most important unitary operations are single-qubit operators known as Pauli operators or Pauli matrices, denoted by X, Y, and Z, respectively, and defined as

$$X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle \tag{4}$$
$$Y(\alpha|0\rangle + \beta|1\rangle) = i\beta|0\rangle - i\alpha|1\rangle \tag{5}$$
$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle \tag{6}$$

The simplest version of measurements is a *projective measurement*. A *projector* is a linear operator P such that $P^2 = P$. An *observable* is a collection of projectors $\{P_i\}$ satisfying $\sum_i P_i = I$, and a projective measurement is the operation an observable $\{P_i\}$ exerts on a state $|\phi\rangle$. A measurement is generally probabilistic: the result state is $\frac{P_i|\phi\rangle}{\sqrt{\langle\phi|P_i|\phi\rangle}}$ with probability $\langle\phi|P_i|\phi\rangle$. A measurement on a mixed state can be naturally generalized. A more general version of measurement, known as *POVM* ("Positive Operator-Valued Measurement"), is more conveniently described using the density matrix notation. A POVM is a collection of *measurement operators* $\{M_i\}$, satisfying that $\sum_i M_i^\dagger M_i = I$, and the result of such a measurement on a quantum state ρ is state $\frac{M_i \rho M_i^\dagger}{\mathrm{Tr}(M_i^\dagger M_i \rho)}$ with probability $\mathrm{Tr}(M_i^\dagger M_i \rho)$. To see that POVM is indeed a more general notion, observe that it includes unitary operations as a special case. It can be shown, however, that any POVM can be realized by unitary operator and projective measurements with ancillary qubits.

The formalism of *super-operators* is used to describe how a quantum system evolves with its environment. A super-operator, normally denoted by $\mathcal{E}$, is a linear operator over density matrices defined as

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{7}$$

where $\sum_i E_i^\dagger E_i \leq I$. We say $\mathcal{E}$ is *trace-preserving*, if $\sum_i E_i^\dagger E_i = I$.

2.3 Quantum Information Theory

We review some of the basic notions in quantum information theory. We do not attempt to give a complete or comprehensive survey on this topic. Again, the readers are refereed to Nielsen and Chuang [66] for more comprehensive treatise.

2.3.1 Entropy

The *entropy* of a quantum state ρ is denoted by $S(\rho)$ and known as the *von Neumann entropy.* It is defined as

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) \tag{8}$$

where the logarithm is base-2.

It is not hard to derive from the definition that all pure states have entropy zero and the maximum entropy of an n-qubit system is n, which is achieved by the completely mixed state $\frac{I}{2^n}$.

2.3.2 Entanglement

In this thesis we will be mainly interested in bipartite systems shared between Alice and Bob. In such a bipartite system, the *entanglement* of a pure state $|\phi\rangle$, denoted by $\mathsf{E}(|\phi\rangle)$, is defined to be the von Neumann entropy of the mixed state obtained by tracing out Bob's subsystem. In other words,

$$\mathsf{E}(|\phi\rangle) = S(\mathrm{Tr}_B(|\phi\rangle\langle\phi|)) \tag{9}$$

A pure state is *entangled* if its entanglement is non-zero, and is otherwise *disentangled* or *separable.* A mixed state is disentangled if it can be expressed as an ensemble $\{p_i, |\phi_i\rangle\}$ where each $|\phi_i\rangle$ is disentangled. All other mixed states are entangled. However, there isn't an agreed-up definition on the amount of entanglement of a mixed state.

For a bipartite system consisting of n qubit pairs (or $2n$ qubits in total), its maximum possible entanglement is n. The most important among the maximally entangled states are the four *Bell states*, defined as

$$\Phi^+ = \frac{1}{\sqrt{2}}(|0\rangle^A|0\rangle^B + |1\rangle^A|1\rangle^B) \tag{10}$$

$$\Phi^- = \frac{1}{\sqrt{2}}(|0\rangle^A|0\rangle^B - |1\rangle^A|1\rangle^B) \tag{11}$$

$$\Psi^+ = \frac{1}{\sqrt{2}}(|\,0\rangle^A|\,1\rangle^B + |\,1\rangle^A|\,0\rangle^B) \quad (12)$$

$$\Psi^- = \frac{1}{\sqrt{2}}(|\,0\rangle^A|\,1\rangle^B - |\,1\rangle^A|\,0\rangle^B) \quad (13)$$

These are maximally entangled two-qubit pure states.

The Bell states are closely related to the Pauli matrices. In particular, it is easy to verify that unitary operators of the form $I \otimes U$, where $U \in \{X, Y, Z\}$ translates one Bell state to another. For example, we have $(I \otimes X)\,\Phi^+ = \Psi^+$, $(I \otimes Y)\,\Phi^+ = \Psi^-$, and $(I \otimes Z)\Phi^+ = \Phi^-$.

An *EPR pair*, or an Einstein-Podolsky-Rosen pair, refers to the Bell state Φ^+.[3] We denote the state $(\Phi^+)^{\otimes n}$, which represents n perfect EPR pairs, by Φ_n. We also abuse the notation to use Φ_n to denote *both* the vector $|\,\Phi_n\rangle$ and its density matrix $|\Phi_n\rangle\langle\Phi_n|$, when there is no danger of confusion.

2.3.3 Fidelity

The fidelity is a measure of the "closeness" of two quantum states. For two (mixed) states ρ and σ of equal dimension, their fidelity if defined as

$$\mathsf{F}(\rho, \sigma) = \mathrm{Tr}^2(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}). \quad (14)$$

Notice we are using a different definition as in [NC00], where the *square root* of (14) is used.

If $\sigma = |\varphi\rangle\langle\varphi|$ is a pure state, the definition simplifies to

$$\mathsf{F}(\rho, |\varphi\rangle\langle\varphi|) = \langle\varphi\,|\rho|\,\varphi\rangle \quad (15)$$

A special case for the fidelity is when $|\,\varphi\rangle = \Phi_n$ for some n. In this case, we call the fidelity of ρ and $|\,\varphi\rangle$ the *fidelity of state* ρ, denoted as $\mathsf{F}(\rho)$. In other words, we have

$$\mathsf{F}(\rho) = \langle\Phi_n\,|\rho|\,\Phi_n\rangle \quad (16)$$

We are often interested in the fidelity of two states of unequal number of qubits, and in particular, the fidelity of a general bipartite state ρ, and the Bell state Φ^+. This coincides with the definition of fidelity when ρ has dimension 2. When ρ has a higher dimension, we define its *base fidelity* to be the fidelity of the state obtained by tracing out all but the first qubit pair of ρ. We denote the base fidelity of ρ by $\mathsf{F}^{\mathsf{b}}(\rho)$.

3 Preliminaries and Notations

3.1 General Notations

We present some general notations, both classical and quantum, to be used throughout the thesis.

All logarithms are base-2. All vectors are column vectors by default. We use $[n]$ to denote the set $\{0, 1, ..., n-1\}$. If A and B are two sets, then $A \times B$ denotes the Cartesian product between sets A and B.

We often work with symbols from a particular *alphabet*, which is a finite set and is normally denoted by Σ. We always assume the existence of a canonical one-to-one correspondence between an alphabet Σ of size q and the set $[q]$, and often identify Σ with $[q]$.

[3]There exist contexts where an EPR pair refers to the state Ψ^-, for example, in the original paper by Einstein, Podolsky, and Rosen [34], but in this thesis, we use the convention of Φ^+.

A *string* is a sequence of symbols from an alphabet. We often identify a string with a vector and shall use them interchangeably. For a string x of length n, we use $x[j]$ to denote its j-th entry, for $j = 0, 1, ..., n-1$. We often also use a tuple to index an entry in a vector. For example, We index an (ab)-dimensional vector by (x, y), where $x \in [a]$ and $y \in [b]$. In this case, we assume there exists a canonical mapping from $[a] \times [b]$ to $[ab]$. We use $\mathbf{0}_n$ to denote the all-zero vector (whose each entry is 0) of dimension n, and $\mathbf{1}_n$ to denote the all-one vector (whose each entry is 1) of dimensional n. When the dimension is clear from the context, it is often omitted.

The *Hamming distance* between 2 strings x and y of equal length is the number of positions that these 2 strings differ, and is denoted by $\mathsf{dist}(x, y)$. For strings x and y, we use $x; y$ to denote the *concatenation* of these 2 strings.

A *binary string* or *binary vector* is a string over alphabet $\{0, 1\}$. We identify an integer with the binary vector obtained from its binary representation. For a binary vector x, we denote its *Hamming weight* by $|x|$, which is the number of 1's in x. Obviously the Hamming distance between 2 binary strings x and y is simply $|x \oplus y|$, where $x \oplus y$ denote the string obtained by entry-wise XORing x and y.

A classical probabilistic distribution for some alphabet Σ, normally denoted by $\mathcal{D}$, is a mapping from Σ^* to $[0, 1]$, such that $\sum_{x \in \Sigma^*} \mathcal{D}(x) = 1$. A *uniform distribution* over a set S is denoted by $\mathcal{U}_S$, and is defined to be $\mathcal{U}_S(x) = 1/|S|$ for all $x \in S$.

The *correlation* of a pair of random variables X and Y over a distribution $\mathcal{D}$, denoted by $\mathsf{Cor}_{\mathcal{D}}[(X, Y)]$, is the probability they agree minus the probability they disagree.

$$\mathsf{Cor}_{\mathcal{D}}[(X, Y)] = \mathsf{Prob}_{\mathcal{D}}[X = Y] - \mathsf{Prob}_{\mathcal{D}}[X \neq Y]. \tag{17}$$

The *statistical distance* between two distributions X and Y is

$$\mathsf{SD}(X, Y) = \frac{1}{2} \sum_x |\mathsf{Prob}\,[X = x] - \mathsf{Prob}\,[Y - x]| \tag{18}$$

If the statistical distance between X and Y is ϵ, then we say that they are "ϵ-close".

We identify a function with its truth table, which can be written as a vector. For example, we regard a function over $\{0, 1\}^n$ also as a 2^n-dimensional vector. We assume a canonical ordering of n-bit strings.

3.2 Protocols

We focus on two-party protocols executed between Alice and Bob. A protocol is normally denoted by $\mathcal{P}$. Classical protocols can be modeled by two interactive Turing machines à la Goldreich [38]. Quantum protocols can be modeled by two quantum circuits connected by classical wires à la Yao [90]. The actual model of computation isn't essential for this thesis, since all the lower bounds I shall proof are information-theoretical, and therefore are independent from the actual computation model being used, and all the algorithms I present would be efficiently realizable in any of the reasonable computation models.

Next, we will give formal definitions on various aspects of the correlation distillation protocols. However, first we discuss different types of these protocols

Classical vs. Quantum The classical version of correlation distillation protocols work with classical information. At the beginning of the protocols, Alice and Bob share information that are not perfectly correlated, and at the end of the protocol, they outputs classical information that are almost perfectly correlated.

The quantum version of correlation distillation protocols is more appropriately called entanglement distillation protocols. Here, Alice and Bob start with qubits that are imperfectly entangled, and at the end, they output qubits that are almost perfectly entangled.

Recovering vs. Refreshing Intuitively, the *recovering protocols* are the ones that try to recover the information that is "corrupted" by a noisy channel. A bit more formally, a protocol is a recovering protocol, if Alice directly outputs her local input. Consider the situation where Alice sends some information A through a noisy channel, and when Bob receives B from the channel, A and B are not perfectly correlated (or entangled). In a recovering protocol, Alice and Bob try to reconstruct the information A Alice sent out. At the end of the protocol, Alice will output A, and Bob tries to output $\hat{A}$ that is as "close" to A as possible.

Protocols that are not recovering protocols are called *refreshing protocols*. These protocols, on the other hand, aim to generate fresh information that isn't necessarily the original shared information. At the end of a refreshing protocol, Alice and Bob each outputs some information, which we denote as X and Y. The goal is to have X and Y be as correlated (or entangled) as possible.

Non-interactive, One-way, and Two-way Depending on the amount of the communication, a protocol can be *non-interactive*, *one-way*, or *two-way*. A non-interactive protocol is one where Alice and Bob don't communicate at all. They are perhaps the simplest protocols in their class. For interactive protocols, we say a protocol $\mathcal{P}$ is a k-bit protocol, if it contains k bits of communication. In a *one-way* protocol, only one of the players sends information to the other party. We always assume that in this case, it is Alice that sends information to Bob, and Bob sends nothing back. In a *two-way* protocol, Alice and Bob both sends information to each other.

Deterministic, Randomized, and Randomized Public-Coin A distillation protocol is either *deterministic* or *randomized*. Deterministic protocols refer to ones where both Alice and Bob are deterministic. In a randomized protocol, both Alice and Bob are randomized. They both have their own supply of random bits, but they don't share any randomness. A protocol is *randomized public-coin*, if Alice and Bob have read access to a *shared* random string.

Clearly an randomized public-coin protocol is stronger than a randomized one, which in turn is stronger than a deterministic protocol. In fact, refreshing protocols with shared randomness are trivial, since Alice and Bob can simply discard the imperfectly shared information and use the shared randomness entirely. However, shared randomness doesn't trivialize quantum entanglement distillation protocols. In fact, it proves very useful in constructing EDPs.

Absolute vs. Conditional We assume a protocol always terminates. However, we make a distinction between a *successful termination* and an *abort*. Protocols that always successfully terminate are called *absolute protocols*; protocols that may abort are called *conditional protocols*. For a conditional protocol, we assume that besides the normal output, Alice will output a special symbol (either SUCC or FAIL) that indicates if the protocol successfully terminates or aborts. We assume that this special symbol is output in a special tape (in the Turing Machine notation) or a special wire (in the circuit notation), so that it will not be confused with the "normal" output of Alice. We also assume that the special symbol is a piece of classical information.

A classical correlation distillation protocol $\mathcal{P}$ works over a fixed alphabet Σ. Both the input and the output of $\mathcal{P}$ are pairs of strings in Σ.[4] A *string pair* $S \in \Sigma^n \times \Sigma^n$ is written as $S = (S^A, S^B)$, indicating that S^A belongs to Alice and S^B belongs to Bob.

We say $\mathcal{P}$ is a (Σ, n, m)-protocol, if the input string pairs have length n, and the output pairs have length m. We call m the *yield* of the protocol $\mathcal{P}$. Formally we may write this as

$$\mathcal{P}(I) = O \tag{19}$$

where $I \in \Sigma^n \times \Sigma^n$ is the input string pair, and $O \in \Sigma^m \times \Sigma^m$ is the output string pair. At the beginning of the protocol, Alice receives I^A as her local input, and Bob receives I^B as his. At the end of the protocol, Alice outputs O^A as her local output, and Bob outputs O^B. Notice that if $\mathcal{P}$ is randomized, then O can be a random variable.

A quantum entanglement distillation protocol $\mathcal{P}$ works over qubits. The shared quantum state between Alice and Bob can be described by a mixed state ρ. Suppose Alice and Bob share a state consisting of n qubit pairs, then ρ is a mixed state in a Hilbert space of dimension 2^{2n}. The reduced density matrices of Alice and Bob represent the local information they possess regarding to state ρ. We denote them by ρ^A and ρ^B. In other words, we have $\rho^A = \mathrm{Tr}_B[\rho]$ and $\rho^B = \mathrm{Tr}_A[\rho]$.

We say $\mathcal{P}$ is an (n, m)-protocol, if its input consists n qubit pairs and it outputs m qubit pairs. We call m the *yield* of $\mathcal{P}$. Formally we write this as

$$\mathcal{P}(\rho) = \sigma \tag{20}$$

where ρ is a density matrix of dimension 2^{2n} and σ a density matrix of dimension 2^{2m}.

3.3 Noise Models

For both classical and quantum protocols, noise models are used to describe the inputs to the protocols. A noise model is normally denoted by N, and is either classical or quantum, and is either adversarial or probabilistic.

Definition 3.1 (Adversarial Classical Noise Model) *An* adversarial classical noise model *over an alphabet Σ, often denoted by $\mathsf{N}^{\mathsf{ca}}_{\Sigma,n}$, is a set of string pairs.*

$$\mathsf{N}^{\mathsf{ca}}_{\Sigma,n} = \{I_1, I_2, ..., I_M\} \tag{21}$$

where $I_k \in \Sigma^n \times \Sigma^n$ for $k = 1, 2, ..., M$. When there is no danger of confusion, the subscripts Σ and/or n are omitted.

Definition 3.2 (Probabilistic Classical Noise Model) *A* probabilistic classical noise model *over an alphabet Σ, often denoted by $\mathsf{N}^{\mathsf{cp}}_{\Sigma,n}$, is a probabilistic distribution over $\Sigma^n \times \Sigma^n$. When there is no danger of confusion, the subscripts Σ and/or n are omitted.*

Definition 3.3 (Adversarial Quantum Noise Model) *An* adversarial quantum noise model, *often denoted by $\mathsf{N}^{\mathsf{qa}}_n$, is a set of quantum (mixed) states in a 2^{2n}-dimensional Hilbert space.*

$$\mathsf{N}^{\mathsf{qa}}_n = \{\rho_0, \rho_1, ..., \rho_{M-1}\} \tag{22}$$

When there is no danger of confusion, the subscript n is omitted.

[4] In fact, in some of the protocols we study in the thesis, the input and the output alphabets are different. However, they can be viewed as a natural extension to our conversion here.

Definition 3.4 (Probabilistic Quantum Noise Model) *A* probabilistic quantum noise model*, often denoted by $\mathsf{N}_n^{\mathsf{qp}}$, is a single density matrix ρ of dimension 2^{2n}. When there is no danger of confusion, the subscript n is omitted.*

All our definitions on noise models (classical/quantum, adversarial/probabilistic) can be naturally extended to *families* of noise models.

Definition 3.5 (Noise Model Family) *A* noise model family *is an infinite sequence of noise models over a fixed alphabet Σ.*

$$\mathcal{N} = (\mathsf{N}_1, \mathsf{N}_2, ..., \mathsf{N}_n, ...) \tag{23}$$

3.4 Quality of the Protocols

We define measures for the quality of correlation distillation protocols.

3.5 Classical Correlation Distillation Protocols

The quality of a classical protocol is measured by the *correlation* of the string pair it outputs.

Definition 3.6 (Correlation of Classical Protocols) *If a classical correlation distillation protocol $\mathcal{P}$ produces a string pair $O = (O^A, O^B)$ on input I, then its* correlation *on input I is the correlation between O^A and O^B, and it written as as $\mathsf{Cor}[\mathcal{P}(I)]$. The correlation of $\mathcal{P}$ over an adversarial noise model N^{ca}, denoted by $\mathsf{Cor}_{\mathsf{N}^{\mathsf{ca}}}[\mathcal{P}]$, is the minimal correlation of $\mathcal{P}$ over all inputs in N^{ca}*

$$\mathsf{Cor}_{\mathsf{N}^{\mathsf{ca}}}[\mathcal{P}] = \min_{I \in \mathsf{N}^{\mathsf{ca}}} \{\mathsf{Cor}[\mathcal{P}(I)]\} \tag{24}$$

The correlation of $\mathcal{P}$ over a probabilistic noise model N^{cp}, denoted by $\mathcal{P}[\mathsf{N}^{\mathsf{cp}}]$, is the expected correlation of $\mathcal{P}$ over all inputs in N^{ca}

$$\mathsf{Cor}_{\mathsf{N}^{\mathsf{cp}}}[\mathcal{P}] = E_{I \in \mathsf{N}^{\mathsf{cp}}} \{\mathsf{Cor}[\mathcal{P}(I)]\} \tag{25}$$

Definition 3.7 (Perfect Classical Protocol) *A classical correlation distillation protocol $\mathcal{P}$ is* perfect *for a classical noise model N^{c}, if $\mathsf{Cor}_{\mathsf{N}^{\mathsf{cp}}}[\mathcal{P}] = 1$.*

Often there are other constraints on the output besides the correlation. In a recovering protocol, Alice needs to output the original information she sent over. In a refreshing protocol, both Alice and Bob need to output (locally) uniformly distributed bits. The performance of a protocol is measured both in its yield and the correlation of its output with the constraints.

3.6 Quantum Entangle Distillation Protocols

The quality of a quantum protocol is measured by the fidelity of its output and the perfect EPR pairs.

Definition 3.8 (Fidelity of Quantum Protocols) *The fidelity of an entanglement distillation protocol $\mathcal{P}$ on input state ρ is the fidelity of its output, written as $\mathsf{F}(\mathcal{P}(\rho))$. The fidelity of $\mathcal{P}$ over an adversarial noise model N^{qa}, denoted by $\mathsf{F}_{\mathsf{N}^{\mathsf{qa}}}(\mathcal{P})$, is the minimal fidelity of $\mathcal{P}$ on all inputs in N^{qa}*

$$\mathsf{F}_{\mathsf{N}^{\mathsf{qa}}}(\mathcal{P}) = \min_{\rho \in \mathsf{N}^{\mathsf{qa}}} \{F(\mathcal{P}(\rho))\}. \tag{26}$$

The fidelity of a protocol $\mathcal{P}$ over N^{qp} is simply $\mathsf{F}(\mathcal{P}(\mathsf{N}^{\mathsf{qp}}))$.

Definition 3.9 (Perfect Quantum Protocol) *A quantum correlation distillation protocol $\mathcal{P}$ is* perfect *for a quantum noise model $N\mathsf{qc}$, if $\mathsf{F}_{\mathsf{Nqa}}(\mathcal{P}) = 1$.*

Definition 3.10 (Conditional Fidelity) *For an opportunistic protocol $\mathcal{P}$, its* conditional fidelity *over a noise model $N\mathsf{qc}$ is its fidelity conditioned on that $\mathcal{P}$ succeeds (i.e., outputs "SUCC"), and is denoted by $\mathsf{F}^{\mathsf{c}}_{N\mathsf{qc}}(\mathcal{P})$.*

4 Error Correcting Codes and Correlation Distillation Protocols

We discuss the relation between error correcting codes and correlation distillation protocols. In particular, we shall establish two results. The first result relates classical linear error correcting codes to classical correlation distillation protocols by proving that every linear ECC corresponds a CDP of same overhead with respect to the same noise model; the second result relates quantum stabilizer codes to entanglement distillation protocols by proving a similar result, that any stabilizer QECC corresponds a EDP of same overhead with respect to the same noise model.

4.1 Classical Error Correcting Codes and Correlation Distillation Protocols

Here we prove a very general result that relates a very large class of error correcting codes to correlation distillation protocols.

4.1.1 Error Correcting Codes

We describe the notion of Error Correcting Codes very briefly. Generally, an error correcting code is a systematic way of adding redundancy to the information, so that the redundant information is resilient to "small" disturbances. In this thesis we only focus on *block codes*, which encodes messages of a fixed length into code-words of a fixed length.

Definition 4.1 (Classical Error Correcting Code) *A* (classical) error correcting code *of parameter (n, k, d) over an alphabet Σ is function $E : \Sigma^k \mapsto \Sigma^n$, such that for any $x, y \in \Sigma^k$, $x \neq y$,* $\mathsf{dist}(E(x), E(y)) \geq d$. *The function E is called an* encoder. *A string $x \in \alpha^k$ is called a* message, *whose image, $E(x) \in \Sigma^n$ is called its* code-word.

This definition implicitly defines a *decoder* D as well. Consider an (n, k, d)-code. For any string $t \in \Sigma^n$, there can be at most one code-word of Hamming distance less than or equal to $(d-1)/2$ from t. If such a code-word exists, and suppose it is $E(x)$, then t will naturally be decoded to message x. If no such code-word exists, the decoding of t is *undefined*. More formally, $D : \Sigma^n \mapsto \Sigma^k$ is defined as

$$D(t) = \begin{cases} x & \text{if there exists an } x \text{ s.t. } \mathsf{dist}(E(x), t) \leq (d-1)/2 \\ \perp & \text{otherwise} \end{cases} \tag{27}$$

We stress that we focus on the properties of the code-words, rather than *computational complexity* of encoding/decoding. For example, we don't require the encoding and decoding algorithms of the codes to be efficient. Neither do we consider *list decoding*, where some strings more than $(d-1)/2$ away from any code-words may be decoded to a list of "candidate" messages (interested readers are referred to Guruswami's Ph.D. thesis [37] for a comprehensive survey).

4.1.2 Linear Codes

Perhaps the most important class of error correcting codes is the class of *linear codes.* Linear codes are of particular interest because of their simplicity and beautiful mathematical structures. In fact, most of the known good codes belong to the class of linear codes. The alphabet of a linear code is a finite field $\mathbb{F}$, and the encoder E for a linear code is a linear mapping from $\mathbb{F}^k$ to $\mathbb{F}^n$. Therefore E can be succinctly described as an $n \times k$ *generator matrix* G, and the encoding is simply a matrix multiplication: a message x, a k-dimensional vector, is mapped to code-word $G \cdot x$. All the code-words form a k-dimensional subspace in $\mathbb{F}^n$, which is the column space of G[5]. An (n, k, d)-linear code is often denoted as a $[n, k, d]$-code. The square brackets replaces the round parentheses to indicate that it is a linear code.

Given two linear codes E and E', represented by generator matrices G and G', we say they are *equivalent*, if G' can be obtained from G by row permutations and elementary column operations. Intuitively, if E and E' are equivalent, then one is only trivially different from the other, and there exists a very simple correspondence between the code-words of E and E'.

Next, we describe a special form of linear codes, known as the *systematic* codes. The definition is taken from [11, Definition 3.2.4, page 49].

Definition 4.2 (Systematic Code) *A linear code E is a* systematic code*, if its generator matrix G is of the form $G = \begin{bmatrix} I \\ P \end{bmatrix}$, where I is an $k \times k$ identity matrix and P a $(n-k) \times k$ matrix.*

Intuitively, a systematic code is one where a code-word is the messages it encodes concatenated with $(n-k)$ so-called "parity-check symbols".

It is a standard exercise in linear algebra that any linear code is equivalent to a systematic code [11, Theorem 3.2.5, page 80].

4.1.3 The Classical Bounded Corruption Model

We describe a classical noise model that is used by most error correcting codes, namely, the *classical bounded corruption model.*

Definition 4.3 (Classical Bounded Corruption Model) *A* classical bounded corruption model *of parameter (n, t) over alphabet Σ, denoted by $\mathcal{B}^{\mathsf{c}}_{n,t}$, is an adversarial model consisting of all the pairs (a, b), where both a and a are elements of Σ^n and the Hamming distance between a and a is at most t. In other words,*

$$\mathcal{B}^{\mathsf{c}}_{n,t} = \{(a, b) \mid a, b \in \Sigma^n, \mathsf{dist}(a, b) \leq t\} \tag{28}$$

Intuitively, the classical bounded corruption model adversarially corrupts (modifies) up to t symbols in a string of length n.

Now we are ready to state a positive result. We show a relation between systematic linear codes and correlation distillation protocols over the bounded corruption noise model.

Theorem 4.1 *For every systematic linear code E of parameter $[n, k, d]$ over alphabet Σ, there exists a perfect recovering, one-way, (Σ, k, k)-protocol $\mathcal{P}_E$ over a classical bounded corruption noise model $\mathcal{B}^{\mathsf{c}}_{k,(d-1)/2}$ that uses $(n-k)$ bits of communication.*

We present this positive result as a link to relate error correction to correlation distillation. As the result shows, in general, correlation distillation is at least as efficient as error correction, if not more efficient, for the majority of the error correction codes.

[5] The column space of G is the subspace generated by the columns of G.

4.2 Quantum Error Correcting Codes and Entanglement Distillation Protocols

We relate the notion of quantum error correcting codes (QECCs) to entanglement distillation protocols (EDPs), with the focus on their efficiencies.

4.2.1 Quantum Error Correcting Codes

Like their counterparts in classical information theory, quantum error correcting codes are systematic ways of adding redundancy to the quantum information, so that the encoded information is resilient to "small" noises. However, quantum error correction is more complicated. First of all, unlike in the classical case, quantum information cannot be duplicated, due to the No-cloning Theorem [88]. So the redundancy added by QECCs is limited, and measurement of the error syndrome shouldn't yield any information about the encoded message. Second, the noise model is more complicated: one qubit can suffer from a bit flip (an X operator), a phase shift (a Z operator), a bit flip *combined with* a phase shift (a Y operator), or a superposition of them. There are infinitely many (in fact, uncountably many) possible ways to "corrupt" a code-word, and a QECC needs to correct all of them. Indeed, less a decade ago, it wasn't even clear if QECC was possible at all, and a positive answer by Shor [79] and Steane [81] caused quite a surprise in the quantum information community. In a nutshell, QECC is possible because of the following reasons. First, for properly designed codes, the measurement of the error syndrome will only yield information about the *errors* on a code-word, and no information about the encoded message, thus not violating the non-cloning theorem. Second, due to the linearity of quantum mechanics, it suffices to correct the *basis errors*, and all other errors will be automatically corrected (by "collapsing" into one of the basis errors), thus solving the problem of infinitely many errors.

We now formally define QECCs. We always assume that these codes work over qubits, and they are *block codes.*

Definition 4.4 (Quantum Error Correcting Code) *An* error correcting code *of parameter* (n, k, r) *is a pair of quantum circuits* (E, D)*, both over* n *qubits as input (they can have ancillary qubits, initialized to state* $|\,0^m\rangle$*), such that for every* $x \in \{0,1\}^k$*, let* $|\,\phi_x\rangle$ *be defined as* $|\,\phi_x\rangle = E|\,x\rangle|\,0^{n-k}\rangle$ *and for any state* $|\,\psi\rangle$ *that can be obtained from* $|\,\phi_x\rangle$ *by (arbitrarily) modifying its* r *qubits, we have* $D|\,\psi\rangle = |\,x\rangle \otimes \rho$*, where* ρ *is a (possibly mixed) state of* $n-k$ *qubits. We write such a code a* $[\![n, k, r]\!]$*-code.*

4.2.2 The Quantum Bounded Corruption Model

We describe the quantum bounded corruption model, which is the quantum counterpart of the classical bounded corruption model. Correspondingly, this model is used by most quantum error correcting codes.

Before giving the formal definition, we need some additional notations. Recall that X, Y, and Z denote the Pauli operators, while I denotes the identity operator, all over a single qubit. We define $X^0 = Y^0 = Z^0 = I$. We use X_k, Y_k, and Z_k to denote these operators over the k-th qubit. Given a $2n$-bit vector $v = (x_0, x_1, ..., x_{n-1}, z_0, z_1, ...z_{n-1})$, which we call a *Pauli vector*, we can correspond it to a unique *multi-qubit Pauli operator* U_v, defined as

$$P_v = X_0^{x_0} Z_0^{z_0} \otimes \cdots \otimes X_{n-1}^{x_{n-1}} Z_{n-1}^{z_{n-1}} \tag{29}$$

which is a unitary operator over n qubits. Notice that since $X \cdot Z = Y$, we have $X^0 Z^0 = I$, $X^0 Z^1 = Z$, $X^1 Z^0 = X$, and $X^1 Z^1 = Y$. In other words, a Pauli vector designates a unitary operator formed by applying one of the four operators in $\{I, X, Y, Z\}$ to each of the n qubits. We define the *degree* of a Pauli vector to be the number of k's where x_k and z_k are not both 0, and we denote this by $\deg(v)$.

Definition 4.5 (Quantum Bounded Corruption Model) *A quantum bounded corruption model of parameter (n, r), denoted by $\mathcal{B}^{\mathsf{q}}_{n,r}$, is an adversarial quantum noise model consisting of all states of the form $(I \otimes P_v)\Phi_n$, where v is a Pauli vector of degree at most k. In other words,*

$$\mathcal{B}^{\mathsf{q}}_{n,r} = \{(I \otimes P_v)\ \Phi_n \mid \deg(v) \leq r\} \tag{30}$$

Intuitively, the quantum bounded corruption model adversarially corrupts up to r EPR pairs. The corruption appears quite limited, since it only allows applying one of the Pauli operators to Bob's share of the qubit (we call them "Pauli corruptions"). There are certainly more ways to corrupt the qubits; in fact there are uncountably many. However, since Pauli matrices, along with the identity operator, form a basis for one-qubit operations, any corruption can be decomposed into a linear superposition of the Pauli corruptions (or a mixture of them, if the corruption involves measurements).

4.2.3 An Equivalence between QECCs and One-way EDPs

Bennett et. al. [24] showed that every QECC corresponds to a one-way EDP with the same "efficiency". We review their results here.

Theorem 4.2 ([24]) *For every $[\![n, k, r]\!]$-code, there exists a corresponding perfect, deterministic, one-way, (n, k)-protocol over a quantum bounded corruption model $\mathcal{B}^{\mathsf{q}}_{n,r}$ that uses $2n$ bits of communication.*

Theorem 4.3 ([24]) *For every perfect, one-way (n, k)-protocol over a quantum bounded corruption model $\mathcal{B}^{\mathsf{q}}_{n,r}$, there exists a corresponding $[\![n, k, r]\!]$-code.*

4.2.4 Stabilizer Codes and EDPs

Theorems 4.2 and Theorem 4.3 establishes the equivalence between QECCs and EDPs over the quantum bounded corruption model. In particular, Theorem 4.2 shows a positive result on the power of EDPs. However, the construction of the EDPs in this theorem isn't very efficient. Since n teleportation procedures are used, a total of $2n$ bits of communication is deeded. Can we do better than this? The answer is "yes" for a large class of QECCs, namely the stabilizer codes.

Stabilizer Code The class of stabilizer codes is a very general class of quantum error correcting codes, and is the analogue of the class of linear codes in classical error correction. We briefly describe the properties, and the readers are referred to Gottesman [36] and Nielsen and Chuang [66] for a comprehensive tutorial. Informally, a stabilizer code S is a collection of "parity check" operators $S = \{M_0, M_1, ..., M_{l-1}\}$, where each M_i is a Pauli operator, and a state $|\,x\rangle$ is a code-word, if and only if $M_i|\,x\rangle = |\,x\rangle$ for all $i = 1, 2, ..., l-1$. We use $\langle S\rangle$ to denote the subgroup generated by S, and $N(S)$ the normalized of S, which consists of all Pauli operators P such that $P \cdot S \cdot P^\dagger = S$. We say a subspace L is *stabilized* by S, if every element $|\,\phi\rangle \in L$ is invariant under all elements in S. In other words, $L = \{|\,\phi\rangle \mid \forall i \in [l], M_i|\,\phi\rangle = |\,\phi\rangle\}$, and we write this as $L = C(S)$. Then $C(S)$ is also precisely the subspace spanned by all the code-words.

Definition 4.6 (Stablizer Code) *A* $[\![n,k,r]\!]$-stabilizer code S *is an independent set of* $(n-k)$ *Pauli vectors of dimension* $2n$*, denoted by* $S = \{M_0, M_1, ..., M_{n-k-1}\}$*, such that for any two Pauli vectors of degree at most* r P_0*,* P_1*,* $P_0^\dagger P_1 \notin N(S) - \langle S \rangle$*.*

It is known that a $[\![n,k,r]\!]$-stabilizer code is a $[\![n,k,r]\!]$-QECC [36, 66]. In other words, there exists generic constructions of the encoding/decoding circuit pair (E, D) from any stabilizer code. In particular, the decoding circuit D takes the following form. First, a unitary operator M is applied to all n qubits, which, intuitively, computes the $(n-k)$ "parity checks" defined by the $(n-k)$ operators $M_0, M_1, ..., M_{n-k-1} \in S$. Then, $(n-k)$ qubits are measured in the computational basis, resulting an "error syndrome" e. Finally, an appropriate "correction" circuit U_e is applied to the remaining k qubits. In particular, if the error syndrome is 0^{n-k}, then the correction circuit is the identity circuit.

Theorem 4.4 *For every* $[\![n,k,r]\!]$*-stabilizer code, there exists a corresponding perfect, one-way,* (n,k)*-protocol over a quantum bounded corruption model* $\mathcal{B}^{\mathsf{q}}_{n,r}$ *that used* $(n-k)$ *bits of communication.*

Comparing this result to Theorem 4.2, we see a large improvement for communication complexity (from $2n$ to $n-k$). Notice that there exists $[\![n,k,r]\!]$-stabilizer codes where c is a constant and $k = n - O(\log n)$. In this case, Theorem 4.4 yields an exponential improvement over Theorem 4.2. This result appears to be a folk-lore in the quantum information theory community and in particular, appeared as an exercise in Nielsen and Chuang [66, pp.597].

5 Non-Interactive Correlation Distillation

Here we demonstrate a series of negative results that aim to understand one of the most basic problems in the communication complexity of correlation distillation, i.e., how well Alice and Bob can do *if there is no communication at all*?

At the first glimpse of the problem, it may be tempting to answer "nothing interesting". Intuitively, it makes sense; if Alice and Bob don't communicate at all, they have no knowledge about the other parties, and how would they possible "recover" the information?

This intuition is in some sense correct for recovering protocols. Recall that in a recovering protocol, Alice simply outputs her input ($O^A = I^A$), and Bob wishes to output a O^B that is as close to O^A as possible. For an adversarial noise model, the behavior of Bob is determined by the minimax theorem. For a probabilistic noise model, Bob knows I^B and the joint distribution (I^A, I^B), and therefore his optimal strategy is to "guess" I^A according to the Bayes rule. In other words, Bob needs to choose X such that

$$X = \operatorname{argmax}_x \left\{ \frac{\mathcal{D}(x, I^B)}{\sum_y \mathcal{D}(y, I^B)} \right\} \tag{31}$$

where $\mathcal{D}$ is the distribution of (I^A, I^B) according to the noise model. Therefore, the noise model essentially determines the optimal strategy of Alice and Bob for non-interactive recovering protocols.

However, the situation is quite different for refreshing protocols over a probabilistic noise model. In a refreshing protocol, Alice and Bob share a probabilistic noise model, which is a distribution over the string pairs. Alice doesn't need to output her input string verbatim. Rather, Alice and Bob have the liberty to output *anything*. Furthermore, Alice and Bob may gather a large collection of the samples, all from the same distribution, and then hope to "concentrate" the correlation done to a small number of symbols. In this case, the problem of whether Alice and Bob can distill highly correlated bits without communication is not intuitively clear.

In fact, this problem of non-interactive correlation distillation has been considered by various researchers from different perspectives.

Consider the study of information reconciliation. In information reconciliation, Alice and Bob each possess some information that are not perfectly correlated. They wish to distill highly correlated bits by communication, yet maintaining privacy. In this model, Eve, the eavesdropper, can see all the communication between Alice and Bob. Therefore, if Alice and Bob could distill correlated bits non-interactively, this would be ideal for information reconciliation. Moreover, only after having an impossibility result on non-interactive distillation should one consider interactive information reconciliation. In this sense, the problem of non-interactive correlation distillation is the underline problem of the study of information reconciliation, and only a negative answer to this problem can justify the existence of this study.

Similar situation exists in the study of random beacon. In this setting, Alice (the beacon owner) and Bob (the verifier) each possesses the measurement data to an extraterrestrial objects. Due to the measurement error, their data are correlated but not perfectly so. Alice would convert her measurement into a sequence of random bits and publish these bits. The goal of the study on random beacon is to construct a *publicly verifiable* random source, and prevent Alice (the beacon owner) from cheating, i.e., affecting the outcome of the bits. If it is possible to distill highly correlated bits non-interactively, then the random beacon problem would be perfectly solved. Alice distills her bits from the measurement and publish them. Then Bob can apply his part of distillation, and with very high probability the result would agree with the bits Alice publishes. If the bits don't agree, Bob announces that Alice is cheating. In this way Alice would have no intention to cheat, since Bob can catch her cheating with very high probability. Therefore, here again, the problem of non-interactive distillation underlines the study of random beacons, and a negative answer to this problem lays at the foundation of this study.

Given the importance of this problem, it is not surprising that many researchers have considered it. In fact, a basic version of the problem was discovered and proven independently by several researchers since as early as 1991, including Alon, Maurer, Wigderson [3], Mossel and O'Donnell [61], and Yang [91].

We shall prove a sequence of negative answers to various versions of this problem. We assume that all protocols considered in this section, Alice and Bob only output one bit each. We make this assumption, since it seems to be the minimal requirement for a useful refreshing protocol. In some of the results, we would be considering protocols whose output alphabets differ from their input alphabets.

5.1 Tensor Product Noise Models

The noise models we discuss in this section are of a special form, which we call the "tensor product noise models". First, we review the definitions of the tensor product.

Definition 5.1 (Tensor Product of Vectors) *The* tensor product *of a n-dimensional vector v and an m-dimensional vector u is a (nm)-dimensional vector, denoted by w, such that $w[(x, y)] = v[x] \cdot u[y]$, for $x \in [n]$ and $y \in [m]$. We use $v^{\otimes k}$ to denote the vector obtained by taking the tensor product of k copies of v, and call it the n-*th tensor power *of v.*

Definition 5.2 (Tensor Product of Matrices) *The* tensor product *of an $a \times c$ matrix A and a $b \times d$ matrix B is an $(ab) \times (cd)$ matrix P, such that $P_{(x,z),(y,w)} = A_{x,y} \cdot B_{z,w}$ for $x \in [a]$, $y \in [b]$, $z \in [c]$, and $w \in [d]$. We write this as $P = A \otimes B$. We use $A^{\otimes k}$ to denote the matrix obtained by taking the tensor product of k copies of A, and call it the n-*th tensor power of A.

Definition 5.3 (Tensor Product of Distributions) *The* tensor product *of a distribution $\mathcal{D}_A$ over set A and a distribution $\mathcal{D}_B$ over set B is a distribution $\mathcal{D}$ over set $A \times B$, such that $\mathcal{D}(a,b) = \mathcal{D}_A(a) \cdot \mathcal{D}_B(b)$. We write this as $\mathcal{D} = \mathcal{D}_A \otimes \mathcal{D}_B$. We use $\mathcal{D}^{\otimes k}$ to denote the matrix obtained by taking the tensor product of k copies of $\mathcal{D}$, and call it the n-*th tensor power of $\mathcal{D}$.

Definition 5.4 (Tensor Product Classical Noise Model) *A probabilistic classical noise model $\mathsf{N}^{\mathsf{cp}}_{\Sigma,n}$ is a* tensor product classical noise model, *if there exists a probabilistic distribution $\mathcal{D}$ over $\Sigma \times \Sigma$ such that $\mathsf{N}^{\mathsf{cp}}_{\Sigma,n}$ is formed by the pair $(a_0 a_1 \cdots a_{n-1}, b_0 b_1 \cdots b_{n-1})$, where (a_k, b_k) is independently drawn from $\mathcal{D}$, for $k = 0, 1, ..., n-1$. The distribution $\mathcal{D}$ is called the* base distribution *of $\mathsf{N}^{\mathsf{cp}}_{\Sigma,n}$.*

In other words, the distribution of $\mathsf{N}^{\mathsf{cp}}_{\Sigma,n}$ is simply the n-th tensor power of the distribution $\mathcal{D}$ with symbols rearranged.

5.2 The Binary Symmetric Model

We first prove the negative result to perhaps the most basic version of the problem.

Definition 5.5 (Binary Symmetric Model) *A* binary symmetric model *of parameter (n, p), denoted as $\mathcal{S}_{n,p}$, is a probabilistic noise model defined as follows*

$$\mathcal{S}_{n,p}(a,b) = \frac{1}{2^n}(1-p)^{n-|a \oplus b|} \cdot p^{|a \oplus b|} \tag{32}$$

where $a, b \in \{0,1\}^n$.

The binary symmetric model is indeed a tensor produce noise model, and its base distribution is defined as $\mathcal{D}(0,0) = \mathcal{D}(1,1) = (1-p)/2$ and $\mathcal{D}(0,1) = \mathcal{D}(1,0) = p/2$. This model is closely related to the so-called "Binary Symmetric Channel". Imagine that Alice generates a uniform bit A as her local input, and send it to Bob through a noisy channel that flips each bit independently with probability p. If we denote the bit received by Bob by B, then the distribution of (A, B) is precisely $\mathcal{D}$.

Now suppose bits strings of Alice and Bob are described by $\mathcal{S}_{n,p}$. Alice and Bob each wishes to output one bit, denoted by a and b, respectively, such that the correlation between a and b is maximized. We also require that a and b themselves be unbiased. What's the maximum possible correlation of a and b, if Alice and Bob are not allowed to communicate?

If Alice and Bob simply output the k-th bit of their strings, for any $k \in [n]$, their outputs will have a correlation $1 - 2p$. This method is very simple, and almost looks naïve. Do there exist more sophisticated methods which will yield a higher correlation? Intuitively, it is not entirely clear that there don't. Our first negative result addresses this problem and proves that in fact the "naïve" method is optimal, and no protocol can yield a higher correlation than $1 - 2p$.

First, we need to define a restricted class of protocols, namely, locally uniform protocols.

Definition 5.6 (Locally Uniform Protocols) *A protocol $\mathcal{P}$ is* locally uniform *over a probabilistic noise model N^{cp}, if the distribution of its outputs are locally uniform bits, i.e., both O^A and O^B are uniform distributions over $\{0,1\}$, where $(O^A, O^B) = \mathcal{P}(\mathsf{N}^{\mathsf{cp}})$.*

Theorem 5.1 *The correlation of any locally uniform, randomized, non-interactive protocol over the binary symmetric model of parameter (n,p) is at most $1-2p$ for $p \leq 1/2$.*

The deterministic version of Theorem 5.1 (where the protocol is restricted to deterministic) was discovered and proven independently in as early as 1991 by many researchers, including Alon, Maurer, Wigderson, Mossel, O'Donnell, and Yang [3, 61, 91], and was attributed to "folklore" by Mossel and O'Donnell [61].

We can further extend Theorem 5.1 to protocols that are not locally uniform.

Definition 5.7 (δ-Locally Uniform Protocols) *A protocol $\mathcal{P}$ is δ-*locally uniform *over a probabilistic noise model N^{cp}, if the distribution of its output are locally δ-close to uniform bits, i.e., both O^A and O^B are δ-close to uniform distributions over $\{0,1\}$, where $(O^A, O^B) = \mathcal{P}(\mathsf{N}^{\mathsf{cp}})$.*

Theorem 5.2 *The correlation of any δ-locally uniform, randomized, non-interactive protocol over the binary symmetric model of parameter (n,p) is at most $1-2p(1-4\delta^2)$ for $p \leq 1/2$.*

Theorem 5.2 shows a trade-off between the "local uniformness" of a protocol and its correlation.

5.3 General Noise Models

Here, we extend the previous result to a general class of noise models.

Definition 5.8 (Distribution Matrix) *Let $\mathcal{D}$ be a probabilistic distribution over $\Sigma \times \Sigma$, where $|\Sigma| = q$. We say a $q \times q$ matrix M is the* distribution matrix *for $\mathcal{D}$, if $M_{x,y} = \mathcal{D}(x,y)$ for all $x, y \in \Sigma$.*[6] *We write the distribution matrix of $\mathcal{D}$ by $M_{\mathcal{D}}$.*

Definition 5.9 (Regular Matrix) *A $q \times q$ matrix M is* regular *if it is symmetric and $\mathbf{1}_q$ is the unique eigenvector with the largest absolute eigenvalue. Let ϵ be the difference between the largest absolute eigenvalue and the second largest. Then $q \cdot \epsilon$ is called the* scaled eigenvalue gap *of M. A distribution $\mathcal{D}$ is* regular *if its distribution matrix is regular.*

Notice that a distribution matrix M is non-negative (that every entry is non-negative). By the Perron-Frobenius Theorem [57], if M is symmetric, irreducible, and has $\mathbf{1}_q$ as an eigenvector, then $\mathbf{1}_q$ is the unique eigenvector with the largest eigenvalue, and thus M is regular. Therefore, intuitively, a noise model N^{cp} is regular if it satisfies the following three requirements: that it is *symmetric*, i.e., $\mathsf{N}^{\mathsf{cp}}(a,b) = \mathsf{N}^{\mathsf{cp}}(b,a)$ for every $a, b \in \Sigma$; that it is *locally uniform*, i.e., both the distributions of the local inputs of Alice and Bob are uniform; that it is *connected*, i.e., Σ cannot be partitioned into Σ_0 and Σ_1 such that $\mathsf{N}^{\mathsf{cp}}(a,b) = \mathsf{N}^{\mathsf{cp}}(b,a) = 0$ for all $a \in \Sigma_0$ and $b \in \Sigma_1$. Notice that if a noise model is not connected, that NICD is indeed possible for such a model. Suppose Σ is partitioned into Σ_0 and Σ_1. If Alice and Bob interpret symbols in Σ_0 as a "0" and symbols in Σ_1 as a "1", then they essentially have a noiseless binary noise model, which admits NICD.

[6] Here we identify Σ with $[q]$.

Theorem 5.3 *If $\mathsf{N}^{\mathsf{cp}}_{\Sigma,n}$ is a tensor product noise model whose base distribution is regular with scaled eigenvalue gap ϵ, then the correlation of any δ-locally uniform, randomized, non-interactive $(\Sigma, n, 1)$-protocol over the classical probabilistic noise model $\mathcal{D}^{\otimes n}$ is at most $1 - \epsilon(1 - 4\delta^2)$.*

To see that Theorem 5.3 is indeed a more general result, notice that the base distribution of the binary symmetric model is indeed regular with scaled eigenvalue gap $2p$.

Theorem 5.3 provides a general negative answer to the question of non-interactive correlation distillation. Notice the upper bound on the correlation is independent from n, the size of the input to the protocols. Therefore, if the noise model is regular, then Alice and Bob cannot distill the correlation any higher than what is dictated by the scaled eigenvalue gap, even if they are willing to collect many samples from the same model and then "concentrate" them them into one single symbol.

5.4 The Binary Erasure Noise Model

We prove a similar impossibility result for another noise model, namely the binary erasure noise model. Intuitively, this model describes the situation where Alice sends an unbiased bit to Bob, which is erased (and replaced by a special symbol $\perp$) with probability p.

Definition 5.10 (Binary Erasure Noise Model) *The* binary erasure noise model*, denoted by $\mathcal{E}_p$ is a tensor product noise model with base distribution $\mathcal{D}_{\mathcal{E}}$ over alphabet $\{0, 1, \perp\}$, defined as $\mathcal{D}_{\mathcal{E}}(0,0) = \mathcal{D}_{\mathcal{E}}(1,1) = (1-p)/2$, $\mathcal{D}_{\mathcal{E}}(0,\perp) = \mathcal{D}_{\mathcal{E}}(1,\perp) = p/2$.*

Perhaps the binary erasure noise model is the simplest noise model that is not symmetric, and thus isn't regular. It is, however, a realistic one. Consider as example the situation where Alice and Bob receive their inputs by observing a pulsar. It is quite likely that the noise of the measurements by Alice and Bob are of the "erasure-type", i.e., the corruption of information can be detected. Furthermore, it is also possible that Alice and Bob have different measurement apparatus and different levels of accuracy. In the random beacon problem, Alice (as the beacon owner) might own a more sophisticated (and more expensive) measuring device with higher accuracy, while Bob (as the verifier) has a more noisy measurement device. An extreme case would be that Alice has near-perfect accuracy in her measurement, but Bob's measurement is noisy. Such a situation can be well approximated by the binary erasure noise model.

Notice that in this model, Alice's input is the uniform distribution over $\{0, 1\}$, and Bob's input is 0 and 1 with probability $(1-p)/2$ each, and $\perp$ with probability p. A naïve protocol under this model only uses the first pair of the inputs. Alice outputs her bit, and Bob outputs his bit if his input is 0 or 1, and outputs a random bit if his input is $\perp$. This is a locally uniform protocol with correlation $1 - p$.

The next theorem shows that no protocol can do much better than the naïve protocol.

Theorem 5.4 *The correlation of any locally uniform protocol over the noise model $\mathcal{E}_p$ is at most $\sqrt{1 - p(1 - 4\delta^2)}$.*

We suspect that it is not a tight bound, but it is sufficient to show that it is bounded away from 1 and is independent from n. Therefore, even with perfect accuracy in Alice's measurement, NICD is impossible if Bob's measurement is noisy.

6 A Positive Result on One-bit Correlation Distillation

The impossibility results from the previous section suggest that for many noise models, communication is essential for correlation distillation. Thus it is interesting to ask how much communication is essential. In particular, we were interested in the question "does a single bit of communication help?" We answer this question positively by presenting a protocol that non-trivially distills correlation from the binary symmetric noise model with one bit of communication. This result shows that even the minimal amount of communication is provably more powerful than no communications at all.

Recall that over a binary symmetric noise model $\mathcal{S}_{n,p}$, no non-interactive, locally uniform protocols can have a correlation more than $1 - 2p$. Now, we consider protocols with one bit of communication. Suppose Alice sends one bit to Bob, which Bob receives with perfect accuracy. If we still only require Alice and Bob each to output a single bit, then the problem is trivial: Alice can generate an unbiased bit x and send it to Bob, and then Alice and Bob both output x. This protocol has perfect correlation. Thus, to make the problem non-trivial, we require that Alice and Bob must output two bits each. Suppose Alice outputs (X_1, X_2) and Bob outputs (Y_1, Y_2). We define the correlation of a protocol to be

$$2 \cdot \min_{i=1,2} \left\{ \mathsf{Prob}\left[X_i = Y_i\right] \right\} - 1$$

In this situation, we say a protocol is *locally uniform*, if both (X_1, X_2) and (Y_1, Y_2) are uniformly distributed.

Now we describe a locally uniform protocol of correlation about $1 - 3p/2$. The protocol is called the "AND" protocol. Both Alice and Bob only take the first two bits as their inputs. Alice directly output her bits, and sends the AND of her bits to Bob. Then, intuitively, Bob "guesses" Alice's bits using the Bayes rule and outputs them. A technical issue is that Bob has to "balance" his output so that the protocol is still locally uniform. The detailed description is in Figure 3.

STEP I Alice computes $r := a_1 \wedge a_2$, sends r to Bob, and outputs (a_1, a_2).

STEP II Bob, upon receiving r from Alice:

IF $r = 1$ THEN output $(1, 1)$.
ELSE IF $b_1 = b_2 = 1$ THEN output
- $(0, 0)$ with probability $p/(2 - p)$;
- $(0, 1)$ with probability $(1 - p)/(2 - p)$;
- $(1, 0)$ with probability $(1 - p)/(2 - p)$;

ELSE output (b_1, b_2).

Alice receives input bits a_1, a_2, and Bob received input bits b_1, b_2, where $(a_1 a_2, b_1 b_2)$ is drawn from $\mathcal{S}_p^{\otimes 2}$

Figure 3: The AND protocol

We can easily verify (by a straightforward computation) the following result.

Theorem 6.1 *The AND protocol is a locally uniform protocol with correlation* $1 - \frac{3p}{2} + \frac{p^2}{4-2p}$. ■

This is a constant-factor improvement over the non-interactive case.

This result may seem a little surprising. It appears that Alice isn't fully utilizing the one-bit communication, since she is sending an AND of two bits, whose entropy is less than 1. It is tempting to speculate that by having Alice send the XOR of the two bits, Alice and Bob can obtain better result, since Bob gets more information. Nevertheless, the XOR doesn't work, in some sense due to its "symmetry". Consider the case Alice sends the XOR of her bits to Bob. Bob can compute the XOR of his bits, and if the two XOR's agree, Bob knows that with high probability, both his bits agrees with Alice's. However, if the two XOR's don't agree, Bob knows one of his bits is "corrupted", but he has no information about which one. Furthermore, however Bob guesses, he will be wrong with probability $1/2$. On the other hand, in the AND protocol, if Bob receives a "1" as the AND of the bits from Alice, he knows for sure that Alice has $(1,1)$ and thus he simply outputs $(1,1)$; if $r=0$ and $b_1=b_2=1$, he knows that his input is "corrupted", and he "guesses" Alice's bit according to the Bayes rule of posterior probabilities. If Bob receives a "0" as the AND and $(b_1,b_2)\neq(1,1)$, then the data looks "consistent" and Bob just outputs his bits. In this way, $1/4$ of the time (when Bob receives a 1), Bob knows Alice's bits for sure and can achieve perfect correlation; otherwise Alice and Bob behave almost like in the non-interactive case, which gives $1-2p$ correlation. So the overall correlation is about $1/4\cdot 1+(3/4)\cdot(1-2p)=1-3p/2$.

7 Non-Interactive Entanglement Distillation

We study non-interactive entanglement distillation protocols. As in the case of non-interactive classical correlation distillation, non-interactive entanglement distillation also serves as the most basic problem in study of communication complexity of EDPs. Notice that a priori, it is not necessarily obvious that non-interactive protocols would be useless. In fact, Bennett et. al. [20] constructed a non-interactive entanglement distillation protocol for a specific noise model where Alice and Bob share a large number of identical copies of some pure state.[7] However, as we shall soon see, non-interactive entanglement distillation is impossible for a number of less "benign" noise models.

In this section, we only study protocols that only output one qubit pair, since these are the minimally "useful" protocols, and a lower bound on their fidelities suffices as a general lower bound. In particular, we consider three noise models, namely the bounded decoherence model, the bounded corruption model, and the depolarization model, and prove corresponding bounds on the fidelity of non-interactive EDPs over them. These bounds are tight or almost tight.

7.1 The Bounded Measurement Model

We define the bounded measurement noise model, and prove a tight lower bound on the fidelity of non-interactive protocols over such a model. We first need some more notations. An *error indicator vector* is a n-dimensional vector from an alphabet $\mathbf{v}\in\{0,1,*\}$. The *degree* of a vector $\mathbf{v}$, denoted by $\deg(\mathbf{v})$, is the number of entries in $\mathbf{v}$ that are not "$*$". For each $\mathbf{v}$ corresponds *measurement error state* $|\,\phi_{\mathbf{v}}\rangle$ as $|\,\phi_{\mathbf{v}}\rangle=\bigotimes_{j=0}^{n-1}|\,\phi_j\rangle$, where

$$|\,\phi_j\rangle=\begin{cases}|\,0\rangle^A|\,0\rangle^B & \text{if } \mathbf{v}[j]=0\\ |\,1\rangle^A|\,1\rangle^B & \text{if } \mathbf{v}[j]=1\\ \Phi^+ & \text{if } \mathbf{v}[j]=*\end{cases}$$

The *degree* of a measurement error state $|\,\phi_{\mathbf{v}}\rangle$ is the degree of $\mathbf{v}$.

[7] They call their scheme "entanglement concentration".

Definition 7.1 (Bounded Measurement Model) *A* bounded measurement model *of parameter (n,t), denoted by $\mathcal{M}_{n,t}$, is an adversarial quantum noise model consisting of all measurement error states of degree at most t. In other words,*

$$\mathcal{M}_{m,t} = \{|\,\phi_{\mathbf{v}}\rangle \mid \deg(\mathbf{v}) \leq t\} \tag{33}$$

Intuitively, the bounded measurement model describes the situation where up to t (unknown) EPR pairs are measured in the computational basis (thus each pair results in either $|\,0\rangle|\,0\rangle$ or $|\,1\rangle|\,1\rangle$). Therefore, this model is in some sense more "benign" than the quantum bounded corruption model, where the corruptions on an EPR pair can be more general. However, this simpler model is already interesting enough to ensure a non-trivial result.

Theorem 7.1 *The fidelity of any non-interactive, share-randomized entanglement distillation protocols over a bounded measurement model $\mathcal{M}_{n,r}$ is at most $1 - r/2n$.*

Notice that there exists a very simple non-interactive, share-randomized protocol that achieves a fidelity of $1 - r/2n$. Alice and Bob use their shared randomness to select a random input qubit pair and output them. If this pair is not measured, they have a fidelity of 1; if the pair is measured, they have a fidelity of $1/2$. However, a random pair is measured with probability at most r/n. Therefore, the overall fidelity is at least $1 - r/2n$, and the lower bound in Theorem 7.1 is tight.

7.2 The Bounded Corruption Model

We prove a similar lower bound on the fidelity of non-interactive protocols over a bounded corruption model.

Theorem 7.2 *The fidelity of any non-interactive, share-randomized entanglement distillation protocols over a quantum bounded corruption model $\mathcal{B}^{\mathrm{q}}_{n,r}$ is at most $1 - r/2n$.*

Notice that if Alice and Bob use their shared random bits to select an input pair and output them, they will achieve a fidelity of $1 - r/n$ So this lower bound is almost tight (up to a constant factor).

7.3 The Depolarization Model

Depolarization Model We define the depolarization noise model, which is a commonly used model for quantum noises [87, 66]. Intuitively, a depolarization model of parameter p describes the situation where each of Bob's qubits is replaced by a completely mixed state independently with probability p. In particular, if Alice and Bob initially share the Bell state Φ^+, then the "depolarization" noise moves it to

$$\rho_p = (1 - \frac{3p}{4})|\Phi^+\rangle\langle\Phi^+| + \frac{p}{4}(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|) \tag{34}$$

which is also known as the "Werner state" [87].

Definition 7.2 (Depolarization Model) *A* depolarization model *of parameter (n,p) is a probabilistic quantum noise model defined as $\mathcal{D}_{n,p} = \rho_p^{\otimes n}$.*

Theorem 7.3 *The fidelity of any non-interactive, share-randomized entanglement distillation protocols over a depolarization model $\mathcal{D}_{n,p}$ is at most $1 - p/2$.*

Notice that there exists a very simple non-interactive protocol of fidelity $1-3p/4$. If Alice and Bob simply outputs the first qubit of their shares, the fidelity of the output is $1-3p/4$. Notice that this protocol is deterministic. Therefore the lower bound in Theorem 7.3 is almost tight (up to a constant factor).

8 The Entanglement Noise Model

We study a very general noise model, namely the entanglement noise model. Before we proceed, we motivate this entanglement noise model by drawing an analogy between classical randomness extraction and quantum entanglement distillation.

8.1 Classical Randomness Extraction

Classical randomness extraction is a fascinating topic in theoretical computer science by itself. The motivation for study randomness extraction is that randomness plays an important role in classical computation (see Motwani and Raghavan [62] for a comprehensive explanation), but it can be very expensive, if not impossible, to have a perfect random source that produces unbiased, uncorrelated random bits. Therefore, it is very natural to ask if it is possible to perform randomized computation using less-than-perfect random sources. In particular, is it possible to have an automatic process to convert any randomized computation that was designed to have a perfect random source as input into one that works with imperfect random sources?

A series of results established by various researchers answered positive to this above question, and the notion of randomness extractors was developed along this line of research. Intuitively, a randomness extractor is a procedure that converts input from an imperfect random source to almost-perfect random bits as its output. Technically, an extractor also takes a small number of perfect random bits from an auxiliary input. But the size of auxiliary input is normally logarithmically small as compare to the size of its main input. See Figure 4.

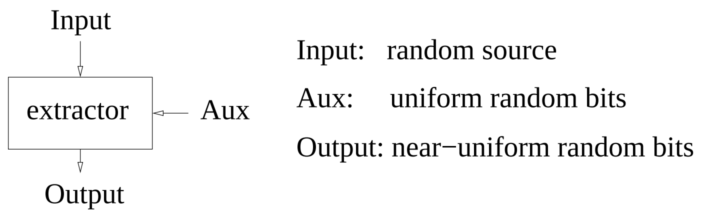


Figure 4: Classical randomness extractor

We briefly review some of the work on extractors and refer the readers to Nisan and Ta-Shma [67] and Shaltiel [77] for a more comprehensive and up-to-date survey. In the early stages of research on extractors, people have considered various specific models of "imperfect random bits". Von Neumann [63] showed that a linear number of perfect random bits can be extracted from independent tosses of a biased coin with unknown bias. Blum [10] extended the model of a biased coin to a Markov chain. Santha and Vazirani [76] considered extractors with many independent, yet adversarial random sources, as input. This contrasts with the modern stage, started by Nisan and Zuckerman [68], where researcher started to study extractors over *arbitrary* input. Today, the state-of-art extractors can extract near-perfect random bits from *random source* [84, 75]. We also have a quite good understanding about the limit of extractors. For example, we know that the yield (size size of the output) of an extractor is determined by the *min entropy* of the input, and that the size of the auxiliary input needs to be logarithmic in the size of input. On the other hand, there exist constructions of extractors that match these limits [84, 75].

8.2 Similarity Between Extractors and EDPs

We discuss the similarity between classical extractors and quantum entanglement distillation protocols. Entanglement plays a central role in quantum information theory and quantum computation. It was argued that entanglement is the essential physical phenomenon that gives quantum computation its power of exponential speed-up over classical computation. Although it is still under heated debate and relentless research whether entanglement is essential for quantum computation [23, 46, 19], it is widely believed that that entanglement plays a crucial part for quantum information theory. However, somewhat like in the case of classical randomness, it is very hard to have a perfect source of entanglement. EPR pairs, as with currently technology, are notoriously hard to maintain. They decohere very easily and become "less entangled". As randomness extractors convert less-than-perfect random bits into near-perfect ones, entanglement distillation protocols convert less entangled quantum states into almost perfect EPR pairs.

There exist even deeper similarities. An extractor, being a deterministic procedure, cannot create randomness by itself. It needs to "distill" the randomness from the input bits into randomness of the purest form, namely unbiased, uncorrelated random bits. An entanglement distillation protocol, being an LOCC protocol, cannot create entanglement by itself. Therefore an EDP also needs to distill the entanglement from the input into EPR pairs, which are the entanglement of the purest form — each pair is maximally entangled and separable from the rest.

Moreover, the early stage of searches on EDPs greatly resembles that on the randomness extractors, in that people have considered various specific models of "imperfect EPR pairs" and constructed protocols over these specific models. As an example, the first work we are aware of on EDPs is by Bennett, Bernstein, Popescu, and Schumacher [20], which used the model where many identical copies of pure state $|\phi\rangle = (\cos\theta|01\rangle + \sin\theta|10\rangle)$ is given as the input. This model resembles the biased coin model used by von Neumann [63]. More complicated models were proposed later, as Bennett, Brassard, Popescu, Schumacher, Smolin, and Wootters [21] studied the case where the input is identical copies of a mixed state. Horodecki, Horodecki, and Horodecki [40, 43] and Rains [71, 72, 73] studied the case where the input is many identical copies of a known pure state. Notice that the classical counterpart of this state would be an input with known distribution, for which case the problem of randomness extraction was long solved by Shannon [78]. This sharp contrast somewhat demonstrates the difficulty of quantum information theory, as very simple problems in classical information theory can become highly non-trivial in quantum.

However, despite the similarities and the correspondence between the early stages in research on randomness extractors and entanglement distillation protocols, there hasn't been a counterpart of the modern stage of extractors in the study of EDPs. In other words, there hasn't much work on EDPs over arbitrary entangled states. This observation naturally motivates the entanglement noise model and the study on EDPs over such a model.

8.3 The Entanglement Noise Model and the Impossibility Result

We describe the entanglement noise model, which contains all pure states of a certain amount of entanglement.

Definition 8.1 (Entanglement Noise Model) *A* entanglement noise model *of parameter* (n, k)*, denoted by* $\mathcal{E}_{n,k}$*, is an adversarial quantum noise model consisting of all* $2n$*-qubit pure states of en-*

tanglement at least k. In other words,

$$\mathcal{E}_{n,k} = \{|\,\phi\rangle \in \mathcal{H}_{2^{2n}} \mid \mathsf{E}(\phi) \geq k\} \tag{35}$$

Unfortunately, there don't exist entanglement distillation protocols over the entanglement noise model. This is true even if we restrict ourselves to starting states with the maximum possible entanglement and only requires the protocol to output a single EPR pair Φ^+.

Theorem 8.1 *There don't exist perfect $(n,1)$-protocols over the entanglement noise model $\mathcal{E}_{n,n}$.*

This is a clear distinction between the situation of classical randomness extraction and quantum entanglement extraction. In the classical case, all the probabilities are non-negative real numbers, and the min entropy of a random distribution already characterizes the distribution well. In the quantum case, the magnitudes are complex numbers, and the entanglement alone isn't good enough to describe the state. Even more interestingly, since one has the freedom to switch bases in quantum, we can build a mixed state which is a mixture of maximally entangled states, yet the mixed state itself is completely disentangled. This phenomenon doesn't seem to have a counterpart in classical probability.

9 The Fidelity Noise Model

We introduce the fidelity noise model and study the communication complexity of entanglement distillation protocols over this model.

With the motivation of studying EDPs for a general class of noise models and the impossibility result for the (too general) entanglement noise model, we consider the fidelity noise model as one that is still quite general, but also useful. Intuitively, the entanglement noise model fails because there exists many maximally entangled states that are orthogonal to each other, and no protocol can work with all of them. Therefore, some "closeness" condition is needed, i.e., we need some guarantee that the input state is close to a fixed maximally entangled state. This intuition naturally leads to the fidelity noise model, which, informally speaking, describes the situation where the input state has a reasonably high fidelity with the perfect EPR pairs.

We give the definition of the fidelity noise model.

Definition 9.1 (Fidelity Noise Model) *A* fidelity noise model *of parameter (n,a), denoted by $\mathcal{F}_{n,f}$, is an adversarial quantum noise model consisting of all $2n$-qubit mixed states of fidelity at least a. In other words,*

$$\mathcal{F}_{n,f} = \{\rho \in \mathcal{H}_{2^{2n}} \mid \mathsf{F}(\rho) \geq f\} \tag{36}$$

This model was also independently considered by Lo and Chau [55] and Shor and Preskill [80] in proving the security of the BB84 quantum key distribution protocol [15], and by Barnum et. al. [22] in studying the so-called "purity-testing protocols".

9.1 Absolute Protocols

We prove that no absolute protocol would work well over a fidelity noise model. In fact, we can prove an even stronger result, which extends to protocols that accept perfect EPR pairs as auxiliary inputs.

Protocols with Auxiliary Input We consider protocols with auxiliary inputs as a slight extension to "standard" entanglement distillation protocols. In addition to the input states, Alice and Bob also receive k EPR pairs (each pair is shared between Alice and Bob) as auxiliary inputs. Obviously a protocol with auxiliary input would be more powerful than one without. An immediate example is that a deterministic protocol with auxiliary inputs can simulate a randomized public-coin protocol, since Alice and Bob can use the shared EPR pairs to simulate shared random bits.

Typically, the size of the auxiliary input, k is very small compared to the size of the input and the output. Since a protocol with k EPR pairs of auxiliary input can trivially output k perfect EPR pairs, we require that m, the size of the output of such a protocol to be greater than k.

Theorem 9.1 *The fidelity of any (n, m)-protocol with $k < m$ EPR pairs as auxiliary inputs over a fidelity model $\mathcal{F}_{n,1-\epsilon}$ is at most $1 - \frac{2^m - 2^k}{2^m} \frac{2^n}{2^n - 1}\epsilon$. Moreover, this lower bound is tight, in that for every n, m, n, there exists an (n, m)-protocol using k EPR pairs as auxiliary inputs of fidelity $1 - \frac{2^m - 2^k}{2^m} \frac{2^n}{2^n - 1}\epsilon$.*

In particular, even in the "minimal case", where $k = 0$ and $m = 1$, the maximum possible fidelity of any protocol is bounded by $1 - \frac{2^{n-1}}{2^n - 1}\epsilon \leq 1 - \epsilon/2$. So it is impossible to arbitrarily increase the fidelity to be close to 1, even with unlimited amount of communication.

Interestingly, we can show that communication almost doesn't help for entanglement distillation over the fidelity model.

Theorem 9.2 *There exists a non-interactive, randomized public-coin entanglement distillation $(n, 1)$-protocol of fidelity $1 - \frac{3}{4}\frac{2^n - \frac{2}{3}}{2^n - 1}\epsilon$ over a fidelity noise model $\mathcal{F}_{n,1-\epsilon}$. Furthermore, this it is almost best possible, in that the fidelity of any non-interactive, randomized public-coin entanglement distillation $(n, 1)$-protocol over the model $\mathcal{F}_{n,1-\epsilon}$ is $1 - \frac{3}{4}\frac{2^{2n}}{2^{2n} - 1}\epsilon$, for $\epsilon \leq \frac{2^{2n} - 1}{2^{2n+1}}$.*

It is interesting to compare this result to a special case of Theorem 9.1, where $k = 0$ and $m = 1$. We see that with communication, the maximum fidelity of a protocol is about $1 - \epsilon/2$, and there exists a protocol that matches this bound exactly. Without communication, the maximum fidelity is about $1 - 3\epsilon/4$, and it is tight, too. Therefore, communication does help in this case, but not much.

9.2 Purity Testing Protocols and Conditional Protocols

Theorem 9.1 spells a negative result for absolute protocol over the fidelity noise model by demonstrating a state ρ such that no LOCC protocol can increase its fidelity significantly. However, the situation is vastly different for the case of conditional protocols. We shall prove that very efficient entanglement distillation protocols exist that can increase the conditional fidelity to as close to 1 as possible. As we shall see, one construction of such protocols is closely related to the notion of purity testing protocols.

Theorem 9.3 *For all integers $n > s$, there exists an conditional, randomized, $(2ns + s)$-bit one-way, $(n, n - s)$ protocol over the fidelity noise model $\mathcal{F}_{n,1-\epsilon}$ with success probability at least $1 - \epsilon$ and conditional fidelity $1 - \frac{2^{-s}}{1 + 2^{-s} - \epsilon}$.*

In fact, a closer look at the proof reveals that of the $(2n + 1)$ bits of communication in this protocol, $2n$ of them are used for selecting a random string, which can be spared if Alice and Bob initially share a random string. This observation leads to the following corollary to Theorem 9.3.

Corollary 9.1 *For all integers $n > s$, there exists an conditional, randomized public-coin, s-bit one-way, $(n, n-s)$ protocol over the fidelity noise model $\mathcal{F}_{n,1-\epsilon}$ with success probability at least $1-\epsilon$ and conditional fidelity $1 - \frac{2^{-s}}{1+2^{-s}-\epsilon}$.* ■

Here, we see an exponential trade-off between the conditional fidelity and the amount of communication: each additional bit communicated will reduce the gap between the conditional fidelity and 1 by almost half. This contrasts sharply with the relation between the fidelity and the communication, where communication does help a little, but by only at most a constant factor.

9.3 Communication Complexity of Protocols over the Fidelity Model

We study the communication complexity of entanglement distillation protocols over the fidelity noise model. We prove a lower bound that matches the result from Corollary 9.1 up to an additive constant. This effectively showed that the construction of Corollary 9.1 is optimal.

Definition 9.2 (Ideal Success Probability) *The* ideal success probability *of a conditional quantum entanglement distillation (n, m)-protocol is the probability that it succeeds over the input Φ_n. A protocol is* ideal *if its ideal success probability is 1.*

Theorem 9.4 *The conditional fidelity of any randomized public-coin s-bit (n, m)-protocol of ideal success probability p is at most $1 - \frac{\epsilon p}{2^{s+1}}$ over a fidelity noise model $\mathcal{F}_{n,1-\epsilon}$*

An immediate corollary of this theorem is that the conditional fidelity of an s-bit ideal protocol is at most $1 - \epsilon/2^{s+1}$. Therefore, to achieve a fidelity or $1-\delta$ on the output, $\log(1/\delta) + \log(\epsilon \cdot p) - 1$ bits of classical communication is needed. On the other hand, Corollary 9.1 yields a communication complexity of $\log(1/\delta) + \log(1-\epsilon)$. In the case where both ϵ and p are constants, these two results match up to an additive constant. It is a rather interesting observation, besides the fact that it implies the optimal of Corollary 9.1 and the tightness of Theorem 9.4. Notice that Theorem 9.4 is proven for protocols that only output a single qubit pair — a minimal possible yield, while the construction from the random hash protocol used by Corollary 9.1 outputs $(n-s)$ qubits — an asymptotically maximum possible yield.[8] Despite the two extreme cases on the yield of the protocols, this two result match nicely.

10 Proposed Work

I propose to continue working on the communication complexity of CDP/EDPs. So far I have obtained a collection of results, but they also open up many new open problems. I list some of them.

1. **Optimality of the AND protocol**

   I have shown that one bit of communication already makes a difference in correlation distillation by demonstrating the AND protocol. Is this optimal?

2. **More Negative Results on Correlation Distillation**

   I have proved a number of negative results on NICD, which serves as the first step towards understanding classical correlation distillation. It would be more desirable to extend these

[8]Notice that because of the exponential trade-off, it is normally sufficient to have $s = o(n)$, and in that case the random hash protocol outputs almost all the qubit pairs as input.

results to the interactive case. An immediate question is: what if Alice sends one bit to Bob? Can we bound the correlation of one-bit protocols?

3. **More Negative Results on Entanglement Distillation**

   As in the case of correlation distillation, I have proven a number of negative results on NIED. Also, the challenge here is to extend these results to the interactive case.

The time-line I propose is as follows.

3/2003 – 3/2004 Continue research on the open problems

3/2004 – 9/2004 Write up thesis

References

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

[39] 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`.

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

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

[42] 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`.

[43] 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`.

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

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

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

[47] 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`.

[48] 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.

[49] 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`.

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

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

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

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

[54] 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.

[55] 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`.

[56] 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`.

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

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

[59] 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.

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

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

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

[63] 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.

[64] 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`.

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

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

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

[68] 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.

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

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

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

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

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

[74] 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`.

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

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

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

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

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

[80] 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`.

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

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

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

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

[85] 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`.

[86] 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`.

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

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

[89] 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.

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

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