Security of Partially Corrupted Quantum Repeater Networks

Adrian Harkness*, Walter O. Krawec†, Bing Wang‡

Abstract

Quantum Key Distribution allows two parties to establish a secret key that is secure against computationally unbounded adversaries. To extend the distance between parties, quantum networks are vital. Typically, security in such scenarios assumes the absolute worst case: namely, an adversary has complete control over all repeaters and fiber links in a network and is able to replace them with perfect devices, thus allowing her to hide her attack within the expected natural noise. In a large-scale network, however, such a powerful attack may be infeasible. In this paper, we analyze the case where the adversary can only corrupt a subset of the repeater network connecting Alice and Bob, while some portion of the network near Alice and Bob may be considered safe from attack (though still noisy). We derive a rigorous finite key proof of security assuming this attack model, and show that improved performance and noise tolerances are possible. Our proof methods may be useful to other researchers investigating partially corrupted quantum networks, and our main result may be beneficial to future network operators.

1 Introduction

Quantum key distribution (QKD) allows for the establishment of secure secret keys between two parties, Alice and Bob, the security of which is guaranteed by the laws of physics. This is unlike classical public key cryptography which necessarily requires computational assumptions placed on the adversary in order to achieve security. See [1–4] for a general survey on QKD.

One of the main limiting factors of QKD performance is distance—since transmissivity decays exponentially with distance, achieving efficient QKD between two parties that are far away from each other remains a tremendous challenge. One promising solution for long-distance QKD is through quantum networks, e.g., *quantum internet* [5–7]. Quantum networks consist of quantum repeaters that are capable of creating shared end-to-end entanglement between parties, even if the repeaters are controlled by an adversary. As such, they provide a much stronger security guarantee than the current day *trusted node networks* [8–15], where the trusted nodes must be trusted.

In almost all QKD performance analyses, the security of the system assumes the absolute worst case, namely that the adversary controls the entire region outside of Alice and Bob's labs. This implies that the adversary controls all repeaters and fiber links in the entire network, and can even replace them with ideal, noiseless devices, and thus "hide" within the expected natural noise. Considering that such networks are meant to allow for long-distance QKD operation, this is an unrealistic scenario. In any realistic operational scenario, it is likely that an adversary can only control a strict subset of repeaters and fiber links. Furthermore, it is also realistic to assume that an adversary can only control a contiguous section of the network, i.e., not scattered, unconnected, repeaters, but instead a connected region of the network, based on the location of the attacker.

In this work, we consider the above realistic *partially corrupted* network scenario. We start with the simplest form of quantum repeater networks, a *quantum repeater chain*, which consists of two end users (Alice and Bob) and a sequence of quantum repeaters connecting the end users; see Figure 1. These

*AH: Industrial and Systems Engineering, Lehigh University, Bethlehem PA USA. Email: adh323@lehigh.edu
†WOK: School of Computing, University of Connecticut, Storrs CT USA. Email: walter.krawec@uconn.edu
‡BW: School of Computing, University of Connecticut, Storrs CT USA. Email: bing@uconn.edu

repeaters perform Bell swap operations to create end-to-end entanglement between two distant parties (we discuss the details of their operation later). Once this end-to-end entanglement is established, parties can run the E91 [16] QKD protocol (the entanglement based version of BB84 [17]) to establish a shared secret key. As we shall see, even in this simple topology of a repeater chain, analyzing security assuming partial corruption is a tremendous challenge. Once the repeater chain is analyzed, we extend our result to general networks where a region close to Alice and a region close to Bob are considered safe or trusted, and the rest of the network is adversarial. Specifically, we further extend our analysis by taking account of multiple paths that may exist between Alice and Bob in a general network setting.

Naturally, a partially corrupted network is an assumption; however, unlike classical key distribution which requires *computational* assumptions, this assumption on the attack model is grounded in physical limitations of the adversary. See Section 2.1 for a more formal description of our assumptions and security model. So far, security analyses of QKD networks assuming alternative attack models, such as this, have received very little attention (see Section 1.1 for a discussion on prior work). Yet analyzing such scenarios is important for a variety of reasons. For instance, we show that drastically improved key-rates and noise tolerances are possible (as we show in Section 5), potentially allowing for early QKD networks to perform at more optimistic levels. Also, by having rigorous proofs of security that can handle alternative, perhaps more realistic, attack models, users of early QKD network systems can have guidelines on how much of the network, and exactly which locations, need to be protected physically, in order to achieve a certain desired key-rate.

Analysis of partially corrupted repeater chain: In this work, we first analyze the performance and security of the E91 protocol operating on a repeater chain consisting of c repeaters, where the adversary is allowed to control a subset of contiguous repeaters and links. Alternatively, one may consider a repeater chain where some of the repeaters and links near Alice and Bob are trusted and better secured. We assume that users can upper-bound the number of adversarial repeaters or, alternatively, can lower-bound the number of honest repeaters in the network.

There are two motivating examples as to why this is a reasonable assumption. First, as discussed above, it is unrealistic that an adversary can control the entire, lengthy, repeater network and replace the entire network with adversarial devices, performing coherent attacks across a large distance. Second, it is likely that at least some repeaters near Alice and Bob will be placed in a secure and trusted location, which an adversary cannot easily gain access to (similar to how trusted nodes are considered physically secure - however securing a repeater is even easier, as it never stores the secret key). Thus, for any path from Alice to Bob, one can assume that the first few repeaters connected to Alice are secure while the last few repeaters connected to Bob are secure, leaving the middle repeaters as potentially under the control of the adversary; see Figure 1. Note that it may be that there are no secure repeaters for some paths, in which case, our key-rate result converges asymptotically to the standard BB84 expression.

Of course, even though there may be multiple honest repeaters and fiber links connecting them, these honest sub-networks are still noisy, and will still introduce detectable noise into the final shared entangled pairs. Thus, when Alice and Bob run a QKD protocol, the observed noise is a function both of Eve's attack and the natural noise in the trusted sub-network. Therefore, for a given observed noise level Q, one would expect that Eve's information is not nearly as high as it would be in the standard assumption case, where all noise is the result of an attack. However, formalizing this in the finite key setting, where a bound on the quantum min entropy [18] is required, is non-trivial, especially for multi-path networks. With min entropy, one must take into account that it is in some ways a "worst-case" entropy and, so, we must be careful when analyzing the system that Eve is not always able to "hide" in the natural noise. We must also deal with finite sampling imprecisions, and also the fact that Eve can interact non-trivially with the honest repeater network (even influencing routing decisions in larger networks). Finally, we must also take into account that the repeater network, including the adversary's portion of it, must send classical messages to users of the protocol, in order for them to apply a correcting Pauli gate. Taken together, these issues make finite key analyses a challenge.

Finite key analyses, however, are vital to understanding the potential performance of a quantum system. Asymptotic analyses are highly interesting, and useful, as theoretical upper-bounds; however finite key

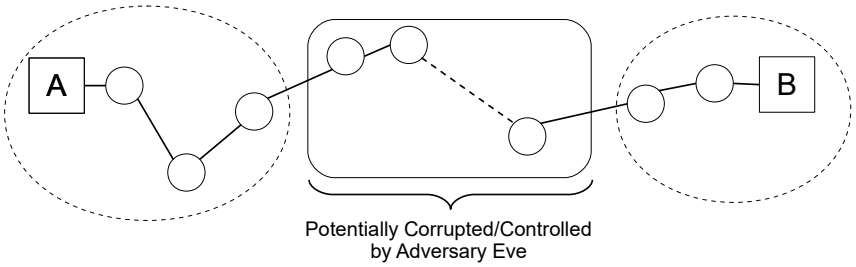

Figure 1: An example repeater chain where the repeaters (solid circles) and links near parties Alice and Bob, (those within the dashed circles), may be considered "safe" or trusted, while all other repeaters and links may, or may not, be adversarial. Note that even though the repeaters near Alice and Bob may be trustworthy, they are still noisy.

scenarios, where Alice and Bob only utilize the network for a finite amount of rounds, are important for understanding the potential performance in more realistic scenarios. Our work shows how to bound the quantum min entropy between Alice and the adversary Eve in this network scenario, thus providing us with a bound on the finite key-rate of the system under this attack model. We develop a novel proof technique for this scenario, taking advantage of a sampling-based framework introduced by Bouman and Fehr in [19], along with proof techniques used for sampling based entropic uncertainty relations [20, 21]. We restrict our attention to noisy but lossless channels as this already presents a large challenge; despite this, we suspect our proof techniques may be extended to deal with lossy channels also, potentially using decoy state methods [22–24]. However, we do not assume uniform noise in the network; some honest links may be noisier than others. We also do not make any assumptions on the adversary's attack within the corrupted sub-network; i.e., it can be any arbitrary general/coherent attack.

We make several contributions in this work. First, we show a quantum min entropy bound for the setting where natural and adversarial noise are mixed in a quantum repeater network. Such a bound allows us to derive key-rate expressions in the practical finite key setting. To prove our new bound, we develop several new techniques which may be broadly applicable outside of this application domain. At a high level, our new results claims that the quantum min entropy, denoted $H_\infty^\epsilon(A|E)$ is bounded by:

$$H_\infty^\epsilon(A|E) \geq n(1 - h(Q - Q_\mathcal{N} + \delta)), \tag{1}$$

where $h(x)$ is the binary Shannon entropy, n is the number of network rounds used (after sampling), Q is the observed X basis noise, $Q_\mathcal{N}$ is a function of the honest network noise (which we assume in this paper that Alice and Bob may at least lower-bound), and δ results from finite sampling imperfections. Our proof takes into account all finite sampling artifacts and imprecisions, allowing users to immediately evaluate key-rates and optimize over user parameters. Our full result is stated in Theorem 2 for the repeater chain scenario.

Analysis of partially corrupted multi-path networks: Following the analysis of repeater chains, we extend the analysis to general multi-path networks. Our full result for general network scenario is in Theorem 3. Similar to Equation 1, we show how the natural noise may, in a way, be deducted from the observed X basis noise. Now, however, we must be careful of multi-paths and routing issues that arise in large-scale networks. We extend our result and show how $Q_\mathcal{N}$ can be computed in the multi-path setting, assuming some repeaters and links near Alice and Bob are honest, but noisy.

For both single-path repeater chains and general multi-path networks, we use our expression to derive finite key-rate expressions, and also asymptotic key-rates. We evaluate our results in a variety of settings

showing that significantly improved key-rates are possible, compared to standard security models consisting of entirely adversarial networks. While that result is not surprising, showing it rigorously is a challenging, but important, problem which we solve in this work.

Finally, our proof method may be broadly applicable to other application domains within quantum cryptography. We build on the quantum sampling framework of Bouman and Fehr and introduce new methods to derive min entropy expressions for systems that are only partially under the control of the adversary.

1.1 Prior Work

We are not the first to consider physical assumptions in the security model of QKD. Much work has been done, for instance, in assuming Eve is bounded in her storage abilities, either in quantity of storage bits [25], or quality of storage memory [26].

We are also not the first to consider a security model based on the communication setup. For instance, several recent papers have considered alternative security models for satellite communication, placing reasonable assumptions on the adversary's capabilities given the channel conditions. In particular, these references take advantage of the fact that satellite communication requires line of sight and it is infeasible for an adversary to completely control the freespace channel between the satellite transmitter and the ground station. In [27], a new "bypass channel" model is introduced which models the practical assumption that an adversary can only capture a portion of the transmitted photons while others will bypass the adversary and arrive at the receiver un-attacked. Ref [28] took this further and argued that attacks against satellite QKD can be detected through classical means, and defined "photon key distribution" protocols to improve performance. Other references [29, 30] have considered security of QKD protocols, particularly freespace ones such as satellite communication, operating over wiretap channels [31]. These are all assumptions placed on the adversary, based on reasonable practical constraints on any attack against QKD. In our work we place what we consider reasonable assumptions on an adversary, based on the impracticality of attacking an entire large-scale network simultaneously. Similar to the work cited above, these assumptions allow for improved performance of the underlying system - though it is up to users of the system to decide if they are comfortable with the assumption. Indeed, users can always revert back to the standard security model (though, in that case, they can no longer take advantage of the improved performance).

Perhaps the closest work to ours is found in [32,33]. Both of these sources investigated the performance of QKD where some of the observed channel noise is assumed to be honest or natural noise (also called trusted noise in some references), while some is adversarial. Both references, however, only considered point-to-point BB84, not a quantum repeater network. Furthermore, [32] only considered collective attack scenarios and, thus, computed a bound on the von Neumann entropy (note that such an analysis could be promoted to general attacks, though the result is usually not as tight, *in the finite key setting*, as deriving a bound directly on the min entropy as we do in this paper). We do not assume the adversary is restricted to collective attacks, thus requiring us to derive a bound on the quantum min-entropy, a more challenging prospect. The second, ref. [33], considered a particular "state replacement" noise model, where the natural noise in the channel consisted of a state being replaced with a truly mixed state. This replacement is done for every single state sent, in an i.i.d. manner and the probability of state replacement is known and characterized. Our work considers repeater networks where some of the network is considered "honest" or safe, but suffers from characterizable noise, while the remainder of the network is considered adversarial. Our proof must take into account the action of the honest repeater network and the classical messages being passed, which was not a requirement in these previous works. We also are able to analyze arbitrary quantum networks beyond simple repeater chains, including multi-path networks.

Other references have considered various "trusted noise" scenarios in the discrete variable case. In [34], the six-state BB84 protocol was analyzed where the signal received by Bob is mixed with white noise (which can be added deliberately by the source, Alice, or naturally, such as by natural light interfering with a free-space satellite QKD link). However, only individual attacks were considered in the asymptotic setting; note that individual attacks are weaker than collective attacks and security against individual attacks does not necessarily imply security against arbitrary, general attacks. In [35], the authors investigated

the performance of BB84 with a particular form of added natural noise, namely collective-rotation noise. However, the security analysis was only against a particular intercept/resend attack strategy, where the adversary measures incoming signals in either the Z or X basis. This was followed up recently in [36] for the six-state BB84 protocol, but again, only for intercept resend attacks. In [37], the benefits of adding noise to an already faulty source were considered and shown to improve BB84. Finally, in [38], the effects of multiple but independent, adversaries on a single point-to-point BB84 link were considered. Only the von Neumann entropy was investigated there.

BB84 style protocols were not the only ones to be considered in the trusted-noise scenario. In [39, 40], the so-called Ping-Pong protocol (introduced in [41]) was analyzed assuming there was either trusted noise in the channel [39] or there was noise added by the source [40]. The Ping-Pong protocol relies on a two-way quantum communication channel, with qubits traveling from Alice, to Bob, then back to Alice. In both these works, only asymptotic analyses were considered and, thus, bounds on von Neumann entropy. Furthermore, no quantum repeaters were considered. Finally, larger scale networks were also considered in [9], though, there, the network consisted only of trusted nodes (not repeaters) and the security model assumed that trusted nodes were corrupted randomly; the goal of that reference was to route QKD paths randomly so that at least one path went through all honest trusted nodes. This is different from our work where we are forced to pass through both the honest, and the dishonest, nodes.

Moving beyond these discrete-variable protocols, several sources have investigated natural and trusted noise in the continuous variable QKD scenario [42, 42–45]; see also [46] for more of a survey in practical continuous variable QKD. However, none of these considered repeater chains (or larger networks) and, instead, assumed natural noise in the channel between source and receiver, trusted noise in the devices, or the intentional addition of noise at the source or receiver.

1.2 Preliminaries

We now introduce some notation and basic definitions we use throughout this work. We will then discuss some more important properties of quantum min entropy and some basic lemmas which will be used later.

Let $\mathcal{A}_d$ be a d-character alphabet which, without loss of generality, we simply assume to be $\mathcal{A}_d = \{0, 1, \cdots, d-1\}$. Given a word $q \in \mathcal{A}_d^N$ and a subset $t \subset \{1, \cdots, N\}$, we write q_t to be the substring of q indexed by subset t (i.e., $q_t = q_{t_1} \cdots q_{t_{|t|}}$) and we write q_{-t} to mean the substring of q indexed by the complement of t. When t is a singleton $t = \{i\}$ we usually just write q_i to mean the i-th character of q. We use $w(q)$ to be the relative Hamming weight of q, defined by:

$$w(q) = \frac{|\{i \ : \ q_i \neq 0\}|}{|q|}.$$

Finally, given two real values $x, y \in \mathbb{R}$ and $\delta > 0$, then we write:

$$x \sim_\delta y$$

if and only if $|x - y| \leq \delta$.

Let P be some probability distribution over $\mathcal{A}_d$, with $P(x)$ being the probability of some outcome $x \in \mathcal{A}_d$. Then, given a word $q \in \mathcal{A}_d^N$, for some $N > 1$, we often write $P(q)$ to mean $P(q) = P(q_1)P(q_2)\cdots P(q_N)$.

If a quantum state (density operator) ρ acts on some Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, we usually write ρ_{AB}; we then write ρ_A to mean the state resulting from the partial trace over B, namely $\rho_A = tr_B \rho_{AB}$. This can be extended to multiple subspaces. Given a pure state $|\psi\rangle$, we write $[\psi]$ to denote $[\psi] = |\psi\rangle\langle\psi|$. Given an orthonormal basis $\mathcal{B} = \{|x_0\rangle, \cdots, |x_{d-1}\rangle\}$ and a word $i \in \mathcal{A}_d^N$, we write $|i\rangle^{\mathcal{B}}$ to mean the word i in the $\mathcal{B}$ basis, namely $|i\rangle^{\mathcal{B}} = |x_{i_1}\rangle \otimes \cdots \otimes |x_{i_N}\rangle$. If no basis is specified, we assume the standard computational basis, namely $|i\rangle = |i_1\rangle \otimes \cdots \otimes |i_N\rangle$. Finally, given ρ and σ, acting on the same Hilbert space, we write $||\rho - \sigma||$ to be the trace distance of ρ and σ defined as: $||\rho - \sigma|| = tr\sqrt{(\rho - \sigma)^*(\rho - \sigma)}$, where A^* is the Hermitian adjoint of operator A.

Bell Basis Notation: We use $|\phi_x^y\rangle$, for $x, y \in \{0,1\}$, to denote the Bell basis states:

$$|\phi_x^y\rangle = \frac{1}{\sqrt{2}}(|0, x\rangle + (-1)^y |1, \bar{x}\rangle), \tag{2}$$

where $\bar{x} = 1 - x$. Later, we will work with multiple Bell states tensored together. For this, we define the *Bell alphabet set of size N* to be:

$$B^N = \{(x, y) \in \{0,1\}^N \times \{0,1\}^N\} \tag{3}$$

Given an element $i = (x, y) \in B^N$, we write $i^{\mathtt{bt}}$ to mean the "x" portion of the string i while we write $i^{\mathtt{ph}}$ to be the y portion. That is, the superscript "$\mathtt{ph}$" will denote the "phase" element of a Bell state, while "$\mathtt{bt}$" will represent the "bit" portion. All subset indexing rules discussed earlier apply to each individual portion of i (e.g., $i_t^{\mathtt{ph}}$ is the y portion of i, but only those indices indexed by t). We then write i_t to mean both x and y portions indexed by t, namely $i_t = (x_t, y_t) \in B^{|t|}$. We write $|\phi_i\rangle$ to mean $|\phi_{i^{\mathtt{bt}}}^{i^{\mathtt{ph}}}\rangle$ with:

$$|\phi_i\rangle = |\phi_{i^{\mathtt{bt}}}^{i^{\mathtt{ph}}}\rangle = |\phi_{x_1}^{y_1}\rangle \otimes |\phi_{x_2}^{y_2}\rangle \otimes \cdots \otimes |\phi_{x_N}^{y_N}\rangle\,. \tag{4}$$

(Recall x_j is the j'th bit of x and similarly for y.)

Finally, we also can add two Bell alphabet elements: given $i, j \in B^N$ with $i = (x, y)$ and $j = (z, u)$, then we write $i + j$ to mean the addition, coordinate-wise, modulo two, namely: $i + j = (x \oplus z, y \oplus u)$, where the strings $x \oplus z$ and $y \oplus u$ are added bit-wise modulo two.

1.3 Quantum Min Entropy

Let X be a random variable taking value i with probability p_i. Then we write $H(X)$ to mean the Shannon entropy of X defined to be $H(X) = -\sum_i p_i \log p_i$ where all logarithms in this paper are base two unless otherwise specified. If X has only two outcomes, then $H(X) = h(p) = -p \log p - (1-p)\log(1-p)$ where $h(p)$ is the binary entropy function. For technical reasons later, we define a function $\bar{h}(p)$ by $\bar{h}(p) = h(p)$ if $p < 1/2$ and $\bar{h}(p) = 1$ otherwise. Thus $\bar{h}(p) \leq \bar{h}(p')$ for every $0 \leq p \leq p' \leq 1$.

Given a quantum state ρ_{AE}, the *conditional quantum min entropy* is defined as [18]:

$$H_\infty(A|E)_\rho = \sup_{\sigma_E} \max\left\{\lambda \in \mathbb{R} \;:\; 2^{-\lambda} I_A \otimes \sigma_E - \rho_{AE} \geq 0\right\}, \tag{5}$$

where the supremum is over all density operators σ_E acting on $\mathcal{H}_E$ and where $A \geq 0$ means operator A is positive semi-definite. Let $\Gamma_\epsilon(\rho) = \{\tau_{AE} \;:\; ||\rho_{AE} - \tau_{AE}|| \leq \epsilon\}$, i.e., the set of all density operators ϵ-close to ρ_{AE} in trace distance. Then, the *smooth min entropy* is defined [18] to be:

$$H_\infty^\epsilon(A|E)_\rho = \sup_{\tau \in \Gamma_\epsilon(\rho)} H_\infty(A|E)_\tau. \tag{6}$$

Quantum min entropy is a vital resource in quantum cryptography as it directly relates to how many uniform random bits may be extracted from a quantum state. Formally, let ρ_{AE} be a *classical quantum* state (cq-state). That is, it may be written in the form $\rho_{AE} = \sum_{a \in \{0,1\}^N} P_A(a)[a]_A \otimes \rho_E^{(a)}$. Then, if one chooses a two-universal hash function at random, $f : \{0,1\}^N \to \{0,1\}^\ell$, disclosing the choice of function to Eve, and hashing the A register to $f(A)$, then it holds [18]:

$$\left|\left|\rho_{f(A),EF} - I/2^\ell \otimes \rho_{EF}\right|\right| \leq 2^{-\frac{1}{2}(H_\infty^\epsilon(A|E)_\rho - \ell)} + 2\epsilon. \tag{7}$$

Above, F is the system representing Alice's random choice of hash function f, while $f(A)$ is the ℓ-bit register resulting from hashing N-bit register A. Essentially, the above states that, so long as the min entropy in the state ρ_{AE} *before* privacy amplification is high enough, one can extract a random string, of size ℓ-bits, that is uniform random and also independent of Eve.

There are several important properties of min entropy that will be useful later. Given a state ρ_{ABC} that is classical in C, namely it can be written in the form $\rho_{ABC} = \sum_c p_c[c] \otimes \rho_{AB}^{(c)}$, then it holds that:

$$H_\infty(A|B)_\rho \geq H_\infty(A|BC)_\rho \geq \min_c H_\infty(A|B)_{\rho^{(c)}}. \tag{8}$$

In particular, the above says that for some mixed state $\rho_{AB} = \sum_c p_c \rho_{AB}^{(c)}$, or a state ρ_{ABC} that is classical in C, the min entropy of the entire state can be lower-bounded by the worst-case entropy over the possible sub-events c.

We conclude this section with two lemmas that will be useful later. The first one, below, allows us to bound the smooth min entropy in a particular state after a measurement operation is performed on part of it, if we know the min entropy of a state that is "close" to it in trace distance:

Lemma 1. (From [47]): Let $\epsilon > 0$, and let ρ and σ be quantum states acting on the same Hilbert space such that $\frac{1}{2}\,||\rho - \sigma|| \leq \epsilon$. Let $\mathcal{F}$ be some completely positive trace preserving (CPTP) map (i.e., some quantum operation, or operations) which, on input a quantum state τ, acts as follows:

$$\mathcal{F}(\tau) = \sum_x p(x|\tau)[x]_X \otimes \tau_{AE}^{(x)}. \tag{9}$$

Then, it holds that:

$$Pr\left(H_\infty^{4\epsilon+2\epsilon^{1/3}}(A|E)_{\rho^{(x)}} \geq H_\infty(A|E)_{\sigma^{(x)}}\right) \geq 1 - 2\epsilon^{1/3}, \tag{10}$$

where the probability is over the random outcome X in the states $\mathcal{F}(\rho)$ and $\mathcal{F}(\sigma)$.

The next lemma that we will need in our proof, allows us to bound the min entropy of a superposition state in the Bell basis, if a measurement is made on the first qubit of every Bell pair:

Lemma 2. (From [48], rewritten using our notation): Let $|\psi\rangle_{XE} = \sum_{i\in J} \alpha_i \left|\phi_{i^{\mathtt{ph}}i^{\mathtt{bt}}}^{i^{\mathtt{ph}}}\right\rangle_X \otimes |E_i\rangle_E$ where $J = \{i \in B^n \ : \ w(i^{\mathtt{ph}}) \leq Q\} \subset B^n$ (for $Q \in [0,1]$). Let ρ_{AE} be the state resulting from taking $|\psi\rangle$ and measuring the first particle of every Bell pair in register X in the computational basis (which results in register A) while the second particle of every Bell pair is traced out. This measurement results in post-measured state ρ_{AE}. Then, it holds that:

$$H_\infty(A|E)_\rho \geq n\left(1 - \bar{h}(Q)\right) \tag{11}$$

1.4 Quantum Sampling

To derive a lower-bound on the quantum min entropy, we will take advantage of a quantum sampling framework introduced by Bouman and Fehr in [19]. In this section, we review some of the main points of this framework, referring the reader to [19] for additional details. The main point of Bouman and Fehr's sampling framework is the ability to promote a classical sampling strategy to a quantum one in such a way that one can argue about the state of the post measured system after sampling a quantum state.

A *classical sampling strategy* for words of length N over some alphabet $\mathcal{A}_d$ is a triple (P_T, g, r) where P_T is a probability distribution over all subsets of $\{1, \cdots, N\}$; g is a *guess function*; and r is a *target function*. Here, $g, r : \mathcal{A}_d^* \to \mathbb{R}$. Typically $g \equiv r$ (which will certainly be the case in this work, where we set $g \equiv r \equiv w$, the Hamming weight function), though this is not required in general. Given a word $q \in \mathcal{A}_d^N$, the sampling strategy will: (1) choose a subset t according to distribution P_T; (2) observe q_t and evaluate $g(q_t)$ (or, will simply observe $g(q_t)$); finally, (3) output this value as a "guess" as to the value of $r(q_{-t})$. That is, the strategy uses $g(q_t)$ (the guess function evaluated on the observed portion of q) to guess at the value of some target function evaluated on the unobserved portion of q.

Let $\delta > 0$, then given a fixed subset t, we define the set of *ideal words* to be those words q where the guess, given q_t, is always δ-close to the target $r(q_{-t})$. Formally:

$$\mathcal{G}_t = \left\{q \in \mathcal{A}_d^N \ : \ g(q_t) \sim_\delta r(q_{-t})\right\}. \tag{12}$$

(Recall $x \sim_\delta y$ only if $|x - y| \leq \delta$.) From this, the *error probability* of the given sampling strategy is defined to be:

$$\epsilon^{cl} = \max_{q \in \mathcal{A}_d^N} Pr\left(q \notin \mathcal{G}_t\right), \tag{13}$$

where the probability, above, is over the choice of subset t chosen according to P_T. Thus, given any string $q \in \mathcal{A}_d^N$, the probability that the given classical sampling strategy fails to produce a δ-close guess of the target value on observing q_t is no higher than ϵ^{cl}.

While the above described sampling strategy applies to a classical word, it may be promoted, in a natural way, to a quantum sampling strategy. Given a quantum state $|\psi\rangle_{AE}$, where the A register lives in some d^N dimensional Hilbert space, the sampling strategy will choose a subset t according to P_T and then *measure* those qudits in A indexed by t in some fixed d-dimensional basis $\mathcal{B}$. This measurement produces a classical output $q_t \in \mathcal{A}_d^{|t|}$ and a quantum post-measured state $|\psi^{t,q_t}\rangle_{A'E}$, which depends on both the subset choice t and the actual observed value q_t. Note that the A' register of the post-measured state, once removing the measured qudits, lives in a $d^{N-|t|}$-dimensional Hilbert space. The question becomes: what can be said of $|\psi^{t,q_t}\rangle_{A'E}$?

Define the space of *ideal states* for subset t with respect to the fixed (but arbitrary) d-dimensional basis $\mathcal{B}$ as follows:

$$\text{span}\left(\mathcal{G}_t\right) \otimes \mathcal{H}_E = \text{span}\left\{|q\rangle^{\mathcal{B}} \ : \ q \in \mathcal{G}_t\right\} \otimes \mathcal{H}_E. \tag{14}$$

An *ideal state*, $|\upsilon^t\rangle$, is defined to be one which lives in this space. Note that, if a basis measurement in the $\mathcal{B}$ basis is made of $|\upsilon^t\rangle$ in subset t, producing outcome $x \in \mathcal{A}_d^{|t|}$, then it is guaranteed that the post-measured state can be written in the form:

$$|\upsilon_x^t\rangle = \sum_{i \in J_x} \alpha_i \, |i\rangle^{\mathcal{B}} \, |E_i\rangle, \tag{15}$$

where:

$$J_x = \left\{i \in \mathcal{A}_d^{N-|t|} \ : \ g(x) \sim_\delta r(i)\right\} \tag{16}$$

Notice that, if the state given is an ideal state with respect to subset t and if the sampling strategy actually chooses t to sample, then the post-measured state is well behaved. Of course, given an arbitrary state $|\psi\rangle_{AE}$, this is not guaranteed. However, Bouman and Fehr's main result, stated in Theorem 1 below, says that, roughly, $|\psi\rangle_{AE}$ should behave like an ideal state, on average over the subset choice.

Theorem 1. (From [19], though reworded here for our application): Let $\delta > 0$ and $|\psi\rangle_{AE}$ be an arbitrary quantum state where the A register consists of N qudits each of dimension d. Let $\mathcal{B}$ be an arbitrary d-dimensional orthonormal basis. Then, given a classical sampling strategy (P_T, g, r) with failure probability ϵ^{cl}, there exists a collection of ideal states $\{|\upsilon^t\rangle\}_t$, indexed over every subset t, such that $|\upsilon^t\rangle \in \text{span}\left(\mathcal{G}_t\right) \otimes \mathcal{H}_E$ (where $\text{span}\left(\mathcal{G}_t\right)$ is defined with respect to basis $\mathcal{B}$) and:

$$\frac{1}{2} \left\| \sum_t P_T(t)[t] \otimes [\psi] - \sum_t P_T(t)[t] \otimes \left[\upsilon^t\right] \right\| \leq \sqrt{\epsilon^{cl}}. \tag{17}$$

Proof. For a proof, see [19]; to see that our rewording of their main result follows from Bouman and Fehr's work, the reader is also referred to [20]. □

To conclude this section, we will introduce the classical sampling strategy we will use later which we denote here by Ψ_4. It operates on the four-dimensional alphabet B^N and is defined as follows: P_T will choose a random subset t of size $m \leq N/2$, uniformly at random from all subsets of $\{1, \cdots, N\}$ of size m. Then, the guess function and target functions are the Hamming weight of the phase component of the word $q \in B^N$. Namely $g(q_t) = w(q_t^{\mathtt{ph}})$ and $r(q_{-t}) = w(q_{-t}^{\mathtt{ph}})$.

To bound the error probability of this strategy, we will actually need to introduce an alternative strategy defined and analyzed in [19], for two character alphabets which we denote Ψ_{hw}. Namely, given a word $q \in \{0,1\}^N$, P_T will choose a uniform random subset of size $m \leq N/2$, observe the relative Hamming weight

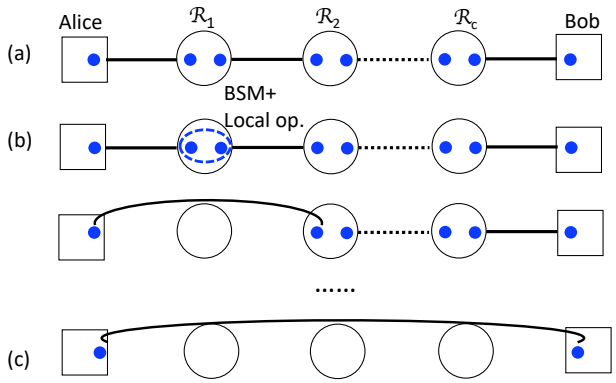

Figure 2: Illustration of the operation of the repeater chain. (a) Link-level distribution of Bell pairs. (b) Bell state measurement (BSM) and local Pauli gate operation at repeater $\mathcal{R}_1$ to create an entanglement between Alice and repeater $\mathcal{R}_2$. (c) End-to-end entanglement between Alice and Bob.

of q_t, namely $g(q_t) = w(q_t)$ and use this as a guess for the target value $r(q_{-t}) = w(q_{-t})$ (i.e., the target value is the Hamming weight of the unobserved portion). It was shown in [19] that the error probability for this strategy is upper-bounded by ϵ_{hw}^{cl} defined to be:

$$\epsilon_{hw}^{cl} \leq 2 \exp\left(-\delta^2 \frac{mN}{N+2}\right). \tag{18}$$

Using this, we can prove the following lemma, bounding the error probability of the sampling strategy Ψ_4:

Lemma 3. Given the sampling strategy Ψ_4 described above, for $m < N/2$, it holds that:

$$\epsilon^{cl} \leq 2 \exp\left(-\delta^2 \frac{mN}{N+2}\right). \tag{19}$$

Proof. Let $\mathcal{G}_t^{(4)}$ be the set of good words induced by sampling strategy Ψ_4 and let $\mathcal{G}_t^{hw}$ be the set of good words for sampling strategy Ψ_{hw}. Pick $q \in B^N$ and let $\widetilde{q} = q^{\mathtt{ph}}$. Then it is obvious that $q \notin \mathcal{G}_t^{(4)} \iff \widetilde{q} \notin \mathcal{G}_t^{hw}$. Thus, $Pr(q \notin \mathcal{G}_t^{(4)}) = Pr(\widetilde{q} \notin \mathcal{G}_t^{hw})$. Since q was arbitrary, and using Equation 18, the result follows. □

2 Network and Security Model

Since our security analysis for general networks directly builds on that of repeater chains, in this section and Section 3, we focus on models and security analysis of repeater chains. In Section 4, we extend our results to general networks. In Section 5, we present numerical results for both repeater chains and general networks.

We consider a repeater chain topology in this work consisting of c repeaters, denoted $\mathcal{R}_1, \cdots, \mathcal{R}_c$, chained in sequence connecting two users Alice and Bob as shown in Fig. 2(a). A repeater in our network is a basic device with two quantum storage ports, one connected to each neighbor. These devices are capable of creating Bell pairs and sending one particle to a neighbor while storing the other in quantum memory; receiving quantum states and storing them in the corresponding storage port; performing Bell measurements on the two qubits in storage; and finally, sending and receiving classical messages. We assume a noisy but lossless quantum communication model in this work, leaving the lossy case to future work.

If the entire repeater chain is honest, the network will perform the following operations on each round (refer also to Fig. 2):

1. First, repeater $\mathcal{R}_1$ will create two Bell pairs and send one particle to Alice and one particle to $\mathcal{R}_2$. The other two particles (one from each pair) are stored in the corresponding storage ports of $\mathcal{R}_1$.

2. Repeater $\mathcal{R}_2$ will then store the received particle from $\mathcal{R}_1$ while creating a new Bell pair and sending one particle to $\mathcal{R}_3$.

3. Repeaters continue to distribute link-level Bell pairs until all repeaters have two particles each while Alice and Bob have one particle each.

4. While the above is happening, repeater $\mathcal{R}_1$ will, as soon as possible, perform a Bell measurement on both particles in its memory, thus creating, ideally, an entangled pair between Alice and repeater $\mathcal{R}_2$; see Fig. 2(b). Furthermore, the outcome of this measurement (which we denote as simply "x, y" if Bell state $|\phi_x^y\rangle$ is observed) is sent to Alice.

5. Alice will, on receipt of the classical message from $\mathcal{R}_1$, apply an appropriate Pauli gate to her particle in the right storage port (received from $\mathcal{R}_1$ and which, should ideally now, be entangled with $\mathcal{R}_2$). This should, in the absence of noise, ensure that Alice and $\mathcal{R}_2$ have the Bell pair $|\phi_0^0\rangle$.

6. As soon as $\mathcal{R}_2$ has two particles in its storage port (namely, as soon as it sends a particle to $\mathcal{R}_3$), it will perform a Bell measurement itself, reporting the outcome to Alice, who applies the correct Pauli gate as before.

7. The above continues until, finally, the last repeater $\mathcal{R}_c$ performs a Bell measurement, reporting the outcome and Alice will perform the correct Pauli operation. In the noise free scenario, Alice and Bob should now share the state $|\phi_0^0\rangle$, independent of the repeaters; see Fig. 2(c).

The above describes the operations of the network, the goal of which is to establish end-to-end entanglement between Alice and Bob. Of course, the ultimate goal of the users is to establish a shared secret key. For this, Alice and Bob will run the entanglement based E91 protocol [49]. We actually consider the more commonly used, biased version, of this protocol, where the Z basis is used for key distillation and the X basis is used only for testing the error rate in the channel [50]. In detail, Alice and Bob will perform the following operations:

1. Alice and Bob use the repeater chain network for N rounds, each round operating as described above. Ideally, this should result in N shared Bell states held between the two users, each of the form $|\phi_0^0\rangle$.

2. Alice and Bob will choose a subset $t \subset \{1, 2, \cdots, N\}$ of size $|t| = m \leq N/2$ and measure those qubits indexed by t in the X basis. This results in outcomes q_A (for Alice) and q_B (for Bob). They broadcast their measurement results and compute the total X basis error string as $q = q_A \oplus q_B$. This should, ideally, be the all zero string if there is no error in the network.

3. The remaining $n = N - m$ qubits held by Alice and Bob are measured in the Z basis. This will be used as their raw-key.

4. Finally, Alice and Bob run an error correcting protocol on their raw keys and a privacy amplification protocol to output their final secret key.

2.1 Adversarial Model and Assumptions

Our goal in this paper is to analyze the scenario where an adversary controls a contiguous subset (sub-network) of the repeaters in the chain, while the remaining repeaters behave honestly. We assume that the corrupted repeaters are contiguously connected and that Eve also controls the fiber lines within this corrupted sub-network (which we call the adversary's *zone of control*). Any repeater outside the corrupted zone of control behaves honestly, and any fiber connection outside the corrupted region is not under adversarial control, but is noisy (i.e., these links are susceptible to natural noise); see Figure 1. This is in contrast to general QKD repeater chain scenarios, where it is assumed that the adversary completely controls all fiber and repeater nodes between Alice and Bob.

As mentioned in Section 1, there are two ways to justify the above assumption. First, in a large QKD repeater chain, it is unlikely that an adversary can gain physical access to all repeaters in the chain and all

fiber links connecting them. Instead, it is more realistic to assume an adversary can only realistically control a "small" subset of those repeaters and that the repeaters controlled by the adversary will be contiguous. An alternative way to justify the assumption is that, it is likely that some repeaters near end users can be placed in secure areas (e.g., in a trusted corporate or government building). Thus, one can justify trusting those repeaters, but not the remaining middle section of the network, connecting the two trusted regions. Note that one does not need to know exactly how many repeaters are adversarial - instead one needs an upper-bound on this; one may just as easily assume that a certain lower-bound of repeaters are trustworthy (but noisy) and then assume the remainder are adversarial.

Our goal is to show that improved key-rates are possible in this security model. We will do so by deriving a bound on the finite key-rate under the network and security model derived here. Before proceeding with our proof in the next section, however, we formally state our security model assumptions and, especially, the attack model afforded to the adversary. The assumptions we make in our security proof are as follows:

Assumption 1: The adversary can corrupt any number of contiguous repeaters in the chain. Furthermore, we assume that Eve can also control all fiber links between repeaters in her zone of control and the fiber links connecting to the nearest honest repeater. We will actually assume that Eve is able to completely replace her corrupted sub-network with her own perfect devices, and perform any quantum attack possible here (i.e., she need not operate within the bounds of a repeater chain and there will be no assumption of natural noise within the corrupted sub-network). Any repeater and fiber link outside her zone of control, however, cannot be attacked by Eve (though will be noisy).
Assumption 2: The adversary can read, but not tamper with, classical messages sent by repeaters outside their zone of control.
Assumption 3: Classical messages are sent after all Bell swaps are performed in the entire network for all rounds. This can be achieved by having the network wait until all N rounds have been performed, before sending the correction messages for the Bell swaps.
Assumption 4: Though Alice and Bob do not know exactly which sub-network is controlled by Eve, they are able to lower bound the amount of natural noise in the honest sub-network. In particular, they are able to lower-bound the so-called *noise parameter* of the network, defined in Definition 2.1.

Out of the above assumptions, Assumption 2 is perhaps the strongest. We actually don't think it's entirely necessary, however could not formally prove our result without it. We leave, as interesting future work, the removal of this assumption. We still feel that, even with the assumption in place, our results are interesting and, furthermore, this assumption is not unreasonable in a large-scale network setting. There may even be ways to enforce it through repeater messaging logs for instance.

2.2 Natural Noise Model

Outside of the adversary's zone of control are the left and right honest repeater sub-networks. Though honest, we will assume these are noisy in the sense that fiber noise, and internal repeater noise, may cause errors in the Bell states being distributed. For our security proof, we will assume the natural noise acts in an i.i.d. manner and leads to a mixed Bell diagonal state. We do not assume the noise is identical in every fiber link (e.g., some may be "noisier" than others).

As before, let c be the total number of repeaters in the chain. Formally, consider the link between honest repeaters $\mathcal{R}_i$ and $\mathcal{R}_{i+1}$ (if $i = 0$, then we are considering the link between Alice and the first repeater $\mathcal{R}_1$, while if $i = c$, then we are considering the link between the last repeater and Bob). Then, we assume that the two-qubit state distributed between $\mathcal{R}_i$ and $\mathcal{R}_{i+1}$ is actually of the form:

$$\rho = \sum_{x \in B} P^i(x)[\phi_x]. \tag{20}$$

where $P^i(x)$ is the probability that the final shared state will be $[\phi_x]$ for some $x \in B$. Note the superscript i indexes the repeater number, since we assume different links may have different noise levels.

After N rounds, we can write the state between honest repeaters i and $i+1$ as follows:

$$\rho = \sum_{x \in B^N} P^i(x)[\phi_x]. \tag{21}$$

Recall, from Section 1.2, we define $P^i(x_1, \cdots, x_N) = P^i(x_1)P^i(x_2)\cdots P^i(x_N)$.

Our security model assumes users know something about the natural noise in the network. To be more precise, we will assume that users can lower-bound the *noise parameter* of the honest sub-network, denoted p^*, which is defined below:

Definition 2.1. Let $P_L^i(\ell)$ and $P_R^i(r)$, for $\ell, r \in B$ be the probability that the i'th link in the left honest sub-network (respectively the right honest sub-network) produces a state $[\phi_\ell]$ (respectively $[\phi_r]$) on any particular single round of the network; see Equation 20. Let j be the number of honest left sub-network links, not including the link connecting the honest network to Eve, and let k be the number of honest right sub-network links, not including the link connecting to Eve (these may be zero if Eve directly connects to Alice or Bob). For any $x \in B$, define:

$$P_L(x) = \sum_{\substack{\ell^1, \cdots, \ell^j \in B \\ \ell^1 \oplus \cdots \oplus \ell^j = x}} P_L^1(\ell^1) \cdots P_L^j(\ell^j)$$

$$P_R(x) = \sum_{\substack{r^1, \cdots, r^k \in B \\ r^1 \oplus \cdots \oplus r^k = x}} P_R^1(r^1) \cdots P_R^k(r^k)$$

If $j = 0$, then we simply set $P_L((0,0)) = 1$, similarly for the right network if $k = 0$. Then, the *noise parameter of the honest sub-network* is defined to be:

$$p^* = \sum_{\substack{x,y \in B \\ x^{\text{ph}} \oplus y^{\text{ph}} = 1}} P_L(x) P_R(y). \tag{22}$$

Note that if $j = k = 0$ (i.e., there are no honest repeaters), then $p^* = 0$.

Essentially, the noise parameter characterizes the probability of there being a phase error in either the left or the right honest sub-networks, but not both. Of course, one can always find a trivial lower-bound for this by setting $p^* = 0$, however, in this case, our key-rate expression will converge towards the normal BB84 key-rate which is expected: if $p^* = 0$, users are assuming there is no natural noise and, so, all observed noise must be the effect of an adversary system. Once $p^* > 0$, our bound begins to improve over BB84 as we show, later, in our evaluation sections.

Finding a reasonable bound on p^* will depend on context. If we take the example of two "safe-zones" (as shown in Figure 1), then users can characterize the link-level noise between each safe-zone repeater and use this to easily determine a value for p^*. This would be a suitable lower-bound since it would assume every repeater outside the two safe-zones is adversarial (which may not actually be true and, so, in reality p^* could be higher, and thus the key-rate could be higher). Our security proof only requires a lower-bound on p^* and users may be pessimistic in their choice of setting for this parameter.

3 Security

We now derive a key-rate expression for the partially corrupted repeater chain as described in the previous section. To do this, we will first show how the system can be reduced to a three-party entanglement based protocol. From this, we will derive a lower-bound on the quantum min entropy $H_\infty^\epsilon(A|E)$ needed to determine a bound on the number of secret key bits as per Equation 7. Our bound will be a function of the observed X-basis noise in the final state shared between Alice and Bob, along with the natural noise in the honest sub-networks (or, rather, a lower-bound on the noise parameter p^* defined above).

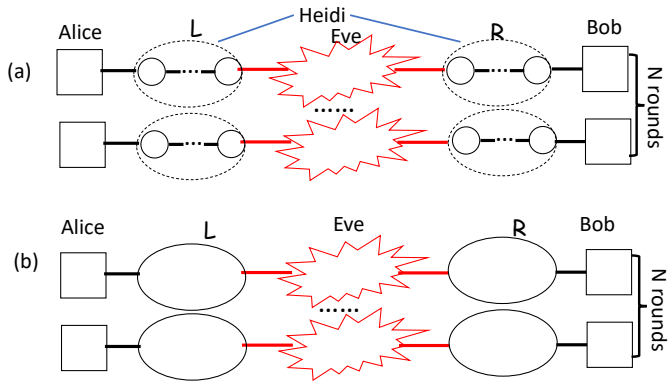

Figure 3: Illustration of the reduction: (a) the original protocol operating in N rounds, and (b) the new protocol after reduction operating in N rounds. Not shown here is that the original protocol (a) also requires classical communication from all repeaters under Eve's control, and each individual repeater while our reduction does not need this. Also not shown is that Eve may receive qubits from honest repeaters in the real protocol (a), however in our reduction (b), she always prepares states and sends them to honest repeaters.

3.1 Reduction to an Entanglement Based Protocol

To analyze the security of a partially corrupted repeater chain, we will first show that it suffices to analyze the key-rate in the following simplified scenario where there are three honest parties: Alice, Bob, and Heidi (four parties total, counting the adversary Eve). Here, Heidi will represent and simulate the honest sub-network in the actual network protocol (both the left and right sections); see Fig. 3(b). We describe this entanglement-based version first, and then later show that analyzing this entanglement based version will lead to results for the actual protocol (described in the previous section).

3.1.1 Entanglement Based Protocol

We now present the entanglement based version in its entirety. Then, in Section 3.1.2, we will show how this is representative of the actual network protocol discussed in Section 2.

In this entanglement-based protocol, Heidi first creates two independent states $|\mathcal{L}\rangle_L$ and $|\mathcal{R}\rangle_R$ of the form:

$$|\mathcal{L}\rangle = \sum_{\ell \in B^N} \sqrt{P_L(\ell)}\, |\phi_\ell\rangle_L\, |F_\ell\rangle \tag{23}$$

$$|\mathcal{R}\rangle = \sum_{r \in B^N} \sqrt{P_R(r)}\, |\phi_r\rangle_R\, |G_r\rangle\,, \tag{24}$$

where $\langle F_\ell | F_{\ell'}\rangle = \delta_{\ell,\ell'}$ and, similarly, $\langle G_r | G_{r'}\rangle = \delta_{r,r'}$ where $\delta_{x,y}$ is the Kronecker Delta function. Furthermore, we have $|G_r\rangle = |G_{r_1}\rangle \otimes \cdots \otimes |G_{r_N}\rangle$ with each $\langle G_{r_i} | G_{r'_i}\rangle = \delta_{r_i,r'_i}$ (and $|F_\ell\rangle$ may be written in a similar tensor form). Note that both states are pure states. The values of P_L and P_R will be determined from the actual honest network she is simulating which will be clear later (essentially, she will be simulating the network and so will set these to values based on the honest network noise, Equation 21). She keeps these states private to herself.

Next, Eve creates an arbitrary $2N$ qubit state, entangled with her private ancilla, denoted $|\widetilde{\psi}\rangle_{ME}$, independent of the Left and Right sub-network states that Heidi created. The M (middle, since Eve is in the middle of the chain) register consists of $2N$ qubits; she then sends the M register to Heidi, while keeping her ancilla private. After this, Heidi, who holds $6N$ qubits currently (the L, M, and R registers - note that each register holds $2N$ qubits), will perform a final network operation $\mathcal{N}$. This will simulate the honest network's final Bell swaps and classical messages being sent from the last honest repeaters (bordering Eve) to Alice.

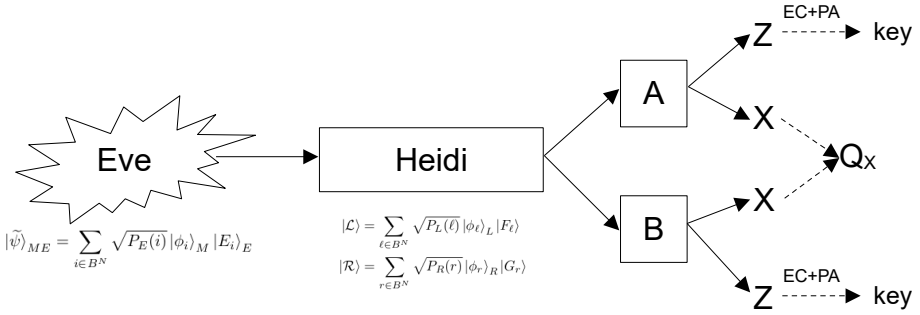

Figure 4: A high-level view of the entanglement-based protocol. First, Eve creates a state $|\widetilde{\psi}\rangle_{ME}$, and sends the M portion to Heidi. Heidi, simulating the honest portion of the network, creates Left and Right network states, then applies the network operator $\mathcal{N}$. She then sends the resulting qubits to Alice and Bob. Alice and Bob then measure some of the qubits in the X basis, used to compute Q_X, the parity of their X basis outcomes. The remaining qubits are measured in the Z basis which is used to produce their final secret key after Error Correction (EC) and Privacy Amplification (PA). We show that security of this entanglement based protocol will imply security of the actual repeater-chain protocol. Not shown in this figure is the classical communication sent from Heidi, and also from Alice and Bob.

This map acts on a $6N$ qubit state $|\phi_\ell, \phi_i, \phi_r\rangle$, for all $\ell, i, r \in B^N$, in the following manner:

$$\mathcal{N}^{\otimes N} |\phi_\ell, \phi_i, \phi_r\rangle = \frac{1}{2^{2N}} \sum_{z,u \in B^N} (-1)^{g(\ell,i,r;z,u)} |\text{“}z,u\text{”}\rangle_{cl} \otimes |\phi_{\ell+i+r}\rangle_{AB} , \tag{25}$$

for some function $g : B^{5N} \to \{0,1\}$ whose exact action, though easy to actually derive by simulating the action of the final left and right sub-network Bell swaps (which we do later), is not important to our current discussion. This map $\mathcal{N}$ will simulate the honest network's final operations of performing Bell swaps at the "border" repeaters (those nearest Eve) and sending the measurement outcomes. It will also simulate the final Pauli fix applied by Alice. Note that the input of g depends on $5N$ Bell states since this is a function of all N rounds and, for each round, there are five important Bell values: the two messages output by the map (output by the honest network or Heidi in this case), and the three input Bell states (from M, L, and R). Also, recall the additive notation for Bell states, defined in Section 1.2.

The above map is actually unitary, which is not obvious from the above definition since g's action is not defined; however, that it is an unitary, will be clear when we write out explicitly how the map operates in the next section. Essentially, it performs a SWAP followed by a delayed Bell basis measurement and recording the result in the "cl" register; it then performs the final Pauli correction which Alice would normally have done. We use quotes in the "cl" register as they will, later, represent the classical message sent from the last two repeaters to Alice.

Finally the A and B registers (which are N-qubits each) are sent to Alice and Bob respectively, while the "cl" register (the classical message register) is measured and the outcome broadcasted to all parties - this represents the final correction term that normally would have been broadcast (i.e., it represents the sum of all the honest messages that normally would have been broadcast, not the entire message transcript that would have been broadcast in the actual prepare and measure protocol). The G and F registers are simply discarded (i.e., traced out). Alice and Bob are then free to run the E91 protocol as normal, namely, they choose a random sample and measure in the X basis to test the fidelity of the state, while measuring the remaining systems in the Z basis to derive a secret key after error correction and privacy amplification. See Figure 4.

3.1.2 Reduction

We claim security of the above entanglement-based protocol will imply security of the actual partially corrupted repeater chain. To show this, we trace the execution of the actual network, and compare with the state that would have been produced in the entanglement based protocol above.

First, since messages are not sent until after all N rounds are complete and, furthermore, since Eve cannot tamper with these messages (see Assumptions 2 and 3 as defined in Section 2.1), Eve cannot adapt her attack based on the results of the honest network's Bell messages. On account of this, giving Eve the ability to prepare all $2N$ qubits simultaneously for those repeaters neighboring her can only give her a greater advantage than in the potentially more realistic case where (1) she would need to feed in qubits to the neighboring repeaters in smaller blocks and/or (2) she would receive qubits prepared by the honest network instead of being free to create and send her own. Thus, we analyze the case where Eve prepares all $2N$ qubits for the neighboring repeaters as this can only be to her advantage - any other scenario would give Eve fewer attack opportunities and, thus, more uncertainty in her system. We can thus assume that Eve prepares the state:

$$|\widetilde{\psi}\rangle_{ME} = \sum_{i \in B^N} \sqrt{P_E(i)}\, |\phi_i\rangle_M |E_i\rangle_E \,, \tag{26}$$

where each $|E_i\rangle$ is some arbitrary normalized, but not necessarily orthogonal, state in Eve's ancilla, and $P_E(i)$ is arbitrary such that $\sum_i P_E(i) = 1$ (we are not assuming an i.i.d. attack). Note that Eve is allowed, in the actual network scenario, to send a classical message transcript (consisting of $2N$-bits for every repeater under her control). However, this message can only cause Alice to apply an incorrect Pauli gate later when correcting the Bell state. Eve can simulate this, without sending a classical message, by applying a suitable Pauli gate herself to her state above, before sending the qubits to the corresponding neighboring honest repeaters. Thus, Eve's ability to send a classical message (the output of her adversarial repeater network), does not give her any additional power if we assume she is allowed to always prepare qubit states and send them to her neighbors and so we do not need to consider it further. We do, however, need to consider the classical messages sent by the honest repeaters as that message transcript may be affected by Eve's state above as we soon see.

Now, let's consider the action of the honest network. First, it attempts to establish link-level entanglement on all edges between honest repeaters (but not between honest repeaters and Eve's corrupted region as those links are under Eve's control as discussed) - see Figure 3. By Assumption 4, the noise in these links results in a mixed Bell state. Let j be the number of fiber links in the left honest network (not counting the fiber link leading to Eve which, we assume, is corrupted) and k be the number of fiber links in the right honest network. Let ρ_L^i (respectively ρ_R^i) be the state of the quantum system shared between nodes on link i on the left (respectively right) sub-network. By Assumption 4 and Equation 21, we can write these states as:

$$\rho_L^i = \sum_{\ell^i \in B^N} P_L^i(\ell^i) [\phi_{\ell^i}]_L \tag{27}$$

$$\rho_R^i = \sum_{r^i \in B^N} P_R^i(r^i) [\phi_{r^i}]_R \tag{28}$$

At this point, the joint state of the network is:

$$\rho_L^1 \otimes \cdots \rho_L^j \otimes \left[\widetilde{\psi}\right] \otimes \rho_R^1 \otimes \cdots \otimes \rho_R^k.$$

The honest network will now perform Bell operations. Note that the actual order of the Bell measurements performed by the network does not matter, since all Bell swaps at this point are performed by honest repeaters. In fact, the network might as well perform Bell swaps on the left and right honest networks while waiting for Eve's $2N$ qubits.

Let's look closer at the Bell swap operation performed by a single honest repeater. Assume that we have a chain: $X - Y - Z$, where $X - Y$ and $Y - Z$ share some quantum state of the form $|\phi_a\rangle$ and $|\phi_b\rangle$ for some

$a, b \in B$. Assume repeater Y is performing the Bell swap. Note that:

$$\begin{aligned}|\phi_a, \phi_b\rangle &= \frac{1}{2}\left(|0, a^{\mathtt{bt}}, 0, b^{\mathtt{bt}}\rangle + (-1)^{b^{\mathtt{ph}}}|0, a^{\mathtt{bt}}, 1, \bar{b}^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}}|1, \bar{a}^{\mathtt{bt}}, 0, b^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}}|1, \bar{a}^{\mathtt{bt}}, 1, \bar{b}^{\mathtt{bt}}\rangle\right) \\ &\cong \frac{1}{2}\left(|a^{\mathtt{bt}}, 0\rangle|0, b^{\mathtt{bt}}\rangle + (-1)^{b^{\mathtt{ph}}}|a^{\mathtt{bt}}, 1\rangle|0, \bar{b}^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}}|\bar{a}^{\mathtt{bt}}, 0\rangle|1, b^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}}|\bar{a}^{\mathtt{bt}}, 1\rangle|1, \bar{b}^{\mathtt{bt}}\rangle\right),\end{aligned}$$

where, above, we simply permuted the subspaces so that the two qubits owned by Y are on the left while the third qubit is the one held by X and the fourth (right-most) qubit is the one held by Z. Repeater Y is now going to perform a Bell measurement on the qubits it holds (the left-two qubits in the above, permuted, state).

If $a^{\mathtt{bt}} = 0$, the above state is found to be:

$$\begin{aligned}|\phi_a, \phi_b\rangle \cong &\frac{1}{2\sqrt{2}}|\phi_0^0\rangle \otimes \left(|0, b^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}}|1, \bar{b}^{\mathtt{bt}}\rangle\right) \\ &+\frac{1}{2\sqrt{2}}|\phi_0^1\rangle \otimes \left(|0, b^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}+1}|1, \bar{b}^{\mathtt{bt}}\rangle\right) \\ &+(-1)^{b^{\mathtt{ph}}}\frac{1}{2\sqrt{2}}|\phi_1^0\rangle \otimes \left(|0, \bar{b}^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}}|1, b^{\mathtt{bt}}\rangle\right) \\ &+(-1)^{b^{\mathtt{ph}}}\frac{1}{2\sqrt{2}}|\phi_1^1\rangle \otimes \left(|0, \bar{b}^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}+1}|1, b^{\mathtt{bt}}\rangle\right)\end{aligned}$$

Otherwise, if $a^{\mathtt{bt}} = 1$, then the state is:

$$\begin{aligned}|\phi_a, \phi_b\rangle \cong &(-1)^{b^{\mathtt{ph}}}\frac{1}{2\sqrt{2}}|\phi_0^0\rangle \otimes \left(|0, \bar{b}^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}}|1, b^{\mathtt{bt}}\rangle\right) \\ &+(-1)^{b^{\mathtt{ph}}+1}\frac{1}{2\sqrt{2}}|\phi_0^1\rangle \otimes \left(|0, \bar{b}^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}+1}|1, b^{\mathtt{bt}}\rangle\right) \\ &+\frac{1}{2\sqrt{2}}|\phi_1^0\rangle \otimes \left(|0, b^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}}|1, \bar{b}^{\mathtt{bt}}\rangle\right) \\ &+\frac{1}{2\sqrt{2}}|\phi_1^1\rangle \otimes \left(|0, b^{\mathtt{bt}}\rangle + (-1)^{a^{\mathtt{ph}}+b^{\mathtt{ph}}+1}|1, \bar{b}^{\mathtt{bt}}\rangle\right)\end{aligned}$$

Thus, for any $a^{\mathtt{bt}}$, we can write the joint state as:

$$|\phi_a, \phi_b\rangle_{XYZ} \cong \frac{1}{2}\sum_{x\in B}(-1)^{f(a,b,x)}|\phi_x\rangle_Y \otimes |\phi_{a+b+x}\rangle_{XZ}, \tag{29}$$

for some function $f : B^3 \to \{0, 1\}$ which can be determined from the above, though the exact mapping is not important at the moment. Essentially, the above is defining a map that applies a SWAP to the middle two qubits which will simulate a delayed measurement of the middle repeater Y (the left-most register will later be measured in the Bell basis, and the outcome reported).

The left two registers are then measured in the Bell basis leading to a classical outcome $x \in B$ which is saved in a classical register spanned by $|\text{“}x\text{”}\rangle$ for all $x \in B$. Note we use quotes, here, to distinguish the fact that this system is classical and will later be used as a message system. The final state, then, is:

$$|\phi_a, \phi_b\rangle \mapsto \frac{1}{4}\sum_{x\in B}[\text{“}x\text{”}] \otimes [\phi_{a+b+x}], \tag{30}$$

where, recall from Section 1.2, $|\phi_{a+b+x}\rangle = |\phi^{a^{\mathtt{ph}}+b^{\mathtt{ph}}+x^{\mathtt{ph}}}_{a^{\mathtt{bt}}+b^{\mathtt{bt}}+x^{\mathtt{bt}}}\rangle$ (where all arithmetic in the subscript and superscript is done bitwise modulo two of course).

Returning to the protocol, let's assume the left and right honest sub-networks perform their Bell swaps N times on each repeater, except for the repeaters neighboring Eve. On the left sub-network, the state becomes, after all $j-1$ repeaters perform the above Bell measurements on all N rounds:

$$\begin{aligned}\rho_L^1 \otimes \cdots \rho_L^j \mapsto & \frac{1}{4^{N(j-1)}} \sum_{x^1,\cdots,x^{j-1} \in B^N} \left[\text{“}x^1, \cdots, x^{j-1}\text{”}\right] \otimes \sum_{\ell^1,\cdots,\ell^j \in B^N} P_L^1(\ell^1) \cdots P_L^j(\ell^j) [\phi_{\ell^1+\cdots+\ell^j+x^1+\cdots+x^{j-1}}] \\ = & \frac{1}{4^{N(j-1)}} \sum_{x^1,\cdots,x^{j-1} \in B^N} \left[\text{“}x^1, \cdots, x^{j-1}\text{”}\right] \otimes \sum_{\ell \in B^N} P_L(\ell) [\phi_{\ell+x^1+\cdots+x^{j-1}}] := \rho_L, \end{aligned} \tag{31}$$

where:

$$P_L(\ell) = \sum_{\substack{\ell^1,\cdots,\ell^j \in B^N \\ \ell^1+\cdots+\ell^j=\ell}} P_L^1(\ell^1) \cdots P_L^j(\ell^j). \tag{32}$$

Similarly, the right honest sub-network's state can be written as:

$$\rho_R = \frac{1}{4^{N(k-1)}} \sum_{y^1,\cdots,y^{k-1} \in B^N} \left[\text{“}y^1, \cdots, y^{k-1}\text{”}\right] \otimes \sum_{r \in B^N} P_R(r) \left[\phi_{r+y^1+\cdots+y^{k-1}}\right], \tag{33}$$

with a similar definition for $P_R(r)$ based on each $P_R^i(\cdot)$. The overall network, then, is in the state:

$$\rho_L \otimes \left[\widetilde{\psi}\right] \otimes \rho_R.$$

The two last repeaters (one to the left of Eve and one to the right) now perform their final Bell swaps. To model this, let's consider a purification of the above network state:

$$\begin{aligned}\rho_L \otimes \left[\widetilde{\psi}\right] \otimes \rho_R = & tr_{GF} \left(\frac{1}{4^{N(j+k-2)}} \sum_{\vec{x},\vec{y}} |\text{“}\vec{x},\vec{y}\text{”}\rangle \langle \text{“}\vec{x},\vec{y}\text{”}| \right. \\ & \left. \otimes P \left(\sum_{\ell,i,r \in B^N} \sqrt{P_L(\ell) P_R(r) P_E(i)} \, |\phi_{\ell+\vec{x}}, \phi_i, \phi_{r+\vec{y}}\rangle \, |F_\ell, G_r, E_i\rangle \right) \right) \end{aligned} \tag{34}$$

where we use $P(|z\rangle) = |z\rangle \langle z|$. Above, the sum is over vectors of messages $\vec{x} = (x^1, \cdots, x^{j-1})$ and $\vec{y} = (y^1, \cdots, y^{k-1})$. Also, we purified the left and right network states independently by appending ancillas spanned by $|F_\ell\rangle$ (for the left honest network) and $|G_r\rangle$ for the right network. Of course $\langle F_\ell | F_{\ell'} \rangle = \delta_{\ell,\ell'}$ and similarly for $\langle G_r | G_{r'} \rangle$. Furthermore, we may write $|F_\ell\rangle = |F_{\ell_1}\rangle \, |F_{\ell_2}\rangle \cdots$ and, similarly, for $|G_r\rangle$ due to the i.i.d. structure of the natural noise..

Consider a particular $\vec{x}$ and $\vec{y}$. Using the SWAP and delayed measurement technique, used to derive Equation 29, twice, first for the left honest repeater which owns half the qubits of $\phi_{\ell+\vec{x}}$ and half the qubits from ϕ_i, then again for the right honest repeater which owns the other half of ϕ_i and half of $\phi_{r+\vec{y}}$, yields the state, for this particular outcome $\vec{x}$ and $\vec{y}$:

$$\begin{aligned} & \sum_{\ell,i,r \in B^N} \sqrt{P_L(\ell) P_R(r) P_E(i)} \, |\phi_{\ell+\vec{x}}, \phi_i, \phi_{r+\vec{y}}\rangle \, |F_\ell, G_r, E_i\rangle \\ \mapsto & \frac{1}{2^{2N}} \sum_{z,u \in B^N} |\phi_z, \phi_u\rangle_{ZU} \otimes \sum_{\ell,i,r \in B^N} (-1)^{g(\ell,i,r;z,u)} \sqrt{P_L(\ell) P_R(r) P_E(i)} \, |\phi_{\ell+i+r+\vec{x}+\vec{y}+z+u}\rangle \, |F_\ell, G_r, E_i\rangle \end{aligned} \tag{35}$$

where the function $g : B^{5N} \to \{0,1\}$ can be determined through the action of function f, though, again, its exact structure is not important to the analysis. Note this is the same function g as in Equation 25. The repeaters will then measure the ZU system resulting in:

$$\frac{1}{4^{2N}} \sum_{z,u \in B^N} [\text{“}z,u\text{”}] \otimes P \left(\sum_{\ell,i,r \in B^N} (-1)^{g(\ell,i,r;z,u)} \sqrt{P_L(\ell) P_R(r) P_E(i)} \, |\phi_{\ell+i+r+\vec{x}+\vec{y}+z+u}\rangle \, |F_\ell, G_r, E_i\rangle \right) \tag{36}$$

Note that, the phase induced by the g function will affect the probability of a repeater observing a particular message z, u - however, working out algebraically exactly this distribution turns out to be not necessary for the min-entropy analysis later; thus, while the g function is important, writing out its exact action is not, for the sake of our security proof.

From the above, the message transcript $\vec{x}$, $\vec{y}$, z, and u are sent to Alice who performs the correct Pauli operations. The ordering of these is not important - let's assume she fixes the $\vec{x}$ and $\vec{y}$ portions first, resulting in state:

$$\sigma = \frac{1}{4^{2N}} \sum_{z,u \in B^N} [\text{“}z, u\text{”}] \otimes P \left(\sum_{\ell,i,r \in B^N} (-1)^{g(\ell,i,r;z,u)} \sqrt{P_L(\ell) P_R(r) P_E(i)} \, |\phi_{\ell+i+r+z+u}\rangle \, |F_\ell, G_r, E_i\rangle \right) \tag{37}$$

Note that the above was all conditioning on a particular, but arbitrary, outcome $\vec{x}$ and $\vec{y}$. Considering, now, all possible $\vec{x}$ and $\vec{y}$ as a mixed state, before Alice applies operators to fix the z and u messages, the entire system, then, can be written as:

$$tr_{GF} \left(\frac{1}{4^{N(j+k-2)}} \sum_{\vec{x},\vec{y}} [\text{“}\vec{x}, \vec{y}\text{”}] \otimes \sigma \right) \tag{38}$$

Note that the $\vec{x}$ and $\vec{y}$ message systems are now independent of the state σ. Thus, regardless of the message outcome of the honest repeater network (the portion that did not interact with the adversary), the overall entropy computation will be identical. This is not too surprising considering the operation of an honest repeater with honest inputs, and the fact that the noise in the left and right honest sub-networks is well characterized. Therefore, there is no need to consider this part of the message transcript when analyzing the security of the protocol. Note that it *is* important to consider the message transcript from the honest repeaters that do interact with Eve (the Z and U messages), as these messages may not be independent of the final state, especially Eve's ancilla state.

Equation 38 represents the system before Alice applies the Pauli gates based on the z and u messages (from the repeaters bordering Eve). Since the $\vec{x}$ and $\vec{y}$ messages are independent, the only important element is the state σ. That is, if we know Eve's uncertainty in σ, we can derive the key-rate of the system. However, it is not difficult to see that the entanglement based protocol, described earlier, will produce exactly the same state σ. Indeed, by tracing the protocol's execution, where Eve produces the same attack state in the entanglement based version, and Heidi uses the honest network probabilities P_L and P_R for her created states, the resulting system in the entanglement based version will produce, exactly, σ. Note that the network operation map $\mathcal{N}^{\otimes N}$ (Equation 25) is defined to simulate, exactly, the Bell swap operations of the honest network, derived above (in particular, to simulate Equation 35). Thus, we can conclude that it suffices to analyze the entanglement based version - any entropy computation there will translate to an equivalent computation in the real network setting (Equation 38).

3.2 Key-Rate Bound

We now derive a key-rate bound for the partially corrupted repeater chain, or, rather, the entanglement based protocol discussed in the previous section. To do so, we first derive a bound on the conditional min entropy after running the E91 protocol in this network setup. Equation 7 can then be used to translate this to a key-rate bound. Our main result is stated, and proven, in the following theorem:

Theorem 2. Let $\epsilon > 0$ and let ρ_{ABE} be the state produced through the entanglement based protocol discussed above in Section 3.1.1, where the A and B registers consist of N qubits each. Let p^* be the noise parameter of the honest network (or a lower-bound on the noise parameter) as defined in Definition 2.1. Assume that Alice and Bob choose a random subset t of size $m \leq N/2$ and measure their corresponding qubits in the X basis resulting in outcome q_A and q_B (which are m-bit strings). Denote by Q_X to be

$Q_X = q_A \oplus q_B$ (this represents the X-basis error string). Alice and Bob then measure their remaining $n = N - m$ qubits in the Z basis resulting in state $\rho_{ABE}^{(t,q_A,q_B)}$. Then it holds that:

$$Pr\left[H_\infty^{8\epsilon+2(2\epsilon)^{1/3}}(A|E)_{\rho^{(t,q_A,q_B)}} \geq n\left(1-\bar{h}\left(\frac{w\left(Q_X\right)-p^*+\delta'}{1-2p^*}+\delta\right)\right)\right] \geq 1-2(2\epsilon)^{1/3}, \tag{39}$$

where the probability is over the subset choice t and the observed outcomes q_A, q_B, and where:

$$\delta = \sqrt{\frac{(N+2)\ln\frac{2}{\epsilon^2}}{mN}} \qquad \text{and} \qquad \delta' = \sqrt{\frac{\ln\frac{2}{\epsilon}}{2m}}. \tag{40}$$

Sketch of Proof: Our proof proceeds in three main steps. First, we will use Theorem 1 to construct ideal states and model the protocol under these states. Next, we will define a new "ideal-ideal" state where the previous ideal states are better behaved in a noisy network. Finally, we analyze the entropy of this ideal-ideal state, and then use Lemma 1 to promote the analysis to the real network state. Note that steps one and three follow from ideas used in the proof of sampling-based entropic uncertainty relations [20, 21].

In some more detail, consider the overall "real" state of the system: Eve creates $|\widetilde{\psi}\rangle_{ME}$, giving the $2N$ qubit M register to the honest network simulator Heidi, while Heidi also creates $|\mathcal{L}\rangle \otimes |\mathcal{R}\rangle$. The state Heidi creates is well known due to our assumptions on the honest network noise; the state that Eve creates is unknown. Heidi then operates on the L, M, and R registers using operator $\mathcal{N}^{\otimes N}$ (see Equation 25). This produces a quantum state ρ_{ABE}. Alice and Bob then choose a random sample t of size $m < N/2$, measure their qubits, indexed by this subset, in the X basis to test the fidelity of the channel, reporting the parity of their outcomes $Q_X \in \{0,1\}^m$ (which should be the all zero string - any "one" in this string indicates an X basis error). The difficulty is that, given a particular Q_X and subset t, we need to know how many errors Eve's arbitrary state induced.

Given Eve's state, we can construct ideal states using Theorem 1 which are, on average over the subset choice, ϵ-close to the real state $|\widetilde{\psi}\rangle$. Heidi will create the same $|\mathcal{L}\rangle$ and $|\mathcal{R}\rangle$ states as before and perform the same network operation, but now on the joint state consisting of an ideal state $|\nu^t\rangle$. Since quantum operations cannot increase trace distance, the resulting state is ϵ-close to the actual state we want to analyze.

Even now, however, analyzing the quantum min entropy of this state cannot easily be done. Instead, we must argue that, with high probability, the natural phase errors cannot always cancel out Eve's induced error. Since quantum min entropy is a "worst-case" entropy, analyzing the entropy of the above "ideal" state will result in a trivial, or at least very poor, bound. Instead, we must next define what we call "ideal-ideal" states - ideal states which have a further ideal property that the natural noise actually adds to Eve's overall induced error, instead of taking away. Furthermore, these ideal-ideal states have the additional property that, given the observed phase error and the known network noise (Definition 2.1), we can upper-bound Eve's phase error, even though we cannot directly observe it. These new states are 2ϵ-close to the actual real state and, so, arguments made about the min-entropy of these ideal-ideal states will translate, using Lemma 1, to the real state, giving us our result.

Proof. We now formally prove Theorem 2.

Step 1 - Ideal State Construction: Consider the entanglement based protocol discussed in Section 3.1.1. Let $|\widetilde{\psi}\rangle_{ME}$ be the state Eve creates, where the M register consists of $2N$-qubits and the E system is arbitrary. The M system is sent to Heidi. As discussed in the previous section, Heidi creates two purified states of the form:

$$|\mathcal{L}\rangle = \sum_{\ell \in B^N} \sqrt{P_L(\ell)}\, |\phi_{\ell^{\mathtt{bt}}}^{\ell^{\mathtt{ph}}}\rangle_L\, |F_\ell\rangle \tag{41}$$

and:

$$|\mathcal{R}\rangle = \sum_{r \in B^N} \sqrt{P_R(r)}\, |\phi_{r^{\mathtt{bt}}}^{r^{\mathtt{ph}}}\rangle_R\, |G_r\rangle\,, \tag{42}$$

where $P_L(\ell)$ and $P_R(r)$ depend on the honest left and right sub-networks that Heidi is simulating (see the previous section and, in particular, Equations 23 and 24). Note the $|F_\ell\rangle$ states are orthonormal and

separable (similar for the $|G_r\rangle$ states). The joint state, therefore, may be written (up to a permutation of the subspaces) as:

$$\sum_{\ell,r\in B^m} \sqrt{P_L(\ell)P_R(r)}\,|\phi^{\ell^{\mathtt{ph}}}_{\ell^{\mathtt{bt}}}\rangle\,|\phi^{r^{\mathtt{ph}}}_{r^{\mathtt{bt}}}\rangle\,|\widetilde{\psi}\rangle_{ME}\,|F_\ell\rangle\,|G_r\rangle \tag{43}$$

From the above state, Heidi will perform the network operation $\mathcal{N}^{\otimes N}$ (see Equation 25), which will simulate the honest sub-networks' Bell swaps, message transmissions, and Alice's final Pauli correction; Heidi then sends N qubits to Alice, N qubits to Bob, and broadcasts the final correction term (a $2N$ bit message). Alice and Bob will then run the E91 protocol on the resulting state. Namely, they will choose a random subset t of size m, measure their qubits indexed by this subset in the X basis, compute and report the parity of the outcomes Q_X (which, ideally, should be the zero string), and then measure the remaining qubits in the Z basis. These last measurements form the raw key which is subsequently processed further using error correction and privacy amplification. Call this final state ρ^t_{ABE} (which is a mixed state over all possible Q_X observations).

Instead of analyzing the actual state of the system above, we will instead apply Theorem 1 and analyze ideal states where sampling is well-behaved. We apply the theorem not to the entire state, Equation 43, but instead to the state Eve prepares $|\widetilde{\psi}\rangle_{ME}$. We use the sampling strategy Ψ_4, analyzed in Lemma 3, with respect to the Bell basis. From this, we have ideal states $\{|\upsilon^t\rangle_{ME}\}_t$, indexed by subsets t, such that:

$$\frac{1}{2}\left|\left|\sum_t P_T(t)[t]\otimes\left(\left[\widetilde{\psi}\right]_{ME}-\left[\upsilon^t\right]_{ME}\right)\right|\right| \leq \sqrt{\epsilon^{cl}} = \epsilon, \tag{44}$$

where the last equality follows from Lemma 3 and our choice of δ. Above, each $|\upsilon^t\rangle_{ME} \in \text{span}\,(\mathcal{G}_t)\otimes\mathcal{H}_E$, with:

$$\mathcal{G}_t = \left\{i\in B^N \;:\; w(i^{\mathtt{ph}}_t)\sim_\delta w(i^{\mathtt{ph}}_{-t})\right\} \tag{45}$$

Note that we are applying Theorem 1 just to the state Eve creates and not to the entire joint state. We now compute the min entropy in this ideal case and will later promote this analysis to the real case (where Eve's states are not ideal).

Consider a particular subset t and ideal state $|\upsilon^t\rangle$. It is clear that we may write this state in the following form (up to a permutation on individual qubit subspaces):

$$|\upsilon^t\rangle \cong \sum_{i_t\in B^m}\sqrt{P_E(i_t)}\,|\phi_{i_t}\rangle\otimes\sum_{i_{-t}\in J_{i_t}}\beta_{i_{-t}|i_t}\,|\phi_{i_{-t}}\rangle\,|E_{i_{-t}|i_t}\rangle\,. \tag{46}$$

where $P_E(i_t)$ is a value determined by Eve, which Alice and Bob cannot directly observe, and where $J_x = \{y\in B^n \;:\; w(y^{\mathtt{ph}})\sim_\delta w(x^{\mathtt{ph}})\}$.

Tensoring this with the honest sub-network states (which we do not apply Theorem 1 to, but instead analyze directly) yields the following state (up to a permutation of subspaces):

$$\begin{aligned}
&\sum_{\ell_t,r_t,i_t\in B^m}\sqrt{P_L(\ell_t)P_R(r_t)P_E(i_T)}\,|\phi_{\ell_t},\phi_{i_t},\phi_{r_t}\rangle\,|F_{\ell_t},G_{r_t}\rangle\\
&\underbrace{\otimes\sum_{\ell_{-t},r_{-t}\in B^n}\sum_{i_{-t}\in J_{i_t}}\sqrt{P_L(\ell_t)P_R(r_t)}\beta_{i_{-t}|i_t}\,|\phi_{\ell_{-t}},\phi_{i_{-t}},\phi_{r_{-t}}\rangle\,|E_{i_{-t}|i_t}\rangle\,|F_{\ell_{-t}},G_{r_{-t}}\rangle}_{\mu(\ell_t,r_t,i_t)}
\end{aligned}$$

$$= \sum_{\ell_t,r_t,i_t\in B^m}\sqrt{P_L(\ell_t)P_R(r_t)P_E(i_T)}\,|\phi_{\ell_t},\phi_{i_t},\phi_{r_t}\rangle\,|F_{\ell_t},G_{r_t}\rangle\otimes|\mu(\ell_t,r_t,i_t)\rangle\,. \tag{47}$$

Note we are only permuting the subspaces for clarity in presentation and to make the algebra simpler; in practice, the parties do not need to do this, and it does not affect the final min entropy bound if users do or do not perform this permutation of subspaces.

Now, the final network operation is performed $\mathcal{N}^{\otimes N}$ (Equation 25) on the above state (Equation 47). However, it is equivalent to analyze the case where the network operates on the subset t first, Alice and Bob measure in the X basis in the t subset only, and then the network operates on the complement $-t$ while Alice and Bob then measure, in the Z basis, the complement qubits $-t$.

After the network operation on t, the state becomes (again, writing the state after permuting subspaces for clarity):

$$\frac{1}{2^{2m}} \sum_{\ell_t, r_t, i_t \in B^m} \sqrt{P_L(\ell_t) P_R(r_t) P_E(i_t)} \left| F_{\ell_t}, G_{r_t} \right\rangle \\ \otimes \sum_{z,u \in B^m} (-1)^{g(\ell_t, i_t, r_t; z, u)} \left| \text{“}z, u\text{”} \right\rangle_{cl} \left| \phi_{\ell_t + i_t + r_t} \right\rangle_{AB} \otimes \left| \mu(\ell_t, r_t, i_t) \right\rangle . \tag{48}$$

(Recall, again, the additive notation for Bell states defined in Section 1.2.)

Now, an X basis measurement is made by Alice and Bob on those qubits indexed by t and the parity is reported (in practice, Alice and Bob broadcast their measurement results and compute the parity, however, ultimately, the parity is the important information). Let X_0 and X_1 be two POVM elements where $X_0 = [+,+]_{AB} + [-,-]_{AB}$ and $X_1 = [+,-]_{AB} + [-,+]_{AB}$. That is, X_0 indicates a parity of zero in Alice and Bob's measurements, i.e., Alice and Bob receive the same measurement outcome, while X_1 indicates an error in Alice and Bob's X basis measurement (i.e., they get opposite measurement outcomes in that basis). The following is easy to verify:

$$X_j \left| \phi_x^y \right\rangle = \begin{cases} \left| \phi_x^y \right\rangle & \text{if } y = j \\ 0 & \text{otherwise} \end{cases}$$

Finally, let $\widetilde{X}$ be the CPTP map which measures Alice's and Bob's qubits indexed by t, records the parity result in a separate register (which we will call the P register), and finally traces out the post measured quantum state. Applying this map $\widetilde{X}$ to the ideal state above (Equation 48), and also tracing out the G and F systems (or, rather, the t portion of the G and F systems), yields:

$$\begin{aligned} \sigma^t =& \frac{1}{4^{2m}} \sum_{z,u \in B^m} \left[\text{“}z, u\text{”} \right]_{cl} \otimes \left(\sum_{\ell, r, i \in B^m} P_L(\ell) P_R(r) P_E(i) \left[l^{\mathtt{ph}} \oplus r^{\mathtt{ph}} \oplus i^{\mathtt{ph}} \right]_P [\mu(\ell, r, t)] \right) \\ =& \frac{1}{4^{2m}} \sum_{z,u \in B^m} \left[\text{“}z, u\text{”} \right]_{cl} \otimes \left(\sum_{i \in B^m} P_E(i) \left[\sum_{\ell, r \in B^m} P_L(\ell) P_R(r) \left[l^{\mathtt{ph}} \oplus r^{\mathtt{ph}} \oplus i^{\mathtt{ph}} \right]_P [\mu(\ell, r, t)] \right] \right) \end{aligned} \tag{49}$$

Note that, above, we have removed the t subscript in the notation for clarity, since the context is clear. Also, observe that the above state is a mixture of states which are not necessarily normalized; that is, the probability of observing any particular z or u is not necessarily uniform due to the influence of the $P_E(i)$ term.

The above is the ideal-state using states constructed from Theorem 1. The real state ρ_{ABE}^t can be found similarly to the above, just substituting in an alternative probability distribution for Eve along with removing the constraint of J_{i_t} in the post measured state $|\mu(\ell, r, t)\rangle$. However, Equation 44, along with the fact that quantum operations cannot increase trace distance, ensures that the real state ρ_{ABE}^t and the above ideal state σ_{ABE}^t, are ϵ-close in trace distance (averaged over all subset choices t).

Step 2 - Defining “Ideal-Ideal” States: Analyzing the entropy in the state σ^t, defined above, despite being composed of ideal states according to Theorem 1, is still challenging. Instead, we will define a new “ideal-ideal” state, τ^t, which is ϵ close in trace distance to σ^t (and therefore 2ϵ close to the original real state ρ).

For any fixed $i \in B^m$, let's consider the expected value of $w(\ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} \oplus i^{\mathtt{ph}})$. Note that the ℓ and r strings are chosen independently of i since they are created from the honest but noisy sub-networks (or, rather,

Heidi in our case, who is simulating the honest sub-networks). Let Y be the random variable taking the value $y = \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} \in \{0,1\}^m$ with probability:

$$P_Y(y) = \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} = y}} P_L(\ell) P_R(r).$$

We compute the expected value of $w(Y \oplus i^{\mathtt{ph}})$ for a given $i \in B^m$. Recall from Definition 2.1, the equation for p^* which, we assume, is known (or lower-bounded) by Alice and Bob.

Let $x = w(i^{\mathtt{ph}})$. We divide $i^{\mathtt{ph}}$ into two substrings: Even (all zeros) and Odd (all ones). Since Y is independent of i, one will expect $m \cdot x \cdot p^*$ ones to appear in the odd substring of $i^{\mathtt{ph}}$ while $m(1-x)p^*$ ones to appear in the even substring. Note any one appearing in the odd substring of $i^{\mathtt{ph}}$ will cause $Y \oplus i^{\mathtt{ph}}$ to be zero (i.e., will decrease the number of ones in $Y \oplus i^{\mathtt{ph}}$) while any one in the even substring will cause $Y \oplus i^{\mathtt{ph}}$ to be one (i.e., will increase the number of ones in $Y \oplus i^{\mathtt{ph}}$). Thus, the expected number of ones in $Y \oplus i^{\mathtt{ph}}$ for fixed $i \in B^m$ is easily found to be:

$$\mu_i = \mathbb{E}(w(Y \oplus i^{\mathtt{ph}}) \mid i) = \underbrace{(x - xp^*)}_{\text{from odd substring}} + \underbrace{(1-x)p^*}_{\text{from even substring}} = x(1-p^*) + (1-x)p^*$$

$$= w(i^{\mathtt{ph}})(1-p^*) + (1 - w(i^{\mathtt{ph}}))p^*. \tag{50}$$

Now, by Hoeffding's inequality, and our choice of δ' from Equation 40, it holds that:

$$Pr\left(|w(Y \oplus i^{\mathtt{ph}}) - \mu_i| \leq \delta'\right) \geq 1 - 2\exp(-2(\delta')^2 m) = 1 - \epsilon, \tag{51}$$

where the probability is over the outcome of $Y = \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}}$.

For any $i \in B^m$, define the set G_i to be:

$$G_i = \{y \in \{0,1\}^m \ : \ |w(y \oplus i^{\mathtt{ph}}) - \mu_i| \leq \delta'\}. \tag{52}$$

From this, we may write σ^t as follows:

$$\sigma^t = \frac{1}{4^{2m}} \sum_{z,u} [\text{“}z,u\text{”}]_{cl} \otimes \left(\sum_{i \in B^m} P_E(i) \otimes \sum_{y \in \{0,1\}^m} P_Y(y) \left[y \oplus i^{\mathtt{ph}}\right]_P \otimes \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} = y}} P_{LR}(\ell, r|y)[\mu(\ell,i,r)] \right)$$

$$= \frac{1}{4^{2m}} \sum_{z,u} [\text{“}z,u\text{”}] \sum_{i \in B^m} P_E(i) \otimes \left(\sum_{y \in G_i} P_Y(y) \left[y \oplus i^{\mathtt{ph}}\right]_P \otimes \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} = y}} P_{LR}(\ell, r|y)[\mu(\ell,i,r)] \right.$$

$$\left. + \sum_{y \notin G_i} P_Y(y) \left[y \oplus i^{\mathtt{ph}}\right]_P \otimes \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} = y}} P_{LR}(\ell, r|y)[\mu(\ell,i,r)] \right) \tag{53}$$

where we define:

$$P_{LR}(\ell, r|y) = \frac{P_L(\ell) P_R(r)}{P_Y(y)}. \tag{54}$$

Now, consider the state τ^t which consists only of “good” strings y:

$$\tau^t = \frac{1}{4^{2m}} \sum_{z,u} [\text{“}z,u\text{”}]_{cl} \sum_{i \in B^m} P_E(i) \otimes \left(\frac{1}{N_i} \sum_{y \in G_i} P_Y(y) \left[y \oplus i^{\mathtt{ph}}\right]_P \otimes \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} + r^{\mathtt{ph}} = y}} P_{LR}(\ell, r|y)[\mu(\ell,i,r)] \right), \tag{55}$$

where, from Equation 51, we have:

$$N_i = \sum_{y \in G_i} P_Y(y) \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} = y}} P_{LR}(\ell, r|y) \geq 1 - \epsilon. \tag{56}$$

(For the above, note that $\sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} \oplus r^{\mathtt{ph}} = y}} P_{LR}(\ell, r|y) = 1.$)

Now, it is not difficult to show, using basic properties of trace distance and the triangle inequality, that the trace distance between τ^t and σ^t is upper bounded by ϵ. Indeed:

$$\begin{aligned}
\frac{1}{2}\left|\left|\sigma^t - \tau^t\right|\right| \leq \frac{1}{2} \sum_{z,u} \frac{1}{4^{2m}} \sum_i P_E(i) \Bigg|\Bigg| & \left(1 - \frac{1}{N_i}\right) \sum_{y \in G_i} P_Y(y) \left[y + i^{\mathtt{ph}}\right]_P \otimes \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} + r^{\mathtt{ph}} = y}} P_{LR}(\ell, r|y)[\mu(\ell, i, r)] \\
& + \sum_{y \notin G_i} P_Y(y) \left[y + i^{\mathtt{ph}}\right]_P \otimes \sum_{\substack{\ell,r \in B^m \\ \ell^{\mathtt{ph}} + r^{\mathtt{ph}} \equiv y}} P_{LR}(\ell, r|y)[\mu(\ell, i, r)] \Bigg|\Bigg| \\
\leq \frac{1}{2} \sum_{z,u} \frac{1}{4^{2m}} & \left(\sum_i P_E(i) \left(\frac{1}{N_i} - 1 \right) N_i + (1 - N_i) \right) \leq \epsilon
\end{aligned}$$

Note that the above holds for any subset t. Since we have that $\frac{1}{2}\left|\left|\sigma^t - \tau^t\right|\right| \leq \epsilon$ for every t, it follows from Equation 44 and the fact that CPTP maps cannot increase trace distance, that $\frac{1}{2}\left|\left|\sum_t P_T(t)[t](\rho^t - \tau^t)\right|\right| \leq 2\epsilon$. Thus, we can actually analyze the entropy in τ^t and then use Lemma 1 to promote the analysis to the real state.

Step 3 - Bounding the Min Entropy: Rewriting τ^t, Equation 55, we find:

$$\tau^t = \sum_{Q_X \in \{0,1\}^m} [Q_X]_P \otimes \sum_{i,y \in G^{(Q_X)}} \frac{P_E(i) P_Y(y)}{N_i} \otimes \sum_{z,u} \frac{1}{4^{2m}} [\text{“}z, u\text{”}] \otimes \sum_{\ell,r} P_{LR}(\ell, r|y)[\mu(\ell, i, r)], \tag{57}$$

where:

$$\begin{aligned}
G^{(Q_X)} &= \left\{ i \in B^m, y \in \{0,1\}^m \ : \ y \oplus i^{\mathtt{ph}} = Q_X \text{ and } y \in G_i \right\} \\
&= \left\{ (i, Q_X \oplus i^{\mathtt{ph}}) \ : \ Q_X \oplus i^{\mathtt{ph}} \in G_i \right\} \\
&\cong \left\{ i \in B^m \ : \ |w(Q_X) - \mu_i| \leq \delta' \right\} \qquad (58) \\
&= \left\{ i \in B^m \ : \ \left| w(Q_X) - (w(i^{\mathtt{ph}})(1 - p^*) + (1 - w(i^{\mathtt{ph}}))p^*) \right| \leq \delta' \right\} \\
&= \left\{ i \in B^m \ : \ \left| w(i^{\mathtt{ph}}) - \frac{w(Q_X) - p^*}{1 - 2p^*} \right| \leq \frac{\delta'}{1 - 2p^*} \right\} = \widetilde{G}^{(Q_X)}. \qquad (59)
\end{aligned}$$

With this, we can continue to manipulate the expression for τ^t as follows:

$$\tau^t = \sum_{Q_X \in \{0,1\}^m} [Q_X]_P \otimes \sum_{i \in \widetilde{G}^{(Q_X)}} \frac{P_E(i) P_Y(Q_X \oplus i^{\mathtt{ph}})}{N_i} \otimes \sum_{z,u} \frac{1}{4^{2m}} [\text{“}z, u\text{”}] \otimes \sum_{\ell,r} P_{LR}(\ell, r|Q_X \oplus i^{\mathtt{ph}})[\mu(\ell, i, r)], \tag{60}$$

At this point, Alice and Bob measure the P register to observe an actual parity string Q_X representing the observed X basis noise. The state then collapses to $\tau^{(t,Q_X)}$ which may be written as (tracing out the P

register which is simply $[Q_X]_P$ after the measurement):

$$\tau^{(t,Q_X)} = \frac{1}{M_{Q_X}} \sum_{i \in \widetilde{G}^{(Q_X)}} \frac{P_E(i) P_Y(Q_X \oplus i^{\mathtt{ph}})}{N_i} \otimes \sum_{z,u} \frac{1}{4^{2m}} [\text{“}z,u\text{”}] \overbrace{\sum_{\ell,r} P(\ell,r|Q_X \oplus i^{\mathtt{ph}}) [\mu(\ell,i,r)]}^{\tau^{(t,Q_X,z,u,i)}}$$
$$= \sum_{i \in \widetilde{G}^{(Q_X)}} \widetilde{P}_E(i) \sum_{z,u} \frac{1}{4^{2m}} [\text{“}z,u\text{”}] \otimes \tau^{(t,Q_X,z,u,i)}. \tag{61}$$

where, above M_{Q_X} is a normalization term, and we define $\widetilde{P}_E(i) = P_E(i) P_Y(Q_X \oplus i^{\mathtt{ph}})/(N_i M_{Q_X})$. Note that each $\tau^{(t,Q_X,z,u,i)}$ is normalized.

At this point, the network operation $\mathcal{N}$ completes on the remaining unmeasured subset $-t$ (those qubits in the $\tau^{(t,Q_X,z,u,i)}$ system) and Alice and Bob measure their remaining systems in the Z basis. Given a particular observed Q_X, we need to bound $H_\infty(A|E)_{\tau^{(t,Q_X)}}$, where the A register is taken to mean Alice's Z basis outcome after the final network operation is performed.

Recalling the definition of $|\mu(\ell,i,r)\rangle$ (see Equation 47) we can write the state of $\tau^{(t,Q_X,z,u,i)}$, after the final network operation is performed on the remaining systems, as:

$$\tau^{(t,Q_X,z,u,i)} = \sum_{\ell,r \in B^m} P_{LR}(\ell,r|Q_X \oplus i^{\mathtt{ph}})$$
$$\times P \left(\sum_{\ell_{-t},r_{-t} \in B^n} \sqrt{P_L(\ell_{-t}) P_R(r_{-t})} \, |F_{\ell_{-t}}, G_{r_{-t}}\rangle \, \frac{1}{2^{2n}} \sum_{z_{-t},u_{-t} \in B^n} |\text{“}z_{-t},u_{-t}\text{”}\rangle_{cl} \right.$$
$$\left. \otimes \sum_{i_{-t} \in J_i} (-1)^{g(\ell_{-t},i_{-t},r_{-t};z_{-t},u_{-t})} \, |\phi_{\ell_{-t}+i_{-t}+r_{-t}}\rangle \, |E_{i_{-t}|i_t}\rangle \right) \tag{62}$$

Then, tracing out the remaining G and F registers while measuring the cl register, yields the state:

$$\tau^{(t,Q_X,z,u,i)} = \sum_{z_{-t},u_{-t}} \sum_{\ell_{-t},r_{-t} \in B^n} \widetilde{P}_{CLR}(z_{-t},u_{-t},\ell_{-t},r_{-t}) [\text{“}z_{-t},u_{-t}\text{”}]$$
$$\otimes \underbrace{P \left(\sum_{i_{-t} \in J_i} (-1)^{g(\ell_{-t},i_{-t},r_{-t};z_{-t},u_{-t})} \, |\phi_{\ell_{-t}+1_{-t}+r_{-t}}\rangle \, |E_{i_{-t}|i_t}\rangle \right)}_{\tau^{(t,Q_X,z,u,i,\ell,r)}}. \tag{63}$$

Recall that, for any observed Q_X, it holds that $i \in \widetilde{G}^{(Q_X)}$ since τ is our ideal-ideal state. Combining this knowledge, and using Equation 8, for any t and Q_X we have:

$$H_\infty(A|E)_{\tau^{(t,Q_X)}} \geq \min_{i \in \widetilde{G}^{Q_X}} \min_{z,u,\ell,r} H_\infty(A|E)_{\tau^{(t,Q_X,z,u,i,\ell,r)}}. \tag{64}$$

Using Lemma 2, along with Equation 63, we have:

$$\min_{i \in \widetilde{G}^{Q_X}} \min_{z,u,\ell,r} H_\infty(A|E)_{\tau^{(t,Q_X,z,u,i,\ell,r)}} \geq \min_{i \in \widetilde{G}^{(Q_X)}} \left(n - n\bar{h}\left(w(i^{\mathtt{ph}}) + \delta \right) \right) = n \left(1 - \max_{i \in \widetilde{G}^{(Q_X)}} \bar{h}(w(i^{\mathtt{ph}}) + \delta) \right) \tag{65}$$

Considering the definition of $\widetilde{G}^{(Q_X)}$ in Equation 59, it is clear that, for any Q_X and for any $i \in \widetilde{G}^{(Q_X)}$, it holds that:

$$w(i^{\mathtt{ph}}) \leq \frac{w(Q_X) - p + \delta'}{1 - 2p} \tag{66}$$

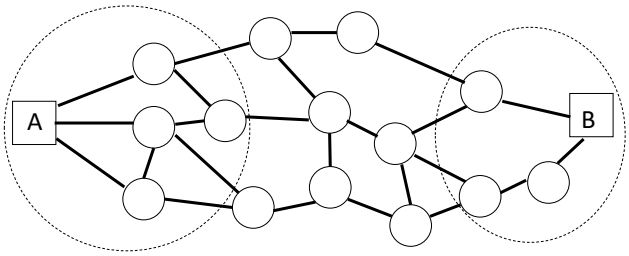

Figure 5: An example general network, where the two squares represent Alice and Bob, and the circles represent repeaters. The links and repeaters close to Alice and Bob that are marked in dashed circles are trusted, but are still noisy. The rest of the nodes and links may, or may not, be adversarial. There are multiple possible network paths between Alice and Bob in the network.

leading us to conclude that:

$$H_\infty(A|E)_{\tau^{(t,Q_X)}} \geq n\left(1-\bar{h}\left(\frac{w(q)-p+\delta'}{1-2p}+\delta\right)\right) \tag{67}$$

Now, of course this was only the ideal-ideal state, however it holds for any choice of t and observed Q_X. Since $\frac{1}{2}\left|\left|\sum_t P_T(t)[t](\rho^t-\tau^t)\right|\right| \leq 2\epsilon$, we can use Lemma 1 to finish the proof. Indeed, note that all operations performed on the two systems were CPTP maps satisfying the lemma's hypothesis, and we take the subset choice and observation of Q_X as the random variable X in that lemma. □

Our above theorem, along with Equation 7, will then allow us to determine a bound on the actual key-rate of the protocol. Setting $\epsilon_{PA} = 17\epsilon + 4(2\epsilon)^{1/3}$, for user specified ϵ, then, the overall key-rate of the protocol will be:

$$\texttt{rate} \geq \frac{N-m}{N}\left(1-\bar{h}\left(\frac{w(Q_X)-p^*+\delta'}{1-2p^*}+\delta\right)\right) - \texttt{leak}_{EC} - \frac{1}{N}\log\frac{1}{\epsilon}, \tag{68}$$

except with a failure probability of at most $\epsilon_{fail} = 2(2\epsilon)^{1/3}$. Above, $\texttt{leak}_{EC}$ is the error correction leakage.

The above is a finite-key bound on the key-rate of this QKD protocol operating over a partially corrupted repeater chain. We may also easily use this to derive an asymptotic bound as shown in the following corollary:

Corollary 3.1. In the asymptotic regime, where the number of signals N approaches infinity, assuming the observed Z and X basis noise are identical (namely Q_X) the key-rate becomes:

$$\texttt{rate}_\infty = 1-\bar{h}\left(\frac{w(Q_X)-p^*}{1-2p^*}\right) - h(w(Q_X)). \tag{69}$$

Proof. First, we may assume collective attacks, whereby the total signal is of the form $\rho_{ABE}^{\otimes N}$ and then, later, use de Finetti style arguments [51] to promote the analysis to general attacks. In the asymptotic setting, we may also set $m = \sqrt{N}$. The result then follows from the quantum asymptotic equipartition property [52] and the fact that $\frac{1}{N-m}\texttt{leak}_{EC}$ will approach $h(w(Q))$. □

4 General Networks: Network Model and Security

Our above results apply to repeater chains, however they can be extended to work with general quantum repeater networks. We model a repeater network in the typical fashion [5–7]: Alice and Bob are connected to each other through a general layout of multiple repeaters and multiple links as shown in Figure 5; note that there may be multiple paths available to Alice and Bob. On a particular network round, the network will

attempt to establish one or more Bell pairs between Alice and Bob by routing entanglement through multiple paths (or chains) of repeaters connecting Alice and Bob. The choice of paths is selected through a routing algorithm, which may be probabilistic and the path selection may be different each network round; some rounds may not produce any viable paths. However, any path starts at Alice, routes through a selection of quantum repeaters, and ends at Bob forming a repeater chain for that path. There may be memory constraints within each repeater that prevents a single repeater from appearing in more than one path on any particular network round, however we are not concerned with this.

This process repeats through multiple network rounds, each round producing zero or more paths (which are, individually, repeater chains) through which entanglement is routed between parties until Alice and Bob share N entangled pairs. For these N pairs, there must have been N paths that produced them. Note that it may have taken more or less actual network rounds to produce these N paths since, on some rounds, multiple paths might have been used leading to more than one entangled pair per round, while on others, no paths were viable. Let $\{\mathcal{P}_1, \cdots, \mathcal{P}_N\}$ be the paths used on a particular usage of the network. Each path is of the form:

$$\mathcal{P}_j = A \to \mathcal{R}_1^j \to \mathcal{R}_2^j \to \cdots \to \mathcal{R}_{c_j}^j \to B, \tag{70}$$

where each $\mathcal{R}_i^j$ represents some repeater in the network. Certain network and routing constraints may impose restrictions on path choices of course, however that is not within scope of the current discussion. Instead, we simply assume that these N paths exist and lead to N quantum states shared between Alice and Bob.

Similar to the repeater chain scenario, in the general network scenario, we will assume that there are certain repeaters near Alice and Bob which are considered "safe" or honest, though still noisy. These repeaters may be in a local connected sub-graph around Alice and Bob, as depicted in Figure 5. Any other repeater outside this region is considered to be in Eve's zone of control. Consider, then, a particular path $\mathcal{P}_j$ as above. This path can be decomposed into a left/middle/right section, namely:

$$\mathcal{P}_j = A \to L_j \to M_j \to R_j \to B \equiv (L_j, M_j, R_j),$$

where L_j consists of all contiguous repeaters in path j near Alice which she trusts while R_j consists of all contiguous repeaters near Bob which he trusts. All other repeaters in M_j, connecting the right-most repeater of L_j to the left-most repeater of R_j, are assumed to be under the control of Eve. Note that it might happen that, for some paths, the left and right sections are different sizes; sometimes they may even be empty, meaning that particular path traveled through no trusted repeaters.

Though, at the end of the day, we are still essentially working with repeater chains, there are several additional layers that must be considered. Of particular importance is the fact that the path choices (i.e., repeater chains) may be very different from each other depending on the size of the network. Also of importance is the actual path selection. To formally analyze the security in this setting, we must make the following assumptions, in addition to (or extending) those made in Section 2.1:

Assumption 5: We assume there is an honest region of the network near Alice and Bob - any repeater in this region is trusted, but introduces natural noise as discussed in Section 2. From this, any path can be decomposed into a "left/middle/right" section as discussed, where the left and right portions pass through the trusted, but noisy, network, while the middle section is assumed to be under full adversary control.
Assumption 6: Eve can fully control the path selection and routing, even the paths used in the honest region of the network. In particular, Eve can even pre-choose all N paths before the network even runs and those are the paths that the network will use while in operation. Her choice may be probabilistic and may be different each time Alice and Bob use the network for a secret key distillation. Note that this is a strong assumption in favor of the adversary.
Assumption 7: The honest portions of the network will always use the prescribed paths and will always honestly report these path selections to Alice and Bob.
Assumption 8: For every repeater in the honest section (i.e., those in L_j and R_j), that section of the network will introduce noise in the same manner as described in Section 2. However, now the probability distribution over link i, P^i (see Equation 21), will depend on the current path j and potentially the entire

path list $\mathcal{P}_1$ through $\mathcal{P}_N$. The latter may be the case if repeaters introduce noise differently based on how they must route information within the honest regions. However, for every path $\mathcal{P}_j$, Alice and Bob can lower-bound the *path noise parameter* for that path, defined in Definition 4.1. They can always set this to zero if a suitable bound cannot be determined, which would imply that this particular path is fully adversarial.

Definition 4.1. Let $\mathcal{P} = \{\mathcal{P}_1, \cdots, \mathcal{P}_N\}$ be a set of paths used by a network and let each $\mathcal{P}_j \equiv (R_j, M_j, L_j)$, where each repeater in R_j and L_j are honest, but noisy (as discussed above and in Section 2.2). Then, for each $j = 1, \cdots, N$, we define the *path noise parameter for path j given $\mathcal{P}$* to be the noise parameter (or a lower-bound) of the given repeater chain according to Definition 2.1, however, now, the probability distribution of the honest portion P_L and P_R will depend on the given $\mathcal{P}_j$ and, potentially, the selection of paths $\mathcal{P}$. We denote the noise parameter for this path to be $p^*[\mathcal{P}_j : \mathcal{P}]$ or, when the context is clear, simply $p^*[\mathcal{P}_j]$.

Note that, it may be hard for Alice and Bob in practice to be able to bound the noise parameters for every possible path through the honest region - however, they may always use the trivial lower-bound of zero.

Under the above assumptions, it is not difficult to see that, first, our reduction in Section 3.1 still applies, though one must make a few minor changes, namely:

1. The protocol begins with Eve choosing $\mathcal{P} = \{\mathcal{P}_1, \cdots, \mathcal{P}_N\}$. She sends this list to Heidi. Note that for any repeater within Eve's zone of control, Eve is not obligated to follow the selected path. Heidi, however, who is simulating the honest network, will honestly obey the path selections for those repeaters not within Eve's zone of control.
2. Heidi will create appropriate left and right states $|\mathcal{L}\rangle_L$ and $|\mathcal{R}\rangle_R$ (Equations 23 and 24), where, now, the distribution P_L and P_R depends on the path choices.
3. Alice and Bob are informed of the path choices $\mathcal{P}$. Though, they do not trust the accuracy of these paths outside the trusted region of the network.

It is not difficult to see that, with these modifications made, the resulting entanglement based protocol will match the state produced by the actual general repeater network. One can see this by tracing out the execution of both the modified entanglement based protocol and the general repeater network scenario as was done in Section 3.1.2 and note that the resulting quantum density operators are identical in both scenarios. Note we are still assuming that the noise in the honest portion of the network is independent across each round (though it may depend on the path and path history). Given this, we may now state our second main result below. The proof of the below theorem is almost identical to Theorem 2, however with a few critical changes which are highlighted in the proof below.

Theorem 3. Let $\epsilon > 0$, $\mathcal{P}$ be the path choices used, and ρ_{ABE} be the state produced through the entanglement based protocol for a general repeater network using the given $\mathcal{P}$. The A and B portions of the above state consist of N qubits each. Define δ and δ' as in Theorem 2. Let $\{p_1^*, \cdots, p_k^*\}$ be the unique path noise parameters for the given paths; namely it is an enumeration of the set $\{p^*[\mathcal{P}_1], \cdots, p^*[\mathcal{P}_N]\}$ (note that $k \leq N$ and recall $p^*[\mathcal{P}_j] = p^*[\mathcal{P}_j \ : \ \mathcal{P}]$ is the path noise parameter for path j given $\mathcal{P}$ as defined in Definition 4.1). Finally, let m_j be the number of times the path with parameter p_j^* is used in the sampled subset. Then, if Alice and Bob choose a random subset t of size $m \leq N/2$ and measure those qubits in the X basis resulting in outcome q_A and q_B and quantum state $\rho^{(t,q_A,q_B)}$, and if Alice measures the remainder of her qubits in the Z basis, it holds that:

$$Pr\left[H_\infty^{8\epsilon+2(2\epsilon)^{1/3}}(A|E)_{\rho^{(t,q_A,q_B)}} \geq n\left(1 - \bar{h}\left(\widetilde{w}(Q_X, p_1^*, \cdots, p_k^*) + \delta\right)\right)\right] \geq 1 - 2(2\epsilon)^{1/3}, \tag{71}$$

where $\widetilde{w}(Q_X, p_1^*, \cdots, p_k^*)$ is defined to be:

$$\widetilde{w}(Q_X, p_1^*, \cdots, p_k^*) = \max_{x_1, \cdots, x_k} \left(\sum_{j=1}^k \frac{m_j}{m} x_j \ : \ -\delta' \leq w(Q_X) + \sum_{j=1}^k \frac{m_j}{m}\left(2x_j p_j^* - x_j - p_j^*\right) \leq \delta', \text{ and } x_j \in [0,1] \right) \tag{72}$$

A weaker bound may also be found by setting $p^*_{\min} = \min(p^*_1, \cdots, p^*_k)$, in which case it holds that:

$$Pr\left[H_\infty^{8\epsilon+2(2\epsilon)^{1/3}}(A|E)_{\rho^{(t,q_A,q_B)}} \geq n\left(1-\bar{h}\left(\frac{w(Q_X)-p^*_{\min}+\delta'}{1-2p^*_{\min}}+\delta\right)\right)\right] \geq 1-2(2\epsilon)^{1/3}, \tag{73}$$

Proof. To prove this theorem, we follow the proof of Theorem 2, identically, up to the derivation of the ideal-ideal state in Equation 55. The previous bound on $w(i^{\mathtt{ph}})$ (for some $i \in G^{(Q_X)}$) no longer applies in this case, since Eve may adapt the noise in her state based on the path selection. For example, she may introduce more noise in honest paths that are less noisy than others (as an example). However, it is clear that, if we can find an alternative upper-bound to $w(i^{\mathtt{ph}})$, then the remainder of the proof of Theorem 2 will apply.

As in the proof of Theorem 2, let Y be the random variable indicating the phase error of the combined left and right honest sections of the network (where, now, the distribution on Y depends on the path choices, however each round is still independent). Let $\langle j \rangle$ be the subset of all N paths where a path was chosen such that p^*_j is the noise parameter for that path. That is:

$$\langle j \rangle = \left\{\ell \in \{1,2,\cdots,N\} \ : \ p^*[\mathcal{P}_\ell \ : \ \mathcal{P}] = p^*_j\right\}. \tag{74}$$

Thus $\bigcup_{j=1}^k \langle j \rangle = \{1,\cdots,N\}$ and $\langle j \rangle \cap \langle j' \rangle = \emptyset$ whenever $j \neq j'$. Then, since the noise in each honest sub-network is still independent across each round, we have for any $\ell \in \langle j \rangle$ that $Pr(Y_\ell = 1) = p^*_j$. (Before, we simply had $Pr(Y_\ell = 1) = p^*$ for all $\ell = 1,\cdots,N$.) Note that for any $y \in \{0,1\}^m$, it holds that $Pr(Y = y) = Pr(Y_1 = y_1)Pr(Y_2 = y_2)\cdots Pr(Y_m = y_m)$ due to our independence assumption on the noise in the honest network (Eve's noise may not be independently distributed of course). Note that $Pr(Y = y)$ may be determined or bounded through the give noise parameters.

Returning to $i^{\mathtt{ph}}$, we want to determine $\mu_i = \mathbb{E}(Y \oplus i^{\mathtt{ph}} \mid i)$ as in the proof of Theorem 2. We decompose $i^{\mathtt{ph}}$ into substrings $i_{\langle 1 \rangle}, i_{\langle 2 \rangle}, \cdots, i_{\langle k \rangle}$, where $i_{\langle j \rangle}$ is the substring of $i^{\mathtt{ph}}$, indexed by those rounds using noise parameter p^*_j, namely, all rounds in $\langle j \rangle$. Let $w_j = w(i_{\langle j \rangle}) = \frac{1}{m_j} wt(i_j)$, where $m_j = |i_{\langle j \rangle}| = |\langle j \rangle|$, namely where m_j is the number of rounds for which p^*_j is the noise parameter. Recall that $w(\cdot)$ is the relative Hamming weight (the relative number of ones in the input string) and $wt(\cdot)$ is the Hamming weight (the total number of one's in the input string).

As in the proof of Theorem 2, we will decompose each $i_{\langle j \rangle}$ into even and odd parts. Then, if Y produces a "one" in an even part (where $i_{\langle j \rangle}$ is zero), that will increase the total Hamming weight of $i^{\mathtt{ph}}$, while a one in an odd part will decrease it. Given this, we have, for each j:

$$wt(Y_j \oplus i_{\langle j \rangle}) = wt(i_j) - p^*_j wt(i_j) + (m_j - wt(i_j))p^*_j = m_j(w(i_j)(1-p^*_j) + (1-w(i_j))p^*_j). \tag{75}$$

Now, the total expected value of μ_i, then, is simply the sum of the above, over all j, divided by the total size of $i^{\mathtt{ph}}$, namely, divided by $m = \sum_j m_j$. This yields:

$$\mu_i = \sum_{j=1}^k \frac{m_j}{m}\left(w(i_j)(1-p^*_j) + (1-w(i_j))p^*_j\right).$$

Since each Y_i is independent, Equation 51 still holds and so does our decomposition of σ^t (Equation 53), and construction of the ideal-ideal state, τ^t (Equation 57) both also hold (with the same trace distance between them). Next, we revisit Equation 58 which requires us to consider the difference: $|w(Q_X) - \mu_i| \leq \delta'$.

First, consider the difference between them (without the absolute value):

$$\begin{aligned} w(Q_X) - \mu_i &= w(Q_X) - \left(\sum_{j=1}^{k} \frac{m_j}{m} \left(w(i_{\langle j \rangle})(1-p_j^*) + (1-w(i_{\langle j \rangle}))p_j^* \right) \right) \\ &= w(Q_X) - \left(\sum_j \frac{m_j}{m} w(i_{\langle j \rangle}) - \sum_j \frac{m_j}{m} w(i_{\langle j \rangle}) p_j^* + \sum_j \frac{m_j}{m} p_j^* - \sum_j \frac{m_j}{m} w(i_{\langle j \rangle}) p_j^* \right) \\ &= w(Q_X) - \left(w(i^{\mathtt{ph}}) + \sum_j \frac{m_j}{m} p_j^* - 2 \sum_j \frac{m_j}{m} w(i_{\langle j \rangle}) p_j^* \right), \end{aligned} \tag{76}$$

where, above, we used the fact that:

$$\sum_j \frac{m_j}{m} w(i_{\langle j \rangle}) = \frac{1}{m} \sum_j wt(i_{\langle j \rangle}) = w(i^{\mathtt{ph}}).$$

Returning to $G^{(Q_X)}$ (Equation 58), that set remains the set of all $i \in B^m$ satisfying $|w(Q_X) - w(i^{\mathtt{ph}})| \leq \delta$, however, when $k > 1$, now, we can no longer simplify this to implying $\left| w(i^{\mathtt{ph}}) - \frac{w(Q_X)-p^*}{1-2p^*} \right| \leq \frac{\delta'}{1-2p^*}$ (as we did in our proof of Theorem 2; however, as expected, when $k = 1$, we can make this simplification). Thus, we keep $G^{(Q_X)}$ to be simply:

$$G^{(Q_X)} = \left\{ i \in B^m \ : \ -\delta' \leq w(Q_X) - \left(w(i^{\mathtt{ph}}) + \sum_j \frac{m_j}{m} p_j^* - 2 \sum_j \frac{m_j}{m} w(i_{\langle j \rangle}) p_j^* \right) \leq \delta' \right\}$$

Continuing with the proof, following the proof of Theorem 2, Equation 65 still holds, we just need a new upper-bound on $w(i^{\mathtt{ph}})$. However, since $i \in G^{(Q_X)}$, if we set $w(i^{\mathtt{ph}}) = \widetilde{w}(Q_X, p_1^*, \cdots, p_k^*)$ (where the latter is defined in Equation 72), it is clear that we get an upper-bound on the actual $w(i^{\mathtt{ph}})$. In a run of the protocol, Alice and Bob know $w(Q_X)$, since that is the observed X basis noise; they also know $\frac{m_j}{m}$ since they have the honest path selections list. They also know p_j^* by Assumption 8. The only thing they cannot directly observe is $w(i_{\langle j \rangle})$ for each $i_{\langle j \rangle}$. However, they may optimize over all possible values, satisfying the given constraint that $i \in G^{(Q_X)}$ which is exactly what the $\widetilde{w}(Q_X, p_1^*, \cdots, p_k^*)$ function does. This will give a worst case bound on the relative Hamming weight of $w(i^{\mathtt{ph}})$ (the phase error introduced by Eve in the sampled subset), needed for Equation 65, and thus proves Equation 71. Alternatively, if we simply replace all occurrences of p_j^* with $\min(p_1^*, \cdots, p_k^*)$, it is clear that this will produce a worst-case upper bound on $w(i^{\mathtt{ph}})$, thus proving Equation 73. This completes the proof for the general network scenario. □

5 Evaluation

We now evaluate our key-rate bounds in quantum networks and compare them with those obtained from fully corrupted networks, i.e., those following standard BB84 assumption. In the following, we first present the results for repeater chains and then general network settings.

5.1 Results for Quantum Repeater Chains

We evaluate our key-rate bounds in both finite key (Equation 68) and asymptotic (Equation 69) settings. As we will soon see, our security model allows for significantly higher key-rates when some of the network can be assumed honest, when compared to the standard BB84 assumption, which assumes the entire network is adversarial. This shows the benefit of incorporate knowledge of honest repeaters into QKD key-rate calculations.

Our evaluation setup will assume a repeater chain with five repeaters (six fiber links total) connecting Alice to Bob. We will consider scenarios where the number of honest nodes varies from zero (a fully corrupted network) to four. We will also assume depolarizing channels connect all honest parties, and that the total observed noise can be modeled as a depolarizing channel. The latter is an assumption made just for our evaluations in order to simulate reasonable values for the expected observed noise $w(Q_X)$. That is, we are assuming the adversary's attack introduces noise that can be modeled as a depolarizing channel, for the sake of evaluation. Finally, given this setup, we will evaluate both the finite key and the asymptotic behavior of the partially corrupted repeater chain and compare with the standard BB84 expression (which assumes a fully corrupted network). For BB84, we will compare with finite key (denoted `BB84-F`) and asymptotic (denoted `BB84-A`) where appropriate.

To evaluate key-rates, we need to compute what the expected value of $w(Q_X)$ would be in a general repeater chain scenario. Then, we must determine reasonable lower-bounds on p^* in the given adversarial model. To do this, we designed a Python program which simulates the action of a repeater chain, computing the overall expected noise, given the link level noise. We simulate the case where each link suffers depolarizing noise which is a valid noise model for our network assumption. Such a depolarizing channel maps a two qubit state ρ to:

$$\mathcal{E}_q(\rho) = (1-q)\rho + \frac{q}{4}I, \tag{77}$$

where I is the identity operator on two qubits. In particular, given the total number of repeaters c, and a link level noise parameter q, our program will compute the total expected noise in the network (i.e., the value of $w(Q_X)$). We then use this simulator to determine a bound on p^* by having it compute what the noise would be in a smaller chain.

Although each link can have a different depolarizing parameter, we assume for our evaluations that they are all identically q. In our evaluations, we assume each round is independent and identical to the others; thus after a single round, the final state of the full network (after all Bell measurements and Pauli corrections are performed) is:

$$\rho_{full} = \sum_{i \in B} P_{q,c}(i^{\mathtt{bt}}, i^{\mathtt{ph}})[\phi_i]. \tag{78}$$

The X-basis error rate of the full network is then the probability of a phase-flip occurring:

$$w\left(Q_X\right) = P_{q,c}(0,1) + P_{q,c}(1,1). \tag{79}$$

We use our Python program to determine the value of $P_{q,c}(\mathtt{bt}, \mathtt{ph})$, thus allowing us to determine $w(Q_X)$, the expected total observed error rate in the chain. This also allows us to determine p^* by simulating smaller honest sub-networks separately using our Python simulator (i.e., by determining $P_{q,c'}$ for $c' < c$).

Figure 6 shows how the total observed noise accumulates in repeater networks of varying levels of corruption. In networks of fixed size, a larger honest sub-network corresponds to a higher percentage of the total measured noise being natural instead of adversarial. This means that less information is leaked to the adversary, and higher key-rates can be obtained.

We next evaluate our finite key-rate bound (Equation 68), by setting $m = .07N$ and $\epsilon = 10^{-36}$. Such a setting for ϵ will imply a failure probability and an ϵ_{PA}-secure key (see Equation 7), both on the order of 10^{-12}. We assume $\mathtt{leak}_{EC}$ is simply $1.2h(w(Q_X)+\delta)$. We simulate networks with five total repeaters (six total links) and analyze the cases where zero, two, and four repeaters are honest. Note that when the number of honest repeaters is zero, the entire network is assumed to be under adversarial control.

To benchmark our key rate against prior work, we use the finite BB84 key rate from [53], namely:

$$\mathtt{BB84\text{-}F} = \frac{N-m}{N}\left(1 - \bar{h}\left(w(Q_X)+\nu\right) - 1.2\bar{h}\left(w(Q_X)+\nu\right)\right), \tag{80}$$

where

$$\nu = \sqrt{\frac{N(m+1)\ln\left(2/\epsilon\right)}{m^2 n}}. \tag{81}$$

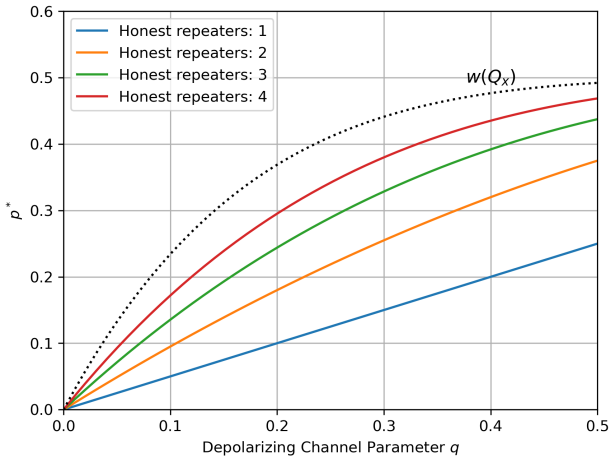

Figure 6: Repeater chain: the total observed X-basis noise $w(Q_X)$ (top, Dashed line) and honest network noise parameters p^* (Solid lines) as the link-level depolarizing noise q increases. Here we assume a five repeater (six link) network. Noise parameter p^* is computed for honest network sizes ranging from one to four repeaters.

As seen in Figure 7, our finite key rate can significantly outperform standard BB84 (which assumes a completely adversarial network), so long as one is willing to assume at least some of the repeaters are honest but noisy. Note that, as seen in this figure, if one assumes the entire network is corrupted (thus $p^* = 0$), our finite key rate requires more signals than BB84-F on fully corrupted networks to recover the same key-rate. This is not unexpected, however, and is an artifact of our proof method. In our proof, we need to sample twice to perform our ideal-ideal state analysis, thus giving worse bounds than BB84 with a fully adversarial network, where this is not required. However, asymptotically the two key-rates (ours and standard BB84) converge. When we take honest repeaters into account on partially corrupted networks, our key-rates outperform BB84-F, which is the entire point of our security proof. Indeed, our results show that even assuming a small number of honest repeaters (even one next to Alice and Bob for instance), can lead to significant improvements in overall QKD performance.

Figure 8 shows the noise tolerances of our finite key result, for $N = 10^7$ and 10^8 signal rounds. On fully corrupted networks, we again see that BB84-F is more robust to total measured noise especially when less signals are transmitted (which is, again, an artifact of our proof method). However, when assumptions of partial corruption can be made, our model provides higher key-rates and noise tolerances than BB84-F.

To compare our asymptotic key-rate (Equation 69) with BB84 in the standard security model, we use the well known BB84 rate from [54]:

$$\texttt{BB84-A} = 1 - 2\bar{h}(w(Q_X)). \tag{82}$$

We see in Figure 9 that our key-rates exactly align with BB84-A on fully corrupted networks. On partially corrupted networks, our results produce higher key-rates for all noise levels with any non-zero number of honest repeaters. This figure also shows that our result converges asymptotically to standard BB84 results, when one assumes a completely corrupted network (setting $p^* = 0$).

5.2 Results for General Quantum Networks

Using Theorem 3, we now perform evaluations for a general network. Instead of simulating an entire quantum network, we assume a network with three trusted paths on Alice's side and two on Bob's side. This setting leads to a total of six possible p^* values (since the noise parameter takes into account both the left and right portion - thus there are six possible total combinations of left/right sections of trusted regions). We will

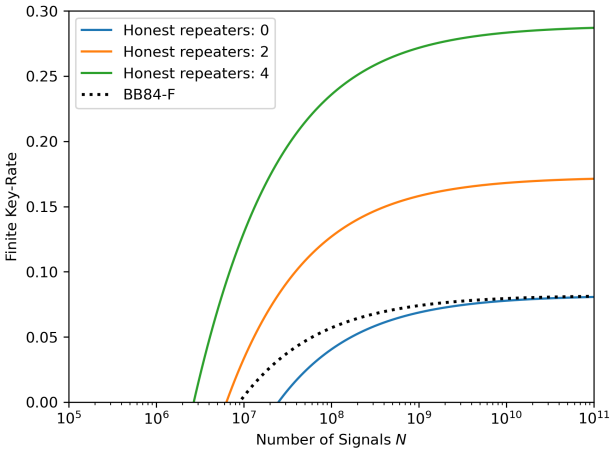

Figure 7: Repeater chain: the finite key-rate (y-axis) as the number of signals N increases (x-axis) in a five repeater chain for various numbers of honest repeaters (Solid lines). We compare to BB84 assuming a fully corrupted network (dashed line). For this graph, we set the link-level noise in each link to be $q = 3\%$.

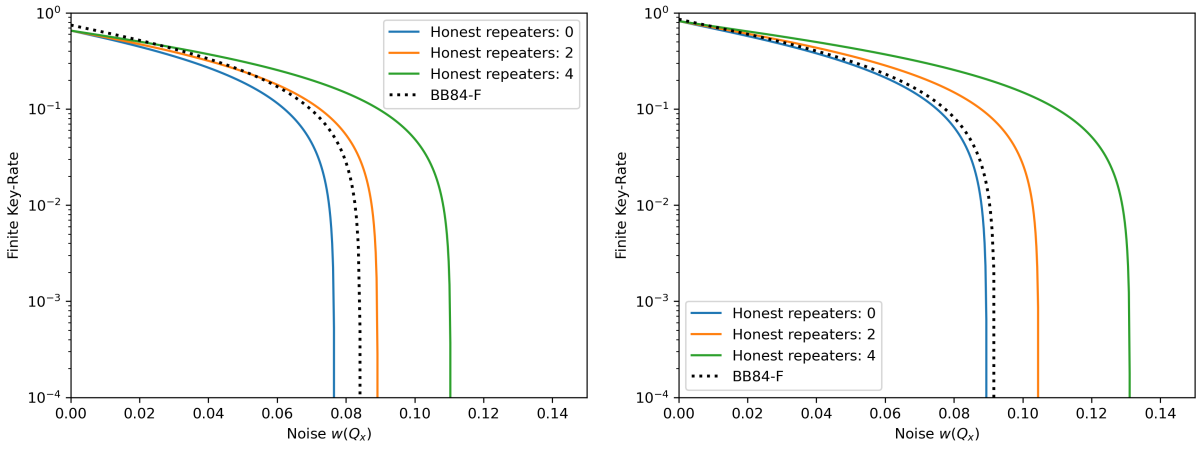

Figure 8: Repeater chain: finite key-rates versus total observed X-basis noise in a five repeater chain with $N = 10^7$ signals (left) and $N = 10^8$ signals (right). Note that higher noise tolerances are possible when one assumes at least some of the repeaters are honest, but noisy.

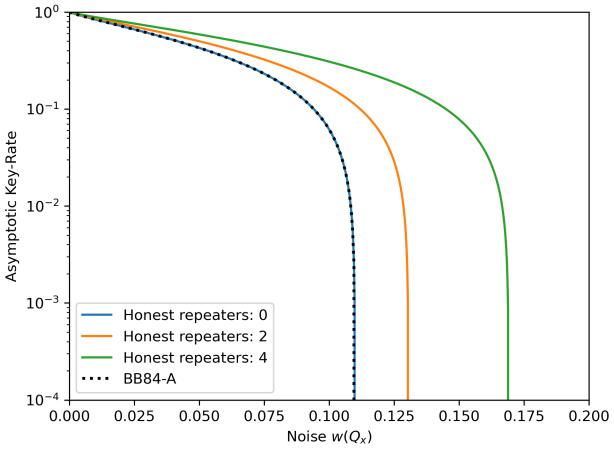

Figure 9: Repeater chain: asymptotic key-rates versus total X-basis noise in a five repeater chain. With zero honest repeaters (i.e., a fully corrupted network), our key-rate result converges with asymptotic BB84. As the number of honest repeaters in the network increases, our protocol outperforms asymptotic BB84, showing rigorously that increased noise tolerances and key-rates are possible in a partially corrupted setting.

assume the network has run, establishing a key between Alice and Bob leading to a total observed X basis noise of Q_X. Alice and Bob are given the path choices for the network. We assume on a particular round, for evaluation purposes, that the network operated such that the list of noise parameters is:

$$(p_1^*, \cdots, p_6^*) = (0.01, 0.02, 0.015, 0.05, 0.00, 0.03) \tag{83}$$

and that the ratio of these paths being chosen in the sampled portion is:

$$\left(\frac{m_1}{m}, \cdots, \frac{m_6}{m}\right) = (0.40, 0.10, 0.15, 0.05, 0.10, 0.20). \tag{84}$$

Notice that p_5^* is zero, indicating that Alice and Bob cannot characterize its noise. Given the above parameters, we may plot the finite key-rate of the system, using Theorem 3 (along with Equation 7) for various numbers of signals N and various observed noise levels Q_X. We use the same settings as before (i.e., same security parameter, error correction leakage rate, and sampling rate). This is shown in Figure 10, comparing with BB84 (using Equation 80). As with the repeater chain scenario, we see that, depending on the number of signals and the honest network noise, our result can produce higher key-rates than BB84-F, which assumes the entire network is adversarial. However, for "low" levels of honest noise and a low number of signals, the standard adversarial model (i.e., prior work) shows better key rates as shown in this same figure. As discussed with the repeater chain evaluations, this is an artifact of our proof technique, especially the double sampling, whose sampling errors improve as the number of signals increases. However, both our result, and the standard adversarial model, can be used - users may simply take the maximum of both results for the actual achievable keyrate.

In the above, we assume that Alice and Bob have no knowledge about p_5^*. We now assume that Alice and Bob have an estimate of p_5^* as 0.06. Figure 11 compares the key-rates with and without this knowledge of p_5^*. We show the results of three settings in the figure. For each setting, the results are shown in two curves with the same color, one solid and the other dashed, corresponding to cases with and without knowledge of p_5^*, respectively. We see that for all the settings, knowing p_5^* leads to a significant increase in key-rate, which demonstrates the benefits of improving estimates of the noise on the honest portion of the network.

Finally, Figure 12 is similar to Figure 10, except, now, we use the following, higher, path noise parameters:

$$(p_1^*, \cdots, p_6^*) = (0.06, 0.06, 0.04, 0.05, 0.05, 0.03) \tag{85}$$

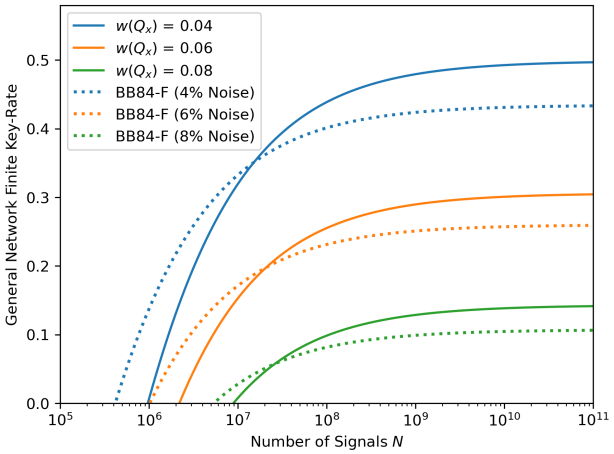

Figure 10: General quantum network: comparing the finite key-rates using our results (solid lines) which assumes a partially trusted network, and standard BB84 (dashed lines) which assumes a fully adversarial network for a general repeater network for three levels of observed X basis noise. For the solid lines, we use noise path parameters and ratios as shown in Equations 83 and 84 to evaluate the key-rate. Note that for a smaller number of signals, prior work surpasses ours - this is due to the relatively low natural noise bounds (i.e., the values of p_j^*) and the fact that our proof uses a "double sampling" technique which lowers the key-rate as discussed in the repeater chain evaluations and in the text here. Indeed, relative to the observed X basis noise, our path noise parameters for this graph are low. As the number of signals increases, the sampling error introduced by our double sampling technique vanishes leading to higher key-rates compared to the standard adversarial model.

and the same values for relative m_j's as before. For this honest network noise, we see our key-rate always outperforms BB84-F. For instance, at 7% observed X basis noise, BB84-F using the standard adversarial model can generate a key at a rate of nearly 15% while our result, assuming a partially honest network, generates a key at a rate of roughly 35%.

Taken together, these evaluations demonstrate that significantly increased noise tolerance and efficiency (i.e., increased key-rates) are possible when using our results and assuming at least some repeaters in a repeater network are honest. This also shows that it can be highly beneficial to secure at least some portions of a future quantum network as, in this case, greatly increased performance would be possible. However, for "low" levels of honest noise (or, alternatively, for weak lower-bounds on the honest noise), our results perform sub-optimally which is an artifact of our proof technique. However, both our result and the standard adversarial model are lower-bounds on the key-rate. Thus users may simply take the maximum of both to get the actual key-rate.

6 Closing Remarks

In this paper, we analyzed the case of a partially trusted (or partially corrupted) repeater network. Several motivating examples justify this security assumption: in particular, in a large-scale network, it is unreasonable to expect an adversary to be able to completely replace all devices on the network with perfect ones and, thus, "hide" within the expected natural noise. There may also be cases where certain repeaters live in a safe area, where they can be trusted (as with trusted nodes). Current day networks utilize trusted nodes which must be kept secure; securing repeaters may be significantly easier (since they don't store key material), while policing fiber links close to the source for "wiretapping" is not unreasonable, thus making this a reasonable assumption.

While it is expected that higher key-rates are possible in this scenario, proving it in the finite-key scenario

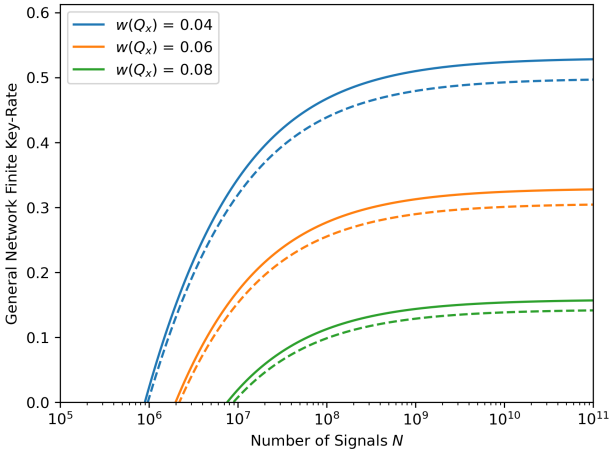

Figure 11: General quantum network: comparing our results when Alice and Bob improve their estimate of the honest noise. Dashed lines assume noise parameters as indicated in Equation 83 while solid lines are the same, except now $p_5^* = 0.06$. This shows that improving estimates of the honest noise, even for one path in a network, can significantly increase key-rates.

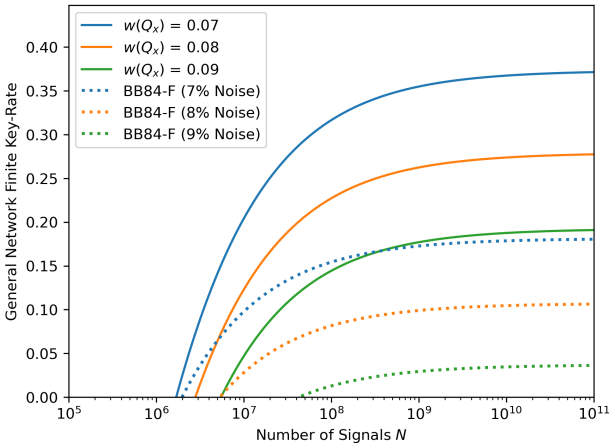

Figure 12: General quantum network: comparing our results (solid line) to the standard adversarial model (dashed line) using path noise parameters in Equation 85 representing higher known natural noise than that used in Figure 10. In this case we see our results always surpass the standard adversarial model.

is non-trivial. We derived a rigorous finite-key security proof for this setting; our proof techniques may be broadly applicable to other scenarios where there is a mix of trusted noise and adversarial noise in a quantum network. We also evaluated our results, comparing with standard security assumptions and showed that, even with a small number of trusted repeaters, higher key-rates and noise tolerances are possible. This shows the benefit in physically securing at least some portion of future quantum networks, perhaps those nodes and links near parties, even if one cannot secure the entire network from adversary attack.

Many interesting future problems remain. First, it would be highly interesting to investigate lossy channels. We suspect our proof method can be adapted to lossy channels, though we leave a rigorous proof as future work. Second, investigating practical device imperfections (e.g., multi-photon sources and imperfect detectors) would also be beneficial. This would also allow for future experimental evaluations - for instance by setting up a small point-to-point system, and evaluating the noise in that link, one may extrapolate to explore how our results would operate in a larger scale network.

Acknowledgments: AH was supported by the Defense Advanced Research Projects Agency (DARPA) ONISQ grant W911NF2010022, titled The Quantum Computing Revolution and Optimization: Challenges and Opportunities. WOK would like to acknowledge support from the NSF under grant number 2143644.

References

[1] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4), 2020.

[3] Omar Amer, Vaibhav Garg, and Walter O Krawec. An introduction to practical quantum key distribution. *IEEE Aerospace and Electronic Systems Magazine*, 36(3):30–55, 2021.

[4] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020.

[5] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

[6] Marcello Caleffi, Angela Sara Cacciapuoti, and Giuseppe Bianchi. Quantum internet: From communication to distributed computing! In *Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication*, pages 1–4, 2018.

[7] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[8] Paul Toliver, Robert J Runser, Thomas E Chapuran, Janet L Jackel, Thomas C Banwell, Matthew S Goodman, Richard J Hughes, Charles G Peterson, Derek Derkacs, Jane E Nordholt, et al. Experimental investigation of quantum key distribution through transparent optical switch elements. *IEEE Photonics Technology Letters*, 15(11):1669–1671, 2003.

[9] Cuong Le Quoc, Patrick Bellot, and Akim Demaille. Stochastic routing in large grid-shaped quantum networks. In *2007 IEEE International Conference on Research, Innovation and Vision for the Future*, pages 166–174. IEEE, 2007.

[10] Hao Wen, ZhengFu Han, YiBo Zhao, GuangCan Guo, and PeiLin Hong. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network. *Science in China Series F: Information Sciences*, 52(1):18–22, 2009.

[11] Yoshimichi Tanizawa, Ririka Takahashi, and Alexander R Dixon. A routing method designed for a quantum key distribution network. In *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 208–214. IEEE, 2016.

[12] Chao Yang, Hongqi Zhang, and Jinhai Su. The qkd network: model and routing scheme. *Journal of Modern Optics*, 64(21):2350–2362, 2017.

[13] Miralem Mehic, Peppino Fazio, Stefan Rass, Oliver Maurhart, Momtchil Peev, Andreas Poppe, Jan Rozhon, Marcin Niemiec, and Miroslav Voznak. A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks. *IEEE/ACM Transactions on Networking*, 2019.

[14] Qiong Li, Yaxing Wang, Haokun Mao, Jiameng Yao, and Qi Han. Mathematical model and topology evaluation of quantum key distribution network. *Optics Express*, 28(7):9419–9434, 2020.

[15] Piotr K Tysowski, Xinhua Ling, Norbert Lütkenhaus, and Michele Mosca. The engineering of a scalable multi-site communications system utilizing quantum key distribution (qkd). *Quantum Science and Technology*, 3(2):024001, 2018.

[16] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991.

[17] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. New York, 1984.

[18] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[19] Niek J Bouman and Serge Fehr. Sampling in a quantum population, and applications. In *Annual Cryptology Conference*, pages 724–741. Springer, 2010.

[20] Keegan Yao, Walter O Krawec, and Jiadong Zhu. Quantum sampling for finite key rates in high dimensional quantum cryptography. *IEEE Transactions on Information Theory*, 68(5):3144–3163, 2022.

[21] Walter O Krawec. Quantum sampling and entropic uncertainty. *Quantum Information Processing*, 18(12):368, 2019.

[22] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical review letters*, 91(5):057901, 2003.

[23] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[24] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, 94(23):230503, 2005.

[25] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.

[26] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

[27] Masoud Ghalaii, Sima Bahrani, Carlo Liorni, Federico Grasselli, Hermann Kampermann, Lewis Wooltorton, Rupesh Kumar, Stefano Pirandola, Timothy P Spiller, Alexander Ling, et al. Satellite-based quantum key distribution in the presence of bypass channels. *PRX Quantum*, 4(4):040320, 2023.

[28] Tom Vergoossen, Robert Bedington, James A Grieve, and Alexander Ling. Satellite quantum communications when man-in-the-middle attacks are excluded. *Entropy*, 21(4):387, 2019.

[29] Ziwen Pan, Kaushik P Seshadreesan, William Clark, Mark R Adcock, Ivan B Djordjevic, Jeffrey H Shapiro, and Saikat Guha. Secret-key distillation across a quantum wiretap channel under restricted eavesdropping. *Physical Review Applied*, 14(2):024044, 2020.

[30] A Vázquez-Castro, Davide Rusca, and Hugo Zbinden. Quantum keyless private communication versus quantum key distribution for space links. *Physical Review Applied*, 16(1):014006, 2021.

[31] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[32] Markus Mertz, Hermann Kampermann, Zahra Shadman, and Dagmar Bruß. Quantum key distribution with finite resources: Taking advantage of quantum noise. *Physical Review A*, 87(4):042312, 2013.

[33] Michael Graifer, Yuval Kochman, and Ofer Shayevitz. Quantum key distribution with state replacement. In *2023 59th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1–8. IEEE, 2023.

[34] Z Shadman, H Kampermann, T Meyer, and D Bruß. Optimal eavesdropping on noisy states in quantum key distribution. *International Journal of Quantum Information*, 7(01):297–306, 2009.

[35] Mhlambululi Mafu, Comfort Sekga, and Makhamisa Senekane. Security of bennett–brassard 1984 quantum-key distribution under a collective-rotation noise channel. In *Photonics*, volume 9, page 941. MDPI, 2022.

[36] Kevin Garapo, Mhlambululi Mafu, and Francesco Petruccione. Intercept-resend attack on six-state quantum key distribution over collective-rotation noise channels. *Chinese Physics B*, 25(7):070303, 2016.

[37] Erik Woodhead. Tight asymptotic key rate for the bennett-brassard 1984 protocol with local randomization and device imprecisions. *Physical Review A*, 90(2):022306, 2014.

[38] Eylee Jung, Mi-Ra Hwang, DaeKil Park, Hungsoo Kim, Eui-Soon Yim, and Jin-Woo Son. Attack of many eavesdroppers via optimal strategy in quantum cryptography. *Physical Review A*, 79(3):032339, 2009.

[39] Vishal Sharma, U Shrikant, R Srikanth, and Subhashish Banerjee. Decoherence can help quantum cryptographic security. *Quantum Information Processing*, 17:1–16, 2018.

[40] Shrikant Utagi, R Srikanth, and Subhashish Banerjee. Ping-pong quantum key distribution with trusted noise: non-markovian advantage. *Quantum Information Processing*, 19:1–12, 2020.

[41] Kim Boström and Timo Felbinger. Deterministic secure direct communication using entanglement. *Physical Review Letters*, 89(18):187902, 2002.

[42] Vladyslav C Usenko and Radim Filip. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Physical Review A*, 81(2):022318, 2010.

[43] Stefano Pirandola. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Physical Review Research*, 3(4):043014, 2021.

[44] Chengji Liu, Changhua Zhu, Min Nie, Hong Yang, and Changxing Pei. Composable security for inter-satellite continuous-variable quantum key distribution in the terahertz band. *Optics Express*, 30(9):14798–14816, 2022.

[45] Raúl García-Patrón and Nicolas J Cerf. Continuous-variable quantum key distribution protocols over noisy channels. *Physical Review Letters*, 102(13):130501, 2009.

[46] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[47] Walter O Krawec. Security of a high dimensional two-way quantum key distribution protocol. *Advanced Quantum Technologies*, 5(10):2200024, 2022.

[48] Walter O Krawec. Entropic uncertainty for biased measurements. In *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, volume 1, pages 1220–1230. IEEE, 2023.

[49] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[50] Hoi-Kwong Lo, Hoi-Fung Chau, and M Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18(2):133–165, 2005.

[51] Robert König and Renato Renner. A de finetti representation for finite symmetric quantum states. *Journal of Mathematical physics*, 46(12), 2005.

[52] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on information theory*, 55(12):5840–5847, 2009.

[53] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3(1):634, 2012.

[54] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.