MDPI

Article

A New Security Proof for Twin Field QKD

Walter O. Krawec [1]

[1] University of Connecticut, Storrs CT USA; walter.krawec@uconn.edu

Abstract: Twin Field QKD (TF-QKD) protocols allow for increased key-rates over long distances when compared to standard QKD protocols. They are even able to surpass the PLOB bound without the need for quantum repeaters. In this work, we revisit a previous TF-QKD protocol and derive a new, simple, proof of security for it. We also look at several variants of the protocol and investigate their performance, showing some interesting behavior due to the asymmetric nature of the protocol.

Keywords: Quantum Cryptography; Twin Field QKD; Quantum Information Theory

1. Introduction

Quantum key distribution (QKD) allows for two parties to establish a shared secret key that is secure even against computationally unbounded adversaries. This is a task that is impossible to achieve using classical communication alone, unless computational assumptions are made on the adversary's capabilities. However, QKD has several limitations, especially in terms of distance. See [1–3] for a general survey on QKD.

In general the key-rate of a QKD system is severely restricted by the total transmittance of the channel between parties. Several strategies can mitigate this, including trusted node networks [4–6] and quantum repeaters [7–9]. Quantum network research, in general, is a rapidly growing topic both for QKD [10] and the more general Quantum Internet [11] (the latter of which can support QKD, but also other applications such as distributed computing [12–14] and distributed quantum sensing [15–18]). However, an interesting third alternative to boosting QKD distances are so-called twin-field QKD (TF-QKD) protocols [19–24] which can even beat the PLOB bound [25].

Proving security of QKD protocols (TF or otherwise) is an important task, and developing novel proof techniques can be vital to advancing the state of the art (in addition to providing an additional proof of security which, itself, is interesting). Since TF-QKD can already be demonstrated experimentally over long distances [26,27] (even up to over 800km [28]), it is important to study, rigorously, the underlying security proofs for these systems as they are applicable using today's technology. Doing so affords researchers more mathematical tools to handle new protocols, and may even lead to improvements in performance under certain conditions as newer techniques may provide more optimistic security results in some cases (or, more formally, more optimistic bounds on the quantum min entropy between the users and an adversary system).

In this paper, we re-visit a TF-QKD protocol introduced in [19] and develop an entirely new proof of security using methods of quantum sampling as introduced in [29], and sampling based entropic uncertainty relations [30]. Our proof is fairly simple and can be used potentially for other TF-QKD protocols. In particular, our method might be easily adapted to the sending-not-sending TF protocol [31].

While our new proof does not improve on previously produced key-rates, we feel it is still interesting to develop alternative methods. Indeed, by now numerous proofs of security have been performed for BB84 all leading to the same result; yet different methods can be applied to different protocols later "down the road," and so developing alternative techniques is an important area of research in quantum cryptography. We also make two small changes to the original protocol (which our new security proof can handle easily) and

Citation: Krawec, W. O. A New Security Proof for Twin Field QKD. *Appl. Sci.* **2023**, *1*, 0. https://doi.org/

Received:
Revised:
Accepted:
Published:

show some interesting behavior of these new protocols, including improved performance. We are not aware of these two variants in the current literature, making them a second contribution of this paper.

2. Preliminaries

We now introduce some notation and other preliminary concepts and technical lemmas that will be important in our work later. Let $\mathcal{A}_d = \{0, 1, \cdots, d-1\}$ be a d-dimensional alphabet. Given a word $q \in \mathcal{A}_d^N$ and a subset $t \subset \{1, \cdots, N\}$, we write q_t to denote the substring of q which is indexed by t and q_{-t} to mean the substring indexed by the complement of t. If t is a singleton $t = \{i\}$, we often simply write q_i to represent the i'th character of q.

Given $\delta > 0$ and two real numbers x, y, then we write:

$$x \sim_\delta y \iff |x - y| \leq \delta. \tag{1}$$

Given a word $q \in \mathcal{A}_d^N$ and a particular character $a \in \mathcal{A}_d$, we write $\#_a(q)$ to mean the number of times a appears in the word q, namely:

$$\#_a(q) = |\{j \ : \ q_j = a\}|. \tag{2}$$

We use $\#_{a,b}(q)$ to mean the number of times a and b appear in q, namely:

$$\#_{a,b}(q) = |\{j \ : \ q_j = a \text{ or } q_j = b\}|. \tag{3}$$

Let X be a random variable taking value x_i with probability p_i. Then $H(X)$ denotes the Shannon entropy of X, namely $H(X) = -\sum_i p_i \log_2 p_i$. All logarithms in the paper are base two unless otherwise specified. We use $h(x)$ to mean the binary Shannon entropy, defined $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$.

A quantum state or density operator is a Hermitian positive semi-definite operator of unit trace, acting on some Hilbert space $\mathcal{H}$. If ρ_{AE} acts on $\mathcal{H}_A \otimes \mathcal{H}_E$, we write ρ_A to be the quantum state resulting from a partial trace over E, namely $\rho_A = tr_E \rho_{AE}$. This notation is similar for states acting on additional Hilbert spaces.

The Bell basis [32–34] is spanned by states $\{|\phi_0\rangle, \cdots, |\phi_3\rangle\}$, where:

$$\begin{aligned}
|\phi_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle) \\
|\phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle + |{-}{+}\rangle) \\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle - |{-}{-}\rangle) \\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|{+}{-}\rangle - |{-}{+}\rangle)
\end{aligned} \tag{4}$$

where, above, $|+\rangle$ and $|-\rangle$ are the Hadamard basis states, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Given a word $i \in \mathcal{A}_4^N$, we write $|\phi_i\rangle$ to mean $|\phi_i\rangle = |\phi_{i_1}\rangle \otimes \cdots |\phi_{i_N}\rangle$.

Given a density operator ρ_A we write $H(A)_\rho$ to be the von Neumann entropy of ρ_A defined to be $H(A)_\rho = -tr(\rho_A \log_2 \rho_A)$. The conditional quantum min entropy is defined to be [35]:

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

where $A \geq B$ is used to indicate that the operator $A - B$ is positive semi-definite. The smooth conditional min entropy, denoted $H_\infty^\epsilon(A|E)_\rho$, is defined to be [35]:

$$H_\infty^\epsilon(A|E)_\rho = \sup_{\sigma_{AE}} H_\infty(A|E)_\sigma, \tag{6}$$

where the supremum is over all density operators σ_{AE} such that $||\rho_{AE} - \sigma_{AE}|| \leq \epsilon$, where $||A||$ is the trace distance of operator A.

Quantum min entropy is a vital quantity in quantum cryptography as it relates directly to the number of uniform random secret bits one may extract from a quantum state [35]. In particular, given ρ_{AE} where the A register is classical and the E register is quantum, *privacy amplification* may be used to extract a uniform secret bit string. Let σ_{KE} be the result after applying the privacy amplification process to ρ_{AE}. Then, it holds that [35]:

$$\left|\left|\sigma_{KE} - \frac{I}{2^\ell} \otimes \sigma_E\right|\right| \leq 2^{-\frac{1}{2}(H_\infty^\epsilon(A|E)_\rho - \ell)} + 2\epsilon = \epsilon_{PA}. \tag{7}$$

In particular, after privacy amplification, the resulting output is almost a uniform random ℓ-bit string, independent of Eve's system. To determine a suitable size for ℓ, one need only measure the min entropy of the state ρ_{AE} before privacy amplification. For a given ϵ_{PA}, the final key is said to be ϵ_{PA} secure.

Quantum min entropy has a number of useful properties that we will require later. First, given a state of the form $\rho_{AEZ} = \sum_z p_z |z\rangle\langle z| \otimes \rho_{AE}^{(z)}$ (i.e., a state classical on Z), it holds that:

$$H_\infty(A|E)_\rho \geq H_\infty(A|EZ)_\rho \geq \min_z H_\infty(A|E)_{\rho^{(z)}}. \tag{8}$$

The following lemma allows us to bound the entropy in a state after performing a certain type of quantum operation on it, if we know the min entropy in a suitable state that is close in trace distance:

Lemma 1. (From [36]): Let ρ and σ be two quantum states and $\mathcal{F}$ be some CPTP map that acts as follows:

$$\mathcal{F}(\rho) = \sum_x p_x |x\rangle\langle x| \otimes \rho_{AE}^{(x)}$$
$$\mathcal{F}(\sigma) = \sum_x q_x |x\rangle\langle x| \otimes \sigma_{AE}^{(x)}$$

Then it holds that:

$$Pr\left(H_\infty^{4\epsilon+3\epsilon^{1/3}}(A|E)_{\rho^{(x)}} - H_\infty(A|E)_{\sigma^{(x)}} \geq 0\right) \geq 1 - 2\epsilon^{1/3}, \tag{9}$$

where the probability is over the outcome x and $\epsilon \geq \frac{1}{2}||\rho - \sigma||$.

Finally, the following lemma lets us bound the min entropy of a superposition of Bell states (the lemma is found in [37], though its proof uses techniques similar to those in [29,35] for bounding the min entropy of a general superposition state):

Lemma 2. (From [37] based on a proof in [29,35]): Let $Q \in [0, 1/2]$ and:

$$|\psi\rangle_{ABE} = \sum_{\substack{i \in \mathcal{A}_4^N \\ \frac{1}{N}\#_{1,3}(i) \leq Q}} \alpha_i |\phi_i\rangle_{AB} |E_i\rangle = \sum_i \alpha_i |\phi_{i_1}\rangle_{A_1B_1} |\phi_{i_2}\rangle_{A_2B_2} \cdots |\phi_{i_N}\rangle_{A_NB_N} |E_i\rangle, \tag{10}$$

where, recall $\#_{1,3}(i)$ is the number of times 1 and 3 appear in the string i. Let ρ_{AE} be the state resulting from taking $|\psi\rangle$, measuring all A particles in the Z basis and then tracing out the B register. Then, it holds that:

$$H_\infty(A|E)_\rho \geq N(1 - h(Q)). \tag{11}$$

2.1. Quantum Sampling

Our new proof of security will utilize a quantum sampling framework introduced by Bouman and Fehr in [29]. In this section we review some of their work that we will need later.

A classical sampling strategy over $\mathcal{A}_d^N$ is a triple of algorithms. First, is a process that randomly chooses a subset $t \subset \{1, \cdots, N\}$ with probability $P_T(t)$. Second, is a guessing function $g : \mathcal{A}_d^* \to \mathbb{R}$. Third is a target function $r : \mathcal{A}_d^* \to \mathbb{R}$. The strategy will first choose a random subset and observe q_t. Next, a guess is computed $g(q_t)$; this guess should be δ-close to the value of the target function, but evaluated on the unobserved portion of the string $r(q_{-t})$. That is, $g(q_t) \sim_\delta r(q_{-t})$.

Formally, fix $\delta > 0$ and a subset t. Then, define the set of good words to be:

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

Recall, we write $x \sim_\delta y$ if and only if $|x - y| \leq \delta$. A good word is one where the guess is always δ-close to the target for the given subset t. The classical error probability of the sampling strategy is defined simply to be:

$$\epsilon_\delta^{cl} = \max_{q \in \mathcal{A}_d^N} Pr_t(q \notin \mathcal{G}_t). \tag{13}$$

From this definition, it holds that for any word $q \in \mathcal{A}_d^N$, if the sampling strategy is performed on it, the probability that it fails (namely that the guess is not δ-close to the target) is at most ϵ_δ^{cl}.

The main result from [29] was to extend this to the quantum domain. A classical sampling strategy can be promoted to a quantum one in a natural way: given a quantum state $|\psi\rangle_{AE}$ where the A register consists of N qudits, each qudit of dimension d, one chooses a subset t and measures the qudits, indexed by t, in some d-dimensional orthonormal basis $\{|0\rangle^B, \cdots, |d-1\rangle^B\}$. This measurement results in a classical outcome q_t. Then, according to Bouman and Fehr's main result, the unmeasured portion behaves like a superposition of words that are δ close to the guess (with respect to the given target). To formalize this, fix a basis B and consider the following space:

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

This subspace is called the ideal subspace; a state within it is called an ideal state. Note that if one is given an ideal state $|\nu^t\rangle$ (which only makes sense at the moment for a specific subset t according to this definition and thus the superscript index), and if one performs a measurement in the B basis on subset t resulting in outcome $q_t \in \mathcal{A}_d^{|t|}$, the post measured state must collapse to one that is of the form:

$$|\nu_q^t\rangle = \sum_{\substack{i \in \mathcal{A}_4^{N-|t|} \\ g(q_t) \sim_\delta r(i)}} \alpha_i \, |i\rangle^B \otimes |E_i\rangle \, . \tag{15}$$

Namely, it must collapse to a superposition of words that are δ-close to the observed value (again, with respect to the given guess and target functions). Of course, states may not be necessarily ideal - the following theorem, however, says that for any quantum state, one can define a collection of ideal states that are ϵ-close in trace distance to the given state.

Theorem 1. (From [29] though re-worded slightly for our application and approach): Let $\delta > 0$, B be a d-dimensional orthonormal basis, and $|\psi\rangle_{AE}$ be a pure quantum state where the A register consists of N qudits, each qudit of dimension d. It is assumed that the dimension of each system N is known. Given a classical sampling strategy with error probability ϵ_δ^{cl}, then there exists a collection of ideal states $\{|\nu^t\rangle\}_t$, indexed by all subsets t such that $P_T(t) > 0$, such that:

$$|\nu^t\rangle \in \text{span}(\mathcal{G}_t) \otimes \mathcal{H}_E \tag{16}$$

and, furthermore:

$$\frac{1}{2}\left\|\sum_t P_T(t)\left|t\right\rangle\left\langle t\right|\otimes\left|\psi\right\rangle\left\langle\psi\right| - \sum_t P_T(t)\left|t\right\rangle\left\langle t\right|\otimes\left|\nu^t\right\rangle\left\langle\nu^t\right|\right\| \leq \sqrt{\epsilon_\delta^{cl}}. \tag{17}$$

Note that, the original proof of Theorem 1 assumes Eve's ancilla is finite dimensional. This is without loss of generality in our proof since we are considering ideal sources.

Before leaving this section, we discuss an important sampling strategy which we will use later. This strategy was analyzed in [37] for Bell states. Given a word $q \in \mathcal{A}_4^{n+m}$, choose a subset of size m uniformly at random from all m-size subsets of $\{1, \cdots, n+m\}$. The guess and target functions are simply $g(x) = r(x) = \frac{1}{|x|}\#_{1,3}(x)$. This defines the set of good words to be:

$$\mathcal{G}_t = \left\{ q \in \mathcal{A}_4^{n+m} \ : \ \frac{1}{m}\#_{1,3}(q_t) \sim_\delta \frac{1}{n}\#_{1,3}(q_{-t}) \right\}, \tag{18}$$

where, recall, $\#_{1,3}(q_t)$ is the number of 1's and 3's in the word q_t.

The failure probability of this strategy was proven in [37] to be:

$$\epsilon_\delta^{cl} \leq 2\exp\left(-\delta^2 \frac{m(n+m)}{n+m+2}\right). \tag{19}$$

3. Protocol

We now describe the specific TF-QKD protocol, introduced in [19], which we will be analyzing. A single round of the quantum communication stage consists of the following operations:

1. Alice prepares an entangled quantum state of the form:

$$\left|\psi_a\right\rangle = \sqrt{q}\left|0, v\right\rangle_{Aa} + \sqrt{1-q}\left|1, p\right\rangle_{Aa}$$

   where the A register is a private qubit memory while the a register consists of a single photon in either the vacuum state $\left|v\right\rangle_a$ or a non-vacuum state $\left|p\right\rangle_a$. This register will be transmitted to a central server. Finally, q is a publicly known parameter chosen by Alice and Bob which they will optimize over later.
2. Similarly Bob creates the state:

$$\left|\psi_b\right\rangle = \sqrt{q}\left|1, v\right\rangle_{Bb} + \sqrt{1-q}\left|0, p\right\rangle_{Bb}.$$

   The A and B registers are kept private while the a and b registers are sent to a central server.
3. The central server routes the incoming ab registers through a $50:50$ beam splitter with two detectors D_0 and D_1. The outcome of the detectors are reported to Alice and Bob. The possible outcomes are "0" (meaning detector D_0 clicked); "1" (meaning detector D_1 clicked); "*vac*" (meaning no detector clicked); and "*other*" (meaning any other outcome, such as both detectors clicking).
4. If the server reported "*vac*" or "*other*", Alice and Bob discard this round and their private qubits. If the server reported "1" Bob applies a Pauli Z gate to his private ancilla, flipping the phase of the $\left|1\right\rangle_B$ state.
5. If the server reported either "0" or "1", Alice and Bob should now hold a Bell state $\left|\phi_0^0\right\rangle_{AB}$. They will measure their private qubits in either the Z or the X basis. Some of the Z and X measurements will be used to test the fidelity of the state; the remaining Z basis states will be used for key distillation.

We note that there is a simple change to the above protocol which turns it into an equivalent prepare-and-measure protocol where Alice and Bob do not need to measure or hold private memories. For more details on that, the reader is referred to the original paper [19].

To see why the above protocol works, consider a single round. At start, Alice and Bob create the joint state:

$$\begin{aligned}|\psi_0\rangle &= (\sqrt{q}\,|0,v\rangle_{Aa} + \sqrt{1-q}\,|1,p\rangle_{A,a}) \otimes (\sqrt{q}\,|1,v\rangle_{Bb} + \sqrt{1-q}\,|0,p\rangle_{Bb}) \\ &\cong q\,|0,1,v,v\rangle_{ABab} + \sqrt{q(1-q)}(|0,0,v,p\rangle_{ABab} + |1,1,p,v\rangle_{ABab}) + (1-q)\,|1,0,p,p\rangle_{ABab}\,. \end{aligned} \tag{20}$$

At this point the ab registers are sent through a $50:50$ beam splitter. We denote the output modes of the BS to be D_0 and D_1. The action of this splitter we take to simply be (up to phase rotation):

$$\begin{aligned} BS\,|v,v\rangle_{ab} &= |v\rangle_{01} \\ BS\,|p,v\rangle_{ab} &= \frac{1}{\sqrt{2}}(|D_0\rangle_{01} + |D_1\rangle_{01}) \\ BS\,|v,p\rangle_{ab} &= \frac{1}{\sqrt{2}}(|D_0\rangle_{01} - |D_1\rangle_{01}) \\ BS\,|p,p\rangle_{ab} &= |\psi_2\rangle_{01} \end{aligned}$$

where $|\psi_2\rangle_{01}$ is the state resulting from the action of the beam splitter on receipt of two photons, one from Alice and one from Bob; the exact description of this state is not important for the following discussion.

After applying the BS to Equation 20, but before measuring the output of the BS, the state evolves to (after permuting subspaces):

$$q\,|v\rangle_{01}\,|01\rangle_{AB} + \sqrt{q(1-q)}(|0\rangle_{01}\,|\phi_0\rangle_{AB} - |1\rangle_{01}\,|\phi_1\rangle_{AB}) + (1-q)\,|\psi_2\rangle_{01}\,|10\rangle_{AB}\,. \tag{21}$$

At this point, a measurement of the BS output register is performed and the outcome broadcast. Assuming $1-q$ is "small", whenever a "D_0" or "D_1" is measured, Alice and Bob's state should collapse to an entangled Bell state; when the outcome is D_1, Bob will apply a Pauli Z gate to transform the state $|\phi_1\rangle$ to $|\phi_0\rangle$. Of course $1-q>0$, so there will be some error in the multi-photon case, and this is something that users must optimize over. Thus, interestingly, for this TF-QKD protocol, even when there is no channel noise and everything is ideal, there will always be some error in Alice and Bob's raw key which error correction must later repair.

At this point, we comment that two varieties of the above protocol may be introduced which we denote Π-`Zero` and Π-`One`. For Π-`Zero`, Alice and Bob will only use rounds where the server reports an outcome of D_0 (if any other outcome is reported, including D_1, that round is discarded); similarly, Π-`One` is defined to be the same, but Alice and Bob will only use rounds where the server reports an outcome of D_1. The original protocol, where Alice and Bob use rounds where the server reports either D_0 or D_1 will be denoted Π-`Total`. While Π-`Zero` and Π-`One` may discard more rounds, we show later that improvements in key-rates can be found in some instances based on channel statistics. This is due to the asymmetric nature of the protocol (which we discuss in more detail in Section 5.1). We are not aware of these slight modifications being analyzed in prior literature.

3.1. Entanglement Based Version

Instead of analyzing the above protocol we will, instead, analyze the following entanglement based protocol. It is not difficult to see that security of the following entanglement based version will imply security of the above prepare-and-measure version. The entanglement based version operates as follows:

1. Eve creates a quantum state $|\psi\rangle_{ABCE}$, where the A and B portions consist of N qubits each, while the C portion lives in a Hilbert space spanned by orthonormal basis $\mathcal{C} = \{|\text{“}c\text{”}\rangle\}$ for all $c \in \{\text{“0”},\text{“1”},\text{“}v\text{”},\text{“?”}\}^N$ (here, “v” will denote a vacuum observation

and "?" an "other" event). The E portion is arbitrary. Alice and Bob are given the A and B registers while the C register is sent to a trusted third party Charlie.

2. Charlie measures his entire C register in the $\mathcal{C}$ basis, broadcasting the result to all parties. Alice and Bob discard all qubits rounds where the reported outcome was "vac" or "?". Let N_c be the number of remaining systems not discarded.
3. Alice and Bob choose a random subset $t \subset \{1, \cdots, N_c\}$ of size m_c (which may depend on N_c), and measure their respective systems, indexed by this subset, in the X basis which they subsequently broadcast to determine the fidelity of their state.
4. Alice and Bob measure the remaining systems in the Z basis, leading to their raw key. They then further process this through error correction and privacy amplification as normal.

Entanglement based versions of Π-`Zero` and Π-`One` are defined similarly, with only step 2 changing.

Note that in the entanglement based version, Bob does not apply a Pauli correction gate - since Eve gets to prepare not only Alice and Bob's state, but also the state that would normally have been output from the BS, it is to Eve's advantage to "simulate" the Pauli correction before sending to Bob (though, of course, she doesn't have to - however not doing so would lead to additional X basis noise). It is not difficult to see that security of the entanglement based version, above, will imply security of the actual TF-QKD protocol. In the next section, we show a new proof of security, deriving an entropy bound for the entanglement based version, which will subsequently produce a key-rate bound for the TF-QKD protocol.

We note that the protocols above are not novel - they are, at most, very slight variations of protocols from [19]. Π-`Total` is identical to prior work in [19], while Π-`Zero` and Π-`One` are only minor variations of that protocol. As discussed in the introduction, the novelty of our work is in an alternative security proof, derived in the following section.

4. New Security Proof

We now present our new proof of security for the above TF-QKD protocol. Our proof uses the quantum sampling framework of Bouman and Fehr [29], discussed above, along with proof techniques used for sampling-based entropic uncertainty relations [30]. Namely, we prove security of the entanglement based version which will imply security of the prepare and measure version. The main result is in the following theorem:

Theorem 2. Let $|\psi\rangle_{ABCE}$ be the state Eve prepares where the A and B portions are N qubits each and the C portion is in a Hilbert space of dimension 4^N. After Charlie's measurement of the C register, let $c \in \{0, 1, v, ?\}^N$ be the resulting outcome and $|\psi^c\rangle_{ABE}$ be the post measured state (tracing out the measured C register). Let N_c be the number of signals not discarded; namely $N_c = \#_{0,1}(c)$ for Π-`Total`, $N_c = \#_0(c)$ for Π-`Zero`, and $N_c = \#_1(c)$ for Π-`One`. Alice and Bob will choose a random sample of size $m_c < N_c/2$, measure those qubits in the X basis and determine the relative number of errors in that basis, denoted Q_X. Then it holds that, except with probability $\epsilon_{fail} = 2\epsilon^{1/3}$, if the remaining $N_c - m_c$ signals are measured in the Z basis:

$$H_\infty^{4\epsilon+3\epsilon^{1/3}}(A|E) \geq (N_c - m_c)(1 - h(Q_X + \delta_c)), \tag{22}$$

where:

$$\delta_c = \sqrt{\frac{(N_c + 2)\ln(2/\epsilon^2)}{m_c N_c}}. \tag{23}$$

Proof. Consider the post-measured state $|\psi^c\rangle_{ABE}$ as discussed in the theorem statement. Without loss of generality, we may write this state as:

$$|\psi^c\rangle_{ABE} = \sum_{i \in \mathcal{A}_4^N} \alpha_i |\phi_i\rangle |E_i^c\rangle . \tag{24}$$

At this point, Alice and Bob discard certain systems based on the value of c. For instance, whenever $c_j \in \{v, ?\}$ they will discard that round; furthermore, if they are running Π-`Zero` (respectively Π-`One`) they will discard rounds when $c_j = 1$ (respectively $c_j = 0$). This effectively traces these systems out. Let N_c be defined as in the theorem statement and $R_C = N - N_C$ (the number of signals Rejected). It is easy to see that this operation, effectively tracing out certain systems of A and B, yields a mixed state which may be written as:

$$\rho^c_{ABE} = \sum_{r \in \mathcal{A}_4^{R_c}} p(r) P \underbrace{\left(\sum_{i \in \mathcal{A}_4^{N_c}} \beta_{i|r} |\phi_i\rangle |E_{i|r}\rangle \right)}_{|\psi^{c,r}\rangle_{ABE}} = \sum_{r \in \mathcal{A}_4^{R_c}} p(r) |\psi^{c,r}\rangle \langle \psi^{c,r}|_{ABE}, \tag{25}$$

where $P(|z\rangle) = |z\rangle \langle z|$. Above, the A and B registers of $|\psi^{c,r}\rangle_{ABE}$ are of N_c qubits each.

At this point, Alice and Bob choose a random subset t of size $m_c < N_c/2$ (which may depend on N_c) with uniform probability $P_T(t)$, and measure their respective systems in the X basis, observing the number of errors in this test set. The remaining qubits are measured in the Z basis. Our goal is to compute the min entropy of this final Z basis measurement.

We now switch to ideal states to complete our analysis. Fix r and c. Then, by Theorem 1, we construct ideal states $\{|\phi^{c,r,t}\rangle\}$ such that for every r, c it holds that:

$$|\phi^{c,r,t}\rangle \in \text{span}(\mathcal{G}_t) \otimes \mathcal{H}_E = \text{span}\left\{ |\phi_i\rangle \ : \ i \in \mathcal{A}_4^{N_c} \text{ and } \frac{1}{m_c} \#_{1,3}(i_t) \sim_\delta \frac{1}{n_c} \#_{1,3}(i_{-t}) \right\} \otimes \mathcal{H}_E \tag{26}$$

and, also:

$$\frac{1}{2} \left\| \sum_t P_T(t) |t\rangle \langle t| \otimes |\psi^{c,r}\rangle \langle \psi^{c,r}| - \sum_t P_T(t) |t\rangle \langle t| \otimes |\phi^{c,r,t}\rangle \langle \phi^{c,r,t}| \right\| \leq \sqrt{\epsilon^{cl}_\delta}. \tag{27}$$

Now, using the sampling strategy discussed earlier, with error probability shown in Equation 19, and choosing δ as in Equation 23, we have $\sqrt{\epsilon^{cl}_\delta} \leq \epsilon$. The above is true for any r and c; of course, by the triangle inequality, it also holds that, for every c, we have:

$$\begin{aligned} &\frac{1}{2} \left\| \sum_r p(r) \sum_t |t\rangle \langle t| \otimes |\psi^{c,r}\rangle \langle \psi^{c,r}| - \sum_r p(r) \sum_t |t\rangle \langle t| \otimes |\phi^{c,r,t}\rangle \langle \phi^{c,r,t}| \right\| \\ \leq &\frac{1}{2} \sum_r p(r) \left\| \sum_t P_T(t) |t\rangle \langle t| \otimes |\psi^{c,r}\rangle \langle \psi^{c,r}| - \sum_t P_T(t) |t\rangle \langle t| \otimes |\phi^{c,r,t}\rangle \langle \phi^{c,r,t}| \right\| \leq \epsilon. \end{aligned} \tag{28}$$

Let $X_0 = |++\rangle \langle ++| + |--\rangle \langle --|$ be the POVM element measuring Alice and Bob's qubit in the X basis and reporting the same result (i.e., no error); let $X_1 = I - X_0$ be the same, but when Alice and Bob's outcomes are different (i.e., an X basis error). Note that $X_1 |\phi_j\rangle = 0$ whenever $j = 0, 2$. Thus, X_1 can only be observed if $j = 1, 3$ (see Equation 4).

After choosing t and measuring using POVM $\{X_0, X_1\}$, resulting in outcome $q_X \in \{0,1\}^{m_c}$, it is clear from Equation 26, that the post measured state must collapse to one that may be written in the form:

$$|\phi^{c,r,t}_{q_X}\rangle = \sum_{\substack{i \in \mathcal{A}_4^{m_c} \\ \#_{1,3}(i) = \#_1(q_X)}} p(i) P \left(\sum_{\substack{j \in \mathcal{A}_4^{n_c} \\ \frac{1}{n_c}\#_{1,3}(j) \sim_\delta \frac{1}{m_c}\#_{1,3}(i)}} |\phi_j\rangle |\widetilde{E}_{j|i}\rangle \right). \tag{29}$$

Alice and Bob subsequently measure their remaining particles in the Z basis leading to their raw keys. Denote by $\sigma_{AE}^{c,r,t}$ the resulting density operator. Using Lemma 2, along with Equation 8, we have:

$$H_\infty(A|E)_{\sigma^{c,r,t}} \geq n_c(1 - h(\#_1(q_X) + \delta_c)). \tag{30}$$

Lemma 1 and Equation 28 completes the proof. □

The actual key-rate of the TF-QKD protocol, then, follows immediately and is stated in the corollary below:

Corollary 4.1. Let $\epsilon > 0$ be given. Then, except with probability $\epsilon_{fail} = 2\epsilon^{1/3}$, if the key-length of the TF-QKD protocol is set to:

$$\ell = n_c(1 - h(Q_X + \delta_c)) - \texttt{leak}_{EC} - 2\log_2 \frac{1}{\epsilon} \tag{31}$$

where $\texttt{leak}_{EC}$ is the information leaked during error correction, the final resulting key is ϵ_{PA}-secure, for $\epsilon_{PA} = 9\epsilon + 4\epsilon^{1/3}$.

Proof. This follows immediately from Theorem 2 and Equation 7. □

We note that our key-rate above agrees, asymptotically, with prior work from [19] for Π-`Total` and so our new proof above is simply an alternative method, not one to give higher results necessarily.

5. Evaluation

We now evaluate the key-rate assuming a lossy channel with detector mismatches and inefficiencies. In particular, each channel will have a transmittance of $\sqrt{\eta}$. We will assume, for evaluation purposes, that the server is honest, but has faulty devices. Thus, the server will perform the correct measurement, however the detectors will have non-zero dark count rate p_d and will have non-unit efficiency f. The measurement may also be misaligned in that it may report "0" when it should have, ideally, observed "1".

To evaluate, we require certain expected values for N_c along with the expected noise. Let $p(0)$ (respectively $p(1)$) be the probability that the server sends the message "0" (respectively "1"). Then the expected value of N_C is simply $N(p(0) + p(1))$, where N is the total number of rounds Alice and Bob perform the protocol. To find these values under our evaluation setup, we trace the protocol's execution.

First, consider the joint state created by Alice and Bob:

$$\begin{aligned}&\left(\sqrt{q}\,|0,v\rangle_{Aa} + \sqrt{1-q}\,|1,p\rangle_{Aa}\right) \otimes \left(\sqrt{q}\,|1,v\rangle_{Bb} + \sqrt{1-q}\,|0,p\rangle_{Bb}\right)\\ \cong& q\,|0,1,v,v\rangle_{ABab} + (1-q)\,|1,0,p,p\rangle_{ABab} + \sqrt{q(1-q)}(|0,0,v,p\rangle_{ABab} + |1,1,p,v\rangle_{ABab}).\end{aligned} \tag{32}$$

The qubits are sent through a lossy channel which, as in [19], we model as a beamsplitter with transmittance $\sqrt{\eta}$. In particular:

$$\begin{aligned}BS\,|p\rangle &= \sqrt{\eta}\,|p\rangle + \sqrt{1-\eta}\,|\widetilde{v}\rangle\\ BS\,|v\rangle &= |v\rangle\,.\end{aligned}$$

Note we introduce a new state $|\widetilde{v}\rangle$ to ensure the above is unitary, however $|v\rangle$ and $|\widetilde{v}\rangle$ cannot be distinguished by the parties and will look like a vacuum in either case.

The above causes the joint state to evolve to:

$$\begin{aligned} &q\,|01vv\rangle + (1-q)\,|10\rangle\,(\eta\,|pp\rangle + (1-\eta)\,|\widetilde{v}\widetilde{v}\rangle + \sqrt{\eta(1-\eta)}(|p\widetilde{v}\rangle + |\widetilde{v},p\rangle)) \\ &+\sqrt{q(1-q)}(|00\rangle\,(\sqrt{\eta}\,|v,p\rangle + \sqrt{1-\eta}\,|v,\widetilde{v}\rangle) + |11\rangle\,(\sqrt{\eta}\,|p,v\rangle + \sqrt{1-\eta}\,|\widetilde{v},v\rangle)) \end{aligned} \tag{33}$$

At this point, the system enters the server's measurement device which, before the actual measurement is performed, we model as a unitary operator C where for any $x, y \in \{v, \widetilde{v}\}$:

$$\begin{aligned} C\,|x,y\rangle &= |x,y\rangle \\ C\,|p,x\rangle &= (\alpha\,|D_0\rangle + \beta\,|D_1\rangle)\,|x\rangle \\ C\,|x,p\rangle &= (\beta\,|D_0\rangle - \alpha\,|D_1\rangle)\,|x\rangle \\ C\,|p,p\rangle &= |\psi_2\rangle \end{aligned}$$

Ideally, $\alpha = \beta = 1/\sqrt{2}$. Note that the additional $|x\rangle$ system in the above definitions are used only to ensure unitarity of C and the fact that the server's subsequent measurement cannot distinguish between $|v\rangle$ and $|\widetilde{v}\rangle$. Following the application of C, the server will measure the first of the two systems in its control leading to the reported outcome. Note that, since $|v\rangle$ and $|\widetilde{v}\rangle$ are technically indistinguishable, both observations are reported simply as a "vacuum" by the server.

Applying C to the joint state in Equation 33, but before the actual measurement, yields:

$$\begin{aligned} &q\,|01\rangle\,|vv\rangle + (1-q)\,|10\rangle\,(\eta\,|\psi_2\rangle + (1-\eta)\,|\widetilde{v},\widetilde{v}\rangle \\ &+\sqrt{\eta(1-\eta)}([\alpha+\beta]\,|D_0,\widetilde{v}\rangle + [\alpha-\beta]\,|D_1,\widetilde{v}\rangle)) \\ &+\sqrt{q(1-q)}(|00\rangle\,(\sqrt{\eta}(\beta\,|D_0,v\rangle - \alpha\,|D_1,v\rangle) + \sqrt{1-\eta}\,|v,\widetilde{v}\rangle)) \\ &+\sqrt{q(1-q)}(|11\rangle\,(\sqrt{\eta}(\alpha\,|D_0,v\rangle + \beta\,|D_1,v\rangle) + \sqrt{1-\eta}\,|\widetilde{v},v\rangle)) \end{aligned} \tag{34}$$

At this point, the server measures and reports the outcome. This measurement will be affected by dark counts (p_d) and the detector efficiency (f). For simplicity in evaluation, we will simply assume that the double-photon outcomes (namely, $|\psi_2\rangle$) do not interfere, constructively or destructively, with the other terms in the $|10\rangle_{AB}$ term. We will simply assume, then, that the probability of observing a $|D_0\rangle$ in $|\psi_2\rangle$ is p_2^0 and the probability of observing $|D_1\rangle$ is p_2^1. It turns out that, since q is large generally, this term does not significantly affect the key-rate and so this assumption does not play a major role in hurting or benefiting the key-rate. From this, we have:

$$\begin{aligned} p(0) &= q^2\frac{p_d}{2} + (1-q)^2\left(\eta^2 p_2^0 + (1-\eta)^2\frac{p_d}{2} + \eta(1-\eta)(\alpha+\beta)^2 f\right) \\ &\quad + q(1-q)\left(\eta\beta^2 f + (1-\eta)\frac{p_d}{2} + \eta\alpha^2 f + (1-\eta)\frac{p_d}{2}\right) \\ &= q^2\frac{p_d}{2} + (1-q)^2\left(\eta^2 p_2^0 + (1-\eta)^2\frac{p_d}{2} + \eta(1-\eta)(\alpha+\beta)^2 f\right) \\ &\quad + q(1-q)(\eta f + (1-\eta)p_d) \end{aligned} \tag{35}$$

Similarly, we find:

$$\begin{aligned} p(1) &= q^2\frac{p_d}{2} + (1-q)^2\left(\eta^2 p_2^1 + (1-\eta)^2\frac{p_d}{2} + \eta(1-\eta)(\alpha-\beta)^2 f\right) \\ &\quad + q(1-q)(\eta f + (1-\eta)p_d) \end{aligned}$$

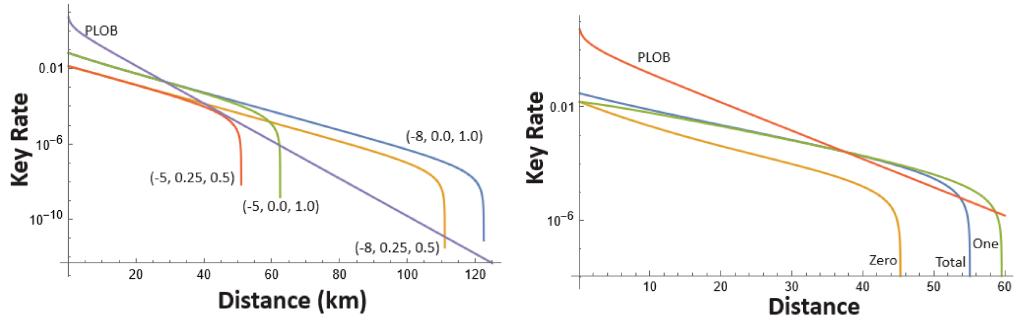

Figure 1. Left: Asymptotic key-rate of the TF-QKD protocol version Π-`Total`. Here (x, y, z) implies $p_d = 10^x$, $\alpha = \sqrt{1/2 + y}$ and $f = z$. We also compare with the PLOB bound [25]. If d is the distance to Alice and Bob, we set $\eta = 10^{-(d/2)/10}$. Right: Asymptotic key rate of TF-QKD protocol Π-`Total`, Π-`Zero`, and Π-`One`. Here we set $p_d = 10^{-5}$, $\alpha = \sqrt{3/4}$, and $f = 0.8$. Note that our key-rate agrees asymptotically with that from [19] for Π-`Total` and so we do not plot a comparison; we are not aware of a key-rate result for Π-`Zero` or Π-`One`. We note that Π-`One` can give strictly higher keyrates and support longer distances.

Next, we need the Z basis and X basis noise, conditioned on Alice and Bob not discarding the round; i.e., conditioned on the server sending a non-vacuum message in the Π-`Total` protocol case; or conditioned on sending either "0" or "1" for the Π-`Zero` or Π-`One` protocol case. Let $Q_{Z,0}$ be the probability of a Z basis error *and* the server sending the message "0". Similarly define $Q_{Z,1}$, $Q_{X,0}$, and $Q_{X,1}$. From the above equations, these expressions are easily found to be:

$$Q_{Z,0} = q^2\frac{p_d}{2} + (1-q)^2\left(\eta^2 p_2^0 + (1-\eta)^2\frac{p_d}{2} + \eta(1-\eta)f(\alpha+\beta)^2\right) \tag{36}$$

$$Q_{Z,1} = q^2\frac{p_d}{2} + (1-q)^2\left(\eta^2 p_2^1 + (1-\eta)^2\frac{p_d}{2} + \eta(1-\eta)f(\alpha-\beta)^2\right) \tag{37}$$

$$\begin{aligned} Q_{X,0} = {} & \frac{1}{2}q^2\frac{p_d}{2} + \frac{1}{2}(1-q)^2(\eta^2 p_2^0 + (1-\eta)^2\frac{p_d}{2} + \eta(1-\eta)f(\alpha+\beta)^2) \\ & + \frac{1}{2}q(1-q)(\eta(\beta-\alpha)^2 f + (1-\eta)\frac{p_d}{4}) \end{aligned} \tag{38}$$

$$\begin{aligned} Q_{X,1} = {} & \frac{1}{2}q^2\frac{p_d}{2} + \frac{1}{2}(1-q)^2(\eta^2 p_2^0 + (1-\eta)^2\frac{p_d}{2} + \eta(1-\eta)f(\alpha-\beta)^2) \\ & + \frac{1}{2}q(1-q)(\eta(\alpha-\beta)^2 f + (1-\eta)\frac{p_d}{4}) \end{aligned} \tag{39}$$

From these, the needed conditional noise values may be determined for our evaluation scenario.

In our evaluations, we set $q = 0.95$ which was found to be roughly the optimal value. We also set $p_2^0 = p_2^1$ to be $1/2$. We found no significant affect on the key-rate for other values, due to the high value of q and so simply make this value $1/2$. For finite key rates, we set $m_c = \sqrt{N_C}$.

To evaluate, we use Corollary 4.1, setting $\texttt{leak}_{EC} = 1.2h(Q+\delta)$, where Q is the Z basis error noise (e.g., $Q = (Q_{Z,0} + Q_{Z,1})/(p(0) + p1)$ for Π-`Total`; similar for other protocol settings). A graph of the resulting asymptotic keyrates are shown in Figure 1 (comparing to the PLOB bound [25]). Finite key results are shown in Figure 2. Note that our key-rates agree asymptotically to previous results for the Π-`Total` version and so we do not compare to prior work for that setting; for other settings (namely Π-`Zero` and Π-`One`), we are not aware of any security proof, and so there is no comparison beyond comparing to Π-`Total`.

5.1. A Discussion on the Asymmetric Nature of the Protocol

It is worth taking a closer look as to why Π-`Zero` and Π-`One` perform differently from the standard version Π-`Total`. Consider, first, Equations 36 and 37. Note that, even under

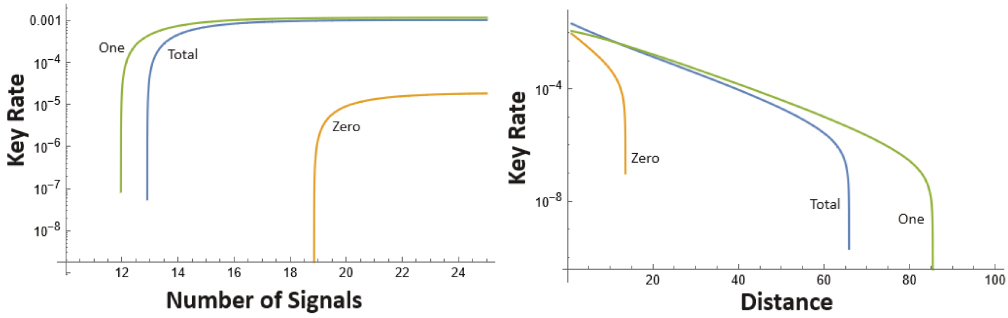

Figure 2. Left: Key-rate as a function of the number of signals (note that x-axis is log-scale). Here, $p_d = 10^{-8}$, distance is 25km; $\alpha = \sqrt{3/4}$; and $f = .8$; Right: Finite key-rate as a function of distance; here we use the same parameters as in the left figure, but with $N = 10^{15}$. Again, we note that Π-`One` can outperform the other two protocol modes of operation.

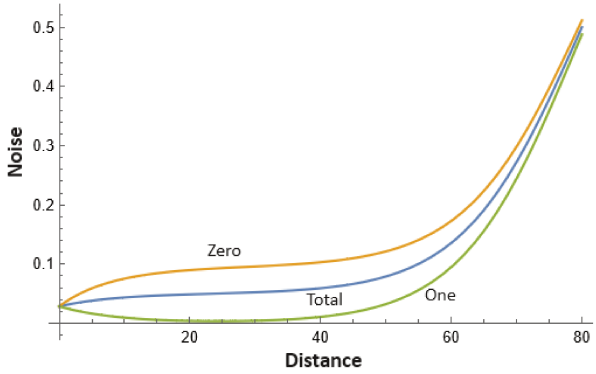

Figure 3. Showing the total Z basis error rate for Π-`Zero` (top), Π-`Total` (middle) and Π-`One` (bottom). Lower is better as it indicates less raw key error. The asymmetric nature of the protocol causes there to be fewer errors when the server sends the message 1. See text for further discussion.

ideal conditions of $p_d = 0$, $f = 1$, and $\alpha = \beta = 1/\sqrt{2}$ (which is what would be expected if all devices were perfect and there were simply natural loss η), then for any $\eta > 0$, it holds that $Q_{Z,1} < Q_{Z,0}$. Similarly, $Q_{X,1} < Q_{X,0}$. The same inequalities hold for imperfect devices (i.e., when $p_d > 0$ and $f < 1$). This can be seen more clearly in Figure 3. Thus, anytime the server sends the message 0, there is actually a greater chance of error than in the 1 message case. Therefore, under most conditions and under this channel scenario, discarding all messages of 0 actually improves performance of the system. Of course, users may decide *after* measuring the channel statistics to determine which mode of operation to perform - thus, users can always optimize over their choice of protocol after the quantum data has been transmitted, and can therefore always choose the mode that will return the higher number of key-bits. It would be interesting to analyze these three protocols under other channel scenarios, beyond depolarizing. Note that our security proof can handle *any* channel scenario - we choose depolarization channels only for our evaluations in this section.

6. Closing Remarks

In this paper, we revisited a TF-QKD protocol introduced in [19] and derived a new proof of security for it. Our new proof uses methods from quantum sampling techniques [29]. While our new proof agrees with prior work and, so, does not show higher key-rates compared to prior work, we still feel alternative proof techniques are interesting and important. We also investigated two slight variants of the protocol and showed how they can lead to improved key-rates in some scenarios.

Many interesting future problems remain. Perhaps the most fruitful would be to further explore the two variants and see if additional improvements can be made. Furthermore, a finite-key proof using decoy-state methods (using our sampling based proof approach) would be interesting, especially for Π-`Zero` and Π-`One`. Adapting our proof technique to other TF-QKD protocols would also be very interesting; a particular candidate to start with would be the sending or not sending (SNS) TF-QKD protocol [31] due to its similar encoding mechanism. Also, it would be interesting to discover whether or not asymmetric protocols (similar to Π-`Zero` and Π-`One` analyzed in this work) can be defined and shown to be more efficient for such protocols like the SNS TF-QKD mechanism.

Also, leading into more practical device considerations, it is known that for single photon interference protocols (such as the TF protocol discussed in this paper), there are still challenges with matching the mode of the photon and detector which ultimately affects the protocol's performance [38]. Such issues must be considered in future work to address applicability issues of the protocol.

Acknowledgments: The author would like to thank the reviewers for their helpful comments which greatly improved the quality of the manuscript. The author would also like to acknowledge support from the NSF under grant number 2143644.

1. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301.
2. Amer, O.; Garg, V.; Krawec, W.O. An introduction to practical quantum key distribution. *IEEE Aerospace and Electronic Systems Magazine* **2021**, *36*, 30–55.
3. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *arXiv preprint arXiv:1906.01645* **2019**.
4. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.; et al. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics* **2009**, *11*, 075001.
5. Zhang, Q.; Xu, F.; Chen, Y.A.; Peng, C.Z.; Pan, J.W. Large scale quantum key distribution: challenges and solutions. *Optics express* **2018**, *26*, 24260–24273.
6. Tysowski, P.K.; Ling, X.; Lütkenhaus, N.; Mosca, M. The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD). *Quantum Science and Technology* **2018**, *3*, 024001.
7. Kimble, H.J. The quantum internet. *Nature* **2008**, *453*, 1023–1030.
8. Wehner, S.; Elkouss, D.; Hanson, R. Quantum internet: A vision for the road ahead. *Science* **2018**, *362*, eaam9288.
9. Amer, O.; Krawec, W.O.; Wang, B. Efficient routing for quantum key distribution networks. In Proceedings of the 2020 IEEE International Conference on Quantum Computing and Engineering (QCE). IEEE, 2020, pp. 137–147.
10. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials* **2022**, *24*, 839–894.
11. Rozenman, G.G.; Kundu, N.K.; Liu, R.; Zhang, L.; Maslennikov, A.; Reches, Y.; Youm, H.Y. The quantum internet: A synergy of quantum information technologies and 6G networks. *IET Quantum Communication* **2023**.
12. Van Meter, R.; Devitt, S.J. The path to scalable distributed quantum computing. *Computer* **2016**, *49*, 31–42.
13. Yimsiriwattana, A.; Lomonaco Jr, S.J. Distributed quantum computing: A distributed Shor algorithm. In Proceedings of the Quantum Information and Computation II. SPIE, 2004, Vol. 5436, pp. 360–372.
14. Cuomo, D.; Caleffi, M.; Cacciapuoti, A.S. Towards a distributed quantum computing ecosystem. *IET Quantum Communication* **2020**, *1*, 3–8.
15. Zhang, Z.; Zhuang, Q. Distributed quantum sensing. *Quantum Science and Technology* **2021**, *6*, 043001.
16. Ge, W.; Jacobs, K.; Eldredge, Z.; Gorshkov, A.V.; Foss-Feig, M. Distributed quantum metrology with linear networks and separable inputs. *Physical review letters* **2018**, *121*, 043604.

17. Proctor, T.J.; Knott, P.A.; Dunningham, J.A. Multiparameter estimation in networked quantum sensors. *Physical review letters* **2018**, *120*, 080501.
18. Eldredge, Z.; Foss-Feig, M.; Gross, J.A.; Rolston, S.L.; Gorshkov, A.V. Optimal and secure measurement protocols for quantum sensor networks. *Physical Review A* **2018**, *97*, 042337.
19. Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Information* **2019**, *5*, 64.
20. Yin, H.L.; Chen, Z.B. Finite-key analysis for twin-field quantum key distribution with composable security. *Scientific reports* **2019**, *9*, 17113.
21. Wang, Z.H.; Wang, R.; Yin, Z.Q.; Wang, S.; Lu, F.Y.; Chen, W.; He, D.Y.; Guo, G.C.; Han, Z.F. Tight finite-key analysis for mode-pairing quantum key distribution. *Communications Physics* **2023**, *6*, 265.
22. Zhang, X.X.; Wang, Y.; Jiang, M.S.; Zhou, C.; Lu, Y.F.; Bao, W.S. Finite-key analysis of asymmetric phase-matching quantum key distribution with unstable sources. *JOSA B* **2021**, *38*, 724–731.
23. Maeda, K.; Sasaki, T.; Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nature communications* **2019**, *10*, 3140.
24. Guillermo, C.L.; Álvaro, N.; Koji, A.; Go, K.; Marcos, C.; Mohsen, R. Tight finite-key security for twin-field quantum key distribution. *npj Quantum Information* **2021**, *7*.
25. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nature communications* **2017**, *8*, 15043.
26. Liu, H.; Jiang, C.; Zhu, H.T.; Zou, M.; Yu, Z.W.; Hu, X.L.; Xu, H.; Ma, S.; Han, Z.; Chen, J.P.; et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. *Physical Review Letters* **2021**, *126*, 250502.
27. Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.J.; Han, Z.Y.; Ma, S.Z.; Hu, X.L.; Li, Y.H.; Liu, H.; et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. *Nature Photonics* **2021**, *15*, 570–575.
28. Wang, S.; Yin, Z.Q.; He, D.Y.; Chen, W.; Wang, R.Q.; Ye, P.; Zhou, Y.; Fan-Yuan, G.J.; Wang, F.X.; Chen, W.; et al. Twin-field quantum key distribution over 830-km fibre. *Nature photonics* **2022**, *16*, 154–161.
29. Bouman, N.J.; Fehr, S. Sampling in a quantum population, and applications. In Proceedings of the Annual Cryptology Conference. Springer, 2010, pp. 724–741.
30. Yao, K.; Krawec, W.O.; Zhu, J. Quantum sampling for finite key rates in high dimensional quantum cryptography. *IEEE Transactions on Information Theory* **2022**, *68*, 3144–3163.
31. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Physical Review A* **2018**, *98*, 062323.
32. Bell, J.S. On the einstein podolsky rosen paradox. *Physics Physique Fizika* **1964**, *1*, 195.
33. Braunstein, S.L.; Mann, A.; Revzen, M. Maximal violation of Bell inequalities for mixed states. *Physical Review Letters* **1992**, *68*, 3259.
34. Sych, D.; Leuchs, G. A complete basis of generalized Bell states. *New Journal of Physics* **2009**, *11*, 013006.
35. Renner, R. Security of quantum key distribution. *International Journal of Quantum Information* **2008**, *6*, 1–127.
36. Krawec, W.O. Security of a High Dimensional Two-Way Quantum Key Distribution Protocol. *Advanced Quantum Technologies* **2022**, *5*, 2200024.
37. Krawec, W.O. Entropic Uncertainty for Biased Measurements. *To appear: Proc. IEEE QCE 2023. arXiv preprint arXiv:2305.09753* **2023**.
38. Chen, Z.; Wang, X.; Yu, S.; Li, Z.; Guo, H. Continuous-mode quantum key distribution with digital signal processing. *npj Quantum Information* **2023**, *9*, 28.