QKD parameter estimation by two-universal hashing leads to faster convergence to the asymptotic rate

Dimiter Ostrev

Abstract

This paper proposes and proves security of a QKD protocol which uses two-universal hashing instead of random sampling to estimate the number of bit flip and phase flip errors. This protocol dramatically outperforms previous QKD protocols for small block sizes. More generally, for the two-universal hashing QKD protocol, the difference between asymptotic and finite key rate decreases with the number n of qubits as cn^{-1}, where c depends on the security parameter. For comparison, the same difference decreases no faster than $c'n^{-1/3}$ for an optimized protocol that uses random sampling and has the same asymptotic rate, where c' depends on the security parameter and the error rate.

1 Introduction

Quantum Key Distribution allows two users, Alice and Bob, to agree on a shared secret key using an authenticated classical channel and a completely insecure quantum channel. There are information theoretic security proofs for QKD protocols (for example [17, 16, 8, 6, 1, 21, 20] among many others). Quantum key distribution has also been realized experimentally and is commercially available. The rare combination of information theoretic security and practical achievability has attracted considerable attention to QKD.

A QKD protocol has several important parameters:

1. Block size: the number of pairs of qubits that Alice and Bob receive. Following [20, Part 1], this paper considers entanglement based protocols and defines the block size as the number of qubits after sifting.
2. Output size: the number of bits of secret key that the protocol produces.
3. Key rate: the ratio of output size to block size. The higher the key rate is, the more efficiently the protocol converts the available quantum resource to a secret key.
4. Security level: the distance of the output from an ideal secret key. The lower the security level, the better the guarantee that no future evolution

of the protocol output and adversary registers will be able to distinguish between the output and an ideal key.

5. Robustness: the amount and type of noise that the protocol can tolerate without aborting. In particular, the QKD protocol should be able to tolerate at the very least the imperfections of whatever quantum channel and entanglement source is used to implement the protocol.

Existing QKD protocols and security proofs exhibit trade-offs between these parameters: improving the security or robustness of the protocol worsens the key rate. These trade-offs are particularly severe when the block size is small. The phenomenon that the key rate of a QKD protocol deteriorates significantly for small block sizes has been called finite size effect [13, Sections II-C and IX].

The finite size effect has practical consequences in cases when the quantum phase of the protocol is particularly difficult to implement. As an example, consider the problem of using QKD between users who are far apart on the surface of the earth. The Micius satellite experiment [23] tried to solve this problem by using a satellite to distribute entangled photon pairs to two ground stations that are 1120km apart. However, sending entangled photon pairs from space to earth is difficult. In the Micius experiment, several nights of good weather had to pass until the ground stations accumulated sifted block size 3100. The error rate that the ground stations needed to tolerate was 4.51%. Reference [9] performed a state-of-the-art security analysis on this data, and concluded that security levels better than around 10^{-6} lead to no secret key at all, while at security level 10^{-6}, only six bits of secret key are extracted. Several nights, 6 bits of secret key, security level 10^{-6}: this is not enough to fulfil the promise of QKD for high levels of security, and not enough to justify the complexity and cost of QKD equipment. Something else is needed.

Where can further improvement be found? Finite key analysis for QKD protocols of the BBM92 type is already mature. Reference [9] managed to prove a slightly tighter upper bound on the tail probability for random sampling, and thus obtain a small improvement over reference [20]. However, this cannot continue much further: there are also lower bounds on the tail probability for random sampling.

Can the equipment for transmitting entangled photon pairs from space to earth be improved by several orders of magnitude? Perhaps, but that appears not so easy to do, and would involve a major technological advance.

This paper proposes a different path: to consider QKD protocols where Alice and Bob can apply CNOT gates in addition to single qubit measurements. Later discussion will make clear how this helps, but for now, focus on the widespread belief that protocols with single qubit operations are practical, while other QKD protocols are impractical. It is true that QKD protocols that use the CNOT gate are not easy to implement with present technology. However, this need not remain so in the future. Indeed, what is practical or not practical changes with time. Recall that when the BB84 protocol was published, technology for even single qubit operations was not available. The BB84 protocol started to become practical around two-three decades after its publication. Returning now

to protocols involving the CNOT gate, note that many groups around the world are working on technologies to store and manipulate qubits, striving for better fidelity and more qubits. Thus, there is hope that within the next two-three decades, QKD protocols that use the CNOT gate will also become practical.

In summary, the path of QKD protocols that use the CNOT gate also requires a technological advance. However, referring again to the Micius satellite example, it appears easier to make a moderate advance in CNOT gates and a moderate advance in the transmission of entangled photon pairs from space to earth, rather than to put the entire burden on only one of these approaches.

What kind of QKD protocols become possible if the restriction to single qubit operations is lifted, and the CNOT gate is allowed? How do they perform in comparison to protocols with only single qubit operations? This paper presents one QKD protocol that involves the use of CNOT gates: the two-universal hashing QKD protocol, and proves its security. The two-universal hashing QKD protocol is an entanglement based protocol with block size n, that can tolerate any r bit flip errors and any r phase flip errors, and at the end extract $n - 2\lceil nh(r/n) + 2\log_2(1/\epsilon) + 5\rceil$ secret key bits, that are ϵ close to an ideal secret key.

For small block sizes, the two-universal hashing QKD protocol dramatically outperforms protocols of the BBM92 type. To illustrate, consider again the security analysis developed in the sequence of papers [21, 20, 9] applied to the Micius satellite example.

1. Fix the tolerated error rate at 4.51%, the security level at 10^{-6} and the output size at 6 bits. The BBM92 type protocol with the security proof developed in [21, 20, 9] requires block size 3100. The two-universal hashing protocol requires block size 200.

2. Fix the block size at 3100 and fix the error rate at 4.51%. The BBM92 type protocol with the security proof developed in [21, 20, 9] can extract 6 secret key bits with security level 10^{-6}. The two universal hashing protocol can extract 385 secret key bits with security level 10^{-80}.

The advantage of the two-universal hashing QKD protocol is particularly noticeable for small block sizes; however, it is not limited to them. For fixed error rate $\delta = r/n$ and fixed security parameter ϵ, the asymptotic rate of this protocol is $1-2h(\delta)$, and the deviation of finite from asymptotic rate is between $(4\log_2(1/\epsilon)+10)/n$ and $(4\log_2(1/\epsilon)+12)/n$. By contrast, the deviation of finite from asymptotic key rate for the BBM92 type protocol with the security proof [21, 20, 9] is of the form $cn^{-1/3}$, where c depends on the tolerated error rate and the security level.

What is different about the two-universal hashing protocol and what causes the dramatic improvement in performance? How does the use of CNOT gates help? To start, note that no classical protocol can distinguish between inputs that are suitable for the extraction of a secret key and inputs that are not suitable. The ability to "detect the presence of an eavesdropper" is a uniquely quantum feature and is the central insight that makes QKD possible. This is

the task of parameter estimation. The two-universal hashing protocol performs parameter estimation differently from previous protocols. Indeed, it seems natural to expect that in order to perform better the uniquely quantum task of distinguishing suitable from unsuitable inputs, it is advantageous to allow more general quantum operations for Alice and Bob.

The next few paragraphs explain the disadvantages of parameter estimation as performed in QKD protocols with only single qubit operations. For the purpose of this high level discussion, define parameter estimation as a two party LOCC protocol which performs a partial measurement on the input state and outputs a decision: to accept or reject, and outputs a promise on the post-measurement state in case of acceptance. Parameter estimation protocols can differ in the class of input states on which they accept, the number of ebits they consume, the precision of the promise they provide in case of acceptance, and the probability that parameter estimation accepts but the promise on the post-measurement state does not hold.

Previous QKD protocols perform parameter estimation by random sampling: a random subset of n_{pe} positions is measured and the outcomes are publicly compared. If the error rate on these positions is below some threshold δ, then parameter estimation accepts and outputs the promise that the error rate on the remaining positions is at most $\delta + \nu$, where ν is the gap between observed and inferred error rate.

A significant advantage of parameter estimation by random sampling is that it can be implemented with only single qubit operations for Alice and Bob. Unfortunately, this is also the only advantage of random sampling. The promise that the error rate on the remaining positions is at most $\delta + \nu$ is very weak: n_{pe} ebits have already been sacrificed for parameter estimation, and now further ebits have to be sacrificed for information reconciliation and privacy amplification. The failure probability scales roughly as $exp(-4n_{pe}v^2)$, which is also very weak, despite the fact that it involves an exponential function. To see this, suppose that the target failure probability is e^{-100} and that the target gap is $\nu = 0.01$. Then, n_{pe} has to be chosen to be 250000, clearly orders of magnitude more than can be afforded for block sizes around 1000 or 10000.

By contrast, for the two-universal hashing protocol, $2k$ ebits are sacrificed for parameter estimation. If the test passes, then Alice and Bob know that the post-parameter-estimation state is a particular Bell state of $n - 2k$ ebits; thus, Alice and Bob do not need to sacrifice any further ebits for information reconciliation and privacy amplification. Moreover, the scaling of the failure probability for parameter estimation with the number of sacrificed ebits does not have the ν^2 coefficient in front of the number of sacrificed ebits.

To obtain such a parameter estimation protocol, the present paper builds on a number of previous ideas. The idea that two universal hashing can be used to estimate the number of errors is partially present in the protocols [21, 6], and [6] attributes it to the earlier work [10]. In these protocols, the number of errors in one of the measurement bases is estimated by random sampling, while for the other basis there is a two-universal hash in the information reconciliation phase that is used to ensure correctness. This is also related to the observation

[2, Theorem 6],[16, Section 6.3.2] that two-universal hash functions can be used to achieve information reconciliation with minimum leakage.

A combination of several ideas leads to the extension of the use of two-universal hashing from information reconciliation to a full QKD protocol. Specifically, these ideas are: random matrices over the field with two elements are a two-universal hash family [5], and they are also parity check matrices of classical linear error-correcting codes. Classical linear codes can be used to construct quantum CSS codes [4, 18], and CSS codes can be used to design and prove security of QKD protocols [17]. The present paper also uses a number of technical lemmas related to the stabilizer formalism [7, 3]. Finally, [1] translates the guarantees of classical random sampling to the quantum case. This served as inspiration for the present paper, which translates the guarantees of classical two-universal hashing to the quantum case.

Another group of related works are those that prove security of classical privacy amplification by arguing that it corresponds to a virtual phase error correction, such as [8, 6]. However, note that privacy amplification is a classical protocol for Alice and Bob. As such, privacy amplification requires a promise on the input state to operate, and if an unsuitable input is given, it produces an insecure key. With this in mind, note that the use of virtual phase error correction to prove security of classical privacy amplification is possible, but is not strictly necessary: other proofs of security for privacy amplification exist, for example in [16]. When it comes to the uniquely quantum task of distinguishing suitable from unsuitable inputs, [8, 6] resort to the same technique as all other QKD protocols: single qubit operations and random sampling tail bounds. By contrast, the two-universal hashing QKD protocol takes an input state prepared by the adversary, correctly identifies whether the state is suitable or not, and either produces a secure key or aborts. Here, random linear functions and the stabilizer formalism are used to perform the uniquely quantum task: distinguish suitable from unsuitable inputs.

The rest of this paper is structured as follows: Section 2 introduces material that is needed to present and prove the security of the two universal hashing QKD protocol, including the security and robustness criteria for QKD protocols, a number of useful lemmas related to the stabilizer formalism, the use of two-universal hashing to obtain an optimal information reconciliation protocol, and a number of useful lemmas about random matrices over the field with two elements. Section 3 presents the two-universal hashing QKD protocol and shows that it is secure and robust. Section 4 shows that for fixed security level and tolerated error rate, the finite key rate converges to the asymptotic rate as cn^{-1} for two-universal hashing and as $cn^{-1/3}$ for random sampling, where n is the block size. Section 5 concludes and gives some open problems.

2 Preliminaries

This section presents definitions and results that are used to state and prove the main result on the security and robustness of the two-universal hashing

protocol. Subsection 2.1 recalls the standard security criterion for QKD. Then, subsection 2.2 contains a number of lemmas related to the stabilizer formalism; these are used during the security proof. Finally, subsection 2.3 contains lemmas related to two-universal hashing. Subsection 2.3 also discusses an application of two-universal hashing to approximately compute certain functions from partial information about the input; this is used during the security proof.

2.1 Security and robustness of quantum key distribution

This section recalls the security and robustness criteria from [16] that ensure that a the key produced by QKD can be used in any application. See [15] for a proof of the equivalence of this security criterion and security in the Abstract Cryptography framework for composable security.

As is common in the QKD literature, this paper assumes that the adversary Eve is active in the quantum phase of the protocol but remains passive during the classical phase, i.e. Eve eavesdrops the classical communication but does not attempt to modify or block it. Under this assumption, an entanglement-based QKD protocol is a completely positive trace preserving map that transforms input states ρ_{ABE} of Alice, Bob and Eve into output states $\tilde{\rho}_{W_A W_B CE}$, where W_A, W_B are registers containing Alice and Bob's output: a secret key or indication $\perp$ of protocol abort, and where C is a register containing a transcript of the classical communication between Alice and Bob.

Since registers W_A, W_B contain classical values, the final state $\tilde{\rho}_{W_A W_B CE}$ can be decomposed as

$$\tilde{\rho}_{W_A W_B CE} = |\perp\perp\rangle\langle\perp\perp|_{W_A W_B} \otimes \tilde{\rho}_{CE}(\perp) + \sum_{w_A, w_B} |w_A w_B\rangle\langle w_A w_B|_{W_A W_B} \otimes \tilde{\rho}_{CE}(w_A, w_B)$$

This decomposition is used to formulate the definition of security:

Definition 1. *A QKD protocol is ϵ secure if for all input states ρ_{ABE}, the output state $\tilde{\rho}_{W_A W_B CE}$ is ϵ-close in trace distance to the corresponding ideal state*

$$|\perp\perp\rangle\langle\perp\perp|_{W_A W_B} \otimes \tilde{\rho}_{CE}(\perp) + \sum_{w} \frac{1}{|W|} |ww\rangle\langle ww|_{W_A W_B} \otimes (\tilde{\rho}_{CE} - \tilde{\rho}_{CE}(\perp))$$

where $|W|$ denotes the size of the secret key space.

Alternatively, ϵ-security can be further subdivided into requirements for secrecy and correctness:

Definition 2. *A QKD protocol is ϵ correct if for all input states ρ_{ABE}, the probability*

$$Pr(W_A \neq W_B) = \sum_{w_A \neq w_B} Tr(\tilde{\rho}_{CE}(w_A, w_B))$$

that Alice and Bob accept and output different keys is bounded by ϵ.

Definition 3. *Alice's key is ϵ secret if for all input states ρ_{ABE}, the reduced output state $\tilde{\rho}_{W_A CE}$ is ϵ-close in trace distance to the corresponding ideal state*

$$|\perp\rangle\langle\perp|_{W_A} \otimes \tilde{\rho}_{CE}(\perp) + \sum_w \frac{1}{|W|} |w\rangle\langle w|_{W_A} \otimes (\tilde{\rho}_{CE} - \tilde{\rho}_{CE}(\perp))$$

The following lemma establishes the relation between security and correctness plus secrecy:

Lemma 1. *If a QKD protocol is ϵ secure, then it is ϵ correct and Alice's key is ϵ secret. Conversely, if the protocol is ϵ correct and Alice's key is δ secret, then the protocol is $\epsilon + \delta$ secure.*

Proof. The forward direction follows from monotonicity of the trace distance and its interpretation as distinguishing advantage. The reverse direction follows by considering the hybrid state

$$|\perp\perp\rangle\langle\perp\perp|_{W_A W_B} \otimes \tilde{\rho}_{CE}(\perp) + \sum_w |ww\rangle\langle ww|_{W_A W_B} \otimes \sum_{w'} \tilde{\rho}_{CE}(w, w')$$

and the triangle inequality. □

Next, note that in the standard definition of QKD security (Definition 1) the ideal state, beyond being ϵ close to the real state, satisfies the following additional conditions:

1. The probabilities of accepting and rejecting are the same for the real and ideal state.
2. The real and ideal state differ only in the accept case.
3. The sub-normalized reduced density matrix of registers C, E in the accept case is equal to $\tilde{\rho}_{CE} - \tilde{\rho}_{CE}(\perp)$ for both the real and the ideal state.

Now, suppose an ideal state is found that is ϵ close to the real state, but which does not necessarily satisfy these additional conditions. This suffices to demonstrate security:

Lemma 2. *Suppose that for all input states ρ_{ABE}, there exist positive σ_{CE}^{accept} and σ_{CE}^{reject} such that $Tr(\sigma_{CE}^{accept}) + Tr(\sigma_{CE}^{reject}) = 1$ and such that the output state $\tilde{\rho}_{W_A W_B CE}$ is ϵ-close in trace distance to*

$$|\perp\perp\rangle\langle\perp\perp|_{W_A W_B} \otimes \sigma_{CE}^{reject} + \sum_w \frac{1}{|W|} |ww\rangle\langle ww|_{W_A W_B} \otimes \sigma_{CE}^{accept}$$

Then, the protocol is 2ϵ secure.

Proof. By assumption,

$$\frac{1}{2}\left(\|\tilde{\rho}_{CE}(\perp) - \sigma_{CE}^{reject}\|_1 + \sum_{w_A, w_B} \left\| \tilde{\rho}_{CE}(w_A, w_B) - \frac{1}{|W|} \mathbf{1}(w_A = w_B) \sigma_{CE}^{accept} \right\|_1 \right) \leq \epsilon$$

From the triangle inequality it follows that

$$\frac{1}{2}\left(\|\tilde{\rho}_{CE}(\perp) - \sigma_{CE}^{reject}\|_1 + \left\|\tilde{\rho}_{CE} - \tilde{\rho}_{CE}(\perp) - \sigma_{CE}^{accept}\right\|_1\right) \leq \epsilon$$

The lemma then follows by another application of the triangle inequality. □

Finally, note that a protocol that always aborts is secure, but not useful. For a useful QKD protocol, the probability of acceptance is bounded below by $1-\delta$ for some $\delta \in (0,1)$ on a suitable class of input states. In the present paper, robustness of the two-universal hashing protocol is shown by giving explicit bounds on the probability of acceptance as a function of the input state.

2.2 The Pauli group and the Bell basis

Denote the Pauli matrices by

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

For a row vector $u \in \mathbb{F}_2^{1\times n}$, denote

$$\sigma_1^u = \sigma_1^{u_1} \otimes \ldots \sigma_1^{u_n}, \quad \sigma_3^u = \sigma_3^{u_1} \otimes \cdots \otimes \sigma_3^{u_n}$$

The Pauli group on n qubits is

$$G_n = \{\omega\sigma_1^u\sigma_3^v : \omega \in \{\pm 1, \pm i\}, u, v \in \mathbb{F}_2^{1\times n}\}$$

Matrix multiplication of elements of G_n can be performed in terms of u, v, ω:

$$(\omega\sigma_1^u\sigma_3^v)(\omega'\sigma_1^{u'}\sigma_3^{v'}) = \omega\omega'(-1)^{v\cdot u'}\sigma_1^{u+u'}\sigma_3^{v+v'}$$

This also shows that the map $\mathcal{F} : G_n \to \mathbb{F}_2^{1\times 2n}$ given by

$$\mathcal{F}(\omega\sigma_1^u\sigma_3^v) = \begin{pmatrix} u & v \end{pmatrix}$$

is a group homomorphism.

Any element of the Pauli group squares to either I or $-I$; any two elements g, g' of the Pauli group satisfy

$$gg' = (-1)^{\mathcal{F}(g)\mathcal{S}\mathcal{F}(g')^T} g'g$$

where $\mathcal{S} \in \mathbb{F}_2^{2n\times 2n}$ is the matrix with block form

$$\mathcal{S} = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$$

Say that a tuple of elements of the Pauli group

$$\vec{g} = \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix}$$

is independent if the row vectors $\mathcal{F}(g_i) \in \mathbb{F}_2^{1\times 2n}$ are linearly independent. Given such an independent tuple and given any $x \in \mathbb{F}_2^m$, it is possible to find $g \in G_n$ such that

$$\forall i, \quad g g_i = (-1)^{x_i} g_i g$$

by solving the corresponding linear system of equations over $\mathbb{F}_2$.

A tuple of independent commuting self-adjoint elements of the Pauli group $\vec{g} = (g_1, \dots g_m)^T$ defines a projective measurement on its joint eigenspaces. The measurement outcomes can be indexed by $x \in \mathbb{F}_2^m$ and the corresponding projections are given by

$$P(\vec{g}, x) = 2^{-m} \prod_{j=1}^{m} (I + (-1)^{x_j} g_j)$$

The projections $P(\vec{g}, x)$ form a complete set of orthogonal projections. The elements of the Pauli group map these projections to each other under conjugation, as can be seen from Lemma 3 below. Therefore, the projections $P(\vec{g}, x)$ all have the same rank 2^{n-m}.

Lemma 3. *For all tuples $\vec{g} = (g_1 \dots g_m)^T$ of independent commuting self-adjoint elements of G_n, for all $h \in G_n$, for all $x \in \mathbb{F}_2^m$,*

$$P(\vec{g}, x)h = hP(\vec{g}, x + \mathcal{F}(\vec{g})\mathcal{S}\mathcal{F}(h)^T)$$

where

$$\mathcal{F}(\vec{g}) = \begin{pmatrix} \mathcal{F}(g_1) \\ \vdots \\ \mathcal{F}(g_m) \end{pmatrix}$$

is the matrix with rows $\mathcal{F}(g_1), \dots, \mathcal{F}(g_m)$.

Proof.

$$\begin{aligned} P(\vec{g}, x)h &= 2^{-m} \left(\prod_{j=1}^{m} (I + (-1)^{x_j} g_j) \right) h \\ &= 2^{-m} h \left(\prod_{j=1}^{m} (I + (-1)^{x_j + \mathcal{F}(g_j)\mathcal{S}\mathcal{F}(h)^T} g_j) \right) = hP(\vec{g}, x + \mathcal{F}(\vec{g})\mathcal{S}\mathcal{F}(h)^T) \end{aligned}$$

□

Now, take a tuple $\vec{g}$ of m independent commuting self-adjoint elements, take $k \leq m$ and take a full rank matrix $L \in \mathbb{F}_2^{k\times m}$. The matrix L transforms the tuple $\vec{g}$ to the k-tuple

$$L\vec{g} = L \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} = \begin{pmatrix} \prod_{j=1}^{m} g_j^{L_{1j}} \\ \vdots \\ \prod_{j=1}^{m} g_j^{L_{kj}} \end{pmatrix}$$

The tuple $L\vec{g}$ also consists of independent commuting self-adjoint elements. The transformation of $\vec{g}$ to $L\vec{g}$ satisfies

$$M(L\vec{g}) = (ML)\vec{g}$$

for any $\vec{g}$, L, M of compatible size. The matrix $\mathcal{F}(L\vec{g})$ can be expressed in terms of the matrix $\mathcal{F}(\vec{g})$:

$$\mathcal{F}(L\vec{g}) = \begin{pmatrix} \mathcal{F}(\prod_{j=1}^m g_j^{L_{1j}}) \\ \vdots \\ \mathcal{F}(\prod_{j=1}^m g_j^{L_{kj}}) \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^m L_{1j}\mathcal{F}(g_j) \\ \vdots \\ \sum_{j=1}^m L_{kj}\mathcal{F}(g_j) \end{pmatrix} = L\mathcal{F}(\vec{g})$$

The measurement projections of $L\vec{g}$ can be expressed in terms of the measurement projections of $\vec{g}$.

Lemma 4. *For all $n \geq m \geq k \geq 1$, for all tuples $\vec{g}$ of m independent commuting self-adjoint elements of G_n, for all full rank $L \in \mathbb{F}_2^{k\times m}$, for all $y \in \mathbb{F}_2^k$,*

$$P(L\vec{g}, y) = \sum_{x\in\mathbb{F}_2^m : Lx=y} P(\vec{g}, x)$$

Proof. Take any $i \in \{1, \ldots k\}$, any $x \in \mathbb{F}_2^m$ such that $Lx = y$. Then,

$$\left(\prod_{j=1}^m g_j^{L_{ij}}\right) P(\vec{g}, x) = \left(\prod_{j=1}^m g_j^{L_{ij}}\right) \left(2^{-m} \prod_{j=1}^m (I + (-1)^{x_j} g_j)\right)$$
$$= (-1)^{\sum_{j=1}^m L_{ij}x_j} P(\vec{g}, x) = (-1)^{y_i} P(\vec{g}, x)$$

Then, for any $x \in \mathbb{F}_2^m$ such that $Lx = y$, $P(L\vec{g}, y)P(\vec{g}, x) = P(\vec{g}, x)$ holds. Since $\{P(\vec{g}, x) : Lx = y\}$ is a collection of 2^{m-k} orthogonal projections of rank 2^{n-m} and since $P(L\vec{g}, y)$ has rank 2^{n-k}, the lemma follows. □

The maximally entangled state in $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ is

$$|\psi\rangle = 2^{-n/2} \sum_{z\in\mathbb{F}_2^n} |zz\rangle$$

The collection

$$|\psi_{\alpha\beta}\rangle = I \otimes \sigma_1^{\alpha^T} \sigma_3^{\beta^T} |\psi\rangle, \;\; \alpha, \beta \in \mathbb{F}_2^n$$

is the Bell basis of $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$.

First, the maximally entangled state has the properties:

Lemma 5. *For all matrices $M \in \mathbb{C}^{2^n\times 2^n}$, $M \otimes I|\psi\rangle = I \otimes M^T|\psi\rangle$ and $\langle\psi|I \otimes M|\psi\rangle = 2^{-n}Tr(M)$.*

Proof. Follows by expanding M in the computational basis. □

Pauli group measurements acting on Bell basis states satisfy the following:

Lemma 6. *For all tuples $\vec{g}$ of independent self-adjoint commuting elements of G_n such that the associated projections $P(\vec{g}, x)$ have only real entries when expressed as matrices in the computational basis, for all $\alpha, \beta \in \mathbb{F}_2^n$, for all $x, y \in \mathbb{F}_2^m$,*

$$(P(\vec{g}, x) \otimes P(\vec{g}, y))|\psi_{\alpha\beta}\rangle = \mathbf{1}\left(x = y + \mathcal{F}(\vec{g})\mathcal{S}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right) P(\vec{g}, x) \otimes I|\psi_{\alpha\beta}\rangle$$

where for an expression that takes the values true or false, $\mathbf{1}(expression)$ takes the corresponding values 1 or 0.

Proof. Follows from Lemma 3 and the relation $M \otimes I|\psi\rangle = I \otimes M^T|\psi\rangle$ □

The QKD security proof also uses the following lemma. It gives two equivalent expressions for the projection on the subspace of $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ that corresponds to a specific pattern of bit flip errors or a specific pattern of phase flip errors.

Lemma 7. *For all n, for all $\alpha, \beta \in \mathbb{F}_2^n$,*

$$\sum_{\beta' \in \mathbb{F}_2^n} |\psi_{\alpha\beta'}\rangle\langle\psi_{\alpha\beta'}| = \sum_{z_A \in \mathbb{F}_2^n} |z_A, z_A + \alpha\rangle\langle z_A, z_A + \alpha|$$
$$\sum_{\alpha' \in \mathbb{F}_2^n} |\psi_{\alpha'\beta}\rangle\langle\psi_{\alpha'\beta}| = \sum_{x_A \in \mathbb{F}_2^n} H^{\otimes 2n}|x_A, x_A + \beta\rangle\langle x_A, x_A + \beta|H^{\otimes 2n}$$

Proof. Let $e_1, \ldots e_n$ denote the standard basis of $\mathbb{F}_2^{1\times n}$. For $i \in \{1, 3\}$ and $R \in \{A, B\}$, let $\vec{\sigma}_3^R$ denote the tuple $\sigma_i^{e_1}, \ldots \sigma_i^{e_n}$ acting on register R, and let $\vec{\sigma}_i^{AB}$ denote the tuple $\sigma_i^{e_1} \otimes \sigma_i^{e_1}, \ldots, \sigma_i^{e_n} \otimes \sigma_i^{e_n}$. Note that for all α, β,

$$|\alpha\beta\rangle\langle\alpha\beta|_{AB} = P\left(\begin{pmatrix}\vec{\sigma}_3^A\\ \vec{\sigma}_3^B\end{pmatrix}, \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right) \;;\; |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}| = P\left(\begin{pmatrix}\vec{\sigma}_3^{AB}\\ \vec{\sigma}_1^{AB}\end{pmatrix}, \begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right)$$

The first relation of Lemma 7 now follows from

$$\begin{pmatrix}I & I\end{pmatrix}\begin{pmatrix}\vec{\sigma}_3^A\\ \vec{\sigma}_3^B\end{pmatrix} = \begin{pmatrix}I & 0\end{pmatrix}\begin{pmatrix}\vec{\sigma}_3^{AB}\\ \vec{\sigma}_1^{AB}\end{pmatrix}$$

and Lemma 4. The second relation follows similarly. □

2.3 Approximately computing certain functions from only a two-universal hash of the input

Let $\mathbb{F}_2$ denote the field with two elements and $\mathbb{F}_2^n$ the n-dimensional vector space over this field. Take any subset $S \subset \mathbb{F}_2^n$. Consider the function $f_S : \mathbb{F}_2^n \to S \cup \{\perp\}$ given by

$$f_S(\alpha) = \begin{cases}\alpha & \text{if } \alpha \in S\\ \perp & \text{otherwise}\end{cases}$$

If α specifies errors, then f_S computes whether α belongs to a set S of acceptable errors, if so computes the entire string α, and otherwise outputs an error

message. It is very convenient to have functions of this form when constructing QKD protocols and security proofs.

It turns out that it is possible to approximately compute $f_S(\alpha)$ given only a two universal hash of the input. Recall [5, 22]:

Definition 4. *A family of functions* $\mathbf{H}$ *from finite set* $\mathbf{X}$ *to finite set* $\mathbf{Y}$ *is two-universal with collision probability at most* ϵ *if for all* $x \neq x' \in \mathbf{X}$*,*

$$\Pr_{h \leftarrow \mathbf{H}}(h(x) = h(x')) \leq \epsilon$$

where the probability is taken over h *chosen uniformly from* $\mathbf{H}$*. If no explicit value is specified for the collision probability bound, then the default value* $\epsilon = 1/|\mathbf{Y}|$ *is taken.*

Now, let $\mathbf{H}$ be a two-universal family from $\mathbb{F}_2^n$ to some finite set $\mathbf{Y}$ with collision probability bound ϵ. Let $S = \{s_1, \ldots, s_m\}$. Consider the function $g_S : \mathbf{H} \times \mathbf{Y} \to S \cup \{\perp\}$ given by the deterministic algorithm:

1. On input h, y,
2. For $i = 1, \ldots, m$, if $h(s_i) = y$, output s_i and stop.
3. Output $\perp$.

Then:

Theorem 1. *For all* $n \in \mathbb{N}$*, for all* ϵ*, for all two-universal families* $\mathbf{H} : \mathbb{F}_2^n \to \mathbf{Y}$ *with collision probability bound* ϵ*, for all subsets* $S \subset \mathbb{F}_2^n$*, for all* $\alpha \in \mathbb{F}_2^n$*,*

$$\Pr_{h \leftarrow \mathbf{H}}(f_S(\alpha) \neq g_S(h, h(\alpha))) \leq \epsilon |S|$$

Proof. The event

$$f_S(\alpha) \neq g_S(h, h(\alpha))$$

implies the event

$$\exists s \in S \backslash \{\alpha\} : h(s) = h(\alpha)$$

The union bound and Definition 4 give

$$\Pr_{h \leftarrow \mathbf{H}}(f_S(\alpha) \neq g_S(h, h(\alpha))) \leq \epsilon |S|$$

□

The remainder of this section specializes Theorem 1 to the case that the family $\mathbf{H}$ is a family of matrices over $\mathbb{F}_2$, and the set S is a Hamming Ball.

First, consider the following useful lemmas about random matrices over the field with two elements. Let $\mathbb{F}_2^{n \times k}$ to denote the space of n by k matrices over $\mathbb{F}_2$.

Recall a property of random linear functions that was observed in [5]:

Lemma 8. *Let L be uniformly random in $\mathbb{F}_2^{k\times n}$, and take any fixed $x \in \mathbb{F}_2^n - \{0\}$. Then,* $\Pr_L(Lx = 0) = 2^{-k}$.

Proof. Take i such that $x_i = 1$. Then, $Lx = L_i + L_{-i}x_{-i}$, where L_i is the i-th column of L and where L_{-i}, x_{-i} are formed from L, x by omitting the i-th column and i-th entry respectively. Now, L_i is uniform over $\mathbb{F}_2^k$ and independent from L_{-i}, so Lx is also uniform over $\mathbb{F}_2^k$. □

Thus, for all $y \neq z \in \mathbb{F}_2^n$, $\Pr_L(Ly = Lz) = 2^{-k}$, so random linear functions are two-universal.

Later on, it will be more convenient to select matrices not from all of $\mathbb{F}_2^{k\times n}$, but from the subset consisting of those matrices of rank k. This subset also satisfies the two-universal condition, as the following two lemmas show.

Lemma 9. *For all integers $n \geq k \geq 1$, the number of rank k matrices in $\mathbb{F}_2^{k\times n}$ is $\prod_{i=1}^{k}(2^n - 2^{i-1})$*

Proof. Given $i-1$ linearly independent rows, there are $2^n - 2^{i-1}$ ways to choose the i-th row outside their span. □

Lemma 10. *Take $k \leq n$, let L be a uniformly random rank k matrix in $\mathbb{F}_2^{k\times n}$ and take any $x \in \mathbb{F}_2^n - \{0\}$. Then* $\Pr_L(Lx = 0) = \frac{2^{n-k}-1}{2^n-1} < 2^{-k}$

Proof. Take invertible $M \in \mathbb{F}_2^{n\times n}$ such that $Mx = (1, 0, \ldots, 0)^T$. Then $\Pr(Lx = 0) = \Pr(LM^{-1}Mx = 0)$. Now, find the probability that the first column of LM^{-1} is zero. Note that LM^{-1} is also uniformly distributed over the rank k matrices in $\mathbb{F}_2^{k\times n}$, so the probability its first column is zero is the number of rank k matrices in $\mathbb{F}_2^{k\times(n-1)}$ divided by the number of rank k matrices in $\mathbb{F}_2^{k\times n}$. Lemma 9 implies:

$$\Pr(LM^{-1}Mx = 0) = \frac{\prod_{i=1}^{k}(2^{n-1} - 2^{i-1})}{\prod_{i=1}^{k}(2^n - 2^{i-1})} = \frac{2^{n-k} - 1}{2^n - 1} < 2^{-k}$$

completing the proof of Lemma 10. □

Interestingly, the collision probability bound $\epsilon = \frac{2^{n-k}-1}{2^n-1}$ achieved by the full rank matrices is the lowest possible for a two-universal family $\mathbb{F}_2^n \to \mathbb{F}_2^k$. This follows from a slight strengthening of [5, Proposition 1]:

Lemma 11. *For every family $\mathbf{H}$ (not necessarily two-universal) of functions from finite set $\mathbf{X}$ to finite set $\mathbf{Y}$, there exist $x \neq x' \in \mathbf{X}$ such that*

$$\Pr_{h\leftarrow\mathbf{H}}(h(x) = h(x')) \geq \frac{\frac{|\mathbf{X}|}{|\mathbf{Y}|} - 1}{|\mathbf{X}| - 1}$$

Proof. Follow the same proof as [5] until the point they apply the pigeonhole principle. At that point, observe that the number of non-zero terms in the sum is not only less than $|\mathbf{X}|^2$, as they say there, but is in fact at most $|\mathbf{X}|(|\mathbf{X}| - 1)$.

In more detail, for $h \in \mathbf{H}, x, x' \in \mathbf{X}$, define

$$\delta_h(x, x') = \begin{cases} 1 & \text{if } x \neq x' \wedge h(x) = h(x') \\ 0 & \text{otherwise} \end{cases}$$

For every $h \in \mathbf{H}$ partition $\mathbf{X} = \cup_{y \in \mathbf{Y}} h^{-1}(y)$ then observe that

$$\sum_{x,x' \in \mathbf{X}} \delta_h(x, x') = \sum_{y \in \mathbf{Y}} |h^{-1}(y)|(|h^{-1}(y)| - 1) \geq \frac{|\mathbf{X}|^2}{|\mathbf{Y}|} - |\mathbf{X}|$$

by the quadratic mean-arithmetic mean inequality. Now, sum over $h \in \mathbf{H}$:

$$\sum_{h \in \mathbf{H}} \sum_{x,x' \in \mathbf{X}} \delta_h(x, x') = \sum_{x,x' \in \mathbf{X}} \sum_{h \in \mathbf{H}} \delta_h(x, x') \geq |\mathbf{H}|(\frac{|\mathbf{X}|^2}{|\mathbf{Y}|} - |\mathbf{X}|)$$

Now, $\sum_{h \in \mathbf{H}} \delta_h(x, x')$ is non-zero only when $x \neq x'$. Then, there exist $x \neq x'$ such that

$$\sum_{h \in \mathbf{H}} \delta_h(x, x') \geq |\mathbf{H}| \frac{\frac{|\mathbf{X}|}{|\mathbf{Y}|} - 1}{|\mathbf{X}| - 1}$$

□

Later results will also use the fact that a row submatrix of a random invertible matrix has the uniform distribution over full rank matrices:

Lemma 12. *Take any integers $n \geq k \geq 1$, and any $S \subset \{1, \ldots, n\}$ of size k. Let L be uniformly distributed over invertible matrices in $\mathbb{F}_2^{n \times n}$. Let L_S denote the matrix formed by rows of L with indices in S. Then, L_S is uniformly distributed over full rank matrices in $\mathbb{F}_2^{k \times n}$.*

Proof. Pick any fixed full rank $\Lambda \in \mathbb{F}_2^{k \times n}$. Compute $\Pr(L_S = \Lambda)$ as the number of ways to choose the remaining rows of L, which is $\prod_{i=1}^{n-k}(2^n - 2^{k+i-1})$ divided by the number of invertible matrices in $\mathbb{F}_2^{n \times n}$, which is $\prod_{i=1}^{n}(2^n - 2^{i-1})$. Thus,

$$\Pr(L_S = \Lambda) = \frac{\prod_{i=1}^{n-k}(2^n - 2^{k+i-1})}{\prod_{i=1}^{n}(2^n - 2^{i-1})} = \frac{1}{\prod_{i=1}^{k}(2^n - 2^{i-1})}$$

Thus, L_S is uniform over the full rank matrices in $\mathbb{F}_2^{k \times n}$. □

Applying Theorem 1 when the set S is a Hamming ball requires a bound on the size of Hamming balls. For $x, y \in \mathbb{F}_2^n$, let $d_H(x, y) = |\{i : x_i \neq y_i\}|$ denote the Hamming distance between them. Let $B_n(x, r)$ denote the Hamming ball of radius r around x. Then:

Lemma 13. *For all $n, r \in \mathbb{N}$ such that $2r \leq n$, for all $x \in \mathbb{F}_2^n$, $|B_n(x, r)| < 2^{nh(r/n)}$*

Proof.

$$|B_n(x,r)|2^{-nh(r/n)} = \sum_{i=0}^{r} \binom{n}{i} \left(\frac{r}{n}\right)^r \left(\frac{n-r}{n}\right)^{n-r}$$
$$\leq \sum_{i=0}^{r} \binom{n}{i} \left(\frac{r}{n}\right)^i \left(\frac{n-r}{n}\right)^{n-i} < \sum_{i=0}^{n} \binom{n}{i} \left(\frac{r}{n}\right)^i \left(\frac{n-r}{n}\right)^{n-i} = 1$$

□

From Theorem 1, Lemma 10 and Lemma 13 deduce:

Corollary 1. *For all $n, k, r \in \mathbb{N}$ with $2r \leq n$ and $k \leq n$, for all $\alpha \in \mathbb{F}_2^n$,*

$$\Pr_L(f_{B_n(0,r)}(\alpha) \neq g_{B_n(0,r)}(L, L\alpha)) < 2^{-k+nh(r/n)}$$

where L is chosen uniformly from the full rank matrices in $\mathbb{F}_2^{k\times n}$.

3 The two-universal hashing QKD protocol and its security

Consider the following family $\pi(n,k,r)$ of entanglement-based QKD protocols, parameterized by $n, k, r \in \mathbb{N}$. The interpretation of the parameters is the following: n is the number of qubits that each of Alice and Bob receive, k is the size of each of their syndrome measurements and $n-2k$ is the size of their output secret key, and r is the maximum number of bit flip or phase flip errors on which the protocol does not abort. The protocols output a secret key with security guarantees when $2nh(r/n) < 2k < n$.

It will be clear throughout that the size of the two syndrome measurements can vary independently, and so can the maximum number of tolerated bit flip and phase flip errors, but that would lead to overly complex notation, with five parameters n, k, k', r, r', so it is not pursued explicitly below.

1. Alice and Bob each receive an n qubit state from Eve, and they inform each other that the states have been received.

2. Alice and Bob publicly choose a random invertible $L \in \mathbb{F}_2^{n\times n}$. Let L_1, L_2, L_3 be the matrices formed by the first k rows, the second k rows, and the last $n-2k$ rows of L. Let $M = (L^{-1})^T$, and let M_1, M_2, M_3 be the matrices formed by the first k, second k, and last $n-2k$ rows of M. L_1, M_2 are the parity check matrices of a CSS code. L_3, M_3 contain information about the logical Z and X operators on the codespace.

3. Alice applies the isometry $\sum_z |z, L_1 z\rangle_{AU'_A} \langle z|_A$ and Bob applies the isometry $\sum_z |z, L_1 z\rangle_{BU'_B} \langle z|_B$. This can be done by preparing k ancilla qubits in state 0 and applying a CNOT gate for each entry $L_1(i,j)$ that equals 1.

4. Alice and Bob measure all qubits in registers A, B in the $|+\rangle, |-\rangle$ basis, obtaining outcomes x_A, x_B. Alice and Bob measure all qubits in registers U'_A, U'_B in the computational basis, obtaining outcomes u_A, u_B.

5. Alice and Bob compute $v_A = M_2 x_A$, $v_B = M_2 x_b$, $w_A = M_3 x_A$, $w_B = M_3 x_B$.

6. Alice and Bob discard registers A, B, U'_A, U'_B.

7. Alice and Bob discard x_A, x_B, keeping only v_A, v_B, w_A, w_B. Thus, in effect, Alice and Bob erase $M_1 x_A, M_1 x_B$. Note that the post measurement states in registers A, B, as well as x_A, x_B have to be discarded in such a way that Eve cannot get them.

8. Alice and Bob announce u_A, u_B, v_A, v_B. Alice and Bob compute $s = g_{B_n(0,r)}(L_1, u_A + u_B)$ and $t = g_{B_n(0,r)}(M_2, v_A + v_B)$.

9. If both of these are not $\perp$, then Alice takes w_A to be the output secret key, and Bob takes $w_B + M_3 t$ to be the output secret key.

As is usual in the literature on QKD, the protocol assumes that classical communication takes place over an authenticated channel. Unconditionally secure message authentication with composable security in the Abstract Cryptography framework can be obtained from a short secret key [14], or using an advantage in channel noise [12].

If it is desired that the classical communication is minimized, then the following exchange of messages suffices: Bob confirms to Alice that he has received the qubits, Alice sends to Bob L, u_A, v_A, Bob informs Alice whether both of s, t are not $\perp$. However, the initial formulation above better emphasizes the symmetry of the protocol, and makes clear that it is not important to keep the values u_B, v_B, s, t secret.

The following theorem establishes the security and robustness of the protocols $\pi(n, k, r)$.

Theorem 2. *Take any $n, k, r \in \mathbf{N}$ such that $2nh(r/n) < 2k < n$. Then, the protocol $\pi(n, k, r)$ is $2^{-k/2+nh(r/n)/2+5/2}$ secure.*

Moreover, for any input state ρ_{AB}, the probability that $\pi(n, k, r)$ accepts on input ρ_{AB} is $2^{-k/2+nh(r/n)/2+3/2}$ close to $Tr(\Pi_{n,r}\rho_{AB}\Pi_{n,r})$, where $\Pi_{n,r}$ is the projection on the subspace of systems AB spanned by the Bell states with at most r bit flip and at most r phase flip errors.

3.1 Proof of Theorem 2

The main idea of the proof of Theorem 2 is that the real values $g_{B_n(0,r)}(L_1, u_A + u_B)$ and $g_{B_n(0,r)}(M_2, v_A + v_B)$ computed during the protocol can be replaced by the corresponding ideal values $f_{B_n(0,r)}(\alpha), f_{B_n(0,r)}(\beta)$. From now on, use shorthand notation and skip the subscript $B_n(0, r)$, thus writing f for $f_{B_n(0,r)}$ and g for $g_{B_n(0,r)}$.

The steps of the proof of Theorem 2 are the propositions below. Start by writing the action of the protocol as an isometry followed by a partial trace.

Proposition 1. *Let $\mathcal{E}_{real}$ be the completely positive trace preserving transformation applied by the first eight steps of the protocol. Then, for all input states ρ_{ABE} to the protocol, the output state $\mathcal{E}_{real}(\rho_{ABE})$ of the classical registers $\mathbf{L}, U_A, U_B, V_A, V_B, W_A, W_B, S, T$ and the quantum register of Eve equals*

$$Tr_{AB\mathbf{L}'S'T'U'_AU'_BV'_AV'_BW'_AW'_B}\mathcal{W}\mathcal{V}_{real}\mathcal{U}_{real}\left(\rho\otimes|\mathcal{L}\rangle\langle\mathcal{L}|\right)\mathcal{U}^{\dagger}_{real}\mathcal{V}^{\dagger}_{real}\mathcal{W}^{\dagger}$$

where

$$|\mathcal{L}\rangle=\sum_{L}\sqrt{p_L}|LL\rangle_{\mathbf{L}\mathbf{L}'}$$

is a purification of the choice of random matrix L, where

$$\mathcal{U}_{Real}=\sum_{L,z_A,z_B}|L\rangle\langle L|_{\mathbf{L}}\otimes|z_Az_B\rangle\langle z_Az_B|_{AB}$$
$$\otimes|L_1z_A,L_1z_A,L_1z_B,L_1z_B,g(L_1,L_1(z_A{+}z_B)),g(L_1,L_1(z_A{+}z_B))\rangle_{U_AU'_AU_BU'_BSS'}$$

is an isometry that captures the measurement through which Alice and Bob obtain the values $u_A=L_1z_A$ and $u_B=L_1z_B$ as well as the subsequent computation of the value $s=g(L_1,L_1(z_A+z_B))$, where

$$\mathcal{V}_{Real}=\sum_{L,x_A,x_B}|L\rangle\langle L|_{\mathbf{L}}\otimes\left(H^{\otimes 2n}|x_Ax_B\rangle\langle x_Ax_B|H^{\otimes 2n}\right)_{AB}$$
$$\otimes|M_2x_A,M_2x_A,M_2x_B,M_2x_B,g(M_2,M_2(x_A{+}x_B)),g(M_2,M_2(x_A{+}x_B))\rangle_{V_AV'_AV_BV'_BTT'}$$

is an isometry that captures the measurement through which Alice and Bob obtain the values $v_A=M_2x_A$ and $v_B=M_2x_B$ as well as the subsequent computation of the value $t=g(M_2,M_2(x_A+x_B))$ and where

$$\mathcal{W}=\sum_{L,x_A,x_B}|L\rangle\langle L|_{\mathbf{L}}\otimes\left(H^{\otimes 2n}|x_Ax_B\rangle\langle x_Ax_B|H^{\otimes 2n}\right)_{AB}$$
$$\otimes|M_3x_A,M_3x_A,M_3x_B,M_3x_B\rangle_{W_AW'_AW_BW'_B}$$

is an isometry that captures the measurement through which Alice and Bob obtain the values $w_A=M_3x_A$ and $w_B=M_3x_B$.

Proof. Recall the Stinespring dilation theorem [19]. Systematically express each step of the protocol as an isometry followed by a partial trace.

The step in which Alice and Bob choose the random matrix L can be expressed as preparing the purification $|\mathcal{L}\rangle_{\mathbf{L}\mathbf{L}'}$ and then taking $Tr_{\mathbf{L}'}$.

The steps in which Alice and Bob apply the isometry

$$\sum_{z_A,z_B}|z_A,z_B,L_1z_A,L_1z_B\rangle_{ABU'_AU'_B}\langle z_A,z_B|_{AB}$$

then measure registers U'_A, U'_B in the computational basis, discarding the post-measurement state and keeping only the outcome, then compute the value s can be expressed by the isometry $\mathcal{U}_{real}$ followed by $Tr_{S'U'_AU'_B}$.

The steps in which Alice and Bob measure the qubits in A, B in the $|+\rangle, |-\rangle$ basis obtaining x_A, x_B, then compute v_A, v_B, w_A, w_B, t, then discard the post-measurement state of the qubits in A, B and the outcomes x_A, x_B can be expressed by the product of isometries $\mathcal{WV}_{real}$ followed by $Tr_{ABT'V'_AV'_BW'_AW'_B}$.

Finally, note that all the partial trace operations can be commuted to the end. □

Next, note that $\mathcal{U}_{real}$ can be approximated by an ideal isometry followed by a simulator isometry.

Proposition 2. *Let*

$$\mathcal{U}_{ideal} = \sum_{\alpha,\beta} |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|_{AB} \otimes |f(\alpha), f(\alpha)\rangle_{SS'}$$

This ideal isometry computes whether the number of bit flip errors is acceptable and if so it computes the entire string of bit flip error positions.

Let

$$\mathcal{U}_{simulator} = \sum_{L,z_A,z_B} |L\rangle\langle L|_{\mathbf{L}} \otimes |z_Az_B\rangle\langle z_Az_B|_{AB} \otimes |L_1z_A, L_1z_A, L_1z_B, L_1z_B\rangle_{U_AU'_AU_BU'_B}$$

This isometry captures the measurement through which Alice and Bob obtain the values $u_A = L_1z_A$ and $u_B = L_1z_B$.

Then:

$$\left(\langle\mathcal{L}|\mathcal{U}^\dagger_{ideal}\mathcal{U}^\dagger_{simulator}\right)(\mathcal{U}_{real}|\mathcal{L}\rangle) \geq (1 - 2^{-k+nh(r/n)})I_{AB}$$

Proof. Simplify:

$$\mathcal{U}^\dagger_{simulator}\mathcal{U}_{real} = \sum_{L,z_A,z_B} |L\rangle\langle L|_{\mathbf{L}} \otimes |z_Az_B\rangle\langle z_Az_B|_{AB} \otimes |g(L_1, L_1(z_A + z_B)), g(L_1, L_1(z_A + z_B))\rangle_{SS'}$$

Therefore,

$$\left(\langle\mathcal{L}|\mathcal{U}^\dagger_{ideal}\mathcal{U}^\dagger_{simulator}\right)(\mathcal{U}_{real}|\mathcal{L}\rangle) = \sum_{L,z_A,z_B,\alpha,\beta} p_L|\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|_{AB}|z_Az_B\rangle\langle z_Az_B|_{AB}\langle f(\alpha)|g(L_1, L_1(z_A + z_B))\rangle_S$$

Now, apply Lemma 7:

$$\sum_{L,z_A,z_B,\alpha} p_L \left(\sum_{\beta} |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|_{AB} \right) |z_A z_B\rangle\langle z_A z_B|_{AB} \langle f(\alpha)|g(L_1, L_1(z_A{+}z_B))\rangle_S$$

$$= \sum_{L,z_A,z_B,\alpha,z'_A} p_L |z'_A, z'_A{+}\alpha\rangle\langle z'_A, z'_A{+}\alpha|_{AB} |z_A z_B\rangle\langle z_A z_B|_{AB} \langle f(\alpha)|g(L_1, L_1(z_A{+}z_B))\rangle_S$$

$$= \sum_{z_A,z_B} |z_A z_B\rangle\langle z_A z_B|_{AB} \sum_L p_L \langle f(z_A + z_B)|g(L_1, L_1(z_A + z_B))\rangle$$

$$= \sum_{z_A,z_B} |z_A z_B\rangle\langle z_A z_B|_{AB} \Pr_L(f(z_A + z_B) = g(L_1, L_1(z_A + z_B)))$$

Now, the marginal distribution of L_1 is uniform over the rank k matrices in $\mathbb{F}_2^{k\times n}$ because L is selected uniformly among invertible matrices in $\mathbb{F}_2^{n\times n}$ (Lemma 12). Complete the proof of Proposition 2 by applying Corollary 1. □

Next, perform the same approximation for $\mathcal{V}_{real}$.

Proposition 3. *Let*

$$\mathcal{V}_{ideal} = \sum_{\alpha,\beta} |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|_{AB} \otimes |f(\beta), f(\beta)\rangle_{TT'}$$

This ideal isometry computes whether the number of phase flip errors is acceptable and if so it computes the entire string of phase flip error positions.

Let

$$\mathcal{V}_{simulator} = \sum_{L,x_A,x_B} |L\rangle\langle L|_{\mathbf{L}} \otimes \left(H^{\otimes 2n}|x_A x_B\rangle\langle x_A x_B|H^{\otimes 2n}\right)_{AB} \otimes |M_2 x_A, M_2 x_A, M_2 x_B, M_2 x_B\rangle_{V_A V'_A V_B V'_B}$$

This isometry captures the measurement through which Alice and Bob obtain the values $v_A = M_2 x_A$ and $v_B = M_2 x_B$.

Then:

$$\left(\langle\mathcal{L}|\mathcal{V}_{ideal}^\dagger \mathcal{V}_{simulator}^\dagger\right)(\mathcal{V}_{real}|\mathcal{L}\rangle) \geq (1 - 2^{-k+nh(r/n)}) I_{AB}$$

Proof. As in the proof of Proposition 2, use Lemma 7 to compute

$$\left(\langle\mathcal{L}|\mathcal{V}_{ideal}^\dagger \mathcal{V}_{simulator}^\dagger\right)(\mathcal{V}_{real}|\mathcal{L}\rangle)$$

$$= \sum_{x_A,x_B} \left(H^{\otimes 2n}|x_A x_B\rangle\langle x_A x_B|H^{\otimes 2n}\right)_{AB} \Pr_L(f(x_A{+}x_B) = g(M_2, M_2(x_A{+}x_B)))$$

Now, $M = (L^{-1})^T$ is uniformly distributed over invertible matrices in $\mathbb{F}_2^{n\times n}$, so Lemma 12 and Corollary 1 complete the proof. □

Next, observe that:

Proposition 4. $\mathcal{U}_{simulator}\mathcal{V}_{real} = \mathcal{V}_{real}\mathcal{U}_{simulator}$

Proof. Rewrite:

$$\begin{aligned}\mathcal{U}_{simulator} &= \sum_{L,z_A,z_B} |L\rangle\langle L|_{\mathbf{L}} \otimes |z_A z_B\rangle\langle z_A z_B|_{AB} \otimes |L_1 z_A, L_1 z_A, L_1 z_B, L_1 z_B\rangle_{U_A U'_A U_B U'_B} \\ &= \sum_{L,u_A,u_B} |L\rangle\langle L|_{\mathbf{L}} \otimes |u_A, u_A, u_B, u_B\rangle_{U_A U'_A U_B U'_B} \\ &\quad \otimes \left(\sum_{z_A : L_1 z_A = u_A} |z_A\rangle\langle z_A|\right)_A \otimes \left(\sum_{z_B : L_1 z_B = u_B} |z_B\rangle\langle z_B|\right)_B \\ &= \sum_{L,u_A,u_B} |L\rangle\langle L|_{\mathbf{L}} \otimes |u_A, u_A, u_B, u_B\rangle_{U_A U'_A U_B U'_B} \otimes P(L_1(\vec{\sigma}_3), u_A)_A \otimes P(L_1(\vec{\sigma}_3), u_B)_B\end{aligned}$$

where the last step uses Lemma 4 and the notation of Section 2.2 for the tuple $\vec{\sigma}_3$ of single qubit σ_3 operations.

Similarly, rewrite

$$\begin{aligned}\mathcal{V}_{Real} &= \sum_{L,x_A,x_B} |L\rangle\langle L|_{\mathbf{L}} \otimes \left(H^{\otimes 2n}|x_A x_B\rangle\langle x_A x_B|H^{\otimes 2n}\right)_{AB} \\ &\otimes |M_2 x_A, M_2 x_A, M_2 x_B, M_2 x_B, g(M_2, M_2(x_A + x_B)), g(M_2, M_2(x_A + x_B))\rangle_{V_A V'_A V_B V'_B T T'} \\ &= \sum_{L,v_A,v_B} |L\rangle\langle L|_{\mathbf{L}} \otimes P(M_2(\vec{\sigma}_1), v_A)_A \otimes P(M_2(\vec{\sigma}_1), v_B)_B \\ &\quad \otimes |v_A, v_A, v_B, v_B, g(M_2, v_A + v_B), g(M_2, v_A + v_B\rangle_{V_A V'_A V_B V'_B T T'}\end{aligned}$$

where $\vec{\sigma}_1$ is the tuple of single qubit σ_1 operations.

Proposition 4 now follows by observing that the elements of the two tuples $L_1(\vec{\sigma}_3)$ and $M_2(\vec{\sigma}_1)$ commute and therefore for all u, v, the corresponding projections $P(L_1(\vec{\sigma}_3), u)$ and $P(M_2(\vec{\sigma}_1), v)$ also commute. □

Next, use propositions 1, 2, 3, 4 to construct an ideal transformation that approximates $\mathcal{E}_{real}$:

Proposition 5. *Let $\mathcal{E}_{ideal}$ be the transformation that prepares $|\mathcal{L}\rangle$, then applies isometries $\mathcal{U}_{ideal}$, $\mathcal{V}_{ideal}$, $\mathcal{V}_{simulator}$, $\mathcal{U}_{simulator}$, $\mathcal{W}$, and finally applies $Tr_{AB\mathbf{L}'S'T'U'_A U'_B V'_A V'_B W'_A W'_B}$. Then, the diamond distance of $\mathcal{E}_{real}$ and $\mathcal{E}_{ideal}$ is at most $2^{-k/2+nh(r/n)/2+3/2}$.*

Proof. Take any input state ρ_{ABE} and purify it to $|\phi\rangle_{ABEE'}$. From Proposition 2 deduce that the fidelity of $\mathcal{V}_{real}\mathcal{U}_{simulator}\mathcal{U}_{ideal}|\phi\rangle|\mathcal{L}\rangle$ and $\mathcal{V}_{real}\mathcal{U}_{real}|\phi\rangle|\mathcal{L}\rangle$ is at least $1 - 2^{-k+nh(r/n)}$. Using the relation of fidelity and trace distance for pure states [11, Equation 9.99], the trace distance between these two states is

$$\sqrt{1 - (1 - 2^{-k+nh(r/n)})^2} \leq 2^{-k/2+nh(r/n)/2+1/2}$$

Next, from Proposition 4 deduce

$$\mathcal{V}_{real}\mathcal{U}_{simulator}\mathcal{U}_{ideal}|\phi\rangle|\mathcal{L}\rangle = \mathcal{U}_{simulator}\mathcal{V}_{real}\mathcal{U}_{ideal}|\phi\rangle|\mathcal{L}\rangle$$

Next, from Proposition 3 deduce that the fidelity of $\mathcal{U}_{simulator}\mathcal{V}_{real}\mathcal{U}_{ideal}|\phi\rangle|\mathcal{L}\rangle$ and $\mathcal{U}_{simulator}\mathcal{V}_{simulator}\mathcal{V}_{ideal}\mathcal{U}_{ideal}|\phi\rangle|\mathcal{L}\rangle$ is at least $1-2^{-k+nh(r/n)}$, so the trace distance between them is at most $2^{-k/2+nh(r/n)/2+1/2}$. Finally, from Proposition 1, the triangle inequality and monotonicity of the trace distance deduce that the trace distance between $\mathcal{E}_{real}(\rho)$ and $\mathcal{E}_{ideal}(\rho)$ is at most $2^{-k/2+nh(r/n)/2+3/2}$. □

Next, compute the output state of $\mathcal{E}_{ideal}$:

Proposition 6. *Take any input state ρ_{ABE} and purify it to $|\phi\rangle_{ABEE'}$. Expand ϕ in the Bell basis for Alice and Bob:*

$$|\phi\rangle_{ABEE'} = \sum_{\alpha,\beta\in\mathbb{F}_2^n} |\psi_{\alpha\beta}\rangle_{AB} \otimes |\gamma_{\alpha\beta}\rangle_{EE'}$$

where $|\gamma_{\alpha\beta}\rangle$ are vectors in Eve's space that satisfy

$$\sum_{\alpha,\beta\in\mathbb{F}_2^n} \langle\gamma_{\alpha\beta}|\gamma_{\alpha\beta}\rangle = 1$$

Then, there exists $\sigma^{reject}_{LEE'STU_AV_AW_AU_BV_BW_B}$ that is classical on registers $LSTU_AV_AW_AU_BV_BW_B$ and such that at least one of ST contains $\perp$ and such that

$$\begin{aligned}\mathcal{E}_{ideal}(|\phi\rangle\langle\phi|) &= \sigma^{reject}_{LEE'STU_AV_AW_AU_BV_BW_B} \\ &+ \sum_{L,u_A,v_A,w_A,\alpha,\beta:\alpha,\beta\in B_n(0,r)} p_L|L\rangle\langle L|_{\mathbf{L}} \otimes |\gamma_{\alpha\beta}\rangle\langle\gamma_{\alpha\beta}|_{EE'} \otimes |\alpha,\beta\rangle\langle\alpha,\beta|_{ST} \\ &\otimes 2^{-n}|u_A,v_A,w_A\rangle\langle u_A,v_A,w_A|_{U_AV_AW_A} \\ &\otimes |u_A+L_1\alpha, v_A+M_2\beta, w_A+M_3\beta\rangle\langle u_A+L_1\alpha, v_A+M_2\beta, w_A+M_3\beta|_{U_BV_BW_B}\end{aligned}$$

Proof. Simplify:

$$\mathcal{V}_{ideal}\mathcal{U}_{ideal} = \sum_{\alpha,\beta} |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}| \otimes |f(\alpha), f(\alpha), f(\beta), f(\beta)\rangle_{SS'TT'}$$

Also,

$$\begin{aligned}\mathcal{W}\mathcal{V}_{simulator}\mathcal{U}_{simulator} = &\sum_{L,u_A,u_B,v_A,v_B,w_A,w_B} |L\rangle\langle L|_{\mathbf{L}} \\ &\otimes P\left(\begin{pmatrix} L_1\vec{\sigma}_3 \\ M_2\vec{\sigma}_1 \\ M_3\vec{\sigma}_1 \end{pmatrix}, \begin{pmatrix} u_A \\ v_A \\ w_A \end{pmatrix}\right)_A \otimes P\left(\begin{pmatrix} L_1\vec{\sigma}_3 \\ M_2\vec{\sigma}_1 \\ M_3\vec{\sigma}_1 \end{pmatrix}, \begin{pmatrix} u_B \\ v_B \\ w_B \end{pmatrix}\right)_B \\ \otimes|u_A,u_A,u_B,u_B,v_A,v_A,v_B,v_B,w_A,w_A,w_B,w_B\rangle&_{U_AU'_AU_BU'_BV_AV'_AV_BV'_BW_AW'_AW_BW'_B}\end{aligned}$$

using the notation of section 2.2, the observation that the elements of the three tuples $L_1\vec{\sigma}_3, M_2\vec{\sigma}_1, M_3\vec{\sigma}_1$ are independent and commute, and Lemma 4.

Next, use Lemma 6 to deduce that

$$\begin{aligned}
&\mathcal{WV}_{simulator}\mathcal{U}_{simulator}\mathcal{V}_{ideal}\mathcal{U}_{ideal}|\phi\rangle|\mathcal{L}\rangle \\
&= \sum_{L,u_A,v_A,w_A,\alpha,\beta} \sqrt{p_L}|L,L\rangle_{\mathbf{LL}'} \otimes P\left(\begin{pmatrix} L_1\vec{\sigma}_3 \\ M_2\vec{\sigma}_1 \\ M_3\vec{\sigma}_1 \end{pmatrix}, \begin{pmatrix} u_A \\ v_A \\ w_A \end{pmatrix}\right)_A |\psi_{\alpha\beta}\rangle_{AB} \otimes |\gamma_{\alpha\beta}\rangle_{EE'} \\
&\otimes |u_A, u_A, u_A + L_1\alpha, u_A + L_1\alpha\rangle_{U_AU'_AU_BU'_B} \\
&\otimes |v_A, v_A, v_A + M_2\beta, v_A + M_2\beta\rangle_{V_AV'_AV_BV'_B} \\
&\otimes |w_A, w_A, w_A + M_3\beta, w_A + M_3\beta\rangle_{W_AW'_AW_BW'_B} \\
&\otimes |f(\alpha), f(\alpha), f(\beta), f(\beta)\rangle_{SS'TT'}
\end{aligned}$$

Next, break this up into a sum of two sub-normalized vectors $|\tau_{accept}\rangle$ and $|\tau_{reject}\rangle$, where $|\tau_{accept}\rangle$ contains those terms of the sum with $\alpha, \beta \in B_n(0,r)$ and $|\tau_{reject}\rangle$ contains all other terms of the sum. Note that $Tr_{S'T'}|\tau_{accept}\rangle\langle\tau_{reject}| = 0$ and deduce

$$\begin{aligned}
\mathcal{E}^{ideal}(|\phi\rangle\langle\phi|) = &Tr_{AB\mathbf{L}'S'T'U'_AU'_BV'_AV'_BW'_AW'_B}|\tau_{accept}\rangle\langle\tau_{accept}| \\
&+ Tr_{AB\mathbf{L}'S'T'U'_AU'_BV'_AV'_BW'_AW'_B}|\tau_{reject}\rangle\langle\tau_{reject}|
\end{aligned}$$

Take

$$\sigma^{reject}_{LEE'STU_AV_AW_AU_BV_BW_B} = Tr_{AB\mathbf{L}'S'T'U'_AU'_BV'_AV'_BW'_AW'_B}|\tau_{reject}\rangle\langle\tau_{reject}|$$

Finally, simplify and use Lemma 5 to deduce that

$$\begin{aligned}
&Tr_{AB\mathbf{L}'S'T'U'_AU'_BV'_AV'_BW'_AW'_B}|\tau_{accept}\rangle\langle\tau_{accept}| \\
&= \sum_{L,u_A,v_A,w_A,\alpha,\beta:\alpha,\beta\in B_n(0,r)} p_L|L\rangle\langle L|_{\mathbf{L}} \\
&\otimes |\gamma_{\alpha\beta}\rangle\langle\gamma_{\alpha\beta}|_{EE'} \left(\langle\psi_{\alpha\beta}|P\left(\begin{pmatrix} L_1\vec{\sigma}_3 \\ M_2\vec{\sigma}_1 \\ M_3\vec{\sigma}_1 \end{pmatrix}, \begin{pmatrix} u_A \\ v_A \\ w_A \end{pmatrix}\right)_A |\psi_{\alpha\beta}\rangle\right) \\
&\otimes |u_A, v_A, w_A\rangle\langle u_A, v_A, w_A|_{U_AV_AW_A} \\
&\otimes |u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta\rangle\langle u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta|_{U_BV_BW_B} \\
&\otimes |\alpha,\beta\rangle\langle\alpha,\beta|_{ST} \\
&= \sum_{L,u_A,v_A,w_A,\alpha,\beta:\alpha,\beta\in B_n(0,r)} p_L|L\rangle\langle L|_{\mathbf{L}} \otimes |\gamma_{\alpha\beta}\rangle\langle\gamma_{\alpha\beta}|_{EE'} \otimes |\alpha,\beta\rangle\langle\alpha,\beta|_{ST} \\
&\otimes 2^{-n}|u_A, v_A, w_A\rangle\langle u_A, v_A, w_A|_{U_AV_AW_A} \\
&\otimes |u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta\rangle\langle u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta|_{U_BV_BW_B}
\end{aligned}$$

which completes the proof. □

Finally, note that for any input state ρ_{ABE}, applying the final step of the protocol (the correction of w_B) to $\mathcal{E}_{ideal}(\rho)$ produces an ideal state that satisfies the assumptions of Lemma 2 with $\epsilon = 2^{-k/2+nh(r/n)/2+3/2}$; therefore the protocol is $2^{-k/2+nh(r/n)/2+5/2}$ secure. Moreover, for any input $\rho_{ABE} = Tr_{E'}|\phi\rangle\langle\phi|_{ABEE'}$, the probability that the protocol accepts is within $2^{-k/2+nh(r/n)/2+3/2}$ of

$$\sum_{\alpha,\beta \in B_n(0,r)} \langle\gamma_{\alpha\beta}|\gamma_{\alpha\beta}\rangle = Tr\Pi_{n,r}\rho_{AB}\Pi_{n,r}$$

This completes the proof of Theorem 2.

4 Comparison with previous work

The introduction illustrated the advantage of two-universal hashing over random sampling using specific examples. This section reveals the general pattern behind the examples in the introduction. To study the advantage of the two-universal hashing protocol for all block sizes, fix values for the tolerated error rate and security level, and consider key rate as a function of block size. How fast does key rate converge to the asymptotic value as block size goes to infinity? Subsection 4.1 gives the rate of convergence for the two-universal hashing protocol. Subsection 4.2 gives a bound on the rate of convergence of the random sampling protocol.

4.1 Key rate of the two-universal hashing protocols $\pi(n, k, r)$

Given n qubits per side, the target to tolerate δn bit flip and δn phase flip errors, and a target security parameter ϵ, it suffices to choose $k = \lceil nh(\delta) + 2\log_2(1/\epsilon) + 5\rceil$. The key rate $1 - 2k/n$ then satisfies:

$$1 - 2h(\delta) - \frac{4\log_2(1/\epsilon) + 12}{n} \leq 1 - \frac{2k}{n} \leq 1 - 2h(\delta) - \frac{4\log_2(1/\epsilon) + 10}{n}$$

Therefore, the rate of convergence of the finite to the asymptotic rate is of the form cn^{-1}.

4.2 Key rate of the random sampling protocols

The sequence of works [21, 20, 9] develops QKD protocols and security proofs optimized for the finite key regime. The current evolution of the entanglement-based protocol can be found in [20, Section 3]; the difference between [9] and [20] is only in the random sampling tail bound that is used. For comparison with the present work we take only the case of perfect measurements in the rectilinear and diagonal basis. A summary of the protocol in this case is as follows:

1. Eve prepares a state of $2n$ qubits and sends n to Alice and n to Bob.

2. Alice and Bob agree on a uniformly random choice of either the rectilinear or the diagonal basis measurement for each pair of qubits.

3. Alice and Bob select a uniformly random subset of n_{pe} positions to serve for parameter estimation, leaving the remaining $n_{rk} = n - n_{pe}$ to serve as the raw key.

4. Alice and Bob compare their outcomes on the parameter estimation positions. If the error rate on these positions exceeds a threshold δ, Alice and Bob abort.

5. Alice sends a syndrome of her raw key to Bob, and a two-universal hash of her raw key to Bob. Bob uses the syndrome to correct his raw key, and uses the hash to verify that the correction was successful. For simplicity, take the combined length of syndrome and hash to be the theoretical minimum $n_{rk}h(\delta) - \log_2(\epsilon_{ec})$, where ϵ_{ec} is the desired bound on the probability that the hash test passes but Bob's corrected raw key does not match Alice's.

6. Alice and Bob compress their raw keys to shorter output keys of length n_{out} using a two-universal family of hash functions.

The security ϵ_{qkd} of these protocols can be written in the form

$$\epsilon_{qkd} = \epsilon_{ec} + \inf_{0<\nu<1/2-\delta} (\epsilon_{pa}(\nu) + \epsilon_{pe}(\nu))$$

where ϵ_{ec} is the desired bound on the correctness of the protocol, where

$$\epsilon_{pa}(\nu) = \frac{1}{2\sqrt{\epsilon_{ec}}} 2^{(-n_{rk}(1-h(\delta+\nu)-h(\delta))+n_{out})/2}$$

is a bound on the secrecy of the protocol, and where

$$\epsilon_{pe}(\nu) = \inf_{0<\xi<\nu} \epsilon_{pe}(\nu, \xi)$$

comes from a tail bound for random sampling. The precise form of the function $\epsilon_{pe}(\nu, \xi)$ is given in [9, Lemma 2] and satisfies the equation

$$\left(\frac{\epsilon_{pe}(\nu,\xi)}{2}\right)^2 = exp\left(-\frac{2nn_{pe}\xi^2}{n_{rk}+1}\right) + exp\left(-\frac{2(n+2)(n_{rk}^2(\nu-\xi)^2-1)}{(n(\delta+\xi)+1)(n(1-\delta-\xi)+1)}\right)$$

For the purpose of this section, consider the following lower bound on $\epsilon_{pe}(\nu)$:

Lemma 14. *Suppose $n_{rk} \geq n/2$. Then,*

$$\epsilon_{pe}(\nu) \geq 2exp(-2n_{pe}\nu^2)$$

Proof. Take any $\xi \in (0, \nu)$. Note that

$$\frac{2nn_{pe}\xi^2}{n_{rk}+1} \leq 4n_{pe}\nu^2$$

and therefore

$$exp\left(-\frac{2nn_{pe}\xi^2}{n_{rk}+1}\right) \geq exp\left(-4n_{pe}\nu^2\right)$$

The lemma follows. □

The following bound holds on the key rate of the random sampling protocols:

Theorem 3. *Fix the block size n, the tolerated error rate δ and the security level*

$$\epsilon_{qkd} = \epsilon_{ec} + \inf_{0<\nu<1/2-\delta} (\epsilon_{pa}(\nu) + \epsilon_{pe}(\nu))$$

Then, the key rate n_{out}/n is upper bounded by the larger of $(1-2h(\delta))/2$ and

$$(1-2h(\delta)) - c_1(\epsilon_{qkd},\delta)n^{-1/3} - c_2(\epsilon_{qkd})n^{-1}$$

where

$$c_1(\epsilon_{qkd},\delta) = \frac{3}{2^{5/3}}(1-2h(\delta))^{1/3}\left(\frac{1-h(\delta)}{1/2-\delta}\right)^{2/3}\left(\ln\frac{2}{\epsilon_{qkd}}\right)^{1/3}$$
$$c_2(\epsilon_{qkd}) = 3\log_2(1/\epsilon_{qkd}) + 3\log_2(3) - 4$$

Proof. Take the optimal ν. In case $n_{rk}/n < 1/2$, then

$$\frac{n_{out}}{n} \leq \frac{n_{rk}(1-h(\delta+\nu)-h(\delta))}{n} \leq \frac{1-2h(\delta)}{2}$$

Suppose now that $n_{rk}/n \geq 1/2$. Simplify the problem by eliminating ϵ_{ec}: note that

$$\epsilon_{ec} + \epsilon_{pa}(\nu) = \epsilon_{ec} + \frac{1}{2\sqrt{\epsilon_{ec}}}2^{(-n_{rk}(1-h(\delta+\nu)-h(\delta))+n_{out})/2}$$
$$\geq \frac{3}{2^{4/3}}2^{(-n_{rk}(1-h(\delta+\nu)-h(\delta))+n_{out})/3}$$

with equality if and only if

$$\epsilon_{ec} = \frac{1}{2^{4/3}}2^{(-n_{rk}(1-h(\delta+\nu)-h(\delta))+n_{out})/3}$$

Use this and Lemma 14 to deduce

$$\frac{3}{2^{4/3}}2^{(-n_{rk}(1-h(\delta+\nu)-h(\delta))+n_{out})/3} + 2exp(-2n_{pe}\nu^2) \leq \epsilon_{qkd}$$

From this, deduce further:

$$-n_{rk}(1-h(\delta+\nu)-h(\delta)) + n_{out} \leq 3\log_2\epsilon_{qkd} + 4 - 3\log_2(3)$$
$$-2n_{pe}\nu^2 \leq \ln(\epsilon_{qkd}) - \ln(2)$$

Rewrite the first inequality as

$$n_{out} \leq n(1-2h(\delta)) - n_{pe}(1-2h(\delta)) - n_{rk}(h(\delta+\nu)-h(\delta)) + 3\log_2 \epsilon_{qkd} + 4 - 3\log_2(3) \tag{1}$$

Now, apply the inequality $a + b \geq 3a^{1/3}(b/2)^{2/3}$ to the second and third term:

$$\begin{aligned} n_{pe}(1-2h(\delta)) + n_{rk}(h(\delta+\nu)-h(\delta)) \\ \geq \frac{3}{2^{2/3}} n_{pe}^{1/3}(1-2h(\delta))^{1/3} n_{rk}^{2/3}(h(\delta+\nu)-h(\delta))^{2/3} \\ \geq \frac{3}{2^{2/3}} n_{pe}^{1/3}(1-2h(\delta))^{1/3} (n/2)^{2/3} (h(\delta+\nu)-h(\delta))^{2/3} \end{aligned}$$

Further, use the line through $(\delta, h(\delta))$ and $(1/2, 1)$ to obtain

$$h(\delta+\nu) - h(\delta) \geq \nu \frac{1-h(\delta)}{1/2-\delta}$$

then combine this with $n_{pe}\nu^2 \geq 0.5 \ln(2/\epsilon_{qkd})$ to obtain

$$n_{pe}^{1/3}(h(\delta+\nu)-h(\delta))^{2/3} \geq \left(\frac{1-h(\delta)}{1/2-\delta}\right)^{2/3} \left(\frac{1}{2}\ln\frac{2}{\epsilon_{qkd}}\right)^{1/3}$$

Thus,

$$\begin{aligned} n_{pe}(1-2h(\delta)) + n_{rk}(h(\delta+\nu)-h(\delta)) \\ \geq \frac{3}{2^{5/3}}(1-2h(\delta))^{1/3} \left(\frac{1-h(\delta)}{1/2-\delta}\right)^{2/3} \left(\ln\frac{2}{\epsilon_{qkd}}\right)^{1/3} n^{2/3} \end{aligned}$$

Combining with (1) proves the Theorem. □

5 Conclusion and open problems

The present paper has proposed and proved security of a QKD protocol that uses two-universal hashing instead of random sampling to perform the uniquely quantum task of distinguishing suitable from unsuitable inputs. This protocol dramatically outperforms previous QKD protocols for small block sizes. More generally, the speed convergence to the asymptotic rate for the two-universal hashing protocol is cn^{-1}, whereas for an optimized random sampling protocol, the speed of convergence is no faster than $c'n^{-1/3}$.

As discussed already in the introduction, random sampling protocols involve only single qubit preparation and measurement, whereas the two-universal hashing protocol presented here requires Alice and Bob also to be able to store qubits for a short time while they agree on the matrix L, and to apply CNOT gates. It appears that the use of two-qubit gates is necessary for the improved performance, but this has not yet been mathematically proven. Can the speed of convergence cn^{-1} be achieved using only single qubit operations, or is there

some fundamental limit that prevents this? Another line of research related to the distinction between single and two-qubit quantum operations would be to develop quantum hardware capable of performing QKD protocols involving the CNOT gate.

Second, the algorithm given in section 2.3 for computing the function $g_{B_n(0,r)}$ is not efficient. This leads to the following open problem: is there a probability distribution over CSS codes, such that the marginal distributions of the two parity check matrices satisfy a two-universal hashing condition with some good collision probability bound, and such that each of the two parity check matrices has additional structure that allows efficient computation of $g_{B_n(0,r)}$ during the protocol? There is a long history in information theory of approximating the performance of random codes with brute force decoding by more structured codes with efficient decoding, so there is reason to hope that the same can be done in the present case.

Third, the arguments in the present paper are for the case where Alice and Bob can apply perfect quantum operations. It thus remains an open problem to generalize the present security proof to the case of imperfect devices.

Acknowledgment

This work was supported by the Luxembourg National Research Fund, under CORE project Q-CoDe (CORE17/IS/11689058). The author would like to thank Prof. Marco Tomamichel and two anonymous reviewers for helpful comments.

References

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

[2] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 410–423. Springer, 1993.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78:405–408, Jan 1997.

[4] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[5] J Lawrence Carter and Mark N Wegman. Universal classes of hash functions. *Journal of computer and system sciences*, 18(2):143–154, 1979.

[6] Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau. Practical issues in quantum-key-distribution postprocessing. *Physical Review A*, 81(1), Jan 2010.

[7] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Physical Review A*, 54(3):1862, 1996.

[8] Masato Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009.

[9] Charles Ci-Wen Lim, Feihu Xu, Jian-Wei Pan, and Artur Ekert. Security analysis of quantum key distribution with small block length and its application to quantum space communications. *Physical Review Letters*, 126(10), Mar 2021.

[10] Norbert Lütkenhaus. Estimates for practical quantum cryptography. *Physical Review A*, 59(5):3301, 1999.

[11] Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information. 2010.

[12] Dimiter Ostrev. Composable, unconditionally secure message authentication without any secret key. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 622–626. IEEE, 2019.

[13] 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. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[14] Christopher Portmann. Key recycling in authentication. *IEEE Transactions on Information Theory*, 60(7):4383–4396, 2014.

[15] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution, 2014.

[16] Renato Renner. *Security of quantum key distribution*. PhD thesis, ETH Zurich, 2005.

[17] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[18] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996.

[19] W Forrest Stinespring. Positive functions on c*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[20] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, Jul 2017.

[21] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature communications*, 3(1):1–6, 2012.

[22] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of computer and system sciences*, 22(3):265–279, 1981.

[23] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(7813):501–505, 2020.