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. For this 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 [15, 14, 1, 18] 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.

An important parameter for a QKD protocol and security proof is the key rate: the number of final secret key bits produced divided by the number of qubits used in the quantum phase of the protocol. Previous works consider the key rate in two regimes: asymptotic and finite. The asymptotic key rate is the limit of the key rate as the number of qubits go to infinity, while the finite key rate is given as a formula that is valid for all, or almost all, positive integer numbers of qubits. The finite key rate is less than the asymptotic rate; therefore, the faster the convergence, the better.

As an example, consider [18], which gives a QKD protocol and security proof optimized for the finite key regime. In [18, Section Discussion], the authors argue that for an instance of their protocol that can tolerate error rate q, the

*Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, 6 Avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg. Email: dimiter.ostrev@uni.lu

asymptotic key rate is $(1-2h(q))$, where h is the binary Shannon entropy. For the finite key rate, the authors give a fairly complex formula that has to be maximized over the choice of parameters, subject to the fairly complex constraint that the protocol does not needlessly abort in the absence of the adversary. Other than the general argument for convergence to $1-2h(q)$, [18] gives only numerical results, so the speed ot convergence remains unclear. However, the present paper shows that the difference between asymptotic and finite key rate for the protocols [18] is at least $cn^{-1/3}$ where c is a constant that depends on the error rate and security parameter and n is the number of qubits for which Alice and Bob choose the same basis.

The phenomenon that the key rate of a QKD protocol deteriorates significantly for small block sizes has been called finite size effect [11, Sections II-C and IX]. This effect holds not just for the example protocol [18], but for all QKD protocols known so far. In fact, in [18], the authors express a belief that the finite size effect is due to unavoidable statistical fluctuations in the parameter estimation step, and argue that their protocol is essentially optimal in the finite key regime.

The present paper proposes a QKD protocol whose key rate converges to the asymptotic rate much faster than previous QKD protocols. Specifically, this is an entanglement based QKD protocol where Alice and Bob each use n qubits, can tolerate any r bit flip errors and any r phase flip errors, and at the end extract $n-2\lceil nh(r/n)+2\log_2(1/\epsilon)+3\rceil$ secret key bits, that are ϵ close to an ideal secret key in the sense of the Abstract Cryptography framework for composable security. For fixed error rate $q=r/n$ and fixed security parameter ϵ, the asymptotic rate of this protocol is $1-2h(q)$, and the deviation of finite from asymptotic rate is between $(4\log_2(1/\epsilon)+6)/n$ and $(4\log_2(1/\epsilon)+8)/n$.

The main novelty in the QKD protocol proposed here is that it uses two universal hashing instead of random sampling to estimate the number and position of both bit flip and phase flip errors. By avoiding random sampling altogether, the protocol also avoids statistical fluctuations.

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 protocol [18]. This protocol estimates the number of errors in one of the measurement bases 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 builds on an earlier observation [2, Theorem 6],[14, 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, 16], and CSS codes can be used to design and prove security of QKD protocols [15]. The present paper also uses a number of technical lemmas related to the stabilizer formalism [6, 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.

The rest of this paper is structured as follows: Section 2 revisits the use of two-universal hashing to obtain an optimal information reconciliation protocol and gives 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 the transformation applied by the protocol is close to an ideal transformation. Section 4 uses this result to establish the security of the protocol in the Abstract Cryptography framework for composable security. Section 5 compares the key rate of the present protocol to the key rate of the protocol in [18], and proves the lower bound $cn^{-1/3}$ on the difference between finite and asymptotic rate for the protocol [18]. Section 6 concludes and gives some open problems.

2 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, 19]:

Definition 1. *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 $\mathbf{H} : \mathbb{F}_2 \to \mathbf{Y}$ 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 1 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 1. *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 2. *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 3. *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 $Mx = (1, 0, \dots, 0)^T$. 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 2 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 3. ☐

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 4. *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 5. *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 6. *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.

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

□

From Theorem 1, Lemma 3 and Lemma 6 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 [12], or using an advantage in channel noise [10].

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.

Now, consider the security of this protocol. The following notation is needed to state the main result. 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 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

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

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

Without loss of generality, assume that Eve prepares a pure tri-partite state $|\phi\rangle_{ABE}$ and gives to Alice and Bob their parts. Any strategy for Eve that prepares a mixed state ρ_{ABE} can be thought of as an equivalent strategy that prepares a purification $|\phi\rangle_{ABEE'}$ of ρ_{ABE} and then ignores register E'. Any input state $|\phi\rangle_{ABE}$ can be expanded in terms of the Bell basis for Alice and Bob:

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

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

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

The first eight steps of protocol $\pi(n, k, r)$ take as input a quantum state in registers A, B and output a classical probability distribution in registers $\mathbf{L}STU_AV_AW_AU_BV_BW_B$; let $\mathcal{E}^{real}$ be the completely positive trace preserving map that captures this transformation. Let

$$\Pi_{ST}^{accept} = \sum_{\alpha,\beta\in B_n(0,r)} |\alpha,\beta\rangle\langle\alpha,\beta|_{ST}$$

be the projection on the case that both s, t are not $\perp$ and so Alice and Bob accept.

The main result on the security of the QKD protocol demonstrates that the transformation $\mathcal{E}^{real}$ is close to an ideal transformation:

Theorem 2. *Take any $n, k, r \in \mathbf{N}$ such that $2nh(r/n) < 2k < n$. Then, there exists a completely positive trace preserving map $\mathcal{E}^{ideal}$ with input registers A, B and output registers $\mathbf{L}STU_AV_AW_AU_BV_BW_B$ such that for all input states*

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

the following two statements hold:

1. *The states $\mathcal{E}^{real}(|\phi\rangle\langle\phi|_{ABE})$ and $\mathcal{E}^{ideal}(|\phi\rangle\langle\phi|_{ABE})$ are $2^{-k/2+nh(r/n)/2+3/2}$ close in trace distance*
2. $\Pi^{accept}\mathcal{E}^{ideal}(|\phi\rangle\langle\phi|_{ABE})\Pi^{accept}$ *equals*

$$\sum_{L\in\mathbb{F}_2^{n\times n};u_A,v_A\in\mathbb{F}_2^k;w_A\in\mathbb{F}_2^{n-2k};\alpha,\beta\in B_n(0,r)} |\gamma_{\alpha\beta}\rangle\langle\gamma_{\alpha\beta}|_E \otimes p_L|L\rangle\langle L|_{\mathbf{L}} \otimes |\alpha,\beta\rangle\langle\alpha,\beta|_{ST}$$
$$\otimes\, 2^{-n}|u_A, v_A, w_A\rangle\langle u_A, v_A, w_A|_{U_AV_AW_A}$$
$$\otimes|u_A{+}L_1\alpha, v_A{+}M_2\beta, w_A{+}M_3\beta\rangle\langle u_A{+}L_1\alpha, v_A{+}M_2\beta, w_A{+}M_3\beta|_{U_BV_BW_B}$$

where p_L denotes the probability of choosing matrix L.

Section 4 shows that Theorem 2 implies that the protocols $\pi(n, k, r)$ are secure in the Abstract Cryptography framework for composable security. For now, focus on proving Theorem 2. The proof uses a number of lemmas related to the stabilizer formalism; these are in subsection 3.1. The proof of Theorem 2 is in subsection 3.2.

3.1 The Pauli group and the Bell basis

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 7 below. Therefore, the projections $P(\vec{g}, x)$ all have the same rank 2^{n-m}.

Lemma 7. *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 8. *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 $i \in \{1, \dots k\}$, any $x \in \mathbb{F}_2^m$ such that $Lx = y$. Then,

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

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. □

Next, consider the Bell basis. First, the maximally entangled state has the properties:

Lemma 9. *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 10. *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 7 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 11. *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 11 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 8. The second relation follows similarly. □

3.2 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. *For all input states $|\phi\rangle_{ABE}$ to the protocol, the output state $\mathcal{E}^{real}(|\phi\rangle\langle\phi|)$ 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*

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

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 [17]. 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 $\mathcal{W}\mathcal{V}_{real}$ followed by $Tr_{ABT'V'_AV'_BW'_AW'_B}$.

Finally, note that all the partial trace operations can be commuted to the end. $\square$

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 11:

$$\begin{aligned}
&\sum_{L,z_A,z_B,\alpha} p_L \left(\sum_\beta |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|_{AB} \right) |z_A z_B\rangle\langle z_A z_B|_{AB} \langle f(\alpha)|g(L_1, L_1(z_A{+}z_B))\rangle_S \\
&= \sum_{L,z_A,z_B,\alpha,z'_A} p_L |z'_A, z'_A{+}\alpha\rangle\langle z'_A, z'_A{+}\alpha|_{AB} |z_A z_B\rangle\langle z_A z_B|_{AB} \langle f(\alpha)|g(L_1, L_1(z_A{+}z_B))\rangle_S \\
&\quad = \sum_{z_A,z_B} |z_A z_B\rangle\langle z_A z_B|_{AB} \sum_L p_L \langle f(z_A + z_B)|g(L_1, L_1(z_A + z_B))\rangle \\
&\qquad = \sum_{z_A,z_B} |z_A z_B\rangle\langle z_A z_B|_{AB} \Pr_L(f(z_A + z_B) = g(L_1, L_1(z_A + z_B)))
\end{aligned}$$

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 5). 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

$$\begin{aligned}
\mathcal{V}_{simulator} = \sum_{L,x_A,x_B} &|L\rangle\langle L|_{\mathbf{L}} \otimes \left(H^{\otimes 2n}|x_A x_B\rangle\langle x_A x_B|H^{\otimes 2n}\right)_{AB} \\
&\otimes |M_2x_A, M_2x_A, M_2x_B, M_2x_B\rangle_{V_A V'_A V_B V'_B}
\end{aligned}$$

This isometry captures the measurement through which Alice and Bob obtain the values $v_A = M_2x_A$ and $v_B = M_2x_B$.

Then:

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

Proof. As in the proof of Proposition 2, use Lemma 11 to compute

$$\begin{aligned}
&\left(\langle\mathcal{L}|\mathcal{V}^\dagger_{ideal}\mathcal{V}^\dagger_{simulator}\right)(\mathcal{V}_{real}|\mathcal{L}\rangle) \\
&= \sum_{x_A,x_B} \left(H^{\otimes 2n}|x_A x_B\rangle\langle x_A x_B|H^{\otimes 2n}\right)_{AB} \Pr_L(f(x_A{+}x_B) = g(M_2, M_2(x_A{+}x_B)))
\end{aligned}$$

Now, $M = (L^{-1})^T$ is uniformly distributed over invertible matrices in $\mathbb{F}_2^{n\times n}$, so Lemma 5 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:

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

where the last step uses Lemma 8 and the notation of Section 3.1 for the tuple $\vec{\sigma}_3$ of single qubit σ_3 operations.

Similarly, rewrite

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

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 2, 3, 4 to construct the ideal transformation and complete the proof of Theorem 2:

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 conclusions of Theorem 2 are satisfied.*

Proof. Take any input state $|\phi\rangle_{ABE}$. 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 [9, 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 the first conclusion of Theorem 2.

Next, 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 3.1, 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 8.

Next, use Lemma 10 to deduce that

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

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. Since Π^{accept}_{ST} commutes with the partial trace, deduce

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

Finally, simplify and use Lemma 9 to deduce that

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

so the second conclusion of Theorem 2 also holds. □

4 Security in the Abstract Cryptography Framework

Subsection 4.1 gives a brief review of Abstract Cryptography, then subsection 4.2 discusses modeling QKD security in this framework, and finally subsection 4.3 proves that the protocols $\pi(n,k,r)$ are secure in the sense of Abstract Cryptography.

4.1 Review of Abstract Cryptography

This is only a brief exposition; for more details, see for example [7, 8, 13].

A resource is an interactive algorithm with three interfaces on which Alice, Bob and Eve can submit inputs and receive outputs. Two resources can be put together in parallel, meaning that Alice, Bob and Eve have access to the interfaces of both. The parallel composition of resources $\mathcal{R}, \mathcal{S}$ is denoted $\mathcal{R}\|\mathcal{S}$.

A converter is an interactive algorithm with two interfaces. The inside interface communicates with a resource, and the outside interface communicates with a user. Converter α attached to interface $i \in \{A, B, E\}$ of resource $\mathcal{R}$ is denoted by $\alpha_i\mathcal{R}$.

Thus, various interactive algorithms that connect Alice, Bob and Eve can be described using resources and converters and operations that put two resources in parallel, and attach a converter to a given interface of a resource.

On the set of interactive algorithms with three interfaces define a pseudo-metric:

Definition 2. *The distance of resources $\mathcal{R}, \mathcal{S}$ is*

$$d(\mathcal{R}, \mathcal{S}) = \sup_{\mathcal{D}} |\Pr(\mathcal{D}\mathcal{R} = 1) - \Pr(\mathcal{D}\mathcal{S}) = 1|$$

where the supremum is taken over interactive algorithms $\mathcal{D}$ that connect to the three interfaces of a resource and output 0 or 1. Such an interactive algorithm is called a distinguisher.

This pseudometric generalizes the trace distance of quantum states. It has the following metric and monotonicity properties:

Lemma 12. *For all resources $\mathcal{R}, \mathcal{S}, \mathcal{T}$, all converters α, and all interfaces $i \in \{A, B, E\}$:*

1. *(identity)* $d(\mathcal{R}, \mathcal{R}) = 0$
2. *(symmetry)* $d(\mathcal{R}, \mathcal{S}) = d(\mathcal{S}, \mathcal{R})$
3. *(triangle inequality)* $d(\mathcal{R}, \mathcal{T}) \leq d(\mathcal{R}, \mathcal{S}) + d(\mathcal{S}, \mathcal{T})$
4. *(non-increasing under a converter)* $d(\alpha_i \mathcal{R}, \alpha_i \mathcal{S}) \leq d(\mathcal{R}, \mathcal{S})$
5. *(non-increasing under a resource in parallel)* $d(\mathcal{R} \| \mathcal{T}, \mathcal{S} \| \mathcal{T}) \leq d(\mathcal{R}, \mathcal{S})$

This lemma can be proved directly from the definitions.

Next, consider the following additional terminology, and use it to formulate the definition of construction. A protocol is a pair for converters, one for Alice and one for Bob. A filter is a converter whose goal is to block Eve from doing harm. A filtered resource is a pair of a resource and an associated filter. A simulator is a converter whose goal is to make Eve's interface to one resource appear like the interface to another. With this, define:

Definition 3. *A protocol $\pi = (\pi_A, \pi_B)$ constructs filtered resource $(\mathcal{S}, \xi)$ from filtered resource $(\mathcal{R}, \eta)$ within ϵ, denoted $(\mathcal{R}, \eta) \xrightarrow{\pi, \epsilon} (\mathcal{S}, \xi)$, if*

1. *(Close with Eve blocked)* $d(\pi_A \pi_B \eta_E \mathcal{R}, \xi_E \mathcal{S}) \leq \epsilon$
2. *(Close with full access for Eve) There exists a simulator θ_E such that*

$$d(\pi_A \pi_B \mathcal{R}, \theta_E \mathcal{S}) \leq \epsilon$$

This definition follows the real-world ideal-world paradigm in cryptography. $\mathcal{S}$ is the ideal functionality that Alice and Bob want, and $\mathcal{R}$ is the real functionality that they have available. The first condition in the definition is needed for example in order to rule out trivial protocols that always reject. The quantification $\exists \theta_E$ in the second condition is needed to allow freedom in describing Eve's interface to the ideal $\mathcal{S}$ and yet prevent trivial distinguishers that simply look at the type of Eve's interface.

The definition of construction satisfies parallel and sequential composition:

Theorem 3. *1. If* $(\mathcal{R}, \eta) \xrightarrow{\pi,\epsilon} (\mathcal{S}, \xi)$ *and* $(\mathcal{R}', \eta') \xrightarrow{\pi',\epsilon'} (\mathcal{S}', \xi')$ *then*

$$(\mathcal{R}\|\mathcal{R}', \eta\|\eta') \xrightarrow{\pi\|\pi',\epsilon+\epsilon'} (\mathcal{S}\|\mathcal{S}', \xi\|\xi')$$

2. If $(\mathcal{R}, \eta) \xrightarrow{\pi,\epsilon} (\mathcal{S}, \xi)$ *and* $(\mathcal{S}, \xi) \xrightarrow{\tau,\delta} (\mathcal{T}, \mu)$ *then* $(\mathcal{R}, \eta) \xrightarrow{\tau\pi,\epsilon+\delta} (\mathcal{T}, \mu)$

This theorem follows from the properties of the operations on resources and converters and the properties of distance.

4.2 Modeling QKD security in Abstract Cryptography

Now, specialize to the case of QKD. First, define the ideal system that a QKD protocol tries to construct: the blockable secret key $\mathcal{KEY}_n$ given by the pseudo-code: "On input 1 from Eve, draw a uniformly random string in $\mathbb{F}_2^n$ and output it to Alice and Bob. On input 0 from Eve, output $\perp$ to Alice and Bob." The filter for $\mathcal{KEY}_n$ is parametrized by $\delta \in [0, 1]$ and is given by $\mu_\delta =$ "With probability δ output 0 to $\mathcal{KEY}$ and with probability $1 - \delta$ output 1 to $\mathcal{KEY}$."

Next, look at the real resources that Alice and Bob have. First, they have an authenticated classical channel, described by the resource $\mathcal{AUTH} =$ " On input *message* from Alice/Bob, output *message* to Bob/Alice and also to Eve." The filter η for $\mathcal{AUTH}$ blocks Eve from seeing the message.

Next, Alice and Bob need a quantum resource, which for entanglement based protocols is $\mathcal{QENT}_n$= "On input from Eve of a state ρ_{AB} of $2n$ qubits, output the n qubits in system A to Alice and the n qubits in system B to Bob."

A filter ξ for $\mathcal{QENT}_n$ is comletely characterized by the $2n$-qubit state ρ_{AB} that it submits to the resource. The following notation will be useful: for $r \leq n$ let

$$\delta_r(\xi) = 1 - Tr\left(\left(\sum_{\alpha,\beta \in B_n(0,r)} |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|\right)\rho_{AB}\left(\sum_{\alpha,\beta \in B_n(0,r)} |\psi_{\alpha\beta}\rangle\langle\psi_{\alpha\beta}|\right)\right)$$

4.3 Security of the two-universal hashing protocols $\pi(n, k, r)$ in Abstract Cryptography

From Theorem 2, deduce:

Corollary 2. *For every* $n, k, r \in \mathbb{N}$ *such that* $2nh(r/n) < 2k < n$*, for every filter* ξ *for* $\mathcal{QENT}_n$*,*

$$(\mathcal{QENT}_n, \xi)\|(\mathcal{AUTH}, \eta) \xrightarrow{\pi(n,k,r),2^{-k/2+nh(r/n)/2+3/2}} (\mathcal{KEY}_{n-2k}, \mu_{\delta_r(\xi)})$$

Proof. To simplify notation, n, k, r, δ are left implicit during the proof.

Start by defining the following resources and converters:

1. Resource $\mathcal{R}$: "on input ρ_{AB} at interface E, apply $\mathcal{E}^{real}$, output L, s, t, u_A, u_B, v_A, v_B at all three interfaces A, B, E, and additionally output w_A at interface A and w_B at interface B."

2. Resource $\mathcal{S}$: "on input ρ_{AB} at interface E, apply $\mathcal{E}^{ideal}$, output L, s, t, u_A, u_B, v_A, v_B at all three interfaces A, B, E, and additionally output w_A at interface A and w_B at interface B."

3. Simulator θ_E: "on input ρ_{AB} at interface E, apply $\mathcal{E}^{ideal}$, output L, s, t, u_A, u_B, v_A, v_B at interface E, if $s \neq \perp \wedge t \neq \perp$ output 1 at the inside interface to $\mathcal{KEY}$, else output 0 to $\mathcal{KEY}$."

4. Converter ϖ_A: "On input L, s, t, u_A, u_B, v_A, v_B, w_A at the inside interface, if $s \neq \perp \wedge t \neq \perp$ output w_A at the outside interface, else output $\perp$ at the outside interface."

5. Converter ϖ_B: "On input L, s, t, u_A, u_B, v_A, v_B, w_B at the inside interface, if $s \neq \perp \wedge t \neq \perp$ output $w_B + M_3 t$ at the outside interface, else output $\perp$ at the outside interface."

Then, the following relation holds:

$$d(\pi_A \pi_B (\mathcal{QENT} \| \mathcal{AUTH}), \varpi_A \varpi_B \mathcal{R}) = 0$$

Thus, it suffices to show the following:

$$\begin{aligned} d(\varpi_A \varpi_B (\xi \| \eta)_E \mathcal{R}, \mu_E \mathcal{KEY}) &\leq 2^{-k/2 + nh(r/n)/2 + 3/2} \\ d(\varpi_A \varpi_B \mathcal{R}, \theta_E \mathcal{KEY}) &\leq 2^{-k/2 + nh(r/n)/2 + 3/2} \end{aligned}$$

From Theorem 2, deduce that $d(\mathcal{R}, \mathcal{S}) \leq 2^{-k/2 + nh(r/n)/2 + 3/2}$. Then, using monotonicity of the distance, deduce

$$\begin{aligned} d(\varpi_A \varpi_B (\xi \| \eta)_E \mathcal{R}, \varpi_A \varpi_B (\xi \| \eta)_E \mathcal{S}) &\leq 2^{-k/2 + nh(r/n)/2 + 3/2} \\ d(\varpi_A \varpi_B \mathcal{R}, \varpi_A \varpi_B \mathcal{S}) &\leq 2^{-k/2 + nh(r/n)/2 + 3/2} \end{aligned}$$

Thus, it suffices to show

$$\begin{aligned} d(\varpi_A \varpi_B (\xi \| \eta)_E \mathcal{S}, \mu_E \mathcal{KEY}) &= 0 \\ d(\varpi_A \varpi_B \mathcal{S}, \theta_E \mathcal{KEY}) &= 0 \end{aligned}$$

The two resources $\varpi_A \varpi_B (\xi \| \eta)_E \mathcal{S}, \mu_E \mathcal{KEY}$ are of the same type: they take no input, and produce a string of size $n - 2k$ or an error at interfaces A, B. For the resource $\mu_E \mathcal{KEY}$, the joint distribution of the two outputs is

$$\delta |\perp, \perp\rangle\langle\perp, \perp|_{K_A K_B} + (1 - \delta) 2^{-n+2k} \sum_{y \in \mathbb{F}_2^{n-2k}} |y, y\rangle\langle y, y|_{K_A K_B}$$

Since the parameter of μ is chosen to match $\delta_r(\xi)$, the joint distribution of the two output strings is the same for $\varpi_A \varpi_B (\xi \| \eta)_E \mathcal{S}$. Thus, $d(\varpi_A \varpi_B (\xi \| \eta)_E \mathcal{S}, \mu_E \mathcal{KEY}) = 0$.

Next, the two resources $\varpi_A \varpi_B \mathcal{S}, \theta_E \mathcal{KEY}$ are of the following type: they take input a state of $2n$ qubits at interface E, then produce classical outputs

$L, s, t, u_a, u_B, v_A, v_B$ at interface E and produce outputs $y_A, y_B \in \mathbb{F}_2^{n-2k} \cup \{\perp\}$ at interfaces A, B.

A distinguisher between $\varpi_A \varpi_B \mathcal{S}, \theta_E \mathcal{KEY}$ can prepare any pure state

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

and submit systems A, B at the E interface. For both resources $\varpi_A \varpi_B \mathcal{S}, \theta_E \mathcal{KEY}$, the state $\mathcal{E}^{ideal}(|\phi\rangle\langle\phi|)$ is computed internally and then the measurement of $\Pi_{ST}^{accept}, I_{ST} - \Pi_{ST}^{accept}$ is applied. However, in the case "accept", the two resources derive the output secret keys differently: $\varpi_A \varpi_B \mathcal{S}$ derives them from w_A, w_B, L, t, while $\theta_E \mathcal{KEY}$ draws a new independent string. Nevertheless, the joint distribution of outputs is the same for both cases, as can be seen from the identity:

$$\begin{aligned}
&Tr_{W_A W_B}\Bigg(\sum_{L \in \mathbb{F}_2^{n\times n}; u_A, v_A \in \mathbb{F}_2^k; w_A \in \mathbb{F}_2^{n-2k}; \alpha,\beta \in B_n(0,r)} |\gamma_{\alpha\beta}\rangle\langle\gamma_{\alpha\beta}|_E \otimes p_L |L\rangle\langle L|_{\mathbf{L}} \\
&\otimes |\alpha,\beta\rangle\langle\alpha,\beta|_{ST} \otimes 2^{-n} |u_A, v_A, w_A\rangle\langle u_A, v_A, w_A|_{U_A V_A W_A} \\
&\otimes |u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta\rangle\langle u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta|_{U_B V_B W_B} \\
&\otimes |w_A, w_A\rangle\langle w_A, w_A|_{Y_A Y_B} \Bigg) \\
&= Tr_{W_A W_B}\Bigg(\sum_{L \in \mathbb{F}_2^{n\times n}; u_A, v_A \in \mathbb{F}_2^k; w_A \in \mathbb{F}_2^{n-2k}; y \in \mathbb{F}_2^{n-2k}; \alpha,\beta \in B_n(0,r)} |\gamma_{\alpha\beta}\rangle\langle\gamma_{\alpha\beta}|_E \otimes p_L |L\rangle\langle L|_{\mathbf{L}} \\
&\otimes |\alpha,\beta\rangle\langle\alpha,\beta|_{ST} \otimes 2^{-n} |u_A, v_A, w_A\rangle\langle u_A, v_A, w_A|_{U_A V_A W_A} \\
&\otimes |u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta\rangle\langle u_A + L_1\alpha, v_A + M_2\beta, w_A + M_3\beta|_{U_B V_B W_B} \\
&\otimes 2^{-n+2k} |y, y\rangle\langle y, y|_{Y_A Y_B} \Bigg)
\end{aligned}$$

Thus, $d(\varpi_A \varpi_B \mathcal{S}, \theta_E \mathcal{KEY}) = 0$ and the proof of Corollary 2 is complete. □

5 Comparison with previous work

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

Given n qubits per side, the target to tolerate r bit flip and r phase flip errors, and a target security parameter ϵ, it suffices to choose $k = \lceil nh(r/n) + 2\log_2(1/\epsilon) + 3 \rceil$. Thus, from corollary 2 it follows that for all filters ξ

$$(\mathcal{QENT}_n, \xi) \| (\mathcal{AUTH}, \eta) \xrightarrow{\pi(n,k,r),\epsilon} (\mathcal{KEY}_{n-2\lceil nh(r/n)+2\log_2(1/\epsilon)+3\rceil}, \mu_{\delta_r(\xi)}) \quad (1)$$

If the tolerated error rate is fixed to be $r/n = q$, a constant independent of n, and the security parameter ϵ is fixed, then, when n goes to infinity, the key

rate converges to $1 - 2h(q)$ and the deviation of finite from asymptotic rate is between $(4\log_2(1/\epsilon)+6)/n$ and $(4\log_2(1/\epsilon)+8)/n$.

5.2 The random sampling protocols

Recall the protocols of [18], which are here called the TLGR12 family of protocols after the names of the authors and the year of publication. For a fair comparison to the protocols $\pi(n,k,r)$, adapt the TLGR12 protocols as much as possible to be consistent with the notation and assumptions in the present paper. In particular, convert TLGR12 to an entanglement based protocol, assume perfect measurement devices, plug in the optimal information reconciliation protocol by two-universal hashing from Section 2, and change the correctness-and-secrecy security definition of [18] to the abstract cryptography security definition of the present paper. For this last change, use the discussion in [13, Section 4 and Appendix B] and take the correctness and secrecy parameters to be $\epsilon_{cor} = \epsilon_{sec} = \epsilon/2$ where ϵ is the Abstract Cryptography construction distance parameter. Thus, the following protocols are obtained:

1. Eve prepares a state of $2n$ qubits and gives half to Alice and half to Bob. Alice and Bob inform each other that they have received the qubits.

2. Alice and Bob choose a random subset of n_{pe} positions to serve for parameter estimation. The remaining $n_{rk} = n - n_{pe}$ positions serve for the generation of the raw key.

3. Alice and Bob measure the parameter estimation positions in the computational basis and compare the outcomes. If the outcomes differ in more than r_{pe} positions, Alice and Bob reject.

4. Alice and Bob measure the raw key positions in the $|+\rangle, |-\rangle$ basis, obtaining outcomes x_A, x_B. They perform information reconciliation: Alice chooses a random linear function L with output length

$$n_{rk} h\left(\frac{r_{rk}}{n_{rk}}\right) + \log_2 \frac{1}{\epsilon} + 1,$$

sends to Bob L, Lx_A, and Bob computes the function $g_{B_{n_{rk}(0,r_{rk})}}(L, Lx_A + Lx_B)$ from Section 2.

5. If Bob did not reject during information reconciliation, then Alice and Bob choose a random two-universal hash function with output length

$$n_{out} = n_{rk}\left(1 - h\left(\frac{r_{pe}}{n_{pe}} + \sqrt{\frac{n(n_{pe}+1)}{n_{rk}n_{pe}^2}\ln\frac{4}{\epsilon}}\right) - h\left(\frac{r_{rk}}{n_{rk}}\right)\right) - 3\log_2\frac{1}{\epsilon} - 4$$

and use it to obtain the output secret key.

The following bound holds on the key rate of the TLGR12 protocols:

Theorem 4. *Assume*

$$\frac{r_{pe}}{n_{pe}} \geq \frac{r}{n} \quad \text{and} \quad \frac{r_{rk}}{n_{rk}} \geq \frac{r}{n}$$

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

$$(1-2h(q)) - 3\left(\frac{(1-2h(q))(1-h(q))^2}{8(1/2-q)^2}\ln\frac{4}{\epsilon}\right)^{1/3} n^{-1/3} - \frac{3\log_2\frac{1}{\epsilon}+4}{n}$$

where $q = r/n$. In particular, when q, ϵ are fixed and n goes to infinity, the key rate converges to $1-2h(q)$ no faster than $cn^{-1/3}$.

Before proving Theorem 4, consider the assumptions $r_{pe}/n_{pe}, r_{rk}/n_{rk} \geq r/n$. Note that for the two-universal hashing protocol $\pi(n,k,r)$, Corollary 2 implies that for all $\alpha, \beta \in B_n(0,r)$, $\pi(n,k,r)$ aborts with probability at most ϵ on input $|\psi_{\alpha\beta}\rangle$. Therefore, for a fair comparison, the same would be required of the TLGR12 protocols. This would in turn imply that a random sample of n_{pe} positions out of n contains more than r_{pe} out of r errors with probability at most ϵ, and a random sample of n_{rk} out of n positions contains more than r_{rk} out of r errors with probability around ϵ. This in turn would imply that r_{rk}, r_{pe} must exceed the respective means by $c\sqrt{\ln(1/\epsilon)}$ standard deviations, so

$$\frac{r_{pe}}{n_{pe}} \geq \frac{r}{n} + c\sqrt{\ln\frac{1}{\epsilon}}\sqrt{\frac{r(n-r)n_{rk}}{n_{pe}n^3}}$$
$$\frac{r_{rk}}{n_{rk}} \geq \frac{r}{n} + c\sqrt{\ln\frac{1}{\epsilon}}\sqrt{\frac{r(n-r)n_{pe}}{n_{rk}n^3}}$$

It turns out however that even the weaker inequalities $r_{pe}/n_{pe}, r_{rk}/n_{rk} \geq r/n$ in the assumptions of Theorem 4, suffice to prove the $1-2h(q)-c'n^{-1/3}$ upper bound on the key rate.

Proof of Theorem 4. Start with

$$\frac{n_{out}}{n} \leq \frac{n_{rk}}{n}\left(1 - h\left(\frac{r}{n} + \sqrt{\frac{n(n_{pe}+1)}{n_{rk}n_{pe}^2}\ln\frac{4}{\epsilon}}\right) - h\left(\frac{r}{n}\right)\right) - \frac{3\log_2\frac{1}{\epsilon}+4}{n}$$

Now, consider the line through $(r/n, h(r/n))$ and $(1/2, 1)$ and obtain:

$$h\left(\frac{r}{n} + \sqrt{\frac{n(n_{pe}+1)}{n_{rk}n_{pe}^2}\ln\frac{4}{\epsilon}}\right) \geq h\left(\frac{r}{n}\right) + \frac{1-h(r/n)}{1/2-r/n}\sqrt{\frac{n(n_{pe}+1)}{n_{rk}n_{pe}^2}\ln\frac{4}{\epsilon}}$$

Thus, the key rate of the TLGR12 protocol is upper bounded by

$$\frac{n_{rk}}{n}\left(1-2h\left(\frac{r}{n}\right)-\frac{1-h(r/n)}{1/2-r/n}\sqrt{\frac{n(n_{pe}+1)}{n_{rk}n_{pe}^2}\ln\frac{4}{\epsilon}}\right)-\frac{3\log_2\frac{1}{\epsilon}+4}{n}$$
$$=\left(1-2h\left(\frac{r}{n}\right)\right)-\left(1-2h\left(\frac{r}{n}\right)\right)\frac{n_{pe}}{n}$$
$$-\frac{n_{rk}}{n}\frac{1-h(r/n)}{1/2-r/n}\sqrt{\frac{n(n_{pe}+1)}{n_{rk}n_{pe}^2}\ln\frac{4}{\epsilon}}-\frac{3\log_2\frac{1}{\epsilon}+4}{n}$$
$$=\left(1-2h\left(\frac{r}{n}\right)\right)-\frac{3\log_2\frac{1}{\epsilon}+4}{n}$$
$$-\left(\left(1-2h\left(\frac{r}{n}\right)\right)\frac{n_{pe}}{n}+\frac{1-h(r/n)}{1/2-r/n}\sqrt{\frac{n_{rk}(n_{pe}+1)}{nn_{pe}^2}\ln\frac{4}{\epsilon}}\right)$$

Now, focus on the sum of two terms on the last line. If $n_{pe}\geq n/2$ then $(1-2h(q))n_{pe}/n\geq(1-2h(q))/2$. Else, $n_{pe}<n/2$, so simplify:

$$\frac{n_{rk}(n_{pe}+1)}{nn_{pe}}=1-\frac{n_{pe}}{n}+\frac{1}{n_{pe}}-\frac{1}{n}\geq\frac{1}{2}$$

and thus the sum of the two terms is lower bounded by

$$(1-2h(q))\frac{n_{pe}}{n}+\frac{1-h(q)}{1/2-q}\sqrt{\frac{1}{2n_{pe}}\ln\frac{4}{\epsilon}}$$

As a function of n_{pe}, this expression is of the form $ax+bx^{-1/2}$ and its minimum is attained at $x=(2a/b)^{-2/3}$ and has the value $3(ab^2/4)^{1/3}$. Thus, the sum of two terms is lower bounded by

$$\frac{(1-2h(q))}{n}n_{pe}+\frac{1-h(q)}{1/2-q}\sqrt{\frac{1}{2}\ln\frac{4}{\epsilon}}n_{pe}^{-1/2}\geq 3\left(\frac{(1-2h(q))(1-h(q))^2}{8(1/2-q)^2}\ln\frac{4}{\epsilon}\right)^{1/3}n^{-1/3}$$

as needed. Theorem 4 follows. □

6 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. The advantage of this protocol is that the speed convergence to the asymptotic rate is governed by a function of the form cn^{-1}, whereas for an optimized random sampling protocol, the speed of convergence is no faster than $c'n^{-1/3}$. However, fast convergence to the asymptotic rate is not the only desirable property of a QKD protocol. Considering other criteria leads to the following open problems.

First, random sampling protocols of the prepare and measure type 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. 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 would be to develop quantum hardware capable of performing the two-universal hashing QKD protocol.

Second, the algorithm given in section 2 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?

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).

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 Robert Calderbank, Eric M Rains, Peter W Shor, and Neil JA Sloane. Quantum error correction and orthogonal geometry. *Physical Review Letters*, 78(3):405, 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. In *Proceedings of the ninth annual ACM symposium on Theory of computing*, pages 106–112. ACM, 1977.

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

[7] Ueli Maurer. Constructive cryptography-a new paradigm for security definitions and proofs. *TOSCA*, 6993:33–56, 2011.

[8] Ueli Maurer and Renato Renner. Abstract cryptography. In *In Innovations in Computer Science*. Citeseer, 2011.

[9] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

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

[11] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, 2020.

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

[13] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. *arXiv preprint arXiv:1409.3525*, 2014.

[14] Renato Renner. *Security of quantum key distribution.* PhD thesis, Swiss Federal Institute of Technology Zurich, https://arxiv.org/pdf/quant-ph/0512258.pdf, 2005.

[15] Peter W Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[16] Andrew Steane. Multiple-particle interference and quantum error correction. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 452, pages 2551–2577. The Royal Society, 1996.

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

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

[19] 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.