Efficient Simulation for Quantum Message Authentication

Anne Broadbent[(✉)] and Evelyn Wainewright

Department of Mathematics and Statistics, University of Ottawa, Ottawa, Canada
{abroadbe,ewain031}@uottawa.ca

Abstract. Quantum message authentication codes are families of keyed encoding and decoding maps that enable the detection of tampering on encoded quantum data. Here, we study a new class of simulators for quantum message authentication schemes, and show how they are applied in the context of two codes: the *Clifford* and the *trap* code. Our results show for the first time that these codes admit an *efficient simulation* (assuming that the adversary is efficient). Such efficient simulation is typically crucial in order to establish a composable notion of security.

1 Introduction

Quantum cryptography is the study of the security of information processing in a quantum world. While quantum key distribution [4] is today the most widely successful quantum cryptographic technology [7,12], quantum information effectively re-defines many cryptographic paradigms [6]. Among these is the need for new definitions and protocols for cryptographic tasks that operate on quantum data, such as quantum secret sharing [9] and quantum multi-party computation [3]. Another fundamental task is quantum message authentication.

Quantum message authentication schemes, introduced in [2], are families of keyed encoding and decoding maps which allow for the detection of tampering on encoded quantum data. These codes were originally given in a very efficient form, based on *purity testing* [2], and were shown to also satisfy a composable security notion [14].

Further quantum message authentication schemes have been proposed, including the *signed polynomial code*[1,3], the trap code [5] and the *Clifford* code [1,11]. These schemes have a nice algebraic form, which makes them particularly easy to study. Perhaps the main reason for interest in these schemes is that they have a sufficient amount of "structure" to enable evaluation of quantum gates over the encoded data (this technique is called *quantum computing on authenticated data (QCAD)*). This has lead to protocols for multi-party quantum computation [3], quantum one-time programs [5] and the verification of quantum computations [1].

The security of quantum message authentication schemes is typically defined in terms of the existence of a *simulator* that, given access only to the ideal functionality for quantum message authentication (which is a virtual device that

either transmits the quantum data directly and outputs "accept", or replaces it with a dummy state and outputs "reject"), is able to emulate the behaviour of the adversary so that the real-world protocol (involving the adversary) is statistically indistinguishable from the ideal-world protocol (involving the simulator). This type of definition fits in the quantum Universal Composability (UC)[8,16] framework, as long as we add a further condition: if the adversary runs in polynomial time, so must the simulator (an *efficient* simulation). Until now, direct efficient simulations were known only for the purity-testing based codes [2].

In this work, we show a new family of efficient simulators for quantum message authentication schemes. The main idea is that the simulator replaces the entire codeword by half-EPR pairs (keeping the remaining half to itself), and runs the adversary on these entangled states (as well as the reference system for the original input). After the attack is applied, the simulator performs Bell basis measurements in order to verify the integrity of the EPR pairs. So long as enough EPR pairs are found to be intact, the simulator makes the ideal functionality "accept"; otherwise, it makes it "reject". It is well-known that this Bell basis measurement will detect any non-identity Pauli attack—given the structure of the codes that we analyze, we show that this is sufficient.

We apply this type of simulator to the Clifford and trap quantum message authentication codes. We note that the Clifford code was previously proven secure according to an algebraic definition, without an efficient simulation [1,11], and that the trap scheme was proven secure according to a simulator for a more elaborate ideal functionality for *quantum one-time programs* [5]. We thus establish for the first time efficient simulators for these codes (note, however, that we make extensive use of the algebraic tools developed in these prior works, and that we achieve the same security bounds). We also note that the idea of using EPR-pair testing as a proof technique for quantum message authentication has appeared in [2], where a more elaborate type of testing (called *purity testing*) is used.

Roadmap. The remainder of the paper is structured as follows. In Sect. 2, we give some details on the standard notation and well-known facts that are used throughout. In Sect. 3, we formally define quantum message authentication in terms of correctness and security. Section 4 gives the Clifford and trap schemes, while in Sect. 5 we show security of the schemes.

2   Preliminaries

Here, we present basic notation (Sect. 2.1) and well-known facts about the Pauli (Sect. 2.2) and Clifford (Sect. 2.3) groups.

2.1   Basic Notation

We assume the reader is familiar with the basics of quantum information [15], but nevertheless give a quick review of the most relevant notation in this section. We will use the density operator formalism to represent quantum states. Density matrices are represented with a greek letter, typically ρ. The subscripts

of the quantum states indicate which spaces (registers) the states reside in. We therefore represent the density operator for the state in the M register as ρ_M.

The *trace norm* of a state, ρ, denoted $\|\rho\|_1$, is defined as $\|\rho\|_1 = tr[\sqrt{\rho^\dagger \rho}]$. The *trace distance* between two states ρ and σ, denoted $D(\rho, \sigma)$, is defined as $D(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1$. The trace distance is a measure of distiguishability between the two states ρ and σ. The trace distance is equal to 0 if and only if ρ and σ are the same state (and therefore indistinguishable) and the trace distance is equal to 1 if and only if ρ and σ are orthogonal (and therefore perfectly distinguishable). The trace norm, and therefore the trace distance, satisfies the triangle inequality: $\|\rho + \sigma\|_1 \leq \|\rho\|_1 + \|\sigma\|_1$.

Let $\mathcal{B}(\mathcal{H})$ be the space of bounded linear operators acting on a Hilbert space, $\mathcal{H}$. Given $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H}_1)$ and $\mathcal{B} \subseteq \mathcal{B}(\mathcal{H}_2)$ then given a linear map T from $\mathcal{A} \to \mathcal{B}$, T is called *positive* if $T(A) \geq 0$ for all positive $A \in \mathcal{A}$. T is a *completely positive* map, (CP map), if $T \otimes Id : \mathcal{A} \otimes \mathcal{B} \to \mathcal{B}(\mathcal{H}_1) \otimes \mathcal{B}(\mathbb{C}^n)$ is positive for all $n \in \mathbb{N}$. In this case, Id is the identity map on $\mathcal{B}(\mathbb{C}^n)$ and $\mathbb{C}^n$ is isomorphic to a complex Hilbert space of dimension n. A map, T, is *trace preserving* if $tr(T(\rho)) = tr(\rho)$. T is a *quantum channel* if it is a *completely positive* and *trace preserving* map ($CPTP$ map). A family of quantum maps is *polynomial-time* if they can be written as a polynomial-time uniform family of quantum circuits. A quantum state is *polynomial-time generated* if it given as the output of a polynomial-time quantum map (which takes as input the all-zeros state) [17].

A permutation map, denoted throughout by π, is a unitary operation that acts on n qubits and permutes the order of the n qubits. This can equivalently be seen as a permutation, σ, of the indices of the qubits, where π would take the ith qubit to the $\sigma(i)^{th}$ position. Permutation maps are orthogonal, real valued matrices so $\pi^{-1} = \pi^\dagger$. We use Π_n to denote the set of all permutation maps on n qubits.

We denote a two-qubit maximally entangled pure state as $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. This is one of four Bell states. The other three Bell states are also maximally entangled pure states, $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, and $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The four Bell states are orthogonal and form a basis for two-qubit states. The four Bell states are therefore perfectly distinguishable and so we can perform a projective measurement into the Bell basis and determine which of the four Bell states we have. This is called a *Bell basis measurement*.

An $[[n, 1, d]]$-code is a quantum error correcting code that encodes one logical qubit into n qubits and has distance d; if $d = 2t + 1$, the code can correct up to t bit or phase flips. We assume that the decoding map can always be applied, but if more than t errors are present, it is not guaranteed to decode to the original input.

2.2 Pauli Matrices

The single-qubit *Pauli matrices* are given by:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ and } Y = iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{1}$$

Recall that if we allow complex coefficients, the any single-qubit gate can be written as a linear combination of the four single-qubit Pauli matrices.

An n-qubit Pauli matrix is given by the n-fold tensor product of single-qubit Paulis. We denote the set of all n-qubit Pauli matrices by $\mathbb{P}_n$, where $|\mathbb{P}_n| = 4^n$. Any n-qubit unitary operator, U, can also be written as a linear combination of n-qubit Paulis, again allowing for complex coefficients. This gives $U = \sum_{P \in \mathbb{P}_n} \alpha_P P$, with $\sum_{P \in \mathbb{P}_n} |\alpha_P|^2 = 1$, since U is unitary. This is called the *Pauli decomposition* of a unitary quantum operation.

The *Pauli weight* of an n-qubit Pauli, denoted $\omega(P)$, is the number of non-identity Paulis in the n-fold tensor product. We will also define sets of Paulis composed only of specific Pauli matrices, such as $\{I, X\}^{\otimes n}$ which is the set of all n-qubit Paulis composed of only I and X Paulis, or $\{I, Z\}^{\otimes n}$ which is the set of all n-qubit Paulis composed of only I and Z Paulis. Finally, Paulis are self-inverses, so $P = P^{-1} = P^\dagger$.

The following lemma, called the *Pauli Twirl* [10], shows how we can greatly simplify expressions that involve the twirling of an operation by the Pauli matrices:

Lemma 2.1 (Pauli Twirl). *Let P, P' be Pauli operators. Then for any ρ it holds that:*

$$\frac{1}{|\mathbb{P}_n|} \sum_{Q \in \mathbb{P}_n} Q^\dagger P Q \rho Q^\dagger P'^\dagger Q = \begin{cases} 0, & P \neq P' \\ P \rho P^\dagger, & \text{otherwise}. \end{cases}$$

2.3 Clifford Group

The *Clifford group*, $\mathcal{C}_n$, on n qubits are unitaries that map Pauli matrices to Pauli matrices (up to a phase of ± 1 or $\pm i$). Specifically, if $P \in \mathbb{P}_n$, then for all $C \in \mathcal{C}_n$, $\alpha C P C^\dagger \in \mathbb{P}_n$, for some $\alpha \in \{\pm 1, \pm i\}$. Not only do Cliffords map Paulis to Paulis, but they do so with a uniform distribution [1]:

Lemma 2.2 (Clifford Randomization). *Let P be a non-identity Pauli operator. Applying a random Clifford operator (by conjugation) maps it to a Pauli operator chosen uniformly over all non-identity Pauli operators. More formally, for every $P, Q \in \mathbb{P}_n \setminus \{\mathbb{I}\}$, it holds that:*

$$\left| \{C \in \mathcal{C}_n | C^\dagger P C = Q\} \right| = \frac{|\mathcal{C}_n|}{|\mathbb{P}_n| - 1}.$$

We also state a lemma that is analogous to the Pauli twirl, the *Clifford Twirl* [10].

Lemma 2.3 (Clifford Twirl). *Let $P \neq P'$ be Pauli operators. For any ρ it holds that:*

$$\sum_{C \in \mathcal{C}_n} C^\dagger P C \rho C^\dagger P' C = 0.$$

Finally, we note that sampling a uniformly random Clifford can be done efficiently [13].

3   Quantum Message Authentication

Following [11], we define a *quantum message authentication scheme* as a pair of
encoding and decoding maps that satisfy the following:

Definition 1 (Quantum Message Authentication Scheme). A *quantum message authentication scheme* is a polynomial-time set of encoding and decoding channels $\{(\mathcal{E}_k^{M \to C}, \mathcal{D}_k^{C \to MF}) \mid k \in \mathcal{K}\}$, where $\mathcal{K}$ is the set of possible keys, M is the input system, C is the encoded system, and F is a flag system that is spanned by two orthogonal states: $|\mathrm{acc}\rangle$ and $|\mathrm{rej}\rangle$, such that for all ρ_M, $(\mathcal{D}_k \circ \mathcal{E}_k)(\rho_M) = \rho_M \otimes |\mathrm{acc}\rangle \langle \mathrm{acc}|$.

In order to define security for a quantum message authentication scheme, we first consider a reference system R, so that the input can be described as ρ_{MR} and we can furthermore assume that the system consisting of the encoded message, together with the reference system, undergoes a unitary adversarial attack U_{CR}. For a fixed key, k, we thus define the *real-world* channel as:

$$\mathscr{E}_k^{MR \to MRF} : \rho_{MR} \mapsto (\mathcal{D}_k \otimes \mathbb{I}_R)(U_{CR}(\mathcal{E}_k \otimes \mathbb{I}_R)(\rho_{MR})U_{CR}^\dagger), \qquad (2)$$

where $\mathbb{I}_R$ is the identity map on the reference system, R. From now on, we will not include the identity maps, since it will be clear from context which system undergoes a linear map and which one does not.

Security is given in terms of the existence of a *simulator*, which has access only to the ideal functionality. This ideal functionality either accepts (and leaves the message register M intact), or rejects (and outputs a fixed state Ω_M); the simulator can interact with the ideal functionality by selecting *accept* or *reject*. In both cases, the simulator can also alter the reference system R. This ideal-world process is modeled by the quantum channel $\mathscr{F}$, called the *ideal* channel, where for each attack, U_{CR}, there exists two CP maps $\mathscr{U}^{acc}$ and $\mathscr{U}^{rej}$ acting only on the reference system R such that $\mathscr{U}^{acc} + \mathscr{U}^{rej} = \mathbb{1}$:

$$\mathscr{F}^{MR \to MRF} : \rho_{MR} \to (\mathbb{1}_M \otimes \mathscr{U}_R^{acc})\rho_{MR} \otimes |\mathrm{acc}\rangle \langle \mathrm{acc}|$$
$$+ tr_M((\mathbb{1}_M \otimes \mathscr{U}_R^{rej})\rho_{MR})\Omega_M \otimes |\mathrm{rej}\rangle \langle \mathrm{rej}| . \qquad (3)$$

Definition 2 (Security of Quantum Message Authentication). Let $\{(\mathcal{E}_k^{M \to C}, \mathcal{D}_k^{C \to MF}) \mid k \in \mathcal{K}\}$ be a quantum message authentication scheme, with keys k chosen from $\mathcal{K}$. Then the scheme is ϵ-secure if for all attacks, there exists a simulator such that:

$$D\Big(\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \mathscr{E}_k(\rho_{MR}), \mathscr{F}(\rho_{MR})\Big) \leq \epsilon, \forall \rho_{MR}. \qquad (4)$$

Furthermore, we require that if $\mathcal{E}_k$ is polynomial-time in the size of the input register M, then $\mathscr{F}$ is also polynomial-time in the size of the input register, M.

We note that this definition is similar to the definition in [11]; however we require a *polynomial-time simulation* whenever the attack is polynomial-time.

This does not limit the proof to polynomial-time attacks, but merely restricts the simulator to have at most the complexity of the attack. This condition being satisfied is typically a crucial ingredient in order for the composability to carry through [16].

4 Quantum Message Authentication Schemes

Here, we present two quantum message authentication schemes, the *Clifford* code (Sect. 4.1) and the *trap* code (Sect. 4.2). The two encoding procedures both proceed by appending trap qubits (in a fixed state) to the message register, and then *twirling* by a Clifford (for the Clifford code) or a Pauli (for the trap code). The trap code also has a permutation in addition to the Pauli twirl acting on the message register. Decoding simply consists of undoing the permutation in the trap code and then in both cases measuring the traps to check for any sign of tampering. In the case of the Clifford code, only one set of traps (all in the same state) is needed because the Clifford twirl breaks any Pauli attack into a uniform mixture of Paulis which is detected on the traps with high probability. The trap code, however, relies on two sets of traps (in two different states) with both a Pauli twirl and a permutation of the message and trap qubits. Furthermore, the trap scheme requires that we first *encode* the input message into an error correcting code (essentially, this is because the Pauli twirl is not as powerful as the Clifford twirl and will catch only high-weight Pauli attacks with the error correcting code taking care of the low-weight ones).

4.1 The Clifford Code

We define a message authentication scheme using a Clifford encryption as follows:

1. The encoding, $\mathcal{E}_k^{M \to C}$, takes as input an n-qubit message in the M system; it appends an additional d-qubit trap register in the state $|0\rangle \langle 0|^{\otimes d}$. A uniformly random Clifford is then applied to the resulting $n+d$-qubit register, according to the key, k. The output register is called C.
   Mathematically, the encoding, $\mathcal{E}_k^{M \to C}$, indexed by a secret key, k, on input ρ_M (where C_k the kth Clifford) is given by:

$$\mathcal{E}_k : \rho_M \mapsto C_k(\rho_M \otimes |0\rangle \langle 0|^{\otimes d})C_k^{\dagger}. \tag{5}$$

2. The decoding, $\mathcal{D}_k^{C \to MF}$, takes the C register and applies the inverse Clifford, according to the key, k. The last d qubits are then measured in the computational basis. If this measurement returns $|0\rangle \langle 0|^{\otimes d}$ then an additional qubit $|\text{acc}\rangle \langle \text{acc}|$ is appended in the flag system, F. If the measurements return anything else, then the remaining system, M, is traced out and replaced with a fixed n-qubit state, Ω_M, and an additional qubit, $|\text{rej}\rangle \langle \text{rej}|$, is appended in the flag system.
   Mathematically, the decoding, $\mathcal{D}_k^{C \to MF}$, also indexed by the secret key, k, is given by:

$$\mathcal{D}_k : \rho_C \mapsto tr_0(\mathcal{P}_{acc} C_k^\dagger (\rho_C) C_k \mathcal{P}_{acc}^\dagger) \otimes |\text{acc}\rangle \langle \text{acc}|$$
$$+ tr_{M,0}(\mathcal{P}_{rej} C_k^\dagger (\rho_C) C_k \mathcal{P}_{rej}^\dagger) \Omega_M \otimes |\text{rej}\rangle \langle \text{rej}|, \qquad (6)$$

where $\mathcal{P}_{acc} = \mathbb{1}^{\otimes n} \otimes |0\rangle \langle 0|^{\otimes d}$ and $\mathcal{P}_{rej} = \mathbb{1}^{\otimes (n+d)} - \mathcal{P}_{acc}$ are measurement projectors representing the trap qubits being in their initial states or altered, respectively. Finally, tr_0 refers to the trace over the d trap qubits.

4.2   The Trap Code

We define a trap code message authentication scheme as follows:

1. The encoding, $\mathcal{E}_k^{M \to C}$, takes as input ρ_M and applies an $[[n, 1, d]]$-error correcting code to the single-qubit M register, which will correct up to t errors (where $d = 2t + 1$). It then appends two additional n-qubit trap registers, the first in the state $|0\rangle \langle 0|^{\otimes n}$ and the second in the state $|+\rangle \langle +|^{\otimes n}$. The resulting $3n$-qubit register is then permuted and a Pauli encryption is applied, according to the key, k. The resulting register is called C.
Mathematically the encoding, $\mathcal{E}_k^{M \to C}$, indexed by a two-part secret key $k = (k_1, k_2)$ is given by:

$$\mathcal{E}_k : \rho_M \mapsto P_{k_2} \pi_{k_1} (Enc_M(\rho_M) \otimes |0\rangle \langle 0|^{\otimes n} \otimes |+\rangle \langle +|^{\otimes n}) \pi_{k_1}^\dagger P_{k_2}, \qquad (7)$$

where $Enc_M(\rho_M)$ represents the input state after the error correcting code has been applied to the M system, π_{k_1} is the k_1^{th} permutation and P_{k_2} is the k_2^{th} Pauli matrix.
We note that we use the error-correcting properties of the code only (it is sufficient in our context to simply correct low-weight Paulis on the message, as opposed detecting them and rejecting).

2. The decoding, $\mathcal{D}_k^{C \to MF}$, takes the C register and applies the inverse Pauli and then the inverse permutation according to the key, k. The last n qubits are then measured in the Hadamard basis and the second last n qubits are measured in the computational basis. If these two measurements return $|+\rangle \langle +|^{\otimes n}$ and $|0\rangle \langle 0|^{\otimes n}$ respectively, then an additional qubit $|\text{acc}\rangle \langle \text{acc}|$ is appended in the flag system F and the resulting M register is decoded (according to the error correcting code applied in the encoding). If the measurements return anything else, then the remaining system M is traced out and replaced with a fixed single-qubit state Ω_M and an additional qubit, $|\text{rej}\rangle \langle \text{rej}|$, is appended in the flag system.
Define $\mathbb{P}_\mathcal{E} = \{P \otimes R \otimes Q | P \in \mathbb{P}_n, R \in \{I, Z\}^{\otimes n}, Q \in \{I, X\}^{\otimes n}\}$. Then define the measurement projector corresponding to the protocol accepting as $\mathcal{P}_{acc} = \mathbb{1}^{\otimes n} \otimes |0\rangle \langle 0|^{\otimes n} \otimes |+\rangle \langle +|^{\otimes n}$. The accepted states are then the states that can be achieved by applying any $P \in \mathbb{P}_\mathcal{E}$ to $\rho_M \otimes |0\rangle \langle 0|^{\otimes n} \otimes |+\rangle \langle +|^{\otimes n}$. We define $\mathcal{P}_{rej} = \mathbb{1}^{\otimes 3n} - \mathcal{P}_{acc}$, the measurement projector corresponding to the protocol rejecting, where the states achieved by applying any $P \in \mathbb{P}_{3n} \backslash \mathbb{P}_\mathcal{E}$ to $Enc_M(\rho_M) \otimes |0\rangle \langle 0|^{\otimes n} \otimes |+\rangle \langle +|^{\otimes n}$ are rejected.
Mathematically, the decoding, $\mathcal{D}_k^{C \to MF}$, also indexed by the two-part secret key, k, is given by:

$$\mathcal{D}_k : \rho_C \mapsto Dec_M tr_{0,+}(\mathcal{P}_{acc}\pi_{k_1}^\dagger P_{k_2}(\rho_C)P_{k_2}\pi_{k_1}\mathcal{P}_{acc}^\dagger) \otimes |acc\rangle\langle acc|$$

$$+tr_{M,0,+}(\mathcal{P}_{rej}\pi_{k_1}^\dagger P_{k_2}(\rho_C)P_{k_2}\pi_{k_1}\mathcal{P}_{acc}^\dagger)\Omega_M \otimes |rej\rangle\langle rej| , \qquad (8)$$

where Dec_M is the decoding of the error correcting code applied in the encryption and $tr_{0,+}$ refers to the trace over the last two sets of n trap qubits.

5 Security of Quantum Message Authentication Schemes

In this section, we present simulation-based proofs for the Clifford (Sect. 5.1) and the trap (Sect. 5.2) codes. At a high level, the security of the two codes is analyzed in very similar ways (see the discussion in Sect. 1). The main idea (in both cases) is to use a simulator that replaces the encoded message in C with half EPR pairs, without encryption in the Clifford code, and with only a permutation in the trap code; the attack is then applied to these half EPR pairs, as well as any reference system R. From there we are able to compare the accepted and rejected states between the real world and ideal protocols in order to find the upper bound for the trace distance between them. We will notice that these differences are the cases where the real world protocol accepts something that the simulator rejects. Specifically, this is where an attack gets through and changes a logical qubit but is not detected in the traps. Of course, these same states are not rejected by the real world protocol but they are rejected by the simulator. Because the Clifford twirl maps any non-identity Pauli attack to a uniform mixture of non-identity Paulis, the bound for this distance is simple to compute in the case of the Clifford code. In the case of the trap code, a more complicated argument is needed based on permuting the attack and a combinatorial argument that bounds the undetected attacks that can alter the logical data.

5.1 Security of the Clifford Code

Simulator. Recall (Sect. 3) that the simulator interacts with the ideal functionality by only altering the reference system and selecting either *accept* or *reject*. Given the attack, U_{CR}, to which the simulator has access, the simulator will apply the attack to half EPR pairs in place of the C system and then perform a Bell basis measurement on the EPR pairs. It will select *accept* if the EPR pairs are still in their original state, and *reject* otherwise. Let $\mathcal{P}_{acc}^{\mathscr{U}} = \mathbb{1}_{MR} \otimes |\Phi^+\rangle\langle\Phi^+|_{C_1C_2}^{\otimes(n+d)}$ and $\mathcal{P}_{rej}^{\mathscr{U}} = \mathbb{1} - \mathcal{P}_{acc}^{\mathscr{U}}$. The ideal channel is then:

$$\mathscr{F}^{MR \to MRF} : \rho_{MR} \to$$
$$tr_{C_1C_2}(\mathcal{P}_{acc}^{\mathscr{U}}U_{C_1R}(\rho_{MR} \otimes |\Phi^+\rangle\langle\Phi^+|_{C_1C_2}^{\otimes(n+d)})U_{C_1R}^\dagger\mathcal{P}_{acc}^{\mathscr{U}\dagger}) \otimes |acc\rangle\langle acc|$$
$$+tr_M(tr_{C_1C_2}(\mathcal{P}_{rej}^{\mathscr{U}}U_{C_1R}(\rho_{MR} \otimes |\Phi^+\rangle\langle\Phi^+|_{C_1C_2}^{\otimes(n+d)})$$
$$U_{C_1R}^\dagger\mathcal{P}_{rej}^{\mathscr{U}\dagger}))\Omega_M \otimes |rej\rangle\langle rej| . \qquad (9)$$

According to the above, we define $\mathscr{U}^{acc}$ and $\mathscr{U}^{rej}$ that satisfy Eq. (3) as:

$$\mathscr{U}^{acc} : \rho_R \to tr_{C_1 C_2}(\mathcal{P}^{\mathscr{U}}_{acc} U_{C_1 R}(\rho_R \otimes |\Phi^+\rangle \langle\Phi^+|^{\otimes(n+d)}_{C_1 C_2})U^\dagger_{C_1 R}\mathcal{P}^{\mathscr{U}\dagger}_{acc}), \qquad (10)$$

and

$$\mathscr{U}^{rej} : \rho_R \to tr_{C_1 C_2}(\mathcal{P}^{\mathscr{U}}_{rej} U_{C_1 R}(\rho_R \otimes |\Phi^+\rangle \langle\Phi^+|^{\otimes(n+d)}_{C_1 C_2})U^\dagger_{C_1 R}\mathcal{P}^{\mathscr{U}\dagger}_{rej}). \qquad (11)$$

For a fixed attack $U_{CR} = \sum_{P \in \mathbb{P}_{n+d}} \alpha_P P_C \otimes U^P_R$, with $\sum_{P \in \mathbb{P}_{n+d}} |\alpha_P|^2 = 1$, we note the effects of $\mathscr{U}^{acc}$ and $\mathscr{U}^{rej}$, recalling, of course, that $\mathscr{U}^{acc}(\rho_{MR})$ is understood to be $(\mathbb{1}_M \otimes \mathscr{U}^{acc})(\rho_{MR})$, with the same understanding for $\mathscr{U}^{rej}$:

$$\mathscr{U}^{acc}(\rho_{MR}) = tr_{C_1 C_2}(\mathcal{P}^{\mathscr{U}}_{acc} U_{C_1 R}(\rho_{MR} \otimes |\Phi^+\rangle \langle\Phi^+|^{\otimes(n+d)}_{C_1 C_2})U^\dagger_{C_1 R}\mathcal{P}^{\mathscr{U}\dagger}_{acc})$$
$$= |\alpha_{\mathbb{1}}|^2 (\mathbb{1}_M \otimes U^{\mathbb{1}}_R)\rho_{MR}(\mathbb{1}_M \otimes U^{\mathbb{1}\dagger}_R) \qquad (12)$$

$$\mathscr{U}^{rej}(\rho_{MR}) = tr_{C_1 C_2}\Big(\mathcal{P}^{\mathscr{U}}_{rej}\Big(\sum_{P \neq \mathbb{1}} |\alpha_P|^2 P_{C_1} \otimes U^P_R \Big)$$

$$\qquad (\rho_{MR} \otimes |\Phi^+\rangle \langle\Phi^+|^{\otimes(n+d)}_{C_1 C_2})\Big(\sum_{P \neq \mathbb{1}} |\alpha_P|^2 P_{C_1} \otimes U^{P\dagger}_R \Big)\mathcal{P}^{\mathscr{U}\dagger}_{rej}\Big)$$

$$= \sum_{P \neq \mathbb{1}} |\alpha_P|^2 (\mathbb{1}_M \otimes U^P_R)(\rho_{MR})(\mathbb{1}_M \otimes U^{P\dagger}_R). \qquad (13)$$

We are now ready to state and prove our main theorem on the security of the Clifford message authentication scheme.

Theorem 5.1. *Let* $\{(\mathcal{E}^{S \to C}_k, \mathcal{D}^{C \to SF}_k) \mid k \in \mathcal{K}\}$ *be the Clifford quantum message authentication scheme, with parameter d. Then the Clifford code is an ϵ-secure quantum authentication scheme, for $\epsilon \leq \frac{3}{2^d}$.*

Proof. We will follow the proof structure used in [1,11].

Using the simulator described above, we wish to show that:

$$D\Big(\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \mathcal{E}_k(\rho_{MR}), \mathscr{F}(\rho_{MR})\Big) \leq \epsilon, \forall \rho_{MR}. \qquad (14)$$

Consider a general attack U_{CR}, written as $U_{CR} = \sum_{P \in \mathbb{P}_{n+d}} \alpha_P P_C \otimes U^P_R$ where $\sum_{P \in \mathbb{P}_{n+d}} |\alpha_P|^2 = 1$. The real-world channel is then represented as:

$$\mathcal{E}_k^{MR \to MRF} : \rho_{MR} \mapsto \mathcal{D}_k\Big(\Big(\sum_{P \in \mathbb{P}_{n+d}} \alpha_P P_C \otimes U^P_R \Big)\mathcal{E}_k(\rho_{MR})$$

$$\Big(\sum_{P \in \mathbb{P}_{n+d}} \overline{\alpha_P} P_C \otimes U^{P\dagger}_R \Big)\Big). \qquad (15)$$

We will use $\psi = \rho_{MR} \otimes |0\rangle \langle 0|^{\otimes d}$ to simplify the following expressions. Consider the effect of the real protocol on input ρ_{MR} with attack $\sum_{P \in \mathbb{P}_{n+d}} \alpha_P P_C \otimes U_R^P$, conditioned on acceptance:

$$\frac{1}{|\mathcal{K}|} \sum_{k \epsilon \mathcal{K}} tr_0 \Big(\mathcal{P}_{acc} C_k^\dagger \Big(\sum_{P \in \mathbb{P}_{n+d}} \alpha_P P_C \otimes U_R^P \Big) (C_k \psi C_k^\dagger)$$
$$\Big(\sum_{P \in \mathbb{P}_{n+d}} \overline{\alpha_P} P_C^\dagger \otimes U_R^{P\dagger} \Big) C_k \mathcal{P}_{acc}^\dagger \Big) \otimes |acc\rangle \langle acc| . \qquad (16)$$

Now we can apply the Clifford Twirl (Lemma 2.3), since the sum over all keys is, of course, the sum over all Cliffords (since the keys index all $n + d$-qubit Cliffords) and then simply split the sum over all Paulis into the case with the identity Pauli from the attack, and all other Paulis. What we are left with is:

$$\frac{1}{|\mathcal{K}|} \sum_{k \epsilon \mathcal{K}} tr_0 \Big(\sum_{P \in \mathbb{P}_{n+d}} |\alpha_P|^2 \mathcal{P}_{acc} C_k^\dagger (P_C \otimes U_R^P)(C_k \psi C_k^\dagger)$$
$$(P_C^\dagger \otimes U_R^{P\dagger}) C_k \mathcal{P}_{acc}^\dagger \Big) \otimes |acc\rangle \langle acc|$$
$$= \frac{1}{|\mathcal{K}|} \sum_{k \epsilon \mathcal{K}} tr_0 \Big(|\alpha_{\mathbb{1}}|^2 \mathcal{P}_{acc} C_k^\dagger (\mathbb{1}_C \otimes U_R^{\mathbb{1}})(C_k \psi C_k^\dagger)$$
$$(\mathbb{1}_C \otimes U_R^{\mathbb{1}\dagger}) C_k \mathcal{P}_{acc}^\dagger \Big) \otimes |acc\rangle \langle acc|$$
$$+ \frac{1}{|\mathcal{K}|} \sum_{k \epsilon \mathcal{K}} tr_0 \Big(\sum_{P \neq \mathbb{1}} |\alpha_P|^2 \mathcal{P}_{acc} C_k^\dagger (P_C \otimes U_R^P)(C_k \psi C_k^\dagger)$$
$$(P_C^\dagger \otimes U_R^{P\dagger}) C_k \mathcal{P}_{acc}^\dagger \Big) \otimes |acc\rangle \langle acc| . \qquad (17)$$

Clearly the first term is exactly what the simulator will accept, and the second term is in exactly the right form to use a Clifford Randomization (Lemma 2.2), resulting in:

$$= \mathscr{U}^{acc}(\rho_{MR}) \otimes |acc\rangle \langle acc|$$
$$+ \frac{1}{|\mathcal{C}_n|} tr_0 \Big(\sum_{\tilde{P} \neq \mathbb{1}} \sum_{P \neq \mathbb{1}} |\alpha_P|^2 \frac{|\mathcal{C}_n|}{|\mathbb{P}_n| - 1} \mathcal{P}_{acc} (\tilde{P}_C \otimes U_R^P) \psi$$
$$(\tilde{P}_C^\dagger \otimes U_R^{P\dagger}) \mathcal{P}_{acc}^\dagger \Big) \otimes |acc\rangle \langle acc| . \qquad (18)$$

The $\tilde{P}$s are the results of the Clifford Randomization applied to a Pauli, P. The randomization is not applied to the reference system, so the U_R^P terms are not changed by the randomization. We can use the properties of the trace to move the trace inside the first sum, and we can move the $\frac{|\mathcal{C}_n|}{|\mathbb{P}_n|-1}$ coefficient out of both of the sums:

$$= \mathscr{U}^{acc}(\rho_{MR}) \otimes |acc\rangle \langle acc|$$
$$+ \frac{1}{|\mathcal{C}_n|} \frac{|\mathcal{C}_n|}{|\mathbb{P}_n| - 1} \Big(\sum_{\tilde{P} \neq \mathbb{1}} tr_0 \sum_{P \neq \mathbb{1}} |\alpha_P|^2 \, \mathcal{P}_{acc}(\tilde{P}_C \otimes U_R^P)\psi$$
$$(\tilde{P}_C^\dagger \otimes U_R^{P\dagger})\mathcal{P}_{acc}^\dagger \Big) \otimes |acc\rangle \langle acc| . \tag{19}$$

We recognize the R register in the second sum as the states that the simulator will reject. Recall that the simulator is in terms of the sum over all non-identity Paulis and includes the α_P coefficients. We can therefore write the previous line in terms of the simulator as:

$$= \mathscr{U}^{acc}(\rho_{MR}) \otimes |acc\rangle \langle acc|$$
$$+ \frac{1}{|\mathbb{P}_{n+d}| - 1} \Big(\sum_{\tilde{P} \neq \mathbb{1}} tr_0 \mathcal{P}_{acc}(\tilde{P}_C(\mathscr{U}^{rej}(\rho_{MR})$$
$$\otimes |0\rangle \langle 0|^{\otimes d})\tilde{P}_C^\dagger)\mathcal{P}_{acc}^\dagger \Big) \otimes |acc\rangle \langle acc| . \tag{20}$$

If we let $\mathbb{P}_t$ be the set of all Paulis that do not alter the trap qubits, then when we apply $\mathcal{P}_{acc}$ to the above, we end up with the sum over the $\tilde{P} \in \mathbb{P}_t \setminus \{\mathbb{1}\}$. Therefore the previous line can be simplified to:

$$= \mathscr{U}^{acc}(\rho_{MR}) \otimes |acc\rangle \langle acc|$$
$$+ \frac{1}{|\mathbb{P}_{n+d}| - 1} \sum_{\tilde{P} \in \mathbb{P}_t \setminus \mathbb{1}} tr_0(\tilde{P}_C(\mathscr{U}^{rej}(\rho_{MR}) \otimes |0\rangle \langle 0|^{\otimes d})\tilde{P}_C^\dagger) \otimes |acc\rangle \langle acc| .$$
$$\tag{21}$$

The effect of the real protocol on input ρ_{MR} with attack $\sum_{P \in \mathbb{P}_{n+d}} \alpha_P P_C \otimes U_R^P$, conditioned on rejection, can be manipulated in the same way:

$$\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Big(tr_{M,0} \Big(\mathcal{P}_{rej} \mathcal{C}_k^\dagger \Big(\sum_{P \in \mathbb{P}_{n+d}} \alpha_P P_C \otimes U_R^P \Big)(C_k(\psi)C_k^\dagger)$$
$$\Big(\sum_{P \in \mathbb{P}_{n+d}} \overline{\alpha_P} P_C^\dagger \otimes U_R^{P\dagger} \Big) C_k \mathcal{P}_{rej}^\dagger \Big) \Big) \Omega_M \otimes |rej\rangle \langle rej|$$
$$= \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Big(tr_{M,0}(|\alpha_{\mathbb{1}}|^2 \mathcal{P}_{rej} C_k^\dagger (\mathbb{1}_C \otimes U_R^{\mathbb{1}})(C_k(\psi)C_k^\dagger)$$
$$(\mathbb{1}_C \otimes U_R^{\mathbb{1}\dagger}) C_k \mathcal{P}_{rej}^\dagger \Big) \Big) \Omega_M \otimes |rej\rangle \langle rej|$$
$$+ \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Big(tr_{M,0} \Big(\sum_{P \neq \mathbb{1}} |\alpha_P|^2 \mathcal{P}_{rej} C_k^\dagger (P_C \otimes U_R^P)(C_k(\psi)C_k^\dagger)$$
$$(P_C^\dagger \otimes U_R^{P\dagger}) C_k \mathcal{P}_{rej}^\dagger \Big) \Big) \Omega_M \otimes |rej\rangle \langle rej|$$

$$= \frac{1}{|\mathbb{P}_{n+d}| - 1} \sum_{\tilde{P} \neq \mathbb{1}} \sum_{P \neq \mathbb{1}} |\alpha|^2 \left(tr_{M,0}(\mathcal{P}_{acc}(\tilde{P}_C \otimes U_R^P)(\psi) \right.$$

$$\left. (\tilde{P}_C^\dagger \otimes U_R^{P\dagger})\mathcal{P}_{acc}^\dagger) \right) \Omega_M \otimes |\text{rej}\rangle \langle\text{rej}|$$

$$= tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}|$$

$$- \frac{1}{|\mathbb{P}_{n+d}| - 1} tr_M \left(\sum_{P \in \mathbb{P}_t \backslash \mathbb{1}} \mathcal{U}^{rej}(\rho_{MR}) \right) \Omega_M |\text{rej}\rangle \langle\text{rej}|$$

$$= tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}|$$

$$- \frac{4^n 2^d - 1}{|\mathbb{P}_{n+d}| - 1} tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}| . \tag{22}$$

When we combine the accepted states and the rejected states into the real world protocol given by Eq. (15), we can write it in terms of the simulator as:

$$\mathcal{D}_k(U_{CR}\mathcal{E}_k(\rho_{MR})U_{CR}^\dagger)$$
$$= \mathcal{U}^{acc}(\rho_{MR}) \otimes |\text{acc}\rangle \langle\text{acc}|$$
$$+ \frac{1}{|\mathbb{P}_{n+d}| - 1} \sum_{\tilde{P} \in \mathbb{P}_t \backslash \mathbb{1}} tr_0(\tilde{P}_C(\mathcal{U}^{rej}(\rho_{MR}) \otimes |0\rangle \langle0|^{\otimes d})\tilde{P}_C^\dagger) \otimes |\text{acc}\rangle \langle\text{acc}|$$
$$+ tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}|$$
$$- \frac{4^n 2^d - 1}{|\mathbb{P}_{n+d}| - 1} tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}| . \tag{23}$$

We can therefore write Eq. (14) as:

$$\frac{1}{2} \left\| \mathcal{U}^{acc}(\rho_{MR}) \otimes |\text{acc}\rangle \langle\text{acc}| \right.$$
$$+ \frac{1}{|\mathbb{P}_{n+d}| - 1} \sum_{\tilde{P} \in \mathbb{P}_t \backslash \mathbb{1}} tr_0(\tilde{P}_C(\mathcal{U}^{rej}(\rho_{MR}) \otimes |0\rangle \langle0|^{\otimes d})\tilde{P}_C^\dagger) \otimes |\text{acc}\rangle \langle\text{acc}|$$
$$+ tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}|$$
$$- \frac{4^n 2^d - 1}{|\mathbb{P}_{n+d}| - 1} tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}|$$
$$\left. - (\mathcal{U}^{acc}(\rho_{MR}) \otimes |\text{acc}\rangle \langle\text{acc}| + tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}|) \right\|_1$$
$$= \frac{1}{2} \left\| \frac{1}{|\mathbb{P}_{n+d}| - 1} \sum_{\tilde{P} \in \mathbb{P}_t \backslash \mathbb{1}} tr_0(\tilde{P}_C(\mathcal{U}^{rej}(\rho_{MR}) \otimes |0\rangle \langle0|^{\otimes d})\tilde{P}_C^\dagger) \otimes |\text{acc}\rangle \langle\text{acc}| \right.$$
$$\left. - \frac{4^n 2^d - 1}{|\mathbb{P}_{n+d}| - 1} tr_M(\mathcal{U}^{rej}(\rho_{MR}))\Omega_M \otimes |\text{rej}\rangle \langle\text{rej}| \right\|_1 \tag{24}$$

Since $|\mathbb{P}_t \setminus \mathbb{1}| = 4^n 2^d - 1$, and the maximum trace distance between two states is 1, we can see that by the triangle inequality, the above is bounded by:

$$
\begin{aligned}
&\leq \frac{4^n 2^d - 1}{|\mathbb{P}_{n+d}| - 1} \\
&= \frac{4^n 2^d - 1}{4^{n+d} - 1} = \frac{1 - \frac{1}{4^n 2^d}}{2^d - \frac{1}{4^n 2^d}} \\
&\leq 3 \times \frac{1}{2^d}.
\end{aligned}
\tag{25}
$$

This concludes the proof, showing that the Clifford code is $\frac{3}{2^d}$-secure. $\qquad\square$

This is identical to the bound of $\frac{6}{2^d}$ achieved in [11] when we consider that we use the trace distance in our definition of security, and [11] uses the trace norm, which differs from the trace distance by a factor of 2.

5.2   Security of the Trap Code

Simulator. Recall (Sect. 3) that the simulator interacts with the ideal functionality by only altering the reference system and selecting either *accept* or *reject*. Given the attack, U_{CR}, to which the simulator has access, the simulator will apply the attack to randomly permuted half EPR pairs in place of the C system and then de-permute the EPR pairs and perform a Bell basis measurement. It will select *accept* if the first n of the EPR pairs have $\leq t$ errors, the next n of the EPR pairs are either unchanged or have phase flip errors, and the last n of the EPR pairs are either unchanged or have bit flip errors. It will select *reject* otherwise. Let $\mathbb{P}_{\mathscr{F}} = \{P \otimes R \otimes Q | P \in \mathbb{P}_n, \omega(P) \leq t, R \in \{I, Z\}^{\otimes n}, Q \in \{I, X\}^{\otimes n}\}$. Specifically, $\mathbb{P}_{\mathscr{F}}$ is the set of all Paulis that the ideal protocol will accept being applied to the half EPR pair—Paulis that would apply at most t non-identity Paulis on the message space and would not alter the $|0\rangle\langle 0|^{\otimes n}$ or the $|+\rangle\langle +|^{\otimes n}$ traps in the real world protocol. Finally, define the measurement projector corresponding to the simulator selecting *accept* as:

$$
\begin{aligned}
\mathcal{P}_{acc}^{\mathscr{U}} &= \sum_{Q \in \{I,X\}^{\otimes n}} \sum_{R \in \{I,Z\}^{\otimes n}} \sum_{P \in \mathbb{P}_n | \omega(P) \leq t} \mathbb{1}_{MR} \otimes (P \otimes R \otimes Q)_{C_1} \\
&\qquad\qquad |\Phi^+\rangle\langle\Phi^+|_{C_1 C_2}^{\otimes 3n} (P \otimes R \otimes Q)_{C_1} \\
&= \sum_{P \in \mathbb{P}_{\mathscr{F}}} \mathbb{1}_{MR} \otimes (P_{C_1} |\Phi^+\rangle\langle\Phi^+|_{C_1 C_2}^{\otimes 3n} P_{C_1}^\dagger),
\end{aligned}
\tag{26}
$$

and the measurement projector corresponding to the simulator selecting *reject* as:

$$
\mathcal{P}_{rej}^{\mathscr{U}} = \mathbb{1} - \mathcal{P}_{acc}^{\mathscr{U}}.
\tag{27}
$$

The ideal channel with attack U_{C_1R} is therefore:

$$
\mathscr{F}^{MR \to MRF} : \rho_{MR} \to tr_{C_1C_2} \frac{1}{|\Pi_{3n}|} \sum_{\pi \in \Pi_{3n}} \Big(\mathcal{P}^{\mathscr{U}}_{acc} \pi^{\dagger}_{C_1} U_{C_1R} \pi_{C_1}
$$

$$
(\rho_{MR} \otimes |\Phi^+\rangle \langle \Phi^+|^{\otimes 3n}_{C_1C_2}) \pi^{\dagger}_{C_1} U^{\dagger}_{C_1R} \pi_{C_1} \mathcal{P}^{\mathscr{U}\dagger}_{acc} \Big) \otimes |acc\rangle \langle acc|
$$

$$
+ tr_M \Big(tr_{C_1C_2} \frac{1}{|\Pi_{3n}|} \sum_{\pi \in \Pi_{3n}} \Big(\mathcal{P}^{\mathscr{U}}_{rej} \pi^{\dagger}_{C_1} U_{C_1R} \pi_{C_1} (\rho_{MR} \otimes |\Phi^+\rangle \langle \Phi^+|^{\otimes 3n}_{C_1C_2})
$$

$$
\pi^{\dagger}_{C_1} U^{\dagger}_{C_1R} \pi_{C_1} \mathcal{P}^{\mathscr{U}\dagger}_{rej} \Big) \Big) \Omega_M \otimes |rej\rangle \langle rej| . \tag{28}
$$

For a fixed attack $U_{CR} = \sum_{P \in \mathbb{P}_{3n}} \alpha_P P_C \otimes U^P_R$, with $\sum_{P \in \mathbb{P}_{3n}} |\alpha_P|^2 = 1$ and where for the sake of brevity we will represent $\rho_{MR} \otimes |\Phi^+\rangle \langle \Phi^+|^{\otimes 3n}_{C_1C_2}$ with $\phi_{MRC_1C_2}$, the ideal channel becomes:

$$
\mathscr{F}^{MR \to MRF} : \rho_{MR} \to
$$

$$
tr_{C_1C_2} \frac{1}{|\Pi_{3n}|} \sum_{\pi \in \Pi_{3n}} \Big(\mathcal{P}^{\mathscr{U}}_{acc} \pi^{\dagger}_{C_1} \Big(\sum_{P \in \mathbb{P}_{3n}} \alpha_P P_{C_1} \otimes U^P_R \Big) \pi_{C_1} \phi_{MRC_1C_2}
$$

$$
\pi^{\dagger}_{C_1} \Big(\sum_{P \in \mathbb{P}_{3n}} \overline{\alpha_P} P_{C_1} \otimes U^{P\dagger}_R \Big) \pi_{C_1} \mathcal{P}^{\mathscr{U}\dagger}_{acc} \otimes |acc\rangle \langle acc|
$$

$$
+ tr_M \Big(\mathcal{P}^{\mathscr{U}}_{rej} \pi^{\dagger}_{C_1} \Big(\sum_{P \in \mathbb{P}_{3n}} \alpha_P P_{C_1} \otimes U^P_R \Big) \pi_{C_1} \phi_{MRC_1C_2}
$$

$$
\pi^{\dagger}_{C_1} \Big(\sum_{P \in \mathbb{P}_{3n}} \overline{\alpha_P} P_{C_1} \otimes U^{P\dagger}_R \Big) \pi_{C_1} \mathcal{P}^{\mathscr{U}\dagger}_{rej} \Big) \Omega_M \otimes |rej\rangle \langle rej| \Big). \tag{29}
$$

From here we will move the permutations to act on the attack Paulis, since they're all applied to the same register, C_1:

$$
= tr_{C_1C_2} \frac{1}{|\Pi_{3n}|} \sum_{\pi \in \Pi_{3n}} \Big(\Big(\mathcal{P}^{\mathscr{U}}_{acc} \Big(\sum_{P \in \mathbb{P}_{3n}} \alpha_P \pi^{\dagger}_{C_1} P_{C_1} \pi_{C_1} \otimes U^P_R \Big) \phi_{MRC_1C_2}
$$

$$
\Big(\sum_{P \in \mathbb{P}_{3n}} \overline{\alpha_P} \pi^{\dagger}_{C_1} P_{C_1} \pi_{C_1} \otimes U^{P\dagger}_R \Big) \mathcal{P}^{\mathscr{U}\dagger}_{acc} \Big) \otimes |acc\rangle \langle acc|
$$

$$
+ tr_M \Big(\mathcal{P}^{\mathscr{U}}_{rej} \Big(\sum_{P \in \mathbb{P}_{3n}} \alpha_P \pi^{\dagger}_{C_1} P_{C_1} \pi_{C_1} \otimes U^P_R \Big) \phi_{MRC_1C_2}
$$

$$
\Big(\sum_{P \in \mathbb{P}_{3n}} \overline{\alpha_P} \pi^{\dagger}_{C_1} P_{C_1} \pi_{C_1} \otimes U^{P\dagger}_R \Big) \mathcal{P}^{\mathscr{U}\dagger}_{rej} \Big) \Omega_M \otimes |rej\rangle \langle rej| \Big). \tag{30}
$$

Finally we apply the projectors:

$$
= tr_{C_1 C_2} \frac{1}{|\Pi_{3n}|} \sum_{\pi \in \Pi_{3n}} \Bigg(\Big(\sum_{P | \pi^\dagger P \pi \in \mathbb{P}_{\mathscr{F}}} |\alpha_P|^2 \, (\pi_{C_1}^\dagger P_{C_1} \pi_{C_1} \otimes U_R^P)(\phi_{MRC_1 C_2})
$$

$$
(\pi_{C_1}^\dagger P_{C_1} \pi_{C_1} \otimes U_R^{P\dagger}) \Big) \otimes |\text{acc}\rangle \langle \text{acc}|
$$

$$
+ tr_M \Big(\sum_{P | \pi^\dagger P \pi \notin \mathbb{P}_{\mathscr{F}}} |\alpha_P|^2 \, (\pi_{C_1}^\dagger P_{C_1} \pi_{C_1} \otimes U_R^P)(\phi_{MRC_1 C_2})
$$

$$
(\pi_{C_1}^\dagger P_{C_1} \pi_{C_1} \otimes U_R^{P\dagger}) \Big) \Omega_M \otimes |\text{rej}\rangle \langle \text{rej}| \Bigg). \tag{31}
$$

We are now ready to present our main theorem on the security of the trap code:

Theorem 5.2. *Let* $\{(\mathcal{E}_k^{S \to C}, \mathcal{D}_k^{C \to SF}) \mid k \in \mathcal{K}\}$ *be the trap quantum message authentication scheme with parameter* t, *the number of bit or phase flip errors that the error correcting code applied to the input message qubit can correct. Then the trap code is an* ϵ-*secure quantum message authentication scheme, for* $\epsilon \leq (\frac{1}{3})^{t+1}$.

Proof. Using the simulator described above, we wish to show that:

$$
D\Big(\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \mathcal{E}_k(\rho_{MR}), \mathscr{F}(\rho_{MR})\Big) \leq \epsilon, \forall \rho_{MR}. \tag{32}
$$

Consider a general attack U_{CR}, written as $U_{CR} = \sum\limits_{P \in \mathbb{P}_{3n}} \alpha_P P_C \otimes U_R^P$ with $\sum\limits_{P \in \mathbb{P}_{3n}} |\alpha_P|^2 = 1$. Let $\psi = Enc_M(\rho_{MR}) \otimes |0\rangle \langle 0|^{\otimes n} \otimes |+\rangle \langle +|^{\otimes n}$. The real-world channel is then represented as:

$$
\mathscr{E}_k^{MR \to MRF} : \rho_{MR} \mapsto \mathcal{D}_k \Big(\Big(\sum_{P \in \mathbb{P}_{3n}} \alpha_P P_C \otimes U_R^P \Big) \mathcal{E}_k(\rho_{MR})
$$

$$
\Big(\sum_{P \in \mathbb{P}_{3n}} \overline{\alpha_P} P_C \otimes U_R^{P\dagger} \Big) \Big) \tag{33}
$$

$$
= \frac{1}{|\mathcal{K}|} tr_{0,+} \sum_{k \in \mathcal{K}} \Bigg(Dec_M \Big(\mathcal{P}_{acc} \pi_{k_1}^\dagger P_{k_2} \Big(\sum_{P \in \mathbb{P}_{3n}} \alpha_P P_C \otimes U_R^P \Big) P_{k_2} \pi_{k_1} \psi
$$

$$
\pi_{k_1}^\dagger P_{k_2} \Big(\sum_{P \in \mathbb{P}_{3n}} \overline{\alpha_P} P_C \otimes U_R^{P\dagger} \Big) P_{k_2} \pi_{k_1} \mathcal{P}_{acc}^\dagger \Big) \otimes |\text{acc}\rangle \langle \text{acc}|
$$

$$
+ tr_M \Big(\mathcal{P}_{rej} \pi_{k_1}^\dagger P_{k_2} \Big(\sum_{P \in \mathbb{P}_{3n}} \alpha_P P_C \otimes U_R^P \Big) (P_{k_2} \pi_{k_1} \psi \pi_{k_1}^\dagger P_{k_2})
$$

$$
\Big(\sum_{P \in \mathbb{P}_{3n}} \overline{\alpha_P} P_C \otimes U_R^{P\dagger} \Big) P_{k_2} \pi_{k_1} \mathcal{P}_{rej}^\dagger \Big) \Omega_M \otimes |\text{rej}\rangle \langle \text{rej}| \Bigg). \tag{34}
$$

From here we apply the Pauli Twirl (Lemma 2.1):

$$
= \frac{1}{|\mathcal{K}_1|} tr_{0,+} \sum_{k_1 \in \mathcal{K}_1} \Bigg(Dec_M \Big(\mathcal{P}_{acc} \pi_{k_1}^{\dagger} \Big(\sum_{P \in \mathbb{P}_{3n}} |\alpha_P|^2 (P_C \otimes U_R^P) \pi_{k_1} \psi
$$
$$
\pi_{k_1}^{\dagger} (P_C \otimes U_R^{P\dagger}) \Big) \pi_{k_1} \mathcal{P}_{acc}^{\dagger} \Big) \otimes |acc\rangle \langle acc|
$$
$$
+ tr_M \Big(\mathcal{P}_{rej} \pi_{k_1}^{\dagger} \Big(\sum_{P \in \mathbb{P}_{3n}} |\alpha_P|^2 (P_C \otimes U_R^P) \pi_{k_1} \psi
$$
$$
\pi_{k_1}^{\dagger} (P_C \otimes U_R^{P\dagger}) \Big) \pi_{k_1} \mathcal{P}_{rej}^{\dagger} \Big) \Omega_M \otimes |rej\rangle \langle rej| \Bigg). \tag{35}
$$

Since the permutations act on the same register as the attack Paulis, we can move the permutations to be considered to be acting on the Paulis instead of the message and traps:

$$
= \frac{1}{|\mathcal{K}_1|} tr_{0,+} \sum_{k_1 \in \mathcal{K}_1} \Bigg(Dec_M \Big(\mathcal{P}_{acc} \Big(\sum_{P \in \mathbb{P}_{3n}} |\alpha_P|^2 (\pi_{k_1}^{\dagger} P_C \pi_{k_1} \otimes U_R^P) \psi
$$
$$
(\pi_{k_1}^{\dagger} P_C \pi_{k_1} \otimes U_R^{P\dagger}) \Big) \mathcal{P}_{acc}^{\dagger} \Big) \otimes |acc\rangle \langle acc|
$$
$$
+ tr_M \Big(\mathcal{P}_{rej} \Big(\sum_{P \in \mathbb{P}_{3n}} |\alpha_P|^2 (\pi_{k_1}^{\dagger} P_C \pi_{k_1} \otimes U_R^P) \psi
$$
$$
(\pi_{k_1}^{\dagger} P_C \pi_{k_1} \otimes U_R^{P\dagger}) \Big) \mathcal{P}_{rej}^{\dagger} \Big) \Omega_M \otimes |rej\rangle \langle rej| \Bigg). \tag{36}
$$

Finally we apply the projectors and notice that $\mathcal{K}_1 = \Pi_{3n}$:

$$
= \frac{1}{|\Pi_{3n}|} tr_{0,+} \sum_{\pi \in \Pi_{3n}} \Bigg(Dec_M \Big(\sum_{P | \pi^{\dagger} P \pi \in \mathbb{P}_{\mathscr{E}}} |\alpha_P|^2 (\pi^{\dagger} P_C \pi \otimes U_R^P) \psi
$$
$$
(\pi^{\dagger} P_C \pi \otimes U_R^{P\dagger}) \Big) \otimes |acc\rangle \langle acc|
$$
$$
+ tr_M \Big(\sum_{P | \pi^{\dagger} P \pi \in \mathbb{P}_{3n} \backslash \mathbb{P}_{\mathscr{E}}} |\alpha_P|^2 (\pi^{\dagger} P_C \pi \otimes U_R^P) \psi
$$
$$
(\pi^{\dagger} P_C \pi \otimes U_R^{P\dagger}) \Big) \Omega_M \otimes |rej\rangle \langle rej| \Bigg). \tag{37}
$$

Then:

$$
\frac{1}{2} \Big\| \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \mathscr{E}_k(\rho_{MR}) - \mathscr{F}(\rho_{MR}) \Big\|_1
$$
$$
= \frac{1}{2} \Big\| \frac{1}{|\Pi_{3n}|} \sum_{\pi \in \Pi_{3n}} \Big(tr_{0,+} \Big(Dec_M \Big(\sum_{P | \pi^{\dagger} P \pi \in \mathbb{P}_{\mathscr{E}}} |\alpha_P|^2 (\pi^{\dagger} P_C \pi \otimes U_R^P) \psi
$$

$$\left(\pi^\dagger P_C \pi \otimes U_R^{P\dagger}\right)\right) \otimes |\mathrm{acc}\rangle\langle\mathrm{acc}|$$

$$+ tr_M\left(\sum_{P|\pi^\dagger P\pi \in \mathbb{P}_{3n}\setminus\mathbb{P}_{\mathscr{E}}} |\alpha_P|^2\,(\pi^\dagger P_C\pi \otimes U_R^P)\psi\right.$$

$$\left.\left(\pi^\dagger P_C\pi \otimes U_R^{P\dagger}\right)\right)\Omega_M \otimes |\mathrm{rej}\rangle\langle\mathrm{rej}|\right)$$

$$- tr_{C_1 C_2}\left(\sum_{P|\pi^\dagger P\pi \in \mathbb{P}_{\mathscr{F}}} |\alpha_P|^2\,(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^P)(\phi_{MRC_1 C_2})\right.$$

$$\left.\left(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^{P\dagger}\right)\right) \otimes |\mathrm{acc}\rangle\langle\mathrm{acc}|$$

$$- tr_{MC_1 C_2}\left(\sum_{P|\pi^\dagger P\pi \notin \mathbb{P}_{\mathscr{F}}} |\alpha_P|^2\,(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^P)(\phi_{MRC_1 C_2})\right.$$

$$\left.\left(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^{P\dagger}\right)\right)\Omega_M \otimes |\mathrm{rej}\rangle\langle\mathrm{rej}|\right)\Bigg\|_1. \tag{38}$$

We will subtract the accepted states in the ideal protocol from those accepted in the real protocol and we will subtract the rejected states in the real protocol from the rejected states in the ideal protocol. Note that $\mathbb{P}_{\mathscr{E}} \setminus \mathbb{P}_{\mathscr{F}} = \{P \otimes R \otimes Q | P \in \mathbb{P}_n, \omega(P) > t, R \in \{I, Z\}^{\otimes n}, Q \in \{I, X\}^{\otimes n}\}$.

$$= \frac{1}{2}\Bigg\|\frac{1}{|\Pi_{3n}|}\sum_{\pi \in \Pi_{3n}}\sum_{P|\pi^\dagger P\pi \in \mathbb{P}_{\mathscr{E}}\setminus\mathbb{P}_{\mathscr{F}}}\left(tr_{0,+}\Big(Dec_M(|\alpha_P|^2\,(\pi^\dagger P_C\pi \otimes U_R^P)\psi\right.$$

$$\left.\left(\pi^\dagger P_C\pi \otimes U_R^{P\dagger})\Big)\right) \otimes |\mathrm{acc}\rangle\langle\mathrm{acc}|$$

$$- tr_{MC_1 C_2}\Big(|\alpha_P|^2\,(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^P)(\phi_{MRC_1 C_2})$$

$$\left.\left(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^{P\dagger}\right)\Big)\Omega_M \otimes |\mathrm{rej}\rangle\langle\mathrm{rej}|\right)\Bigg\|_1. \tag{39}$$

Here we will use the triangle inequality to remove the sums from the trace distance:

$$\leq \frac{1}{2}\frac{1}{|\Pi_{3n}|}\sum_{\pi \in \Pi_{3n}}\sum_{P|\pi^\dagger P\pi \in \mathbb{P}_{\mathscr{E}}\setminus\mathbb{P}_{\mathscr{F}}}\Bigg\|tr_{0,+}\Big(Dec_M(|\alpha_P|^2\,(\pi^\dagger P_C\pi \otimes U_R^P)\psi$$

$$\left(\pi^\dagger P_C\pi \otimes U_R^{P\dagger})\Big)\right) \otimes |\mathrm{acc}\rangle\langle\mathrm{acc}|$$

$$- tr_{MC_1 C_2}\Big(|\alpha_P|^2\,(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^P)(\phi_{MRC_1 C_2})$$

$$\left(\pi_{C_1}^\dagger P_{C_1}\pi_{C_1} \otimes U_R^{P\dagger}\right)\Big)\Omega_M \otimes |\mathrm{rej}\rangle\langle\mathrm{rej}|\Bigg\|_1. \tag{40}$$

Since the maximum trace distance between two states is 1 we have:

$$\leq \frac{1}{|\Pi_{3n}|}\sum_{k_1 \in \mathcal{K}_1}\sum_{P|\pi^\dagger P\pi \in \mathbb{P}_{\mathscr{E}}\setminus\mathbb{P}_{\mathscr{F}}} |\alpha_P|^2. \tag{41}$$

Now if we let η_P be the number of permutations, π of P such that $\pi^\dagger P \pi \in \mathbb{P}_{\mathscr{E}} \setminus \mathbb{P}_{\mathscr{F}}$, then the above can be written as:

$$= \frac{1}{|\Pi_{3n}|} \sum_{P \in \mathbb{P}_{3n}} \eta_P \times |\alpha_P|^2 . \tag{42}$$

In Appendix A, we give Lemma A.1, which gives us $\eta_P \leq \binom{n}{t+1}(t+1)!$ $(3n - (t+1))!$. Thus, since $\sum\limits_{P \in \mathbb{P}_{3n}} |\alpha_P|^2 = 1$, the above expression can be bounded by:

$$\leq \frac{1}{(3n)!} \times \binom{n}{t+1}(t+1)!(3n-(t+1))!$$

$$= \frac{\prod\limits_{i=1}^{n} i \prod\limits_{i=1}^{3n-t-1} i}{\prod\limits_{i=1}^{n-t-1} i \prod\limits_{i=1}^{3n} i} = \frac{\prod\limits_{i=n-t}^{n} i}{\prod\limits_{i=3n-t}^{3n} i} = \prod_{i=0}^{t} \frac{n-t+i}{3n-t+i}$$

$$\leq \prod_{i=0}^{t} \frac{1}{3} = \left(\frac{1}{3}\right)^{t+1} \tag{43}$$

Therefore, $D\left(\frac{1}{|\mathcal{K}|} \sum\limits_{k \in \mathcal{K}} \mathscr{E}_k(\rho_{MR}), \mathscr{F}(\rho_{MR})\right) \leq (\frac{1}{3})^{t+1}, \forall \rho_{MR}.$ □

We note that this is very similar to the bound in [5] of $(\frac{2}{3})^{d/2}$: note that the trap code in [5] uses the error *detection* property of the code. Since a code of distance d can detect up to $d/2$ errors, this bound is consistent with our bound of $(\frac{1}{3})^{t+1}$.

A   Appendix

Lemma A.1. *For a fixed $P \in \mathbb{P}_{3n}$, let η_P denote the number of permutations π of P such that $\pi^\dagger P \pi \in \mathbb{P}_{\mathscr{E}} \setminus \mathbb{P}_{\mathscr{F}}$ Then for all P:*

$$\eta_P \leq \binom{n}{t+1}(t+1)!(3n-(t+1))!. \tag{44}$$

An intuitive argument for the above lemma is that η_P can be upper-bounded by fixing a Pauli $P \in \{I, X\}^{3n}$ of weight $t+1$. We show that a Pauli with greater weight will have $\leq \eta_P$ possible allowed permutations. To find the number of possible allowed permutations, we will consider the first n positions, where we require at least $t+1$ non-identity Paulis (for a total of $\binom{n}{t+1}(t+1)!$ permutations). The remaining positions are then simply permuted, since we have used all of the non-identity Paulis already, contributing a multiplicative factor of $(3n-(t+1))!$ permutations. This is formalized below (where we also consider general attack Paulis consisting of combinations of X, Y and Z).

Proof. In order to find an upper bound for η_P, we look to find the Pauli, P, that has the largest number of permutations, π, such that $\pi^\dagger P \pi \in \mathbb{P}_{\mathcal{E}} \setminus \mathbb{P}_{\mathcal{F}}$.

For a Pauli P with $\omega(P) = d$, we write $d = d_x + d_y + d_z + x_1 + y + z_1 + x_2 + z_2$ for values $d_x, d_y, d_z, x_1, y, z_1, x_2, z_2$ as follows:

1. d_x, d_y, d_z where $d_x + d_y + d_z = t + 1$. These are the $t + 1$ X, Y, and Z Paulis that must be applied to the first n qubits for the Pauli to be in $\mathbb{P}_{\mathcal{E}} \setminus \mathbb{P}_{\mathcal{F}}$.
2. y where $y + d_y$ is the total number of Y Paulis in P and y are the additional Y Paulis applied to the first n qubits. Note that Y Paulis cannot be applied to either set of traps without altering them.
3. x_1, x_2 where $x_1 + x_2 + d_x$ is the total number of X Paulis in P and x_1 are the additional X Paulis applied to the first n qubits and x_2 are the X Paulis applied to the $|+\rangle\langle+|^{\otimes n}$ traps.
4. z_1, z_2 where $z_1 + z_2 + d_z$ is the total number of Z Paulis in P and z_1 are the additional Z Paulis applied to the first n qubits and z_2 are the Z Paulis applied to the $|0\rangle\langle0|^{\otimes n}$ traps.

Then the possible permutations on P are found by multiplying the following terms:

1. $\binom{n}{d_x, d_y, d_z, n-t-1} d_x! d_y! d_z!$ Which is the number of ways to choose the required $t + 1$ spots for the minimum number of Paulis applied to the first n qubits, multiplied by the number of ways of permuting each of the sets of X, Y, and Z Paulis. Note that this term simplifies to $\frac{n!}{(n-t-1)!}$,
2. $\binom{n-t-1}{x_1} x_1!$, the number of ways to apply x_1 additional X Paulis to the first n qubits,
3. $\binom{n-t-1-x_1}{y} y!$, the number of ways to apply y additional Y Paulis to the first n qubits,
4. $\binom{n-t-1-x_1-y}{z_1} z_1!$, the number of ways to apply z_1 additional Z Paulis to the first n qubits,
5. $\binom{n}{x_2} x_2!$, the number of ways to apply x_2 X Paulis to the n traps that will not be changed by them,
6. $\binom{n}{z_2} z_2!$, the number of ways to apply z_2 Z Paulis to the n traps that will not be changed by them, and
7. $(3n - (d_x + d_y + d_z + x_1 + y + z_1 + x_2 + z_2))!$ the number of ways to permute the remaining identity qubits, which simplifies to $(3n - d)!$.

The product, once simplified, is then:

$$\eta_P = \frac{n! n! n! (3n - d)!}{(n - t - 1 - x_1 - y - z_1)!(n - x_2)!(n - z_2)!}$$

$$= \prod_{n-t-x_1-y-z_1}^{n} i \prod_{n-x_2+1}^{n} i \prod_{n-z_2+1}^{n} i \prod_{i=1}^{3n-t-1-x_1-y-z_1-x_2-z_2} i \qquad (45)$$

Since t is fixed, in order to maximize the above expression, we need to minimize x_1, y, z_1, x_2, z_2. This is achieved by setting $x_1 = y = z_1 = x_2 = z_2 = 0$, and therefore $d = t + 1$: we thus find that $\eta_P \leq \prod_{n-t}^{n} i \prod_{i=1}^{3n-t-1} i = \binom{n}{t+1}(t+1)!(3n - (t + 1))!$. $\qquad \square$

References

1. Aharonov, D., Ben-Or, M., Eban, E.: Interactive proofs for quantum computations. In: Innovations in Computer Science–ICS 2010, pp. 453–469 (2010). arXiv:0810.5375

2. Barnum, H., Crépeau, C., Gottesman, D., Smith, A., Tapp, A.: Authentication of quantum messages. In: 43rd Annual Symposium on Foundations of Computer Science–FOCS 2002, pp. 449–458 (2002). doi:10.1109/SFCS.2002.1181969

3. Ben-Or, M., Crépeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: 47th Annual Symposium on Foundations of Computer Science–FOCS 2006, pp. 249–260, (2006). doi:10.1109/FOCS.2006.68

4. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984)

5. Broadbent, A., Gutoski, G., Stebila, D.: Quantum one-time programs. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 344–360. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40084-1_20

6. Broadbent, A., Schaffner, C.: Quantum cryptography beyond quantum key distribution. Des. Codes Crypt. **78**, 351–382 (2016). doi:10.1007/s10623-015-0157-4

7. Bruß, D., Erdélyi, G., Meyer, T., Riege, T., Rothe, J.: Quantum cryptography: a survey. ACM Comput. Surv. (CSUR) **39**(2) (2007). doi:10.1145/1242471.1242474

8. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: 42nd Annual Symposium on Foundations of Computer Science FOCS 2001, pp. 136–145 (2001). doi:10.1109/SFCS.2001.959888

9. Cleve, R., Gottesman, D., Lo, H.-K.: How to share a quantum secret. Phys. Rev. Lett. **83**(3), 648–651 (1999). doi:10.1103/PhysRevLett.83.648

10. Dankert, C., Cleve, R., Emerson, J., Livine, E.: Exact and approximate unitary 2-designs and their application to fidelity estimation. Phys. Rev. A **80**, 012304 (2009). doi:10.1103/PhysRevA.80.012304

11. Dupuis, F., Nielsen, J.B., Salvail, L.: Actively secure two-party evaluation of any quantum operation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 794–811. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32009-5_46

12. Fehr, S.: Quantum cryptography. Found. Phys. **40**(5), 494–531 (2010). doi:10.1007/s10701-010-9408-4

13. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. thesis, California Institute of Technology (1997). arXiv:quant-ph/9705052

14. Hayden, P., Leung, D., Mayers, D.: Universal composable security of quantum message authentication with key recycling. In: QCRYPT 2011 (2011)

15. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)

16. Unruh, D.: Universally composable quantum multi-party computation. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 486–505. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_25

17. Watrous, J.: Guest column: an introduction to quantum information and quantum circuits. ACM SIGACT News **42**(2), 52–67 (2011). doi:10.1145/1998037.1998053