Tamper Detection Against Unitary Operators

Naresh Goud Boddu[1] and Upendra Kapshikar[2]

[1]NTT Research, Sunnyvale, USA
[2]Center for Quantum Technologies, National University of Singapore, Singapore

Security of a storage device against a tampering adversary has been a well-studied topic in classical cryptography. Such models give black-box access to an adversary, and the aim is to protect the stored message or abort the protocol if there is any tampering. The study of these models has led to some important cryptographic and communication primitives, such as tamper detection codes and non-malleable codes. In this work, we extend the scope of the theory of tamper detection codes against an adversary with quantum capabilities. We consider encoding and decoding schemes that are used to encode a k-qubit quantum message $|m\rangle$ to obtain an n-qubit quantum codeword $|\psi_m\rangle$. A quantum codeword $|\psi_m\rangle$ can be adversarially tampered via a unitary U from some known tampering unitary family $\mathcal{U}_{\mathsf{Adv}}$ (acting on $\mathbb{C}^{2^n}$), resulting in $U|\psi_m\rangle\langle\psi_m|U^\dagger$. Firstly, we initiate the general study of *quantum tamper detection codes*, which detect if there is any tampering caused by the action of a unitary operator. In case there was no tampering, we would like to output the original message. We show that quantum tamper detection codes exist for any family of unitary operators $\mathcal{U}_{\mathsf{Adv}}$, such that $|\mathcal{U}_{\mathsf{Adv}}| < 2^{2^{\alpha n}}$ for some constant $\alpha \in (0, 1/6)$; provided that unitary operators satisfy one additional condition:

- Far from the identity: for each $U \in \mathcal{U}_{\mathsf{Adv}}$, we require that its inner product with the identity operator is not too big, that is, $|\langle \mathbb{I}, U\rangle| = |\mathrm{Tr}(U)| \leq \phi 2^n$, where ϕ is suitably chosen parameter.

Quantum tamper detection codes that we construct can be considered to be quantum variants of *classical tamper detection codes* studied by Jafargholi and Wichs ['15], which are also known to exist under similar restrictions. Additionally, we show that when the message set $\mathcal{M}$ is classical, such a construction can be realized as a *non-malleable code* against an adversary having access to any $\mathcal{U}_{\mathsf{Adv}}$ of size up to $2^{2^{\alpha n}}$.

1 Introduction

Traditionally, cryptographic schemes have been analyzed assuming that an adversary has only black-box access to the underlying functionality and no way to manipulate the internal state. *Tamper-resilient cryptography* is a model in cryptography where an adversary is allowed to tamper with the internal state of a device (without necessarily knowing what it is) and then observe the outputs of the tampered device. By doing so, an attacker may learn additional sensitive information that would not be available otherwise. One natural approach to protect against such attacks is to encode the data on the device in some way. One can try to use error-correcting codes such as Reed-Solomon codes, but

such an encoding will prevent tampering with bounded Hamming weights, typically less than the distance of codes. Tamper detection codes introduced by Jafargholi and Wichs [1] provide meaningful guarantees on the integrity of an encoded message in the presence of a tampering adversary, even in settings where error correction and error detection may not be possible.

Consider the following: suppose one wants to store a message in a database accessible to an adversary. The adversary is then allowed to tamper the stored message using a function f from some function family $\mathcal{F}_{\mathsf{Adv}}$. Naturally, from a decent storage, we expect two properties -

- If there is tampering, we should be able to detect it with high probability.
- If there was no tampering, then we should always be able to recover the original message.

Let $\mathcal{M}$ be the set of messages, and let the storage be labelled by $\mathcal{C}$. For such a scheme, we require an encoder (Enc) from $\mathcal{M}$ to $\mathcal{C}$ and a decoding procedure (Dec) that reverses this operation. The decoder Dec is additionally allowed to output a special symbol $\perp$, to indicate that the message was tampered. The experiment can be modelled as a simple three-step procedure:

a) A message $m \in \mathcal{M}$ is encoded via a (possibly randomized) encoder $\mathsf{Enc} : \mathcal{M} \to \mathcal{C}$, yielding a codeword $c = \mathsf{Enc}(m)$.

b) An adversary can tamper c (non-trivially) via a function f from some known tampering function family $\mathcal{F}_{\mathsf{Adv}}$, resulting in $\hat{c} = f(c)$.

c) The tampered codeword $\hat{c}$ is then decoded to a candidate message $\hat{m} \in \mathcal{M} \cup \{\perp\}$ using a (possibly randomized) decoder $\mathsf{Dec} : \mathcal{C} \to \mathcal{M} \cup \{\perp\}$.

The properties that we desire from this scheme are:

A. $\Pr\left(\mathsf{Dec}\left(\mathsf{Enc}(m)\right) = m\right) = 1$ (*Completeness*).

B. $\Pr\left(\mathsf{Dec}\left(f\left(\mathsf{Enc}(m)\right)\right) = \perp\right) \geq 1 - \epsilon$ (*Soundness*).

Property A indicates that if no one tampers anything, we can always get back the original message. Property B states that the decoder can detect every non-trivial tampering with probability [1] at least $1 - \epsilon$. If some encoding and decoding scheme (Enc, Dec) satisfies the above properties, we say that it is an ϵ-secure tamper detection code (for family $\mathcal{F}_{\mathsf{Adv}}$).

Note that Property B can hold in two different degrees. One, it is valid for all messages m; where we call the scheme to be a strong tamper detection code (or simply tamper detection code). And two, it can be valid for a randomly chosen m, in which case we say the scheme is a weak tamper detection code. In this work, we restrict ourselves to the strong form of tamper detection.

For tampering to be meaningful, we assume that f is not the identity map. It is easy to see that for any function family $\mathcal{F}_{\mathsf{Adv}}$, the storage size $|\mathcal{C}|$ has to be greater than or equal to $|\mathcal{M}|$. Otherwise, the encoding scheme will be many-to-one, and Property A can not be satisfied. Also, the larger the family $\mathcal{F}_{\mathsf{Adv}}$ becomes, the stronger the adversary gets, and we expect the size of $\mathcal{C}$ to increase. This raises a natural question: for a given $\mathcal{M}$ and $\mathcal{F}_{\mathsf{Adv}}$, how large does $\mathcal{C}$ need to be?

[1] The probability stated above is taken over the randomness of the encoder and decoder.

Connection to Error Detection. One can note a fairly straightforward relation between tamper detection codes and error detection codes. Consider an error-correcting code with minimum distance d. Then, one can use it as a tamper detection code (with $\epsilon = 0$) against an adversary of bounded Hamming weight. In tamper detection, we aim to prevent against a much stronger adversary. Of course, one can not have an error-detecting code of an arbitrary distance, and hence, tamper detection comes at the cost of some uncertainty in decoding, reflected in Property B. Additionally, in the case of tamper detection, Property B only requires that tampering to be detected. In particular, we have no requirement to recover the original message. In contrast, the Hamming weight bound of $\frac{d}{2}$ on the adversary in the case of error detection guarantees such a recovery.

Relaxed Tamper Detection. The motivation for a tamper detection code is to construct a storage where it is hard for an adversary to change an encoding of a message to the encoding of some other message. A similar effect can be achieved if one considers the following property instead of Property B.

B′. $\Pr\left(\mathsf{Dec}\left(f\left(\mathsf{Enc}\left(m\right)\right)\right) = \{m, \perp\}\right) \geq 1 - \epsilon$ (*Relaxed soundness*).

Here, in case of tampering, a decoder is either allowed to detect tampering or output the original message m. In this case, although there was some tampering and the decoder does not necessarily detect it (by outputting $\perp$), the storage still managed to revert back to the original message. Clearly, Property B implies Property B′; hence we refer to a code satisfying Property A and B′ as a relaxed tamper detection code.

1.1 Previous works

The above experiment has been extensively studied, both in the weak and the general form, when the message set $\mathcal{M}$ and storage $\mathcal{C}$ are classical strings [1, 2, 3]. In the classical setup, one typically has $\mathcal{M} = \{0,1\}^k$, $\mathcal{C} = \{0,1\}^n$, and a tampering family $\mathcal{F}_{\mathsf{Adv}} \subset \mathcal{F}_n \setminus \mathbb{1}_n$ where $\mathcal{F}_n$ is the set of all possible Boolean functions from n-bits to n-bits, $\mathcal{F}_n = \{f : \{0,1\}^n \to \{0,1\}^n\}$. Suppose we restrict ourselves to encoding and decoding strategies that are deterministic. In that case, tamper detection schemes do not exist even for the family of additive tampering $\mathcal{F}_\Delta = \{f_{\mathrm{e}}(x) = x \oplus \mathrm{e}\}_{\mathrm{e}}$ where $\mathrm{e} \in \{0,1\}^n \setminus 0^n$. This can be seen as follows: let messages m_0 and m_1 be any two distinct messages with $\mathsf{Enc}(m_0)$ and $\mathsf{Enc}(m_1)$ as their corresponding encodings. Consider the function f_{e} for $\mathrm{e} = \mathsf{Enc}(m_0) \oplus \mathsf{Enc}(m_1)$. The tampering then results in $\mathsf{Dec}(f_{\mathrm{e}}(\mathsf{Enc}(m_i))) = m_{1-i}$ for $i \in \{0,1\}$; making randomness a necessity for tamper detection.

Cramer et al. [4] studied the problem of tamper detection for the function family $\mathcal{F}_\Delta$ and gave corresponding construction of what they refer to as *algebraic manipulation detection codes.*

Algebraic Manipulation Detection (AMD) Codes. These codes provide tamper detection security for the function family $\mathcal{F}_\Delta = \{f_{\mathrm{e}}(x) = x \oplus \mathrm{e},\ \mathrm{e} \neq 0\}$. Formally,

Fact 1 (Theorem 2, [4])**.** *Let q be a prime power and d be a positive integer such that $d < q$. There is an explicit* $(\mathsf{Enc}, \mathsf{Dec})$ *construction that is tamper-secure with parameters* $\left(k = d \log q,\ n = (d+2)\log q,\ \epsilon = \frac{d+1}{q}\right)$ *against* $\mathcal{F}_\Delta$.

Recall that k and n are bit lengths of message and codewords, respectively. The additive overhead of n over k measures the efficiency of AMD codes. An optimal code for parameters k and ϵ has the smallest possible n. For the security parameter $\epsilon \leq 2^{-\lambda}$, Fact 1 gives

$(k,\ k+2\lambda+2\log(d+1),\ 2^{-\lambda})$ AMD codes. Thus, the overhead for codeword length (over the message length) is $2\lambda + 2\log(d+1)$, which was later shown to be optimal up to a multiplicative factor two [5].

Classical Tamper Detection. AMD codes provide tamper detection security against a function family of size 2^n. However, the size of the tampering family $\mathcal{F}_{\mathsf{Adv}}$ can be up to 2^{n2^n} when one considers all classical Boolean functions f from n-bits to n-bits. Thus, it is interesting to see how big this family can be made, while achieving tamper detection. Again, one can see that it is not possible to construct tamper detection codes for the complete family of size 2^{n2^n}. For example, consider a family of functions $\mathcal{F}_{\text{con}} = \{f_i(m) = \mathsf{Enc}(i)\}_{i\in\mathcal{M}}$. No scheme can satisfy Property B (or even B′) for such a family.

Interestingly, Jafargholi and Wichs [1] showed that tamper detection codes indeed exist for any $\mathcal{F}_{\mathsf{Adv}}$ of size upto $2^{2^{\alpha n}}$ (for any constant $\alpha < 1$), as long as every function $f \in \mathcal{F}_{\mathsf{Adv}}$ satisfies two additional conditions:

- High min-entropy: $f(U_X)$ has sufficiently high min-entropy[2], where U_X is the uniform distribution on the domain of f.
- Few fixed points: There are not too many points such that $f(x) = x$.

The condition of high min-entropy avoids functions that put too much weight on a single point in the output. In particular, it avoids functions that are close to constant functions. Similarly, the condition of a few fixed points avoids functions that are close to the identity map. This result shows that tamper detection codes exist against any family that avoids these cases, even for those with size doubly exponential in n. Note that this result is based on a probabilistic argument, and as such, it only shows the existence of such codes, and it is not known if they can be constructed efficiently. However, for smaller families (having sizes upto $2^{\text{poly}(n)}$), one can indeed construct them efficiently [3] in the "common reference string" (CRS) model.

1.2 Our results

In this work, we aim to extend the scope of the theory of tamper detection to include adversaries that are capable of doing quantum operations. Hence, a family of unitary operators is a natural place to start the discussion. In particular, we consider a setting where the space of codewords $\mathcal{C}$ is of quantum states, and an adversary can apply a unitary operator from a known family of unitary operators $\mathcal{U}_{\mathsf{Adv}}$. The analogous question of tamper detection can now be asked in different scenarios:

1. Do tamper detection codes exist when $\mathcal{M}$ is the set of k-bit (classical) messages?
2. Do tamper detection codes exist when $\mathcal{M}$ is the set of k-qubit (quantum) messages?
3. Can these constructions be made efficient, potentially considering families of relatively small size, say, $|\mathcal{U}_{\mathsf{Adv}}| \leq 2^{\text{poly}(n)}$?

The first and the second question are direct analogues of the tamper detection theory when the adversary has their action defined via a unitary operator (instead of classical bits-to-bits manipulation). The first question considers the scenario of protecting classical information from a quantum adversary, whereas, for the second question, the information to be stored is itself quantum. The third question is inspired by the fact that efficient

[2]For a random variable X, it min-entropy is $\mathrm{H}_{\min}(X) = -\log\left(\max_{x\in\mathrm{supp}(X)} \Pr(X=x)\right)$.

classical tamper detection codes (such as AMD codes) exist when the adversarial family has small cardinality. We provide affirmative answers to questions 1 and 2 using probabilistic arguments. Partially addressing question 3, as an example of efficient construction, we show that a natural quantum analogue of classical AMD codes is sufficient for the purpose.

How far does the classical theory take us in question 1? Before going towards *truly* quantum encoding-decoding strategies, one can ask if the existing classical schemes themselves provide us security against unitary tamperings when $\mathcal{M}$ is classical. There is a natural strategy to follow: Consider a classical tamper detection code with the encoder $\mathsf{Enc}_{\mathsf{Cl}}$. Since the encoder is randomized, for a message $m \in \{0,1\}^k$ and randomness r, its encoding is given as $\mathsf{Enc}_{\mathsf{Cl}}(m,r)$. Define $\mathsf{Enc}_Q(m) = R_0 \sum_r |\mathsf{Enc}_{\mathsf{Cl}}(m,r)\rangle$, where R_0 is an appropriate normalization constant. After the adversary acts via a unitary U, the decoder simply measures in the computational basis, forcing the tampering to be effectively classical. Then, one can try to use the classical decoder to recover the message.

The rationale for the above strategy is simple. Although the tampering can be non-classical (that is, not via a function $f : \{0,1\}^n \to \{0,1\}^n$), the decoder can first measure in the computational basis. The resultant operation can now be treated as a (potentially randomized) function from n-bits to n-bits. And thus, a unitary adversary followed by the computational measurement can be simulated by a randomized classical adversary given by $\mathcal{F}_{\mathsf{Adv}}$. However, classical tamper detection does not protect against arbitrary function families. Thus, one would additionally need a statement of the following form:

Given an adversarial unitary family $\mathcal{U}_{\mathsf{Adv}}$ there exists a classical function family $\mathcal{F}_{\mathsf{Adv}}$ such that:

1. There exists a classical tamper detection code against $\mathcal{F}_{\mathsf{Adv}}$.
2. For every $U \in \mathcal{U}_{\mathsf{Adv}}$ and $c \in \{0,1\}^n$, its action followed by measurement in the computational basis can be emulated classically via $\mathcal{F}_{\mathsf{Adv}}$. That is,

   $$\Pr\left(\text{measurement results in } c' \mid \text{codeword was } c\right) = \langle c'|U(c)|c'\rangle = \sum_{f\in\mathcal{F}_{\mathsf{Adv}}} P^U(f)\mathbb{1}_{f(c)=c'},$$

   where $P^U(f)$ is a probability distribution supported on $\mathcal{F}_{\mathsf{Adv}}$ depending only on U (and not on c), and $\mathbb{1}$ is the indicator function.

Typically, one would need $|\mathcal{F}_{\mathsf{Adv}}| \leq 2^{2^{\alpha n}}$ for some appropriately chosen constant $\alpha < 1$ in addition to every f having enough min-entropy and few fixed points. Indeed, one can construct such $\mathcal{F}_{\mathsf{Adv}}$ for some families $\mathcal{U}_{\mathsf{Adv}}$. For example, consider the family of generalized Pauli operators (see Section 2.4.1 for the definition).

Example 1. The unitary operators in the family are indexed by a, b and given as $\sigma_{a,b} = X_a Z_b$. A rather straightforward calculation leads to the following:

- $X_a Z_b$ acting on any c followed by computational basis measurement results in $c + a$ with probability 1.

Now, consider $\mathcal{F}_\Delta = \{f_{\mathrm{e}}(x) = x \oplus \mathrm{e},\ \mathrm{e} \neq 0\}$. Define $P^{a,b}(f_e) = \delta_{a,e}$ where δ is the standard Kronecker delta function. Then it is easy to verify that for $\sigma_{a,b}$ such that $a \neq 0$,

$$\langle c'|\sigma_{a,b}(c)|c'\rangle = \sum_{e\neq 0} P^{a,b}(f_e)\mathbb{1}_{f_e(c)=c'}.$$

Whereas, any $\sigma_{a,b}$ with $a = 0$, the codeword is not even perturbed by the action of $\sigma_{a,b}$

as the Z_b operator can only result in adding a global phase to classical messages. Thus, any (non-trivial) action of a generalized Pauli operator, followed by measurement, can be simulated by $\mathcal{F}_{\mathsf{Adv}} = \mathcal{F}_{\Delta}$. This gives us the following:

Theorem 1 (Quantum AMD codes)**.** *Let q be a prime power and d be an integer such that $0 < d < q$. Let $\mathcal{U}_{\mathsf{P}_N}$ be the group of generalized Pauli operators [3] acting on $n = \log N$ qubits. There exists an efficient $(\mathsf{Enc}, \mathsf{Dec})$ scheme that is relaxed tamper-secure against $\mathcal{U}_{\mathsf{P}_N}$ with parameters $\left(k = d \log q,\ n = (d+2)\log q,\ \epsilon = \left(\frac{d+1}{q}\right)^2\right)$.*

Since there exists a family $\mathcal{F}_{\Delta}$ that can simulate generalized Pauli operators, we can directly use the classical scheme to detect a generalized Pauli operator adversary (see Appendix A for proof). However, it is not clear if, for a general unitary family $\mathcal{U}_{\mathsf{Adv}}$ (following some reasonable conditions), there exists a classical family $\mathcal{F}_{\mathsf{Adv}}$ satisfying conditions 1 and 2. And hence, in general, we can not ascertain that the natural quantum analogue of merely taking superpositions of classical encodings will suffice.

Now, we move on to the main contribution of the work, considering general families of unitary operators. Recall that classical results are proved under two restrictions. One, every function has enough min-entropy. And two, every function has at most a few fixed points (also referred to as the *far from the identity condition*). We also provide our results under similar restrictions. Note that when considering a unitary family, we readily have the min-entropy condition satisfied. So, we additionally impose a condition that captures closeness to the identity. We require that for every unitary operator $U \in \mathcal{U}_{\mathsf{Adv}}$, its inner product with the identity map ($|\langle \mathbb{1}, U\rangle| = |\mathrm{Tr}(U)|$) is bounded away from N. The main contribution of this work can then be stated as follows:

Theorem 2 (Quantum tamper detection for quantum messages)**.** *Let $\mathcal{M}$ be the set of quantum messages and let $\mathcal{U}_{\mathsf{Adv}} \subset \mathcal{U}\left(\mathbb{C}^{2^n}\right)$ be a family of size $2^{2^{\alpha n}}$ for some constant $\alpha < \frac{1}{6}$. Moreover, every $U \in \mathcal{U}_{\mathsf{Adv}}$ is such that $|\mathrm{Tr}(U)| \leq \phi 2^n$, where ϕ is a constant strictly less than 1. Then there exists a quantum tamper detection code against $\mathcal{U}_{\mathsf{Adv}}$.*

Note that in the above theorem, ϕ is not an absolute constant but depends on the size of plaintext space K and the security parameter ϵ.

Although our main motivation is to consider tamperings against quantum messages, as a *warm-up*, we consider the case of classical messages. This will help us to demonstrate our technique, give a brief overview and establish some bounds that will be used later.

Theorem 3 (Quantum tamper detection for classical messages)**.** *Let $\mathcal{M}$ be the set of classical messages and let $\mathcal{U}_{\mathsf{Adv}} \subset \mathcal{U}\left(\mathbb{C}^{2^n}\right)$ be a family of size $2^{2^{\alpha n}}$ for some constant $\alpha < \frac{1}{6}$. Moreover, every $U \in \mathcal{U}_{\mathsf{Adv}}$ is such that $|\mathrm{Tr}(U)| \leq \phi 2^n$, where ϕ is some constant strictly less than 1. Then there exists a quantum tamper detection code against $\mathcal{U}_{\mathsf{Adv}}$.*

We also show that even if one drops the condition on trace, we can achieve a *relaxed* version of quantum tamper detection (where quantum counterparts of Property A and B′ are satisfied). Again, here we state the theorem informally. The formal statement, along with its proof, is presented in Section 3.1.

Theorem 4 (Relaxed quantum tamper detection for classical messages)**.** *Let $\mathcal{M}$ be the set of classical messages and let $\mathcal{U}_{\mathsf{Adv}} \subset \mathcal{U}\left(\mathbb{C}^{2^n}\right)$ be a family of size $2^{2^{\alpha n}}$ for some constant*

[3] The generalized Pauli matrices we define are the so-called non-Hermitian Sylvester Generalized Pauli matrices. See Section 2.4.1 for the definition.

$\alpha < \frac{1}{6}$. *Then there exists a relaxed quantum tamper detection code against* $\mathcal{U}_{\mathsf{Adv}}$.

Note that, Theorem 4 allows us to also include operators that are close to the identity operator. It is not hard to see that such a relaxation to Property B′ is necessary as one can not satisfy Property B with such operators.

Proof overview. Similar to the proof provided by [1], our proofs for Theorem 2, 3 and 4 use probabilistic arguments via Chernoff-like tail bounds for limited independence. Before going ahead, we would like to fix some notation.

For a matrix A, let $A(i)$ denote the i-th column of A, which we will often treat as a vector. When dealing with classical messages, we will denote them as $m \in \mathcal{M}$, whereas for quantum messages, we will use $|m\rangle \in \mathcal{M}$ (or $|s\rangle \in \mathcal{M}$ to explicitly indicate that the message is in superposition). Moreover, we use $K = 2^k$ and $N = 2^n$, for ease of presentation.

Let us first consider the case when $\mathcal{M}$ is the set computational basis states, $\mathcal{M} = \{|m\rangle, m \in \{0,1\}^k\}$. Our scheme uses a strategy where encoding is done by a Haar-random isometry V. For a fixed $V \in \mathcal{U}\left(\mathbb{C}^N\right)$, our encoding scheme is fairly natural; we encode a classical message m as the m-th column of V, giving $\mathsf{Enc}(m) = |V(m)\rangle$.

Then the quantum tampering experiment can be thought of as below:

1. A k-bit message m is encoded in n-qubits via V, resulting in $|\psi_m\rangle = \mathsf{Enc}(m) = |V(m)\rangle$.
2. An adversary then tampers with $U \in \mathcal{U}_{\mathsf{Adv}}$, resulting in the state $U|\psi_m\rangle\langle\psi_m|U^\dagger$.
3. For $i \in \{1, 2, \ldots, K\}$, define $\Pi_i = |\psi_i\rangle\langle\psi_i|$ and let $\Pi_\perp = \mathbb{1} - \sum_i \Pi_i$. The decoder measures with the POVM $\{\Pi_1, \ldots, \Pi_K, \Pi_\perp\}$.
4. If the measurement results in $\Pi_\perp$, then abort with detection of tampering. Otherwise, apply $V^\dagger$ and output the resulting candidate message $\hat{m}$.

The completeness of the protocol is easy to check. To show that the above encoding-decoding is ϵ-tamper secure, one needs $\Pi_\perp$ to be a high probability event for any non-trivial tampering; $\mathrm{Tr}\left(\Pi_\perp U|\psi_m\rangle\langle\psi_m|U^\dagger\right) \geq 1 - \epsilon$ (*Soundness*). For that, we define the following random variables:

- $X_{js} = |\langle\psi_j|U|\psi_s\rangle|^2$ denotes the probability that message s was decoded to j.
- $X_s = \sum_{j \neq s} X_{js}$ denotes the probability of decoding s to a message other than s and $\perp$.

Measurement results in either the same $\Pi_s = |\psi_s\rangle\langle\psi_s|$ (with probability $P_{\mathsf{same}} = X_{ss}$) or one of the $\Pi_j = |\psi_j\rangle\langle\psi_j|$ that is different from s (with probability P_{diff}) or $\Pi_\perp$ that indicates the tampering (with probability $P_\perp$). Thus, $P_{\mathsf{same}} + P_{\mathsf{diff}} + P_\perp = 1$. Recall that we need to lower bound the probability of obtaining $P_\perp$. We do this by upper bounding P_{same} and P_{diff}, which requires us to prove sharp Chernoff-like tail bounds for random variables X_{ss} and X_s, respectively. This completes our proof for $\mathcal{M} = \{0,1\}^k$.

The setup when $\mathcal{M}$ is quantum (that is, messages to be stored are k-qubit states), is slightly more involved. Let $|s\rangle \in \mathcal{M}$ be a message that we want to store. Note that we need to preserve not only 2^k basis states but also the arbitrary superposition; arbitrary message $|s\rangle$ is a linear combination of computational basis states $|s\rangle = \sum_i \alpha_i |b_i\rangle$. Suppose one uses a direct linear extension of the earlier encoding-decoding strategy, $\mathsf{Enc}(|s\rangle) = \sum_i \alpha_i \mathsf{Enc}(b_i)$. The measurement in step 3 is done over the basis encodings $\{\mathsf{Enc}(b_i)\}$, and hence it can destroy the superposition. To recover $|s\rangle$, it is necessary to keep $|s\rangle$ intact, and in particular,

the resulting state after the measurement should not be disturbed too much from the pre-measurement state $\mathsf{Enc}(|s\rangle)$. To remedy this, we modify the decoder slightly, where we do measurement with a two-outcome POVM (instead of $K+1$ outcomes). The binary POVM we use corresponds to the projection on $\mathsf{Enc}(\mathcal{M}) = V(\mathcal{M})$ (and its orthogonal complement). Hence, for $|s\rangle \in \mathcal{M}$, we require that any adversarial unitary $U \in \mathcal{U}_{\mathsf{Adv}}$ takes $\mathsf{Enc}(|s\rangle)$ to a vector in the orthogonal complement of $V(\mathcal{M})$. This reduces the problem of tamper security of $|s\rangle$ to Chernoff-like tail bounds for a slightly different random variable $X_m = \langle\psi_m|U\ (\mathsf{Enc}|s\rangle)\,(\mathsf{Enc}|s\rangle)^\dagger\ U^\dagger|\psi_m\rangle$.

To prove sharp Chernoff-like tail bounds for random variables X_{ss}, X_s, and X_m, we use techniques from representation theory. The proof uses Weingarten calculus and some properties of the symmetric group.

We note that Theorem 3 (regarding the security of classical messages) follows as a corollary of Theorem 2 (regarding the security of quantum messages), as the former is a strict subset of the latter. Nonetheless, we include it as we also show Theorem 3 in the relaxed form, on an adversarial family with no trace bound needed (see Theorem 4). This is further used to show the existence of *non-malleable codes* via a standard reduction (see Theorem 7) against a unitary family of size upto of size $2^{2^{n/6}}$.

Related Works and Future Directions.

Since Shor's work on the existence of error-correcting structures for the quantum framework [6], there has been a rich history of quantum error correction [7, 8, 9, 10]. One can draw similar parallels between quantum error correction and quantum tamper detection as those present in the classical framework. In particular, tamper detection schemes try to handle an error set that is not bounded by weight with a possible loss in the ability to correct.

Quantum Authentication Schemes (QAS). The work of [11, 12] studies the notion of non-malleability in quantum authentication schemes. In quantum authentication schemes, both the encoder and decoder have a pre-shared private random key K that is not accessible to an adversary. We require that in the absence of an adversary, the received state should be the same as the sent state, and otherwise, with high probability, either the decoder rejects, or the received state is the same as that sent by the encoder. It is known that such quantum authentication schemes exist (for example, Clifford authentication [11]), whereas tamper detection schemes are keyless. Similarly, a few other works have also considered a "tampering" adversary [13, 14]. Again, these works are keyed primitives, making them different from tamper detection that works without keys.

Classically, tamper detection codes have turned out to be a fruitful object with rich applications. The work of [15] introduced non-malleable codes for which decoding a tampered codeword either results in an original message or a message unrelated to m. The work of [1] made the connection between tamper detection and non-malleable codes more explicit; by giving a modular construction of non-malleable codes out of weak tamper detection codes and leakage-resilient codes. There is a vast body of literature that considers tampering attacks using other approaches besides non-malleable codes and tamper detection codes (see [16, 17, 18, 19, 20, 21, 22, 23, 24, 25]). We refer to [15] for a more detailed comparison between these approaches and non-malleable codes, which have been a central object of study in recent times.

1.3 Subsequent works on tamper detection and non-malleable codes

On tamper detection in the qubit-wise tampering model

In [26], Bergamaschi studied a particular subclass of tamper detection codes, namely, against an adversary holding only Pauli operators. In what they refer to as *PMD codes*, they construct an efficient tamper detection scheme against such a Pauli adversary when (plaintext) messages are quantum. Hence, as mentioned by them, PMD codes can be thought of as a natural generalization of quantum AMD codes. We would also like to point out that the existence of such codes for quantum messages is also implied by our work as the family of Pauli operators falls within the scope of Theorem 8. As an application, they use PMD codes to construct keyless authentication codes against qubit-wise tamperings, a task that is provably impossible, solely with a classical encoding.

On non-malleability in the split-state tampering model

In another work, Aggarwal, Boddu and Jain [27] defined the notion of non-malleable codes for classical messages against quantum adversaries (having access to shared entanglement) in the *split-state model*, where cipher-text is split into two parts, and the adversary is allowed to tamper them independently (via unitaries of the form $U_1 \otimes U_2$).

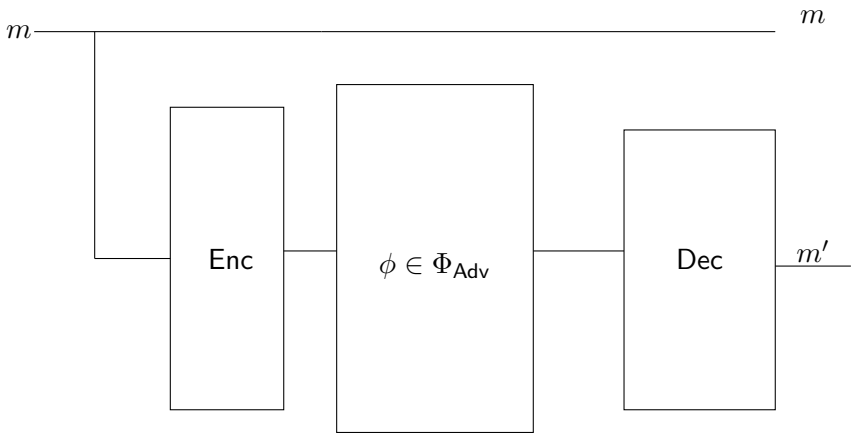

Figure 1: Tampering process.

Definition 1.1 ([27] non-malleable codes against adversary family Φ_{Adv})**.** *We say that an encoding-decoding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ *(see Definition 2.2 and Figure 1) is* ϵ*-non-malleable secure against adversary family* Φ_{Adv} *for classical messages* $\mathcal{M}$*, if for all* $m \in \mathcal{M}, \phi \in \Phi_{\mathsf{Adv}}$*, the following holds:*

$$\mathsf{Dec}\left(\phi\left(\mathsf{Enc}(m)\mathsf{Enc}(m)^\dagger\right)\right) \approx_\epsilon p_\phi m + (1-p_\phi)\eta_\phi,$$

where (p_ϕ, η_ϕ) *depend only on adversary* ϕ*. Here* $p_\phi \in [0,1]$ *and* η_ϕ *are independent of original message* m*.*

This work considers a much more general class of unitaries (which are not necessarily in a split form). Of course, this comes at the cost that their constructions are explicit and efficient, whereas our constructions are probabilistic and existential. Note that this is also seen in the classical tamper detection literature, where split-state codes are efficient, whereas the codes against a general adversary are known to exist (without any explicitly known construction).

Organization of the paper

For a quantum adversary with access to unitary operators, the *Haar* measure is the canonical measure to work with. For getting bounds on unitary operators, we use Weingarten functions as a tool. Well-known, relevant results are summarized in Section 2.5. Additionally, Section 2 also contains elementary observations on permutation groups, along with some technical proofs. In Appendix A, we prove Theorem 1; in Section 3, we prove Theorem 3 and Theorem 4; and in Section 4, we prove Theorem 2. All the proofs involve technical tail bounds regarding moments of certain random variables, which we include in Appendix B and C.

2 Preliminaries

2.1 Some notation

All the logarithms are evaluated to the base 2. Consider a finite-dimensional Hilbert space $\mathcal{H}$ endowed with an inner product $\langle \cdot, \cdot \rangle$ (we only consider finite-dimensional Hilbert spaces). For $p \geq 1$ we write $\| \cdot \|_p$ for the Schatten p-norm. We use $\rho_1 \approx_\epsilon \rho_2$ to mean that $\|\rho_1 - \rho_2\|_1 \leq \epsilon$. A similar convention will be followed for two probability distributions as well. A quantum state (or a density matrix or a state) is a positive semi-definite matrix on $\mathcal{H}$ with the trace equal to 1. It is called *pure* if and only if its rank is 1. Let $|\psi\rangle$ be a unit vector on $\mathcal{H}$, that is $\langle \psi, \psi \rangle = 1$. The topological space of norm-1 vectors (the unit N-sphere) in a normed N-dimensional vector space V, is denoted as $\mathbb{S}^{(N-1)}(V)$. When V is clear from the context, we drop it. For an n-dimensional vector v, we will use the standard notation $v = (v_1, \ldots, v_n)$ and thus v_i will refer to the i-th coordinate. Similarly, for a matrix M, we will denote its i, j-th entry by M_{ij}.

- A *unitary* operator $U : \mathcal{H} \to \mathcal{H}$ is such that $U^\dagger U = UU^\dagger = \mathbb{I}$. The set of all unitary operators on $\mathcal{H}$ is denoted by $\mathcal{U}(\mathcal{H})$.
- An *isometry* $V : \mathcal{H}_A \to \mathcal{H}_B$ is such that $V^\dagger V = \mathbb{I}_A$ and $VV^\dagger = \Pi_{V(\mathcal{H}_A)}$, where $\Pi_{V(\mathcal{H}_A)}$ is the projection on the image of $\mathcal{H}_A$ under V.
- A *POVM* $\{M, \mathbb{I} - M\}$ is a 2-outcome quantum measurement for $0 \leq M \leq \mathbb{I}$. We use the shorthand $\overline{M} = \mathbb{I} - M$, where $\mathbb{I}$ is clear from the context. Similarly, a measurement M_A acting on a combined space $\mathcal{H}_A \otimes \mathcal{H}_B$ will be used to represent $M_A \otimes \mathbb{I}_B$.
- A k-outcome POVM is defined by a collection $\{M_1, M_2, \ldots, M_k\}$, where $0 \leq M_i \leq \mathbb{I}$ for every $i \in [k]$ and $\sum_i M_i = \mathbb{I}$.

We now state the following useful facts.

2.2 Some elementary bounds

Fact 2. *For any integer $n \geq 1$*

$$\frac{n^n}{e^{n-1}} \leq n! \leq \frac{n^{n+1}}{e^{n-1}}.$$

Fact 3. *Let U be a unitary operator on $\mathbb{C}^N$. Then $|\mathrm{Tr}(U)| \leq N$.*

Fact 4. *For positive integers k, n such that $1 \leq k \leq n$,*

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

2.3 Definitions for Tamper Detection

Definition 2.1 (ϵ-net (Lemma 5.2, [28]))**.** *Fix an $\epsilon > 0$. Then there exists an integer N and a set of vectors $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\}$ in $\mathbb{S}^{d-1}$ such that the following properties hold:*

- $N \leq \left(\frac{4d}{\epsilon}\right)^d$.
- *For any state $|\psi\rangle \in \mathbb{S}^{d-1}$, there exists $j \in [N]$ such that $\||\psi\rangle - |\psi_j\rangle\|_1 \leq \epsilon$.*

Definition 2.2 (Quantum encoding and decoding schemes)**.** *Let $\mathsf{Enc} : \mathcal{M} \longrightarrow \mathbb{S}^{N-1}$ be a map and $\mathsf{Dec} : \mathbb{S}^{N-1} \longrightarrow \mathcal{M} \cup \{\perp\}$. Then, we say that $(\mathsf{Enc}, \mathsf{Dec})$ is an encoding-decoding scheme if the following holds: for all $m \in \mathcal{M}$, $\Pr\left(\mathsf{Dec}\left(\mathsf{Enc}(m)\right) = m\right) = 1$.*

Definition 2.3 (Tamper detection (against unitary adversaries))**.** *Let $\mathcal{U}_{\mathsf{Adv}} \subset \mathcal{U}\left(\mathbb{C}^N\right)$ be a family of unitary operators. We say that an encoding-decoding scheme $(\mathsf{Enc}, \mathsf{Dec})$ is ϵ-tamper secure against family $\mathcal{U}_{\mathsf{Adv}}$ for messages $\mathcal{M}$, if for all $m \in \mathcal{M}, U \in \mathcal{U}_{\mathsf{Adv}}$, the following holds:*

$$\Pr\left(\mathsf{Dec}\left(U\left(\mathsf{Enc}(m)\right)\left(\mathsf{Enc}(m)\right)^\dagger U^\dagger\right) = \perp\right) \geq 1 - \epsilon.$$

Furthermore, if $\mathcal{M} = \{0,1\}^k$, we say that $(\mathsf{Enc}, \mathsf{Dec})$ is $\left(K = 2^k, N, \epsilon\right)$-tamper secure for classical messages, whereas if $\mathcal{M} = \mathbb{S}^{K-1}$, we say that $(\mathsf{Enc}, \mathsf{Dec})$ is (K, N, ϵ)-tamper secure for quantum messages.

Now we define a *relaxed version* of tamper detection. In this version, the aim of a decoder is to either detect tampering or output the original message. Compared to the original definition of tampered detection, the relaxed version has a scope to revert a tampering, without even detecting it. Since our result holds for classical messages (against unitary tamperings), we define relaxed tamper detection only for classical messages but one can define an analogous notion for quantum messages as well.

Definition 2.4 (Relaxed tamper detection)**.** *Let $\mathcal{U}_{\mathsf{Adv}} \subset \mathcal{U}\left(\mathbb{C}^N\right)$ be a family of unitary operators and let $\mathcal{M} = \{0,1\}^k$. We say that an encoding-decoding scheme $(\mathsf{Enc}, \mathsf{Dec})$ is (K, N, ϵ)-tamper secure in the relaxed setting (against $\mathcal{U}_{\mathsf{Adv}}$), if for all $m \in \mathcal{M}$, $U \in \mathcal{U}_{\mathsf{Adv}}$, the following holds:*

$$\Pr\left(\mathsf{Dec}\left(U\left(\mathsf{Enc}(m)\right)\left(\mathsf{Enc}(m)\right)^\dagger U^\dagger\right) = \{\perp, m\}\right) \geq 1 - \epsilon.$$

Definition 2.5 (Adversarial unitary families)**.** *Let $\mathcal{U}_{\mathsf{Adv}} \subset \mathcal{U}\left(\mathbb{C}^N\right)$ be a family of unitary operators such that the following holds:*

1. *For all $U \in \mathcal{U}_{\mathsf{Adv}}$, we have, $|\mathrm{Tr}\left(U\right)| \leq \phi N$.*
2. *$|\mathcal{U}_{\mathsf{Adv}}| \leq 2^{N^\alpha}$.*

We call $\mathcal{U}_{\mathsf{Adv}}$ as an (N, α, ϕ) adversarial unitary family or simply (N, α, ϕ) family.

Definition 2.6 (Random Haar encoding and decoding schemes)**.** *Let* H *be a random unitary drawn from* $\mathcal{U}\left(\mathbb{C}^N\right)$ *(according to the Haar measure). Let* V *be the following matrix constructed by restricting* H *to its first* K *columns:*

$$V = (\mathrm{H}_1, \mathrm{H}_2, \ldots, \mathrm{H}_K).$$

Note that V *is an isometry. Consider the following encoding and decoding scheme.*

- *Let* $V(i)$ *denote the* i*-th column of* V*. For* $m \in [K]$*, define* $\mathsf{Enc}(m) = |\psi_m\rangle = |V(m)\rangle$*.*

  If the message set $\mathcal{S}$ *is quantum, the extension is canonical. For* $|s\rangle = \sum_m \alpha_m |m\rangle$*, the encoding is* $\mathsf{Enc}(|s\rangle) = \sum_m \alpha_m \mathsf{Enc}(m)$*.*

- Dec *to be implemented according to the following procedure:*

  Let $\Pi_i = |\psi_i\rangle\langle\psi_i|$ *and* $\Pi_\perp = \mathbb{I} - \sum_i \Pi_i$*. To decode a message* $|\theta\rangle$*, we measure* $|\theta\rangle$ *in a two-valued POVM* $\left\{\sum_i \Pi_i, \Pi_\perp\right\}$*. Let* ψ' *be the post-measurement state. If the measurement results in* $\perp$ *then abort (indicating tamper detection); otherwise the decoder outputs* $V^\dagger(\psi')V$*.*

Note that if the message set is classical $(\mathcal{M} = \{0,1\}^k)$*, then the decoder can be reduced to the following action:*

- $\mathsf{Dec}_{\mathsf{Cl}}$*: Measure* $|\theta\rangle$ *in the POVM* $\{\Pi_1, \Pi_2, \ldots, \Pi_K, \Pi_\perp\}$ *, if it results in* Π_i *then output* i*.*

Below we give the necessary details of permutation groups, generalized Pauli matrices, Haar random unitary operators, and Weingarten unitary calculus, which will be required to state our results. We refer the reader to [29] for details on Weingarten unitary calculus.

2.4 Permutation groups

Let S_n be the symmetric group of degree n acting canonically on the set $[n] := \{1, 2, \ldots, n\}$. Let $\mathrm{H} \leq S_n$ be a permutation group. For $x \in [n]$, *orbit* of x under H, denoted as $\mathcal{O}_\mathrm{H}(x)$ is the set of elements that can be reached from x via H,

$$\mathcal{O}_\mathrm{H}(x) = \{y \in [n] : \ \exists h \in \mathrm{H}, \ y = h(x)\}.$$

We say that x is fixed by H if $\mathcal{O}_\mathrm{H} = \{x\}$. Otherwise, we say that H moves x. We denote the set of elements fixed by H as $\mathsf{Fix}\,(\mathrm{H})$ and the set of elements moved as $\mathsf{Move}\,(\mathrm{H})$. By extension, for $\sigma \in S_n$ we write $\mathsf{Fix}(\sigma)$ and $\mathsf{Move}(\sigma)$ to mean $\mathsf{Fix}\,(\langle\sigma\rangle)$ and $\mathsf{Move}\,(\langle\sigma\rangle)$ respectively, where $\langle\sigma\rangle$ is the group generated by σ.

Given a $\sigma \in S_n$, orbits for $\mathrm{H} = \langle\sigma\rangle$ partition the set $[n]$ into disjoint subsets as $\mathcal{O}_\mathrm{H}$ gives an equivalence relation. When one writes σ as a permutation in a disjoint cycle form, each orbit is a cycle of σ and each cycle is an orbit, and hence, we denote an orbit (or a disjoint cycle) by c. Let $C\,(\sigma)$ denote the set of orbits c under $\mathrm{H} = \langle\sigma\rangle$.

For an orbit c, let $odd(c)$ denote the number of odd elements in it and $even(c)$ be the number of even elements in it. We define an evaluation map Val on orbits of σ. An orbit c is given a value equal to the difference between the number of odd and even elements it contains.

$$\mathsf{Val}(c) = |odd(c) - even(c)|.$$

We also extend the evaluation map to S_n by assigning a value for each permutation. In this case, a permutation will get a value equal to the sum of the values of all of its orbits.

$$\mathsf{Val}(\sigma) = \sum_{c \in C(\sigma)} \mathsf{Val}(c) = \sum_{c \in C(\sigma)} |odd(c) - even(c)|.$$

We denote the set of orbits with value 1 by $C_1(\sigma)$. It is easy to see that σ has full valuation n if and only if it preserves the parity; that is, it takes odd elements to odd elements and even elements to even elements.

A transposition is a cycle of size 2. Every permutation $\sigma \in S_n$ can be written as a product of transpositions. Let $\mathsf{T}(\sigma)$ denote the minimum number of transpositions required to obtain σ. It is known that $\mathsf{T}(\sigma) + |C(\sigma)| = n$. We use e to represent identity permutation.

Lemma 1. *For any $\sigma \in S_n$, we have $|\mathsf{Fix}(\sigma)| \geq 2|C(\sigma)| - n$.*

Proof. Clearly if $|C(\sigma)| \leq \frac{n}{2}$, the lemma is trivially true. Suppose $|C(\sigma)| > \frac{n}{2}$.

Note that $\mathsf{Move}(\sigma) \leq 2\mathsf{T}(\sigma)$ and hence $|\mathsf{Move}(\sigma)| \leq 2(n - |C(\sigma)|)$. Since $\mathsf{Move}(\sigma) + \mathsf{Fix}(\sigma) = n$, we get $|\mathsf{Fix}(\sigma)| \geq 2|C(\sigma)| - n$. □

Observation 1. *It follows from the definition that, for any permutation σ and for any transposition τ, $\mathsf{T}(\tau\sigma) = \mathsf{T}(\sigma\tau) \leq \mathsf{T}(\sigma) + 1$. Also, the number of cycles can increase or decrease by 1. If elements moved by τ are in the same cycle of σ, then C increases by 1, and if they are in different cycles it decreases by 1. $|C(\sigma)| - 1 \leq |C(\sigma\tau)| = |C(\tau\sigma)| \leq |C(\sigma)| + 1$.*

For $i \in [0 : n-1]$, let $\Sigma_i := \{\sigma \in S_n : \mathsf{T}(\sigma) = i\}$ denote the number of permutations σ such that the number of transpositions in σ is i.

Observation 2. *For $i \in [0 : n-1]$ we have, $|\Sigma_i| \leq \binom{n}{2}^i$.*

Let $\mathcal{B}_{2n}$ be the set of permutations on $2n$ letters that take odd elements to even elements and vice-versa.

$$\mathcal{B}_{2n} := \{\beta \in S_{2n} : \text{ for all } x, x + \beta(x) = 1 \mod 2\}.$$

Lemma 2. *For any $\alpha \in S_{2t}$ and $\beta \in \mathcal{B}_{2t}$, we have $|\mathsf{C}(\beta\alpha)| - \mathsf{T}(\alpha) \leq t$.*

Proof. We will prove this by induction on $\mathsf{T}(\alpha)$.

Base Case: $\mathsf{T}(\alpha) = 0$, that is, $\alpha = e$. Note that for $\beta \in \mathcal{B}_{2n}$, every cycle must have a length of at least two as β can not fix any element. Thus, $|C(\beta)| \leq \frac{2t}{2} = t$.

Induction Hypothesis (IH): For all α' such that $\mathsf{T}(\alpha') \leq T_0 - 1$, we have, $|\mathsf{C}(\beta\alpha')| - \mathsf{T}(\alpha') \leq t$.

We will show that the upper bound holds for α with $\mathsf{T}(\alpha) = T_0$.

The General Case: Let $C(\alpha) = \{C_1, C_2, \ldots, C_l\}$. Since $\alpha \neq e$, there exists a cycle of length strictly greater than one. Without loss of generality, let that be C_l and $C_l = (x_1\ x_2\ \ldots\ x_m)$.

Let $\alpha' = C_1 C_2 \ldots C_{l-1}\,(x_1\ x_2\ \ldots\ x_{m-1})\,(x_m)$. Alternatively, α' can be obtained from α by fixing x_m, that is,

$$\alpha'(x) = x_1 \qquad \text{if } x = x_{m-1}$$

$$= x_m \qquad \text{if } x = x_m$$
$$= \alpha(x) \qquad \text{if } x \notin \{x_m, x_{m-1}\}.$$

$|C(\alpha')| = |C(\alpha)| + 1$ which gives $\mathsf{T}(\alpha') = \mathsf{T}(\alpha) - 1$. By IH, $|\mathsf{C}(\beta\alpha')| - T(\alpha') \leq t$. Also, $\alpha = \alpha'\,(x_{m-1}\ x_m)$. Thus, $|C(\beta\alpha)| = |C(\beta\alpha'\,(x_{m-1}\ x_m)\,| \leq C(\beta\alpha') + 1$. The inequality follows from Observation 1. Putting this along with $\mathsf{T}(\alpha) = \mathsf{T}(\alpha') + 1$ we get the lemma. □

Since T is invariant under inverse, we can replace $\mathsf{T}(\alpha)$ by $\mathsf{T}(\alpha^{-1})$. Furthermore, $\mathsf{T}(\alpha) + |C(\alpha)| = 2t$. Hence we get the following:

Corollary 5. *For $\alpha \in S_{2t}$ and $\beta \in \mathcal{B}_{2t}$, we have, $|C(\alpha)| + |C(\beta\alpha^{-1})| \leq 3t$.*

2.4.1 Generalized Pauli matrices

Let q be a prime power and $\mathbb{F}_q$ be the field of size q. And let ω denote the q-th primitive root of unity. Let X_a and Z_b be the following collection of operators indexed by $a, b \in \mathbb{F}_q$.

$$X_a = \sum_{x \in \mathbb{F}_q} |x + a\rangle\langle x|$$
$$Z_b = \sum_{x \in \mathbb{F}_q} \omega^{bx} |x\rangle\langle x|.$$

The group of generalized Pauli matrices is generated by $\langle X_1, Z_1\rangle$. Generalized Pauli matrices obey the twisted commutation relations given by

$$X_a Z_b = \omega^{-ab} Z_b X_a.$$

2.5 Weingarten unitary calculus

Weingarten functions are used for evaluating integrals over the unitary group $\mathcal{U}(\mathbb{C}^N)$ of products of matrix coefficients [29]. The expectation of products of entries (also called moments or matrix integrals) of Haar-distributed unitary random matrices can be described in terms of a special function on the permutation group. Such considerations go back to Weingarten [30], Collins [31]. This function is known as the (unitary) Weingarten function and is denoted by Wg. Let S_p be the symmetric group on $[p] = \{1, 2, ..., p\}$. Let $i = (i_1, \ldots, i_p)$, $i' = (i'_1, \ldots, i'_p)$ be p-tuples of positive integers from $\{1, 2, \ldots, N\}$. We use the notation $\delta_\sigma(i, i') = \delta_{i_1 i'_{\sigma(1)}} \delta_{i_2 i'_{\sigma(2)}} \ldots \delta_{i_p i'_{\sigma(p)}}$, where δ is the standard Kronecker delta function. For $\alpha \in S_p, p \leq N$,

$$\mathrm{Wg}(\alpha, N) = \int_{\mathcal{U}(\mathbb{C}^N)} U_{11} \ldots U_{pp} \overline{U_{1\alpha(1)}} \ldots \overline{U_{p\alpha(p)}} dU$$

where U is a Haar-distributed unitary random matrix on $\mathbb{C}^N$, dU is the normalized Haar measure, and Wg is called the (unitary) Weingarten function. A crucial property of the Weingarten function $\mathrm{Wg}(\alpha, N)$ is that it depends only on the conjugacy class (or alternatively, on the cycle structure) of permutation α. So, $\mathrm{Wg}\,(\alpha, N)$ can as well be denoted as $\mathrm{Wg}\left(\left[l_1, l_2, \ldots, l_{|C(\alpha)|}\right], N\right)$ where $c_1, c_2, \ldots, c_{|C(\alpha)|}$ are cycles of α having lengths $l_1, l_2, \ldots, l_{|C(\alpha)|}$ respectively.

Fact 6 (General matrix integration [32, 30, 31])**.** *Let N be a positive integer and $i = (i_1, \ldots, i_p)$, $i' = (i'_1, \ldots, i'_p)$, $j = (j_1, \ldots, j_p)$, $j' = (j'_1, \ldots, j'_p)$ be p-tuples of positive integers from $\{1, 2, \ldots, N\}$. Then,*

$$\int_{\mathcal{U}(\mathbb{C}^N)} U_{i_1 j_1} \cdots U_{i_p j_p} \overline{U_{i'_1 j'_1}} \cdots \overline{U_{i'_p j'_p}} dU = \sum_{\sigma,\tau \in S_p} \delta_\sigma(i, i') \delta_\tau(j, j') \mathrm{Wg}(\tau\sigma^{-1}, N)$$

where $\delta_\sigma(i, i') = \delta_{i_1 i'_{\sigma(1)}} \delta_{i_2 i'_{\sigma(2)}} \ldots \delta_{i_p i'_{\sigma(p)}}$ and δ is the standard Kronecker delta function.

If $p \neq p'$, then

$$\int_{\mathcal{U}(\mathbb{C}^N)} U_{i_1 j_1} \cdots U_{i_p j_p} \overline{U_{i'_1 j'_1}} \cdots \overline{U_{i'_{p'} j'_{p'}}} dU = 0.$$

The following result encloses all the information we need for our computations about the asymptotics of the Wg function; see [31] for a proof.

Fact 7 (Asymptotics of Weingarten functions (Section 2.6.3, [29]))**.** *For $\sigma \in S_t$,*

$$\mathrm{Wg}(\sigma, N) = \mathcal{O}\left(\frac{N^{|C(\sigma)|}}{N^{2t}}\right) \qquad \text{as } N \to \infty\,. \tag{1}$$

Fact 8 (Proposition 2.4, [29])**.** *For all $t \geq 1$,*

$$\sum_{\sigma \in S_t} \mathrm{Wg}(\sigma, N) = \frac{1}{N(N+1)\cdots(N+t-1)}\,. \tag{2}$$

Other than the sum of the Weingarten function, one more quantity that will be important for us is its L_1 norm. Here, we derive a useful expression for that.

Lemma 3. *For all $t \geq 1$,*

$$\sum_{\sigma \in S_t} |\mathrm{Wg}(\sigma, N)| = \frac{1}{N(N-1)\cdots(N-(t-1))}\,. \tag{3}$$

Proof. Let ρ_{sign} denote the sign representation of the symmetric group. Let G denote the inverse of Wg in $\mathbb{C}[S_t]$. It is well known that $G = \prod_{k=1}^{t} (N + J_k)$ where J_k is k-th *Jucys-Murphy element*, defined as follows:

$$J_k = (1,2) + (2,3) + \cdots + (k-1, k)\,.$$

Now $G = \prod_{k=1}^{t} (N + J_k)$ gives

$$\rho_{sign}(G) = \rho_{sign}\left(\prod_{k=1}^{t} (N + J_k)\right).$$

Inverting both sides,

$$\rho_{sign}(\mathrm{Wg}) = \left(\rho_{sign}\left(\prod_{k=1}^{t} (N + J_k)\right)\right)^{-1}$$

$$
\begin{aligned}
&= \left(\prod_{k=1}^{t} \rho_{sign}(N + J_k)\right)^{-1} \\
&= \left(\prod_{k=1}^{t} (N - (k-1))\right)^{-1} \\
&= \frac{1}{N(N-1)(N-2)(N-(t-1))} \,. \qquad \square
\end{aligned}
$$

We give some values of the Weingarten functions for the unitary group $\mathcal{U}(\mathbb{C}^N)$ taken from [31] upto third moments.

$$
\begin{aligned}
\mathrm{Wg}([1], N) &= \frac{1}{N} \,, & \mathrm{Wg}([1,1], N) &= \frac{1}{N^2-1} \,, \\
\mathrm{Wg}([2], N) &= \frac{-1}{N(N^2-1)} \,, & \mathrm{Wg}([1,1,1], N) &= \frac{N^2-2}{N(N^2-1)(N^2-4)} \,, \\
\mathrm{Wg}([2,1], N) &= \frac{-1}{(N^2-1)(N^2-4)} \,, & \mathrm{Wg}([3], N) &= \frac{2}{N(N^2-1)(N^2-4)} \,.
\end{aligned}
$$

3 A Warm-up: Quantum tamper detection codes for classical messages

In this section, we consider quantum tamper detection codes for classical messages. We give a probabilistic proof that quantum tamper detection codes for classical messages exist.

Theorem 5. *Let $\mathcal{U}_{\mathsf{Adv}}$ be an $\left(N, \alpha, \sqrt{\frac{\epsilon}{2K}}\right)$ family such that $\left(\frac{1}{6} - \alpha\right)\log(N) \geq \log(K) + \log\left(\frac{1}{\epsilon}\right) + 2$. Then there exists a (K, N, ϵ)-tamper secure scheme for classical messages. Furthermore, a uniformly random encoding and decoding strategy according to Haar measure (see $(\mathsf{Enc}, \mathsf{Dec}_{\mathsf{CI}})$ in Definition 2.6) gives such a code with probability at least $1 - \mathcal{O}\left(\frac{KN}{2^{N^\alpha}}\right)$.*

Proof. We show that an encoding and decoding strategy, as given in Definition 2.6, gives a tamper detection code for the given set of parameters.

For a fixed unitary $U \in \mathcal{U}_{\mathsf{Adv}}$, let us define random variables $X_{js} = |\langle\psi_j|U|\psi_s\rangle|^2$ for $j, s \in \mathcal{M}$. Here the randomness is over the Haar measure in choosing $(\mathsf{Enc}, \mathsf{Dec})$ strategy as an isometry V. Let $X_s = \sum_{j \neq s} X_{js}$. The random variable X_{js} denotes the probability that message j was decoded given that message s was encoded. Similarly, X_s denotes the probability that the procedure resulted in an incorrectly decoded message. Both X_{js} and X_s are non-negative random variables with values less than or equal to 1.

Let $\mathcal{E}$ be the event that $(\mathsf{Enc}, \mathsf{Dec})$ is not an ϵ-secure tamper detection code against $\mathcal{U}_{\mathsf{Adv}}$. Then,

$$
\begin{aligned}
\Pr(\mathcal{E}) &\leq \Pr\left(\exists U \in \mathcal{U}_{\mathsf{Adv}}, s \in \{0,1\}^k \quad \text{s.t.} \quad X_s + X_{ss} \geq \epsilon\right) \\
&\leq \sum_{U \in \mathcal{U}_{\mathsf{Adv}}} \sum_{s \in \{0,1\}^k} \Pr\left(X_s + X_{ss} \geq \epsilon\right) \\
&\leq \sum_{U \in \mathcal{U}_{\mathsf{Adv}}} \sum_{s \in \{0,1\}^k} \sum_{j \in \{0,1\}^k \neq s} \Pr\left(X_{js} \geq \frac{\epsilon}{K}\right) + \sum_{U \in \mathcal{U}_{\mathsf{Adv}}} \sum_{s \in \{0,1\}^k} \Pr\left(X_{ss} \geq \frac{\epsilon}{K}\right) \\
&\leq |\mathcal{U}_{\mathsf{Adv}}| K^2 \Pr\left(X_{js} \geq \frac{\epsilon}{K}\right) + |\mathcal{U}_{\mathsf{Adv}}| K \Pr\left(X_{ss} \geq \frac{\epsilon}{K}\right)
\end{aligned}
$$

$$= |\mathcal{U}_{\mathsf{Adv}}| K^2 \Pr(\mathcal{E}_1) + |\mathcal{U}_{\mathsf{Adv}}| K \Pr(\mathcal{E}_2).$$

To bound $\Pr(\mathcal{E}_1) = \Pr\left(X_{js} \geq \frac{\epsilon}{K}\right)$ and $\Pr(\mathcal{E}_2) = \Pr\left(X_{ss} \geq \frac{\epsilon}{K}\right)$ using a Chernoff-like argument, we need to calculate moments of random variable X_{js} and X_{ss}. Note that we could not directly use Chernoff bound to bound $\sum_j X_{js}$ as for different $j_1 \neq j_2$, the random variables $X_{j_1 s}$ and $X_{j_2 s}$ are not independent of each other. Naturally, the problem of calculating moments of random variable X_{js} is closely related to Weingarten unitary calculus (see Section 2.5) as our encoding strategy is Haar random.

Here we present first-order moments for variables X_{js} and X_{ss}. Computation for higher moments is similar but slightly more involved and can be found in the Appendix B.

For readability we use $\phi = \sqrt{\frac{\epsilon}{2K}}$. Thus, $\mathcal{U}_{\mathsf{Adv}}$ is an (N, α, ϕ) family.

First moment of random variable X_{js} and X_{ss}:

We begin with the first moment of X_{js}.

$$\begin{aligned}
X_{js} &= |\langle\psi_j|U|\psi_s\rangle|^2 \\
&= \langle\psi_j|U|\psi_s\rangle\langle\psi_s|U^\dagger|\psi_j\rangle \\
&= \langle j|V^\dagger U V|s\rangle\langle s|V^\dagger U^\dagger V|j\rangle \\
&= \left(\sum_{l_1,k_1} U_{l_1k_1} V^*_{l_1 j} V_{k_1 s}\right)\left(\sum_{l_2,k_2} U^\dagger_{l_2k_2} V^*_{l_2 s} V_{k_2 j}\right) \\
&= \sum_{l_1,k_1}\sum_{l_2,k_2}\left(U_{l_1k_1} U^\dagger_{l_2k_2} V_{k_1 s} V_{k_2 j} V^*_{l_1 j} V^*_{l_2 s}\right).
\end{aligned}$$

A. When $j \neq s$,

$$\begin{aligned}
\mathbf{E}[X_{js}] &= \mathbf{E}[|\langle\psi_j|U|\psi_s\rangle|^2] \\
&= \sum_{l_1,k_1}\sum_{l_2,k_2}\left(U_{l_1k_1} U^\dagger_{l_2k_2}\, \mathbf{E}\left[V_{k_1 s} V_{k_2 j} V^*_{l_1 j} V^*_{l_2 s}\right]\right) \\
&= \sum_{l_1,k_1}\sum_{l_2,k_2}\left(U_{l_1k_1} U^\dagger_{l_2k_2}\left(\sum_{\alpha,\beta\in S_2}\delta_\alpha(k_1k_2, l_1l_2)\delta_\beta(sj, js)\mathrm{Wg}(\beta\alpha^{-1}, N)\right)\right).
\end{aligned}$$

The final equality is due to Fact 6. Note that when $j \neq s$ and $\beta = \mathbb{I}$, we get, $\delta_\beta(sj, js) = 0$. Thus, the only terms that survive are those corresponding to $\beta = (1\ 2)$.

$$\begin{aligned}
\mathbf{E}[X_{js}] &= \sum_{l_1,k_1,l_2,k_2} U_{l_1k_1} U^\dagger_{l_2k_2}\left(\delta(k_1k_2, l_1l_2)\mathrm{Wg}((1\ 2)((1)(2))^{-1}, N) + \delta(k_1k_2, l_2l_1)\mathrm{Wg}((1\ 2)(1\ 2)^{-1}, N)\right) \\
&= \sum_{l_1=k_1}\sum_{l_2=k_2} U_{l_1k_1} U^\dagger_{l_2k_2}\mathrm{Wg}((1\ 2), N) + \sum_{l_1=k_2}\sum_{l_2=k_1} U_{l_1k_1} U^\dagger_{l_2k_2}\mathrm{Wg}((1)(2), N) \\
&= \mathrm{Tr}(U)\mathrm{Tr}(U^\dagger)\cdot\mathrm{Wg}((1\ 2), N) + \mathrm{Tr}(UU^\dagger)\cdot\mathrm{Wg}((1)(2), N) \\
&= \frac{-\mathrm{Tr}(U)\mathrm{Tr}(U^\dagger)}{N(N^2-1)} + N\cdot\frac{1}{N^2-1} \\
&= \frac{N^2 - \mathrm{Tr}(U)\mathrm{Tr}(U^\dagger)}{N(N^2-1)}
\end{aligned}$$

$$= \frac{N^2 - |\mathrm{Tr}(U)|^2}{N(N^2-1)}$$
$$\leq \frac{2}{N}\,.$$

B. When $j = s$,

$$\begin{aligned}
\mathbf{E}[X_{ss}] &= \mathbf{E}[|\langle\psi_s|U|\psi_s\rangle|^2] \\
&= \sum_{l_1,k_1}\sum_{l_2,k_2}\left(U_{l_1k_1}U^\dagger_{l_2k_2}\,\mathbf{E}\left[V_{k_1s}V_{k_2s}V^*_{l_1s}V^*_{l_2s}\right]\right) \\
&= \sum_{l_1,k_1}\sum_{l_2,k_2}\left(U_{l_1k_1}U^\dagger_{l_2k_2}\left(\sum_{\alpha,\beta\in S_2}\delta_\alpha(k_1k_2,l_1l_2)\delta_\beta(ss,ss)\mathrm{Wg}(\beta\alpha^{-1},N)\right)\right) && \text{(from Fact 6)} \\
&= \sum_{\alpha\in S_2}\left(\sum_{l_1,k_1,l_2,k_2}U_{l_1k_1}U^\dagger_{l_2k_2}\delta_\alpha(k_1k_2,l_1l_2)\left(\sum_{\beta\in S_2}\mathrm{Wg}(\beta\alpha^{-1},N)\right)\right) \\
&= \sum_{\alpha\in S_2}\left(\sum_{l_1,k_1,l_2,k_2}U_{l_1k_1}U^\dagger_{l_2k_2}\delta_\alpha(k_1k_2,l_1l_2)\left(\frac{1}{N(N+1)}\right)\right) && \text{(from eq. (2))} \\
&= \frac{1}{N(N+1)}\left(\sum_{l_1=k_1}\sum_{l_2=k_2}U_{l_1k_1}U^\dagger_{l_2k_2} + \sum_{l_1=k_2}\sum_{l_2=k_1}U_{l_1k_1}U^\dagger_{l_2k_2}\right) \\
&= \frac{\mathrm{Tr}(U)\mathrm{Tr}(U^\dagger) + \mathrm{Tr}(UU^\dagger)}{N(N+1)} \\
&= \frac{N + |\mathrm{Tr}(U)|^2}{N(N+1)} \leq \phi^2 + \frac{1}{N} && \text{(since } |\mathrm{Tr}(U)| \leq \phi N\text{).}
\end{aligned}$$

Thus, we get the following bounds:

$$\mathbf{E}\left[X_{js}\right] \leq \frac{2}{N} \quad \textit{and} \quad \mathbf{E}[X_{ss}] \leq \phi^2 + \frac{1}{N}\,.$$

Similarly, we get higher moment bounds (see Appendix B);

$$\mathbf{E}\left[X^t_{js}\right] \leq \mathcal{O}\left(\frac{t^4}{N}\right)^t \quad \textit{and} \quad \mathbf{E}[X^t_{ss}] \leq \mathcal{O}\left(\left(\frac{t^2}{N}\right)^t + t\phi^{2t}\right). \tag{4}$$

Now we proceed to bound the probability $\Pr\left(X_{js} \geq \frac{\epsilon}{K}\right)$.

$$\begin{aligned}
\Pr\left(X_{js} \geq \frac{\epsilon}{K}\right) &\leq \Pr\left(e^{\theta X_{js}} \geq e^{\frac{\theta\epsilon}{K}}\right) \\
&\leq \frac{\mathbf{E}[e^{\theta X_{js}}]}{e^{\frac{\theta\epsilon}{K}}} \\
&= \frac{1}{e^{\frac{\theta\epsilon}{K}}}\sum_i \frac{\theta^i\,\mathbf{E}[X^i_{js}]}{i!} \\
&= \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\sum_{i=0}^{N^{1/5}}\frac{\theta^i\,\mathbf{E}(X^i_{js})}{i!} + \sum_{i\geq N^{1/5}+1}\frac{\theta^i\,\mathbf{E}(X^i_{js})}{i!}\right)
\end{aligned}$$

$$
\begin{aligned}
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\sum_{i=0}^{N^{1/5}} \frac{\theta^i}{i!}\mathcal{O}\left(\frac{i^4}{N}\right)^i + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_{js}^i)}{i!}\right) && \text{(from eq. (4))}\\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\sum_{i=0}^{N^{1/5}} \frac{1}{i!}\mathcal{O}\left(\frac{\theta}{N^{1/5}}\right)^i + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_{js}^i)}{i!}\right)\\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\sum_{i=0}^{N^{1/5}} \frac{1}{i!}\mathcal{O}\left(\frac{\theta}{N^{1/5}}\right)^i + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_{js}^{N^{1/5}})}{i!}\right)\\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\mathcal{O}\left(e^{\frac{\theta}{N^{1/5}}}\right) + \mathcal{O}\left(\frac{e^\theta}{N^{\frac{1}{5}N^{1/5}}}\right)\right)\\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\mathcal{O}\left(e^{\frac{\theta}{N^{1/5}}} + e^{\theta-\frac{1}{5}N^{1/5}\ln(N)}\right)\\
&\leq \frac{1}{e^{\frac{N^{1/6}\epsilon}{K}}}\mathcal{O}\left(1+1\right) && \text{(choosing } \theta = N^{\frac{1}{6}})\\
&\leq \mathcal{O}\left(e^{-\frac{N^{1/6}\epsilon}{K}}\right). && (5)
\end{aligned}
$$

Similarly when $j = s$, we bound the probability $\Pr\left(X_{ss} \geq \frac{\epsilon}{K}\right)$.

$$
\begin{aligned}
\Pr\left(X_{ss} \geq \frac{\epsilon}{K}\right) &\leq \Pr\left(e^{\theta X_{ss}} \geq e^{\frac{\theta\epsilon}{K}}\right)\\
&\leq \frac{\mathbf{E}[e^{\theta X_{ss}}]}{e^{\frac{\theta\epsilon}{K}}}\\
&= \frac{1}{e^{\frac{\theta\epsilon}{K}}}\sum_i \frac{\theta^i\,\mathbf{E}[X_{ss}^i]}{i!}\\
&= \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\sum_{i=0}^{N^{1/5}} \frac{\theta^i\,\mathbf{E}(X_{ss}^i)}{i!} + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_{ss}^i)}{i!}\right)\\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\ \mathcal{O}\left(\sum_{i=0}^{N^{1/5}} \frac{\theta^i}{i!}\left(i\phi^{2i} + \left(\frac{1}{N^{3/5}}\right)^i\right) + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_{ss}^i)}{i!}\right)\\
& && \text{(from eq. (4))}\\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\ \mathcal{O}\left(N\sum_{i=0}^{N^{1/5}} \frac{(\theta\phi^2)^i}{i!} + \sum_{i=0}^{N^{1/5}} \frac{1}{i!}\left(\frac{\theta}{N^{3/5}}\right)^i + \left(\left(\frac{1}{N^{3/5}}\right)^{N^{1/5}} + N\phi^{N^{1/5}}\right)e^\theta\right)\\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\ \mathcal{O}\left(Ne^{\theta\phi^2} + e^{\frac{\theta}{N^{3/5}}} + e^{\theta-\frac{3}{5}N^{1/5}\ln(N)} + e^{\theta+\ln(N)-N^{1/5}\ln(1/\phi)}\right)\\
&\leq e^{-\frac{N^{1/6}\epsilon}{K}}\ \mathcal{O}\left(Ne^{N^{\frac{1}{6}}\phi^2} + 1 + 1 + 1\right) && \left(\text{choosing } \theta = N^{\frac{1}{6}}\right)\\
&\leq e^{-\frac{N^{\epsilon\frac{1}{6}}}{K}}\ \mathcal{O}\left(Ne^{\frac{\epsilon N^{\frac{1}{6}}}{4K}} + 1\right) && \left(\text{since } \phi = \sqrt{\tfrac{\epsilon}{4K}}\right)\\
&\leq \mathcal{O}\left(Ne^{-\frac{3\epsilon N^{\frac{1}{6}}}{4K}}\right) && (6)
\end{aligned}
$$

$$
|\mathcal{U}_{\mathsf{Adv}}|K^2\Pr\left(\mathcal{E}_1\right) = |\mathcal{U}_{\mathsf{Adv}}|K^2\Pr\left(X_{js} \geq \frac{\epsilon}{K}\right)
$$

$$
\begin{aligned}
&\leq |\mathcal{U}_{\mathsf{Adv}}| K^2 \ \mathcal{O}\left(e^{-\frac{N^{1/6}\epsilon}{K}}\right) && \text{(from eq. (5))} \\
&\leq 2^{N^\alpha} K^2 \mathcal{O}\left(e^{-4N^\alpha}\right) \\
&\leq K^2 \mathcal{O}\left(2^{N^\alpha} 2^{-4N^\alpha}\right) \\
&\leq \mathcal{O}\left(\frac{K^2}{2^{N^\alpha}}\right). && (7)
\end{aligned}
$$

The third inequality follows from the choice of our parameters;

$$
\left(\frac{1}{6} - \alpha\right) \log(N) \geq \log(K) + \log\left(\frac{1}{\epsilon}\right) + 2.
$$

Similarly, we have,

$$
\begin{aligned}
|\mathcal{U}_{\mathsf{Adv}}| K \Pr\left(\mathcal{E}_2\right) &= |\mathcal{U}_{\mathsf{Adv}}| K \Pr\left(X_{ss} \geq \frac{\epsilon}{K}\right) \\
&\leq |\mathcal{U}_{\mathsf{Adv}}| K \mathcal{O}\left(N e^{-\frac{3\epsilon N^{\frac{1}{6}}}{4K}}\right) && \text{(from eq. (6))} \\
&\leq 2^{N^\alpha} K \mathcal{O}\left(N e^{-3N^\alpha}\right) \\
&\leq K \mathcal{O}\left(N 2^{N^\alpha} 2^{-3N^\alpha}\right) \\
&\leq \mathcal{O}\left(\frac{KN}{2^{N^\alpha}}\right). && (8)
\end{aligned}
$$

The third follows from our choice of parameters: $\left(\frac{1}{6} - \alpha\right) \log(N) \geq \log(K) + \log\left(\frac{1}{\epsilon}\right) + 2$. Thus, it follows from eq. (7) and (8) that

$$
\Pr\left(\mathcal{E}\right) \leq |\mathcal{U}_{\mathsf{Adv}}| K^2 \Pr\left(\mathcal{E}_1\right) + |\mathcal{U}_{\mathsf{Adv}}| K \Pr\left(\mathcal{E}_2\right) \leq \mathcal{O}\left(\frac{KN}{2^{N^\alpha}}\right). \qquad \square
$$

3.1 Relaxed tamper detection for classical messages

We would like to point out that an interesting side result follows from our previous calculation. It follows that one can get a *relaxed* version of tamper detection even if even when the family $\mathcal{U}_{\mathsf{Adv}}$ does not satisfy the *far from identity* condition. Recall that, in the relaxed version, we aim to either output the original message or detect that it was tampered and output $\perp$. In principle, the relaxed version allows us to revert back to the original message without detecting tampering. Such a "reversion without detection" is inherent to the quantum setting due to the action of measurement operators. For example, consider a message m encoded as $|\psi\rangle$. Suppose a unitary takes $|\psi\rangle$ to $\frac{1}{\sqrt{2}}\left(|\psi\rangle + |\psi'\rangle\right)$ where $|\psi'\rangle$ is orthogonal to the space of codewords. The measurement of the decoder can result in $|\psi'\rangle$ indicating that there was tampering. If the measurement results in $|\psi\rangle$, we can not detect the tampering, but nonetheless, the decoder still outputs the correct message $\widehat{m} = m$. Thus, one gets a qualitatively similar version of tamper detection where the decoder either aborts or returns the correct plaintext.

Theorem 6. *Let $\mathcal{U}_{\mathsf{Adv}}$ be an $(N, \alpha, 1)$ family such that $\left(\frac{1}{6} - \alpha\right) \log(N) \geq \log(K) + \log\left(\frac{1}{\epsilon}\right) + 2$. Then a uniform Haar random encoding-decoding strategy is (K, N, ϵ)-relaxed tamper secure with probability at least $1 - \mathcal{O}\left(\frac{K^2}{2^{N^\alpha}}\right)$.*

Proof. For a fixed unitary U, recall that random variables were defined as follows: $X_{js} = |\langle\psi_j|U|\psi_s\rangle|^2$ and $X_s = \sum_{j\neq s} X_{js}$. Let $\mathcal{E}$ be the event that $(\mathsf{Enc}, \mathsf{Dec})$ is not an ϵ-secure relaxed tamper detection code against $\mathcal{U}_{\mathsf{Adv}}$.

$$\begin{aligned}
\Pr(\mathcal{E}) &\leq \Pr\left(\exists U \in \mathcal{U}_{\mathsf{Adv}}, s \in \{0,1\}^k \quad s.t. \quad X_s \geq \epsilon\right) \\
&\leq \sum_{U\in\mathcal{U}_{\mathsf{Adv}}} \sum_{s\in\{0,1\}^k} \Pr(X_s \geq \epsilon) \\
&\leq \sum_{U\in\mathcal{U}_{\mathsf{Adv}}} \sum_{s\in\{0,1\}^k} \sum_{j\in\{0,1\}^k\neq s} \Pr\left(X_{js} \geq \frac{\epsilon}{K}\right) \\
&\leq |\mathcal{U}_{\mathsf{Adv}}| K^2 \Pr\left(X_{js} \geq \frac{\epsilon}{K}\right) \\
&\leq \mathcal{O}\left(\frac{K^2}{2^{N^\alpha}}\right) \qquad \text{(from eq. (7)).}
\end{aligned}$$

□

From relaxed tamper detection to non-malleability

The relaxed form of tamper detection aims to either output the original message, or detect that it was tampered (indicated by the output $\perp$). On the other hand, a non-malleable code insists that we either output the original message or an unrelated message, but with an additional requirement that the probability (of a message being the same) depends only on the adversarial unitary U. And hence, it is not a priori clear if relaxed tamper detection will immediately give non-malleable security. In particular, the probability distribution may depend on U, as well as the original message s. However, this potential dependency on s can be removed by first analysing the distribution for an average s. Then, a standard average-case to worst-case reduction shows that non-malleability can be achieved by incurring a nominal hit in the parameters. This line of argument of first going to an average case setting to remove the dependency on s, followed by a reduction to worst case non-malleability is fairly common (see for example, Section 3.3 in [33]). We include it below.

Claim 1. *Let* $(\mathsf{Enc}, \mathsf{Dec})$ *be* ϵ*-secure relaxed tamper detection scheme. Let* S *be the uniform distribution on* $\mathcal{M} = \{0,1\}^k$*. Then,*

$$\mathsf{Dec}\left(U\left(\mathsf{Enc}(S)\mathsf{Enc}(S)^\dagger\right)U^\dagger\right) \approx_{2\epsilon} p_U S + (1-p_U)\perp,$$

where $p_U = \frac{1}{2^k}\sum_s X_{ss}$.

Proof. Note that, since S is the uniform distribution, each s is sampled with probability $\frac{1}{2^k}$, and moreover, any particular s gives back the same s on decoding with probability $p_{\mathsf{same}}(s)$, some different s' with $p_{\mathsf{diff}}(s)$ and $\perp$ with probability $p_\perp(s)$. And hence, we can represent the relevant distribution as the following convex combination:

$$\mathsf{Dec}\left(U\left(\mathsf{Enc}(S)\mathsf{Enc}(S)^\dagger\right)U^\dagger\right) = \frac{1}{2^k}\sum_s p_{\mathsf{same}}(s)S + \frac{1}{2^k}\sum_s p_{\mathsf{diff}}(s)S' + \frac{1}{2^k}\sum_s p_\perp(s)\perp.$$

Since $(\mathsf{Enc}, \mathsf{Dec})$ is ϵ-secure relaxed tamper detection code, $p_{\mathsf{diff}}(s) \leq \epsilon$, for all s.

Thus, $\frac{1}{2^k}\sum_s p_{\mathsf{diff}}(s) \leq \epsilon$. The claim now follows by noting that $p_{\mathsf{same}(s)} = X_{ss}$. □

Theorem 7. *Let $\mathcal{U}_{\mathsf{Adv}}$ be an $(N, \alpha, 1)$ family such that $\left(\frac{1}{6} - \alpha\right)\log(N) \geq 2\log(K) + \log\left(\frac{1}{\epsilon}\right) + 2$. Then a uniform Haar random encoding-decoding strategy $(\mathsf{Enc}, \mathsf{Dec})$ is a 2ϵ-secure non-malleable code (for classical messages against $\mathcal{U}_{\mathsf{Adv}}$) with probability at least $1 - \mathcal{O}\left(\frac{K^2}{2^{N^\alpha}}\right)$.*

Proof. Let $p_U = \frac{1}{2^k}\sum X_{ss}$ and $\eta = \perp$. Set $\epsilon' \leftarrow \frac{\epsilon}{K}$.

Then, by choice of parameters, $\left(\frac{1}{6} - \alpha\right)\log(N) \geq \log(K) + \log\left(\frac{1}{\epsilon'}\right) + 2$. Hence, by Theorem 6, a Haar random encoding-decoding is ϵ'-secure relaxed tamper detection code with probability at $1 - \mathcal{O}\left(\frac{K^2}{2^{N^\alpha}}\right)$. Furthermore, by Claim 1,

$$\mathsf{Dec}\left(U\left(\mathsf{Enc}(S)\mathsf{Enc}(S)^\dagger\right)U^\dagger\right) \approx_{2\epsilon'} p_U S + (1 - p_U) \perp . \tag{9}$$

Now,

$$\begin{aligned}
&\|\mathsf{Dec}\left(U\left(\mathsf{Enc}(s)\mathsf{Enc}(s)^\dagger\right)U^\dagger\right) - p_U s + (1 - p_U) \perp \|_1 \\
&\leq 2^k \cdot \|\mathsf{Dec}\left(U\left(\mathsf{Enc}(S)\mathsf{Enc}(S)^\dagger\right)U^\dagger\right) - p_U S + (1 - p_U) \perp \|_1 \\
&\leq 2^k \cdot 2\epsilon' && \text{(from eq. (9))} \\
&\leq 2\epsilon . && \square
\end{aligned}$$

4 Tamper Detection Codes for Quantum Messages

In this section, we consider quantum tamper detection codes for quantum messages. Again, we give a probabilistic proof that quantum tamper detection codes exist for quantum messages. Our probabilistic methods are similar, but some subtle intricacies are involved for quantum messages due to superposition.

Theorem 8. *Let $\mathcal{U}_{\mathsf{Adv}}$ be an $\left(N, \alpha, \sqrt{\frac{\epsilon}{2K}}\right)$ family such that $\left(\frac{1}{6} - \alpha\right)\log(N) \geq \log k + \log\left(\frac{1}{\epsilon}\right) + 2$ and let $\delta = 2^{2+\log K - \frac{N^\alpha}{K}}$. Then a uniformly random Haar encoding and decoding strategy (see $(\mathsf{Enc}, \mathsf{Dec})$ in Definition 2.6) is a $(K, N, \epsilon + \delta)$-tamper secure scheme with probability at least $1 - \mathcal{O}\left(\frac{KN}{2^{N^\alpha}}\right)$.*

Proof. Let $\mathcal{M} = \{|\theta_1\rangle, |\theta_2\rangle, \ldots, |\theta_M\rangle\}$ be a δ-net of $\mathbb{S}^{K-1}$ from Definition 2.1 such that $M \leq (\frac{4K}{\delta})^K$ and $\delta = 2^{2+\log K - \frac{N^\alpha}{K}}$. Let $|\theta\rangle$ be an arbitrary quantum message from δ-net. We express θ in the computational basis with a_i as coefficients; $|\theta\rangle = \sum_{m=1}^K a_m|m\rangle$. Recall $|\psi_m\rangle = V|m\rangle$.

For $m \in [K]$, let $X_m = \left(\langle\psi_m|\, U\, (\mathsf{Enc}|\theta\rangle)(\mathsf{Enc}|\theta\rangle)^\dagger U^\dagger|\psi_m\rangle\right)$ and $X = \sum_m X_m$.

Note that for a fixed U,

$$X_m = \left(\sum_{i=1}^K \sum_{j=1}^K a_i a_j^* \langle\psi_m|U|\psi_i\rangle\langle\psi_j|U^\dagger|\psi_m\rangle\right). \tag{10}$$

Recall that Π is a projector on the space of codewords, that is, $\Pi = \sum_{i=1}^K |\psi_i\rangle\langle\psi_i|$.

$$
\begin{aligned}
X &= \mathrm{Tr}\left(\Pi\, U\mathsf{Enc}(|\theta\rangle(\mathsf{Enc}(|\theta\rangle)^\dagger U^\dagger\right) \\
&= \sum_{m=1}^{K} X_m \\
&= \sum_{m=1}^{K}\left(\langle\psi_m|U\left(\sum_{i=1}^{K}\sum_{j=1}^{K} a_i a_j^* |\psi_i\rangle\langle\psi_j|\right)U^\dagger|\psi_m\rangle\right) && \text{(from eq. (10))} \\
&= \sum_{m=1}^{K}\left(\sum_{i=1}^{K}\sum_{j=1}^{K} a_i a_j^* \langle\psi_m|\, U|\psi_i\rangle\langle\psi_j|U^\dagger|\psi_m\rangle\right).
\end{aligned}
$$

Let $\mathcal{E}$ be the event that $(\mathsf{Enc}, \mathsf{Dec})$ is not ϵ-secure against $\mathcal{U}_{\mathsf{Adv}}$. Again, for bounding the probability of $\mathcal{E}$, we need the higher moments of X_m, the calculation of which we defer to Appendix C.

$$
\mathbf{E}[X_m^t] \leq \mathcal{O}\left(\left(\frac{t^2}{N}\right)^t + t\phi^{2t}\right). \tag{11}
$$

After this, an argument similar to the previous one (breaking sum into two parts; $t \leq N^{1/5}$ and $t > N^{1/5}$ followed by union bound over all messages and accounting for the size of $|\mathcal{U}_{\mathsf{Adv}}|$) directly can be applied. For completeness, we provide it here.

$$
\begin{aligned}
\Pr\left(X_m \geq \frac{\epsilon}{K}\right) &\leq \Pr\left(e^{\theta X_m} \geq e^{\frac{\theta\epsilon}{K}}\right) \\
&\leq \frac{\mathbf{E}[e^{\theta X_m}]}{e^{\frac{\theta\epsilon}{K}}} \\
&= \frac{1}{e^{\frac{\theta\epsilon}{K}}}\sum_i \frac{\theta^i\,\mathbf{E}[X_m^i]}{i!} \\
&= \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\sum_{i=0}^{N^{1/5}} \frac{\theta^i\,\mathbf{E}(X_m^i)}{i!} + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_m^i)}{i!}\right) \\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\left(\sum_{i=0}^{N^{1/5}} \frac{\theta^i}{i!}\mathcal{O}\left(\left(\frac{i^2}{N}\right)^i + i\phi^{2i}\right) + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_m^i)}{i!}\right) && \text{(from eq. (11))} \\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\,\mathcal{O}\left(\sum_{i=0}^{N^{1/5}} \frac{\theta^i}{i!}\left(i\phi^{2i} + \left(\frac{1}{N^{3/5}}\right)^i\right) + \sum_{i\geq N^{1/5}+1} \frac{\theta^i\,\mathbf{E}(X_{ss}^i)}{i!}\right) \\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\,\mathcal{O}\left(N\sum_{i=0}^{N^{1/5}} \frac{(\theta\phi^2)^i}{i!} + \sum_{i=0}^{N^{1/5}} \frac{1}{i!}\left(\frac{\theta}{N^{3/5}}\right)^i + \left(\left(\frac{1}{N^{3/5}}\right)^{N^{1/5}} + N\phi^{N^{1/5}}\right)e^\theta\right) \\
&\leq \frac{1}{e^{\frac{\theta\epsilon}{K}}}\,\mathcal{O}\left(Ne^{\theta\phi^2} + e^{\frac{\theta}{N^{3/5}}} + e^{\theta - \frac{3}{5}N^{1/5}\ln(N)} + e^{\theta + \ln(N) - N^{1/5}\ln(1/\phi)}\right) \\
&\leq \mathcal{O}\left(Ne^{-\frac{3\epsilon N^{\frac{1}{6}}}{4K}}\right).
\end{aligned}
$$

And finally, with the union bound,

$$
\Pr(\mathcal{E}) \leq \Pr\left(\exists\, U, |\theta\rangle \in \mathcal{U}_{\mathsf{Adv}} \times \mathcal{M} \text{ such that } X \geq \epsilon\right)
$$

$$
\begin{aligned}
&\leq \sum_{U\in\mathcal{U}_{\mathsf{Adv}}}\sum_{|\theta\rangle\in\mathcal{M}} \Pr\left(X\geq\epsilon\right)\\
&\leq \sum_{U\in\mathcal{U}_{\mathsf{Adv}}}\sum_{|\theta\rangle\in\mathcal{M}} \Pr\left(\sum_{m=1}^{K} X_m\geq\epsilon\right)\\
&\leq \sum_{U\in\mathcal{U}_{\mathsf{Adv}}}\sum_{|\theta\rangle\in\mathcal{M}}\sum_{m=1}^{K} \Pr\left(X_m\geq\frac{\epsilon}{K}\right)\\
&\leq |\mathcal{U}_{\mathsf{Adv}}||\mathcal{M}|K\Pr\left(X_m\geq\frac{\epsilon}{K}\right)\\
&\leq 2^{N^\alpha}2^{N^\alpha}K\mathcal{O}\left(Ne^{-\frac{3\epsilon N^{\frac{1}{6}}}{4K}}\right)\\
&\leq \mathcal{O}\left(\frac{KN}{2^{N^\alpha}}\right).
\end{aligned}
$$

□

5 Conclusion and future work

Our main result exhibits the existence of quantum tamper detection codes for large families of unitary operators of size upto $2^{2^{\alpha n}}$. Since the proof is probabilistic, one natural direction would be to give a constructive proof for quantum tamper detection codes. However, it should be noted that such efficient constructions are not known even against a classical adversary of such a large size. Typically, efficient constructions are known for families of size $2^{\mathrm{poly}(n)}$ in the CRS model. Hence, one has to first find out families of relatively small size (and of some interest) against which tamper detection can be made efficient. We present one such example, the family of generalized Pauli operators. There are other natural follow-up questions:

- An arbitrary quantum adversary is capable of doing CPTP operations. Can we provide quantum tamper detection security for families of CPTP maps? As a first work in this line, we restrict ourselves to unitary tamperings.
- Similar to the classical result of [1], can we obtain an efficient construction of tamper detection codes for an arbitrary family of unitary operators of size $2^{s(n)}$ where s is an arbitrary polynomial in n?
- Classically tamper detection codes exist for any $\alpha < 1$. In the current work, we show the existence of unitary tamper detection codes for $\alpha < \frac{1}{6}$. Although we note that with careful optimization of parameters, the same analysis goes through for any $\alpha < \frac{1}{4}$, it will be interesting to see if we can get tamper detection codes for $\alpha \geq \frac{1}{4}$, possibly using some other techniques.
- Classical tamper detection codes turned out to be an important component in the construction of classical non-malleable codes. Even in the case of unitary tamperings against classical messages, we show that tamper detection can lead to meaningful non-malleable guarantees. It would be interesting to see if a similar approach can be taken for quantum messages as well.

Acknowledgment

We thank Thiago Bergamaschi for the helpful discussions. The work of Naresh Goud Boddu was done while he was a PhD student at the Centre for Quantum Technologies (CQT),

NUS, Singapore. This work is supported by the Prime Minister's Office, Singapore and the Ministry of Education, Singapore, under the Research Centres of Excellence program.

References

[1] Zahra Jafargholi and Daniel Wichs. "Tamper detection and continuous non-malleable codes". In Yevgeniy Dodis and Jesper Buus Nielsen, editors, Theory of Cryptography. Pages 451–480. Berlin, Heidelberg (2015). Springer Berlin Heidelberg.

[2] M. Cheraghchi and V. Guruswami. "Capacity of non-malleable codes". IEEE Transactions on Information Theory **62**, 1097–1118 (2016).

[3] Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, and Daniel Wichs. "Efficient non-malleable codes and key-derivation for poly-size tampering circuits". In Phong Q. Nguyen and Elisabeth Oswald, editors, Advances in Cryptology – EUROCRYPT 2014. Pages 111–128. Berlin, Heidelberg (2014). Springer Berlin Heidelberg.

[4] Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padró, and Daniel Wichs. "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors". In Nigel Smart, editor, Advances in Cryptology – EUROCRYPT 2008. Pages 471–488. Berlin, Heidelberg (2008). Springer Berlin Heidelberg.

[5] Ronald Cramer, Carles Padró, and Chaoping Xing. "Optimal algebraic manipulation detection codes in the constant-error model". In Yevgeniy Dodis and Jesper Buus Nielsen, editors, Theory of Cryptography. Pages 481–501. Berlin, Heidelberg (2015). Springer Berlin Heidelberg.

[6] Peter W Shor. "Scheme for reducing decoherence in quantum computer memory". Physical review A **52**, R2493 (1995).

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

[8] Daniel Gottesman. "Stabilizer codes and quantum error correction". PhD thesis. Caltech. (1997). url: https://thesis.library.caltech.edu/2900/2/THESIS.pdf.

[9] A.Yu. Kitaev. "Fault-tolerant quantum computation by anyons". Annals of Physics **303**, 2–30 (2003).

[10] Andrew M Steane. "Error correcting codes in quantum theory". Physical Review Letters **77**, 793 (1996).

[11] Gorjan Alagic and Christian Majenz. "Quantum non-malleability and authentication". In Jonathan Katz and Hovav Shacham, editors, Advances in Cryptology – CRYPTO 2017. Pages 310–341. Cham (2017). Springer International Publishing.

[12] Andris Ambainis, Jan Bouda, and Andreas Winter. "Nonmalleable encryption of quantum information". Journal of Mathematical Physics **50**, 042106 (2009).

[13] A. Broadbent and Sébastien Lord. "Uncloneable quantum encryption via random oracles". IACR Cryptol. ePrint Arch. **2019**, 257 (2019).

[14] Daniel Gottesman. "Uncloneable encryption". Quantum Info. Comput. **3**, 581–602 (2003).

[15] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. "Non-malleable codes". J. ACM**65** (2018).

[16] Mihir Bellare, David Cash, and Rachel Miller. "Cryptography secure against related-key attacks and tampering". In Dong Hoon Lee and Xiaoyun Wang, editors, Advances in Cryptology – ASIACRYPT 2011. Pages 486–503. Berlin, Heidelberg (2011). Springer Berlin Heidelberg.

[17] Mihir Bellare and David Cash. "Pseudorandom functions and permutations provably secure against related-key attacks". In Tal Rabin, editor, Advances in Cryptology – CRYPTO 2010. Pages 666–684. Berlin, Heidelberg (2010). Springer Berlin Heidelberg.

[18] Mihir Bellare and Tadayoshi Kohno. "A theoretical treatment of related-key attacks: Rka-prps, rka-prfs, and applications". In Eli Biham, editor, Advances in Cryptology — EUROCRYPT 2003. Pages 491–506. Berlin, Heidelberg (2003). Springer Berlin Heidelberg.

[19] Mihir Bellare, Kenneth G. Paterson, and Susan Thomson. "Rka security beyond the linear barrier: Ibe, encryption and signatures". In Xiaoyun Wang and Kazue Sako, editors, Advances in Cryptology – ASIACRYPT 2012. Pages 331–348. Berlin, Heidelberg (2012). Springer Berlin Heidelberg.

[20] Sebastian Faust, Krzysztof Pietrzak, and Daniele Venturi. "Tamper-proof circuits: How to trade leakage for tamper-resilience". In Luca Aceto, Monika Henzinger, and Jiří Sgall, editors, Automata, Languages and Programming. Pages 391–402. Berlin, Heidelberg (2011). Springer Berlin Heidelberg.

[21] Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, and Tal Rabin. "Algorithmic tamper-proof (atp) security: Theoretical foundations for security against hardware tampering". In Moni Naor, editor, Theory of Cryptography. Pages 258–277. Berlin, Heidelberg (2004). Springer Berlin Heidelberg.

[22] Vipul Goyal, Adam O'Neill, and Vanishree Rao. "Correlated-input secure hash functions". In Yuval Ishai, editor, Theory of Cryptography. Pages 182–200. Berlin, Heidelberg (2011). Springer Berlin Heidelberg.

[23] Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. "Private circuits ii: Keeping secrets in tamperable circuits". In Serge Vaudenay, editor, Advances in Cryptology - EUROCRYPT 2006. Pages 308–327. Berlin, Heidelberg (2006). Springer Berlin Heidelberg.

[24] Yael Tauman Kalai, Bhavana Kanukurthi, and Amit Sahai. "Cryptography with tamperable and leaky memory". In Phillip Rogaway, editor, Advances in Cryptology – CRYPTO 2011. Pages 373–390. Berlin, Heidelberg (2011). Springer Berlin Heidelberg.

[25] Krzysztof Pietrzak. "Subspace lwe". In Ronald Cramer, editor, Theory of Cryptography. Pages 548–563. Berlin, Heidelberg (2012). Springer Berlin Heidelberg.

[26] Thiago Bergamaschi. "Pauli manipulation detection codes and applications to quantum communication over adversarial channels" (2023). Available at `https://arxiv.org/abs/2304.06269`.

[27] Divesh Aggarwal, Naresh Goud Boddu, and Rahul Jain. "Quantum secure non-malleable codes in the split-state model". IEEE Transactions on Information Theory (2023).

[28] Roman Vershynin. "Introduction to the non-asymptotic analysis of random matrices" (2010). arXiv:1011.3027.

[29] Yinzheng Gu. "Moments of random matrices and weingarten function'' (2013).

[30] Don Weingarten. "Asymptotic behavior of group integrals in the limit of infinite rank". Journal of Mathematical Physics **19**, 999–1001 (1978).

[31] Benoît Collins. "Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability". International Mathematics Research Notices **2003**, 953–982 (2003).

[32] Benoît Collins and Piotr Śniady. "Integration with Respect to the Haar Measure on Unitary, Orthogonal and Symplectic Group". Communications in Mathematical Physics **264**, 773–795 (2006). arXiv:math-ph/0402073.

[33] Naresh Goud Boddu, Vipul Goyal, Rahul Jain, and João Ribeiro. "Split-state non-malleable codes and secret sharing schemes for quantum messages" (2023). arXiv:2308.06466.

A Quantum AMD codes

Let $\mathbb{F}_q$ be the field of size q with characteristic p. Let d be an integer such that p does not divide $d+2$. Consider the following function $f : \mathbb{F}_q^d \times \mathbb{F}_q \to \mathbb{F}_q$ defined by

$$f(s_1, s_2, \ldots, s_d, r) = \sum_{i=1}^{d} s_i r^i + r^{d+2}.$$

We consider an encoding and decoding strategy analogous to classical encoding [4]. The analysis and proof also follow similar lines and are fairly straightforward. Here we present the same for the sake of completeness. For compactness, we will use s to denote $(s_1, s_2, \ldots, s_d) \in \mathbb{F}_q^d$. We will also use $v_{i:j}$ to denote the restriction of the vector v to coordinates from i through j. That is, for a vector $v = (v_1, v_2, \ldots, v_n)$, the restriction $v_{i:j} = (v_i, v_{i+1}, \ldots, v_j)$.

- Let Enc be a quantum encoding defined as below:

$$\mathsf{Enc} : V|(s_1, s_2, \ldots, s_d)\rangle \to |\psi_s\rangle = \frac{1}{\sqrt{q}} \sum_{r \in [q]} |s, r, f(s, r)\rangle.$$

- Let Dec be the POVM $\{\Pi_\perp, \Pi_{s \in \mathbb{F}_q^d}\}$ such that

$$\Pi_s = |\psi_s\rangle\langle\psi_s| \text{ and } \Pi_\perp = \mathbb{1} - \sum_{s \in \mathbb{F}_q^d} \Pi_s \,.$$

Claim 2. $\left| \sum_{r \in \mathbb{F}_q} \langle f((s + x_{1:d}), r + x_{d+1}) || f(s, r) + x_{d+2} \rangle \right|^2 \leq (d+1)^2 \,.$

Proof. Note that the following equation

$$\sum_{i=1}^{d} (s_i + x_i)(r + x_{d+1})^i + (r + x_{d+1})^{d+2} = \sum_{i=1}^{d} s_i r^i + r^{d+2} + x_{d+2}$$

gives a $d+1$ degree polynomial in r. Hence, for at most $d+1$ values of r, we can get $f((s + x_{1:d}), r + x_{d+1}) = f(s, r) + x_{[d+2]}$. The desired inequality now follows. □

Theorem 9. *The above* $(\mathsf{Enc}, \mathsf{Dec})$ *construction is quantum tamper secure (in the relaxed form) against generalized Pauli matrices with parameters* $\left(d \log q, (d+2) \log q, \left(\frac{d+1}{q}\right)^2\right)$.

Proof. Let the error term due to generalized Pauli unitary X be $x = (x_1, x_2, \ldots, x_{d+2})$ to indicate the tampering by

$$X^x = X^{x_1} \otimes X^{x_2} \otimes \cdots \otimes X^{x_{d+2}}.$$

Similarly let the error term due to generalized Pauli unitary Z be $z = (z_1, z_2, \cdots, z_{d+2})$ to indicate the tampering by

$$Z^z = Z^{z_1} \otimes Z^{z_2} \otimes \cdots \otimes Z^{z_{d+2}}.$$

For any message $s = (s_1, s_2, \ldots, s_d)$, the state of the message after encoding and the tampering operation is

$$X^x Z^z |\psi_s\rangle = \frac{1}{\sqrt{q}} \sum_{r\in[q]} \omega^{\langle z_{1:d}, s\rangle + z_{d+1} r + z_{d+2} f(r,s)} |(s_1 + x_1, \ldots, s_d + x_d), r + x_{d+1}, f(s_1, \ldots, s_d, r) + x_{d+2}\rangle.$$

For any other message $s' = (s'_1, s'_2, \ldots, s'_d) \neq s$, the probability of outputting s' when the encoded message s is tampered by $X^x Z^z$ is given by the probability $|\langle \psi_{s'} | X^x Z^z | \psi_s \rangle|^2$. Thus, the probability of outputting a different message can be bounded as follows:

$$\begin{aligned}
&\sum_{s'\neq s} |\langle \psi_{s'} | X^x Z^z | \psi_s \rangle|^2 \\
&= \sum_{s'\neq s} \left| \frac{1}{q} \sum_{r,r'\in[q]} \omega^{<z_{1:d}, s> + z_{d+1} r + z_{d+2} f(r,s)} \langle s', r', f(s', r') | s + x_{1:d}, r + x_{d+1}, f(s,r) + x_{d+2} \rangle \right|^2 \\
&= \left| \frac{1}{q} \sum_{r\in[q]} \omega^{<z_{1:d}, s> + z_{d+1} r + z_{d+2} f(r,s)} \langle f((s + x_{1:d}), r + x_{d+1}) || f(s,r) + x_{d+2} \rangle \right|^2 \\
&\leq \left| \frac{1}{q} \sum_{r\in[q]} \langle f((s + x_{1:d}), r + x_{d+1}) || f(s,r) + x_{d+2} \rangle \right|^2 \\
&\leq \left(\frac{d+1}{q} \right)^2 \qquad \text{(from Claim 2).} \quad \square
\end{aligned}$$

B Higher moments for classical messages

Similar to the case of the first-order moments, we start expressing X_{js} as a sum of products. We then deal with both the cases $j = s$ and $j \neq s$ individually.

Higher moments of random variable X_{js} and X_{ss}:

$$
\begin{aligned}
X_{js}^t &= |\langle\psi_j|U|\psi_s\rangle|^{2t} \\
&= \left(\langle\psi_j|U|\psi_s\rangle\langle\psi_s|U^\dagger|\psi_j\rangle\right)^t \\
&= \left(\sum_{l_1,k_1} U_{l_1k_1}V^*_{l_1j}V_{k_1s}\right)\left(\sum_{l_2,k_2} U^\dagger_{l_2k_2}V^*_{l_2s}V_{k_2j}\right)\cdots\left(\sum_{l_{2t-1},k_{2t-1}} U_{l_{2t-1}k_{2t-1}}V^*_{l_{2t-1}j}V_{k_{2t-1}s}\right)\left(\sum_{l_{2t},k_{2t}} U^\dagger_{l_{2t}k_{2t}}V^*_{l_{2t}s}V_{k_{2t}j}\right) \\
&= \sum_{l_1,k_1}\sum_{l_2,k_2}\cdots\sum_{l_{2t-1},k_{2t-1}}\sum_{l_{2t},k_{2t}}\left(U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}V_{k_1s}V_{k_2j}\ldots V_{k_{2t-1}s}V_{k_{2t}j}V^*_{l_1j}V^*_{l_2s}\ldots V^*_{l_{2t-1}j}V^*_{l_{2t}s}\right).
\end{aligned}
$$

Before going ahead, we would like to introduce some shorthand and notation, given the number of terms involved in expressions to come.

Definition B.1. *For a unitary operator, let U^{c_i} be defined as follows:*

$$U^{c_i} = U \text{ if } c_i \text{ is odd and}$$
$$U^{c_i} = U^\dagger \text{ if } c_i \text{ is even.}$$

For definitions of $C(\alpha), C_1(\alpha), \Sigma_i$ and $\mathsf{Val}(\alpha)$ see Section 2.4. See Section 2.5 for the definition of δ as well as other notations regarding Weingarten functions.

A. When $j \neq s$,

$$
\begin{aligned}
\mathbf{E}[X_{js}^t] &= \mathbf{E}[|\langle\psi_j|U|\psi_s\rangle|^{2t}] \\
&= \sum_{l_1,k_1}\cdots\sum_{l_{2t},k_{2t}}\left(U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\,\mathbf{E}\left[V_{k_1s}V_{k_2j}\ldots V_{k_{2t-1}s}V_{k_{2t}j}V^*_{l_1j}V^*_{l_2s}\ldots V^*_{l_{2t-1}j}V^*_{l_{2t}s}\right]\right) \\
&= \sum_{l_1,k_1}\cdots\sum_{l_{2t},k_{2t}} U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\left(\sum_{\alpha,\beta\in S_{2t}}\delta_\alpha(k_1\ldots k_{2t},l_1\ldots l_{2t})\delta_\beta(sj\ldots sj,js\ldots js)\mathrm{Wg}(\beta\alpha^{-1},N)\right) \\
&= \sum_{\alpha\in S_{2t}}\left[\left(\sum_{k_1=l_{\alpha(1)}}\cdots\sum_{k_{2t}=l_{\alpha(2t)}} U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\right)\left(\sum_{\beta\in S_{2t}}\delta_\beta(sj\ldots sj,js\ldots js)\mathrm{Wg}(\beta\alpha^{-1},N)\right)\right] \\
&= \sum_{\alpha\in S_{2t}}\left[\left(\prod_{(c_1\ c_2\ \ldots\ c_e)\,\in\, C(\alpha)}\mathrm{Tr}(U^{c_1}U^{c_2}\cdots U^{c_e})\right)\left(\sum_{\beta\in S_{2t}}\delta_\beta(sj\ldots sj,js\ldots js)\mathrm{Wg}(\beta\alpha^{-1},N)\right)\right] \\
&\qquad\qquad\text{(from Definition B.1)} \\
&= \sum_{\alpha\in S_{2t}}\sum_{\beta\in S_{2t}}\left[\left(\prod_{(c_1\ c_2\ \ldots\ c_e)\,\in\, C(\alpha)}\mathrm{Tr}(U^{c_1}U^{c_2}\ldots U^{c_e})\right)\left(\delta_\beta(sj\ldots sj,js\ldots js)\mathrm{Wg}(\beta\alpha^{-1},N)\right)\right] \\
&\leq \sum_{\alpha\in S_{2t}}\sum_{\beta\in S_{2t}}\left[\left(\prod_{(c_1\ c_2\ \ldots\ c_e)\,\in\, C(\alpha)}|\mathrm{Tr}(U^{\mathsf{Val}(c_1\ c_2\ldots c_e)})|\right)\left(\delta_\beta(sj\ldots sj,js\ldots js)|\mathrm{Wg}(\beta\alpha^{-1},N)|\right)\right]
\end{aligned}
$$

$$
\begin{aligned}
&\leq \sum_{\alpha\in S_{2t}}\sum_{\beta\in S_{2t}}\left[\left(\prod_{(c_1\ c_2\ \dots\ c_e)\ \in\ C(\alpha)} N\right)\left(\delta_\beta(sj\dots sj, js\dots js)|\mathrm{Wg}(\beta\alpha^{-1},N)|\right)\right] && \text{(from Fact 3)}\\
&\leq \sum_{\alpha\in S_{2t}}\sum_{\beta\in S_{2t}}\left[N^{|C(\alpha)|}\mathcal{O}\left(\delta_\beta(sj\dots sj, js\dots js)\frac{N^{|C(\beta\alpha^{-1})|}}{N^{4t}}\right)\right] && \text{(from eq. (1))}\\
&= \sum_{\alpha\in S_{2t}}\sum_{\beta\in S_{2t}}\left[\mathcal{O}\left(\delta_\beta(sj\dots sj, js\dots js)\frac{N^{|C(\alpha)|+|C(\beta\alpha^{-1})|}}{N^{4t}}\right)\right]\\
&= \sum_{\alpha\in S_{2t}}\sum_{\beta\in\mathcal{B}_{2t}}\mathcal{O}\left[\frac{N^{|C(\alpha)|+|C(\beta\alpha^{-1})|}}{N^{4t}}\right]\\
&\leq \sum_{\alpha\in S_{2t}}\sum_{\beta\in\mathcal{B}_{2t}}\left[\mathcal{O}\left(\frac{1}{N^t}\right)\right] && \text{(from Corollary 5)}\\
&\leq (2t)!(t)!\left[\mathcal{O}\left(\frac{1}{N^t}\right)\right]\\
&\leq \mathcal{O}\left(\frac{t^4}{N}\right)^t && \text{(from Fact 2)}\,.
\end{aligned}
$$

B. When $j = s$,

$$
\begin{aligned}
&\mathbf{E}\left[X_{ss}^t\right] = \mathbf{E}\left[|\langle\psi_s|U|\psi_s\rangle|^{2t}\right]\\
&= \sum_{l_1,k_1}\cdots\sum_{l_{2t},k_{2t}}\left(U_{l_1k_1}U^\dagger_{l_2k_2}\dots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\,\mathbf{E}\left[V_{k_1s}V_{k_2s}\dots V_{k_{2t-1}s}V_{k_{2t}s}V^*_{l_1s}V^*_{l_2s}\dots V^*_{l_{2t-1}s}V^*_{l_{2t}s}\right]\right)\\
&= \sum_{l_1,k_1}\cdots\sum_{l_{2t},k_{2t}}U_{l_1k_1}U^\dagger_{l_2k_2}\dots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\left(\sum_{\alpha,\beta\in S_{2t}}\delta_\alpha(k_1\dots k_{2t},l_1\dots l_{2t})\delta_\beta(ss\dots ss,ss\dots ss)\mathrm{Wg}(\beta\alpha^{-1},N)\right)\\
&= \sum_{\alpha\in S_{2t}}\left[\left(\sum_{k_1=l_{\alpha(1)}}\cdots\sum_{k_{2t}=l_{\alpha(2t)}}U_{l_1k_1}U^\dagger_{l_2k_2}\dots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\right)\left(\sum_{\beta\in S_{2t}}\delta_\beta(ss\dots ss,ss\dots ss)\mathrm{Wg}(\beta\alpha^{-1},N)\right)\right]\\
&= \sum_{\alpha\in S_{2t}}\left[\left(\prod_{(c_1\ c_2\dots c_e)\in C(\alpha)}\mathrm{Tr}(U^{c_1}U^{c_2}\cdots U^{c_e})\right)\left(\frac{1}{N(N+1)\cdots(N+2t-1)}\right)\right] && \text{(from Definition B.1)}\\
&\leq \sum_{\alpha\in S_{2t}}\left[\left(\prod_{c\in C(\alpha)}|\mathrm{Tr}(U^{\mathsf{Val}(c)})|\right)\left(\frac{1}{N(N+1)\cdots(N+2t-1)}\right)\right]\\
&= \sum_{\alpha\in S_{2t}}\left[\left(\prod_{c\in C_1(\alpha)}|\mathrm{Tr}(U)|\prod_{c\in C(\alpha)\setminus C_1(\alpha)}|\mathrm{Tr}(U^{\mathsf{Val}(c)})|\right)\left(\frac{1}{N(N+1)\cdots(N+2t-1)}\right)\right]\\
&\leq \sum_{\alpha\in S_{2t}}\left[\left((\phi N)^{|C_1(\alpha)|}N^{|C(\alpha)|-|C_1(\alpha)|}\right)\left(\frac{1}{N(N+1)\cdots(N+2t-1)}\right)\right] && \text{(from Fact 3)}\\
&\leq \sum_{\alpha\in S_{2t}}\left[\left(\phi^{|\mathsf{Fix}(\alpha)|}N^{|C(\alpha)|}\right)\left(\frac{1}{(2t)!\binom{N+2t-1}{2t}}\right)\right] && \text{(since } \mathsf{Fix}(\alpha)\subseteq C_1(\alpha)\text{)}\\
&= \left(\frac{1}{(2t)!\binom{N+2t-1}{2t}}\right)\sum_{i=1}^{2t}\left[\sum_{\alpha\in S_{2t}:C(\alpha)=i}\left(\phi^{|\mathsf{Fix}(\alpha)|}N^{|C(\alpha)|}\right)\right]
\end{aligned}
$$

$$
\begin{aligned}
&\leq \left(\frac{1}{(2t)!\binom{N+2t-1}{2t}}\right)\left(\sum_{i=1}^{t-1}\left[\sum_{\alpha\in S_{2t}:C(\alpha)=i} N^i\right]+\sum_{i=t}^{2t}\left[\sum_{\alpha\in S_{2t}:C(\alpha)=i}\left(\phi^{2i-2t}N^i\right)\right]\right) && \text{(from Lemma 1)}\\
&= \left(\frac{1}{(2t)!\binom{N+2t-1}{2t}}\right)\left(\sum_{i=1}^{t-1}\left[|\Sigma_{2t-i}|N^i\right]+\sum_{i=t}^{2t}\left[|\Sigma_{2t-i}|\left(\phi^{2i-2t}N^i\right)\right]\right)\\
&\leq \left(\frac{1}{(2t)!\binom{N+2t-1}{2t}}\right)\left(\sum_{i=1}^{t-1}\left[\binom{2t}{2}^{2t-i}N^i\right]+\sum_{i=t}^{2t}\left[\binom{2t}{2}^{2t-i}\left(\phi^{2i-2t}N^i\right)\right]\right) && \text{(from Observation 2)}\\
&= \left(\frac{\binom{2t}{2}^{2t}}{(2t)!\binom{N+2t-1}{2t}}\right)\left(\sum_{i=1}^{t-1}\left[\left(\frac{N}{\binom{2t}{2}}\right)^i\right]+\frac{1}{\phi^{2t}}\sum_{i=t}^{2t}\left[\left(\frac{\phi^2N}{\binom{2t}{2}}\right)^i\right]\right)\\
&\leq \left(\frac{e^{2t-1}(e^2t^2)^{2t}(2t)^{2t}}{(2t)^{2t}(N+2t-1)^{2t}}\right)\left(\sum_{i=1}^{t-1}\left[\left(\frac{N}{t^2}\right)^i\right]+\frac{1}{\phi^{2t}}\sum_{i=t}^{2t}\left[\left(\frac{\phi^2N}{t^2}\right)^i\right]\right) && \text{(from Fact 2)}\\
&= \frac{1}{e}\left(\frac{e^3t^2}{N+2t-1}\right)^{2t}\left(\sum_{i=1}^{t-1}\left[\left(\frac{N}{t^2}\right)^i\right]+\frac{1}{\phi^{2t}}\sum_{i=t}^{2t}\left[\left(\frac{\phi^2N}{t^2}\right)^i\right]\right)\\
&\leq \frac{1}{e}\left(\frac{e^3t^2}{N+2t-1}\right)^{2t}\left(2\left[\left(\frac{\sqrt{N}}{t}\right)^{2t}\right]+\frac{t}{\phi^{2t}}\left[\left(\frac{\phi^2N}{t^2}\right)^{2t}\right]\right) && \text{(since } 4t^2\leq N\text{)}\\
&\leq \mathcal{O}\left(\left(\frac{t\sqrt{N}}{N+2t-1}\right)^{2t}+\frac{t}{\phi^{2t}}\left(\frac{\phi^2N}{N+2t-1}\right)^{2t}\right)\\
&\leq \mathcal{O}\left(\left(\frac{t^2}{N}\right)^t+t\phi^{2t}\right).
\end{aligned}
$$

C Higher moments for quantum messages

We start by representing X_m^t as a sum of products and then move on to calculating higher moments.

Higher moments of random variable X_m:

$$
\begin{aligned}
X_m^t &= \left(\sum_{i=1}^{K}\sum_{j=1}^{K} a_i a_j^* \langle\psi_m|U|\psi_i\rangle\langle\psi_j|U^\dagger|\psi_m\rangle\right)^t \\
&= \left(\sum_{i=1}^{K}\sum_{j=1}^{K} a_i a_j^* \left(\sum_{l_1,k_1} U_{l_1k_1}V^*_{l_1m}V_{k_1i}\right)\left(\sum_{l_1,k_1} U^\dagger_{l_2k_2}V^*_{l_2j}V_{k_2m}\right)\right)^t \\
&= \left(\sum_{i_1,j_1,\ldots i_t,j_t=1}^{K} a_{i_1}\ldots a_{i_t}a^*_{j_1}\ldots a^*_{j_t}\right. \\
&\qquad \left.\left(\sum_{l_1,k_1,\ldots l_{2t},k_{2t}} \left(U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}V_{k_1i_1}V_{k_2m}\ldots V_{k_{2t-1}i_t}V_{k_{2t}m}V^*_{l_1m}V^*_{l_2j_1}\ldots V^*_{l_{2t-1}m}V^*_{l_{2t}j_t}\right)\right)\right).
\end{aligned}
$$

Thus,

$$
\begin{aligned}
\mathbf{E}[X_m^t] &= \sum_{i_1,j_1=1}^{K}\ldots\sum_{i_t,j_t=1}^{K} a_{i_1}\ldots a_{i_t}a^*_{j_1}\ldots a^*_{j_t}\left(\sum_{l_1,k_1}\sum_{l_2,k_2}\cdots\sum_{l_{2t-1},k_{2t-1}}\sum_{l_{2t},k_{2t}}\right. \\
&\qquad \left.\left(U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\,\mathbf{E}\left[V_{k_1i_1}V_{k_2m}\ldots V_{k_{2t-1}i_t}V_{k_{2t}m}V^*_{l_1m}V^*_{l_2j_1}\ldots V^*_{l_{2t-1}m}V^*_{l_{2t}j_t}\right]\right)\right) \\
&= \sum_{i_1,j_1=1}^{K}\ldots\sum_{i_t,j_t=1}^{K} a_{i_1}\ldots a_{i_t}a^*_{j_1}\ldots a^*_{j_t}\left(\sum_{l_1,k_1}\sum_{l_2,k_2}\cdots\sum_{l_{2t-1},k_{2t-1}}\sum_{l_{2t},k_{2t}}\right. \\
&\qquad \left.\left(U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\left(\sum_{\alpha,\beta\in S_{2t}}\delta_\alpha(k_1\ldots k_{2t},l_1\ldots l_{2t})\delta_\beta(i_1m\ldots i_tm,mj_1\ldots mj_t)\mathrm{Wg}(\beta\alpha^{-1},N)\right)\right)\right) \\
&= \sum_{\alpha\in S_{2t}}\left[\left(\sum_{k_1=l_{\alpha(1)}}\cdots\sum_{k_{2t}=l_{\alpha(2t)}} U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\right)\right. \\
&\qquad \left.\left(\sum_{\beta\in S_{2t}}\mathrm{Wg}(\beta\alpha^{-1},N)\left[\sum_{i_1,\cdots i_t,j_1,\cdots j_t=1}^{K} a_{i_1}\ldots a_{i_t}a^*_{j_1}\ldots a^*_{j_t}\delta_\beta(i_1m\ldots i_tm,mj_1\ldots mj_t)\right]\right)\right] \\
&= \sum_{\alpha\in S_{2t}}\left[\left(\sum_{k_1=l_{\alpha(1)}}\cdots\sum_{k_{2t}=l_{\alpha(2t)}} U_{l_1k_1}U^\dagger_{l_2k_2}\ldots U_{l_{2t-1}k_{2t-1}}U^\dagger_{l_{2t}k_{2t}}\right)\left(\sum_{\beta\in S_{2t}}\mathrm{Wg}(\beta\alpha^{-1},N)|a_m|^{2l(\beta)}\right)\right] \\
&= \sum_{\alpha\in S_{2t}}\left[\left(\prod_{(c_1\ c_2\ldots c_e)\in C(\alpha)}\mathrm{Tr}(U^{c_1}U^{c_2}\cdots U^{c_e})\right)\left(\sum_{\beta\in S_{2t}}\mathrm{Wg}(\beta\alpha^{-1},N)|a_m|^{2l(\beta)}\right)\right] \\
&\le \sum_{\alpha\in S_{2t}}\left[\left(\prod_{c\in C(\alpha)}|\mathrm{Tr}(U^{\mathsf{Val}(c)})|\right)\left(\sum_{\beta\in S_{2t}}|\mathrm{Wg}(\beta\alpha^{-1},N)|\right)\right] \\
&= \sum_{\alpha\in S_{2t}}\left[\left(\prod_{c\in C_1(\alpha)}|\mathrm{Tr}(U)|\prod_{c\in C(\alpha)\setminus C_1(\alpha)}|\mathrm{Tr}(U^{\mathsf{Val}(c)})|\right)\left(\frac{1}{N(N-1)\cdots(N-2t+1)}\right)\right] \\
&\le \sum_{\alpha\in S_{2t}}\left[\left((\phi N)^{|C_1(\alpha)|}N^{|C(\alpha)|-|C_1(\alpha)|}\right)\left(\frac{1}{N(N-1)\cdots(N-2t+1)}\right)\right] \qquad \text{(from Fact 3)}
\end{aligned}
$$

$$
\begin{aligned}
&\leq \sum_{\alpha \in S_{2t}} \left[\left(\phi^{|\mathsf{Fix}(\alpha)|} N^{|C(\alpha)} \right) \left(\frac{1}{(2t)! \binom{N}{2t}} \right) \right] && \text{(from Lemma 3)} \\
&= \left(\frac{1}{(2t)! \binom{N}{2t}} \right) \sum_{i=1}^{2t} \left[\sum_{\alpha \in S_{2t} : C(\alpha) = i} \left(\phi^{|\mathsf{Fix}(\alpha)|} N^{|C(\alpha)|} \right) \right] \\
&\leq \left(\frac{1}{(2t)! \binom{N}{2t}} \right) \left(\sum_{i=1}^{t-1} \left[\sum_{\alpha \in S_{2t} : C(\alpha) = i} N^i \right] + \sum_{i=t}^{2t} \left[\sum_{\alpha \in S_{2t} : C(\alpha) = i} \left(\phi^{2i-2t} N^i \right) \right] \right) && \text{(from Corollary 5)} \\
&= \left(\frac{1}{(2t)! \binom{N}{2t}} \right) \left(\sum_{i=1}^{t-1} \left[|\Sigma_{2t-i}| N^i \right] + \sum_{i=t}^{2t} \left[|\Sigma_{2t-i}| \left(\phi^{2i-2t} N^i \right) \right] \right) \\
&\leq \left(\frac{1}{(2t)! \binom{N}{2t}} \right) \left(\sum_{i=1}^{t-1} \left[\binom{2t}{2}^{2t-i} N^i \right] + \sum_{i=t}^{2t} \left[\binom{2t}{2}^{2t-i} \left(\phi^{2i-2t} N^i \right) \right] \right) && \text{(from Fact 2)} \\
&= \left(\frac{\binom{2t}{2}^{2t}}{(2t)! \binom{N}{2t}} \right) \left(\sum_{i=1}^{t-1} \left[\left(\frac{N}{\binom{2t}{2}} \right)^i \right] + \frac{1}{\phi^{2t}} \sum_{i=t}^{2t} \left[\left(\frac{\phi^2 N}{\binom{2t}{2}} \right)^i \right] \right) \\
&\leq \left(\frac{e^{2t-1} (e^2 t^2)^{2t} (2t)^{2t}}{(2t)^{2t} (N)^{2t}} \right) \left(\sum_{i=1}^{t-1} \left[\left(\frac{N}{t^2} \right)^i \right] + \frac{1}{\phi^{2t}} \sum_{i=t}^{2t} \left[\left(\frac{\phi^2 N}{t^2} \right)^i \right] \right) && \text{(from Fact 4)} \\
&= \frac{1}{e} \left(\frac{e^3 t^2}{N} \right)^{2t} \left(\sum_{i=1}^{t-1} \left[\left(\frac{N}{t^2} \right)^i \right] + \frac{1}{\phi^{2t}} \sum_{i=t}^{2t} \left[\left(\frac{\phi^2 N}{t^2} \right)^i \right] \right) \\
&\leq \frac{1}{e} \left(\frac{e^3 t^2}{N} \right)^{2t} \left(2 \left[\left(\frac{\sqrt{N}}{t} \right)^{2t} \right] + \frac{t}{\phi^{2t}} \left[\left(\frac{\phi^2 N}{t^2} \right)^{2t} \right] \right) \\
&\leq \mathcal{O} \left(\left(\frac{t\sqrt{N}}{N} \right)^{2t} + \frac{t}{\phi^{2t}} \left(\frac{\phi^2 N}{N} \right)^{2t} \right) \\
&\leq \mathcal{O} \left(\left(\frac{t^2}{N} \right)^t + t\phi^{2t} \right).
\end{aligned}
$$