Quantum homomorphic encryption from quantum codes

Yingkai Ouyang, Si-Hui Tan, and Joseph F. Fitzsimons

Quantum homomorphic encryption from quantum codes

Yingkai Ouyang, Si-Hui Tan, and Joseph F. Fitzsimons

Singapore University of Technology and Design, 8 Somapah Road, Singapore and
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore*

The recent discovery of fully-homomorphic classical encryption schemes has had a dramatic effect on the direction of modern cryptography. Such schemes, however, implicitly rely on the assumptions that solving certain computation problems are intractable. Here we present a quantum encryption scheme which is homomorphic for arbitrary classical and quantum circuits which have at most some constant number of non-Clifford gates. Unlike classical schemes, the security of the scheme we present is information theoretic and hence independent of the computational power of an adversary.

I. INTRODUCTION

Harnessing the power of quantum mechanics to build cryptosystems [1, 2] is a key motivation for developing quantum technologies. Quantum cryptography often provides information-theoretic security guarantees relying only on the correctness of quantum mechanics, and avoids the need for assumptions about the computational hardness of certain problems as is common place in many classical cryptographic protocols. Such successful quantum approaches to cryptographic problems include secure randomness generation [3, 4], coin-flipping [5–7], secret sharing [8–10] and bit-commitment [11–14]. One area in particular that has seen significant progress in recent years is the development of quantum cryptographic protocols for delegated computation [15], which includes blind quantum computation [16–21], and verifiable quantum computation [22–27]. Homomorphic encryption has been recognised as an important primitive for building secure delegated computation protocols for many decades [28]. It provides a processing functionality for encrypted quantum data which stays secret during the evaluation, and a scheme is said to be *fully-homomorphic* if it allows for arbitrary quantum computation. Despite widespread interest in this problem, it was not until 2009 that the first computationally secure classical scheme for fully homomorphic encryption (FHE) was discovered [29], with many improvements following rapidly from this initial discovery [30, 31]. Recently this topic also has drawn attention within the quantum information community [32–37]. One might wonder if quantum cryptosystems can offer unconditionally secure homomorphic encryption schemes and whether homomorphic encryption could be extended to allow for evaluation of quantum circuits.

Like their classical counterparts, quantum homomorphic encryption (QHE) schemes comprise of four parts: key generation, encryption, evaluation, and decryption. Unlike blind quantum computation [16], in which the computation to be performed forms part of the secret, QHE schemes do not have secret circuit evaluations. Rather, they serve to obscure only the information that

is contained within the state to be processed using the chosen circuit. The extent to which a scheme is secure depends on its specifics, and in previous work has varied depending on the precise nature of the set of computations which can be performed on the encrypted input. QHE schemes described in Refs. [36, 37] offer some information theoretic security, but this is only in the form of a gap between the information accessible with and without the secret key, a notion of security which does not imply the stronger notion of security under composition. These schemes are also limited in the set of operations that can be performed on the encrypted data. The scheme in [36] only allows computations in the BosonSampling model, while that in [37] is not known to support encoded universal quantum computing. Recently Dulek, Schaffner and Speelman [38] used the garden-hose model of computation with Broadbent and Jeffery's quantum homomorphic schemes [39] to allow the evaluation of polynomial-depth circuits. Several other schemes for computing on encrypted data have previously been introduced which offer universal quantum computation, but require interactions between the client and evaluator [32–35]. This requirement for interaction places them outside of the formalism of homomorphic encryption.

The difficulty in creating a perfectly secure quantum fully-homomorphic encryption (QFHE) scheme persists, and is in line with the no-go results that perfect [40] and approximate [41] information-theoretic security whilst enabling arbitrary processing of encrypted data is impossible, unless the size of the encoding grows exponentially. Nonetheless, given the growing interest in QHE schemes and the multitude of possibilities, Broadbent and Jeffery set out to provide a rigorous framework for defining QHE schemes [39], basing their security definitions on the requirement for indistinguishability of codewords under chosen plaintext attack. Broadbent and Jeffery also require that a quantum *fully* homomorphic encryption satisfies two properties: correctness and compactness. Perfect correctness occurs when the evaluated output on the cipherstate after decryption is equivalent to the output of the direct evaluation on the quantum plaintext. A scheme is compact if the circuit complexity of decryption algorithm does not depend on the computation to be evaluated and scales only polynomially in the size of the plaintext. An important implication of the

---

compactness requirement for QHE schemes is that the decryption algorithm of such schemes cannot in any way depend on the evaluated computation. This necessarily implies that a one-time-padding scheme, where random Paulis encrypt the quantum input, does not qualify as a QHE scheme. This is because the decryption algorithm of a one-time-padding scheme is not independent of the evaluated computation.

We present a QHE scheme that supports evaluation of quantum circuits with a constant number of T-gates on multiple copies of the input qubits while providing strong information theoretic security guarantees. The proposed scheme, which requires the encoder to be able to produce the multiple copies of the input state, builds on constructions taken from quantum codes to provide gates for universal quantum computation. The block of qubits that contains the code is embedded in a larger set of qubits that are initialized in a maximally mixed state. The qubits are then shuffled in a specific but random way to hide the qubits that contain that code. In our scheme, the evaluation of each T-gate succeeds with a probability of half. This leads to a trade-off between the size of the encoding and the success probability, since the probability of success can be amplified by encoding several instances of the plaintext in parallel. To achieve a constant success probability, however, the size of this encoding would scale exponentially in the total number of T-gates to be performed, Hence, in order to maintain compactness, we restrict evaluation to circuits containing at most some constant number of T gates. The computational model that we consider is non-trivial in the sense that even performing just the Clifford operations on an arbitrary quantum input is known to be hard unless the polynomial hierachy collapses [42–45].

Our protocol guarantees that the trace distance between ciphertexts corresponding to arbitrary pairs of quantum inputs is exponentially suppressed in the key size less half the total number of qubits used for the quantum input. An encryption scheme has entropic security if an adversary whose min-entropy on the encrypted message is upper bounded cannot guess any function of the message [46, 47]. When the quantum min-entropy of the source in our scheme is sufficiently large, the trace distance between ciphertexts is exponentially suppressed in only the key size. Since an exponentially suppressed trace distance implies entropic security [46], our scheme is also secure for high entropy quantum inputs on any number of qubits with a constant key size.

This is a significantly stronger security guarantee than previous homomorphic encryption schemes presented in Ref. [36] and Ref. [37]. Moreover the computation power of our scheme is similar to that of Broadbent and Jeffery's while avoiding reliance on the classical homomorphic encryption scheme. This use of classical fully homomorphic encryption is the weakest link in the Broadbent-Jeffery cryptosystem, since it relies on computational assumptions [52]. When considering the case of no T-gates, it is instructive to compare the decryption complexities of
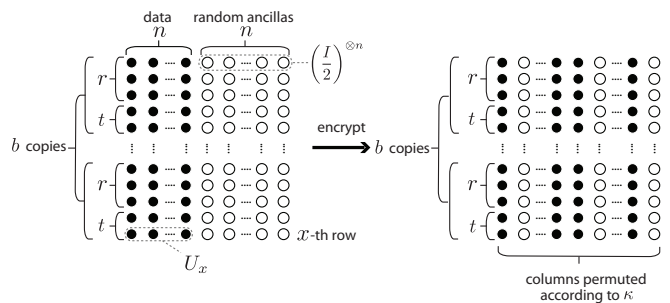

FIG. 1: The shaded circles represent data qubits. Within the x-th row, the n data qubits are in a code encoded by U_x. The unshaded circles are ancilla qubits which are completely mixed. There are b copies of r logical qubits. A random permutation of the columns completes the encryption procedure of our quantum homomorphic encryption scheme.

our QHE scheme and the non-QHE quantum one-time padding scheme. In the one-time padding scheme, it is necessary for the decryption routine to take into account a description of the entire circuit which has been performed. Due to the number of Clifford group operations, this implies that the decryption algorithm has complexity at least quadratic in the plaintext size. In contrast our QHE scheme requires only a linear complexity for decryption, as long as it has at most a constant number of T-gates in the evaluated computation.

II. OUR QHE SCHEME

Our QHE scheme takes as its input a r-qubit state ρ_{input}, and t independent copies of the magic state $|T\rangle\langle T| = \frac{I}{2} + \frac{X+Y}{2\sqrt{2}}$, all arranged in a single column (See Figure 1), where I, X, Y, Z are the usual Pauli matrices. We then introduce $(2n-1)$ more columns of maximally mixed qubits to obtain a grid of qubits with $r + t$ rows and $2n$ columns. Here, we require $\frac{n-1}{4}$ to be a non-negative integer. Of the new columns introduced, $n-1$ of them are incorporated as data qubits while the remaining n columns are used as ancillae in the encryption. An encoding quantum circuit $U = U_1 \otimes \cdots \otimes U_{r+t}$ applies row-wise on the first n columns, where U_x operates on the x-th row (see Figure 2). We take A_x and B_x to denote the first and last $n-1$ gates in U_x respectively, so that $U_x = B_x A_x$. Applying U spreads the quantum input from just the first column to the first n columns. Since every qubit not residing on the first column is maximally mixed, the encoding circuit on each row encodes the quantum data on the first column into a random quantum code, the resultant quantum information of which resides in a random codespace on the first n columns. Namely on the x-th row, the encoding maps an arbitrary state $\rho_{\text{input}} = \frac{I+r_X X+r_Y Y+r_Z Z}{2}$ in the first column and with maximally mixed states on the remaining $n-1$ columns to the mixed state $U_x \left(\frac{I+r_X X+r_Y Y+r_Z Z}{2} \otimes ((\frac{I}{2})^{\otimes n-1}) \right) U_x^\dagger$ which is equiva-
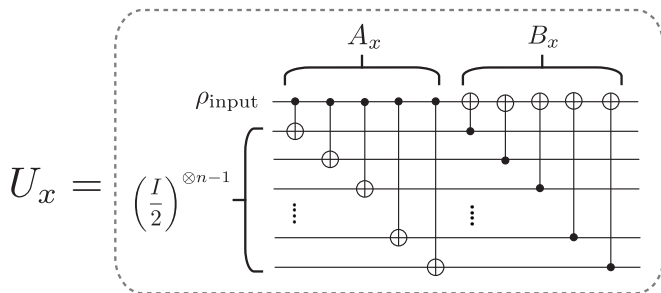
FIG. 2: Figure shows the encoding quantum circuit $U_x = B_x A_x$ that is applied on the first n qubits in the x-th row. Each line represents one qubit and the gates are applied in the order from left to right.

lent to $2^{-n}(I^{\otimes n} + r_X X^{\otimes n} + r_Y Y^{\otimes n} + r_Z Z^{\otimes n})$. We emphasize at this point that any state in our random codespace is a highly mixed state. Encryption is then achieved via randomly permuting the $2n$ columns using a secret permutation κ. Permuting the columns brings the quantum information to be processed from the first n columns to the columns $k_1, \ldots, k_n$, where $1 \leq k_1 < \cdots < k_n \leq 2n$. For the decryption algorithm, one performs the inverse permutation of the columns κ^{-1}, followed by the inverse unitary $U^\dagger$ on the first n columns of the grid. Finally every qubit in the rows $r+1$ to $r+t$ are measured in the computation basis. The quantum output of our scheme is then located on the first r rows of the first column of our grid of qubits.

The single qubit logical Clifford operators of each of our random codes on n qubits are transversal gates on those n qubits. This means that a logical G operator on the x-th row is $G^{\otimes n}$ that operates on the first n-columns for every Clifford gate G in the set generated by $\{S, H\}$ where $S = |0\rangle\langle 0| + i|1\rangle\langle 1|$ and $H = \frac{X+Z}{\sqrt{2}}$ is the Hadamard matrix. To see this, notice that $U_x(Z \otimes I^{\otimes n-1}) = B_x A_x(Z \otimes I^{\otimes n-1}) = B_x(Z \otimes I^{\otimes n-1})A_x = Z^{\otimes n} B_x A_x = Z^{\otimes n} U_x$. Hence our encoding circuit U_x maps the physical Z on one qubit to $Z^{\otimes n}$. Similarly, $U_x(X \otimes I^{\otimes n-1}) = B_x A_x(X \otimes I^{\otimes n-1}) = B_x X^{\otimes n} A_x = X^n \otimes X^{\otimes n-1} B_x A_x$. Since n is odd, we get $U_x(X \otimes I^{\otimes n-1}) = X^{\otimes n} U_x$. Thus our encoding circuit U_x maps the physical X on one qubit to $X^{\otimes n}$. Since $Y = iXZ$ and $n-1$ is also divisible by 4, our encoding circuit U_x maps the physical Y on one qubit to $Y^{\otimes n}$. Now $X^{\otimes n}$ and $Z^{\otimes n}$ anticommute because n is odd, and the $Y^{\otimes n}$ anticommutes with $X^{\otimes n}$ and $Z^{\otimes n}$. Upon conjugation by $H^{\otimes n}$, $X^{\otimes n}$ becomes $Z^{\otimes n}$ and vice versa, and $Y^{\otimes n}$ becomes $-Y^{\otimes n}$. Upon conjugation by $S^{\otimes n}$ gate, $X^{\otimes n}$ and $Y^{\otimes n}$ become $Y^{\otimes n}$ and $-X^{\otimes n}$ respectively. Transversality of the logical CNOT with control and target on distinct rows follows immediately from the transversality of the logical X operation. Thus the transversal Clifford operations on the n columns containing the encoded quantum data are precisely the logical Clifford operations.

The evaluator operates independently and identically (i.i.d) on not n but $2n$ columns of qubits, n columns of

which are the maximally mixed state. The i.i.d structure of the evaluator's operations allows these operations to commute with any secret permutation of the columns of the qubits on the grid. In addition, the evaluators' operations necessarily map the n columns of qubits initialized in the maximally mixed state to the maximally mixed state, thereby implementing i.i.d quantum operations on only the columns containing the encoded quantum data. This allows the evaluator to perform transversal gates on the n columns with the quantum data without knowing where they are located.

The evaluation algorithm takes as input a sequence of unitary operations $(V_1, \ldots, V_d)$ to be performed securely on r qubits, where each V_i applies either a Clifford gate or a T gate locally on a single qubit, or applies a CNOT locally on a pair of qubits. The number of T-gates to be applied locally amongst the unitary operations $V_1, \ldots, V_d$ is at most t. The circuit to be evaluated is $V = V_d \ldots V_1$, where the evaluator applies homomorphisms of the gates V_1 to V_d sequentially.

When V_i is a unitary operation that applies a Clifford gate G locally on the x-th qubit, the evaluator can apply the logical G-gate on our random code on the x-th row without any knowledge of the data columns $k_1, \ldots, k_n$. To do so, the evaluator simply applies the unitary $G^{\otimes 2n}$ on the $2n$ qubits located on the x-th row on each copy. Since conjugating a maximally mixed state $\frac{I}{2}$ by any qubit unitary operation yields also a maximally mixed state, the net effect is to apply the unitary $G^{\otimes n}$ on the qubits in the encrypted data columns $k_1, \ldots, k_n$ on the x-th row, which is the logical G-gate on the x-th row.

When V_i is a unitary operation that applies a CNOT gate with control on the x-th qubit and target on the y-th qubit, denoted as $\mathrm{CNOT}_{x,y}$, the evaluator can also apply the corresponding logical CNOT gate on our random code on the x-th and y-th row without any knowledge of the data columns $k_1, \ldots, k_n$. To do so, the evaluator simply applies a CNOT with control qubit on the x-th row and the j-th column and target qubit on the y-th row and the j-th column for every $j = 1, \ldots, 2n$. As before, the net effect is to apply the unitary $\mathrm{CNOT}^{\otimes n}$ on the qubits in the encrypted data columns $k_1, \ldots, k_n$ with control qubits on the x-th row and target qubits on the y-th row, which is the correct logical CNOT-gate, which we denote as $\overline{\mathrm{CNOT}}_{x,y}$.

When V_i is a unitary operation that applies the k-th non-Clifford gate $T = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$ on the x-th qubit, the evaluator has to perform gate teleportation [48, 49]. Now consider gate teleportation of a single-qubit gate T. Omitting the correction operation required by gate teleportation allows this procedure to succeed with probability $\frac{1}{2}$ as depicted in Figure 3. The principle of deferred measurement [50] allows deferment of the required measurement until decryption. To implement gate teleportation of the logical T operation, the evaluator applies homomorphisms for $\mathrm{CNOT}_{x,r+k}$ and $\mathrm{CNOT}_{r+k,x}$ sequentially. Because of the ancilla columns being in the maximally mixed state, the unitary $\overline{\mathrm{CNOT}}_{x,r+k}$ followed
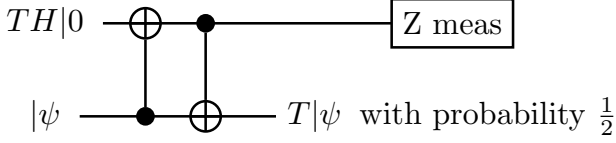
FIG. 3: Gate teleportation of the T-gate without correction.

by the unitary $\overline{\text{CNOT}}_{r+k,x}$ are effectively applied on the data columns $k_1, \ldots, k_n$. For the data qubits encoded on the random codespace, this action implements a logical T gate on the random codespace with probability $\frac{1}{2}$ when the outcome of the logical Z-measurement is 0. This scheme works because by replacing each Pauli in the Pauli decomposition of $|T\rangle\langle T|$ with the corresponding logical Pauli, we obtain precisely the logical $|T\rangle\langle T|$-state. We emphasize that the outcome of the logical Z-measurement is a flag for the correctness of the implementation of the T-gate; if the outcome is 0 the gate is successfully implemented, otherwise the implementation fails.

Our scheme with heralded success satisfies the correctness condition of Broadbent and Jeffery. Each copy of our scheme yields the correct quantum output with constant probability 2^{-t}. Extra copies simply amplify the probability of success. Thus although each instance of our scheme implements T non-deterministically, it has *heralded* perfect completeness: namely, $b = \lfloor\sqrt{\frac{\alpha}{2}} + 1\rfloor^2 2^{2t}$ copies of our scheme yields the correct output in at least one copy with probability at least $1 - e^{-\alpha}$, and we know which of the b copies yield the correct output. A large α amplifies the success probability close to unity.

In the three-part algorithm for the decryption, $U^\dagger$ requires $2(n-1)b(r+t)$ gates, and unpermuting of the columns requires at most $(2n-1)b(r+t)$ gates (the largest cycle contained in any element of S_{2n} is a $(2n)$-cycle which can be written as a product of $2n-1$ swaps). The remainder of the decryption involves a readout of Z measurements and discarding a subsystem. Since t is constant, b is also constant, and the total number of gates required for decryption scales linearly with r and is independent of the depth of the circuit to be evaluated. Hence, our scheme is compact for the family of circuits on r qubits with a constant maximum number of T gates and any number of Clifford gates.

Randomly permuting the columns of qubits obfuscates the subset of columns where the quantum information resides, thereby encrypting the quantum data. The maximum trace distance between any two quantum ciphertexts with min-entropy h is

$$\epsilon \leq \sqrt{2^{p-h}} \binom{2n}{n}^{-1/2}, \qquad (1)$$

where $p = b(r + t)$. In the worst case, where $h = 0$, ϵ is exponentially suppressed in n as long as the key size

n grows linearly with the input size r. However when $t = 0, b = 1$ and $h = r - x$ for any constant x, the key size n can be independent of the input size r while having ϵ being exponentially suppressed in n. In both cases, any two quantum ciphertexts are essentially the maximally mixed state and hence indistinguishable in our scheme.

To obtain Eq. (1), we first obtain a Pauli decomposition of any arbitrary state that the evaluator receives. Let the density matrices ρ and ρ' on b copies of $2n(r+t)$ qubits be any two arbitrary inputs to the scheme before encoding and encryption. Let $\widetilde{\rho}$ and $\widetilde{\rho}'$ be the corresponding states after encoding and encryption. Then $\epsilon = \frac{1}{2}\max_{\rho,\rho'} \|\widetilde{\rho} - \widetilde{\rho}'\|_{\text{tr}}$. In this maximization, only the $p = b(r + t)$ qubits in the first column are arbitrary, and the remaining columns are in the maximally mixed state. Note that $\|\widetilde{\rho} - \widetilde{\rho}'\|_{\text{tr}} = \text{Tr}(M(\widetilde{\rho} - \widetilde{\rho}'))$ for some optimal Hermitian M diagonal in the same basis as $\widetilde{\rho} - \widetilde{\rho}'$, with eigenvalues equal to $+1$ or -1. More precisely, if $\widetilde{\rho} - \widetilde{\rho}'$ has the spectral decomposition $\sum_i \lambda_i |i\rangle\langle i|$, then $M = \sum_i \text{sign}(\lambda_i)|i\rangle\langle i|$, where $\text{sign}(\lambda_i) = 1$ if $\lambda_i \geq 0$ and $\text{sign}(\lambda_i) = -1$ otherwise. Now define $\sigma_0 = I, \sigma_1 = X, \sigma_2 = Y$, and $\sigma_3 = Z$. Let $\mathcal{M}_{p,2n}(\mathbb{Z}_4)$ denote the set of all matrices with p rows and $2n$ columns and entries from $\{0, 1, 2, 3\}$. Given any matrix $A \in \mathcal{M}_{p,2n}(\mathbb{Z}_4)$, let $a_{x,y}$ denote its component in the x-th row and the y-th column. Define the unitary matrix σ_A to be one that applies $\sigma_{a_{x,y}}$ on the x-th row and y-th column of our grid of qubits for every $x = 1, \ldots, p$ and $y = 1, \ldots, 2n$. Define the set of all column permutations of σ_A as S_A, and the corresponding symmetric sum of σ_A as $\widetilde{\sigma}_A = \sum_{\tau \in S_A} \tau$. Let Ω denote the set of non-zero column vectors of length p with entries from $\{0, 1, 2, 3\}$. For all $\mathbf{v} \in \Omega$, let $\varphi(\mathbf{v})$ denote a matrix with p rows and $2n$ columns such that its first n columns are identical to $\mathbf{v}$ and the last n columns have all entries equal to zero. Notice that for distinct $\mathbf{v}, \mathbf{v}' \in \Omega$, $\widetilde{\sigma}_{\varphi(\mathbf{v})}$ and $\widetilde{\sigma}_{\varphi(\mathbf{v}')}$ are also distinct. Let $\mathcal{S}$ denote some minimal subset of $\mathcal{M}_{p,2n}(\mathbb{Z}_4)$ such that $\{\widetilde{\sigma}_A : A \in \mathcal{S}\} = \{\widetilde{\sigma}_A : A \in \mathcal{M}_{p,2n}(\mathbb{Z}_4)\}$. Now we can always have $\varphi(\mathbf{v}) \in \mathcal{S}$ for every $\mathbf{v} \in \Omega$. Let $\widetilde{M} = \frac{1}{(2n)!}\sum_\pi \pi M \pi^\dagger$, where π is any column permutation. Then we can write $\widetilde{M} = \sum_{A \in \mathcal{S}} a_A \widetilde{\sigma}_A$, for appropriate real constants a_A.

Linearity and the cyclic property of the trace give $\text{Tr}(M(\widetilde{\rho} - \widetilde{\rho}')) = \text{Tr}(\widetilde{M}(\rho - \rho'))$. Using the decomposition $\rho - \rho' = \sum_{\mathbf{v} \in \Omega} \frac{r_\mathbf{v} - r'_\mathbf{v}}{2^{2np}} \sigma_{\varphi(\mathbf{v})}$ for appropriate real constants $r_\mathbf{v}$ and $r'_\mathbf{v}$, the decomposition of $\widetilde{M}$, the linearity of trace, and the triangle inequality, we get

$$\|\widetilde{\rho} - \widetilde{\rho}'\|_{\text{tr}} \leq \sum_{\mathbf{v} \in \Omega} \sum_{B \in \mathcal{S}} \left| \text{Tr}\, a_B \widetilde{\sigma}_B \frac{(r_\mathbf{v} - r'_\mathbf{v})}{2^{2np}} \sigma_{\varphi(\mathbf{v})} \right|. \qquad (2)$$

Orthogonality of the Pauli operators under the Hilbert-Schmidt inner product gives

$$\|\widetilde{\rho} - \widetilde{\rho}'\|_{\text{tr}} \leq \sum_{\mathbf{v} \in \Omega} \left| \text{Tr}\, a_{\varphi(\mathbf{v})}(r_\mathbf{v} - r'_\mathbf{v}) \right|. \qquad (3)$$

The Cauchy-Schwarz inequality implies that $\|\widetilde{\rho} - \widetilde{\rho}'\|_{\text{tr}} \leq$

$\sqrt{\sum_{\mathbf{v} \in \boldsymbol{\Omega}} a_{\varphi(\mathbf{v})}^2} \sqrt{\sum_{\mathbf{v} \in \boldsymbol{\Omega}} (r_{\mathbf{v}} - r'_{\mathbf{v}})^2}$. Since in Loewner order $\widetilde{M}^2 \leq I$, and hence $\text{Tr}(\widetilde{M}^2) \leq \text{Tr}(I)$, we have $\sum_{\mathbf{v} \in \boldsymbol{\Omega}} a_{\varphi(\mathbf{v})}^2 \binom{2n}{n} \leq 1$. Next we show that $\sum_{\mathbf{v} \in \boldsymbol{\Omega}} (r_{\mathbf{v}} - r'_{\mathbf{v}})^2 \leq 2^{p-h+2}$ if the p-qubit inputs to the first column of our scheme has a quantum min-entropy [51] of h. Let τ and τ' be unencrypted p-qubit states, with $\rho = U(\tau \otimes (I/2)^{\otimes(2n-1)p})U^\dagger$ and $\rho' = U(\tau' \otimes (I/2)^{\otimes(2n-1)p})U^\dagger$. The Pauli decompositions $\tau = 2^{-p} \sum_{\mathbf{v} \in \Omega} r_{\mathbf{v}} \sigma_{\mathbf{v}}$ and $\tau' = 2^{-p} \sum_{\mathbf{v} \in \Omega} r_{\mathbf{v}} \sigma_{\mathbf{v}}$ imply that $\text{Tr}((\tau - \tau')^2) = \sum_{\mathbf{v} \in \Omega} (r_{\mathbf{v}} - r'_{\mathbf{v}})^2 2^{-p}$. Given the min-entropy of τ and τ', their maximum eigenvalue is 2^{-h}. Hence $\text{Tr}((\tau - \tau')^2) \leq 2^{-h+2}$. Then $\sum_{\mathbf{v} \in \Omega} (r_{\mathbf{v}} - r'_{\mathbf{v}})^2 \leq 2^{p-h+2}$ and Eq. (1) can thereby be obtained.

III. DISCUSSIONS

In summary, our QHE scheme encodes the quantum input using random codes, encrypts and decrypts via a secret permutation, and allows the evaluator to compute a constant number of non-Clifford (T) gates on the encrypted data. Since the encrypted quantum ciphertexts are almost indistinguishable, the evaluator is essentially oblivious to the quantum input, which gives our scheme its information-theoretic security. Moreover, our scheme trivially allows homomorphisms of arbitrary reversible linear boolean circuits using the homomorphisms of CNOT and X gates. Our scheme may also offer robustness to noise when the encryptor holds purifications to the maximally mixed states used in the random encodings and performs a recovery operation dependent on the classical measurement outcomes on her ancillary registers, and we leave this for future study. We also like to point out that it is sometimes preferable to use a quantum one-time padding scheme as opposed to our scheme for delegated computation, for example when no T gates need to be performed and when all the input states are stabilized by Clifford gates.

IV. ACKNOWLEDGEMENTS

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, New York, 1984.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[3] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1022–1024, 2010.

[4] U. Vazirani and T. Vidick, "Certifiable quantum dice: Or, true random number generation secure against quantum adversaries," in *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, (New York, NY, USA), pp. 61–76, ACM, 2012.

[5] L. Goldenberg, L. Vaidman, and S. Wiesner, "Quantum gambling," *Phys. Rev. Lett.*, vol. 82, pp. 3356–3359, Apr 1999.

[6] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, "Quantum bit escrow," in *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC, (New York, NY, USA), pp. 705–714, ACM, 2000.

[7] A. Ambainis, "A new protocol and lower bounds for quantum coin flipping," in *Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing*, STOC '01, (New York, NY, USA), pp. 134–142, ACM, 2001.

[8] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, pp. 1829–1834, Mar 1999.

[9] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, pp. 648–651, Jul 1999.

[10] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, p. 042311, Mar 2000.

[11] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, "Reexamination of quantum bit commitment: The possible and the impossible," *Phys. Rev. A*, vol. 76, p. 032328, Sep 2007.

[12] A. Chailloux and I. Kerenidis, "Optimal bounds for quantum bit commitment," in *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, pp. 354–362, Oct 2011.

[13] A. Kent, "Unconditionally secure bit commitment with flying qudits," *New Journal of Physics*, vol. 13, no. 11, p. 113015, 2011.

[14] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," *Physical review letters*, vol. 109, no. 13, p. 130501, 2012.

[15] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, "Composable security of delegated quantum computation," in *Advances in Cryptology–ASIACRYPT 2014*, pp. 406–425, Springer, 2014.

[16] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on*, pp. 517–526, Oct 2009.

[17] D. Aharonov, M. Ben-or, and E. Eban, "Interactive proofs for quantum computations," *arXiv:0810.5375*,

2008.

[18] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," *Science*, vol. 335, no. 6066, pp. 303–308, 2012.

[19] T. Morimae and K. Fujii, "Blind quantum computation protocol in which Alice only makes measurements," *Phys. Rev. A*, vol. 87, p. 050301, May 2013.

[20] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, "Efficient universal blind quantum computation," *Phys. Rev. Lett.*, vol. 111, p. 230501, Dec 2013.

[21] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Optimal blind quantum computation," *Phys. Rev. Lett.*, vol. 111, no. 23, p. 230502, 2013.

[22] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind computation," *arXiv prnote arXiv:1203.5217*, 2013.

[23] B. W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," *Nature*, vol. 496, pp. 456–460, 04 2013.

[24] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, "Experimental verification of quantum computation," *Nat. Phys.*, vol. 9, pp. 727—731, 11 2013.

[25] M. McKague, "Self-testing graph states," in *Theory of Quantum Computation, Communication, and Cryptography* (D. Bacon, M. Martin-Delgado, and M. Roetteler, eds.), vol. 6745 of *Lecture Notes in Computer Science*, pp. 104–120, Springer Berlin Heidelberg, 2014.

[26] M. Hayashi and T. Morimae, "Verifiable measurement-only blind quantum computing with stabilizer testing," *Phys. Rev. Lett.*, vol. 115, p. 220502, Nov 2015.

[27] M. Hayashi and M. Hajdusek, "Self-guaranteed measurement-based quantum computation," *arXiv preprint arXiv:1603.02195*, 2016.

[28] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.

[29] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, STOC '09, (New York, NY, USA), pp. 169–178, ACM, 2009.

[30] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Advances in cryptology–EUROCRYPT 2010*, pp. 24–43, Springer, 2010.

[31] C. Gentry, S. Halevi, and N. Smart, "Fully homomorphic encryption with polylog overhead," in *Advances in Cryptology EUROCRYPT 2012* (D. Pointcheval and T. Johansson, eds.), vol. 7237 of *Lecture Notes in Computer Science*, pp. 465–482, Springer Berlin Heidelberg, 2012.

[32] M. Liang, "Symmetric quantum fully homomorphic encryption with perfect security," *Quantum Information Processing*, vol. 12, no. 12, pp. 3675–3687, 2013.

[33] M. Liang, "Quantum fully homomorphic encryption scheme based on universal quantum circuit," *Quantum Information Processing*, pp. 1–11, 2015.

[34] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, "Quantum computing on encrypted data," *Nat. Commun.*, vol. 5, 01 2014.

[35] A. M. Childs, "Secure assisted quantum computation," *Quantum Info. Comput.*, vol. 5, pp. 456–466, Sept. 2005.

[36] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, "Quantum walks with encrypted data," *Phys. Rev. Lett.*,

vol. 109, p. 150501, Oct 2012.

[37] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, "A quantum approach to homomorphic encryption," *Scientific Reports*, vol. 6, p. 33467, 2016.

[38] Y. Dulek, C. Schaffner, and F. Speelman, "Quantum homomorphic encryption for polynomial-sized circuits," pp. 3–32, 2016.

[39] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low t-gate complexity," in *Annual Cryptology Conference*, pp. 609–629, Springer, 2015.

[40] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Limitations on information-theoretically-secure quantum homomorphic encryption," *Phys. Rev. A*, vol. 90, p. 050303, Nov 2014.

[41] M. Newman and Y. Shi, "Limitations on transversal computation through quantum homomorphic encryption," *arXiv preprint arXiv:1704.07798*, 2017.

[42] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal clifford gates and noisy ancillas," *Physical Review A*, vol. 71, no. 2, p. 022316, 2005.

[43] R. JOZSA and M. V. D. NEST, "Classical simulation complexity of extended clifford circuits," *Quantum Information and Computation*, vol. 14, pp. 0633–0648.

[44] D. E. Koh, "Further extensions of clifford circuits and their classical simulation complexities," *Quantum Information and Computation*, vol. 17, pp. 0262–0282.

[45] A. Bouland, J. F. Fitzsimons, and D. E. Koh, "Complexity classification of conjugated clifford circuits," *arXiv preprint arXiv:1709.01805*, 2017.

[46] S. Desrosiers, "Entropic security in quantum cryptography," *Quantum Information Processing*, vol. 8, no. 4, pp. 331–345, 2009.

[47] S. Desrosiers and F. Dupuis, "Quantum entropic security and approximate quantum encryption," *Information Theory, IEEE Transactions on*, vol. 56, pp. 3455–3464, July 2010.

[48] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, pp. 390–393, 1999.

[49] X. Zhou, D. W. Leung, and I. L. Chuang, "Methodology for quantum logic gate construction," *Phys. Rev. A*, vol. 62, p. 052316, Oct 2000.

[50] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, second ed., 2000.

[51] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Transactions on Information Theory*, vol. 55, pp. 4337–4347, Sept 2009.

[52] We note that since the Broadbent-Jeffery cryptosystem utilises the classical FHE to compute sums of hidden subsets, it may be possible to remove the computational assumptions by replacing the FHE scheme with an information theoretically secure scheme which allows evaluation of only linear circuits. However, no analysis of such a modification has yet appeared in the literature.

Appendix A: Security proof

Here, we provide a detailed proof of Eq. (1). We begin by reviewing some terminology.

In our scheme, qubits are arranged on a grid with p rows and $2n$ columns. In the encryption procedure, the columns of $2n$ qubits are randomly permuted. Hence we consider S_{2n}, a symmetric group of order $2n$, and its representation $\nu_{p,2n}$. For every permutation $\pi \in S_{2n}$, and every $A = \sum_{x=1}^{p} \sum_{y=1}^{2n} a_{x,y} |x\rangle\langle y| \in \mathcal{M}_{p,2n}$, we let $\nu_{p,q} : S_{2n} \to \mathcal{M}(\mathbb{C}^{2np})$ be a representation of S_{2n} such that for every matrix representation $P_\pi = \nu_{p,q}(\pi)$ of $\pi \in S_{2n}$, we have

$$P_\pi \sigma_A P_\pi^\dagger = \bigotimes_{y=1}^{2n} \left(\bigotimes_{y=1}^{p} \sigma_{a_{x,\pi(y)}} \right). \tag{A1}$$

The matrices P_π are the permutation operations that permute the columns in our scheme. With these permutation operations, we can define the set of Paulis generated from all possible column permutations of a particular Pauli σ_A, given by

$$S_A = \left\{ P_\pi \sigma_A P_\pi^\dagger : \pi \in S_{2n} \right\}. \tag{A2}$$

The symmetrized Pauli associated with the Pauli σ_A is the sum of all the terms in S_A given explicitly by $\widetilde{\sigma}_A = \sum_{\tau \in S_A} \tau$.

Eq. (1) provides an upper bound on the trace norm of the difference between two encrypted inputs to our scheme, given by $\widetilde{\rho}$ and $\widetilde{\rho}'$ respectively. Here $\widetilde{\rho}$ and $\widetilde{\rho}'$ are uniform mixtures of all column permutations of the unencrypted input ρ and ρ' respectively, where

$$\widetilde{\rho} = \frac{1}{(2n)!} \sum_{\pi \in S_{2n}} P_\pi \rho P_\pi^\dagger, \quad \widetilde{\rho}' = \frac{1}{(2n)!} \sum_{\pi \in S_{2n}} P_\pi \rho' P_\pi^\dagger. \tag{A3}$$

The matrix $\widetilde{\rho} - \widetilde{\rho}'$ admits the spectral decomposition

$$\widetilde{\rho} - \widetilde{\rho}' = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|, \tag{A4}$$

where $\{|\psi_i\rangle\}$ is an eigenbasis of $\widetilde{\rho} - \widetilde{\rho}'$. Now let $M = \sum_i \mathrm{sgn}(\lambda_i) |\psi_i\rangle \langle \psi_i|$, where $\mathrm{sgn}(x) = 1$ if $x \geq 0$ and $\mathrm{sgn}(x) = -1$ if $x < 0$. From the definition of the trace norm, we have $\|\widetilde{\rho} - \widetilde{\rho}'\|_{\mathrm{tr}} = \mathrm{Tr}\left(M(\widetilde{\rho} - \widetilde{\rho}') \right)$ because

$$\begin{aligned} \|\widetilde{\rho} - \widetilde{\rho}'\|_{\mathrm{tr}} &= \mathrm{Tr}\, |\widetilde{\rho} - \widetilde{\rho}'| \\ &= \mathrm{Tr}\left(\sqrt{(\widetilde{\rho} - \widetilde{\rho}')^2} \right) \\ &= \sum_i |\lambda_i| \\ &= \sum_i \mathrm{sgn}(\lambda_i)\lambda_i \\ &= \mathrm{Tr}\left(M(\widetilde{\rho} - \widetilde{\rho}') \right). \end{aligned} \tag{A5}$$

The trace norm is non-negative, and hence equal to its absolute value. Thus,

$$\|\widetilde{\rho} - \widetilde{\rho}'\|_{\mathrm{tr}} = \left| \mathrm{Tr}\left(M(\widetilde{\rho} - \widetilde{\rho}') \right) \right|, \tag{A6}$$

and using the cyclic property of the trace, we get

$$\|\widetilde{\rho} - \widetilde{\rho}'\|_{\mathrm{tr}} = \left| \mathrm{Tr}\left(\widetilde{M}(\rho - \rho') \right) \right|, \tag{A7}$$

where

$$\widetilde{M} = \frac{1}{(2n)!} \sum_{\pi \in S_{2n}} P_\pi M P_\pi^\dagger. \tag{A8}$$

The decomposition of $\widetilde{M}$ into the symmetrized Paulis and the decomposition of the traceless quantity $\rho - \rho'$ into the usual Paulis can be subsituted into Eq. (A7) to yield

$$\|\widetilde{\rho} - \widetilde{\rho}'\|_{\mathrm{tr}} = \left| \mathrm{Tr}\left(\sum_{A \in S} a_A \widetilde{\sigma}_A \sum_{\mathbf{v} \in \Omega} \frac{r_\mathbf{v} - r'_\mathbf{v}}{2^{2np}} \sigma_{\varphi(\mathbf{v})} \right) \right|. \tag{A9}$$

Recall that Ω is the set of all non-zero column vectors of length p with components from the set $\{0, 1, 2, 3\}$, and for every $\mathbf{v} \in \Omega$, $\varphi(\mathbf{v})$ is a matrix with $2n$ columns where the first n columns are identical to $\mathbf{v}$ and the remaining n columns are zero vectors. Using the orthogonality of the Paulis on Eq. (A9) yields

$$\begin{aligned} \|\widetilde{\rho} - \widetilde{\rho}'\|_{\mathrm{tr}} &= \left| \mathrm{Tr}\left(\sum_{\mathbf{v} \in \Omega} a_{\varphi(\mathbf{v})} \frac{r_\mathbf{v} - r'_\mathbf{v}}{2^{2np}} \sigma_{\varphi(\mathbf{v})}^2 \right) \right| \\ &= \left| \sum_{\mathbf{v} \in \Omega} a_{\varphi(\mathbf{v})} (r_\mathbf{v} - r'_\mathbf{v}) \right|. \end{aligned} \tag{A10}$$

Applying the Cauchy-Schwarz inequality on the above yields

$$\|\widetilde{\rho} - \widetilde{\rho}'\|_{\mathrm{tr}} \leq \sqrt{\sum_{\mathbf{v} \in \mathbf{\Omega}} a_{\varphi(\mathbf{v})}^2} \sqrt{\sum_{\mathbf{v} \in \mathbf{\Omega}} (r_\mathbf{v} - r'_\mathbf{v})^2}. \tag{A11}$$

Now define the input states on only the first column of qubits to be

$$\tau = \frac{I^{\otimes p} + \sum_{\mathbf{v} \in \Omega} r_\mathbf{v} \sigma_\mathbf{v}}{2^p}, \quad \tau' = \frac{I^{\otimes p} + \sum_{\mathbf{v} \in \Omega} r'_\mathbf{v} \sigma_\mathbf{v}}{2^p}. \tag{A12}$$

The maximum eigenvalue of each of these states is 2^{-h}, where h is their min-entropies. We can use these states to obtain an upper bound on $\sum_{\mathbf{v} \in \mathbf{\Omega}} (r_\mathbf{v} - r'_\mathbf{v})^2$. Note that

$$\mathrm{Tr}((\tau - \tau')^2) \leq \|\tau - \tau'\|_{\mathrm{tr}} \|\tau - \tau'\|_\infty, \tag{A13}$$

where $\|\tau - \tau'\|_\infty$ denotes the ∞-norm on the eigenvalues of $\tau - \tau'$. Since $\|\tau - \tau'\|_{\mathrm{tr}} \leq \|\tau\|_{\mathrm{tr}} + \|\tau'\|_{\mathrm{tr}} \leq 1 + 1 = 2$ and $\|\tau - \tau'\|_\infty \leq \|\tau\|_\infty + \|\tau'\|_\infty = 2^{-h} + 2^{-h} = 2^{-h+1}$, we get

$$\mathrm{Tr}((\tau - \tau')^2) \leq 2^{-h+2}. \tag{A14}$$

Note also that by the orthogonality of the Pauli operators,

$$
\begin{aligned}
\mathrm{Tr}((\tau - \tau')^2) &= \mathrm{Tr}\left(\left(\sum_{\mathbf{v}\in\Omega}(r_{\mathbf{v}} - r'_{\mathbf{v}})2^{-p}\sigma_{\mathbf{v}}\right)\right.\\
&\left.\times\left(\sum_{\mathbf{w}\in\Omega}(r_{\mathbf{w}} - r'_{\mathbf{w}})2^{-p}\sigma_{\mathbf{w}}\right)\right)\\
&= \mathrm{Tr}\left(\sum_{\mathbf{v}\in\Omega}(r_{\mathbf{v}} - r'_{\mathbf{v}})^2 2^{-2p}\sigma_{\mathbf{v}}^2\right)\\
&= \sum_{\mathbf{v}\in\Omega}(r_{\mathbf{v}} - r'_{\mathbf{v}})^2 2^{-p}.
\end{aligned}
\tag{A15}
$$

Hence

$$
\sqrt{\sum_{\mathbf{v}\in\boldsymbol{\Omega}}(r_{\mathbf{v}} - r'_{\mathbf{v}})^2} \le 2\sqrt{2^{p-h}}.
\tag{A16}
$$

To obtain an upper bound for $\sqrt{\sum_{\mathbf{v}\in\Omega} a_{\varphi(\mathbf{v})}^2}$, we obtain upper and lower bounds on $\mathrm{Tr}\left(\widetilde{M}^2\right)$. Now we obtain an upper bound for $\mathrm{Tr}\left(\widetilde{M}^2\right)$. By Hölder's inequality, $\mathrm{Tr}\left(\widetilde{M}^2\right) \le \|\widetilde{M}\|_{\mathrm{tr}}\|\widetilde{M}\|_{\infty}$. Convexity of the norms then implies that

$$
\mathrm{Tr}\left(\widetilde{M}^2\right) \le \|M\|_{\mathrm{tr}}\|M\|_{\infty} = 2^{2np}.
\tag{A17}
$$

The lower bound on $\mathrm{Tr}\left(\widetilde{M}^2\right)$ requires us to expand $\widetilde{M}$ in terms of the symmetrized Paulis. Then

$$
\mathrm{Tr}\left(\widetilde{M}^2\right) = \mathrm{Tr}\left(\sum_{A,A'\in S} a_A a_{A'} \tilde{\sigma}_A \tilde{\sigma}_{A'}\right).
\tag{A18}
$$

By the orthogonality of the symmetrized Paulis and linearity of the trace, we get

$$
\begin{aligned}
\mathrm{Tr}\left(\widetilde{M}^2\right) &= \mathrm{Tr}\left(\sum_{A\in S} a_A^2(\tilde{\sigma}_A)^2\right)\\
&= \sum_{A\in S} a_A^2\,\mathrm{Tr}\left((\tilde{\sigma}_A)^2\right)\\
&\ge \sum_{\mathbf{v}\in\Omega} a_{\varphi(\mathbf{v})}^2\,\mathrm{Tr}\left((\tilde{\sigma}_{\varphi(\mathbf{v})})^2\right).
\end{aligned}
\tag{A19}
$$

Now $\tilde{\sigma}_{\varphi(\mathbf{v})}$ is the sum of $\binom{2n}{n}$ Pauli operators, because there are $\binom{2n}{n}$ ways to permute the $2n$ columns of a matrix with n identical columns and n columns of zeros. Thus $\mathrm{Tr}\left(\tilde{\sigma}_{\varphi(\mathbf{v})}^2\right) = \binom{2n}{n}2^{np}$, and

$$
\mathrm{Tr}\left(\widetilde{M}^2\right) \ge \sum_{\mathbf{v}\in\Omega} a_{\varphi(\mathbf{v})}^2 \binom{2n}{n} 2^{2np}.
\tag{A20}
$$

Eqs. (A17) and (A20) together imply that

$$
\sqrt{\sum_{\mathbf{v}\in\Omega} a_{\varphi(\mathbf{v})}^2} \le \binom{2n}{n}^{-1/2}.
\tag{A21}
$$

Hence

$$
\|\tilde{\rho} - \tilde{\rho}'\|_{\mathrm{tr}} \le 2\sqrt{2^{p-h}}\binom{2n}{n}^{-1/2}.
\tag{A22}
$$

The trace distance between two states is half of the trace norm of the difference between the two states, and hence $\epsilon \le \sqrt{2^{p-h}}\binom{2n}{n}^{-1/2}$.