Randomly Rotate Qubits Compute and Reverse

IT-Secure Non-Interactive Fully-Compact Homomorphic Quantum Computations over Classical Data Using Random Bases

Dor Bitan* and Shlomi Dolev†

* Dept. of Mathematics, Ben-Gurion University of the Negev, Beer-Sheva, Israel
† Dept. of Computer Science, Ben-Gurion University of the Negev, Israel, Beer-Sheva, Israel

Abstract

Homomorphic encryption (HE) schemes enable processing of encrypted data and may be used by a user to outsource storage and computations to an untrusted server. A plethora of HE schemes has been suggested in the past four decades, based on various assumptions, and which achieve different attributes. In this work, we assume that the user and server are quantum computers, and look for HE schemes of classical data. We set a high bar of requirements and ask what can be achieved under these requirements. Namely, we look for HE schemes which are efficient, information-theoretically (IT) secure, perfectly correct, and which support homomorphic operations in a fully-compact and non-interactive way. Fully-compact means that decryption costs $\mathcal{O}(1)$ time and space. To the best of our knowledge, there is no known scheme which fulfills all the above requirements. We suggest an encryption scheme based on random bases and discuss the homomorphic properties of that scheme. We demonstrate the usefulness of random bases in an efficient and secure QKD protocol and other applications. In particular, our QKD scheme has safer security in the face of weak measurements.

Keywords: Homomorphic encryption, Quantum computing, Information-theoretic security

I. Introduction

Delegation of computation, while preserving the confidentiality of the data (and sometimes even the program), is a challenging practical task which has kept researches busy ever since it was brought up in 1978 by Rivest, Adelman, and Dertouzos [RAD78]. That problem addresses scenarios similar to the following. A user is holding information in the form of a string x. The user wishes to use the services of a remote server, which will be referred to as *the cloud*, to store x and perform computations over the stored data using computing engines provided by the cloud. Assume that x is confidential, and hence, the user does not want to share x with the cloud infrastructure enterprises. For example, the user may be a financial company and x some information regarding the financial activity of the company. The company wishes to use the services of a distrustful cloud to store the data and perform computations over the data.

In particular, there can be much use in information-theoretically secure (IT-secure) schemes that would enable such a delegation of data and computations. The security of computationally secure schemes is based on (a) unproven assumptions regarding the computational hardness of specific mathematical problems, and (b) the assumption that the computing power of the adversary is insufficient for solving instances of these assumed-to-be-hard mathematical problems. The security of IT-secure schemes is free of such assumptions and is derived from information theory.

Existing solutions to the problem of delegation of computation are based on either the distributed approach of secure multi-party computation (MPC, see [CDN15]) or the single-server approach of homomorphic encryption (HE, see [AAUC18]). MPC-oriented solutions often achieve IT-security, but to support processing of *any* function over the encrypted data they require ongoing communication between the servers among whom the ciphertext is distributed. HE-oriented solutions typically require no communication, but to maintain IT-security, they can support processing of only a limited set of functions over the encrypted data. Fully homomorphic encryption (FHE) schemes, which may support processing of *any* function over the encrypted data, can only achieve computational security.

HE schemes may be described by a collection of four algorithms. We denote by $\mathcal{K}, \mathcal{M}$, and $\mathcal{C}$ the *key space*, the *message space* and the *ciphertext space* of a given scheme, respectively. The algorithms are as follows.

- `Gen` – A key generation algorithm which, given a security parameter input, n, outputs a key, $k \in \mathcal{K}$.
- `Enc` – An encryption algorithm which, given a plaintext input, $x \in \mathcal{M}$, and a key, k, outputs a ciphertext $c \in \mathcal{C}$. We will write $c = \texttt{Enc}_k(x)$ to emphasize that the encryption depends on k.
- `Eval` – An evaluation algorithm which, given a ciphertext input, $c = \texttt{Enc}_k(x)$, and a function, f, outputs $F(c)$, where $F(c)$ is an encryption of $f(x)$ using the same key. Namely, $F(c) = \texttt{Enc}_k\big(f(x)\big)$.
- `Dec` – A decryption algorithm which, given a ciphertext input, $c = \texttt{Enc}_k(x)$, and a key, k, outputs x.

HE schemes may be classified according to their level of security, complexity, and other attributes. Informally, a scheme is secure if the ciphertext leaks negligible amount of information regarding the plaintext. Security is typically formalized in the IT or computational setting using standard privacy definitions. The collection of functions f, for which `Eval` is defined, may be different for different schemes. If `Eval` is defined for all Boolean functions, then the scheme is fully homomorphic. The first FHE scheme was presented in [Gen09], followed by several revisions and further solutions [VDGHV10], [GHS12], [BP16], [GHS16], [XWZ+18]. If `Dec` is efficient, the scheme is *compact*. If `Dec` requires $\mathcal{O}(1)$ time and space, the scheme is *fully compact*. In some schemes (e.g., most quantum one-time pad based schemes, see below), the evaluation algorithm may output an encryption of the evaluated plaintext that uses a different key. Namely, on input $c = \texttt{Enc}_k(x)$, `Eavl` outputs $F(c) = Enc_{k'}(f(x))$, an encryption of $f(x)$ using a different key, k'. Typically, In such schemes, k' is dependent of f, and decryption of the evaluated ciphertext requires the user to modify her keys according to f. Such schemes cannot achieve full compactness.

Quantum computers threaten the security of computationally secure schemes. If built in-scale, they may allow feasible solutions to problems that are currently considered impractical to solve. For example, Deutsch and Jozsa showed in 1992 that quantum computers could solve certain problems exponentially faster than classical computers [DJ92]. Shor suggested in 1994 algorithms that may be invoked by quantum computers to compute discrete logarithms and factor large integers in polynomial time [Sho94], two problems that are considered computationally hard and stand in the basis of many commonly used computationally secure cryptographic schemes. In 1996, Grover presented a quantum search algorithm that finds a desired record in an N records database in $O(\sqrt{N})$ steps [Gro96]. Bennett and Brassard [BB84] presented a quantum key distribution (QKD) protocol, which enables two distant parties to agree on a random key with IT-security. These are but four well-known algorithms out of numerous results established in the growing field of quantum computation [Jor18].

In light of these results, it is natural to ask if an IT-secure FHE scheme may be achieved using quantum computers. In 2014, it was shown by [YPDF14] that it is impossible to construct an efficient IT-secure quantum FHE (QFHE) scheme. Specifically, the size of the encryption of an IT-secure QFHE scheme must grow exponentially with the input size. The non-existence of efficient IT-secure QFHE may also be deduced from different arguments, as in [ABC$^+$19]. Either way, efficient IT-secure encryption schemes can be used to homomorphically evaluate only a subset of all possible functions. Such schemes are quantum homomorphic encryption (QHE) schemes, e.g., [RFG12], [Lia13], [TKO$^+$16], [OTF18]. Other works use computationally-secure FHE schemes to construct computationally-secure QFHE schemes. E.g., [BJ15], [DSS16], [ADSS17], [Mah18], [Bra18]. Quantum schemes with homomorphic properties are often based on the quantum one-time pad (QOTP) encryption scheme, suggested in [AMTdW00]. There, Pauli gates are randomly applied to the qubits to obtain IT-secure encryption.

Different schemes are based on different assumptions regarding the capabilities of the parties. QHE schemes typically assume that the server has full quantum capabilities. Assumptions regarding the quantum abilities of the user vary on a broad spectrum between a classical user (with no quantum abilities at all) and a fully quantum user. When the user has (at least some) quantum abilities, the information x held by that user may either be classical or quantum (of course, if the user has no quantum abilities, x can only be classical). In this work, we assume that both the user and the server have full quantum abilities. Namely, they both can: (a) generate qubits in the computational basis; (b) manipulate qubits using quantum logic gates; (c) transmit qubits between each other; (d) measure qubits. We assume that the information held by x is classical. The function f that is to be homomorphically evaluated over x may either be a classical or quantum algorithm.

In this work, we look for QHE schemes that enable users to delegate classical data to be stored and processed by a distrustful cloud and have the following properties.

- Efficient.
- IT-secure.
- Fully compact.
- Perfectly correct. I.e., the ciphertext always decrypts to the right plaintext, except for errors that may arise due to the nature of noisy physical implementations of quantum schemes.
- Non-interactive. I.e., no interaction is allowed other than the user sending $c = \mathtt{Enc}_k(x)$ to the server, and the server replying with $F(c) = \mathtt{Enc}_k\big(f(x)\big)$.

We ask which operations may be homomorphically applied to encrypted data under these properties. To the best of our knowledge, there is no known QHE scheme that guarantees all these properties.

Our results. We suggest here a new approach to encrypt and outsource the storage of classical data while enabling IT-secure quantum gate computations over the encrypted data. Our method is based on using a specific family of random bases to encrypt classical bits. Our schemes support fully-compact IT-secure homomorphic evaluation of NOT and Hadamard gates, and also $CNOT$ gates, where the control qubits are set in none-random basis. The latter implies that cascading is possible only in specific yet important cases. We detail applications of our constructions, including random basis QKD, coalitions-resilient secure multi-party XOR computation, and secure quantum pseudo-telepathy scheme. We note that, while some of these applications may also be constructed using other existing QHE schemes, our schemes support these applications while maintaining IT-security, full compactness, perfect correctness, and non-interactively. In particular, we believe that our random basis QKD scheme has many important practical use cases. All our schemes, based on adding extra randomness, have safer security implications in the face of weak measurements.

Related work. Broadbent suggested in [Bro15] a client-server scheme based on combining the QOTP encryption scheme with a computationally secure classical FHE scheme. Their scheme enables delegation of quantum information to a quantum server and homomorphic processing of a universal set of quantum gates over the encrypted data. However, their scheme falls short of achieving the properties listed above. First, their scheme employs a computationally-secure FHE protocol, which makes their scheme only computationally secure (as mentioned, we are interested in IT-secure schemes). Second, their scheme requires quantum and classical interaction between the user and the server for the processing of non-Clifford gates (the scope of this work is constructing non-interactive schemes). Third, their scheme is not fully compact, as it requires the user to update the keys used to encrypt the data throughout the computation. Namely, to homomorphically evaluate a quantum circuit over encrypted data, the client should re-adjust her knowledge of the encryption keys on each relevant quantum wire after each gate processing. That re-adjustment requires $\mathcal{O}(s)$ work, where s is the size of the circuit. As mentioned, in this work we look for fully-compact schemes — schemes in which the complexity of `Dec` is $\mathcal{O}(1)$.

An approach similar to [Bro15] was adopted by [BJ15]. There, two schemes were proposed. The first has a decryption procedure whose complexity scales with the square of the number of T-gates and hence falls short of achieving full compactness. The second scheme uses a quantum evaluation key of length given by a polynomial of degree exponential in the circuit's T-gate depth, yielding a homomorphic scheme only for quantum circuits with constant T-depth. The evaluation key includes auxiliary qubits that encode the required corrections that should be performed over the processed data. Since a large number of possible corrections must be available, the length of the evaluation key is exponential in the circuit's T-gate depth, yielding a homomorphic scheme that is efficient only for quantum circuits with constant T-depth. Both the schemes of [Bro15] and [BJ15] are only computationally secure.

Dulek et al. [DSS16] built on the framework of [BJ15] and used a classical FHE scheme to construct quantum gadgets that allow perfect correction of the errors that occur during the homomorphic evaluation of T-gates on encrypted quantum data. These gadgets give rise to an efficient non-interactive QFHE scheme. Their scheme is compact, but not fully compact, since decryption requires the user to apply classical changes to the keys according to f. Furthermore, it is only computationally secure.

Mahadev presented in [Mah18] a non-interactive FHE scheme for quantum circuits that uses classical keys. The scheme allows a classical user to delegate quantum computations to a quantum server, while the server is unable to learn any information about the computation. Their scheme is based on QOTP, is only computationally secure, and is not perfectly correct as it has positive error probability.

Brakerski [Bra18] used the high-level outline of [Mah18] to construct a computationally secure QFHE scheme which enables homomorphic evaluation of classical circuits with bounded depth over classical

data and with improved correctness. To support unbounded depth, they further rely on a circular security assumption.

Childs [Chi05] discussed ways in which a powerful quantum server may assist a user in performing operations while preserving the confidentiality of the data. In their work, the user is assumed to have capabilities significantly inferior to those of the server. In particular, the user is only allowed to generate qubits in the $|0\rangle$ state, store qubits, perform swap and Pauli gates, and perform no measurements. Under these considerations, they suggest a (QOTP based) way in which the server may perform measurements on encrypted data. They also suggest algorithms which enable the server to help the user in performing a universal set of quantum gates over encrypted data, but these algorithms are neither compact nor non-interactive — they require the user to perform at least as many operations as the server for each gate, and some of them require rounds of client-server interaction. In particular, they suggest a non-compact way of performing Hadamard gates over the encrypted qubits, while we suggest here a fully compact, efficient, non-interactive, IT-secure and perfectly correct way of homomorphically applying Hadamard gates to encrypted qubits.

Rhode et al. presented in [RFG12] a protocol that enables a quantum user to manipulate client data in two models of restricted quantum computation — the boson sampling and quantum walk models. Their protocol is non-interactive, fully compact, and assumes no computational hardness assumptions and no limitations on the computing power of the adversary. However, in their scheme, the same key is used for encoding each of the input qubits, and hence, their scheme withstands no standard cryptographic criterion of security. Tan et al. [TKO$^+$16] improved on [RFG12] and presented a protocol that supports a class of quantum computations, including and beyond boson sampling, with improved security (under similar assumptions). However, they achieve no standard criterion of IT-security, as they only bound the amount of information accessible to an adversary.

Ouyang, Tan, and Fitzsimons [OTF18] took a different approach and further improved on the results of [TKO$^+$16]. Built on constructions taken from quantum codes, they achieved an encryption scheme that supports evaluation of circuits with a constant number of non-Clifford gates. Though achieving stronger security guarantees than [RFG12], [TKO$^+$16], their scheme withstands no standard cryptographic criterion of security. Furthermore, their scheme is neither perfectly correct nor fully compact. It suggests a tradeoff between the size of the encoding and the success probability, where achieving constant success probability costs in increasing the size of the encoding exponentially with the total number of T gates.

[Lia13] constructed a QOTP-based quantum encryption scheme which, given the encryption key, permits any unitary transformation to be evaluated on an arbitrary encrypted n-qubit state. Their scheme is efficient, compact, and IT-secure against an eavesdropper who may intercept an encrypted message (before or after evaluation). However, their scheme suggests no solution to the main problem discussed in this paper, as their evaluation algorithm is dependent on the key. Under such restriction, the server must hold the key to compute on the encrypted data. Given the key, the server may decrypt and read the message, which by no means provides the user with any level of privacy. They also constructed a scheme in which the evaluation algorithm is independent of the key, but it only supports trivial operations that are independent of the key.

Paper organization. In Section II, we present our random basis encryption scheme. In Section III, we discuss the homomorphic properties of our scheme. Several applications are discussed in Section IV. Section V concludes the work. Relevant background on quantum computation, notations, some of the proofs, and one application may be found in the Appendix.

II. The Random Basis Encryption Scheme

We begin with some intuition. Our main intention is encrypting the classical bits 0 and 1 while enabling some operations to be performed homomorphically over the ciphertext. Typically, these bits are encoded in quantum computation as the elements $|0\rangle$ and $|1\rangle$ of the standard basis of $\mathbb{H} = \mathbb{C}^2$. Of course, that encoding is by no means an encryption of the bits. Approaching proper encryption, we take some random $(\theta, \varphi) \in [0, 2\pi]^2$, set $|\psi_0\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix}$, and think of $|\psi_0\rangle$ as an encryption of $|0\rangle$ using (θ, φ) as the encryption key. The plaintext qubits $|0\rangle$ and $|1\rangle$ are orthogonal. To maintain orthogonality of the ciphertext, we set $|\psi_1\rangle = \begin{pmatrix} \sin(\theta/2) \\ -e^{i\varphi}\cos(\theta/2) \end{pmatrix}$ to be the encryption of $|1\rangle$ using the same key. One may readily verify that $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal. For random $(\theta, \varphi) \in [0, 2\pi]^2$, the elements $|\psi_0\rangle$ and $|\psi_1\rangle$ constitute a random orthonormal basis of $\mathbb{H}$, denoted $B_{(\theta,\varphi)}$. Now, as mentioned, we want that encryption to support some homomorphic operations in a fully-compact non-interactive IT-secure way. First, we require supporting homomorphic NOT gates. We want $|\psi_0\rangle$ to be equal (up to a global phase factor) to $NOT\,|\psi_1\rangle$ (and vice versa). This requirement compels $\varphi = \pm\pi/2$. Hence, for $(\theta, \varphi) \in [0, 2\pi] \times \{\pm\frac{\pi}{2}\}$, the random basis $B_{(\theta,\varphi)}$ is NOT-invariant.

The discussion above, and the inability of determining the coordinates of an arbitrary qubit, given a realization of it, give rise to the following QHE scheme of classical data, which allows a user to outsource the storage of confidential information to an untrusted server. We now present the algorithms `Gen`, `Enc`, and `Dec`. In the next section, we construct `Eval`, and detail operations which may be homomorphically applied to the ciphertext in a fully-compact and non-interactive way.

The Random Basis Encryption scheme

`Gen` **(key generation):** Output a uniformly random pair (θ, φ) from $[0, 2\pi] \times \{\frac{\pi}{2}, -\frac{\pi}{2}\}$.

`Enc` **(encryption):** On input message $b \in \mathcal{M}$ and a key $k = (\theta, \varphi)$:

- Generate the qubit $|b\rangle$.
- Let $K = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ e^{i\varphi}\sin(\theta/2) & -e^{i\varphi}\cos(\theta/2) \end{pmatrix} \in M_2(\mathbb{C})$ and apply K to $|b\rangle$ to obtain $|q\rangle = K\,|b\rangle$.
- Output $|q\rangle$.

`Dec` **(decryption):** On input ciphertext $|\psi\rangle$ and a key $k = (\theta, \varphi)$:

- Let $K^\dagger$ denote the conjugate transpose of K, where K is as in `Enc` and apply $K^\dagger$ to $|\psi\rangle$.
- Measure $K^\dagger\,|\psi\rangle$ in reference to the computational basis.
- Output the outcome of the measurement.

The matrix K defined in the scheme is the unitary matrix whose columns are the elements of $B_{(\theta,\varphi)}$. Multiplying the elements of the computational basis, $\{|0\rangle, |1\rangle\}$, by K, we obtain the elements of $B_{(\theta,\varphi)}$. We refer to the encryption algorithm as taking the elements of the computational basis to the elements of the random basis $B_{(\theta,\varphi)}$. Since K is a unitary transformation, $K^\dagger$ is its inverse, and hence, given (θ, φ), the decryption algorithm takes the elements of $B_{(\theta,\varphi)}$ to the elements of the computational basis. Of course, the scheme may be applied bit-wise to a string x of classical bits to enable outsourcing the storage of x to an untrusted quantum server. The scheme is perfectly correct. Indeed, assume that $|q\rangle$ is the encryption of $b \in \{0, 1\}$ using (θ, φ). By `Enc`, $|q\rangle = K\,|b\rangle$. In `Dec`, $K^\dagger$ is applied to $|q\rangle$. One has $K^\dagger\,|q\rangle = K^\dagger K\,|b\rangle = |b\rangle$. Since $|b\rangle$ is a pure state, measuring it in reference to the computational basis, we get b with probability 1. In the appendix, we prove that the scheme is IT-secure. In `Gen`, the key is chosen from an infinite set. Implementing this might be challenging. Remark 1 below discusses how $\mathcal{K}$ may be made discrete and the security consequences of this procedure.

III. Quantum Gate Computations

We now explore the consequences of homomorphically applying quantum gates to the ciphertext by the distrustful quantum server. Obviously, any gate that commutes with the family of the encryption gates K, may be homomorphically applied to the encrypted data. Several unitary operations are typically used in quantum computing. We now investigate the consequences of applying some of these typically-used quantum gates to a random basis $B_{(\theta,\varphi)}$ encryption of classical data.

The NOT gate. The NOT gate is the unitary transformation that interchanges the elements of the computational basis: $|b\rangle \to |1-b\rangle$. The matrix representation of NOT in the computational basis is $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. What happens when one applies an X gate to an element of a random basis $B_{(\theta,\varphi)}$? A simple calculation will show that, applying an X gate to an element of $B_{(\theta,\varphi)}$ we get the other element of that basis, up to a global phase factor. Since $e^{i\varphi} = \pm i$, we have

$$X|\psi_0\rangle = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} \cos(\theta/2) \\ \pm i\sin(\theta/2) \end{smallmatrix}\right) = \left(\begin{smallmatrix} \pm i\sin(\theta/2) \\ \cos(\theta/2) \end{smallmatrix}\right) = \pm i\left(\begin{smallmatrix} \sin(\theta/2) \\ \mp i\cos(\theta/2) \end{smallmatrix}\right) = \pm i\,|\psi_1\rangle\,.$$

Similarly, $X|\psi_1\rangle = \mp|\psi_0\rangle$. To conclude, applying a NOT gate to elements of $B_{(\theta,\varphi)}$ we get the same effect as when applying it to an element of the computational basis. Consequently, X gates may be homomorphically applied to encrypted data.

The $CNOT$ gate. The $CNOT$ gate is a two-qubit gate, whose matrix representation in the computational basis of $\mathbb{H}^{\otimes 2}$ is

$$\left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right).$$

Tensor products of the elements of the computational basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{H}$, give the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ of $\mathbb{H}^{\otimes 2}$. Applying the $CNOT$ gate to the elements of the latter basis, we leave $|00\rangle$ and $|01\rangle$ unchanged, and interchange $|10\rangle$ and $|11\rangle$. In other words, if the first qubit is $|0\rangle$, then the second qubit is left unchanged, and if the first qubit is $|1\rangle$, then a NOT gate is applied to the second qubit. For this reason, this gate is called *the controlled-NOT gate*. The first qubit is *the control qubit* and the second is *the target qubit*.

What happens if one applies a $CNOT$ gate to the elements of a random basis of $\mathbb{H}^{\otimes 2}$? Namely, let $B_{(\theta,\varphi)} = \{|\psi_0\rangle, |\psi_1\rangle\}$ and $B_{(\theta',\varphi')} = \{|\psi'_0\rangle, |\psi'_1\rangle\}$ two orthonormal bases of H. Tensor products of the elements of $B_{(\theta,\varphi)}$ and $B_{(\theta',\varphi')}$ give the following orthonormal basis of $\mathbb{H}^{\otimes 2}$:

$$\{|\psi_0\psi'_0\rangle, |\psi_0\psi'_1\rangle, |\psi_1\psi'_0\rangle, |\psi_1\psi'_1\rangle\}.$$

Is the *control-target structure* kept when applying $CNOT$ to the elements of that basis, leaving $|\psi_0\psi'_0\rangle$ and $|\psi_0\psi'_1\rangle$ unchanged, and interchanging $|\psi_1\psi'_0\rangle$ and $|\psi_1\psi'_1\rangle$? The answer turns out to be negative. Applying a $CNOT$ gate to these elements, we take each of them to a superposition of the others.

Can we find a quantum gate (using ancillary qubits, perhaps) that keeps the control-target structure when applied to the elements of a random basis of $\mathbb{H}^{\otimes 2}$? Again, the answer is negative. For example, if such a gate P exists, it must leave $|\psi_0\psi_0\rangle$ unchanged and take $|\psi_1\psi_1\rangle$ to $|\psi_1\psi_0\rangle$, regardless of θ and φ. Taking $\theta' = \pi - \theta$ and $\varphi' = \pi - \varphi$, we switch between $|\psi_0\rangle$ and $|\psi_1\rangle$, implying a contradiction when examining P's operation on $|\psi_0\psi_0\rangle$ and $|\psi_1\psi_1\rangle$. For example, consider the following two cases. First, if $\theta = 0$ and $\varphi = \pi$, we have $|\psi_0\rangle = |0\rangle$ and $|\psi_1\rangle = |1\rangle$. Second, if $\theta = \pi$ and $\varphi = 0$, we have $|\psi_0\rangle = |1\rangle$ and $|\psi_1\rangle = |0\rangle$. In the first case, $P|\psi_0\psi_0\rangle = P|00\rangle$ and $P|\psi_1\psi_1\rangle = P|11\rangle$, implying that $|00\rangle$ is unchanged by P and $|11\rangle$ is taken to $|10\rangle$. On the other hand, in the second case, $P|\psi_0\psi_0\rangle = P|11\rangle$ and $P|\psi_1\psi_1\rangle = P|00\rangle$, implying that $|11\rangle$ is unchanged and $|00\rangle$ is taken to $|01\rangle$. By the first case, $|00\rangle$ is unchanged, but by the second case, it is taken to $|01\rangle$. The contradiction shows that such a P cannot exist.

Nevertheless, by applying a $CNOT$ gate to the elements of a *partially-random* basis $\{|0\rangle, |1\rangle\} \otimes B_{(\theta,\varphi)}$ of $\mathbb{H}^{\otimes 2}$ we do keep the target-control structure. The elements of such a basis are

$$|0\psi_0\rangle = \begin{pmatrix} \cos(\theta/2) \\ \pm i\sin(\theta/2) \\ 0 \\ 0 \end{pmatrix}, |0\psi_1\rangle = \begin{pmatrix} \sin(\theta/2) \\ \mp i\cos(\theta/2) \\ 0 \\ 0 \end{pmatrix}, |1\psi_0\rangle = \begin{pmatrix} 0 \\ 0 \\ \cos(\theta/2) \\ \pm i\sin(\theta/2) \end{pmatrix}, |1\psi_1\rangle = \begin{pmatrix} 0 \\ 0 \\ \sin(\theta/2) \\ \mp i\cos(\theta/2) \end{pmatrix}.$$

Applying a $CNOT$ gate to these elements, we leave $|0\psi_b\rangle$ unchanged and interchange $|1\psi_b\rangle$ and $|1\psi_{1-b}\rangle$, up to a global phase factor. In fact,

$$CNOT\,|1\psi_0\rangle = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \cos(\theta/2) \\ \pm i\sin(\theta/2) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \pm i\sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix} = \pm i \begin{pmatrix} 0 \\ 0 \\ \sin(\theta/2) \\ \mp i\cos(\theta/2) \end{pmatrix} = \pm i\,|1\psi_1\rangle\,, \qquad (1)$$

and a similar computation shows that $CNOT\,|1\psi_1\rangle = \mp i\,|1\psi_0\rangle$. Since the last two entries of $|0\psi_b\rangle$ are zero, applying a $CNOT$ gate we leave them unchanged. To conclude, $CNOT$ gates may be homomorphically applied to systems of two qubits when the control qubit is an element of the computational basis and the target qubit is an element of $B_{(\theta,\varphi)}$.

C^nNOT gates. For a positive integer n, the C^nNOT gate is an $n+1$ qubit gate, whose matrix representation in the computational basis of $\mathbb{H}^{\otimes(n+1)}$ is the matrix obtained from the identity matrix of order 2^{n+1} by replacing its bottom right block $\left(\begin{smallmatrix} 1&0 \\ 0&1 \end{smallmatrix}\right)$ with the block $\left(\begin{smallmatrix} 0&1 \\ 1&0 \end{smallmatrix}\right)$. Namely, the NOT and $CNOT$ gates discussed above are the special cases $n=0$ and $n=1$, respectively, of C^nNOT. Similarly to (1), one may readily verify that, given a random basis $B_{(\theta,\varphi)}$,

$$C^nNOT\,|b_1b_2\ldots b_n\psi_b\rangle = \begin{cases} |b_1b_2\ldots b_n\psi_{1-b}\rangle\,, & \prod_{i=1}^n b_i = 1, \\ |b_1b_2\ldots b_n\psi_b\rangle\,, & \text{otherwise.} \end{cases} \qquad (2)$$

Hence, C^nNOT gates may be homomorphically applied to systems of qubits when the control qubits are elements of the computational basis and the target qubit is an element of $B_{(\theta,\varphi)}$.

The Hadamard gate. The Hadamard gate is the unitary transformation, whose matrix representation in the computational basis is $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1&1 \\ 1&-1 \end{smallmatrix}\right)$. H takes the elements of the computational basis to the elements of $B_{(\frac{\pi}{4},0)} = \left\{\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right), \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)\right\}$. When measuring any of the elements of $B_{(\frac{\pi}{4},0)}$ in reference to the computational basis, the probabilities of obtaining zero or one are both $\frac{1}{2}$. What happens when one applies H to an element of a random basis $B_{(\theta,\varphi)}$? Explicitly, what are the probabilities of obtaining zero or one when measuring an element of $H\left[B_{(\theta,\varphi)}\right]$ in reference to $B_{(\theta,\varphi)}$? By Equation (5) (in the appendix), the probability of obtaining zero when measuring $H\,|\psi_0\rangle$ in reference to $B_{(\theta,\varphi)}$ is the square of the absolute value of the inner product of $H\,|\psi_0\rangle$ and $|\psi_0\rangle$. Since

$$H\,|\psi_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1&1 \\ 1&-1 \end{pmatrix}\begin{pmatrix} \cos(\theta/2) \\ \pm i\sin(\theta/2) \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \cos(\theta/2)\pm i\sin(\theta/2) \\ \cos(\theta/2)\mp i\sin(\theta/2) \end{pmatrix}, \qquad (3)$$

the inner product is $\langle\psi_0|H|\psi_0\rangle = \frac{\cos\theta}{\sqrt{2}}$. Taking the square of the result, one finds that the probability of obtaining a zero outcome when measuring $H\,|\psi_0\rangle$ in reference to $B_{(\theta,\varphi)}$, is $\frac{\cos^2\theta}{2}$. Since the probabilities add up to one, when measuring $H\,|\psi_0\rangle$ in reference to $B_{(\theta,\varphi)}$ the outcome one is obtained with probability $\frac{1+\sin^2\theta}{2}$. Similar computations yield similar results for $|\psi_1\rangle$. Explicitly, when measuring $H\,|\psi_1\rangle$ in reference to $B_{(\theta,\varphi)}$, the probability of obtaining the outcome one is $\frac{\cos^2\theta}{2}$ and the probability of obtaining the outcome zero is $\frac{1+\sin^2\theta}{2}$. To conclude, applying a Hadamard gate to an element of a random basis, the probabilities of the elements of the basis in the superposition we get are in general not $\frac{1}{2}$ each.

These results are rather unfortunate since they imply that the Hadamard gate does not create an equally weighted superposition when applied to an element of a random basis, and hence cannot be applied to the encrypted data homomorphically. Is there a quantum gate that takes elements of every $B_{(\theta,\varphi)}$ basis to an equally weighted superposition of the elements of that basis? We give a positive answer to that question in the form of the following quantum gate that uses an ancillary $|0\rangle$ qubit:

$$D = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}.$$

D is the matrix representation (in the computational basis) of the quantum gate used in [EPR35] to create *Bell states*. This gate is the two-qubit quantum circuit established by first applying a Hadamard gate to the first qubit, and then a $CNOT$ gate to that system of two qubits, where the first qubit is the control qubit and the second is the target qubit. That circuit is illustrated in Figure 1.

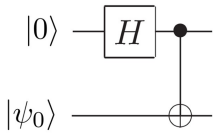

Figure 1: Random Based D gate.

We now prove that, applying a D gate to a tensor product of $|0\rangle$ and an element of a random basis, measuring the second qubit in reference to that same random basis, the probabilities of obtaining the outcomes zero and one are both $\frac{1}{2}$. Explicitly, let $|\psi_b\rangle$ an element of a random basis, $B_{(\theta,\varphi)}$, where $\varphi =$ and $\theta \in [0, 2\pi]$. We have

Lemma 1. *D is a quantum gate which takes tensor products of the form $|0\psi_b\rangle$ to a system of two qubits, such that, measuring that system in reference to $\{|0\rangle, |1\rangle\} \otimes B_{(\theta,\varphi)}$, the probability of each of the outcomes zero and one for the second qubit is $\frac{1}{2}$.*

The proof of Lemma 1 appears in the appendix. To conclude, the D gate may be homomorphically applied to the elements of a random basis, using an ancillary $|0\rangle$ qubit, resulting in the same effect as when applying a Hadamard gate to the elements of the computational basis – creating a superposition of the elements of that basis with equal probabilities. We note that the ancillary qubit may be generated by the server with no interference of or interaction with the user.

IV. Applications

Coalitions-resilient secure multi-party XOR computation. Consider the following scenario. Each of N honest-but-curious participants, $\mathcal{P}_i$, $1 \leq i \leq N$, is holding a bit $b_i \in \{0, 1\}$. The participants are interested in learning the XOR of their bits, $b_1 \oplus \cdots \oplus b_N$, without revealing their own bits. One trivial solution to that problem is as follows (see Figure 2).

- One of the participants, say $\mathcal{P}_1$, picks $b'_0 \in \{0, 1\}$ uniformly at random.
- For $1 \leq i \leq N$: $\mathcal{P}_i$ computes $b'_i := b'_{i-1} \oplus b_i$ and sends the result to the next participant.
- $\mathcal{P}_1$ computes $b'_N \oplus b'_0 (= b_1 \oplus \cdots \oplus b_N)$, and sends the result to the other participants.

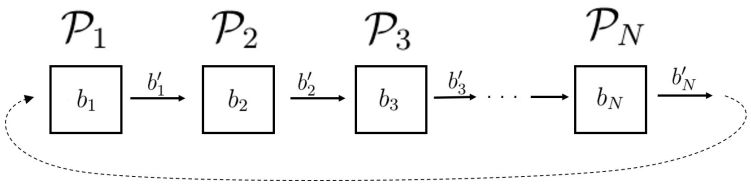

Figure 2: A trivial solution to the multi-party XOR computation problem.

This solution is vulnerable to attacks of coalitions of *honest-but-curious* participants, trying to gain information regarding the bits of other participants. E.g., $\mathcal{P}_{k-1}$ and $\mathcal{P}_{k+1}$ can learn $\mathcal{P}_k$'s bit by computing $b'_{k-1} \oplus b'_k$. More generally, $\mathcal{P}_m$ and $\mathcal{P}_{m+l}$ can learn the XOR of the bits of the participants $\mathcal{P}_{m+1}, \ldots, \mathcal{P}_{m+l-1}$.

One application of our random basis encryption scheme is the following solution to the multi-party XOR computation problem, which is resilient to such attacks of coalitions of honest-but-curious participants. The scheme is illustrated in Figure 3, and its stages are as follows:

- $\mathcal{P}_1$ picks $b \in \{0, 1\}$ uniformly at random and uses the random basis encryption scheme to generate an encryption $|\psi_b\rangle$ of b.
- For $1 \leq i \leq N$:
  - If $b_i = 1$, then $\mathcal{P}_i$ applies a NOT gate to the received qubit.
  - $\mathcal{P}_i$ transmits the qubit to the next participant.
- $\mathcal{P}_1$ decrypts the received qubit to obtain an outcome b'. Computing $b \oplus b'$, she obtains the desired XOR of the bits of all the participants and sends the result to them.

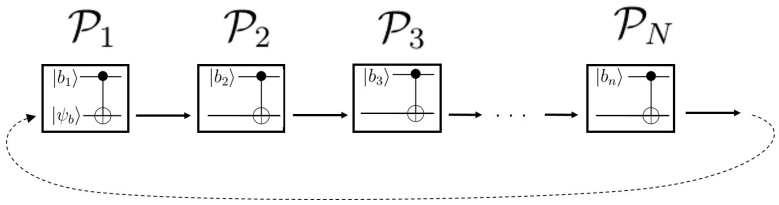

Figure 3: The coalitions-resilient solution to the multi-party XOR computation problem.

At each stage, the qubit received by a participant $\mathcal{P}_i$ is an encryption of a random bit. Since our encryption scheme is IT-secure, measuring that encryption-qubit, $\mathcal{P}_i$ obtains zero and one with equal probabilities, regardless of the actual value of the encrypted bit. Hence, using our IT-secure random basis encryption scheme, coalitions of honest-but-curious participants cannot gain any information regarding the bits of the other participants. In fact, allowing the participants in that coalition to perform measurements is a slight deviation from the definition of being honest-but-curious. Honest-but-curious participants cannot deviate from the protocol, but only attempt to gain further information from the data that they receive during the execution of the protocol. As mentioned above, our scheme remains IT-secure even if we allow that deviation.

In the event that a certain $\mathcal{P}_i$ does deviate from the protocol, and performs a measurement of the qubit, it may yield an erroneous result. Repeated executions of the protocol will reveal that with high probability: If no measurements are performed, the same result will be obtained in all the executions. If measurements are performed, they will produce a random sequence of results that will most probably not be constant.

A Random Basis CNOT Quantum Key Distribution (QKD) scheme. The random basis encryption scheme requires that the participants hold a shared key. Nevertheless, it may also be used to construct a two-stage (random basis) QKD scheme, in which one participant sends to another information in the form of a string of classical bits. That information may be a key, to be used in a symmetric key encryption scheme, or simply plain data. Suppose Alice holds a bit $b \in \{0, 1\}$, and wishes to send it privately to Bob. To this end, Alice and Bob may follow the following single-bit two-stage encryption scheme.

1) Bob randomly picks b' from $\{0, 1\}$, uses the random basis encryption scheme to generate an encryption $|\psi_{b'}\rangle$ of b', and then transmits $|\psi_{b'}\rangle$ to Alice.
2) If $b = 1$ Alice applies a NOT gate to $|\psi_{b'}\rangle$; otherwise, she leaves it unchanged.
3) Alice sends the qubit back to Bob, who decrypts it and obtains a bit, b''.
4) Bob computes $b'' \oplus b'$ to obtain b.

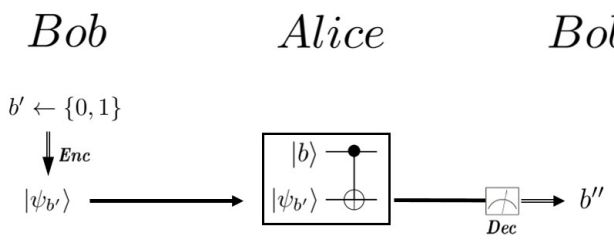

Figure 4: Sharing Key by Random Basis.

The scheme is illustrated in Figure 4. Obviously, it may be applied bit-wise to a sequence of bits of any length.

Security. Since our random basis encryption scheme is IT-secure, the random basis QKD scheme is IT-secure against an adversary that is limited to eavesdropping. However, the scheme is susceptible to man-in-the-middle attacks like the following. An adversary may operate as follows.

1) Intercept the encrypted qubit $|b'\rangle$ sent from Bob to Alice and store it.
2) Generate and send to Alice a falsify $|0\rangle$ qubit (as if it was Bob's qubit).
3) Receive the qubit back from Alice and measure it to obtain b.
4) Apply a NOT gate to Bob's (original) stored qubit, conditioned on b, and send it back to Bob (as if Alice sent it).

This way, the adversary can learn Alice's message without being caught. Our scheme may be made resilient to such attacks by adding a stage in which Alice and Bob communicate over a classical (non-encrypted) channel to expose such adversarial attacks, and prevent the adversary from gaining any valuable information. Explicitly, assume that Alice wishes to use our scheme to send Bob n bits, $b_1 b_2 \dots b_n$. Denote by $|\psi_{b'_i}\rangle$, $1 \leq i \leq n+l$, encryptions of $n+l$ random bits b'_i, generated by Bob using our random basis encryption scheme at stage 1 of the random basis QKD scheme. After Bob transmits these $n+l$ qubits to Alice, and before stage 2, Bob and Alice talk over the telephone. Alice randomly chooses a subset $L \subseteq [n+l]$ of size l and tells L to bob. Bob reveals the keys he used for encrypting the bits b'_j for all $j \in L$. Alice then uses these keys to decrypt the corresponding qubits and tells Bob the results she obtained. If the l bits obtained by Alice differ from Bob's random bits, the parties abort. Otherwise, they continue with stage 2 of the scheme using the n qubits that were not measured.

Weak measurements and comparison with other schemes. An adversary may attempt to gain information regarding the encrypted data following the framework of the *weak measurement model*, suggested by Aharonov et al. [ABP$^+$02] and described in [EC11], [TC13]. Weak measurements enable accumulating information regarding the state of the qubit while not collapsing the state, but only biasing it a little. Weak measurements consist of two stages. First, we weakly interact the subject qubit with an ancillary qubit using a two-qubit gate. Then, we (strongly) measure the ancillary qubit. The outcome of the (strong) measurement of the ancillary qubit is the outcome of the weak measurement of the subject qubit. This process enables imprecisely measuring quantum states, outsmarting the uncertainty principle [EC11]. Our scheme, based on adding extra randomness to the encryption process, has safer security implications against weak measurements.

Bennett and Brassard [BB84] presented the first QKD scheme. In their scheme, Alice sends Bob random bits encoded as qubits in either the computational basis $\{|0\rangle, |1\rangle\}$ or the diagonal basis $\{|+\rangle, |-\rangle\}$. The bit 0 is always encoded by either $|0\rangle$ or $|+\rangle$, and the bit 1 is always encoded by either $|1\rangle$ or $|-\rangle$. An adversary may intercept the qubits sent from Alice to Bob, perform weak measurements over them and accumulate some information regarding their state, and send them to Alice as if they were never intercepted. Such an attack may give the adversary a non-negligible advantage at a reduced risk of being caught. In our QKD scheme, 0 and 1 bits may have the same encoding, and hence, weak measurement attacks give the adversary no advantage. As shown in the security proof of our scheme (Appendix B),

even if the adversary is given all the entries of the density matrix representing the encrypted state, it leaks no information regarding the plaintext. Namely, for every $\rho = \texttt{Enc}_{(\theta,\varphi)}\big(0\big)$, there exist valid θ', φ' such that $\rho = \texttt{Enc}_{(\theta',\varphi')}(1)$. Furthermore, our scheme may be used to transmit not only a random key but any binary message. Hence, our scheme provides a method for Alice and Bob to communicate securely using two rounds of interaction via an authenticated quantum channel.

Kak presented in [Kak06] a protocol which suggests a method for Alice and Bob to communicate securely using three rounds of interaction via an authenticated quantum channel. In Kak's scheme, before the protocol executes, two orthogonal states are set as the encodings of the bits. Then, Alice applies a random rotation A to the encoding of her message b and sends it to Bob. In turn, Bob applies a random rotation B to the bit and sends it back to Alice, which now rotates the qubit in the opposite direction by applying $A^\dagger$ to it. Alice now sends the qubit back to Bob, which applies $B^\dagger$ to it and obtains the encoding of Alice's bit. While Kak's scheme requires three round of interaction, our scheme requires only two rounds. Furthermore, in Kak's scheme, Alice and Bob should agree on an encoding of the bits before the execution of the scheme. In our scheme, no such requirement is presented.

Deng and Long suggested in [DL04] a method for secure communication between Alice and Bob. Similarly to [Bra18], their scheme use qubits only in the computational or diagonal basis, and hence their scheme is vulnerable to weak measurement attacks.

V. Discussion

We have suggested an encryption scheme of classical data using quantum computers, based on a specific family of random bases. We have proved that our scheme is IT-secure, and showed that it allows a user to outsource confidential data to a distrustful quantum server. We have examined the homomorphic properties of our scheme and showed that the NOT gate may be applied homomorphically to the encrypted data. Likewise, any gate that commutes (up to a global phase factor) with the family of unitary matrices K, defined in $\texttt{Enc}$, may be applied homomorphically to the encrypted data. We have constructed a quantum gate that uses an ancillary qubit and allows applying Hadamard gates to encrypted data. We have shown that controlled-NOT gates may be applied to systems of qubits, where the control qubits are plaintext qubits and the target qubits are encrypted using a random basis. Encrypted bits are not used as control qubits in our system since any ordered (orthonormal) basis may be chosen as a key, including pairs of bases composed of the same elements in reversed order. We support these homomorphic operations in an efficient, fully-compact, non-interactive, perfectly correct, and IT-secure way.

We have shown how our scheme may be used to perform multi-party computation of binary XOR in a way that guarantees perfect security even under an attack of coalitions of honest-but curious participants. We demonstrated how our scheme may be used to establish a symmetric key by a two-stage random basis QKD scheme. We have suggested a protocol enabling two distant parties securely obtain an entangled pair to be used in a quantum pseudo telepathy game. All our schemes are based on extra randomness, which gives safer security implications in face of weak measurements. We believe that our new approach and techniques suggest a possible direction for future research on IT-secure quantum homomorphic encryption.

REFERENCES

[AAUC18] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (CSUR)*, 51(4):79, 2018.

[ABC+19] Dorit Aharonov, Zvika Brakerski, Kai-Min Chung, Ayal Green, Ching-Yi Lai, and Or Sattath. On quantum advantage in information theoretic single-server pir. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 219–246, Cham, 2019. Springer International Publishing.

[ABP+02] Yakir Aharonov, Alonso Botero, Sandu Popescu, Benni Reznik, and Jeff Tollaksen. Revisiting hardy's paradox: counterfactual statements, real measurements, entanglement and weak values. *Physics Letters A*, 301(3-4):130–138, 2002.

[ADSS17] Gorjan Alagic, Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum fully homomorphic encryption with verification. In *Advances in Cryptology - ASIACRYPT 2017 - Proceedings of the 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Part I*, pages 438–467, 2017.

[AMTdW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000*, pages 547–553, 2000.

[BB84] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. IEEE New York, 1984.

[BBT03] Gilles Brassard, Anne Broadbent, and Alain Tapp. Multi-party pseudo-telepathy. In *Workshop on Algorithms and Data Structures*, pages 1–11. Springer, 2003.

[BBT05] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005.

[BJ15] Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low t-gate complexity. In *Proceedings of Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Part II*, pages 609–629, 2015.

[BP16] Zvika Brakerski and Renen Perlman. Lattice-based fully dynamic multi-key fhe with short ciphertexts. In *Annual Cryptology Conference*, pages 190–213. Springer, 2016.

[Bra18] Zvika Brakerski. Quantum FHE (almost) as secure as classical. In *Advances in Cryptology - CRYPTO 2018 - Proceedings of the 38th Annual International Cryptology Conference, Part III*, pages 67–95, 2018.

[Bro15] Anne Broadbent. Delegating private quantum computations. *Canadian Journal of Physics*, 93(9):941–946, 2015.

[CDN15] Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen. *Secure multiparty computation*. Cambridge University Press, 2015.

[Chi05] Andrew M. Childs. Secure assisted quantum computation. *Quantum Information & Computation*, 5(6):456–466, 2005.

[DJ92] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A*, 439(1907):553–558, 1992.

[DL04] Fu-Guo Deng and Gui Lu Long. Secure direct communication with a quantum one-time pad. *Physical Review A*, 69(5):052319, 2004.

[DSS16] Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum homomorphic encryption for polynomial-sized circuits. In *Advances in Cryptology - CRYPTO 2016 - Proceedings of the 36th Annual International Cryptology Conference, Part III*, pages 3–32, 2016.

[EC11] Avshalom C Elitzur and Eliahu Cohen. The retrocausal nature of quantum measurement revealed by partial and weak measurements. In *AIP Conference Proceedings*, volume 1408, pages 120–131. AIP, 2011.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[Gen09] Craig Gentry. *A fully homomorphic encryption scheme*. Stanford University, 2009.

[GHS12] Craig Gentry, Shai Halevi, and Nigel P Smart. Fully homomorphic encryption with polylog overhead. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 465–482. Springer, 2012.

[GHS16] Craig B Gentry, Shai Halevi, and Nigel P Smart. Homomorphic evaluation including key switching, modulus switching, and dynamic noise management, March 8 2016. US Patent 9,281,941.

[Gro96] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

[Jor18] Stephen Jordan. Quantum algorithm zoo, 2018. http://math.nist.gov/quantum/zoo.

[Kak06] Subhash Kak. A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, 19(3):293–296, 2006.

[Lia13] Min Liang. Symmetric quantum fully homomorphic encryption with perfect security. *Quantum information processing*, 12(12):3675–3687, 2013.

[LK14] Yehuda Lindell and Jonathan Katz. *Introduction to modern cryptography*. Chapman and Hall/CRC, 2014.

[Mah18] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS*, pages 332–338, 2018.

[Mer90] N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373, 1990.

[NC02] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[OTF18] Yingkai Ouyang, Si-Hui Tan, and Joseph F Fitzsimons. Quantum homomorphic encryption from quantum codes. *Physical Review A*, 98(4):042334, 2018.

[RAD78] Ronald L Rivest, Len Adleman, and Michael L Dertouzos. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

[RFG12] Peter P Rohde, Joseph F Fitzsimons, and Alexei Gilchrist. Quantum walks with encrypted data. *Physical review letters*, 109(15), 2012.

[Sho94] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. Ieee, 1994.

[TC13] Boaz Tamir and Eliahu Cohen. Introduction to weak measurements and weak values. *Quanta*, 2(1):7–17, 2013.

[TKO$^+$16] Si-Hui Tan, Joshua A Kettlewell, Yingkai Ouyang, Lin Chen, and Joseph F Fitzsimons. A quantum approach to homomorphic encryption. *Scientific reports*, 6:33467, 2016.

[VDGHV10] Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 24–43. Springer, 2010.

[XWZ$^+$18] Jian Xu, Laiwen Wei, Yu Zhang, Andi Wang, Fucai Zhou, and Chong-zhi Gao. Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures. *Journal of Network and Computer Applications*, 107:113–124, 2018.

[YPDF14] Li Yu, Carlos A Pérez-Delgado, and Joseph F Fitzsimons. Limitations on information-theoretically-secure quantum homomorphic encryption. *Physical Review A*, 90(5):050303, 2014.

VI. APPENDIX A – THE ROLE OF BASES IN QUANTUM COMPUTING

To address a broad spectrum of readers, we here give a brief overview of the basics of quantum computation. Further details on the topic may be found in [NC02]. The basic building block of quantum computation protocols is the *qubit*. The qubit is the quantum version of the classical bit used in classical computing. Whereas a classical bit may be described as an element of $\{0,1\}$, a qubit may be described as a unit vector in the Hilbert space $\mathbb{C}^2$. Denote $\mathbb{H}=\mathbb{C}^2$, and $|0\rangle$ and $|1\rangle$ be the elements $\binom{1}{0}$ and $\binom{0}{1}$ of $\mathbb{H}$, respectively. $\{|0\rangle, |1\rangle\}$ is the *computational basis* of $\mathbb{H}$. We use the Ket notation and denote qubits by $|\psi\rangle$. A system composed of n qubits is described by a unit vector of $\mathbb{H}^{\otimes n}$, the n-fold tensor product of $\mathbb{H}$ with itself. Such a system of n qubits is the quantum version of an n-long string of classical bits.

An arbitrary qubit $|\psi\rangle \in \mathbb{H}$ may be described by its coordinates in the computational basis using four real numbers: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha,\beta \in \mathbb{C}$. If $|\psi_1\rangle$ and $|\psi_2\rangle$ are two elements of $\mathbb{H}$ such that $|\psi_1\rangle = e^{i\gamma}|\psi_2\rangle$ for some $\gamma \in \mathbb{R}$, then $|\psi_1\rangle$ and $|\psi_2\rangle$ are *equal up to a global phase factor*. Global phase factors have no influence on quantum computations, and hence may be ignored. Hence, and as $|\psi\rangle$ is a unit vector, one may write $|\psi\rangle$ using only two real numbers:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle,$$

where $\theta,\varphi \in \mathbb{R}$. This is the *Bloch sphere representation* of $|\psi\rangle$. The name sphere representation comes from the fact that θ and φ may be used to visualize $|\psi\rangle$ as a unit vector in $\mathbb{R}^3$.

In classical computing, strings of classical bits are manipulated using logic gates, information is represented as a string of bits, and the function to be computed over the information is represented as a logic circuit, which is composed of logic gates. In quantum computing, systems of qubits are manipulated using *quantum gates*, information is represented as a system of qubits and the function to be computed over the information is represented as a *quantum circuit*, which is composed of quantum gates. In order *to implement* a classical computation, bits are *physically realized* and the physical realizations of the bits are manipulated using physical realizations of logic gates. To implement quantum computations, qubits are physically realized, and these physical realizations of the qubits are manipulated using physical realizations of quantum gates. While classical logic gates are Boolean functions, quantum gates are unitary operators on Hilbert spaces. We use the Kronecker product notation to represent unitary operations as matrices.

Quantum computers may be used to perform computations that have been performed using classical computers, as well as other tasks. For example, any information that may be represented classically as a string of bits may be represented in the quantum model as a tensor product of elements of the computational basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{H}$. Then, any classical circuit may be implemented in the quantum model using a quantum circuit composed of *Toffoli gates*, which is the quantum version of the classical universal *NAND* gate.

Reading quantum information. A physical realization of a qubit may come in different forms. However, according to the postulates of quantum mechanics, no matter what form of realization is chosen, given a physical realization of an arbitrary qubit, $|\psi\rangle$, *one cannot determine its coordinates.* This phenomenon is known as *the uncertainty principle*. The inability to determine the coordinates of an arbitrary qubit is not an issue of insufficient measuring devices, but a consequence of the fundamental laws of quantum mechanics. According to these laws, an arbitrary qubit may be realized (up to a certain amount of precision, dependent of the accuracy of the equipment used), but it cannot be read. Qubits may be *measured*. Measurements of qubits are performed *in reference to a chosen orthonormal basis of* $\mathbb{H}$ and the outcome of the measurement is random, either zero or one, as detailed below. As a result of the measurement, the qubit is transformed into one of the two qubits of that orthonormal basis. The probability of obtaining each of the possible outcomes is the square of the absolute value of the corresponding coordinate of the qubit in the chosen basis. Explicitly, given $\theta,\varphi \in \mathbb{R}$, denote

$$|\psi_0\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix}, \qquad |\psi_1\rangle = \begin{pmatrix} \sin(\theta/2) \\ -e^{i\varphi}\cos(\theta/2) \end{pmatrix}, \tag{4}$$

and denote by $B_{(\theta,\varphi)}$ the orthonormal basis $\{|\psi_0\rangle, |\psi_1\rangle\}$ of $\mathbb{H}$. For a qubit $|\psi\rangle \in \mathbb{H}$ and an orthonormal basis $B_{(\theta,\varphi)}$ of $\mathbb{H}$, write $|\psi\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle$. When $|\psi\rangle$ is measured in reference to $B_{(\theta,\varphi)}$, there is a probability of $|\alpha|^2$ that $|\psi\rangle$ will transform into $|\psi_0\rangle$, yielding the outcome 0, and a probability of $|\beta|^2$ that it will transform into $|\psi_1\rangle$, yielding the outcome 1. We say that, when $|\psi\rangle$ is measured in reference to the basis $B_{(\theta,\varphi)}$, it *collapses* into one of the elements of that basis. Given $B_{(\theta,\varphi)}$, an orthonormal basis of $\mathbb{H}$, any unit vector $|\psi\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle$ is *a superposition of* $|\psi_0\rangle$ *and* $|\psi_1\rangle$, and the elements of $B_{(\theta,\varphi)}$ are *pure states in reference to* $B_{(\theta,\varphi)}$. Since $B_{(\theta,\varphi)}$ is an orthonormal basis, α and β are the inner products of $|\psi\rangle$ and the elements of $B_{(\theta,\varphi)}$. In general, if $B = \{|v_1\rangle, \ldots, |v_n\rangle\}$ is an orthonormal basis of an n-dimensional Hilbert space and $|v\rangle = \sum_{j=1}^{n} \alpha_j |v_j\rangle$, the inner product of $|v_k\rangle$ and $|v\rangle$, denoted by $\langle v_k|v\rangle$, is

$$\langle v_k|v\rangle = \left\langle v_k \middle| \sum_{j=1}^{n} \alpha_j |v_j\rangle \right\rangle = \sum_{j=1}^{n} \alpha_j \langle v_k|v_j\rangle = \alpha_k. \tag{5}$$

Hence, $|\alpha|^2 = |\langle\psi_0|\psi\rangle|^2$ and $|\beta|^2 = |\langle\psi_1|\psi\rangle|^2$. This fact is used in this paper to compute the probabilities of obtaining the different outcomes when measuring a given qubit (or a system of qubits) in reference to a given orthonormal basis. Measurements of systems of l qubits are performed in reference to orthonormal bases of $\mathbb{H}^{\otimes l}$, and result in a collapse of the system into one of the elements of that basis. The possible outcomes of such a measurement are the corresponding binary strings of length l, and the probability of obtaining each of the possible outcomes is the square of the absolute value of the corresponding coordinate of the system in the chosen basis. These may be computed using (5). E.g., consider $l = 2$, and let $B_{(\theta,\varphi)} = \{|\psi_0\rangle, |\psi_1\rangle\}$ and $B_{(\theta',\varphi')} = \{|\psi'_0\rangle, |\psi'_1\rangle\}$ two orthonormal bases of $\mathbb{H}$. Tensor products of elements of these bases give the following orthonormal basis $\{|\psi_0\psi'_0\rangle, |\psi_0\psi'_1\rangle, |\psi_1\psi'_0\rangle, |\psi_1\psi'_1\rangle\}$, denoted $B_{(\theta,\varphi)} \otimes B_{(\theta',\varphi')}$ of $\mathbb{H}^{\otimes 2}$. Given a system of two qubits, measuring that system in reference to $B_{(\theta,\varphi)} \otimes B_{(\theta',\varphi')}$ is equivalent to measuring the first qubit in reference to $B_{(\theta,\varphi)}$ and the second qubit in reference to $B_{(\theta',\varphi')}$.

VII. Appendix B - security proof of the random basis encryption scheme

We now prove that the random basis encryption scheme is IT-secure. We do it in two different ways. First, as our scheme deals with encrypting and computing over classical data, we give a proof based on standard security definitions of classical schemes. Namely, we use a variant of a standard privacy definition from [LK14]. The second proof follows a standard privacy definition from the quantum setting derived from [AMTdW00].

As described in Section I, an encryption scheme is composed of three algorithms, `Gen`, `Enc` and `Dec`. $\mathcal{M}$, $\mathcal{K}$ and $\mathcal{C}$ are the message space, key space and ciphertext space of the scheme, respectively. In our case, $\mathcal{M} = \{0,1\}$ and $\mathcal{K} = [0, 2\pi] \times \{\pm\frac{\pi}{2}\}$. What is $\mathcal{C}$? On the one hand, $\mathcal{C}$ is the set of possible outputs of `Enc`, implying that $\mathcal{C} = \mathbb{H}$. On the other hand, a ciphertext cannot indicate the encrypted information if it is not read. To read information from a qubit, one must measure that qubit. The output of such a measurement is an element of $\{0,1\}$, implying that $\mathcal{C} = \{0,1\}$. The first (classical approach) proof uses the latter interpretation of $\mathcal{C}$, and the second (quantum approach) proof uses the former.

We begin with the classical approach. Assume that an adversary is holding an encryption $|q\rangle$ of b generated using some key $(\theta,\varphi) \in \mathcal{K}$. The adversary wishes to use $|q\rangle$ to find b, or to gain any information that will enable a better guess of b. The adversary is only able to measure $|q\rangle$ in reference to any orthonormal basis he chooses. If the measurement is performed in reference to any orthonormal basis other than $B_{(\theta,\varphi)}$, then each of the outcomes zero or one may be obtained with positive probability.

We now rigorously prove that, no matter which orthonormal basis $B_{(\theta_0,\varphi_0)}$ is used by the adversary to measure $|q\rangle$, the probability of each of the outcomes zero or one is $\frac{1}{2}$, regardless of the actual value of b.

We now define the security criterion. Since Gen is a probabilistic algorithm, given a message $m \in \mathcal{M}$, the probability distribution over $\mathcal{K}$ induces a probability distribution over $\mathcal{C}$. An encryption scheme is *perfectly secure* if all messages $m \in \mathcal{M}$ induce the same probability distribution over $\mathcal{C}$. Formally (see [LK14, Lemma 2.3]):

Definition 1. *An encryption scheme (*Gen, Enc, Dec*) over a message space $\mathcal{M}$ is perfectly secure if for every probability distribution over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$, and every $c \in \mathcal{C}$:*

$$Pr[C = c|M = m_0] = Pr[C = c|M = m_1],$$

where C and M are the random variables denoting the value of the ciphertext and the message, respectively.

By Definition 1, perfect security of the random basis encryption scheme follows from

Lemma 2. *Let $(\theta_0, \varphi_0) \in [0, 2\pi]^2$. One has*

$$Pr\big[\mathbf{M}\big(\,|\psi_0\rangle\,, B_{(\theta_0,\varphi_0)}\big) = 0\big] = Pr\big[\mathbf{M}\big(\,|\psi_1\rangle\,, B_{(\theta_0,\varphi_0)}\big) = 0\big], \tag{6}$$

where

- *$B_{(\theta_0,\varphi_0)}$ is the orthonormal basis used by an adversary to measure an encryption of a bit,*
- *$|\psi_0\rangle$ and $|\psi_1\rangle$ are as in (4), and are encryptions of zero and one, obtained using our scheme,*
- *$\mathbf{M}\big(\,|\psi\rangle\,, B_{(\theta_0,\varphi_0)}\big)$ is the random variable denoting the result obtained when measuring $|\psi\rangle$ in reference to $B_{(\theta_0,\varphi_0)}$,*
- *the probability is over the choice of (θ, φ) from $[0, 2\pi]^2$ and the inherent randomness of quantum measurements.*

Proof. We begin with computing the expression on the left-hand side $Pr\big[\mathbf{M}\big(\,|\psi_0\rangle\,, B_{(\theta_0,\varphi_0)}\big) = 0\big]$ of (6). That is, computing the probability of obtaining the outcome zero when measuring $|\psi_0\rangle$ in reference to $B_{(\theta_0,\varphi_0)}$ in terms of θ and φ. This probability is the square of the absolute value of the first coordinate of $|\psi_0\rangle$ in the orthonormal basis $B_{(\theta_0,\varphi_0)}$. Denote by $|v_0\rangle$ and $|v_1\rangle$ the elements of $B_{(\theta_0,\varphi_0)}$. As mentioned in (5), the coordinates of $|\psi_0\rangle$ in $B_{(\theta_0,\varphi_0)}$ are given by appropriate inner products. Define $\alpha_0, \beta_0 \in \mathbb{C}$ by $|\psi_0\rangle = \alpha_0\,|v_0\rangle + \beta_0\,|v_1\rangle$. One has

$$\alpha_0 = \langle v_0|\psi_0\rangle = \left\langle \begin{pmatrix} \cos(\theta_0/2) \\ e^{i\varphi_0}\sin(\theta_0/2) \end{pmatrix} \middle| \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi}\sin(\theta/2) \end{pmatrix} \right\rangle = \cos(\theta_0/2)\cos(\theta/2) + e^{i(\varphi-\varphi_0)}\sin(\theta_0/2)\sin(\theta/2).$$

Multiplying by α_0^*, and using routine trigonometric identities, we obtain:

$$|\alpha_0|^2 = \tfrac{1}{2}\Big[\cos^2\tfrac{\theta+\theta_0}{2} + \cos^2\tfrac{\theta-\theta_0}{2} + \sin\theta\sin\theta_0\cos(\varphi-\varphi_0)\Big]. \tag{7}$$

Now, θ and φ are chosen uniformly random from $[0, 2\pi] \times \{\pm\frac{\pi}{2}\}$. The mean value of $|\alpha_0|^2$ over that domain may be computed in various ways. One may compute it using the formula $\overline{f} = \frac{1}{Vol(U)}\int_U f$, which yields $\frac{1}{2}$. By the law of total probability, the right-hand side of (6) is also $\frac{1}{2}$. All in all, we have

$$Pr\big[\mathbf{M}\big(\,|\psi_0\rangle\,, (\theta_0, \varphi_0)\big) = 0\big] = Pr\big[\mathbf{M}\big(\,|\psi_1\rangle\,, (\theta_0, \varphi_0)\big) = 0\big] = \tfrac{1}{2}.\ \square$$

This concludes the classical proof. We have shown that, no matter which orthonormal basis is chosen by the adversary to measure $|q\rangle$, the outcome 0 will be obtained with probability $\frac{1}{2}$, regardless of the actual value of b. By the laws of quantum mechanics, any operation other than measuring the qubit will

yield less information regarding the plaintext. Since measuring the qubit gives no information at all, the scheme is perfectly secure. We now turn to the quantum approach, which interprets the ciphertext space as $\mathbb{H}$. We use the density matrix representation of quantum states and base our claims on a security definition which follows the same line as Definition 3.1 from [AMTdW00] (modified for the continuous setting of our scheme).

Definition 2. *Let $S \subseteq \mathbb{H}$ be a set of qubits, $\mathcal{E} = \{U_i : i \in I\}$ be a set of unitary mappings on $\mathbb{H}$, and ρ_0 be some density matrix. Uniformly at random applying an element of $\mathcal{E}$ to a given element $|s\rangle \in S$ perfectly hides $|s\rangle$ if and only if for all $|s\rangle \in S$ we have*

$$\int_I U_i \left|s\right\rangle \left\langle s\right| U_i^\dagger = \rho_0.$$

In our case, $S = \{|0\rangle, |1\rangle\}$, and $\mathcal{E} = \left\{ \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ e^{i\varphi}\sin(\theta/2) & -e^{i\varphi}\cos(\theta/2) \end{pmatrix} : (\theta, \varphi) \in \mathcal{K} \right\}$. To show that the random basis encryption scheme is perfectly secure, we need to show that

$$\int_{\mathcal{K}} K_{\theta,\varphi} \left|0\right\rangle \left\langle 0\right| K_{\theta\varphi}^\dagger = \int_{\mathcal{K}} K_{\theta\varphi} \left|1\right\rangle \left\langle 1\right| K_{\theta\varphi}^\dagger, \tag{8}$$

where $K_{\theta\varphi} = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ e^{i\varphi}\sin(\theta/2) & -e^{i\varphi}\cos(\theta/2) \end{pmatrix}$. Routine computation shows that the left- and right-hand side of (8) are equal. To conclude, the density matrix that an adversary sees after encryption is the same, regardless of the input. This shows that the random basis encryption scheme is perfectly secure. We note that, since the evaluation algorithm is non-interactive, the adversary gains no new information executing it, and hence the scheme is secure.

Remark 1. In the key generation algorithm of our random basis encryption scheme, the user is required to pick a uniformly random element θ from $[0, 2\pi]$. Implementing random choices from a continuous domain might be technically challenging. However, the set of keys may be made discrete as follows. Let N a positive integer, and $\mathcal{K}_N = \left\{ \frac{2\pi n}{N} : n \in \{1, 2, \ldots, N\} \right\}$. Instead of picking θ from $[0, 2\pi]$, the user may uniformly at random pick θ from $\mathcal{K}_N$. How does that affect the security? In the classical security proof above, the mean value of the right hand side of (7) was computed by integrating over $[0, 2\pi]$. Replacing $[0, 2\pi]$ with $\mathcal{K}_N$, we compute the mean value of the right hand side of (7) by summing over all the possibilities for θ divided by N. Now, it is well known that for any real continuous function f,

$$\int_{[0,2\pi]} f(x)dx = \lim_{N\to\infty} \sum_{n=1}^{N} \tfrac{2\pi}{N} f\left(\tfrac{2\pi n}{N}\right).$$

Hence, by taking large enough N, the mean value of the discrete version can be made arbitrarily close to $\frac{1}{2}$. In the quantum proof, by similar arguments, we can make the left- and right-hand sides of (8) arbitrarily close to each other by taking large enough N. To conclude, taking the discrete version of the key space, we make `Gen` easier to implement in the cost of making the scheme statistically secure (rather than perfectly secure). Either way, the scheme is IT-secure.

VIII. Appendix C — proof of Lemma 1

Proof. Let $\theta \in [0, 2\pi]$ and $\varphi = \pm i$. One has:

$$\begin{aligned} |0\psi_0\rangle &= \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) \otimes \begin{pmatrix} \cos(\theta/2) \\ \pm i \sin(\theta/2) \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) \\ \pm i \sin(\theta/2) \\ 0 \\ 0 \end{pmatrix}, \\ D\,|0\psi_0\rangle &= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} \cos(\theta/2) \\ \pm i \sin(\theta/2) \\ 0 \\ 0 \end{pmatrix} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} \cos(\theta/2) \\ \pm i \sin(\theta/2) \\ \pm i \sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix}. \end{aligned} \tag{9}$$

The probabilities of obtaining each of the possible outcomes, when measuring $D\,|0\psi_0\rangle$ in reference to $\{|0\rangle, |1\rangle\} \otimes B_{(\theta,\varphi)}$, are the squares of the absolute values of the coordinates of $D\,|0\psi_0\rangle$ in that basis. The elements of $\{|0\rangle, |1\rangle\} \otimes B_{(\theta,\varphi)}$ are $|0\psi_0\rangle, |0\psi_1\rangle, |1\psi_0\rangle$ and $|1\psi_1\rangle$. The first, $|0\psi_0\rangle$, has been computed in (9). Now,

$$|1\psi_1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right) \otimes \begin{pmatrix} \sin(\theta/2) \\ \mp i \cos(\theta/2) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \sin(\theta/2) \\ \mp i \cos(\theta/2) \end{pmatrix}. \tag{10}$$

By (9) and (10),

$$\frac{|0\psi_0\rangle \pm i\,|1\psi_1\rangle}{\sqrt{2}} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} \cos(\theta/2) \\ \pm i \sin(\theta/2) \\ \pm i \sin(\theta/2) \\ \cos(\theta/2) \end{pmatrix} = D\,|0\psi_0\rangle\,.$$

This shows that the coordinates of $D\,|0\psi_0\rangle$ in $\{|0\rangle, |1\rangle\} \otimes B_{(\theta,\varphi)}$ are $\frac{1}{\sqrt{2}}, 0, 0$ and $\frac{\pm i}{\sqrt{2}}$. Taking the squares of the absolute values of these coordinates one sees that, measuring in reference to $\{|0\rangle, |1\rangle\} \otimes B_{(\theta,\varphi)}$, the outcome 00 is obtained with probability $\frac{1}{2}$, as so is 11. The probabilities of obtaining the different outcomes when measuring $D\,|0\psi_1\rangle$ in reference to $\{|0\rangle, |1\rangle\} \otimes B_{(\theta,\varphi)}$ may be found by substituting $\theta = \pi - \theta'$ and $\varphi = -\varphi'$. That substitution yields $D\,|0\psi_1\rangle = \frac{|0\psi_1\rangle \mp i|1\psi_0\rangle}{\sqrt{2}}$. Taking the squares of the absolute values, we obtain the desired probabilities. □

IX. Appendix D — The magic square game

A secure Quantum Pseudo-Telepathy scheme. The phrase *Quantum Pseudo-Telepathy* was first introduced in [BBT03], and refers to the use of *quantum entanglement* to eliminate the need for communication in specific multi-party tasks. A comprehensive coverage of the subject may be found in [BBT05]. The simplest example of quantum pseudo-telepathy comes from the *Mermin-Peres magic square game* [Mer90]. In that game, two parties, Alice and Bob, are presented with a 3×3 table. Each of them is required to fill in a part of the table, as follows. Alice is given a number i, $1 \leq i \leq 3$, and needs to put either 0 or 1 at each entry of the i-th row, in such a way that the sum of the three entries will be even. Similarly, Bob is given a j, $1 \leq j \leq 3$, and needs to fill in the j-th column with the constraint that the sum be odd. The numbers i and j are the inputs of the parties. Alice and Bob win the game if they place the same number in the intersection of the row and the column that they fill. The parties do not know i and j ahead of the game, and they cannot communicate after being given these values. They are allowed to communicate before the game begins, discuss game strategies, and send information to each other. It was shown in [BBT05] that there is no classical algorithm that lets Alice and Bob win the game with probability greater than $\frac{8}{9}$, whereas there exists a quantum algorithm that lets them win the game with probability 1. This quantum algorithm is based on having each of the parties hold two qubits out of an entangled system of four qubits. The system of four qubits used in [Mer90] for that purpose is

$$|\Psi\rangle = \tfrac{1}{2}\,|0011\rangle - \tfrac{1}{2}\,|0110\rangle - \tfrac{1}{2}\,|1001\rangle + \tfrac{1}{2}\,|1100\rangle\,.$$

We briefly explain the meaning of entanglement in the system $|\Psi\rangle$. The system $|\Psi\rangle$ is a superposition of four of the elements of the computational basis of $\mathbb{H}^{\otimes 4}$. Measuring that system in reference to the computational basis of $\mathbb{H}^{\otimes 4}$ we get one of the elements of that basis that appear in $|\Psi\rangle$, each with probability $\frac{1}{4}$. Measuring any single qubit from the system $|\Psi\rangle$ in reference to the computational basis of $\mathbb{H}$, each of the outcomes zero and one is obtained with probability $\frac{1}{2}$. Nevertheless, the result of such a measurement will affect the possible outcomes of measurements of other qubits of that system. Specifically, assume that the first qubit of the system $|\Psi\rangle$ has been measured (in reference to the computational basis of $\mathbb{H}$) and that the outcome b was obtained. Then, measuring the third qubit of that system (in reference to the computational basis of $\mathbb{H}$) we get the outcome $1-b$ with probability 1. The same holds for measurements of the second and fourth qubit. Such a system of qubits, on which a measurement of some of the qubits affects the possible outcomes of measurements of other qubits, is an *entangled* system. Entanglement is the core element behind the quantum algorithm that wins the magic square game.

Following is a brief description of the main stages of the winning algorithm as introduced in [Mer90]. Before the game begins, the parties generate a system of four entangled qubits (such as $|\Psi\rangle$) and share it in such a way that Alice holds the first two qubits of the system and Bob holds the other two. The game begins, and the participants are given their inputs. Then, each party applies one of several predetermined quantum gates to his/her qubits according to the input. (Explicit matrix representation of these gates may be found in [BBT05].) Next, the parties measure their qubits (in reference to the computational basis of $\mathbb{H}$) and fill in the first two entries of their row/column according to the outcomes of their measurements. Each of them fills the last entry of her/his row/column according to the parity condition defined above. It was proved in [Mer90] that, by following this algorithm, Alice and Bob are guaranteed to win the game.

Assume that Alice and Bob are two distant parties, willing to participate in the game. To use the algorithm described above, they must share an entangled four-qubit state. They may ask a third party, Charlie, to generate such an entangled state and transmit two qubits to each of them. In that case, two concerns may arise. First, Charlie might be untrustworthy. Second, two adversaries, Eve and Mallory, might intercept Charlie's transmission and use the entangled qubits sent by Charlie for a game of their own, or any other purpose (see Figure 5).

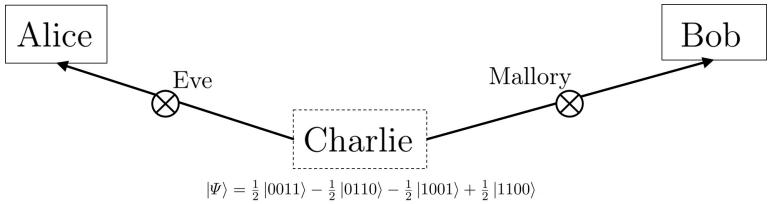

Figure 5: Adversarial attack by two adversaries.

To overcome the possibility that Charlie is untrustworthy, Alice and Bob may decide that one of them, say Alice, will generate the desired four-qubit entangled state and transmit two of the qubits to Bob. This does not solve the second concern. A single adversary, Eve, may intercept the transmission and use the qubits to engage in the Mermin-Peres magic square game with Alice instead of Bob (see Figure 6).

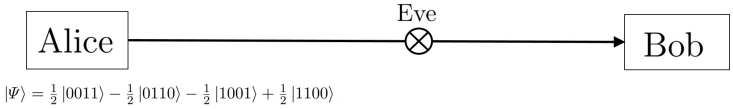

Figure 6: Adversarial attack by a single adversary.

We now show how two distant parties may securely generate and share a system of entangled qubits using our random basis encryption scheme. The constructions we use here, enabling securing this process

against adversarial attacks, are similar to those used above where we construct the D gate. The stages are as follows.

- Alice uses our random basis encryption scheme in order to generate independent encryptions of two 0 bits and two 1 bits. For ease of presentation, we denote that four-qubit system by $|\psi_0\psi_0\psi_1\psi_1\rangle$.We stress that each of the qubits is encrypted independently.
- Alice generates a pair of ancillary $|0\rangle$ qubits and applies the gate described in Figure 7 to her system of six qubits.

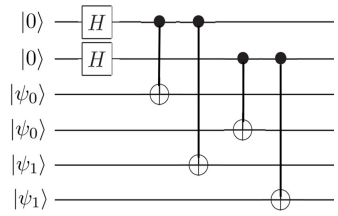

Figure 7: random basis entanglement gate.

- The first two qubits are ancillary qubits, and are not used in the next stages of the scheme. Alice keeps the next two qubits to herself and transmits the last two to Bob.
- Alice and Bob engage in our QKD scheme, during which Alice shares with Bob the keys she used to generate the encrypted qubits in the first stage of this scheme.
- Alice and Bob decrypt the qubits they hold and obtain a system of four entangled qubits.

Each of the qubits that Alice transmits to Bob in the third stage of this scheme is encrypted using a different key, and hence, if an adversary intercepts the transmission and possesses these qubits, then the adversary cannot use them to engage in the game in place of Bob. After decryption, the last four output qubits constitute a system of two pairs of maximally entangled qubits, which may be used to win the magic square game using the same methods as in [Mer90]. Observe that, and Hadamard gate is applied to the first and second qubits of the system. Then, each of these qubits is used as a control qubit in two $CNOT$ gates, where the target qubits are the other four qubits. This procedure results in obtaining the same four qubit state as the one used in [Mer90].

Generally, entanglement is an important resource in quantum computation. Once generated, it should be guaranteed that only the rightful owners of it may be able to use it. The above is but one example of a setting in which entanglement should be secured. Our scheme provided a way of securing that important resource in an IT-secure way.