Randomly Choose an Angle from Immense Number of Angles to Rotate Qubits, Compute and Reverse

For QKD Resilient Against Weak Measurements and Securing Entanglement

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, Beer-Sheva, Israel

Abstract

Homomorphic encryption (HE) schemes enable the 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 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. In contrast to the legacy quantum one-time pad scheme, our scheme is *computation agnostic*. That is, when delegating computations, the user can remain utterly oblivious to the implementation method chosen by the cloud.

We suggest an encryption scheme based on random bases and discuss the homomorphic properties of that scheme. One of the advantages of our scheme is providing better security in the face of weak measurements (WM). Measurements of this kind enable collecting partial information on a quantum state while only slightly disturbing the state. We suggest here a novel QKD scheme based on random bases, which is resilient against WM-based attacks. We demonstrate the usefulness of our scheme in several applications. Notably, we bring up a new concept we call *securing entanglement*. We look at entangled systems of qubits as a resource, used for carrying out quantum computations, and show how our scheme may be used to guarantee that an entangled system can be used only by its rightful owners. To the best of our knowledge, this concept has not been discussed in previous literature.

Keywords: Quantum homomorphic encryption, Information-theoretic security, Quantum key distribution, Weak measurements, Securing entanglement

We would like to thank the Lynne and William Frankel Center for Computer Science, the Rita Altura Trust Chair in Computer Science. This research was also partially supported by a grant from the Ministry of Science and Technology, Israel & the Japan Science and Technology Agency (JST), and the German Research Funding (DFG, Grant#8767581199). We also thank Daniel Berend for discussions, comments and suggestions throughout the research.

I. Introduction

Delegation of computation, while preserving the confidentiality of the data (and sometimes even the program), is a challenging practical task that 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 an untrusted 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 the delegation of computation are based on either the distributed approach of secure multiparty 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 the 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 the processing of only a limited set of functions over the encrypted data. Fully homomorphic encryption (FHE) schemes, which may support the 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 a 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 (i.e., poly-time), 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' depends on f, and decryption of the evaluated ciphertext requires the user to modify her keys according to f. We stress that 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 the user 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 an untrusted cloud and have the following properties.

- IT-secure.
- Efficient. I.e., all algorithms are poly-time.
- Fully compact. I.e., the decryption algorithm requires $\mathcal{O}(1)$ time, regardless of f. This means that the user is not required to apply any transformations to the encryption keys to decrypt the processed data correctly.
- Perfectly correct. I.e., the ciphertext decrypts to the right plaintext with probability 1 (we ignore errors that may arise due to the nature of noisy physical implementations of quantum schemes).
- Non-interactive. I.e., no client-server 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 restrictions. Ambianis et al.'s QOTP scheme, suggested in [AMTdW00], was used to construct QHE scheme that have some of the properties listed above. Several such schemes are reviewed below.

Quantum key distribution (QKD). QKD schemes were the first sign of the significant breakthroughs to come in quantum computing. In their seminal work from 1984, Bennett and Brassard [BB84] presented a scheme (hereafter the BB84 protocol) that utilizes a quantum mechanics phenomenon to enable two distant parties, Alice and Bob, to agree on a random key without relying on any computational hardness assumptions. This result indicated that quantum computers could perform tasks that could not be carried using classical computers.

The BB84 scheme was not only a theoretic breakthrough that paved the way for further theoretic discoveries in the field of quantum computing but was also found to have far-reaching practical applications, as it is feasible to implement it using current-day technology. Private quantum-computing companies (e.g., IDQ and AUREA Technology) offer today quantum-based IT-secure key-exchange services, based on the BB84 protocol, or newer variations of it. Their users include government agencies, financial institutions, companies with distributed offices, and data centers worldwide.

The security of the BB84 protocol (and the following variations of it) is information-theoretic, i.e., it assumes no limitations on the possible computing power of the adversary. The security of these protocols is based on the laws of quantum mechanics. Mainly, it is based on the third postulate of quantum mechanics, which states that measurements of a quantum state cause the state to collapse [NC02]. This phenomenon enables Alice and Bob to reveal eavesdropping attempts. Various attacks on QKD schemes have been suggested over the years. These attacks mainly target weaknesses in the implementation of the scheme and are discussed in, e.g., [GLLP04], [Wan05], [LSMLYWW15], [BP12].

A different approach to attack QKD schemes, which was not previously addressed elsewhere, is based on *weak measurements*. The model of weak measurements, rooted in the work of Aharonov et al. from 1964 [ABL64], then further developed and studied in, e.g., [ED01], [ABP$^+$02], [JK10], [EC11], raises the possibility of weakly measuring a quantum state. That is, gathering a small amount of information regarding the state while only slightly disturbing it, but not collapsing it. In this work, we investigate ways in which weak measurements incur a threat to the security of QKD schemes. Using weak measurements, an eavesdropper may gather information regarding the key obtained by Alice and Bob, while leaving but slight indications of the eavesdropping that has occurred. How does that affect the security of the scheme, the key-generation rate?

Quantum secure direct communication (QSDC) schemes, which are based on similar ideas to those of QKD, enable Alice and Bob to IT-securely exchange not only random keys but also arbitrary messages of their choice. See, e.g., [DL04], [ABP$^+$02] and the references therein. Similarly to QKD schemes, QSDC schemes might also be vulnerable to WM-based attacks.

Related work.
(1) *Computationally secure QHE schemes*. 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 the 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 does not obtain the properties listed above. First, their scheme employs a computationally secure FHE protocol, which makes their scheme only computationally secure (as mentioned, in this work, 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 (while 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 $\mathcal{O}(s)$ time, where s is the size of the circuit. As mentioned, in this work, we look for fully compact schemes — schemes in which $\texttt{Dec}$ requires $\mathcal{O}(1)$ time.

An approach similar to [Bro15] was adopted by [BJ15]. There, two schemes were proposed. The first has a decryption procedure whose time-complexity scales with the square of the number of T-gates (and hence does not obtain 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 (in this work, we are looking for IT-secure schemes).

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 is based on QOTP and 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 does not obtain the requirement of perfect correctness as it has positive error probability. Brakerski [Bra18] used the high-level outline of [Mah18] to construct a computationally secure QFHE scheme that enables homomorphic evaluation of classical circuits with bounded depth over classical data and with improved correctness. To support unbounded depth, [Mah18] further rely on a circular security assumption.

The schemes listed above suggest practical solutions to the problem of homomorphic encryption. However, all these schemes have computational security (and not IT-security) and hence does not obtain the properties in which we are interested in this work. The security of their schemes is based on unproven computational hardness assumptions. The schemes listed below rely on no computational hardness assumptions.

(2) *Other QHE schemes*. As mentioned above, it was shown in [AMTdW00] that QOTP is an IT-secure encryption scheme that supports homomorphic evaluation of Pauli gates. Encryption is performed by randomly applying X and Z gates to qubits, conditioned on a two-bit (classical) key, and decryption is performed by applying the same gates in the opposite direction. However, this method alone provides no means for constructing a QHE scheme that withstands our requirements. In particular, homomorphic evaluation of Clifford gates over QOTP-encrypted data requires that the user perform computations over the classical keys in compliance with the computations that are performed by the server over the encrypted qubits. This requirement results in decryption complexity linear in the size of the circuit, and hence, the scheme is not fully compact. Set side by side, our scheme is *computation agnostic*. That is, the user must care not how the cloud implements the computation.

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 that enable the server to help the user in performing a

universal set of quantum gates over encrypted data. However, 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.

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$^+$16]. Built on constructions taken from quantum codes, they achieved an encryption scheme that supports the evaluation of circuits with a constant number of non-Clifford gates. Though achieving stronger security guarantees than [RFG12], [TKO$^+$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 this 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.

(3) *Weak measurements and QKD*. 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.

Weak measurements are discussed in several places in literature, but never as a tool to attack QKD schemes. In [GDL$^+$10], an improved feedback-control of quantum systems was experimentally shown to be possible using weak measurements. Troupe and Farinholt [TF17] used weak measurements to construct a QKD scheme with an improved key-rate, immunity to detector basis-dependent attacks (such as detector blinding), and other various side-channel attacks. However, they have not considered WM-based attacks against their scheme, and only suggested ways in which Alice and Bob could use WM. In [HK08], weak measurements were used to detect a spin-dependent displacement of photons passing through an air-glass interface, the photonic version of the spin Hall effect in electronic systems.

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 $|-\rangle$. In this work, we consider the following scenario. 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. The same hindrance of using a different set of qubits to encode each classical bit repeats itself in many other QKD schemes, and hence, similar attacks can be applied there too. In our QKD scheme, 0 and 1 bits may have the same encoding, and hence, weak measurement attacks give the adversary no advantage.

Kak presented in [Kak06] a protocol that 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 is executed, 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 for Alice's bit.

We note that Kak's QKD protocol may be resilient against WM-based attacks. However, the scheme we suggest here outperforms Kak's protocol in several aspects. First, our protocol requires only two stages of communication, while Kak's protocol requires three stages of communication – a 50% communication overhead comparing to our scheme. Second, while in Kak's, protocol each of the parties must have the capability of applying arbitrary quantum gates to quantum states, in our protocol, only Bob needs to possess this capability, whereas it is sufficient for Alice to be able to apply only NOT gates to qubits. Furthermore, in Kak's scheme, Alice and Bob should agree on the 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 [BB84], their scheme uses qubits only in the computational or diagonal basis, and hence their scheme is vulnerable to weak measurement attacks, as shown below.

Our contribution. 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 gates, and a modified version of the Hadamard gate, which we show to be useful in several applications. We can also support $CNOT$ gates, where the control qubits are set in a non-random basis (i.e., plaintext qubits). The latter implies that cascading is possible only in specific yet important cases. We detail applications of our constructions, including random basis QKD and coalitions-resilient secure multiparty XOR computation. We note that, while some of these applications may also be constructed using other existing QHE schemes, our schemes are the first to support these applications while maintaining all of the following: IT-security, full compactness, perfect correctness, and non-interactively. The collection of these attributes makes our scheme *computation agnostic*. Furthermore, and most importantly, our schemes have safer security implications in the face of weak measurements, as we discuss below.

Second, in this work, we bring up a new concept called *securing entanglement*. Entanglement is known to be an essential resource in many quantum settings. The utilization of entanglement in communication, computation, and other scenarios is a very active area of research. In practice, entanglement is usually created by direct interactions between subatomic particles. The creation of entangled systems requires efforts and expenditures. We suggest that, once it was created, this resource should be secured in the sense that only its rightful owners will be able to use it.

Paper organization. In Section II, we present our random basis encryption scheme and discuss its homomorphic properties. The concept of securing entanglement is presented in Section III and demonstrated through the use of entangled qubits in a pseudo telepathy game. In Section IV, we describe WM attacks on existing QKD schemes and present our random basis QKD. Section V concludes the work. Relevant background on quantum computation, notations, and some of the proofs 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). A straightforward computation shows that this requirement compels $\varphi = \pm\pi/2$. Hence, for $(\theta, \varphi) \in [0, 2\pi] \times \{\pm\frac{\pi}{2}\}$, the random basis

$$B_{\left(\theta,\pm\frac{\pi}{2}\right)} = \left\{ \begin{pmatrix} \cos(\theta/2) \\ \pm i\sin(\theta/2) \end{pmatrix}, \begin{pmatrix} \sin(\theta/2) \\ \mp i\cos(\theta/2) \end{pmatrix} \right\}$$

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 that may be homomorphically applied to the ciphertext in a fully compact and non-interactive way.

The Random Basis Encryption (RBE) 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.

Homomorphic operations. We now explore the possibility of homomorphically applying quantum gates to the ciphertext by the untrusted quantum server. Obviously, any gate that commutes (up to a global phase factor) 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: $|b\rangle \rightarrow |1-b\rangle$. 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 shows 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 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 $B_{(\frac{\pi}{4},0)} = \left\{\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right), \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right)\right\}$. The elements of $B_{(\frac{\pi}{4},0)}$ are often denoted by $|+\rangle$ and $|-\rangle$. 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

$$H|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \cos(\theta/2) \\ \pm i\sin(\theta/2) \end{smallmatrix}\right) = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} \cos(\theta/2)\pm i\sin(\theta/2) \\ \cos(\theta/2)\mp i\sin(\theta/2) \end{smallmatrix}\right), \tag{1}$$

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.

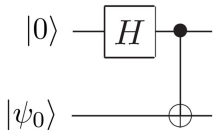

Figure 1: Random Based D gate.

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.

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

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

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,

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

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 (2), one may readily verify that, given a random basis $B_{(\theta,\varphi)}$,

$$C^nNOT|b_1b_2\ldots b_n\psi_b\rangle = \begin{cases} |b_1b_2\ldots b_n\psi_{1-b}\rangle, & \prod_{i=1}^n b_i = 1, \\ |b_1b_2\ldots b_n\psi_b\rangle, & \text{otherwise.} \end{cases} \quad (3)$$

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 $B_{(\theta,\varphi)}$.

To conclude, we have shown that our scheme supports homomorphic NOT operations, and a modified version of the Hadamard gate. It also supports homomorphic $CNOT$ gates, where the control qubits are set in clear.

III. Securing entanglement

Entanglement is an essential resource in quantum computation. In this section, we present a method for securing that important resource in an IT-secure way, using our scheme. One example of a setting in which entanglement is used as a core element is *Quantum Pseudo-Telepathy* games. This concept was introduced in [BBT03] and refers to the use of entanglement to eliminate the need for communication in specific multiparty tasks. Comprehensive coverage of the subject may be found in [BBT05]. An example

of such a task is the *Mermin-Peres magic square game* [Mer90]. In this 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 at 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 and discuss game strategies, or share any information they desire. 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

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

Entanglement is the core element behind not only the quantum algorithm that wins the magic square game but also behind many other breakthrough quantum algorithms. Once generated, it should be guaranteed that only the rightful owners of it would be able to use it. Next, we demonstrate a specific scenario where securing entanglement is required and discuss how it can be done.

Assume that Alice and Bob are two parties that wish to engage in the magic square game. Alternatively, Alice and Bob are two scientists working in distant labs and wish to complete a joint task that requires entanglement. First, we consider the case in which Alice and Bob can get together and jointly generate entangled qubits, or purchase them from a trusted provider. Alice and Bob, having obtained a large number of entangled qubits, store these qubits in their laboratories to use them when the task requires it. Alice and Bob are worried that at the end of the day, when Alice and Bob are no longer at their labs, other people, say, Eve and Mallory will break into their labs. Eve will steal half of each entangled system from Alice's lab, and Mallory will steal the corresponding half from Bob's lab and use the stolen entangled pairs for their own needs. In light of this concern, Alice and Bob are looking for a way to secure their entangled particles to ensure that no one else can use them. Like a smartphones password lock that will not let anyone use the smartphone without knowing the password.

One may suggest that, before leaving their laboratories, Alice and Bob use QOTP to (independently) encrypt each half of each entangled pair. How will it work? For example, assume that Alice and Bob hold two halves of an EPR pair,

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\big).$$

The subscripts A and B indicate the parts of the system held by each party. Alice picks QOTP keys (a_1, a_2) uniformly at random from $\{0,1\}^2$, and Bob similarly picks (b_1, b_2). At the end of the day, to secure the entangled pair, Alice applies $X^{a_1}Z^{a_2}$ to her half, and Bob applies $X^{b_1}Z^{b_2}$ to his part. Doing so, they obtain a new state:

$$X^{a_1}Z^{a_2} \otimes X^{b_1}Z^{b_2}|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}\Big(\big(X^{a_1}Z^{a_2}|0\rangle_A\big)\big(X^{b_1}Z^{b_2}|0\rangle_B\big)\big) + \big(X^{a_1}Z^{a_2}|1\rangle_A\big)\big(X^{b_1}Z^{b_2}|1\rangle_B\big)\Big).$$

Since the encryption keys were picked uniformly at random and independently of each other, the density matrix of the new state is equal to the identity (up to a constant). So it seems like this procedure secures the entangled system in the sense that, without knowing the encryption keys, the encrypted system contains zero amount of entanglement. This claim can be phrased using conventional measures of entanglement like entanglement distillation and entanglement dilution. However, if Eve and Mallory steal

a large amount of OTP-encrypted EPR pairs from Alice and Bob, then they could guess the encryption keys for each pair, and their guess is expected to be *perfectly correct* $\frac{1}{16}$ of the times (on average).

We want to refine this point. Eve and Mallory cannot produce two halves of an entangled system by using local operations and classical communication (LOCC) alone. Stealing OTP-encrypted EPR pairs from Alice and Bob, they can recover the original entangled system with a non-negligible probability using LOCC alone. Then, the recovered systems can be used by Eve and Mallory for their purpose. We conclude that QOTP encryption of EPR pairs reduces the value of a stolen pair to $\frac{1}{16}$ of its original value. In such a situation, it still pays for Eve and Mallory to steal EPR pairs, as 6.25% of them are expected to be usable.

A better way of securing entangled systems by Alice and Bob comes from our random basis encryption scheme. Alice and Bob can use our RBE scheme to encrypt each half of an EPR pair using independent random keys θ_a and θ_b. This way, if Eve and Mallory steal the encrypted qubits and try to decrypt them by guessing the keys, their guess is expected to be perfectly correct zero percent of the time. This makes stolen EPR pairs completely unusable, and in such a situation, the theft of EPR pairs becomes unprofitable.

What happens if Alice and Bob are far apart and cannot get together to generate (or purchase) an entangled system? Being far apart, they may ask a third party, Charlie, to generate such an entangled system and transmit half of it to each of them. In that case, two concerns may arise. First, Charlie might be untrustworthy. Second, Eve and Mallory might intercept Charlie's transmission and use the entangled qubits sent by Charlie for their purposes (see Figure 2).

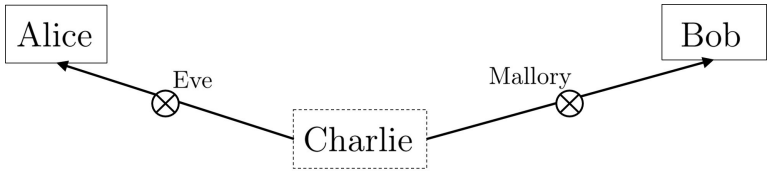

Figure 2: Adversarial attack by two adversaries.

To overcome the possibility that Charlie is untrustworthy, Alice and Bob may decide that one of them, say, Alice will generate the entangled system and transmit half of it to Bob. This does not solve the second concern. A single adversary, Eve, may still intercept the transmission and use the half sent to Bob to engage in the task with Alice (instead of Bob, see Figure 3).

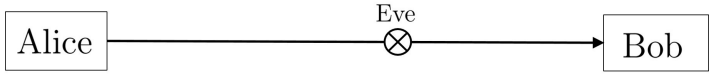

Figure 3: Adversarial attack by a single adversary.

To solve both concerns, Alice and Bob can securely generate and share an EPR pair using our random basis encryption scheme, as follows.

- Alice generates an EPR pair and encrypts each half independently using our RBE scheme.
- Alice keeps the first half to herself and transmits the second half to Bob.
- Alice and Bob communicate through a secure communication channel (possibly, using our QKD scheme presented below) and Alice shares with Bob the key she used to encrypt his half.
- When they need to use the entangled system, Alice and Bob decrypt the qubits they hold and obtain a proper entangled system.

This way, even if Eve intercepts the transmitted qubit, she can not use it to engage in the task instead of Alice without knowing the encryption key.

IV. The Random Basis CNOT Quantum Key Distribution scheme

Quantum key distribution (QKD), first suggested by Bennett and Brassard in 1984, is one of the most celebrated results in quantum computing. The discovery that quantum mechanics enables two distant parties to agree on a joint encryption key while relying on no computational assumptions is one of the most significant breakthroughs in the research on secure communications. However, the BB84 protocol, and most of the QKD schemes that followed it, do not prevent an eavesdropper from gaining any information on the key. Instead, these schemes are designed to enable Alice and Bob to detect eavesdropping attempts with high probability. This is done based on one of the most fundamental postulates of quantum mechanics – information gain is possible only at the cost of disturbing the state. After invoking the quantum part of the QKD scheme, Alice and Bob invoke classical *privacy amplification* (PA) and *data reconciliation* (DR) procedures.

These procedures are required to reduce the amount of information held by a possibly undetected eavesdropper, and to correct possible errors in the key caused by the eavesdropping. However, these procedures reduce the bandwidth and have time, communication, and computational costs. Similarly to the securing entanglement scenario, it would be very helpful if there was a way of reducing the ability of an eavesdropper to gain information from the outset, thereby impairing the motivation to attack the transmission and avoiding these expensive procedures.

In this section, we review two QKD protocols, namely, the BB84 protocol and the QKD scheme suggested by Deng and Long in [DL04], and suggest a new type of attack against these schemes. Our attack is based on *weak measurements* (WM), and it enables the attacker, Eve, to control the probability in which Alice and Bob detect her. Our WM attack allows Eve a tradeoff between the probability of being caught and the amount of information that she can gain in her attack. Then, we introduce our random basis CNOT QKD scheme, based on our RBE scheme. Our scheme, being resilient against such WM attacks, takes a step towards significantly impairing the motivation of a possible adversary.

The BB84 scheme. We now briefly review the BB84 QKD scheme (described in detail also in [NC02]). Alice picks two uniformly random bits a and b and generates the qubit $H^a X^b |0\rangle$. Alice transmits the qubit to Bob, who picks a uniformly random bit c, applies a c-conditioned Hadamard to the qubit, and measures the qubit in the computational basis (see Figure 4).

Figure 4: The BB84 QKD protocol.

Alice and Bob then announce a and c. If a and c are equal (which is expected with probability 0.5), and there was no adversarial interference on the transmission, then the outcome of Bob's measurement is guaranteed to be b (assuming an error-free quantum channel). Alice and Bob repeat this process for $\approx 4n$ qubits. Then, to detect possible eavesdropping, Alice and Bob compare n outcomes of Bob's measurements (randomly chosen from the $2n$ qubits for which $a = c$) with the corresponding b's. If the error rate is too high, Alice and Bob abort. If not, they can bound the amount of information held by an eavesdropper, and then invoke PA and DR procedures to obtain a joint secure key.

Remark 2. We suggest an improvement to the BB84 scheme. Instead of having Bob *guess* the basis Alice used (by randomly choosing $c \in \{0, 1\}$), Bob can notify Alice when he received the qubit, and then Alice can reveal the basis she used (i.e., reveal a). Next, Bob will use the correct basis for measurement 100% of the time. Since Alice's basis is announced only *after* the qubit has already arrived at Bob's safe

hands, Eve cannot use this information (i.e., a) to gain any information on the key. This simple variation of announcing the correct basis by Alice makes all Bob's measurements performed according to the right basis (by setting $c = a$), which results in doubling the key generation rate. This simple variation does not change the security of the scheme and was probably overlooked so far.

WM attack on BB84. Below we describe a WM-based attack on the BB84 QKD scheme. As mentioned in the Introduction, 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. We now demonstrate such a procedure. Let $\varepsilon > 0$ and denote by W_ε the following two-qubit quantum gate

$$W_\varepsilon = \sqrt{\varepsilon} \cdot i \cdot CNOT + \sqrt{1-\varepsilon} \cdot I \otimes I,$$

where I is the identity over a single qubit. One readily verifies that W_ε is unitary. This unitary can be used by Eve to gain information regarding the qubit transmitted from Alice to Bob, leaving but slight indications of her presence. We begin with some intuition. It is known that qubits in the computational basis can be cloned using the $CNOT$ gate and an ancillary $|0\rangle$ qubit. If the qubit designated for cloning is in the computational basis, then performing a $CNOT$ with the ancillary qubit as the target qubit copies the control qubit to the target qubit without disturbing the control qubit. However, if the control qubit is not in the computational basis, the $CNOT$ gate does disturb it (and it, of course, the target cannot be cloned). The W_ε gate is a linear combination of the identity operation on two qubits and the $CNOT$ gate. The smaller ε is, the closer W_ε is to the identity operation. If a qubit $|\psi\rangle$ is in one of the four states $|0\rangle, |1\rangle, |+\rangle$ or $|-\rangle$, we can apply W_ε to $|\psi\rangle$ and an ancillary $|0\rangle$ qubit and then measure the ancilla. This way, if $|\psi\rangle$ is either $|0\rangle$ or $|1\rangle$ we can gain a small amount of information regarding $|\psi\rangle$ without disturbing it, and if $|\psi\rangle$ is either $|+\rangle$ or $|-\rangle$ then we (get no information but) only slightly disturb the state.

The key-bit guessing game. The WM-attack is described in the setting of the *key bit guessing game*. This game attempts to encapsulate the essence of a QKD scheme being IT-secure against eavesdropping attempts by measuring the amount of information that can be gained by an eavesdropper *before* the PA and DR procedures are invoked. The participants in this game are Alice, Bob, and Eve. We assume that the participants can generate qubits in the computational basis, apply quantum gates to the qubits, and measure qubits. Alice and Bob are connected via a noiseless quantum channel and an authenticated classical public channel. Eve has full access to the quantum channel and is constantly listening to the public channel. Eve is computationally unbounded.

The key-bit guessing game is defined as follows. The parties are given a positive integer input n. Alice and Bob engage in a QKD protocol of their choice to obtain a key of $\approx n$ bits, while $\approx 4n$ qubits can be transmitted between them. We assume that $2n$ qubits are used by Alice and Bob for the eavesdropping check. As mentioned, in practice, as part of the QKD protocol, Alice and Bob use DR (which are, essentially, error-correcting codes) and PA (essentially, cryptographic hash functions). However, the necessity of these procedures depends on the maximal amount of information that may be obtained by an adversary. Reducing the amount of information accessible to an adversary increases the capacity of the channel and diminishes the need for error-correction and hash procedures. Hence, our game assumes no PA and DR processes are carried. Having full access to the quantum channel, Eve decides on a strategy of her choice and may intercept qubits, measure them, replace them with other qubits of her choice, apply quantum gates to qubits, etc. At the last stage of the game, Alice and Bob decide if they want to abort the game. If they do, then no one wins. If not, then all parties simultaneously announce their output. Alice outputs her key, an n-bit string $k_A = a_1 \dots a_n$, Bob outputs

his key, $k_B = b_1 \dots b_n$, and Eve outputs either $\perp$ or a pair (e, i), where i is an integer and e is a bit. Eve wins the game if $a_i = b_i = e$. This is equivalent to Eve correctly guessing a key bit.

We now describe the WM attack against BB84. Eve randomly picks $j \in \{1, \dots, 4n\}$, prepares an ancilla $|0\rangle$ qubit, applies W_ε to the j'th qubit transmitted from Alice to Bob and the ancilla, and sends Alice's qubit to Bob. Eve measures the ancilla and obtains an outcome e (illustrated in Figure 5).

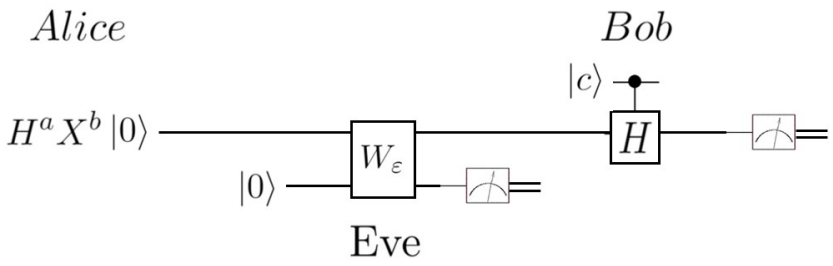

Figure 5: The weak measurement attack on BB84.

Next, Eve is listening to the discussion of Alice and Bob over the public channel and finds whether Bob measured the j'th qubit in the right basis (i.e, if $a = c$). If not, Eve outputs $\perp$. If $a = c$, then Eve keeps on listening to find whether the j'th qubit was used by Alice and Bob for eavesdrop-checking or not. If it was, then Eve outputs $\perp$. If not, then the outcome of Bob's measurement on the j'th qubit is Bob's i'th key-bit, and Eve outputs (e, i). We assume that Alice and Bob abort only if they used the bit for eavesdropping-check and got different results. Hence, if Eve delivers an output (and not $\perp$) then Alice and Bob do not abort.

We now analyze the described attack - how much information is gained by Eve, and what is the probability that Alice and Bob detect Eve's presence. We are only interested in the cases where Alice and Bob measured the j'th qubit in the same basis, i.e., $a = c$. Consider the system of two qubits where the first qubit is the qubit transmitted from Alice to Bob and the second qubit is the ancillary qubit used by Eve for the WM attack. If $a = c = 0$, then that system of two qubits is in the state

$$(1-b)\left(\sqrt{1-\varepsilon} + \sqrt{\varepsilon} \cdot i\right)|00\rangle + b \cdot \sqrt{1-\varepsilon} \cdot |10\rangle + \sqrt{\varepsilon} \cdot i \cdot b \cdot |11\rangle ,$$

and if $a = c = 1$, then the system of two qubits is in the state

$$\frac{\sqrt{1-\varepsilon}+(-1)^b\sqrt{1-\varepsilon}+i\cdot\sqrt{\varepsilon}}{2}|00\rangle + (-1)^b \cdot \frac{i\cdot\sqrt{\varepsilon}}{2}|01\rangle + \frac{\sqrt{1-\varepsilon}+i\cdot\sqrt{\varepsilon}-(-1)^b\sqrt{1-\varepsilon}}{2}|10\rangle - (-1)^b \cdot \frac{i\cdot\sqrt{\varepsilon}}{2}|11\rangle .$$

We use the probabilities of the different possible outcomes of measurements of Bob and Eve given by these states to compute the total success probability of Eve given that $a = c$ (see Figure 6).

The pairs (x, y) in the bottom of the probabilities tree indicate the outcomes of the measurements of Bob (x) and Eve (y). The numbers in the green rectangles indicate the probabilities of the cases in which Eve correctly guessed the key-bit without causing an erroneous outcome for Bob. This happens with probability $\frac{1}{2} + \frac{\varepsilon}{8}$. The numbers in the red ovals indicate the probabilities of the cases in which Eve's attack resulted in Bob measuring an erroneous result. This happens with probability $\frac{\varepsilon}{4}$, and in these cases, if Alice and Bob use this bit for eavesdropping-check, then they will detect Eve's presence and abort. The purple hexagons indicate the probabilities of the cases in which Bob gets the right result, and Eve fails in guessing the key bit. In these cases, if Alice and Bob use this bit for eavesdropping-check, they will not detect Eve's presence. We conclude that using the WM-attack described above via the W_ε gate, Eve can gain an $\frac{\varepsilon}{8}$ advantage in guessing a key-bit while reducing the risk of getting caught.

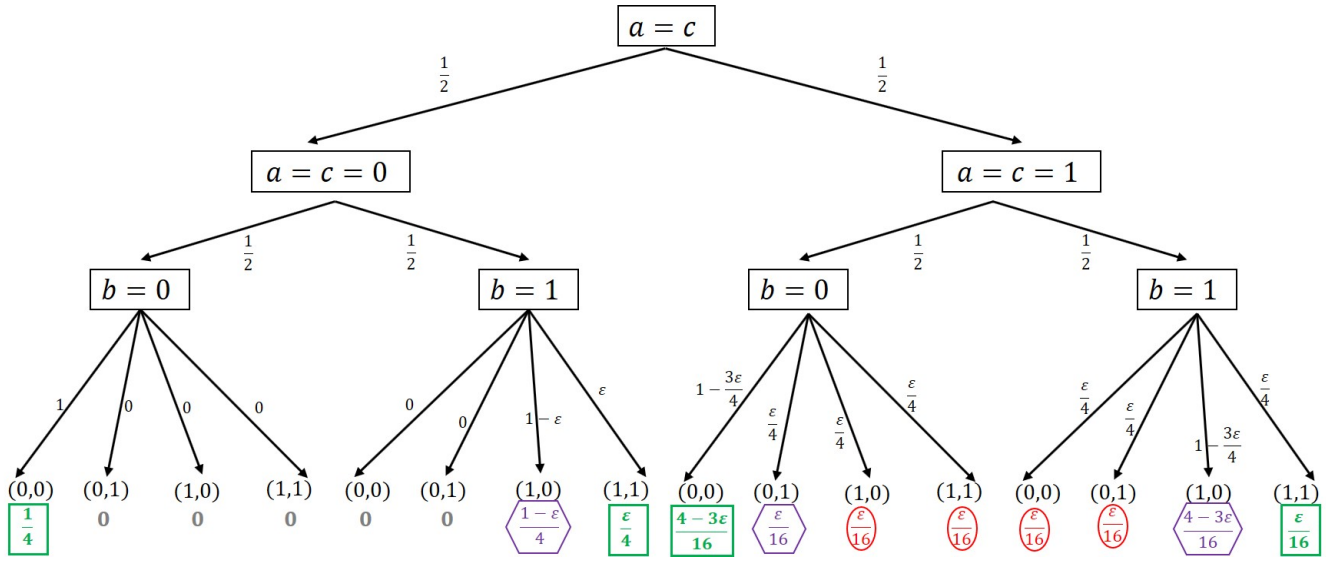

Figure 6: Probabilities of possible outcomes for the W_ε attack.

The DL04 scheme. We now briefly review the QKD scheme suggested by Deng and Long in [DL04] (hereafter, the DL04 scheme). At the first stage of the scheme, Bob picks uniformly random bits a and b and generates the qubit $H^a X^b |0\rangle$. Bob repeats the process (independently) $2n$ times and transmits the $2n$ qubits to Alice. Next, Alice randomly picks some of the qubits, say n, measures each of the selected qubits in either the standard or Hadamard basis (randomly) and announces the outcomes to Bob[1]. Next, if Bob finds that the error rate is low enough (say, no errors were found), then there are n qubits left (the ones that were not measured) with which they continue. Alice picks $c \in \{0,1\}$ and applies a c-conditioned U gate to the first qubit, where $U = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Alice repeats the process for all the n qubits she has not measured yet and sends the qubits back to Bob. The unitary U interchanges (up to a global phase factor) the elements of each of the relevant bases. I.e., $|0\rangle \overset{U}{\leftrightarrow} |1\rangle$ and $|+\rangle \overset{U}{\leftrightarrow} |-\rangle$. Knowing the a's, Bob decrypts the qubits and measures them to get $b \oplus c$, from which, knowing b, c is readily extractible. The scheme is illustrated in Figure 7.

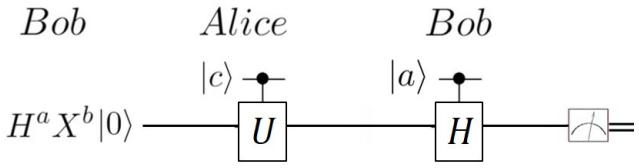

Figure 7: The DL04 scheme.

WM attack on DL04. Below we describe a WM-based attack on the DL04 scheme. This attack is based on the same idea as the attack on the BB84 scheme we described above, and uses the W_ε gate. Eve randomly picks $j \in \{1, \ldots, 2n\}$. The j'th qubit is the objective qubit for the attack. Eve prepares an ancilla $|0\rangle$ qubit, applies W_ε to the j'th qubit transmitted from Bob to Alice and the ancilla, and sends Bob's qubit to Alice. Eve measures the ancilla and obtains an outcome e_1. Next, Eve is listening to the measurement outcomes of Alice, announced over the classical public channel, and finds whether Alice measured the j'th qubit for eavesdropping check. If she did, Eve outputs $\perp$. If not, then Eve prepares another $|0\rangle$ ancilla. Denote by i to new location of the objective qubit among the n qubits that were not

[1]This scheme can also be improved at this stage by using the same idea that we mentioned at Remark 2. Instead of Alice randomly choose the measurement basis, she can tell Bob which qubits she chose, Bob will reveal the corresponding a's, and Alice will use this information to measure the qubits in the right basis. This will improve the probability of detecting possible adversarial eavesdropping attempts

measured. Eve applies W_ε to the i'th qubit transmitted from Alice to Bob and the ancilla and sends the qubit to Bob. Eve measures the (new) ancilla and obtains an outcome e_2, and outputs $(e_1 \oplus e_2, i)$. The attack is illustrated in Figure 8.

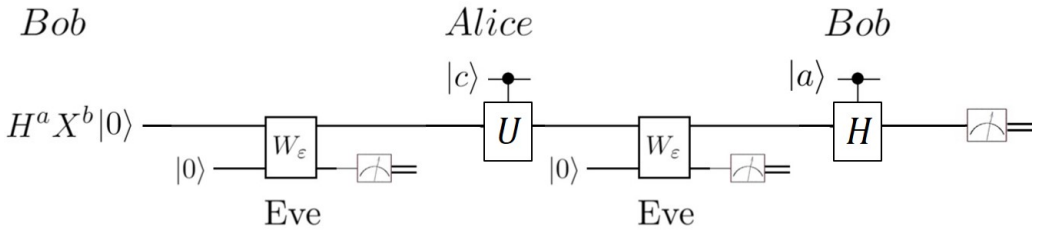

Figure 8: The WM attack on the DL04 scheme.

We now analyze the described attack - how much information is gained by Eve, and what is the probability that Alice and Bob detect Eve's presence. We begin with some intuition. As before, if $a = 0$, applying W_ε does not change the objective qubit. In these cases, Alice and Bob cannot detect Eve's presence, and Eve can learn $\mathcal{O}(\varepsilon^2)$ information. The exponent 2 comes from the fact that Eve should correctly detect the state in both directions. When $a = 1$, Eve gets no information but only slightly disturbs the state.

First, we consider the case in which Alice used the objective qubit (the one chosen by Eve), for eavesdropping check. In this case, Eve outputs $\perp$. However, what is the probability that Alice and Bob Detect Eve's presence on the line? Observe that this case (partly illustrated at the left part of Figure 8), is completely identical to the BB84 case described above (illustrated in Figure 5). Here, Bob is the one that generates one of the four qubits $|0\rangle, |1\rangle, |+\rangle$ or $|-1\rangle$ (with probability $\frac{1}{4}$ each), Eve's attack is identical (applying W_ε with an ancilla), and Alice is the one who measures in the standard or Hadamard basis. As computed above, the probability that Alice and Bob disagree (and hence detect Eve's presence) is $\frac{\varepsilon}{4}$.

Next, we consider the case in which Alice did not choose the objective qubit for the eavesdropping check. Now, Alice applies a c conditioned U to the objective qubit and transmits it back to Bob. Eve applies a second to the objective qubit with an ancilla and measures the ancilla to obtain an outcome e_2. What is the probability that Eve's guess on c is correct, i.e., $e_1 \oplus e_2 = c$? We have

Lemma 3. The probability that Eve's guess is correct is $\frac{1}{2} + \frac{6\varepsilon^2 - 3\varepsilon^3}{16 - 8\varepsilon}$.

The proof of Lemma 3 may be found in the appendix. To conclude, using our WM attack on DL04, Eve can get an $\mathcal{O}(\varepsilon^2)$ advantage guessing Alice's while being caught with probability $\frac{\varepsilon}{4}$.

Our scheme. The random basis encryption scheme 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 string of n classical bits $b = b_1 \dots b_n \in \{0,1\}^n$, and wishes to send b privately to Bob. To this end, Alice and Bob may follow the following scheme (illustrated in Figure 9).

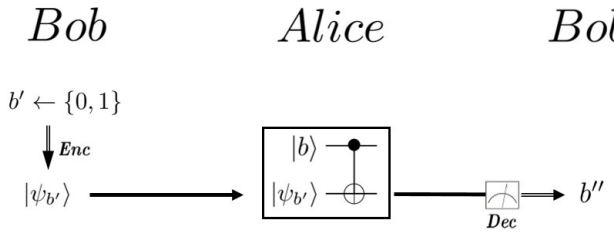

Figure 9: Sharing Key by Random Basis.

The two-stage random basis $CNOT$-QKD scheme.

1) Bob randomly picks $b' = b'_1 \dots b'_{2n}$ from $\{0,1\}^{2n}$.
2) For $1 \leq i \leq 2n$, Bob uses the random basis encryption scheme to generate an (independent) encryption $|\psi_{b'_i}\rangle$ of b'_i, and transmits $|\psi_{b'_i}\rangle$ to Alice.
3) Alice randomly picks n of the qubits received from Bob. She calls Bob over a public channel, announces the positions of the qubits she chose, and Bob reveals the keys used for encrypting these qubits.
4) Alice decrypts the n qubits she chose, using the keys obtained at the previous stage, and announces the outcomes to Bob, which in turn, checks the correctness of the outcomes to detect possible adversarial eavesdropping attempts. If the error rate is small enough, they proceed to the next stage.
5) Alice now uses the n qubits that she did not measure at the previous stage, and for $1 \leq i \leq n$, if $b_i = 1$ Alice applies a NOT gate to the i'th qubit; otherwise, she leaves it unchanged.
6) Alice sends the n qubits that were not measured by her back to Bob, who decrypts them and obtains a string, b''.
7) Denote by $\tilde{b} \in \{0,1\}^n$ the n-bit string obtained from b' after omitting the n bits chosen by Alice at stage 3. Bob computes $b'' \oplus \tilde{b}$ to obtain b.

The correctness and security of the scheme follows directly from the security of the random basis encryption scheme. However, unlike the BB84 and DL04 schemes, our scheme is resilient against WM attacks. The WM attacks described above rely on the fact that in both the BB84 and DL04 schemes, in 50% of the cases the objective qubit is in the standard basis, and in these cases, an adversary can copy and measure the qubit without disturbing it. The disturbance (and hence, the possibility of being caught) occurs only when the qubit is in the Hadamard basis. In the WM attacks, the adversary can control the probability of getting caught by the choice of ε. In our scheme, a qubit is in the standard basis 0% of the time, which leaves no room for any kind of adversarial attempts.

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 discussed its homomorphic properties. The homomorphic operations that we support are supported by our scheme in an efficient, fully compact, non-interactive, perfectly correct, and IT-secure way and most importantly, with safer security in the face of adversarial attacks based on weak measurements.

We have suggested a protocol enabling two distant parties to securely obtain an entangled pair, and to secure stored entangled qubits. In so doing, we first brought up the concept of securing the resource of entanglement. We demonstrated how our scheme might be used to establish a symmetric key by a two-stage random basis QKD scheme. We believe that our new approach and techniques suggest a possible direction for future research on IT-secure quantum homomorphic encryption and quantum computation and information.

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.

[ABL64] Yakir Aharonov, Peter G. Bergmann, and Joel L. Lebowitz. Time symmetry in the quantum process of measurement. *Phys. Rev.*, 134:B1410–B1416, Jun 1964.

[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.

[BP12] Samuel L Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Physical review letters*, 108(13):130502, 2012.

[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.

[ED01] Avshalom C. Elitzur and Shahar Dolev. Nonlocal effects of partial measurements and quantum erasure. *Phys. Rev. A*, 63:062109, May 2001.

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

[GDL+10] GG Gillett, RB Dalton, BP Lanyon, MP Almeida, Marco Barbieri, Geoff J Pryde, JL OâĂŹbrien, KJ Resch, SD Bartlett, and AG White. Experimental feedback control of quantum systems using weak measurements. *Physical review letters*, 104(8):080503, 2010.

[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.

[GLLP04] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004.

[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.

[HK08] Onur Hosten and Paul Kwiat. Observation of the spin hall effect of light via weak measurements. *Science*, 319(5864):787–790, 2008.

[JK10] Andrew N Jordan and Alexander N Korotkov. Uncollapsing the wavefunction by undoing quantum measurements. *Contemporary Physics*, 51(2):125–147, 2010.

[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.

[LSMLYWW15] Wang Le, Zhao Sheng-Mei, Gong Long-Yan, and Cheng Wei-Wen. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum. *Chinese Physics B*, 24(12):120307, 2015.

[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.

[TF17] James E Troupe and Jacob M Farinholt. Quantum cryptography with weak measurements. *arXiv preprint arXiv:1702.04836*, 2017.

[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.

[Wan05] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, 94(23):230503, 2005.

[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 can 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 — proof of Lemma 2

Proof. We begin with some notations regarding the WM attack on DL04 described above. Recall that, at the first stage of DL04, Bob chooses $a, b \in \{0,1\}$ uniformly at random and sends $H^a X^b |0\rangle$ to Alice. We denote by $|\psi_1\rangle$ the two qubit system whose first qubit is the qubit sent from Bob to Alice, and the second qubit of $|\psi_1\rangle$ is Eve's (first) $|0\rangle$ ancilla. Namely, $|\psi_1\rangle = (H^a X^b |0\rangle) \otimes |0\rangle$. $|\psi_2\rangle$ denotes $W_\varepsilon |\psi_1\rangle$. Recall that Eve measures the right qubit of $|\psi_2\rangle$ to obtain e_1. We denote by $|\psi_3\rangle$ the two-qubit system whose left qubit is the left qubit of $|\psi_2\rangle$ after Eve measures the right qubit of $|\psi_2\rangle$, and the right qubit of $|\psi_3\rangle$ is Eve's new $|0\rangle$ ancilla. $|\psi_4\rangle$ is the system obtained from $|\psi_3\rangle$ after Alice applies a c-conditioned U to its left qubit. $|\psi_5\rangle$ denotes $W_\varepsilon |\psi_4\rangle$. These notations are illustrated at Figure 10.

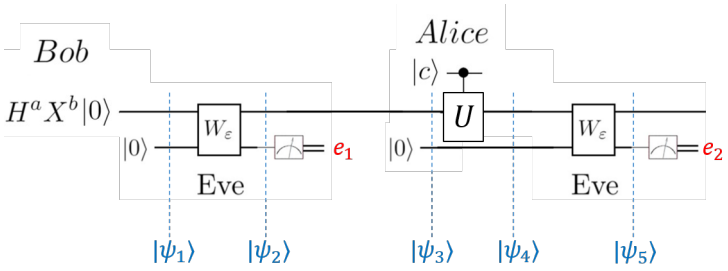

Figure 10: The WM attack on DL04.

Recall that Eve measures the right qubit of $|\psi_5\rangle$ to obtain e_2. Eve's guess is $e_1 \oplus_2$. The guess is correct if $e_1 \oplus e_2 = c$. To compute the probability of Eve guessing c correctly we examine all the possibilities for $(a, b, c) \in \{0,1\}^3$. Each possibility occurs with probability $\frac{1}{8}$ (We assume that c is chosen uniformly at random).

- First case: $a = 0$.
  - Assume $(b, c) = (0, 0)$. In this case, $|\psi_1\rangle = |00\rangle$, and hence $|\psi_2\rangle = W_\varepsilon |\psi_1\rangle = \sqrt{\varepsilon} i \cdot CNOT + \sqrt{1-\varepsilon} \cdot I \otimes I |00\rangle = |00\rangle$. Next, Eve measures the right qubit of $|\psi_2\rangle$ and obtains $e_1 = 0$ with probability 1. Now, $|\psi_3\rangle = |00\rangle$, and since $c = 0$, we have $|\psi_4\rangle = |00\rangle$ and $|\psi_5\rangle = |00\rangle$ as well. Measuring the right qubit of $|\psi_5\rangle$ Eve obtains $e_2 = 0$ with probability 1, which implies that Eve's guess in this case is $e_1 \oplus e_2 = 0 \oplus 0 = 0$. Since here $c = 0$, the guess is correct. This contributes $\frac{1}{8}$ to the total success probability.
  - Assume $(b, c) = (0, 1)$. Here, e_1 and $|\psi_3\rangle$ are the same as in the previous case since Alice's choice of c is only reflected at $|\psi_4\rangle$. Now, $|\psi_4\rangle = |10\rangle$, and hence $|\psi_5\rangle = W_\varepsilon |10\rangle = i\sqrt{\varepsilon} |11\rangle + \sqrt{1-\varepsilon} |10\rangle$. When Eve measures the right qubit of $|\psi_5\rangle$ she obtains the outcome $e_2 = 1$ with probability ε, and the outcome $e_2 = 0$ is obtained with probability $1 - \varepsilon$. The former possibility implies a correct guess (since $e_1 \oplus e_2 = 0 \oplus 1 = 1 = c$), which contributes $\frac{\varepsilon}{8}$ to the total success probability.
  - Assume $(b, c) = (1, 0)$. Here, $|\psi_1\rangle = |10\rangle$. Now, $|\psi_2\rangle = W_\varepsilon |10\rangle = i\sqrt{\varepsilon} |11\rangle + \sqrt{1-\varepsilon} |10\rangle$. Measuring the right qubit of $|\psi_1\rangle$ Eve obtains $e_1 = 1$ with probability ε and $e_1 = 0$ with probability $1 - \varepsilon$. Either way, $|\psi_4\rangle = |10\rangle$ and $|\psi_5\rangle = i\sqrt{\varepsilon} |11\rangle + \sqrt{1-\varepsilon} |10\rangle$. Measuring the right qubit of $|\psi_5\rangle$, Eve obtains $e_2 = 1$ with probability ε and $e_2 = 0$ with probability $1 - \varepsilon$. Since $c = 0$, the correct guesses come from the cases where $(e_1, e_2) = (0, 0)$ or $(e_1, e_2) = (1, 1)$. The former possibility has probability of $(1 - \varepsilon)^2$, and the latter occurs with probability ε^2. This contributes $\frac{(1-\varepsilon)^2}{8} + \frac{\varepsilon^2}{8} = \frac{1-2\varepsilon+2\varepsilon^2}{8}$ to the total success probability.
  - Assume $(b, c) = (1, 1)$. Since Alice's choice of c is only reflected at $|\psi_4\rangle$, the probabilities for e_1 are as in the previous case, and $|\psi_3\rangle = |10\rangle$. Here $c = 1$, and hence $|\psi_4\rangle = |00\rangle$, which implies that $|\psi_5\rangle = W_\varepsilon |00\rangle = |00\rangle$. Measuring the right qubit of $|\psi_5\rangle$, Eve obtains the outcome $e_2 = 0$ with probability 1. If $e_1 = 1$ was obtained before, then Eve's guess is correct since

$1 \oplus 0 = 1$. Since the outcome $e_1 = 1$ is obtained with probability ε we conclude that this case contributes $\frac{\varepsilon}{8}$ to the total success probability.

All in all, the contribution of the case $a = 0$ to the total success probability is

$$\tfrac{1}{8} + \tfrac{2\varepsilon}{8} + \tfrac{(1-\varepsilon)^2}{8} + \tfrac{\varepsilon^2}{8} = \tfrac{1}{4} + \tfrac{\varepsilon^2}{8}.$$

- Second case: $a = 1$. First, we note that the left qubit of $|\psi_1\rangle$ is $H^a X^b |0\rangle = H|b\rangle = |0\rangle + (-1)^b |1\rangle$. If $b = 0$ then the left qubit of $|\psi_1\rangle$ is $|+\rangle$, and if $b = 1$ then it is $|-\rangle$. We write $|\psi_1\rangle = |\pm\rangle |0\rangle$. Now, $|\psi_2\rangle = W_\varepsilon |\pm\rangle |0\rangle = W_\varepsilon\Big(\frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{\sqrt{2}}|10\rangle\Big)$. Recall that $W_\varepsilon = \sqrt{\varepsilon} i \cdot CNOT + \sqrt{1-\varepsilon} \cdot I \otimes I$. We have

$$|\psi_2\rangle = \sqrt{1-\varepsilon}\Big(\tfrac{1}{\sqrt{2}}|00\rangle \pm \tfrac{1}{\sqrt{2}}|10\rangle\Big) + i\sqrt{\varepsilon}\Big(\tfrac{1}{\sqrt{2}}|00\rangle \pm \tfrac{1}{\sqrt{2}}|11\rangle\Big).$$

Rearranging, we get

$$|\psi_2\rangle = \tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}|00\rangle \pm \tfrac{\sqrt{1-\varepsilon}}{\sqrt{2}}|10\rangle \pm i\tfrac{\sqrt{\varepsilon}}{\sqrt{2}}|11\rangle.$$

Measuring the right qubit of $|\psi_2\rangle$, Eve obtains the outcome $e_1 = 1$ with probability $\frac{\varepsilon}{2}$, regardless of b. The outcome $e_1 = 0$ is obtained with probability $1 - \frac{\varepsilon}{2}$. We examine each possibility.

  - If the outcome $e_1 = 1$ was obtained (which happens with probability $\frac{\varepsilon}{2}$) then the left qubit of $|\psi_2\rangle$ collapses to $|1\rangle$. Now, there are two possibilities for c.
    - If $c = 1$ then $|\psi_4\rangle = |00\rangle$, which implies that $|\psi_5\rangle = |00\rangle$ as well. Measuring the right qubit of $|\psi_5\rangle$ Eve obtains the outcome $e_2 = 0$ with probability 1. Since we assume here $e_1 = 1$, Eve's guess, $1 \oplus 0 = 1$, is correct. This contributes $\frac{\varepsilon}{8}$ to the total success probability.
    - If $c = 0$ then $|\psi_4\rangle = |10\rangle$, which implies that $|\psi_5\rangle = W_\varepsilon|10\rangle = i\sqrt{\varepsilon}|11\rangle + \sqrt{1-\varepsilon}|10\rangle$. Measuring the right qubit of $|\psi_5\rangle$, Eve obtains the outcome $e_2 = 1$ with probability ε, which compels a correct guess, $1 \oplus 1 = 0 = c$. This contributes $\frac{\varepsilon^2}{8}$ to the total success probability.

  - If the outcome $e_1 = 0$ was obtained (which happens with probability $1 - \frac{\varepsilon}{2}$) then the left qubit of $|\psi_2\rangle$ collapses to

$$\frac{\frac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}|0\rangle \pm \frac{\sqrt{1-\varepsilon}}{\sqrt{2}}|1\rangle}{\Big\|\frac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}|0\rangle \pm \frac{\sqrt{1-\varepsilon}}{\sqrt{2}}|1\rangle\Big\|}.$$

    Using routine algebraic manipulations and joining Eve's (new) $|0\rangle$ ancilla we get

$$|\psi_3\rangle = \sqrt{\tfrac{2}{2-\varepsilon}}\Big(\tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}|00\rangle + \tfrac{\sqrt{1-\varepsilon}}{\sqrt{2}}|10\rangle\Big).$$

    Now, there are two possibilities for c.
    - If $c = 0$ then $|\psi_4\rangle = |\psi_3\rangle$. In this case, since $|\psi_5\rangle = W_\varepsilon|\psi_4\rangle$ we get

$$|\psi_5\rangle = \tfrac{\sqrt{2-2\varepsilon}}{\sqrt{2-\varepsilon}}\Big(\tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}|00\rangle + \tfrac{\sqrt{1-\varepsilon}}{\sqrt{2}}|10\rangle\Big) + \tfrac{i\sqrt{2\varepsilon}}{\sqrt{2-\varepsilon}}\Big(\tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}|00\rangle + \tfrac{\sqrt{1-\varepsilon}}{\sqrt{2}}|11\rangle\Big).$$

      We rearrange $|\psi_5\rangle$ by the standard basis elements and see that the coefficient of $|11\rangle$ is $\frac{i\sqrt{2\varepsilon}}{\sqrt{2-\varepsilon}} \cdot \frac{\sqrt{1-\varepsilon}}{\sqrt{2}}$and the coefficient of $|01\rangle$ in $|\psi_5\rangle$ is 0. Hence, measuring the right qubit of

$|\psi_5\rangle$ Eve obtains the outcome $e_2 = 1$ with probability $\alpha := \frac{\varepsilon(1-\varepsilon)}{2-\varepsilon}$. Hence, the outcome $e_2 = 0$ is obtained with probability $1 - \alpha$. If that happens, we have $e_1 \oplus e_2 = 0 \oplus 0 = 0$, which yields a correct guess. This contributes $\frac{1}{4}(1-\frac{\varepsilon}{2})(1-\alpha)$ to the total success probability.

$*$ If $c = 1$ then Alice applies U to the left qubit of $|\psi_3\rangle$ and hence

$$|\psi_4\rangle = \sqrt{\tfrac{2}{2-\varepsilon}}\Big(\tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}\,|10\rangle + \tfrac{\sqrt{1-\varepsilon}}{\sqrt{2}}\,|00\rangle\Big).$$

Now, $|\psi_5\rangle = W_\varepsilon\,|\psi_4\rangle$. Here we get

$$|\psi_5\rangle = \sqrt{\tfrac{2-2\varepsilon}{2-\varepsilon}}\Big(\tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}\,|10\rangle + \tfrac{\sqrt{1-\varepsilon}}{\sqrt{2}}\,|00\rangle\Big) + i\sqrt{\tfrac{2\varepsilon}{2-\varepsilon}}\Big(\tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}\,|11\rangle + \tfrac{\sqrt{1-\varepsilon}}{\sqrt{2}}\,|00\rangle\Big).$$

Measuring the right qubit of $|\psi_5\rangle$ Eve obtains the outcome $e_2 = 1$ with probability

$$\beta = \Big|i\sqrt{\tfrac{2\varepsilon}{2-\varepsilon}} \cdot \tfrac{\sqrt{1-\varepsilon}+i\sqrt{\varepsilon}}{\sqrt{2}}\Big|^2 = \tfrac{\varepsilon}{2-\varepsilon}.$$

In this case we get $e_1 \oplus e_2 = 0 \oplus 1 = c$, which yields a correct guess. This contributes $\frac{\beta}{4}(1 - \frac{\varepsilon}{2})$ to the total success probability.

All in all, the contribution of the case $a = 1$ to the total success probability is

$$\tfrac{\varepsilon}{8} + \tfrac{\varepsilon^2}{8} + \tfrac{1}{4}(1 - \tfrac{\varepsilon}{2})(1 - \alpha) + \tfrac{\beta}{4}(1 - \tfrac{\varepsilon}{2}).$$

Using routine algebraic manipulations, the reader may readily verify that the contributions of the cases $a = 0$ and $a = 1$ add up to a total success probability of $\frac{1}{2} + \frac{6\varepsilon^2-3\varepsilon^3}{8(2-\varepsilon)}$. $\square$