Experimental Demonstration of Quantum Fully Homomorphic Encryption with Application in a Two-Party Secure Protocol

W. K. Tham,[1,*] Hugo Ferretti,[1] Kent Bonsma-Fisher,[1] Aharon Brodutch,[1,2] Barry C. Sanders,[3,4,5] Aephraim M. Steinberg,[1,5] and Stacey Jeffery[6]

[1]*Department of Physics and Center for Quantum Information and Quantum Control, University of Toronto, 60 St. George Street, Toronto, Ontario, M5S 1A7, Canada*
[2]*The Edward S. Rogers Department of Electrical and Computer Engineering, University of Toronto, 10 Kings College Road, Toronto, Ontario M5S 3G4, Canada*
[3]*Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*
[4]*Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, USA*
[5]*Canadian Institute for Advanced Research, Toronto, Ontario M5G 1M1, Canada*
[6]*QuSoft and CWI, Amsterdam 1098 XG, Netherlands*

(Received 12 November 2018; revised manuscript received 9 August 2019; accepted 19 November 2019; published 18 February 2020)

A fully homomorphic encryption system hides data from unauthorized parties while still allowing them to perform computations on the encrypted data. Aside from the straightforward benefit of allowing users to delegate computations to a more powerful server without revealing their inputs, a fully homomorphic cryptosystem can be used as a building block in the construction of a number of cryptographic functionalities. Designing such a scheme remained an open problem until 2009, decades after the idea was first conceived, and the past few years have seen the generalization of this functionality to the world of quantum machines. Quantum schemes prior to the one implemented here were able to replicate *some* features in particular use cases often associated with homomorphic encryption but lacked other crucial properties, for example, relying on continual interaction to perform a computation or leaking information about the encrypted data. We present the first experimental realization of a quantum fully homomorphic encryption scheme. To demonstrate the versatility of a a quantum fully homomorphic encryption scheme, we further present a toy two-party secure computation task enabled by our scheme.

DOI: 10.1103/PhysRevX.10.011038

Subject Areas: Optics, Quantum Physics, Quantum Information

I. INTRODUCTION

In 1978, Rivest *et al.* first imagined constructing a cryptosystem with the property that a party *without* a valid secret key required for decryption can nevertheless correctly evaluate a function f directly on a ciphertext x, without learning anything about either $f(x)$ or x [1]. In addition to the obvious benefit of being able to delegate computation to a party that is otherwise not trusted with private data, cryptographers have observed that elegant cryptographic solutions to particularly interesting tasks can be constructed on top of a fully homomorphic encryption scheme—secure multiparty computation, noninteractive zero-knowledge proofs, and one-time programs, to name a few [2–6]. Despite the apparent utility of such an encryption scheme, the question of whether it was possible to efficiently construct one remained open until 2009 when the first fully homomorphic encryption (FHE) scheme was constructed for classical machines [7].

In quantum computing, a range of works have studied the closely related problems of secure delegated quantum computing (SDQC) [8–14] wherein Alice may securely delegate a computational task to Bob (who may have a more powerful quantum computer) without revealing her data. But while SDQC is one prominent *use case* for FHE, it does not itself enable the wider gamut of cryptographic applications that a true FHE scheme is capable of. In existing SDQC schemes, Alice and Bob must be allowed to interact repeatedly as they collaborate to perform a computation. The interactions often require either that Alice be cognizant of operation(s) performed by Bob or that Bob foregoes the freedom to choose which computation to perform. These constraints make SDQC ill suited for certain applications of FHE (for example, secure multiparty computation) where

*Corresponding author.
wtham@physics.utoronto.ca

both Alice and Bob must simultaneously be afforded autonomy and privacy—each must be allowed to implement a computation of their choice while keeping private portions of their computation from each other.

Construction of a quantum fully homomorphic encryption (QFHE) scheme was explored more recently. Early QFHE proposals treated the problem in an information-theoretic setting—that is, the resulting encryption scheme must produce ciphertext that is uncrackable even given unlimited computational power. Schemes that were proposed under this model [15,16], and subsequently demonstrated experimentally [17], leaked some explicit information about the plaintext, and are therefore unacceptable under mainstream notions of security. More recent efforts relaxed the information-theoretic setting to one with computational assumptions, at first for circuits of shallow T depth (number of T gates sequentially applied) [18] and subsequently extended for circuits of arbitrary depth [19], yielding the first construction of a true QFHE scheme. Later this was improved to allow QFHE with a classical client [20].

It must be noted that cryptographic security with computational assumptions is standard in classical encryption schemes (including FHE ones), where security hinges on the assumed difficulty of computing particular problems like prime factorization of large integers (which is now known to be efficiently solvable with a quantum computer) or learning with errors (essentially a Gaussian inversion problem with noise, for which an efficient algorithm is not known even for quantum computers). So-called "postquantum" cryptographic schemes, including many classical FHE ones, are built atop problems like learning with errors. In turn, these "quantum-safe" classical FHE schemes are used to endow corresponding QFHE schemes with the necessary properties (see, e.g., Refs. [18,19], which we discuss below), as well as to construct cryptographic schemes for a variety of different settings (for example, when the input or encrypter is entirely classical [20]).

In this work, we implement and experimentally demonstrate for the first time the quantum homomorphic encryption scheme proposed by Broadbent and Jeffery [18]. This scheme was extended in Dulek *et al.* to a quantum *fully* homomorphic encryption scheme, applicable to circuits of arbitrary T depth, but is beyond the reach of current experimental techniques [19]. However, for shallow T depth circuits, the scheme of Broadbent and Jeffery suffices. For a small-scale proof-of-concept implementation, ours exhibits all the necessary attributes for a QFHE scheme and clearly illustrates its important operational features in a fully quantum setting. To illustrate the versatility of QFHE over SDQC, we demonstrated a toy problem in which two parties wish to securely compare their quantum states (which precludes, e.g., the scheme in Ref. [20]), which is easily accomplished in our construction. Various two- and three-qubit circuits in these demonstrations are implemented optically in a four-photon setup, with each qubit encoded in photon polarization and one photon serving as herald.

The remainder of this paper is structured as follows. In Sec. II, we place this work on a solid theoretical footing by first outlining the basic requirements of a QFHE scheme (Sec. II A) and then describing in detail the construction of the QFHE scheme we implemented in this work (Sec. II B). Section III describes our experimental apparatus and then proceeds to discuss data showing the core QFHE scheme at work. Finally, Sec. IV details the toy two-party computation task and discusses the experimental setup and data pertaining to it.

II. THEORY BACKGROUND

A. Basics of a homomorphic cryptosystem

A homomorphic encryption scheme derives its name from the fact that *operationally* it behaves *like* a ring homomorphism between plaintext and ciphertext (we call these ϕ and ψ, respectively)—even though, in practice, the encryption-decryption procedures are not constructed as homomorphisms *per se*. Loosely speaking, one constructs a FHE scheme such that for every valid operation on plaintexts (say, multiplication or addition) there is a well-defined operation on the corresponding ciphertexts, such that the output decrypts back to the correct intended plaintext.

In an idealized *quantum* setting where ϕ and ψ are quantum states, this might be written as $\mathcal{D}_{sk}(U'\mathcal{E}_{pk}|\phi\rangle) = \mathcal{D}_{sk}(U'|\psi\rangle) = U|\phi\rangle$, where $\mathcal{E}_{pk}$ and $\mathcal{D}_{sk}$ are encryption-decryption procedures (with keys pk and sk) Alice uses to hide $|\phi\rangle$ from Bob, U is some desired transformation on plaintext ϕ, and U' is a computation on ciphertext $|\psi\rangle$ performed by Bob to effect that desired transformation U.

In practice, whereas U are unitary operations that act on $|\phi\rangle$ only, U' can be supplanted by more complicated operations—for instance, ones that act on both $|\psi\rangle$ along with ancillary quantum as well as classical resources. This more general operation is also called the "evaluation map" (Eval), and all ancillary resources required by Bob to execute the evaluation map are called the "evaluation key," which may be a combination of classical (ζ) and quantum ($|\xi\rangle$) bits. Generally then, for *every* valid $U|\phi\rangle$, we want a corresponding evaluation map such that the output decrypts back to $U|\phi\rangle$:

$$\begin{aligned}&\mathcal{D}_{sk}\{\mathrm{Eval}(U,|\psi\rangle,|\xi\rangle,\zeta)\}\\&\quad=\mathcal{D}_{sk}\{U'(|\psi\rangle\otimes|\xi\rangle),f(\zeta)\}\\&\quad=U|\phi\rangle.\end{aligned}\tag{1}$$

Some subtle but important points worth stressing are that a QFHE scheme must be constructed so that any party (say, Bob) in possession of ciphertext $|\psi\rangle$ must be able to transform it by their choice of an arbitrary evaluation

map that corresponds to the correct operation on the underlying $|\phi\rangle$ without interacting with Alice beyond the initial exchange of ciphertext. Therefore, any attendant resource(s) (i.e., the evaluation key) required by Bob to do so must be generated by Alice at the same time as the secret key, and transmitted to him alongside $|\psi\rangle$. In SDQC applications, by contrast, this restriction becomes less important, since through interactions during the computation Bob can request these resources and Alice can supply them as and when they become necessary. Furthermore, a QFHE scheme must be compact. That is to say, the encryption and decryption operations must be easily computed even when U becomes increasingly complex. Otherwise a *trivial* QFHE solution exists where Bob, instead of manipulating $|\psi\rangle$ himself, simply returns a list of instructions that Alice must perform as part of her decoding operation.

The scheme that we experimentally implement in this work, which closely follows Broadbent and Jeffery [18], satisfies both noninteractivity and compactness as long as there is only a small, fixed number of T gates (defined below) within the quantum circuit that defines U. In Sec. II B, we describe our handling of T gates and the origins of this restriction, along with comparisons to relevant previous works. The astute reader will recognize difficulties with T gates in the quantum setting as being somewhat analogous to the case of multiplication operations in *classical* homomorphic schemes, that were subsequently resolved in Ref. [7]. In the quantum setting, restrictions on the number of T gates were removed by Dulek *et al.*, but experimental implementation of that scheme is beyond reach at present [19].

B. QFHE scheme

The workhorse of our encryption scheme is the Pauli mixing operation $\mathcal{E}_{\vec{a},\vec{b}}|\phi\rangle = Z^{\vec{a}}X^{\vec{b}}|\phi\rangle$. Here, $|\phi\rangle$ is an arbitrary n-qubit plaintext state, $\vec{a},\vec{b} \in \{0,1\}^n$ are two classical n bit strings, and Z and X are standard Pauli operators. The notation $Z^{\vec{a}}X^{\vec{b}}$ is to be interpreted as $\otimes_k Z^{a_k}X^{b_k} = (Z^{a_1}X^{b_1}) \otimes \cdots \otimes (Z^{a_n}X^{b_n})$. If $\vec{a}$ and $\vec{b}$ are randomly selected from a uniform distribution on each use or shot, then they serve as single-use encryption keys or one-time pads. To an eavesdropper with no access to $\vec{a}$ and $\vec{b}$, the resulting state appears to have been drawn from the fully mixed or random state that bears no resemblance to the original plaintext $|\phi\rangle$ [21]:

$$\sum_{\vec{a},\vec{b}} \frac{1}{2^{2n}} Z^{\vec{a}}X^{\vec{b}}|\phi\rangle\langle\phi|Z^{\vec{a}}X^{\vec{b}} = \mathcal{I}_n/2^n, \tag{2}$$

where $\mathcal{I}_n$ is the $2^n \times 2^n$ identity matrix.

This approach has a desirable property in relation to Clifford gates (i.e., unitary operators generated by the set $\{X, Y, Z, H, \text{CNOT}\}$; see Fig. 1 for definitions). Invariance

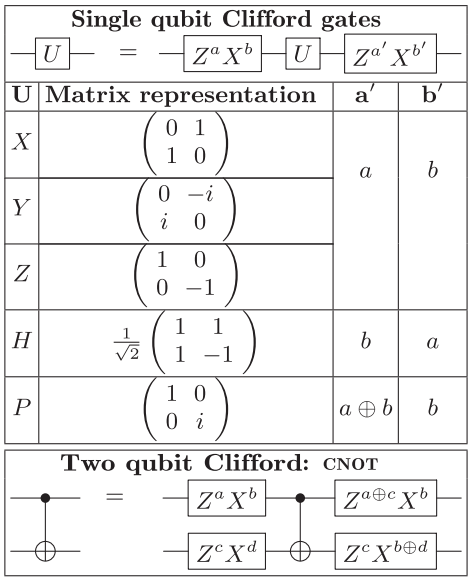

FIG. 1. Key transformation under Clifford gates. In circuit diagrams above, Z^aX^b and $Z^{a'}X^{b'}$ are encrypting and decrypting maps performed by Alice. The symbol $\oplus$ denotes addition modulo 2.

of the Pauli group under conjugation by Clifford operators means that decrypting a ciphertext that had been modified by a Clifford gate requires only Pauli gates. Suppose Alice prepares quantum ciphertext $|\psi\rangle = \mathcal{E}_{\vec{a},\vec{b}}|\phi\rangle = Z^{\vec{a}}X^{\vec{b}}|\phi\rangle$ and sends it to Bob who acts on it with a unitary U before returning it to Alice (we momentarily drop the prime in U' that distinguishes between ciphertext and plaintext quantum operations—for Clifford gates, they are the same). If $U = U_c$ is a Clifford gate, then Alice decodes the result simply by applying another pair of Pauli operators:

$$\begin{aligned}\mathcal{D}_{\vec{a}',\vec{b}'}(U_c|\psi\rangle) &= \mathcal{D}_{\vec{a}',\vec{b}'}(U_c Z^{\vec{a}}X^{\vec{b}}|\phi\rangle) \\ &= Z^{\vec{a}'}X^{\vec{b}'}U_c Z^{\vec{a}}X^{\vec{b}}|\phi\rangle \\ &= U_c|\phi\rangle,\end{aligned} \tag{3}$$

where $\vec{a}'$ and $\vec{b}'$ are decryption keys (see Fig. 1).

Pauli mixing had previously been discussed and used in SDQC schemes [8,14,21]. In this work, as in Broadbent and Jeffery [18], we introduce the following important additions to elevate it to a homomorphic scheme. As she prepares $|\psi\rangle$, Alice also prepares and sends to Bob as follows.

(1) Addition no. 1. Her Pauli keys $(\vec{a},\vec{b})$, encrypted with a *classical* homomorphic encryption scheme (call this Enc). Bob modifies $\text{Enc}(\vec{a},\vec{b})$ appropriately as he performs his computation on $|\psi\rangle$.
(2) Addition no. 2. Ancillary qubits $|\xi\rangle$ that depend only on her Pauli keys $(\vec{a},\vec{b})$. In performing his computation on $|\psi\rangle$, these ancillary qubits are either

consumed or discarded, as necessitated by Bob's evaluation map.

It is important to emphasize that the additional resources $|\xi\rangle$ and $\mathrm{Enc}(\vec{a},\vec{b})$ are prepared by Alice in a front-loaded fashion, *at the same time* as $|\psi\rangle$, and transmitted to Bob all at once so that further interactions between Bob and Alice will not be necessary. Below we elaborate on the purpose of these additional resources.

1. Addition no. 1

Notice, from Eq. (3) and Fig. 1, that decryption keys $(\vec{a}',\vec{b}')$ are determined both by the encryption keys $(\vec{a},\vec{b})$ (which only Alice knows) and U (which Bob performs). In a SDQC setting where Alice knows ahead of time which operation(s) Bob performs or otherwise learns about it as they interact during the computation, this is not a problem (cf. Refs. [8,14]). In a QFHE setting where Alice does not *a priori* know Bob's choice of operation(s), we must engineer a means for her to acquire them at the end of Bob's computation.

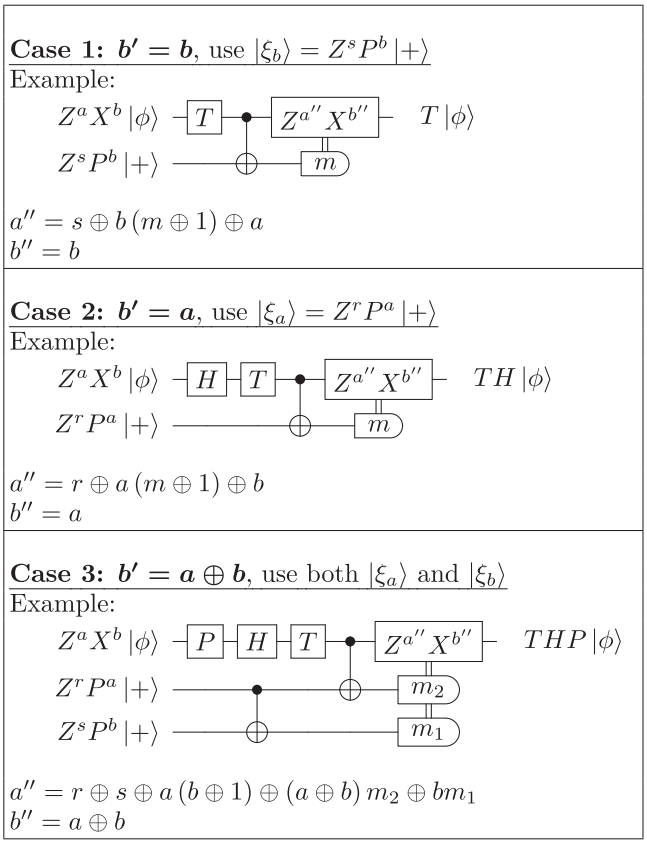

FIG. 2. The ancilla qubit(s) usage in three canonical cases for single-qubit Clifford sequences followed by a T gate. By a' and b' we denote the result of transforming decryption keys a and b in accordance with Fig. 1 for every Clifford operation that precedes the T gate (which here are the gate sequences T, TH, and THP). Here, $r,s \in \{0,1\}$ are random bits that secure $|\xi_a\rangle$ and $|\xi_b\rangle$, respectively.

In making addition no. 1, we are leveraging the existence of a classical FHE [7,22] scheme to allow Bob to modify Alice's decryption keys as necessary so that they remain valid regardless of his choice of operation(s). Since Enc is chosen to be homomorphic, Bob can transform an encrypted representation of Alice's Pauli encryption keys, $\mathrm{Enc}(\vec{a},\vec{b})$, to the corresponding decryption keys, $\mathrm{Enc}(\vec{a}',\vec{b}')$, without actually *knowing* what those keys are. When the computation is done, Bob returns $\mathrm{Enc}(\vec{a}',\vec{b}')$ to Alice, who decrypts it to obtain $(\vec{a}',\vec{b}')$, whereupon she can decrypt $U'|\psi\rangle$. The necessary transformation(s) from $\mathrm{Enc}(\vec{a},\vec{b}) \to \mathrm{Enc}(\vec{a}',\vec{b}')$ are enumerated in Fig. 1 (if Bob chooses to perform a Clifford gate) and Fig. 2 (if he performs a non-Clifford T gate; we discuss this case in the next section). Since in a QFHE setting adversaries are assumed to have quantum computing capabilities, it is important for us to note that our choice of Enc, an existing classical FHE scheme based on the learning-with-errors problem, is widely believed (though not *proven*) to be secure even against such a quantum-capable adversary [23].

2. Addition no. 2

In addition to Clifford gates, a universal quantum computer must be complemented by at least one non-Clifford element [24]. A standard choice that we use in this work is the T gate ($T = |0\rangle\langle 0| + e^{i\pi/4}|1\rangle\langle 1|$). Unlike Clifford operators, unfortunately, the T gate does *not* generally preserve the Pauli group by conjugation. Therefore, Bob's operating on Alice's ciphertext with a T gate may introduce an erroneous phase that must be corrected:

$$\begin{aligned} T|\psi\rangle &= T(Z^a X^b |\phi\rangle) \\ &= P^b Z^a X^b (T|\phi\rangle) \end{aligned} \tag{4}$$

(for convenience of exposition, we drop the vector notation on a and b in the remainder of this section, momentarily focusing instead on the case of single-qubit plaintexts). Since the desired plaintext operation is $T|\phi\rangle$, the term P^b that appears in the last line is extraneous and must be undone before further gates in the computation are performed or decryption is done (by Pauli gates as before).

Effecting the necessary correction $P^{\dagger b}$ without divulging b, part of Alice's encryption keys, to Bob (thereby compromising the encryption) had also been a central challenge in other works. In an early SDQC scheme [8], each time a T gate is performed, two rounds of quantum communication are necessary, during which Alice can decide (on Bob's behalf) whether or not a P gate is applied. In an improved scheme [14], the additional rounds of quantum interaction can be reduced with Alice preparing the ancillary qubit $Z^r P^b |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i(2r+b)\pi/2}|1\rangle)$ and Bob teleporting it onto $|\psi\rangle$ with the circuit in Fig. 3 (see the Appendix C for a

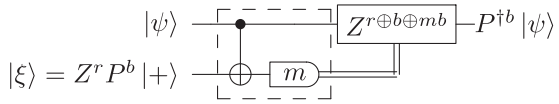

FIG. 3. Securely applying a $P^{\dagger b}$ phase correction with aid of an appropriate ancilla. Since r is a random bit, Bob (represented by dashed box) remains ignorant of Alice's key b.

derivation of the action of this circuit). Here, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $r \in \{0,1\}$ is a random bit, and b is Alice's Pauli X key. Yet another variation replaces $|\xi\rangle$ in Fig. 3 with $Z^r P^d|+\rangle$, where d is another random bit, which can be produced at the outset and supplements it with the classical bit $b \oplus d$ as needed [14].

Still, both SDQC schemes just discussed are interactive. As we have seen, any operation(s) performed by Bob on $|\psi\rangle$ potentially causes the Pauli decryption keys to change. So if a T gate is preceded by other gates, the *effective* Pauli key b' that determines whether a $P^\dagger$ correction is required generally differs from Alice's original Pauli encryption key b and is not known to her *a priori*. Therefore, she is only able to prepare the appropriate ancillary resources that Bob needs ($|\xi\rangle = Z^r P^b|+\rangle$ or classical bit $b \oplus d$) after learning about those other gates through a midcomputation round of interaction. The need for this kind of interaction, as previously discussed, is unacceptable for QFHE.

In this work (following Broadbent and Jeffery [18]), by anticipating the set of possible phase corrections, we can front-load preparation of ancillary qubits $|\xi\rangle$ so that Bob's handling of T-gate evaluations can be noninteractive. Consider an arbitrary Clifford circuit followed by a single T gate. Observe from Fig. 1 that any sequence of single-qubit Clifford gates can transform the Pauli X key in only three distinct ways: either it remains unchanged ($b' = b$) or it is swapped or added with the Pauli Z key (i.e., $b' = a$ or $b' = a \oplus b$). When a two-qubit Clifford gate (say, a CNOT) is added into the mix in an N-qubit circuit, the set of possible effective b' on the nth qubit can only be composed of *sums* (modulo 2) of all the Pauli keys:

$$b'_n = \left(\sum_{j\in A_n} a_j + \sum_{k\in B_n} b_k\right) \mod 2, \tag{5}$$

where $A_n, B_n \subseteq \{1,2,\ldots,N\}$ depend on the Clifford circuit in question.

A key enabler of our scheme is the circuit shown in Fig. 4 (see Appendix C for details on the operation of this circuit). Even though there are altogether 2^{2N} possible values for b'_n in this case, Alice need only prepare $2N$ ancillary qubits of the form $|\xi_{a_j}\rangle = Z^r P^{a_j}|+\rangle$ and $|\xi_{b_k}\rangle = Z^s P^{b_k}|+\rangle$. Here, $r, s \in \{0,1\}$ are random bits that are meant to secure $|\xi_{a_j}\rangle$ and $|\xi_{b_k}\rangle$. By selectively applying that circuit on some of these $2N$ ancillary qubits, Bob can synthesize an appropriate qubit for any one of 2^{2N} possible b'_n that takes the

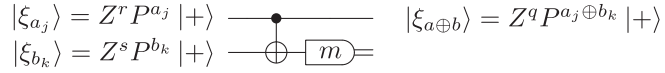

FIG. 4. Circuit to combine ancillary qubits $Z^r P^{a_j}|+\rangle$ and $Z^s P^{b_k}|+\rangle$ produces a new ancillary qubit $Z^q P^{a\oplus b}|+\rangle$. This way, Bob can generate any one of 2^{2N} possible ancillary qubits whose phase takes the form of *sums* (modulo 2) of Alice's Pauli keys a_j and b_k.

additive form of Eq. (5). Crucially, a_j and b_k are Alice's initial Pauli keys, not the decryption keys that are modified by any of Bob's operations. They are therefore known to Alice ahead of time, allowing her to front-load their preparation and avoid subsequent interactions with Bob. For the $N = 1$ case, we summarize in Fig. 2 how Bob might handle the phase correction for each of three possible

Algorithm 1. QFHE: Summary of protocol.

Alice:
1. Generate random keys and prepare ancillas.
   (a) Generate Pauli keys $\vec{a}, \vec{b} \in \{0,1\}^N$.
   (b) Generate keys pk and sk for Enc (a classical FHE scheme); call "keygen()" in HElib (see Refs. [22,25]).
   (c) Prepare sufficient set of ancillas $\{|\xi\rangle\}$ for anticipated T depth. For T depth 1, these are $|\xi_{a_j}\rangle = Z^{r_j}P^{a_j}|+\rangle$ and $|\xi_{b_k}\rangle = Z^{s_k}P^{b_k}|+\rangle$ for each $j,k \in \{1,2,\ldots,N\}$, and $r_j, s_k \in \{0,1\}$ are random bits. For greater T depths, ancillas with phases multiplicative in a_k and b_k must be anticipated and prepared (cf. Fig. 2).
2. Encrypt:
   (a) Encrypt quantum plaintext ($|\phi\rangle$): $|\psi\rangle = Z^{\vec{a}}X^{\vec{b}}|\phi\rangle$.
   (b) Encrypt Pauli keys: $(\vec{a}, \vec{b}) \to \mathrm{Enc}_{pk}(\vec{a}, \vec{b})$.
3. Send $|\psi\rangle$, $\{|\xi\rangle\}$, $\mathrm{Enc}_{pk}(\vec{a}, \vec{b})$, and pk to Bob.

Bob:
For each intended gate, $U_l \in \{U_1, U_2, \ldots, U_L\}$:
1. Apply the gate: $|\psi\rangle \to U_l|\psi\rangle$.
2. If $U_l = T$ (i.e., is non-Clifford):
   (a) Based on all preceding operations $\{U_1, U_2, \ldots, U_{l-1}\}$, generate ancilla $|\xi'\rangle$ through repeated use of circuit in Fig. 4 on $\{|\xi\rangle\}$.
   (b) Apply phase correction on $|\psi\rangle$ with circuit in Fig. 3 and $|\xi'\rangle$.
3. Homomorphically update Pauli keys:

$$\mathrm{Enc}_{pk}(\vec{a}, \vec{b}) \xrightarrow{U_1} \mathrm{Enc}_{pk}(\vec{a}', \vec{b}') \xrightarrow{U_2} \mathrm{Enc}_{pk}(\vec{a}'', \vec{b}'') \cdots$$

   If U_l is Clifford, update rules are shown in Fig. 1. If $U_l = T$, they are shown in Fig. 2 for T depth 1 circuits. Update rules for greater T depth circuits can be inferred from those.
4. Return $|\psi\rangle$ and final set of Pauli keys $\mathrm{Enc}_{pk}(\vec{a}'', \vec{b}'')$.

Alice:
1. Decrypt Pauli keys: $\mathrm{Enc}_{pk}(\vec{a}'', \vec{b}'') \to (\vec{a}'', \vec{b}'')$.
2. Decrypt $|\psi\rangle$: $Z^{\vec{a}''}X^{\vec{b}''}|\psi\rangle = U_L \ldots U_3 U_2 U_1|\phi\rangle$.

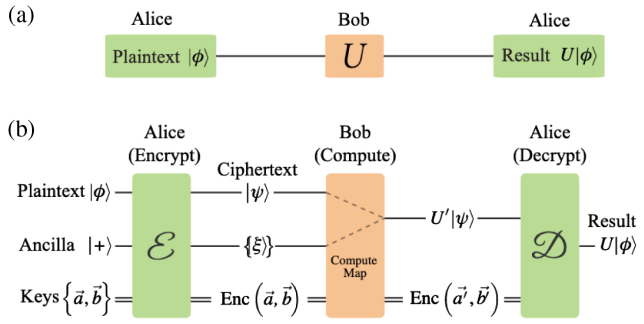

FIG. 5. Diagram of our QFHE scheme. (a) The intended computation U performed by Bob directly on plaintext $|\phi\rangle$. (b) The same computation U performed via QFHE. Here $\mathcal{E}$ and $\mathcal{D}$ are encryption and decryption operations. The computational map performed by Bob is a quantum channel that depends on the intended computation on U, and consumes some ancillas $|\xi\rangle$ in the process. Classically homomorphically encrypted Pauli keys $\mathrm{Enc}(\vec{a},\vec{b})$ are modified along the way. Alice decrypts $\mathrm{Enc}(\vec{a},\vec{b})$, which allows her to decrypt $|\psi\rangle$ and obtain the desired output $U|\phi\rangle$.

values of b' (which correspond to the gate sequences T, TH, and THP) with just two ancillary qubits from Alice.

Thus far, we have only discussed our QFHE scheme in the context of pure Clifford circuits followed by a lone T gate. The case of circuits with greater T depth (i.e., number of layers of T gates sequentially applied) is more complicated. After a T gate had been applied, multiplicative terms in the updated Pauli keys (see Fig. 2) can appear and b' may no longer take the form of Eq. (5). If Bob subsequently performs another T gate, he may no longer be able to synthesize the correct state to perform post-T-gate phase corrections from just the $2N$ ancillary qubits discussed above. If the T depth of Bob's intended circuit is bounded ahead of time, Alice can still anticipate all possible phase corrections and prepare the necessary minimal set of ancillas that Bob may need. However, the number of possibilities grows doubly exponentially quickly with T depth, making our scheme unsuitable for deep circuits. A clever trick by Dulek *et al.* gets around this limitation, but its experimental implementation is currently out of reach [19].

For the purposes of our proof-of-principle experimental implementation, we content ourselves with a demonstration of the smallest nontrivial case—that of a Clifford sequence and a single T gate, on three qubits (one data or plaintext and two ancillary qubits). We believe that this sufficiently illustrates the main mechanisms by which our QFHE scheme operates. Algorithm 1 and Fig. 5 summarize the full QFHE scheme being implemented.

III. EXPERIMENTAL REALIZATION

We implemented the core QFHE protocol described above in Sec. II B in an optical setup. Our implementation accommodates a total of three (1 data and 2 ancilla) logical qubits and is capable of performing arbitrary single-qubit rotations, but is limited to a single two-qubit gate per pair of qubits and to circuits of T depth one (i.e., no cascaded T gates). These latter restrictions are simply due to the limited scale of the specific setup we constructed in our laboratory, and do not imply any fundamental limitation of the protocol in general.

Qubits in our implementation are encoded in the polarization degree of freedom (d.o.f.) of photons. Single-qubit gates are realized using standard birefringent polarization optics. Two-qubit gates, specifically controlled-X (CNOT) and controlled-Z gates, are implemented postselectively by leveraging bosonic bunching or the Hong-Ou-Mandel (HOM) effect [26–29]. Figure 6 shows a schematic of our optical apparatus. The apparatus is discussed in further detail in Sec. III B.

Photons in our experiment are produced in a type-I spontaneous parametric down-conversion (SPDC) source. The source is a 2-mm-thick BBO crystal pumped with 404-nm blue light in a double-pass configuration (the blue pump is retroreflected to pass through the BBO crystal a second time, so that SPDC can occur on both the forward and reverse passes). Down-converted 808-nm photons are collected at an opening angle of 3° on both passes (see Fig. 7). The 404-nm SPDC pump is generated via second harmonic generation, which is itself pumped with a Ti:sapphire laser (Coherent Chameleon Ultra) configured to pulse with a repetition rate of 80 MHz, center wavelength

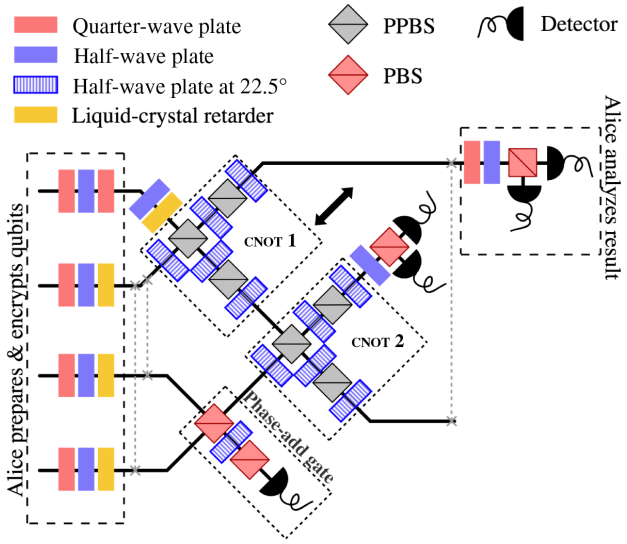

FIG. 6. Schematic of optical circuit designed to implement each canonical case enumerated in Fig. 2. Each incoming rail from the left is a separate photon from a SPDC event (see Fig. 7 for source schematic). Liquid-crystal retarders allow us to modulate the phase of a qubit much more quickly and precisely than a motorized wave plate mount. Two-qubit gates shown here in dashed boxes can be bypassed as necessary, either by swapping a photon onto another rail (gray dashed lines) or by translating "CNOT 1" out of the optical path.

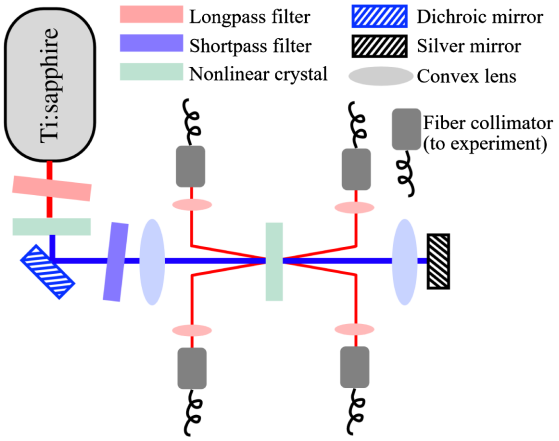

FIG. 7. Schematic of our double-pass SPDC source. The pump (blue) is retroreflected to make a second pass through the BBO crystal.

of 808 nm, and transform-limited pulse duration of 150 fs. During use, photons from this source are spectrally narrow band filtered (3 nm FWHM, Edmund Optics). When power for the blue (404 nm) pump is set to average at 10 mW, the source produces photons at a rate of approximately 5000 pairs/s with a heralding efficiency of about 16% (before losses accrued in optical gates), and fourfold coincidences of 0.5 quads/s. Our detectors are a combination of Perkin-Elmer (now Excelitas) SPCM-AQRH-W2 and SPCM-AQ4C modules coupled to home-built coincidence logic configured to operate with a coincidence window of 4 ns.

The classical FHE that we have selected for encrypting all classical bits is the "Brakerski-Gentry-Vaikuntanathan" scheme [22] as implemented in the HElib library [25], lightly modified for easy integration with the experiment. The library was called with a plaintext base $p = 2$, security parameter $k = 80$, and number of plaintext slots $l = 150$. Briefly, these parameters specify the encoding used by HElib and the corresponding size and structure of the resulting ciphertext. While a detailed description of these is beyond the scope of this paper, we refer the interested reader to Ref. [30].

A core experimental goal in this paper is to demonstrate that our QFHE implementation does indeed allow Bob to perform an arbitrary computation on ciphertext $|\psi\rangle$ securely, faithfully, and without assistance from Alice (the latter being a key differentiator between our QFHE scheme and previous SDQC protocols). Recall from Sec. II B that this is enabled by encrypting plaintext $|\phi\rangle$ with randomized Pauli operators, along with the following differences from previous experimentally demonstrated protocols.

(1) Pauli encryption keys are themselves encrypted with a classical FHE scheme.
(2) Ancillary qubits necessary for the evaluation of T gates encode those Pauli encryption keys in a way that allows Alice to prepare them at the same time as $|\psi\rangle$, independently of Bob's chosen gates.

Since by now, the encrypt-compute-decrypt process is well established for Clifford gates under this Pauli mixing approach to hiding qubits (e.g., in Ref. [14]), we shall not revisit this experimentally. Instead, we focus on our implementation's handling of T gates and, by extension, point 2 here. We show that the front-loaded preparation of ancilla qubits and their use during computation in a noninteractive way as described in Sec. II B yields the correct final results, even while $|\psi\rangle$ remains securely encrypted. Of note, point 2 here is particularly salient experimentally speaking, since the apparatus with which Bob performs a T-gate evaluation on $|\psi\rangle$ with the requisite phase correction is at times complex, requiring the implementation of a more specialized and efficient two-photon gate (see Sec. III A).

While implementing point 1 is experimentally straightforward (requiring only some additional code to be integrated with our control software), they are nevertheless crucial parts of our QFHE scheme. To highlight their importance, we concocted a toy two-party secure computation task that is easily solved with our QFHE scheme thanks to point 1 and experimentally demonstrated it in Sec. IV.

A. Fusion gate for adding phases

We digress briefly to describe the "phase-add gate" (also known as a "type-I fusion gate" [31]). It is a two-photon optical gate based on bosonic bunching and acting on the polarization d.o.f. that is central in our QFHE implementation. This optical gate, while less general, boasts a higher postselection success probability than the standard alternatives. In Appendix B, we show experimental data testing its operation.

Consider two photons, indistinguishable but for polarization, interfering at a beam splitter. If that beam splitter is carefully designed so fully transmit horizontal polarized photons ($T_H = 1, R_H = 0$) while partially reflecting vertical polarized photons ($T_H = 1/3$, $R_H = 2/3$), one can easily show that the effective operation in the polarization basis upon postselection on coincidence (i.e., one photon in each output port) is a controlled-Z gate [28]. In Fig. 6 we refer to such an optical element as a partially polarizing beam splitter (PPBS). Along with Hadamard or H gates (which are easily realized with birefringent optics like a half-wave plate), this is a standard approach to implement the CNOT operation between polarization qubits encoded in two photons. Note that this gate works only 1/9 of the time.

For our purposes, however, a general CNOT is not necessary. As an example, in case 3 of Fig. 2, the CNOT between ancillas merely serves as a means of accomplishing phase addition (modulo π) between $|\xi_b\rangle$ and $|\xi_a\rangle$. That is, we want a channel such that $(|0\rangle + e^{i\phi_a}|1\rangle)_a \otimes (|0\rangle + e^{i\phi_b}|1\rangle)_b \to (|0\rangle + e^{i(\phi_a+\phi_b)}|1\rangle)_a$.

Leveraging the fact that our ancillas are confined to states on the equator of the Bloch sphere, we can be more efficient by replacing the PPBS with a fully polarizing beam splitter (PBS), i.e., $T_V = 0$, $R_V = 1$. Consider the mode transformation of the PBS followed by an H gate on one output arm, acting on ancilla states $|0\rangle + e^{i\phi_a}|1\rangle$ and $|0\rangle + e^{i\phi_b}|1\rangle$ (in our convention, a photon in H or V polarization encodes $|0\rangle$ or $|1\rangle$, respectively):

$$\frac{1}{2}(\hat{a}_H^\dagger + e^{i\phi_a}\hat{a}_V^\dagger)(\hat{b}_H^\dagger + e^{i\phi_b}\hat{b}_V^\dagger) \rightarrow \frac{1}{2\sqrt{2}}\hat{a}_H^\dagger(\hat{b}_H^\dagger + \hat{b}_V^\dagger) - \frac{e^{i(\phi_a+\phi_b)}}{2\sqrt{2}}\hat{a}_V^\dagger(\hat{b}_H^\dagger - \hat{b}_V^\dagger), \quad (6)$$

where $\hat{a}^\dagger$ and $\hat{b}^\dagger$ are bosonic creation operators in the two input or output modes of the PBS. Subscripts on these operators label polarization. The H gate following the PBS acts on mode b. In the last line, we have omitted terms that do not contribute to simultaneous detection events between modes a and b. Finally, we postselect on a coincident detection event in the two spatial modes. When the photon in mode b is in H (or V)—i.e., $|0\rangle$ (or $|1\rangle$)—the photon in mode a is left in state $|\xi'\rangle$:

$$\text{if } \hat{b}_V^\dagger|0\rangle, \quad \text{then } |\xi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i(\phi_a+\phi_b)}|1\rangle);$$
$$\text{if } \hat{b}_H^\dagger|0\rangle, \quad \text{then } |\xi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i(\phi_a+\phi_b)}|1\rangle). \quad (7)$$

When a V polarized photon is found in mode b, $|\xi'\rangle$ is exactly the qubit state that we expect when classical bit $m_1 = 0$ on the middle rail in case 3 of Fig. 2. If on the other hand an H polarized photon is found in mode b, $|\xi'\rangle$ does not quite correspond to the $m_1 = 1$ case in Fig. 2. But it nevertheless carries the correct phase modulo π. We can therefore choose to either implement a feed-forward correction (for example, by electronically triggering a Pauli Z in mode a upon the detection of an H photon in mode b), or we may simply modify the key transformation rule indicated in Fig. 2 to read

$$a'' = r \oplus s \oplus a(b \oplus 1) \oplus (a \oplus b)m_2 \oplus m_1, \quad (8)$$

where we now define $m_1 = 0$ when postselection on $\hat{b}_V^\dagger$ succeeds and $m_1 = 1$ when $\hat{b}_H^\dagger$ succeeds.

Note that the success probability for postselection of each polarization on the b mode photon is $1/4$, so that the total probability of successful operation of the optical gate is $1/2$. This is far more efficient than $1/9$ for the standard alternative, e.g., a general purpose CNOT.

B. Setup and methodology

Our QFHE scheme was implemented for one data qubit, two ancillary qubits, and a lone T gate—the smallest nontrivial system that is instructive to implement. The main novel aspect of our QFHE implementation that is worthwhile to test and highlight experimentally is the way in which it accommodates T gates in a noninteractive way. As previously discussed (Sec. II B), in our setting of an arbitrary sequence of single-qubit Clifford gates followed by one T gate, the Pauli X decryption key b' can branch into just three distinct values, each of which requires a different phase correction and a different use of the ancillary qubits. Therefore, rather than testing all possible single-qubit Clifford sequences, it is sufficient to probe our QFHE implementation with just three canonical examples, one for each branch of the Pauli X decryption key. The three examples are enumerated in Fig. 2 and they correspond to Bob acting on $|\psi\rangle$ to effect the computations: $T|\phi\rangle$, $TH|\phi\rangle$, and $THP|\phi\rangle$, respectively. While longer Clifford sequences may precede the T gate, the manner in which ancillary qubits and therefore two-qubit or two-photon gates are used—by far the greatest source of errors and losses in our QFHE implementation—does not vary from these three canonical examples. With the optical apparatus shown in Fig. 6 we implemented the circuits in Fig. 2. We now briefly describe that apparatus.

Alice prepares and encrypts her data qubit in the photon on the top left rail. She also prepares two ancillas, $|\xi_a\rangle$ and $|\xi_b\rangle$, encoded in photons on the two bottommost rails. When implementing cases 1 and 2 (i.e., when Bob evaluates $T|\phi\rangle$ or $TH|\phi\rangle$), the phase-add gate is not required, so we swap the appropriate ancilla up into the second rail, where it is then allowed to interact with the ciphertext qubit at "CNOT 1". When implementing case 3 (i.e., when Bob evaluates $THP|\phi\rangle$), phases on both ancillas are first summed at the phase-add gate (see Sec. III A). Meanwhile, the ciphertext qubit is allowed to bypass CNOT 1 (relevant optical components are moved out of that photon's path). The ciphertext qubit that began as the top left photon now propagates directly to "CNOT 2," where it is entangled with the remaining ancilla (the other now serves as a herald for successful operation of the phase-add gate). All (classical) bits resulting from measurement that Bob performs while evaluating $T|\phi\rangle$, $TH|\phi\rangle$, or $THP|\phi\rangle$ are sent back to Alice in order that she be able to perform decryption correctly.

Note that the setup is noninteractive. Throughout the computation, Bob has all the resources he needs and his only interactions with Alice are limited to receiving or returning ciphertext $|\psi\rangle$ and ancillary resources at the start or end of his computation. In turn, at no point does Alice need to be informed about Bob's choice of computation in order to faithfully decrypt $|\psi\rangle$. This is what sets our scheme apart from earlier SDQC schemes.

To verify that the protocol works as advertised, Alice prepares and sends a variety of plaintext states to Bob as inputs to his operation(s). She decrypts and measures states that Bob returns in a variety of bases so as to be able to

tomographically infer the effective process map for his computaiton or evaluation. If indeed the protocol is correct, Alice's tomographic reconstruction of Bob's process should closely match the ideal T, TH, or THP unitary operators.

We further repeat the experiment, this time with Alice's secret keys purged and replaced with a set of erroneous keys. In this case, we expect the tomographically reconstructed process to be the completely depolarizing channel instead. Decryption (Dec) with erroneous keys is accomplished by asking HElib to generate two sets of keys, sk_1 and sk_2, and programming Alice to compute $\mathrm{Dec}_{sk_2}[\mathrm{Enc}_{sk_1}(a,b,r,s)]$, thereby simulating what an attacker with no access to the correct key sk_1 might observe.

C. Data and results

Figures 8–10 show plots of how pure states spanning the surface of a Bloch sphere transform under the unitaries T, TH, and THP, respectively (canonical single-qubit cases enumerated in Fig. 2). Figures 8(a), 9(a), and 10(a) represent every possible (pure) plaintext state by a unique color. For example, white or black at the poles represents the initial plaintext input state $|0\rangle$ or $|1\rangle$ whereas saturated bright red or yellow along the equator represents input plaintext states $|+\rangle$ or $|0\rangle + e^{i\pi/3}|1\rangle$, respectively. Figures 8(b), 9(b), and 9(b) show how these input plaintext states transform under an ideal T, TH, or THP gate sequence.

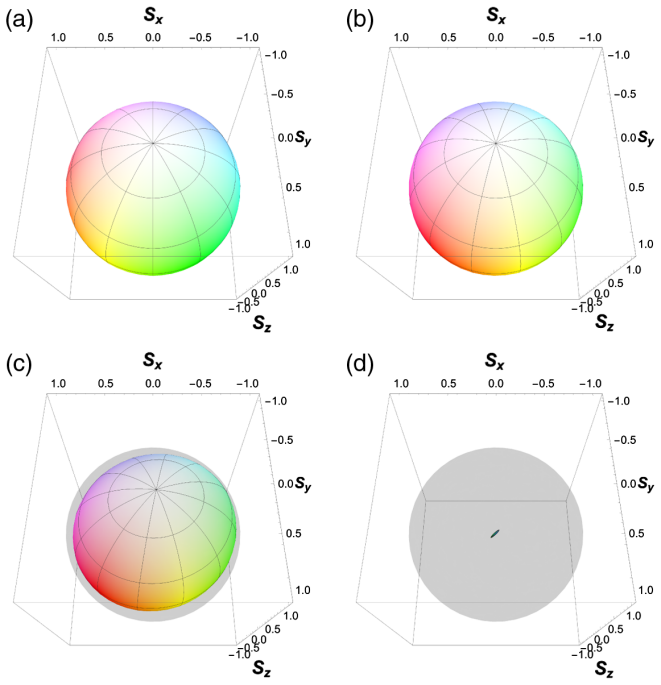

FIG. 8. Tomographic reconstruction of T unitary operator. From top left to bottom right: (a) initial Bloch sphere of pure states, (b) simulation of that Bloch sphere under ideal T, (c) experimental reconstruction with correct decryption, and (d) experimental reconstruction with bad decryption.

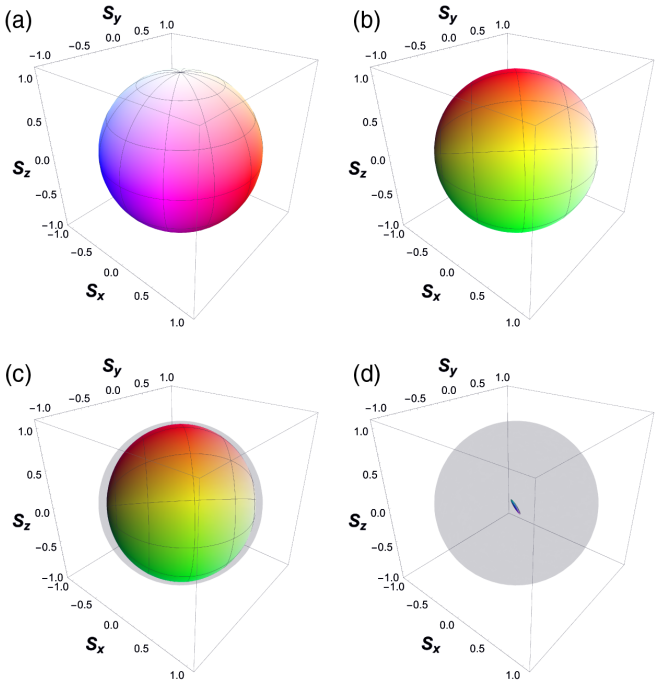

FIG. 9. Tomographic reconstruction of TH unitary operator. From top left to bottom right: (a) initial Bloch sphere of pure states, (b) simulation of that Bloch sphere under ideal TH, (c) experimental reconstruction with correct decryption, and (d) experimental reconstruction with bad decryption.

For example, an ideal T operation corresponds to a rotation by $\pi/4$ about the S_z axis on the Bloch sphere, a fact that can be clearly seen by comparing Figs. 8(a) and 8(b).

Figures 8(c), 9(c), and 10(c) show the corresponding experimentally realized transformations, performed by Bob, when Alice *correctly decrypts* the output state. These should ideally closely resemble Figs. 8(b), 9(b), and 10(b). Finally, Figs. 8(d), 9(d), and 10(d) show tomographic reconstructions of the effective transformation when decryption *is not* done properly. Without decryption, the output state should resemble the maximally mixed state (represented as a point with coordinates $S_x = S_y = S_z = 0$ in the middle of the Bloch sphere) regardless of Alice's input plaintext state and Bob's operation(s).

The effective process maps used in the bottom row of Figs. 8–10 were inferred through process tomography on experimental data (after decoding by Alice) using standard maximum likelihood estimation [32]. In both cases, an overcomplete set of preparations $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\}$ and measurements $\{\sigma_x, \sigma_y, \sigma_z\}$ was used. For each preparation and measurement configuration, ∼450 shots were accumulated for the T and TH cases, and approximately ∼100 shots for the THP case. The significantly lower average photon count per configuration in the latter case is a consequence of the reduced postselection success probability from having to perform two two-qubit gates. More precisely, the operation of the phase-add gate

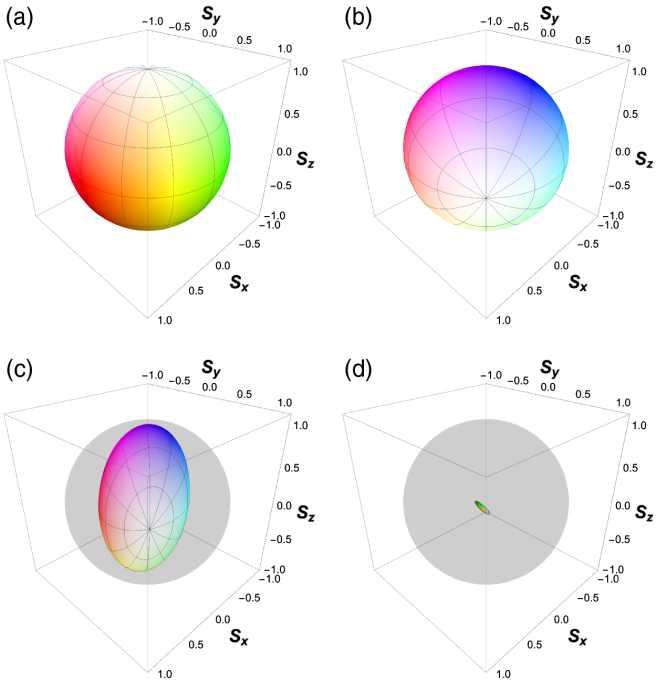

FIG. 10. Tomographic reconstruction of *THP* unitary operator. From top left to bottom right: (a) initial Bloch sphere of pure states, (b) simulation of that Bloch sphere under ideal *THP*, (c) experimental reconstruction with correct decryption, and (d) experimental reconstruction with bad decryption.

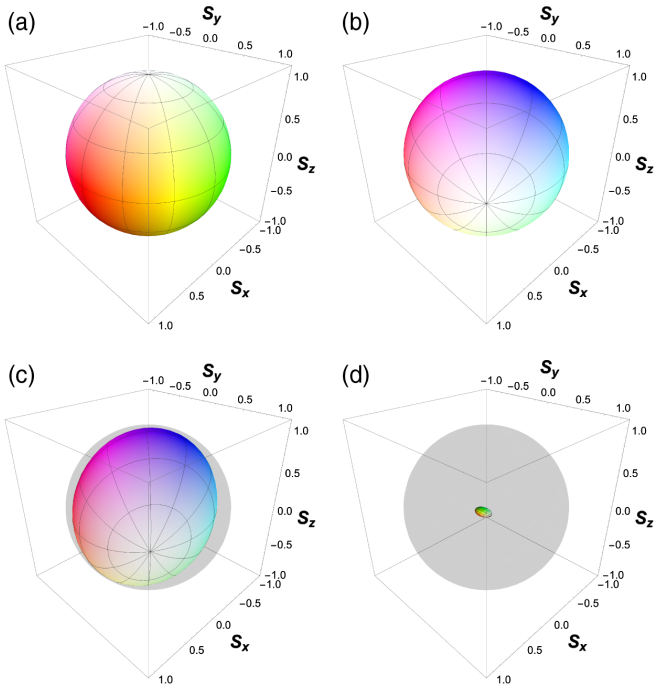

FIG. 11. Background compensated version of Fig. 10.

(shown in Fig. 6 and described in Sec. III A) places an additional postselection penalty that is compounded with the general CNOT gate(s) (that are also postselective). In our implementation of the phase-add gate, that additional postselection has a success rate of 25% since we post-selected only on one polarization (labeled $b_V^\dagger$ in Sec. III A). Equally important is the fact that whereas in the T and TH cases correct operation of a single CNOT gate is heralded by a pairwise coincidence event (detection of one boson per mode, over two modes), in the *THP* case correct operation of two two-qubit gates is heralded by quadruple (double pair) coincidence events—a much rarer occurrence.

In the interest of thoroughness, we have also presented the same data in bar chart in Figs. 12–14. Those figures show the magnitude of elements of the process matrix. In the Kraus representation of a qubit map, $\rho_{\text{out}} = \sum_j K_j \rho_{\text{in}} K_j^\dagger$, the matrix $M_{jk} = \chi_{jk} + i\xi_{jk}$ succinctly defines Kraus operators K_i in terms of a standard Pauli basis: $K_j = \sum_k (\chi_{jk} + i\xi_{jk})\sigma_k$. Here, $\chi, \xi \in \mathbb{R}$ and σ_k is to be interpreted as a Pauli matrix with the following labeling: $\sigma_0 = I$, $\sigma_1 = X$, $\sigma_2 = Y$, and $\sigma_3 = Z$. The top row of Figs. 12–14 shows matrix elements for correctly decrypted qubits, whereas the bottom row of Figs. 12–14 shows the corresponding encrypted one (ideally, the maximally mixed state). Blue bars in all panels indicate matrix elements in the ideal case, whereas yellow bars show the corresponding experimental reconstructions.

Together, Figs. 8–10 allow us to evaluate our proof of concept along two aforementioned metrics: the protocol produces correct decrypted states and the encrypted states remain securely hidden. By comparing the ideal and experimental process maps in panels (b) and (c) of these figures, we can check that the encryption protocol allows Bob to perform the correct unitary operation(s) on Alice's encrypted state. Calculating an average process fidelity allows us to perform a compact quantitative comparison [33]. Here the average process fidelities between Bob's

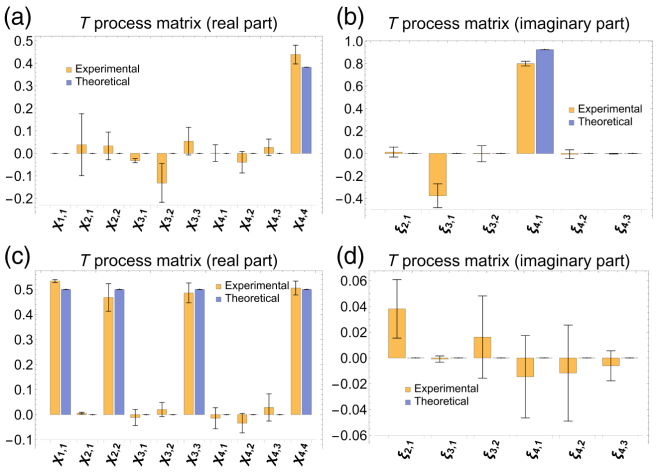

FIG. 12. Tomographic reconstruction of T unitary operator. From top left to bottom right: (a),(b) real and imaginary parts of process matrix, given *correct* decryption, and (c),(d) real and imaginary parts of process matrix, given *wrong* decryption.

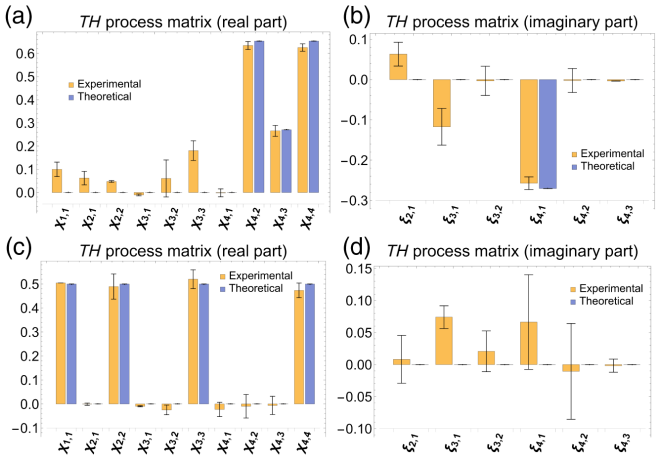

FIG. 13. Tomographic reconstruction of TH unitary operator. From top left to bottom right: (a),(b) real and imaginary parts of process matrix, given *correct* decryption, and (c),(d) real and imaginary parts of process matrix, given *wrong* decryption.

operations, realized experimentally via the QFHE protocol, and the desired ideal T, TH, and THP unitaries are 96.1%, 96.2%, and 83%, respectively. Noting that experimental imperfections (discussed below) make it difficult if not impossible to achieve a perfect 100% fidelity, these relatively high (significantly greater than 50%) fidelities give us confidence as to the correctness of the QFHE scheme.

On security, recall that absent proper decryption, the Pauli mixing encryption step should behave like the fully depolarizing channel, which noninvertibly maps all input plaintext to the maximally mixed state. We can check that our encrypted states (or erroneously decrypted ones) do not leak information about the corresponding plaintext states by comparing Figs. 8(d), 9(d), and 10(d) (effective process maps for improperly decrypted states) to Figs. 8(b), 9(b), and 10(b) (ideal desired unitaries), as well as to an ideal depolarizing channel. In our implementation, the effective process on encrypted states [Figs. 8(d), 9(d), and 10(d)] exhibits average process fidelities with the ideal T, TH, and THP operations [Figs. 8(b), 9(b), and 10(b)] of 51.7%, 47.4%, and 50.2%, respectively. For reference, the process fidelity between the fully depolarizing channel and any ideal unitary is 50%. Furthermore, the processes in Figs. 8(d), 9(d), and 10(d) have average process fidelities with respect to the ideal depolarizing channel of 99.8%, 99.7%, and 99.4%, respectively. The fact that the an improperly decrypted state appears very much like the maximally mixed state gives us confidence that an eavesdropper intercepting encrypted qubits from our implementation can deduce little information about Alice's plaintext state.

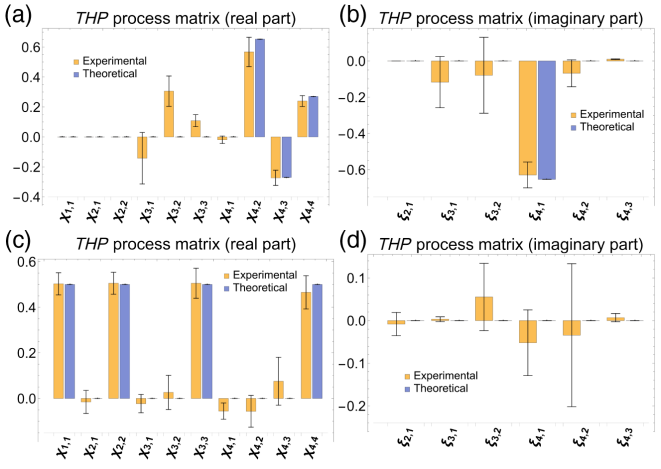

FIG. 14. Tomographic reconstruction of THP unitary operator. From top left to bottom right: (a),(b) real and imaginary parts of process matrix, given *correct* decryption, and (c),(d) real and imaginary parts of process matrix, given *wrong* decryption.

D. Experimental errors

Note that our experimentally reconstructed processes in the case of properly decrypted states [Figs. 8(c), 9(c), and 10(c)] are not perfect unitary maps—they map pure states to somewhat mixed states (i.e., they shrink the Bloch sphere). Since all qubits in our implementation are encoded in the photon polarization d.o.f., single-qubit unitary operations are realized through the use of standard birefringent retarders like half- and quarter-wave plates with extremely high fidelities. The primary limiting factor for our experimental process fidelities therefore is the quality of our two-qubit gates (i.e., the CNOT and phase-add gates).

The dominant source of error in these two-qubit gates, in turn, is imperfect two-photon interference. Recall that these optical two-qubit gates yield the desired process only when second-order interference between two single-mode bosonic creation operators occurs at a beam splitter and is followed by postselection on exactly one boson in each output mode. Imperfect interference implies that even when the postselection is done correctly, pathological terms can persist in the resulting state. Practical limitations in construction of our apparatus (e.g., imperfect alignment of collection modes, defects in collection optics, and variances in spectral profile of narrow band filters) contribute to finite interference contrasts. Furthermore, photons from different SPDC events ("interpair" photons) may not have the same (coherent) spectral correlations that exist between photons from the same SPDC event ("intrapair" ones), thereby partially invalidating the single-mode assumption which further reduces visibility in the latter case.

In our apparatus, intrapair photons exhibited HOM interference contrast of $97.0 \pm 0.5\%$ at a 50/50 BS (~77% at a PPBS, where 80% is expected). Interpair photons, on the other hand, had a HOM contrast of $90.0 \pm 1.5\%$ (~72% at a PPBS). In the case of the THP unitary operator, the issue is further compounded by the need to perform *two* consecutive two-qubit gates—in Fig. 6 these are labeled as the "phase-add" and "CNOT 2" gates, the latter operating by HOM interference between photons

from different SPDC events. This explains the relatively lower fidelity of our realization of the THP unitary compared to T and TH.

A less obvious but equally important effect is the contribution of parasitic processes that leads to unwanted coincidence events, effectively producing false positives on one-boson-per-mode postselection. For instance, higher-order SPDC events that yield more than one photon per output mode can contribute to successful postselection (i.e., coincidence) events that do *not* yield the desired output states. Similarly, because our coincidence windows while small are nevertheless finite, two uncorrelated photons or detector noise can nevertheless register erroneously but positively on our coincidence circuit.

Practical limitations imposed by equipment or procedural imperfections cannot be remedied easily. And while background processes due to higher-order SPDC events can be mitigated by reducing pump power, doing so results in impractically small signals. However, since our apparatus is sufficiently well characterized, we can calculate the expected prevalence of background processes described above and subtract them from our signal in post-processing. A background-subtracted version of Fig. 10, which plots experimental data for the THP unitary operator, is shown in Fig. 11. With background subtraction, process fidelity for the tomographic reconstruction of the THP unitary operator with correct decryption increases from 83% to 94%.

IV. APPLICATION OF QFHE: TWO-PARTY SECURE COMPUTATION

A. Protocol description

In this section, we describe a protocol we developed in order to demonstrate a use case for QFHE that is otherwise difficult to accomplish. Imagine Alice and Bob each possess a qubit state, ρ_α and ρ_β, respectively. They are tasked with comparing their states, for instance, by computing the following distance measure:

$$\mathcal{D}_{\alpha\beta} = \mathrm{Tr}(\rho_\beta^{1/2}\rho_\alpha\rho_\beta^{1/2}). \tag{9}$$

Note that this expression is very reminiscent of the fidelity [24], $F(\rho_\alpha,\rho_\beta)$, albeit with squared summands in the trace. In the pure state limit, $\mathcal{D}_{\alpha\beta}$ reduces to $F^2(\rho_\alpha,\rho_\beta)$.

Now Alice and Bob wish to compute $\mathcal{D}_{\alpha\beta}$ without sharing any more information about their qubit state than strictly necessary. In other words, neither can be allowed to tomographically reconstruct the other's state. Here we describe a protocol that accomplishes this in the "honest-but-curious" setting—i.e., we merely seek to secure data from curious prying eyes, but we assume that Alice and Bob are honest at carrying out their respective parts in the protocol, so no attempt is made at *verifying* the computation to guard against either party intentionally producing erroneous results.

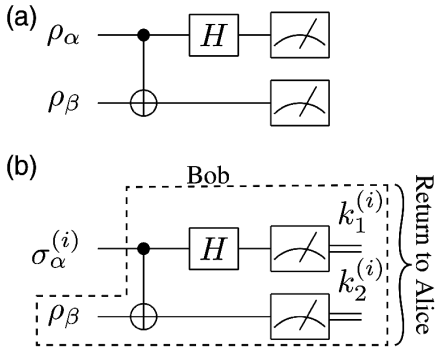

FIG. 15. (a) A simple comparator circuit. (b) A secure comparator that uses our QFHE scheme. Here, $\sigma_\alpha^{(i)}$ is the ith encrypted copy of Alice's qubit, ρ_β is Bob's qubit, and $k_1^{(i)}, k_2^{(i)} \in \{0,1\}$ are classical measurement outcomes.

A simple solution to learning $\mathcal{D}_{\alpha\beta}$ is the comparator circuit shown in Fig. 15(a). It is easy to show (see Appendix A) that under this circuit, the projector $\Pi_{1,1} = |1\rangle\langle 1| \otimes |1\rangle\langle 1|$ has an expectation value that directly yields the infidelity $\langle\Pi_{1,1}\rangle = \frac{1}{2}(1-\mathcal{D}_{\alpha\beta})$. Note that this yields the same statistics as the SWAP test. But we eschew the SWAP test in favor of our comparator circuit so as to obviate the need for a Fredkin (controlled-SWAP) gate that is difficult to implement experimentally. We build our protocol on our simple comparator circuit with the following slight additions.

Invoking our QFHE scheme, Alice encrypts all N copies of her qubit by preparing $\sigma_\alpha^{(1)} \otimes \cdots \otimes \sigma_\alpha^{(N)} = Z^{\vec{a}}X^{\vec{b}}\rho_\alpha^{\otimes N}X^{\vec{b}}Z^{\vec{a}}$ and sends them all at once to Bob along with classically homomorphically encrypted keys $\mathrm{Enc}(\vec{a})$ and $\mathrm{Enc}(\vec{b})$. As before, $\vec{a},\vec{b} \in \{0,1\}^{\otimes N}$ and $X^{\vec{a}}$ is to be interpreted as $X^{a_1} \otimes \cdots \otimes X^{a_N}$. Bob in turn performs the comparator circuit between each of Alice's qubit $\sigma_\alpha^{(i)}$ and a copy of his own ρ_β. Figure 15(b) illustrates this. Upon measuring the ith pair of qubits, Bob homomorphically adds classical outcomes $k_1^{(i)}$ and $k_2^{(i)}$ to Alice's encrypted keys to obtain $\mathrm{Enc}(a_i \oplus k_1^{(i)})$ and $\mathrm{Enc}(b_i \oplus k_2^{(i)})$. Referring to key transformation rules in Fig. 1, observe that upon decryption one can compute

$$\langle\Pi_{1,1}\rangle = \frac{1}{N}\sum_i \{(a_i \oplus k_1^{(i)}) \times (b_i \oplus k_2^{(i)})\}, \tag{10}$$

where addition in the summands are modulo 2, while top-level summation is on the full set of integers.

An additional crucial step in this protocol is for Bob to scramble the order of these classical per-shot results before returning them to Alice:

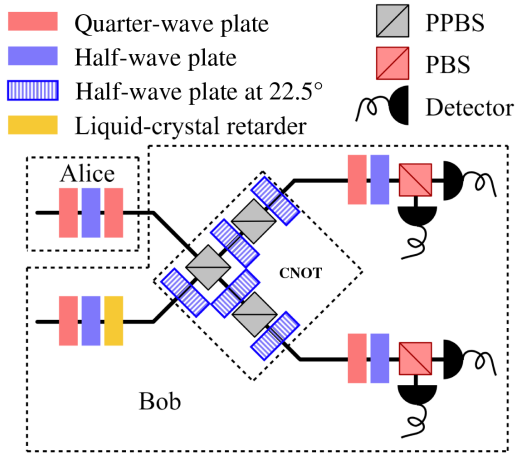

FIG. 16. Experimental setup for our secure comparator two-party protocol.

$$\mathrm{Enc}(a_i \oplus k_1^{(i)}) \to \mathrm{Enc}(a_{s_i} + k_1^{(s_i)}),$$
$$\mathrm{Enc}(b_i \oplus k_2^{(i)}) \to \mathrm{Enc}(b_{s_i} + k_2^{(s_i)}), \tag{11}$$

where s_i is the i-th element in a random permutation on the set $\{1, \ldots, N\}$. This is important in order to ensure the security of Bob's qubit which, unlike Alice's qubit, is *not* encrypted. Absent this scrambling, Alice can prepare and keep track of the inner product between Bob's qubit and a variety of states of her choosing, thereby effectively doing tomography on Bob's state. We stress that Alice can compute the correct $\mathcal{D}_{\alpha\beta}$ despite this scrambling by Bob *precisely* because in our QFHE scheme, Bob has access to—and can manipulate as part of his evaluation key—Alice's (classically homomorphically encrypted) Pauli keys.

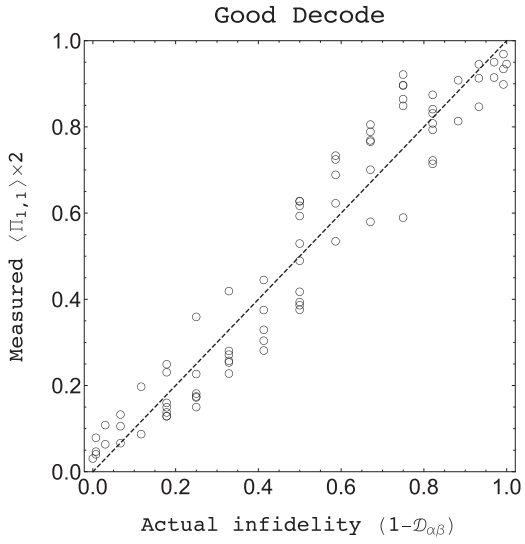

FIG. 17. Plot of measured versus actual infidelity between two states, given correct decryption. Dashed line indicates expected theoretical values.

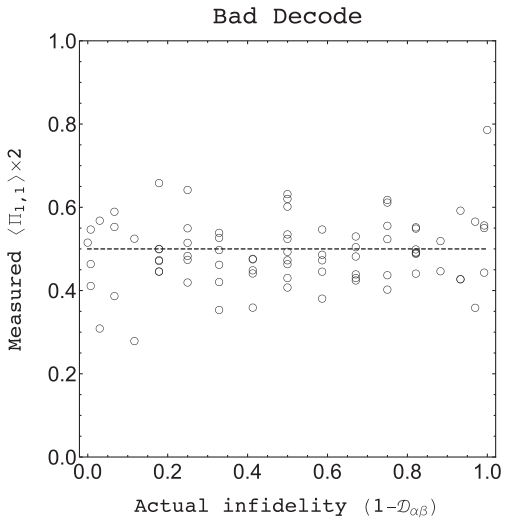

FIG. 18. Plot of measured versus actual infidelity between two states, given wrong decryption. Dashed line indicates expected theoretical values—decrypting with an erroneous key should yield 0.5 (i.e., infidelity relative to the maximally mixed state). Good agreement with this dashed line indicates that result of the computation is well hidden from parties without a valid decryption key.

B. Experimental demonstration

We implement this protocol by using a subset of our full setup, with minimal modifications. Figure 16 illustrates this. Computer-controlled wave plates representing Alice and Bob were programmed to randomly select and prepare qubits from a predefined set of logical or plaintext states (determined by range and precision of motion of our motorized actuators). In Alice's case, these wave plate settings take into account randomly generated one-time pads. The infidelity between Alice's and Bob's states is then measured as described above and plotted against its actual value in Fig. 17. As we have done in previous sections, we also ran the protocol for the same set of logical input states but with an intentionally erroneous decryption key. The result is shown in Fig. 18. The median number of photons or qubits represented by each point in these plots is ~960.

Observe in Fig. 17 that in the case of correct decryption, $2\langle\Pi_{1,1}\rangle$ shows good agreement with theoretically expected values (dashed line), indicating the protocol indeed allows Alice to retrieve the infidelity between her state and Bob's. By comparison, in Fig. 18 where decryption is done incorrectly, $2\langle\Pi_{1,1}\rangle$ hovers near a constant 0.5 (i.e., the infidelity with respect to the maximally mixed state), suggesting that anyone without the secret key gains no information about that infidelity.

V. DISCUSSION

In Sec. III we presented data that showed the QFHE scheme in operation. With proper decryption, Bob was able

to faithfully effect the intended operation with fidelities routinely in excess of 90% (or 80% without background subtraction when said operation is the unitary THP). As discussed in Sec. III D, the main limiting factor was imperfect visibility in two-qubit gates that manifested as dephasing in the decrypted qubit.

Note that the encrypted (or *improperly* decrypted) qubits returned by Bob, while close, are not *exactly* the maximally mixed state (lower panels in Figs. 8–10); in Sec. III C, we reported fidelities with respect to the ideal maximally mixed state in excess of 99%. There are two main contributing factors: measurement shot noise and sampling noise in generating encryption key(s). With a limited key length and number of measurement shots, one's estimates of the expectation values of various measurement operators (in our case $\langle\sigma_x\rangle$, $\langle\sigma_y\rangle$, and $\langle\sigma_z\rangle$) may be imperfect even when the underlying state is the perfectly depolarized or maximally mixed state. We wish to impress upon the reader that this does *not* immediately imply that Alice's plaintext is being leaked—in the same way that unequal heads versus tails in a small number of coin tosses does *not* imply an unfair coin. We calculated that the results we presented in Sec. III were consistent with the ciphertext (or an incorrectly decrypted one) being the maximally mixed state, to within tolerances set by shot or sampling noise in each dataset (for example, see error bars in the bottom panels of Figs. 12–14).

While we are confident that our implementation "works as advertised" within its design constraints (as a demonstration of our QFHE protocol), the question of security when it is used outside of those constraints and potentially subjected to abuse is a more complicated one. To start, all three of our optical two-qubit gates operate via postselections that do not always succeed. This, along with practical experimental losses, means that many photons sharing the same polarization may fail to register on our detectors and can be surreptitiously siphoned off by an attacker. Now whereas a Pauli one-time-padded state (with keys changed on a per-shot basis) appears to an eavesdropper as maximally mixed, a string of many photons all encrypted with the same Pauli keys can be used to infer a pure state (e.g., via state tomography) that is precisely the plaintext qubit $1/4$ of the time.

For an N-qubit state this means that the correct plaintext is one of $\mathcal{O}(4^N)$ possible pure states thus inferred. This is very much analogous to a classical one-time-padded bit string, where the plaintext is one of 2^N possible bit strings. And yet, even if an adversary siphoning many copies of identically prepared ciphertext is unlikely to deduce the corresponding plaintext, they nevertheless gain information about the (unique) eigenbasis of the ciphertext—which would not be possible if each shot is independently keyed, since the maximally mixed state has infinitely many, equally valid eigenbases. In some cases, this can be undesirable. As an example, with $|\xi\rangle$ the ancillary states in our protocol, it is precisely the eigenbasis in which $|\xi\rangle$ is prepared that encodes Alice's Pauli X key. Note that this is directly analogous to the vulnerability of quantum key distribution in some implementations with nonsingle-photon (e.g., weak coherent state) sources [34–37].

In our implementation, we modulated the key refresh rate and detector count time such that the average number of (coincident) detection events per key setting after experimental losses is $\lessapprox 1$. Despite this, noncoincident detection events [e.g., from an "orphaned" SPDC photon whose partner was lost, or events in which our two-photon gate postselection(s) failed] are significantly greater than 1, so our apparatus remains vulnerable to the sort of attack just described. However, we note that this can be mitigated in part by using hardware that enables higher key switching rates (for example, by switching out mechanical motors in our case with, say, Pockels cells) or, indeed, by using on-demand photon sources. We also remind the reader that while postselective two-qubit gates are adequate for small-scale proofs of concept like ours, future implementations can simultaneously be made efficient and more secure by turning to deterministic optical architectures [38–41] or other physical platforms.

VI. CONCLUSION

In this work, we constructed, implemented, and demonstrated a fully homomorphic encryption scheme for universal gate-based quantum computers first proposed in Ref. [18] and extended in Ref. [19]. With this scheme, any party in possession of encrypted qubits may evaluate a quantum circuit of their choice. This is accomplished with the aid of ancillas and classical bits prepared at the time of encryption and transmitted along with the ciphertext. Multiple use of a communication channel, quantum or classical, is not required. Explicit knowledge of the circuit (s) evaluated is not necessary for correct decryption. Furthermore, we make no concessions on security apart from assumptions that underlie the classical homomorphic cryptosystem that we use to construct our scheme. Previously demonstrated schemes compromise on one or more of these attributes.

We also solve the simple task of computing the inner product of two single-qubit states securely, that is, without allowing either party to tomographically characterize the other's qubit. Our encryption scheme provides for an elegant solution to this task, which is otherwise difficult to accomplish.

ACKNOWLEDGMENTS

W. K. T., H. F., K. B.-F., A. B., B. C. S., and A. M. S. acknowledge support from the Natural Sciences and Engineering Research Council (NSERC) of Canada and from the Canadian Institute for Advanced Research (CIFAR); S. J. is supported by an NWO WISE Grant and

an NWO Veni Innovational Research Grant under Project No. 639.021.75; additionally, B. C. S. and S. J. acknowledge funding provided by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (NSF Grant No. PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-2644); and A. B. is grateful for support from the Center for Quantum Information and Quantum Control (CQIQC) Prize Postdoctoral Fellowship. The authors thank A. O. T. Pang and N. Lupu-Gladstein for useful discussions.

APPENDIX A: INFIDELITY MEASURE FROM A SIMPLE COMPARATOR CIRCUIT

The CNOT gate with control in the first register and target in the second is defined as $\mathrm{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_X$, where σ_X is the Pauli X operator. The result of its action on a pair of qubits is

$$\begin{aligned}&\mathrm{CNOT}(\rho_\alpha \otimes \rho_\beta)\mathrm{CNOT}^\dagger \\ &\quad = \rho_\alpha^{(00)}|0\rangle\langle 0| \otimes \rho_\beta + \rho_\alpha^{(11)}|1\rangle\langle 1| \otimes \sigma_X\rho_\beta\sigma_X \\ &\qquad + \rho_\alpha^{(01)}|0\rangle\langle 1| \otimes \rho_\beta\sigma_X + \rho_\alpha^{(10)}|1\rangle\langle 0| \otimes \sigma_X\rho_\beta,\end{aligned}$$

where $\rho^{(ij)} = \langle i|\rho|j\rangle$ denotes the (i, j)-th entry of a given density matrix. We subsequently act on the first register with a Hadamard, i.e., with $H \otimes I = (|+\rangle\langle 0| + |-\rangle\langle 1|) \otimes I$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Of the large number of terms that result, we focus only on those that contribute to $\mathrm{Tr}(\rho_{\mathrm{out}}\Pi_{1,1})$, where $\Pi_{1,1} = |1\rangle\langle 1| \otimes |1\rangle\langle 1|$. Keeping in mind that the Pauli X operator simply permutes rows (columns) of a qubit density matrix when acting on it from the left (right), we have

$$\begin{aligned}\mathrm{Tr}(\rho_{\mathrm{out}}\Pi_{1,1}) &= \mathrm{Tr}\left(\Pi_{1,1}\left\{\frac{|1\rangle\langle 1|}{\sqrt{2}}H \otimes (\rho_\alpha^{(01)}\rho_\beta\sigma_X - \rho_\alpha^{(11)}\sigma_X\rho_\beta\sigma_X) + \frac{|1\rangle\langle 0|}{\sqrt{2}}H \otimes (\rho_\alpha^{(00)}\rho_\beta - \rho_\alpha^{(10)}\sigma_X\rho_\beta)\right\}\right) \\ &= \frac{1}{2}\mathrm{Tr}(\Pi_{1,1}\{|1\rangle\langle 1| \otimes (\rho_\alpha^{(00)}\rho_\beta - \rho_\alpha^{(10)}\sigma_X\rho_\beta - \rho_\alpha^{(01)}\rho_\beta\sigma_X + \rho_\alpha^{(11)}\sigma_X\rho_\beta\sigma_X)\}) \\ &= \frac{1}{2}(\rho_\alpha^{(00)}\rho_\beta^{(11)} - \rho_\alpha^{(10)}\rho_\beta^{(01)} - \rho_\alpha^{(01)}\rho_\beta^{(10)} + \rho_\alpha^{(11)}\rho_\beta^{(00)}) \\ &= \frac{1}{2}[1 - (\rho_\alpha^{(11)}\rho_\beta^{(11)} + \rho_\alpha^{(00)}\rho_\beta^{(00)} + \rho_\alpha^{(10)}\rho_\beta^{(01)} + \rho_\alpha^{(01)}\rho_\beta^{(10)})] \\ &= \frac{1}{2}[1 - \mathrm{Tr}(\rho_\alpha\rho_\beta)] \\ &= \frac{1 - \mathcal{D}_{\alpha\beta}}{2},\end{aligned}$$

where in the penultimate line we have used the fact that ρ_α and ρ_β have unit trace so that $\rho_\alpha^{(00)} = 1 - \rho_\alpha^{(11)}$, for example. Note also that if $\rho_\alpha = |\alpha\rangle\langle\alpha|$ and $\rho_\beta = |\beta\rangle\langle\beta|$ (i.e., they are both pure), then

$$1 - \mathcal{D}_{\alpha\beta} = 1 - |\langle\alpha|\beta\rangle|^2.$$

APPENDIX B: PERFORMANCE OF PHASE-ADD GATE

In order to characterize our phase-add gate, we first prepared two photons, one in each of the two bottommost rails in our experimental apparatus (Fig. 6 of main text), in the state $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ with just the leftmost half- and quarter-wave plates. The liquid-crystal wave plate (LCWP) on one rail was fixed to π retardance so that the photon on that rail is left in $|-\rangle$. The other LCWP was configured to scan its retardance (ϕ) from 0 through $3\pi/2$ (we used Meadowlark variable retarder units with home-built computer-controlled driving electronics). After a Hong-Ou-Mandel interaction at the polarizing beam-splitter (inside dashed box labeled "phase-add gate" in Fig. 6), the photon on the bottommost rail was projected onto $|+\rangle\langle+|$ and we postselected for coincident detection events between the two rails. As discussed in Sec. III A, the other photon must be found in the state $(|H\rangle + e^{i\phi}|V\rangle)/\sqrt{2}$. Over multiple shots (approximately 1000 each), we measured the remaining photon along an informationally overcomplete set of bases (i.e., by projecting onto D/A, H/V, and L/R polarizations) in order to tomographically infer its state.

Figure 19 shows the Bloch vector components of this inferred state as a function of ϕ (LCWP retardance). The sinusoidal oscillation of S_x and S_y (with a π phase shift) is indicative of the phases between the two photons being added in the output photon. In the *absence* of a HOM interaction, the phase-add gate behaves simply as a PBS (transmitting H and reflecting V polarization), that is insensitive to phases written onto either photon (like ϕ). We tested this regime by introducing a path delay between the two photons much greater than their pulse widths ($\approx 5\ \mathrm{mm}/c \gg 150$ fs), in which case $S_x = S_y = S_z = 0$

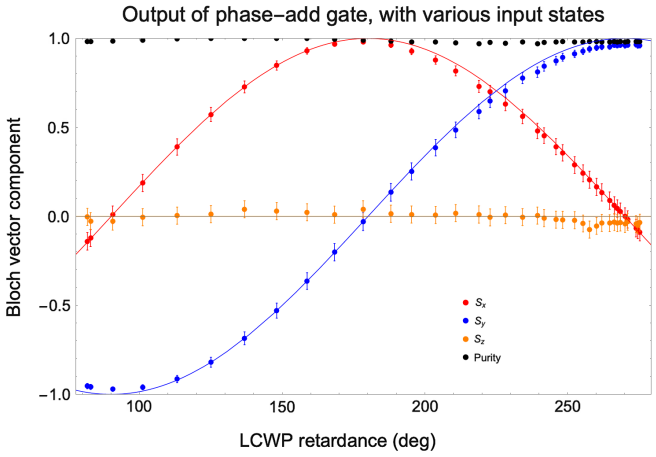

FIG. 19. Bloch vector components of the output photon from phase-add gate as a function of LCWP retardance ϕ. Solid lines are theoretical predictions. The LCWPs prepare photons in the states $(|H\rangle + e^{i\phi}|V\rangle)/\sqrt{2}$ and $(|H\rangle - |V\rangle)/\sqrt{2}$. The output state is consistent with $(|H\rangle + e^{i(\phi+\pi)}|V\rangle)/\sqrt{2}$. Each point represents ≈1000 photons. Density of points is not uniform along x axis because the LCWP's retardance is nonlinear with respect to driving voltage.

regardless of LCWP retardance (not shown here). Finally, we also checked that the phase-add gate operates symmetrically with respect to both input photons. We configured both LCWPs to write phases (say, ϕ and φ) onto both photons and checked that the output polarization is indeed $(|H\rangle + e^{i(\phi+\varphi)}|V\rangle)/\sqrt{2}$ to within error tolerances.

APPENDIX C: CNOTS, TELEPORTATION, AND PHASE-ADD CIRCUITS

In this Appendix, we explain the operation of the circuits in Figs. 3 and 4.

Consider the states

$$\begin{aligned}|\psi\rangle &= \alpha|0\rangle + \beta|1\rangle,\\ |\xi\rangle &= Z^r P^b|+\rangle\\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle),\end{aligned}$$

where $\theta = (2r+b)\pi/2$.

The action of a CNOT gate controlled by $|\psi\rangle$ and targeting $|\xi\rangle$ is

$$\begin{aligned}&\mathrm{CNOT}_{1\to 2}(|\psi\rangle \otimes |\xi\rangle)\\ &= \alpha|0\rangle \otimes |\xi\rangle > + \beta|1 \otimes X|\xi\rangle\\ &= \frac{\alpha}{\sqrt{2}}|0\rangle \otimes (|0\rangle + e^{i\theta}|1\rangle) + \frac{\beta}{\sqrt{2}}|1\rangle \otimes (|1\rangle + e^{i\theta}|0\rangle)\\ &= (\alpha|0\rangle + e^{i\theta}\beta|1\rangle) \otimes \frac{|0\rangle}{\sqrt{2}} + e^{i\theta}(\alpha|0\rangle + e^{-i\theta}\beta|1\rangle) \otimes \frac{|1\rangle}{\sqrt{2}}.\end{aligned}$$

If the outcome from measuring the second register (which we labeled m in Figs. 3 and 4) is 0, then the first register is left in the state $(\alpha|0\rangle + e^{i\theta}\beta|1\rangle) = Z^r P^b|\psi\rangle$. Otherwise (i.e., $m = 1$), up to a global phase, the first register is left in $(\alpha|0\rangle + e^{-i\theta}\beta|1\rangle) = Z^r P^{\dagger b}|\psi\rangle$. Because $P^{\dagger b} = Z^b P^b$, we can write the final state of the first register concisely as $Z^{r\oplus bm} P^b|\psi\rangle$.

In the special case where $|\psi\rangle = Z^s P^a|+\rangle$, a simple substitution yields the phase-addition (modulo π) action of Fig. 4,

$$Z^{r\oplus bm} P^b|\psi\rangle = Z^{r\oplus bm\oplus s} P^{a+b}|+\rangle = Z^q P^{a\oplus b}|+\rangle,$$

where $q = r \oplus bm \oplus s \oplus \lfloor a + b/2 \rfloor$.

[1] R. L. Rivest, L. Adleman, and M. L. Dertouzos, *On Data Banks and Privacy Homomorphisms*, Found. Secure Comput. **4**, 169 (1978).

[2] S. Goldwasser and S. Micali, *Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information*, in *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing (STOC '82)* (ACM Press, New York, 1982), pp. 365–377.

[3] O. Goldreich, S. Micali, and A. Wigderson, *How to Play ANY Mental Game*, in *Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing (STOC '87)* (ACM Press, New York, 1987), pp. 218–229.

[4] O. Goldreich and R. Ostrovsky, *Software Protection and Simulation on Oblivious RAMs*, J. Am. Comput. Mach. **43**, 431 (1996).

[5] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, *One-Time Programs*, in *Advances in Cryptology—CRYPTO 2008*, edited by D. Wagner (Springer, Berlin, 2008), pp. 39–56.

[6] J. Kilian, *A Note on Efficient Zero-Knowledge Proofs and Arguments (Extended Abstract)*, in *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Somputing (STOC '92)* (ACM Press, New York, 1992), pp. 723–732.

[7] C. Gentry, *A Fully Homomorphic Encryption Scheme*, Ph. D. thesis, Stanford University, 2009.

[8] A. M. Childs, *Secure Assisted Quantum Computation*, Quantum Inf. Comput. **5**, 456 (2005).

[9] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, *Universal Blind Quantum Computation*, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, 2009* (IEEE Computer Society, Los Alamitos, CA, 2009), pp. 517–526.

[10] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, *Demonstration of Blind Quantum Computing*, Science **335**, 303 (2012).

[11] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, *Composable Security of Delegated Quantum Computation*, in *Advances in Cryptology—ASIACRYPT 2014*, edited by Palash Sarkar and Tetsu Iwata (Springer, Berlin, 2014), pp. 406–425.

[12] A. Broadbent, G. Gutoski, and D. Stebila, *Quantum One-Time Programs*, in *Advances in Cryptology—CRYPTO 2013*, edited by R. Canetti and J. A. Garay (Springer, Berlin, 2013) pp. 344–360.

[13] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, *Interactive Proofs for Quantum Computations*, arXiv:1704.04487.

[14] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, *Quantum Computing on Encrypted Data*, Nat. Commun. **5**, 3074 (2014).

[15] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, *Quantum Walks with Encrypted Data*, Phys. Rev. Lett. **109**, 150501 (2012).

[16] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, *A Quantum Approach to Homomorphic Encryption*, Sci. Rep. **6**, 33467 (2016).

[17] J. Zeuner, I. Pitsios, S.-H. Tan, A. N. Sharma, J. F. Fitzsimons, R. Osellame, and P. Walther, *Experimental Quantum Homomorphic Encryption*, arXiv:1803.10246.

[18] A. Broadbent and S. Jeffery, *Quantum Homomorphic Encryption for Circuits of Low T-Gate Complexity*, in *Advances in Cryptology—CRYPTO 2015*, edited by R. Gennaro and M. Robshaw (Springer, Berlin, 2015) pp. 609–629.

[19] Y. Dulek, C. Schaffner, and F. Speelman, *Quantum Homomorphic Encryption for Polynomial-Sized Circuits*, in *Advances in Cryptology—CRYPTO 2016*, edited by M. Robshaw and J. Katz (Springer, Berlin, 2016), pp. 3–32.

[20] U. Mahadev, *Classical Homomorphic Encryption for Quantum Circuits*, in *Proceedings of the IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), 2018* (IEEE, New York, 2018), pp. 332–338.

[21] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf, *Private Quantum Channels*, in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, CA, 2000* (IEEE, New York, 2000), pp. 547–553.

[22] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, *(Leveled) Fully Homomorphic Encryption Without Bootstrapping*, ACM Trans. Comput. Theory **6**, 1 (2014).

[23] D. Micciancio and O. Regev, *Lattice-Based Cryptography*, in *Post-Quantum Cryptography*, edited by D. J. Bernstein, J. Buchmann, and E. Dahmen (Springer, Berlin, 2009), pp. 147–191.

[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, 2011).

[25] S. Halevi, HElib, An Implementation of Homomorphic Encryption, https://github.com/shaih/HElib.

[26] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, *Linear Optical Quantum Computing with Photonic Qubits*, Rev. Mod. Phys. **79**, 135 (2007).

[27] C. K. Hong, Z. Y. Ou, and L. Mandel, *Measurement of Subpicosecond Time Intervals between Two Photons by Interference*, Phys. Rev. Lett. **59**, 2044 (1987).

[28] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, *Linear Optics Controlled-Phase Gate Made Simple*, Phys. Rev. Lett. **95**, 210505 (2005).

[29] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, *Demonstration of an All-Optical Quantum Controlled-NOT Gate*, Nature (London) **426**, 264 (2003).

[30] S. Halevi and V. Shoup, *Faster Homomorphic Linear Transformations in HElib*, in *Advances in Cryptology—CRYPTO 2018*, edited by H. Shacham and A. Boldyreva (Springer International Publishing, Cham, Switzerland, 2018), pp. 93–120.

[31] D. E. Browne and T. Rudolph, *Resource-Efficient Linear Optical Quantum Computation*, Phys. Rev. Lett. **95**, 010501 (2005).

[32] J. M. Chow, J. M. Gambetta, L. Tornberg, J. Koch, L. S. Bishop, A. A. Houck, B. R. Johnson, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, *Randomized Benchmarking and Process Tomography for Gate Errors in a Solid-State Qubit*, Phys. Rev. Lett. **102**, 090502 (2009).

[33] L. H. Pedersen, N. M. Møller, and K. Mølmer, *Fidelity of Quantum Operations*, Phys. Lett. A **367**, 47 (2007).

[34] H.-K. Lo, X. Ma, and K. Chen, *Decoy State Quantum Key Distribution*, Phys. Rev. Lett. **94**, 230504 (2005).

[35] H. Inamori, N. Lütkenhaus, and D. Mayers, *Unconditional Security of Practical Quantum Key Distribution*, Eur. Phys. J. D **41**, 599 (2007).

[36] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Security of Quantum Key Distribution with Imperfect Devices*, Quantum Inf. Comput. **5**, 325 (2004).

[37] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Security Aspects of Practical Quantum Cryptography*, in *Advances in Cryptology—EUROCRYPT 2000*, edited by B. Preneel (Springer, Berlin, 2000), pp. 289–299.

[38] R. Raussendorf and H. J. Briegel, *A One-Way Quantum Computer*, Phys. Rev. Lett. **86**, 5188 (2001).

[39] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Measurement-Based Quantum Computation on Cluster States*, Phys. Rev. A **68**, 022312 (2003).

[40] M. A. Nielsen, *Optical Quantum Computation Using Cluster States*, Phys. Rev. Lett. **93**, 040503 (2004).

[41] E. Knill, R. Laflamme, and G. J. Milburn, *A Scheme for Efficient Quantum Computation with Linear Optics*, Nature (London) **409**, 46 (2001).