Editors' Suggestion

Experimental Quantum Homomorphic Encryption Using a Quantum Photonic Chip

Yuan Li,[1] Lin Cao,[2] Wei Luo,[1] Hui Zhang,[1,*] Hong Cai,[1,†] Muhammad Faeyz Karim,[2] Feng Gao,[1]
Joseph Fitzsimons,[3,‡] Qinghua Song,[4,§] and Ai-Qun Liu[1,2,∥]

[1]*Institute of Quantum Technology (IQT), The Hong Kong Polytechnic University,
Hong Kong, 11 Yuk Choi Rd, Hung Hom, Hong Kong*
[2]*Quantum Science and Engineering Centre (QSec), Nanyang Technological University, 639798, Singapore*
[3]*Horizon Quantum Computing, 79 Ayer Rajah Crescent, BASH #03-01, 139955, Singapore*
[4]*Tsinghua Shenzhen International Graduate School, Tsinghua University, Shenzhen 518055, China*

(Received 3 September 2023; accepted 19 March 2024; published 14 May 2024)

A fully homomorphic encryption system enables computation on encrypted data without the necessity for prior decryption. This facilitates the seamless establishment of a secure quantum channel, bridging the server and client components, and thereby providing the client with secure access to the server's substantial computational capacity for executing quantum operations. However, traditional homomorphic encryption systems lack scalability, programmability, and stability. In this Letter, we experimentally demonstrate a proof-of-concept implementation of a homomorphic encryption scheme on a compact quantum chip, verifying the feasibility of using photonic chips for quantum homomorphic encryption. Our work not only provides a solution for circuit expansion, addressing the longstanding challenge of scalability while significantly reducing the size of quantum network infrastructure, but also lays the groundwork for the development of highly sophisticated quantum fully homomorphic encryption systems.

DOI: 10.1103/PhysRevLett.132.200801

Introduction.—Quantum computing, a burgeoning field that harnesses the principles of quantum mechanics for computation, confronts inherent challenges associated with the construction and operation of intricate quantum systems [1–3]. To address these challenges, the client-server model has emerged as a practical approach to quantum computation. In this model, the quantum computer is situated on the server side, enabling clients with limited quantum capabilities to delegate complex computational tasks to the server [4–7]. As a result, the clients can leverage the server's more robust quantum resources, obviating the necessity of constructing and maintaining their own security of quantum systems.

However, in scenarios where privacy is a paramount concern, such as when dealing with sensitive data or proprietary algorithms, both the server and clients may have a vested interest in concealing information about their respective programs or data from each other. This necessitates the deployment of secure protocols to ensure the privacy of computations and data in bipartite quantum computing. To tackle this challenge, researchers have delved into the realm of quantum homomorphic encryption (QHE) [8]. QHE is an encryption method that allows for performing computations on encrypted quantum data without decrypting it, thus preserving the confidentiality of the information. By using QHE, quantum computation can be conducted on private data owned by one party, utilizing a program provided by another party, while minimizing the disclosure of information about the underlying data. Compared with the traditional quantum key distribution system, QHE not only ensures the security of the quantum channel, but also facilitates the combination with quantum computation, which is important for building a robust quantum network.

Several studies have explored the secure delegation of quantum computation through QHE [9–12]. Notably, a scheme that is homomorphic for both Clifford and non-Clifford gates, including the crucial "T" gate required for universal quantum computations, was developed [12]. This scheme proves valuable in the construction of practical quantum networks [13–17]. Furthermore, quantum fully homomorphic encryption, capable of handling arbitrary computations, has been successfully demonstrated using bulk optics [18]. Nevertheless, traditional demonstrations of quantum optical methods have predominantly suffered from bulky configurations and lack of scalability, significantly constraining their practicality. Consequently, concerted efforts are necessary to minimize the size of the optical components, enabling the exploration of innovative avenues for establishing scalable, programmable, stable, and secure channels between clients and servers within quantum networks.

The advancement of integrated photonic chips has played a crucial role in reducing the size of optical components, leading to substantial implications for both quantum computation [19–21] and quantum communication [22–25]. In this Letter, we present a groundbreaking achievement by demonstrating the successful implementation of the quantum fully homomorphic encryption on a silicon photonic chip. This development highlights the capabilities of our chip to facilitate quantum networks that bridge the server and client components. The integration of QHE on an integrated photonic platform signifies a milestone and serves as a significant proof of concept in the realm of quantum network that combines both the quantum communication and computation. Moreover, our work leverages integrated technologies to provide a robust platform for further research and exploration into secure quantum networks. This integration of quantum computing and communication capabilities on a single chip opens up new possibilities for efficient and secure quantum information processing.

A QHE protocol consists of four steps between the client and server part: (1) the client generates random keys that are unknown to the server. (2) The client encodes his qubits with the keys and sends them to the server. (3) The server performs calculations on the received qubits from the client. (4) The server sends the qubits back to the client, who then performs the decoding process using the updated keys.

Figure 1 illustrates a typical configuration for a QHE scheme in a quantum network. It consists of a powerful server capable of handling complex algorithms seamlessly connected to clients for quantum communication. The client in the network possesses an encoding module and a decoding module and aims to execute a quantum operation. However, due to the limitation of clients' computation power, they can encode their qubit states $|\varphi\rangle$ using Pauli Z and X operations to ensure privacy. The encoded qubits are then transmitted to the server. For the transmitted state $|\varphi\rangle$ from client part to the server part, the encoding scheme Z^aX^b is chosen to prevent any potential information leakage to the eavesdropper, which is expressed as

$$1/4 \sum_{a,b\in\{0,1\}} Z^aX^b|\varphi\rangle\langle\varphi|(Z^aX^b)^\dagger = I_2/2,$$

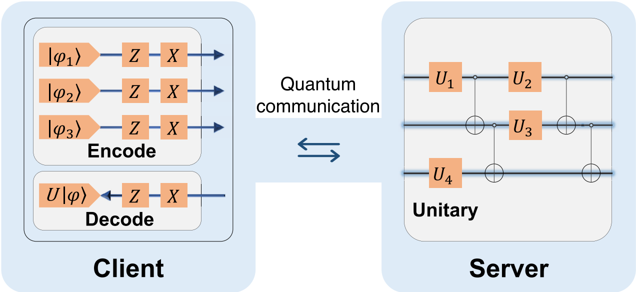

FIG. 1. The principle of QHE. The frame of the quantum network constructed by performing the QHE scheme, which seamlessly bridges the server and client parts. The client part includes the encoding and decoding parts. And the server's role is to perform arbitrary operations on the qubits received from the client part and then send the operated qubits back to the client.

where I_2 is the two-dimension identity matrix. It can be observed from the equation that the encoded state is a totally mixed state to the server part, which assures the security of the protocol. Since any arbitrary complicated circuit on the server part can be decomposed into the realization of two-qubit CNOT gate and single-qubit gates. The two-qubit CNOT gate, Pauli X, Y, Z gates, along with the Hadamard gate $H = \left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)/\sqrt{2}$, and $S = \left(\begin{smallmatrix}1 & 0\\ 0 & i\end{smallmatrix}\right)$ gate, are all Clifford gates. The encoding operator Z^aX^b is the element of the Pauli group for all $a, b \in \{0, 1\}$. For the Clifford gate U, the following equation must be satisfied:

$$UP = P'U,$$

where P and P' are both the Pauli group elements. It implies that for the encoding operation P applying on the arbitrary input state $|\varphi\rangle$, a corresponding decoding operation $(P')^{-1}$ is subsequently applied on the output state to recover the desired state $U|\varphi\rangle$ (see Supplemental Material, Note 1 for details) [26].

However, realizing non-Clifford gate $T = \left(\begin{smallmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{smallmatrix}\right)$ is very important for quantum computation and QHE protocol. For the T gate operating on the encoded state $|\varphi\rangle$, the equation $T(Z^aX^b) = (X^bZ^{a\oplus b})S^bT$ is satisfied, where the global phase is ignored here. It can be observed that the application of the T gate includes a phase error S^b. Thus, the client part is unable to recover the state $T|\varphi\rangle$ after the decoding scheme following the server's execution of T gate on the encoded qubit. Fortunately, the phase error can be eliminated, which enables the recovery of the non-Clifford T gate operation. Based on quantum teleportation, the phase correction is performed for the state $|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)$ with an ancillary qubit encoded in the state $Z^rS^b|+\rangle$ and a CNOT gate that is expressed as

$$\begin{aligned}
&|\psi\rangle Z^rS^b|+\rangle\\
&\longrightarrow (\alpha|0\rangle+\beta|1\rangle)[|0\rangle+(-1)^r(i)^b|1\rangle]\\
&\xrightarrow{\text{CNOT}} \alpha|0\rangle[|0\rangle+(-1)^{r+b/2}|1\rangle]+\beta|1\rangle[(-1)^{r+b/2}|0\rangle+|1\rangle]\\
&\longrightarrow [\alpha|0\rangle+(-1)^{r+b/2}\beta|1\rangle]|0\rangle+[(-1)^{r+b/2}\alpha|0\rangle+\beta|1\rangle]|1\rangle
\end{aligned}$$

The formula shows that when the ancillary qubit is measured in $|0/1\rangle$ basis and $|0\rangle$ is obtained, the input state is changed from $|\psi\rangle$ to $S^b|\psi\rangle$, where r is set to 0. Thus, a phase error correction is performed with the measured results for the ancillary qubit. By realizing the decoding operations on the client part, we can recover the desired output state $T|\varphi\rangle$. For the realization of the unitary operations $U = TU'$, where U' is the Clifford gate, the phase correction procedure is determined by the decryption parameters for U' in the QHE protocol. For example, when $U' = I$ (identity matrix), the phase error is S^b. When $U' = H$, the phase error becomes S^a. While in the case of $U' = HS$, the phase error will be $S^{a\oplus b}$ (see Supplemental

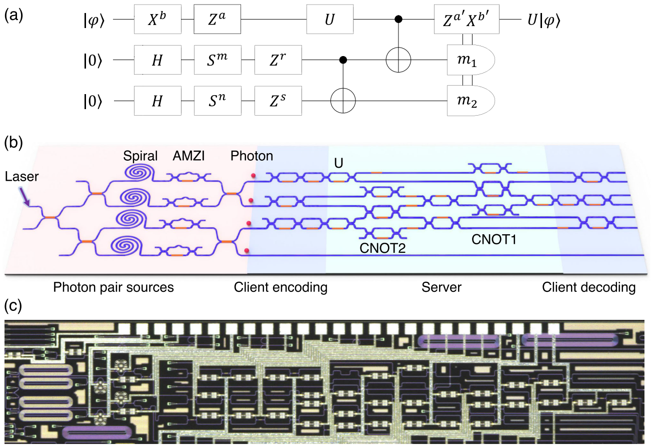

FIG. 2. Silicon quantum photonic processor for realization of QHE protocol. (a) The QHE quantum circuit. The signal qubit and ancillary qubit are encoded first and then passing through the server part for the operation U and phase error correction. The decoding process is performed to recover the operation on signal qubit. Parameters r, s, a, b are random for security. The parameters m, n are for phase error corrections determined by U. (b) Schematic of QHE chip. The quantum photonic chip consists of the photonic pair sources generation and client part and server part. The dual-wavelength pump laser passing through the spiral to generate the photon pair via four-wave mixing process. The residual pump laser is filtered by asymmetric Mach-Zehnder Interferometer (AMZI). And the photons are encoded and decoded by single qubit operations with Mach-Zehnder Interferometer. (c) The micrograph of the whole fabricated quantum photonic chip.

Material, Note 1 for details [26]). Therefore, for the demonstration of $U = T$ and TH gate in the QHE protocol, one parameter is induced for the phase error, necessitating only one CNOT gate. Conversely, when demonstrating $U = THS$ gate, we must perform the phase correction twice for both parameters. As a result, two CNOT gates are required.

Figure 2(a) illustrates the quantum circuit for demonstrating the single-qubit non-Clifford gate for the QHE protocol, where U is the non-Clifford operation performed by the server on the encoded signal qubit from the client. The two encoded ancillary qubits are utilized for the phase error correction. We have experimentally demonstrated the QHE protocol on an advanced quantum photonic chip. This chip consists of three main components: the photon pair source, the client part, and the server part, as depicted in Fig. 2(b). In the photon pair source part, a 500 MHz pump laser with dual wavelengths of 1546.8 nm and 1553.2 nm is generated by injecting a 10 nm bandwidth beam into two narrow bandpass filters (more details are shown in Supplemental Material, Note 2 [26]). Subsequently, the pump beam is split into four paths and injected into the spiral silicon waveguides to generate superpositions of weak squeezed states. These states then pass through 50:50 beam splitters, resulting in the generation of two degenerate photon pair sources with wavelength of 1550 nm through Hong-Ou-Mandel (HOM) interference [21]. The photons are then filtered by dense wavelength-division multiplexing with a 3 dB bandwidth of 0.5 nm after passing through the whole chip. The fourth photon is sent to the superconducting nanowire single-photon detector directly as a trigger signal (the detailed optical circuit is shown in Supplemental Material, Note 2 [26]). The first photon acts as the signal photon and the other two photons are used as ancillary photons for performing the QHE task. Three Mach-Zehnder interferometers are placed in the client encoding part to realize the encoding operations for the signal qubit and ancillary qubits. The server part is composed of two CNOT gates with a postselected probability of 1/9 for each and a unitary operation U that can be set as non-Clifford gate T, TH, and THS for the demonstration of the QHE protocol. When $U = T$ and TH, only the first one pair photon source and CNOT-1 are used for the demonstration. The coincidence count of the output photons is registered by the time tagger. While for $U = THS$, two photon pairs are passing through CNOT-2 and CNOT-1 sequentially, and a four-photon coincidence count event is postselected. The decoding part depends on the measurement of the ancillary qubit, which can be realized by performing the corresponding operations on the acquired coincidence counts. Figure 2(c) is the micrograph of the fabricated silicon photonic chip for the QHE demonstration.

Results and discussion.—In order to obtain high-quality results in the experiment, the brightness of the degenerated photon pair source is set at 2000 Hz to reduce the multiphoton pair emission noise. The CNOT gate, a fundamental two-qubit gate in quantum computing, plays a crucial role in the implementation of the QHE for the phase error correction. To fully characterize the CNOT gate, we prepare the input state of photons in a complete set of basis states and perform quantum process tomography [3], which gives out a fidelity of 0.93 ± 0.01 (see Supplemental Material, Note 3.1 for more details [26]).

Subsequently, we demonstrate the T gate and TH gate operated at the server part that involves the utilization of one photon pair source and one CNOT gate. To explore the functionality of these gates, we select six distinctive input states $|\varphi\rangle$ as test cases for our system, including $H = |0\rangle$, $V = |1\rangle$, $D = (|0\rangle + |1\rangle)/\sqrt{2}$, $A = (|0\rangle - |1\rangle)/\sqrt{2}$, $R = (|0\rangle + i|1\rangle)/\sqrt{2}$, and $L = (|0\rangle - i|1\rangle)/\sqrt{2}$. For the encoding system, we perform the $Z^a X^b$ on signal qubit $|\varphi\rangle$ for the T gate, and for TH gate, we apply either $Z^r S^b$ or $Z^r S^a$ to the signal qubit $|\varphi\rangle$, where $\{a, b, r\} \in \{0, 1\}$. Considering the whole eight situations for the parameters $\{a, b, r\}$ ranging from $\{0,0,0\}$ to $\{1,1,1\}$, we measure the average fidelities for the T gate and TH gate operated on the signal qubit after the decoding process as shown in Figs. 3(a) and 3(d). The obtained results reveal an average fidelity of 0.951 ± 0.008 for the T gate and 0.927 ± 0.008 for the TH gate. For a generic quantum process ε acting on single-qubit density matrix ρ, one has $\varepsilon(\rho) = \sum_{m,n=0}^{3} \chi_{mn} \Gamma_m \rho \Gamma_n^\dagger$,

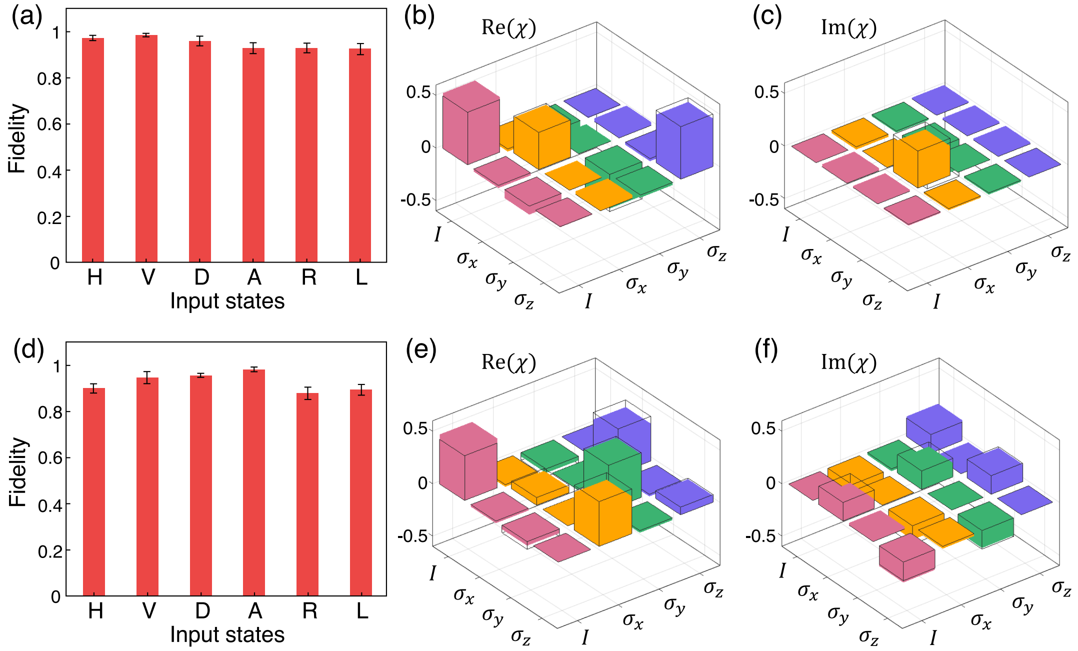

FIG. 3. Quantum measurement of qubit after T and TH unitary operation. (a),(d) The average fidelities measured after the T and TH gates operation for different input states in H, V, D, A, R, and L basis. (b),(e) The reconstructed real part and (c),(f) imaginary part of the process tomography matrix for the T gate and TH gates individually.

where Γ_m is the Pauli matrices for $m = 0$, 1, 2, 3, and the matrix χ_{mn} contains all the information of the process, which gives out a process fidelity for the operation gate. Based on the obtained results for input basis H, V, D, and R, the reconstructed process matrices χ_{exp} for T gate and TH gate are calculated as shown in Figs. 3(b) and 3(c) and Figs. 3(e) and 3(f).

In order to demonstrate the THS gate, two photon pair sources and two CNOT gates are used for two phase error corrections. The HOM interference [28] visibility between different photon pair sources is measured as 0.88 ± 0.05 (see more details in Supplemental Material, Note 3.2 [26]) in the four-photon experiment. However, this process yields a count rate merely 0.5 per hour, rendering it impractical to sample all possible input parameters $\{a, b, r, s\}$ ($Z^a X^b$ for the signal qubit, $Z^r S^a$ and $Z^s S^b$ for ancillary two qubits). As a proof of concept, we focused on demonstrating the THS gate with the input parameter $\{a, b, r, s\} = \{0, 0, 0, 0\}$. For the four selected states H, V, D, and R applied to the input state $|\varphi\rangle$, the measured average fidelities of the output states are 0.808 ± 0.032 as shown in Fig. 4(a). The reconstructed process matrix χ_{exp} for THS gate is shown in Figs. 4(b) and 4(c). It allows us to determine its process fidelity $F = \text{Tr}(\chi_{\text{exp}}\chi_{th}) = 0.651 \pm 0.069$, where χ_{th} is the theoretical process matrix for THS gate.

Compared with bulk optics, the size of the optical circuit has been reduced from several meters to 2 mm, which is more compact for the integration. To showcase the benefits of integrated optics for quantum experiments, we assessed

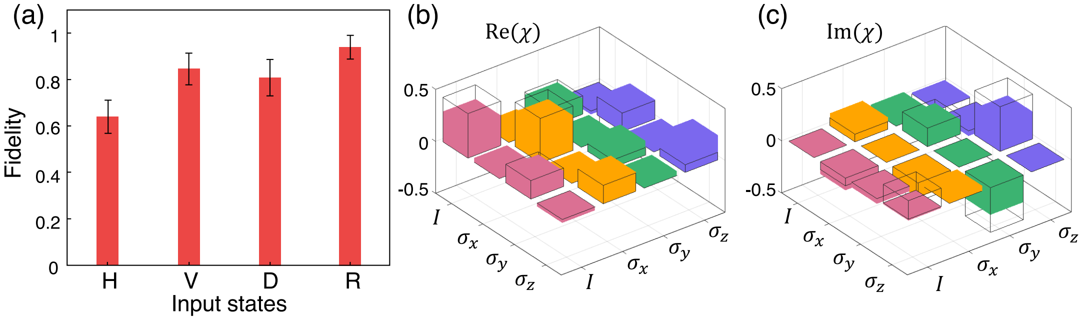

FIG. 4. Quantum measurement of qubit after THS unitary operation. (a) The fidelities measured after the THS gate operation for different input states in H, V, D, and R basis with the encoding parameters $a = 0$, $b = 0$, $r = 0$, and $s = 0$. (b) The reconstructed real part and (c) imaginary part of the process tomography matrix for the THS gate.

the phase stability of a single Mach-Zehnder interferometer by conducting HOM interference between the signal photon and idler photon, revealing a phase drift deviation of 0.72° over seven days (refer to Supplemental Material, Note 3.3 for further details [26]). Furthermore, in the context of multiclient or large-scale quantum networks, the high yield and programmability of photonic chips make experiments more convenient compared to bulk optics.

There are two main factors contributing to imperfect fidelity: (1) unwanted multipair emission. To perform a four-photon experiment, the ideal data should be obtained from two pairs of photons generated by each photon pair source. However, in our experiments, due to photon loss from generation to detection (experimentally calibrated at 5%), three or more pairs of photons are generated with a certain probability due to the Poisson distribution. This introduces significant noise, reducing the experiment's fidelity. (2) Imperfect indistinguishability between different photon pairs. Achieving perfect fidelity requires that different photon pairs generated by four-wave mixing process should be identical to each other. However, in our experiments, distinguishability always exists between different photon pairs, characterized by the visibility V of a HOM interference between two heralded photons from different photon pairs. In our experiment, the visibility V is measured as 0.88 ± 0.05, leading to decreased fidelity (see Supplemental Material, Note 3.2, for more details [26]).

However, with the fabrication advancement in ultralow loss silicon nitride (Si_3N_4) material [33], allowing for high collection efficiency in fabrication, we expect that fabricating the same devices on a Si_3N_4 photonic chip will achieve better fidelity in the future. This, in turn, will improve the performance of the QHE protocol (more details are shown in Supplemental Material, Note 4 [26]).

Conclusion.—In summary, this study employs quantum photonic chips to create, execute, and validate a comprehensive fully homomorphic encryption system tailored for universal gate-based quantum computers. This system empowers individuals possessing cryptographic qubits to evaluate any desired quantum circuit by harnessing auxiliary and classical bits generated during the encryption process and seamlessly transmitted alongside ciphertext. The implementation eliminates the necessity for repetitive utilization of quantum or classical communication channels. Moreover, the decryption process does not require a complete comprehension of the evaluated circuit. Furthermore, we have not yet compromised security beyond the assumptions of the classical homomorphic cryptosystem employed in constructing the system. Our findings highlight the feasibility of implementing a proof of concept of QHE on quantum chip, thereby paving the way toward the realization of compact quantum internet. In future endeavors, it is conceivable to construct the server and the client components on independent photonic chips, strategically positioned at significant long distances from each other.

This work was supported by National Research Foundation (NRF2022-QEP2-02-P16), IMDA, and National Research Foundation Singapore (FCP-NTU-RG-2022-013).

Y. L., L. C. and W. L. contributed equally to this work.

The authors declare that they have no competing interests.

[*]Corresponding author: hui-jovie.zhang@polyu.edu.hk
[†]Corresponding author: helen.cai@polyu.edu.hk
[‡]Corresponding author: joe@horizonquantum.com
[§]Corresponding author: song.qinghua@sz.tsinghua.edu.cn
[‖]Corresponding author: aiqun.liu@polyu.edu.hk

[1] D. P. DiVincenzo, Quantum computation, Science **270**, 255 (1995).

[2] D. R. Simon, On the power of quantum computation, SIAM J. Comput. **26**, 1474 (1997).

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2010).

[4] T. Morimae and K. Fujii, Blind topological measurement-based quantum computation, Nat. Commun. **3**, 1036 (2012).

[5] M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing, Phys. Rev. Lett. **115**, 220502 (2015).

[6] C. A. Pérez-Delgado and J. F. Fitzsimons, Iterated gate teleportation and blind quantum computation, Phys. Rev. Lett. **114**, 220502 (2015).

[7] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature (London) **496**, 456 (2013).

[8] M. Liang, Quantum fully homomorphic encryption scheme based on universal quantum circuit, Quantum Inf. Process. **14**, 2749 (2015).

[9] A. M. Childs, Secure assisted quantum computation, Quantum Inf. Comput. **5**, 456 (2005).

[10] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, Interactive proofs for quantum computations, arXiv:1704.04487.

[11] K. A. 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).

[12] A. Broadbent and S. Jeffery, Quantum homomorphic encryption for circuits of low T-gate complexity, in *Annual Cryptology Conference* (Springer, New York, 2015), pp. 609–629.

[13] H. J. Kimble, The quantum internet, Nature (London) **453**, 1023 (2008).

[14] C. Simon, Towards a global quantum network, Nat. Photonics **11**, 678 (2017).

[15] S.-K. Liao, W. Q. Cai, J. Handsteiner, B. Liu, and J. Yin, Satellite-relayed intercontinental quantum network, Phys. Rev. Lett. **120**, 030501 (2018).

[16] S. Hermans, M. Pompili, H. K. C. Beukers, S. Baier, J. Borregaard, and R. Hanson, Qubit teleportation between non-neighbouring nodes in a quantum network, Nature (London) **605**, 663 (2022).

[17] Q.-C. Sun *et al.*, Quantum teleportation with independent sources and prior entanglement distribution over a network, Nat. Photonics **10**, 671 (2016).

[18] W. K. Tham, H. Ferretti, K. Bonsma-Fisher, A. Brodutch, B. C. Sanders, A. M. Steinberg, and S. Jeffery, Experimental demonstration of quantum fully homomorphic encryption with application in a two-party secure protocol, Phys. Rev. X **10**, 011038 (2020).

[19] J. Carolan *et al.*, Universal linear optics, Science **349**, 711 (2015).

[20] X. Qiang *et al.*, Large-scale silicon quantum photonics implementing arbitrary two-qubit processing, Nat. Photonics **12**, 534 (2018).

[21] Y. Li, L. Wan, H. Zhang, H. Zhu, Y. Shi, L. K. Chin, X. Zhou, L. C. Kwek, and A. Q. Liu, Quantum Fredkin and Toffoli gates on a versatile programmable silicon photonic chip, npj Quantum Inf. **8**, 112 (2022).

[22] P. Sibson *et al.*, Chip-based quantum key distribution, Nat. Commun. **8**, 13984 (2017).

[23] G. Zhang *et al.*, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photonics **13**, 839 (2019).

[24] F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, Detector-integrated on-chip QKD receiver for GHz clock rates, npj Quantum Inf. **7**, 40 (2021).

[25] L. Cao, W. Luo, Y. X. Wang, J. Zou, R. D. Yan *et al.*, Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems, Phys. Rev. Appl. **14**, 011001(R) (2020).

[26] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.132.200801 for more description, which includes Refs. [27–32].

[27] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, Silica-on-silicon waveguide quantum circuits, Science **320**, 646 (2008).

[28] 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).

[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] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Probabilistic quantum logic operations using polarizing beam splitters, Phys. Rev. A **64**, 062311 (2001).

[31] E. Knill, R. Laflamme, and G. J. Milburn, A scheme for efficient quantum computation with linear optics, Nature (London) **409**, 46 (2001).

[32] J. W. Wang *et al.*, Chip-to-chip quantum photonic interconnect by path-polarization interconversion, Optica **3**, 407 (2016).

[33] J. F. Bauters, M. J. R. Heck, D. John, D. Dai, M.-C. Tien, J. S. Barton, A. Leinse, R. G. Heideman, D. J. Blumenthal, and J. E. Bowers, Ultra-low-loss high-aspect-ratio Si_3N_4 waveguides, Opt. Express **19**, 3163 (2011).