npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Experimental quantum homomorphic encryption

Jonas Zeuner[1✉], Ioannis Pitsios[2], Si-Hui Tan[3,4], Aditya N. Sharma[1,5], Joseph F. Fitzsimons[3,4,6], Roberto Osellame[2,7] and Philip Walther[1,8]

Quantum computers promise not only to outperform classical machines for certain important tasks, but also to preserve privacy of computation. For example, the blind quantum computing protocol enables secure delegated quantum computation, where a client can protect the privacy of their data and algorithms from a quantum server assigned to run the computation. However, this security comes with the practical limitation that the client and server must communicate after each step of computation. A practical alternative is homomorphic encryption, which does not require any interactions, while providing quantum-enhanced data security for a variety of computations. In this scenario, the server specifies the computation to be performed, and the client provides only the input data, thus enabling secure noninteractive computation. Here, we demonstrate homomorphic-encrypted quantum computing with unitary transformations of individual qubits, as well as multi-qubit quantum walk computations using single-photon states and non-birefringent integrated optics. The client encrypts their input in the photons' polarization state, while the server performs the computation using the path degree of freedom. Our demonstration using integrated quantum photonics underlines the applicability of homomorphic-encrypted quantum computations, and shows the potential for delegated quantum computing using photons.

npj Quantum Information (2021)7:25 ; https://doi.org/10.1038/s41534-020-00340-8

INTRODUCTION

Secure delegated computing has been a longstanding research goal for both the classical and quantum computation communities. The aim is to provide a client (Alice) access to remote computational resources (Bob), while protecting the privacy of Alice's data and Bob's algorithm. In his seminal 2009 paper, Gentry described the first computationally secure, fully homomorphic encryption scheme for classical computing[1]. Here, "computational security" means that the privacy guarantees of the protocol are based on assumptions about an adversary's computational capabilities; "fully" means that any computation is possible. Blind quantum computation was also introduced in 2009 (refs. [2,3]): this protocol addresses a different situation, in which the data and algorithm both belong to Alice, who wants to use Bob's remote computational resources without revealing them. Blind quantum computation has the advantages of being information-theoretically secure (i.e., it does not rely on assumptions about the adversary's technological capabilities) and allowing multiple rounds of communication between Alice and Bob over the course of the computation. Its efficiency is limited by the need for interaction: Alice and Bob must exchange classical information after each step of the computation. Quantum homomorphic encryption—where, in contrast to the scheme of ref. [1], a quantum computation is performed on quantum information—removes the requirement of interactive computation, but necessarily sacrifices either security or computational power to achieve this, in accordance with a no-go theorem: fully homomorphic encryption is impossible if both perfect privacy and non-exponential resource overhead are required[4,5].

The proposal by Rohde et al.[6] shows that relaxing the requirements for (1) universal quantum computation, and (2) perfect privacy enables novel implementations using photonic quantum processors. Photons feature multiple degrees of freedom for encoding quantum information, enabling homomorphic-encrypted quantum walks. Even though quantum walks provide only subsets of universal quantum computation, such computations are of great interest due to their applicability, ranging from machine learning algorithms[7,8] to search algorithms[9–11] and Boson sampling[12–16]. With respect to the security, it is also shown that in any practical encryption application perfect privacy is not required, as long as the maximum amount of information potentially available to an attacker is sufficiently small. Note that we are addressing the task of encrypting a quantum computation, so the security should not be compared with existing classical techniques for classical computation.

RESULTS

Input encoding

In this experiment, we use single-photon qubit input states and an integrated-optics server to experimentally demonstrate the quantum homomorphic protocol described by Rohde et al.[6]. Quantum walk inputs are typically n photons distributed over m spatial modes, with no more than one photon in each mode. The protocol of ref. [6] hides the distribution of these photons by using the photons' polarization to encode Alice's input for the quantum walk: taking advantage of the fact that orthogonally polarized photons do not interfere. Otherwise empty modes are populated with ancilla photons.

Thus, to implement an m-mode quantum walk of n "walker" photons, rather than inputting one photon into each of n modes and leaving the remaining $m-n$ empty, we also input $m-n$

[1]Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Vienna, Austria. [2]Istituto di Fotonica e Nanotecnologie - Consiglio Nazionale delle Ricerche (IFN-CNR), Milano, Italy. [3]Singapore University of Technology and Design, Singapore, Singapore. [4]Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore. [5]Joint Quantum Institute, University of Maryland, College Park, MD, USA. [6]Erwin Schrödinger International Institute for Mathematics and Physics, Wien, Austria. [7]Department of Physics - Politecnico di Milano, Milano, Italy. [8]Christian Doppler Laboratory for Photonic Quantum Computer, Faculty of Physics, University of Vienna, Vienna, Austria. ✉email: jonas.zeuner@univie.ac.at

Published in partnership with The University of New South Wales

npj nature partner journals

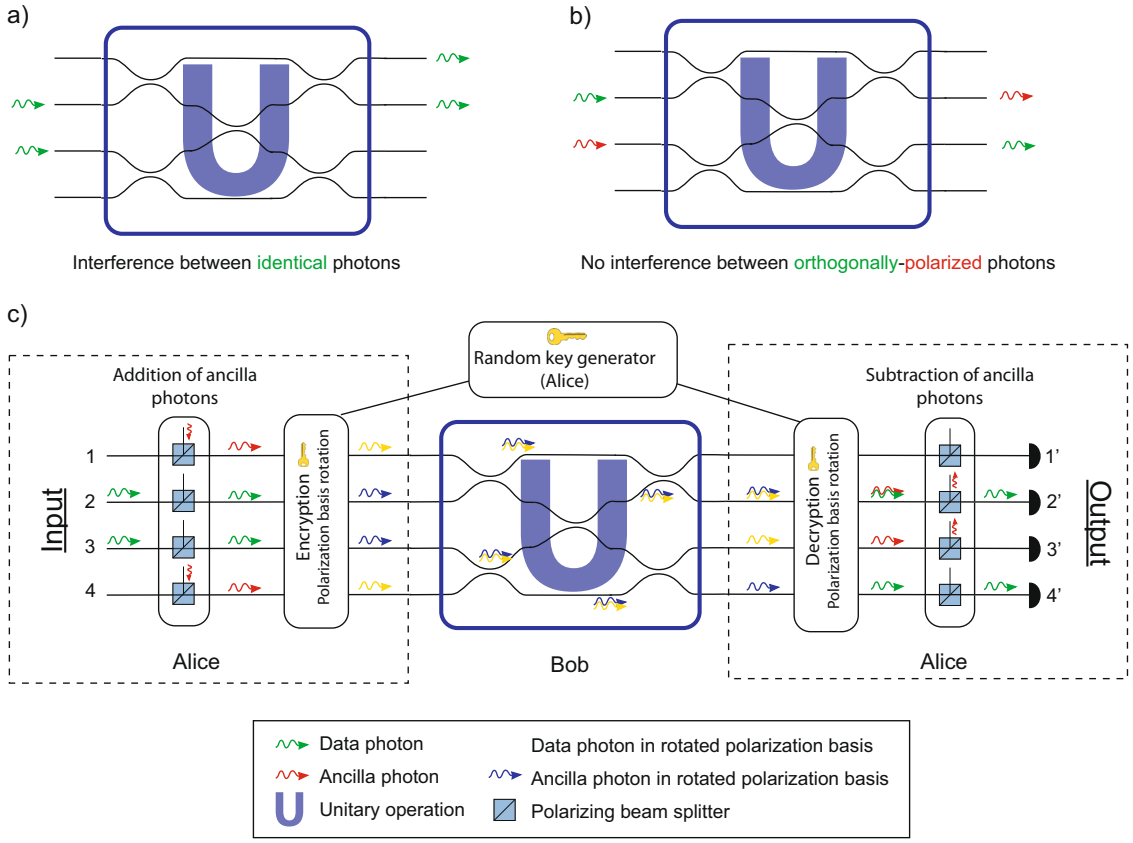

Fig. 1 Homomorphic encryption scheme. a Phase shifters and directional couplers can be used to implement any desired unitary transformation for arbitrary dimensions, either for single- or multi-photon states[27,28]. In the case of indistinguishable photons entering the circuit simultaneously, quantum interference leads to nontrivial outputs of a so-called quantum walk computation. **b** If two orthogonally polarized photons enter the circuit at the same time they are distinguishable and therefore no quantum interference takes place. **c** In the implemented quantum homomorphic encryption scheme, Alice prepares her input state by encoding the desired photon-number state in the {*H*, *V*} polarization basis and then encrypting it by applying a randomly chosen polarization transformation on all photons. Bob performs the quantum computation on the encrypted state and returns the photons to Alice. Alice undoes the previous transformation (R^{-1}) and measures the photons in the {*H*, *V*} basis, obtaining the outcome of the quantum computation. Since Bob has no information about the polarization basis chosen by Alice, his information about Alice's input state is limited.

"dummy" photons in the otherwise empty modes, with polarizations orthogonal to the *n* photons representing the walkers. For example, an input state $|\Psi_{\text{in}}\rangle = |1,0,0,0\rangle$ for a traditional quantum walk (written in the occupation-number basis) would be encoded in this scheme as $|\Psi_{\text{in, encoded}}\rangle = |H,V,V,V\rangle$, where $|H\rangle(|V\rangle)$ represents horizontal (vertical) polarization. Measuring the output photons in the {*H*, *V*} basis then yields the same result as the traditional occupation-number quantum walk. The purpose of this approach is to enable polarization encryption of Alice's input state: without knowing the basis in which Alice's input is encoded, Bob can guess Alice's input state with only limited probability of success. To encrypt the input state Ψ_{in}, Alice randomly chooses a key, a polarization state $|X\rangle$ taken from a set of *d* uniformly distributed points on the Poincaré sphere, where *d* is the number of polarization basis choices available to her. To encrypt her data, Alice rotates the polarizations of her qubits from $|H\rangle$ and $|V\rangle$ to $|X\rangle$ and $|X^{\perp}\rangle$. Alice sends this encrypted state to Bob, who performs the quantum walk. Bob returns the output photons to Alice, and she measures them in the {*X*, $X^{\perp}$} basis, obtaining the result of the quantum walk (Fig. 1).

If Bob tried to decipher Alice's encrypted state, the amount of information he could extract is bounded by the Holevo quantity[17]. One straightforward attack Bob could employ is to randomly choose a basis, in which to measure all *m* photons: in fact, this attack is close to optimal, almost saturating the Holevo bound. In the limit of large *d* and *m*, the success probability of this attack is $p_{\text{B}} = 1/\sqrt{\pi m}$. For an in-depth description of the protocol see ref. [6]. The protocol also ensures the privacy of Bob's algorithm. Since Alice only knows the input and output states of the computation, the amount of information that she can extract about Bob's algorithm is proportional to that of a "black-box" function: the more queries she is allowed to send, the more accurately she can guess the function. It is important to note that both Alice and Bob have an interest in performing a certain computation on a certain input state exactly once, since both of them increasingly compromise the privacy of their respective secrets with increasing number of repetitions of the computation. The no-go theorem[4] asserts that this limitation is unavoidable.

Experimental realization

In our experimental demonstration, Alice produces four photons using two spontaneous parametric down-conversion (SPDC) sources (see "Methods") and prepares them in a randomly chosen polarization state using a polarizer, half-wave plate (HWP), and quarter-wave plate (QWP) for each photon. Alice can create input states of any polarization with a fidelity of (99.5 ± 0.1)%, the main source of error being imperfect polarization compensation of the single-mode fibers leading to the chip. After preparing the encrypted input state, Alice sends the photons to Bob, who performs the quantum walk.

In order for the scheme to work, Bob's chip must implement the same unitary for the photons' path degree of freedom regardless

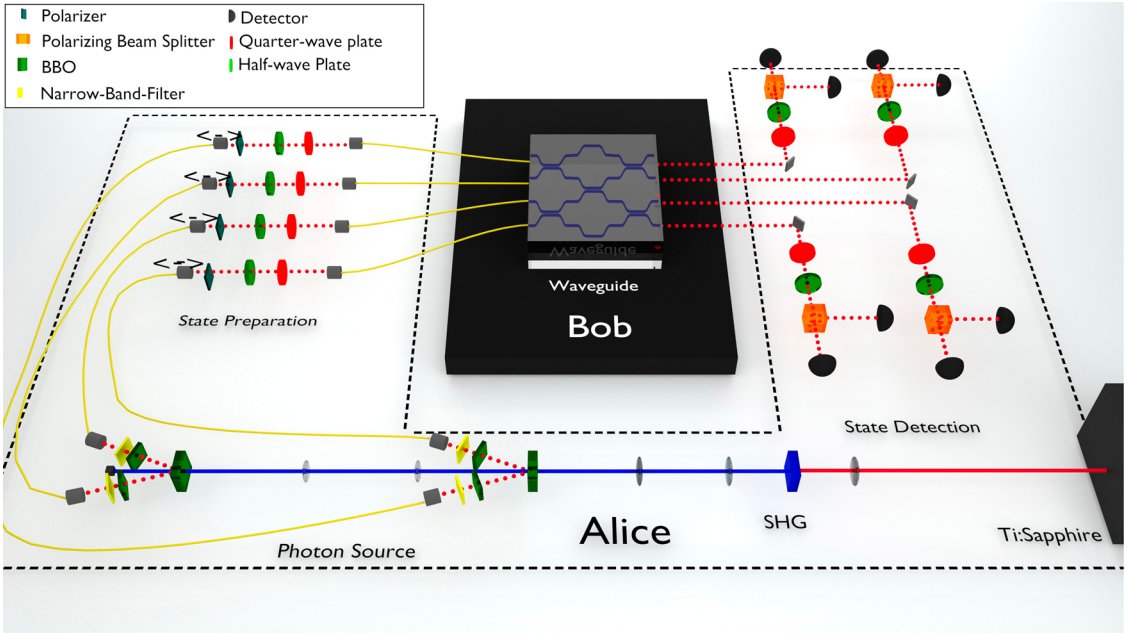

Fig. 2 Experimental setup. A Ti:Sapphire laser is used to pump two nonlinear β-barium borate crystals, each probabilistically producing exactly one pair via type-II spontaneous parametric down conversion. These photons are spectrally filtered and sent through polarizers to prepare a pure, separable four-photon state. The four photons are coupled to single-mode fibers and synchronized in the delay stage, using adjustable free-space delays (indicated by the double arrows). Using half-wave plates (HWPs) and quarter-wave plates (QWPs) Alice can prepare arbitrary polarization states before sending the photons to Bob, who will perform the quantum walk. After exiting Bob's chip, the four output modes are collimated by a lens and sent back to Alice. She uses the detection stage (HWP, QWP, polarizing beam splitter (PBS), and single-photon detector for each photon) to projectively measure the photons and recover the outcome of the quantum walk.

of the input polarizations used—otherwise, the outcome would depend on Alice's choice of key. Although laser-written waveguides support propagation of all polarizations, they typically have slightly different refractive indices for H and V polarizations ($\Delta n \approx 10^{-5}$), making it a challenge to implement nontrivial polarization-independent path unitaries. To achieve this, we used an annealing procedure to fabricate waveguides with birefringences $\Delta n < 10^{-6}$ (see "Methods").

After the quantum walk, Bob returns the photons to Alice, who projects them in her previously chosen polarization basis using QWPs, HWPs, polarizing beam splitters (PBSs), and single-photon detectors. To demonstrate the fidelity of the homomorphic-encrypted quantum walk, we chose a canonical set of two mutually unbiased polarization bases and performed quantum walks with one, two, and three walkers using two different unitaries, each with $m = 4$ inputs and outputs. We used $\{H, V\}$ (parallel and orthogonal, respectively, to the chip surface) and $\{D, A\}$ ($|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$). We characterized the unitary and compared the output probability distributions with theoretical predictions, finding the mean overlap (Bhattacharyya distance[18]) between the predictions and results from all quantum walks to be $(0.995 \pm 0.014)\%$ for the first unitary and $(0.986 \pm 0.012)\%$ for the second (Fig. 2). Note that the fluctuation in the size of the error bar of the simulated data is due to the nonlinear behavior of the sine function: the same error in estimating the phase of the unitary can lead to different errors in output probabilities. The table of the unitaries can be found in Supplementary Note 1.

Security guarantees

The security guarantees for Alice's plaintext input state can be quantified in various ways. The trace distance between the different input states that she can produce with four photons is 0.81 for Hamming distances 1 and 3, and 0.85 for Hamming distance 2 (ref. [19]). As a result, Bob cannot perfectly distinguish any pair of possible plaintexts. Furthermore, the mutual information between her plaintext string and Bob is bounded by the Holevo quantity to be no >1.96 bits (see "Supplementary Information"). To experimentally verify the security of Alice's input, we implemented the attack described above: Bob measures all of Alice's four photons in a randomly chosen basis (here we choose $|H\rangle$ for simplicity). Alice encrypts her plaintext input state (here we use $|1,1,1,1\rangle \equiv |H,H,H,H\rangle$) by choosing between $d = 2$, 3, 4, 6, 12 different linear polarization bases (keys). The probability of Bob guessing Alice's plaintext input state can then be determined from the fraction of fourfold coincidence detections Bob measures with polarization $|H,H,H,H\rangle$ (see Fig. 3a). In the case of $m = 4$ and $d = 2$, Bob has a 50% chance of guessing the correct polarization basis. As the number of bases is increased, Bob's probability of determining the input states asymptotically approaches $p = 0.27$. The privacy of Alice's input state increases with both the number of modes m and number of keys d: Fig. 3b shows this dependence. It is important to note that current technology already enables almost arbitrarily large d, using high-quality phase retarders, and m on the order of dozens, thanks to rapid developments in integrated optics.

DISCUSSION

We have demonstrated homomorphic-encrypted quantum computations for single-photon transformations and quantum walks with up to three walkers. Our photonic system's specially engineered features allowed us to encrypt Alice's plaintext input state in polarization, while performing computations using the path degree of freedom. The security of Alice's plaintext input is necessarily limited by the number of modes used, i.e., by the number of available photons—however, the continuing advances in photon-source technology will enable similar demonstrations using more modes in the future. As mentioned earlier, in this protocol, a computation can only be attempted once, since each successive attempt would reduce security for both parties; to

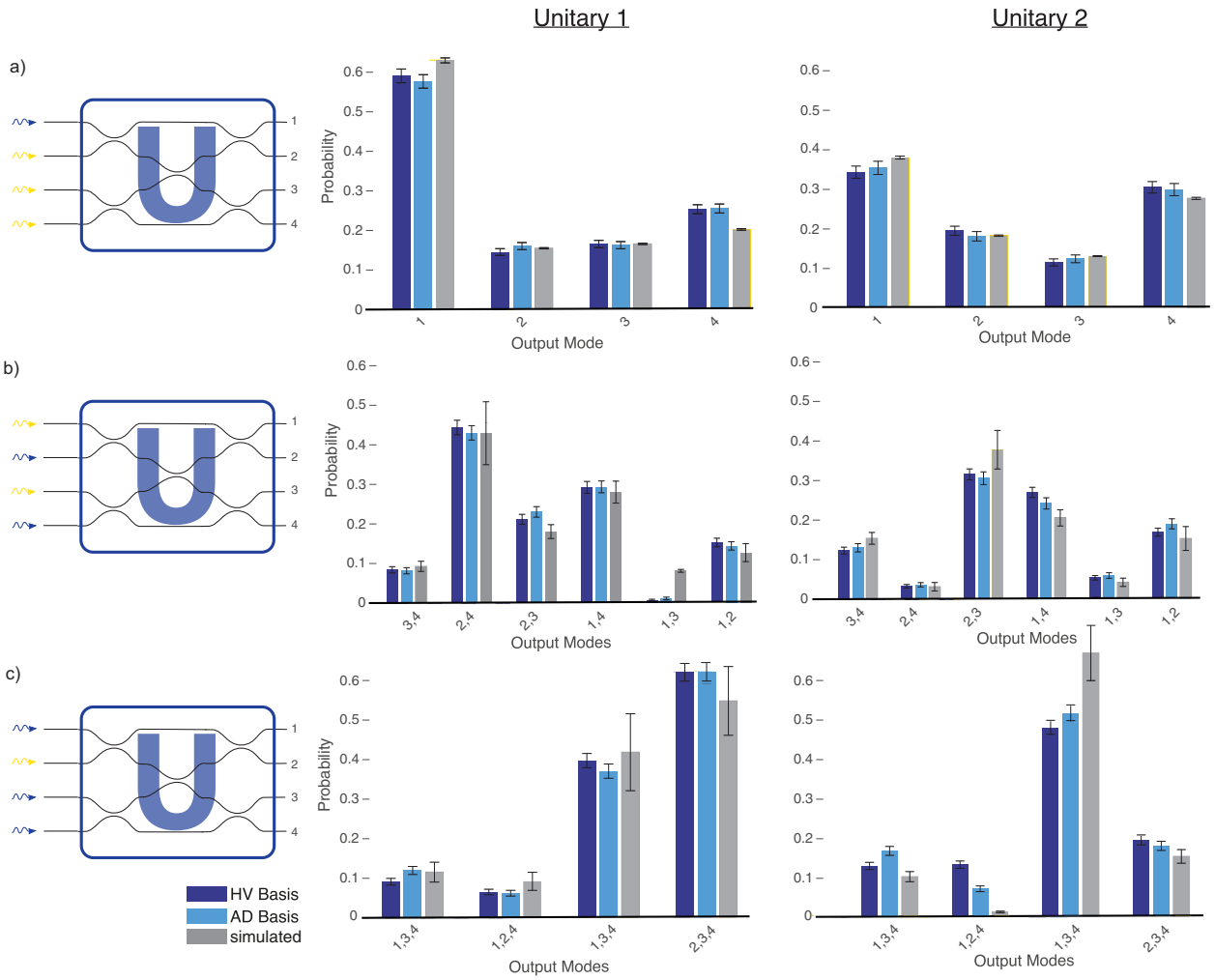

Fig. 3 Results of the encrypted quantum walk. We use two different unitaries to execute multiple encrypted quantum walk computations. **a** Unitary transformation of a single-photon state, **b** quantum walk with two photons, and **c** quantum walk with three photons. Blue photons represent data photons, whereas yellow photons are ancilla photons used to mask the computation that is performed (see Fig. 1). The output probability distribution for two different unitaries is shown. In each case, the computation was performed in two mutually unbiased polarization bases (see "Supplementary Information"). The fidelities (Bhattacharyya distance[18]) between the simulated (see "Methods") and measured probabilities are **a** 0.99±0.02, **b** 0.99±0.02, and **c** 0.99±0.03 and demonstrate the polarization independence of the computation. More data and discussion of error analysis is provided in "Methods" and the "Supplementary Information".

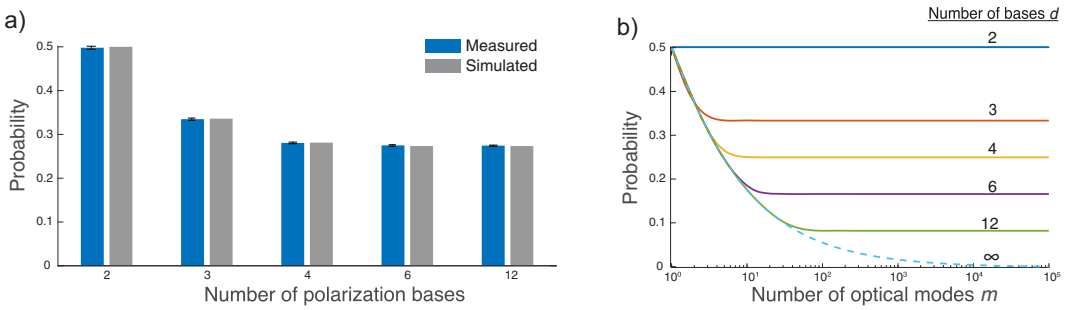

Fig. 4 Privacy of the input state for the computation. A nearly optimal attack is for Bob to measure all of Alice's photons in a randomly chosen basis. The security of Alice's input depends on the number d of polarization bases (keys) d she can choose from and also the number of input modes m. **a** Probability of Bob correctly guessing Alice's input for m=4, as key size is increased from d=2 to d=12. **b** Calculated probability of correctly guessing the input with respect to number of bases d (lines) and modes m. The blue dashed line shows the asymptotic behavior for an infinite key number. All lines are theoretical upper bounds (see "Methods" for formula).

make this technique practical, we would require advances in quantum error correction to increase the probability of successful operation in the presence of loss. Further improvements can be made by encrypting in a different photonic degree of freedom with more than two levels. For example, orbital angular momentum enables, in principle, arbitrarily high-dimensional encoding, and transmission of such states in optical fiber has already been demonstrated[20]. Using an a-level degree of freedom for encoding, instead of polarization, the amount of hidden information can be improved from $\log_2(m)$ scaling to $m\log_2(a/m) + m(\log(2))^{-1}$ (ref. [21]). As we have shown here, although perfect security for universal computation (without exponential resource overhead) is forbidden[4,5], relaxing these conditions can enable interesting applications. Determining the ideal mix of security, performance, and generality of the computation remains an active topic of research.

METHODS

Experimental setup

Our experimental setup is shown in Fig. 4. We generate all four photons using degenerate, noncollinear type-II SPDC. Two separate 2-mm thick β-barium borate (BBO) crystals are pumped by a Ti:Sapphire laser (Coherent Chameleon Ultra II, 789 nm, 150 fs duration, 80 MHz repetition rate, and 3.6 W average power) which has been frequency doubled to 394.5 nm using second harmonic generation in a 5-mm thick lithium triborate crystal. The photons emitted by the crystals pass through 1-mm thick BBO crystals of the same cut angle as the SPDC crystals to compensate for spatial and temporal walk-off before being spectrally filtered by 3-nm bandwidth spectral filters centered at 789 nm, and spatially filtered by single-mode optical fibers (SMFs) of type Nufern 780-HP. All photons pass through polarizers to create pure polarization states and then through a HWP and QWP to enable the creation of arbitrary polarizations states. The QWP and HWP were rotated using highly precise motorized rotation mounts with a precision of 0.02°. Adjustable free-space delay lines are used to synchronize the photons such that they all arrive at the chip within their coherence time of ~300 fs. The photons are coupled to the chip using a 127-µm pitch v-groove array of Nufern 780-HP fibers. The (5×5) µm fiber mode field has a high overlap with the mode field of the waveguides, which are of equivalent size. On the output facet of the chip, the photons are collimated using a lens and sent to the detection stage. Using a QWP, HWP, and a PBS and avalanche photodiodes (APDs), the photons can be detected in any desired polarization basis. The overall transmission (from fiber in-coupling to APDs) was measured to be $(50 \pm 5)\%$.

Waveguide details

The four-mode optical circuit for our quantum walk was fabricated by direct laser writing in Corning Eagle-XG borosilicate glass. The laser source we employed was a Yb:KYW cavity-dumped oscillator at 1030 nm wavelength, emitting pulses of 300 fs duration, and at 1 MHz repetition rate. The laser beam was focused into the bulk of the glass substrate using a 50×, 0.6 NA microscope objective, and the inscription of the optical waveguides was performed by translating the glass (with respect to the objective's focus), with a computer-controlled three-axis Aerotech FiberGlide 3D series stage, at a tangential velocity of 40 mm/s. The waveguides were inscribed at a depth of 170 µm, with 270 mW of laser power, using a multiple irradiation approach (five times per waveguide), and then they were annealed. The thermal processing makes the optical circuits polarization insensitive[22], and leads to more favorable bending losses[23]. Overall, we were able to achieve transmissivities of up to $(52.6 \pm 3)\%$ for 22 mm long devices, with bending radii of 90 mm. We fabricated several different photonic circuits with the geometry shown in Fig. 4, and tuned the power splitting of the directional couplers by modifying their interaction length. We reconstructed the unitary transformations implemented (see "Supplementary Information"), using methods demonstrated in refs. [24,25] and subsequent numerical optimization. The unitaries implemented were chosen randomly by designing a default circuit and adjusting the coupling constant in each of the directional couplers. By carefully designing the optical path lengths and characterizing the coupling constants any desired unitary can be implemented with high precision.

Holevo information

To analyze the amount of information Bob can gain from a single copy of Alice's state, we calculate the Holevo quantity

$$\chi(m) = -\mathrm{Tr}(\rho \log_2 \rho) + \frac{1}{2^m}\sum_{i=0}^{2^m-1} \mathrm{Tr}(\rho_i \log_2 \rho_i), \tag{1}$$

where $\rho = \frac{1}{2^m}\sum_{i=1}^{2^m} \rho_i$ and $\rho_i = \bigotimes_{k=0}^{d-1} R(\frac{k\pi}{d})|P_{ij}\rangle \times \langle P_{ij}|R(-\frac{k\pi}{d})$ and $|P_{ij}\rangle = |H\rangle$, when the jth bit of i is 0, otherwise $|P_{ij}\rangle = |V\rangle$ (ref. [6]). In our experiment $m = 4$ and 12, yielding

$$\chi(4) = 1.9694\,. \tag{2}$$

Note that for elliptical polarization encodings the Holevo information is halved, but the scaling in m remains the same (see "Supplementary Information").

Bob's random attack

The simplest attack is realized by measuring all photons in the same basis as described in ref. [6]. The probability of inferring the correct state is then given by

$$p = \frac{1}{d}\sum_{j=0}^{d-1} \cos^{2m}\left(\frac{j\pi}{d}\right) \tag{3}$$

with the number of spatial modes m and the number of possible polarization bases d.

Measurement errors

The main drawback of down-conversion sources is that their emission is probabilistic. This is especially problematic for our experiment, where the probability of simultaneously generating exactly one pair in each crystal, as desired, equals the probability of generating exactly two pairs in one of the crystals. In our setup, we circumvented this problem by making the pairs from the two sources distinguishable by polarization. For input states, in which one photon has polarization orthogonal to that of the other three, the input polarization could be set to either $|H,H\rangle$ or $|V,V\rangle$ for source 1, as needed, and $|H,V\rangle$ for source 2: then Alice's final polarization measurement would distinguish the events of interest from those in which one crystal created all four photons. We can also deal with input states with two $|H\rangle$ photons and two $|V\rangle$ photons by having sources 1 and 2 produce $|H,H\rangle$ and $|V,V\rangle$, respectively, and rewiring the input channels to the chip as needed. Double-pair emission for input states $|H,H,H,H\rangle$ and $|V,V,V,V\rangle$ cannot be dealt with this way, but these states are not of interest for a quantum walk.

Having suppressed errors from double-pair emission, we must now consider triple-pair emission. The noise contributed by these events is on the order of the sources' per-pulse emission probability, which is 0.14%.

To quantify the spectral distinguishability of our photons, we measured Hong-Ou-Mandel interference visibility for all four combinations of signal and idler from source 1 with signal and idler from source 2. After subtracting statistically expected higher-order noise, we measured the visibilities to be

$$V = \frac{C_{\max} - C_{\min}}{C_{\max}} = 0.88 \pm 0.05, \tag{4}$$

and $V = 0.77 \pm 0.05$ without subtracting higher-order noise. This is the main contributing error, diminishing the overlap with the simulated output distribution in the random walk, and it explains the lowering of the fidelity with increasing photon number. For more discussion of experimental errors in quantum walks, see ref. [26]. We assumed Poissonian error for all single-photon detection rates, so that for N detections, we assume an error of $\epsilon = \sqrt{N}$.

The error in the reconstructed unitary propagates from errors in our intensity measurements, which are in turn used to infer amplitudes and phases. Here, we are able to limit the error on the inferred transmission amplitudes and phases to 1% and 50 mrad, respectively. The discrepancy in error-bar size for the various output possibilities stems from the nature of the unitary: phase errors can lead to large changes in some output probabilities, while having hardly any effect in others.

DATA AVAILABILITY

The authors declare that the main data supporting the finding of this study are available within the article and its Supplementary Information. The additional data can be provided upon request.

Received: 17 April 2019; Accepted: 18 September 2020;
Published online: 05 February 2021

REFERENCES

1. Gentry, C. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC* (Association for Computing Machinery, New York, 2009).
2. Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, 517–526 (IEEE, Los Alamitos, CA, 2009).
3. Barz, S. et al. Demonstration of blind quantum computing. *Science* **335**, 303–308 (2012).
4. Yu, L., Pérez-Delgado, C. A. & Fitzsimons, J. F. Limitations on information-theoretically-secure quantum homomorphic encryption. *Phys. Rev. A* **90**, 050303 (2014).
5. Newman, M. & Shi, Y. Limitations on transversal computation through quantum homomorphic encryption. *Quantum Info. Comput.* **18**, 927–948 (2018).
6. Rohde, P. P., Fitzsimons, J. F. & Gilchrist, A. Quantum walks with encrypted data. *Phys. Rev. Lett.* **109**, 150501 (2012).
7. Adcock, J. et al. Advances in quantum machine learning. Preprint at https://arxiv.org/abs/1512.02900 (2015).
8. Paparo, G. D., Dunjko, V., Makmal, A., Martin-Delgado, M. A. & Briegel, H. J. Quantum speedup for active learning agents. *Phys. Rev. X* **4**, 031002 (2014).
9. Childs, A. M. et al. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the Thirty-fifth Annual Acm Symposium on Theory of Computing*, 59–68 (ACM, 2003).
10. Szegedy, M. Quantum speed-up of markov chain based algorithms. In *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, 32-41 (IEEE Computer Society, Los Alamitos, CA, USA, 2004).
11. Ambainis, A. Quantum walk algorithm for element distinctness. *SIAM J. Comput.* **37**, 210–239 (2007).
12. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, 333–342 (ACM, 2011).
13. Tillmann, M. et al. Experimental boson sampling. *Nat. Photonics* **7**, 540–544 (2013).
14. Spagnolo, N. et al. Experimental validation of photonic boson sampling. *Nat. Photonics* **8**, 615–620 (2014).
15. Broome, M. A. et al. Photonic boson sampling in a tunable circuit. *Science* **339**, 794–798 (2013).
16. Carolan, J. et al. Universal linear optics. *Science* **349**, 711–716 (2015).
17. Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.* **9**, 3–11 (1973).
18. Bhattacharyya, A. On a measure of divergence between two statistical populations defined by their probability distribution. *Bull. Calcutta Math. Soc.* **35**, 99–109 (1943).
19. Hamming, R. W. Error detecting and error correcting codes. *Bell Labs Tech. J.* **29**, 147–160 (1950).
20. Bozinovic, N. et al. Terabit-scale orbital angular momentum mode division multiplexing in fibers. *Science* **340**, 1545–1548 (2013).
21. Tan, S.-H., Kettlewell, J. A., Ouyang, Y., Chen, L. & Fitzsimons, J. F. A quantum approach to homomorphic encryption. *Sci. Rep.* **6**, 33467 (2016).
22. Corrielli, G. et al. Symmetric polarization insensitive directional couplers fabricated by femtosecond laser waveguide writing. Preprint at https://arxiv.org/abs/1801.03764 (2018).
23. Arriola, A. et al. Low bend loss waveguides enable compact, efficient 3d photonic chips. *Opt. Express* **21**, 2978–2986 (2013).
24. Rahimi-Keshari, S. et al. Direct characterization of linear-optical networks. *Opt. Express* **21**, 13450–13458 (2013).
25. Heilmann, R., Gräfe, M., Nolte, S. & Szameit, A. A novel integrated quantum circuit for high-order w-state generation and its highly precise characterization. *Sci. Bull.* **60**, 96–100 (2015).
26. Tillmann, M. et al. Generalized multiphoton quantum interference. *Phys. Rev. X* **5**, 041015 (2015).
27. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58 (1994).
28. Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walmsley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460–1465 (2016).

ACKNOWLEDGEMENTS

P.W. acknowledges support from the research platform TURIS, the Austrian Science Fund (FWF) through the Doctoral Programme CoQuS (no. W1210-4), BeyondC (F7113), and NaMuG (P30067-N36), the United States Air Force Office of Scientific Research via QAT4SECOMP (FA2386-17-1-4011) and Red Bull GmbH. P.W. and R.O. acknowledge support from the European Commission via Photonic Integrated Compound Quantum Encoding (PICQUE; no. 608062), Quantum Simulation on a Photonic Chip (QUCHIP; no. 641039) projects, and High-dimensional quantum Photonic Platform projects (HiPhoP; no. 731473). S.-H.T. and J.F.F. acknowledge support from Singapore's National Research Foundation under NRF award NRF-NRFF2013-01 and from the United States Air Force Office of Scientific Research under grant no. FA2386-15-1-4082.

AUTHOR CONTRIBUTIONS

J.Z and A.N.S. built the setup and carried out data collection, and performed data analysis, I.P. designed and fabricated the chip, S.-H.T. and A.N.S. contributed to the theoretical calculations, J.F.F., R.O., and P.W. supervised the project. All authors contributed to writing the paper.

COMPETING INTERESTS

J.F.F. has financial holdings in Horizon Quantum Computing Pte Ltd.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-020-00340-8.

Correspondence and requests for materials should be addressed to J.Z.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.