PHYSICAL REVIEW A **94**, 020301(R) (2016)

Experimental quantum data locking

Yang Liu,[1,2] Zhu Cao,[3] Cheng Wu,[1,2] Daiji Fukuda,[4] Lixing You,[5] Jiaqiang Zhong,[6] Takayuki Numata,[4] Sijing Chen,[5] Weijun Zhang,[5] Sheng-Cai Shi,[6] Chao-Yang Lu,[1,2] Zhen Wang,[5] Xiongfeng Ma,[3,*] Jingyun Fan,[1,2,†] Qiang Zhang,[1,2,‡] and Jian-Wei Pan[1,2,§]

[1]*Shanghai Branch, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, People's Republic of China*

[4]*National Metrology Institute of Japan, National Institute of Advanced Industrial Science and Technology, 1-1-1 Umezono, Tsukuba, Ibaraki 305-8563, Japan*

[5]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, People's Republic of China*

[6]*Purple Mountain Observatory and Key Laboratory of Radio Astronomy, Chinese Academy of Sciences, 2 West Beijing Road, Nanjing, Jiangsu 210008, People's Republic of China*

(Received 12 May 2016; published 12 August 2016)

Classical correlation can be locked via quantum means: quantum data locking. With a short secret key, one can lock an exponentially large amount of information in order to make it inaccessible to unauthorized users without the key. Quantum data locking presents a resource-efficient alternative to one-time pad encryption which requires a key no shorter than the message. We report experimental demonstrations of a quantum data locking scheme originally proposed by D. P. DiVincenzo *et al.* [Phys. Rev. Lett. **92**, 067902 (2004)] and a loss-tolerant scheme developed by O. Fawzi *et al.* [J. ACM **60**, 44 (2013)]. We observe that the unlocked amount of information is larger than the key size in both experiments, exhibiting strong violation of the incremental proportionality property of classical information theory. As an application example, we show the successful transmission of a photo over a lossy channel with quantum data (un)locking and error correction.

DOI: 10.1103/PhysRevA.94.020301

Introduction. Information security continuously remains the research frontier, driven by both scientific curiosity and the increasing demand for practical applications in secure communications and secure data storage. Conventionally, information security is based on computation complexity, which can be broken if one is equipped with enough computational capacity. Quantum mechanics fundamentally changes the game. The inherent quantum correlation enables exponential speedup in computing and unconditional information security [1]. Quantum key distribution [2,3], which allows two parties to generate secure keys with the help of quantum mechanics, has been demonstrated in metropolitan networks [4–8] and is ready to be commercialized. The most reliable encryption method is to encrypt the message with one-time pad encryption [9], where the required key size is at least as large as the size of the information. Quantum data locking allows one to lock information in quantum states with an exponentially shorter key, presenting an efficient solution to many resource-limited secure applications [10–13].

The incremental proportionality of mutual information is an axiomatic property in classical information theory. Consider the following example with two parties, Alice and Bob, who start with no mutual information. First, Alice classically encodes an n-bit message into an n-bit code word using a k-bit key and sends the encoded message (but not the key) to Bob. The two parties then share n-bit mutual information. After Alice sends the key to Bob, their mutual information increases by k. DiVincenzo, Horodecki, Leung, Smolin, and Terhal (DHLST) [10] found that a k-bit key can increase the mutual information by an amount more than k via quantum means. This striking result of quantum data locking is due to the inherent quantum uncertainty and violates the incremental proportionality property of classical information theory in an extreme manner. Quantum data locking has received much attention since then. It was even considered to hold the potential to reconcile the black-hole information loss [13–15].

One of the key issues for the original quantum data-locking scheme lies in the fact that message information may suffer from significant qubit loss. In 2013, Fawzi, Hayden, and Sen (FHS) developed a loss-tolerant quantum data-locking scheme [11], in which the possible information leakage can be made arbitrarily small in a lossy environment while the unlocked information is significantly larger than the key size [16]. This makes quantum data locking appealing for realistic applications such as secure communication [12,13].

Locking capacity is defined as the maximum accessible information to be locked with exponentially small error probability and information leakage ϵ [17]. It is larger than or equal to the private capacity which is the maximum rate for secure information exchange according to the Holevo information [18,19]. The main drawback of this definition is that the accessible information criterion does not ensure

*xma@tsinghua.edu.cn
†fanjy@ustc.edu.cn
‡qiangzh@ustc.edu.cn
§pan@ustc.edu.cn

composable security in data locking [20]. The composable security may be fulfilled conditional on the bounded quantum storage assumption [16,18] that Eve can keep her qubits only for a limited time (or in limited number), which is satisfied for a memoryless communication channel or the case without good quantum memories. For the latter case, the two parties may perform error reconciliation after Eve's quantum memory decoheres; then the key generated by the quantum locked key distribution is composably secure.

Experimental realization of quantum data locking was considered to be a technical challenge [13]. Here, we report experimental demonstrations of both the DHLST scheme and the FHS scheme with heralded single photons. We develop a robust experimental system with an overall single-photon transmittance η, from preparation to detection, of $>50\%$. We employ two types of state-of-the-art superconducting single-photon detectors, a superconducting nanowire single-photon detector (SNSPD) [21,22] and a superconducting transition-edge sensor (TES) [23,24], in our experiment. The fast time response of SNSPD allows encoding or decoding in real time, which is critical to the FHS scheme, and TES has high single-photon detection efficiency, which is necessary to fulfill the requirement to implement the DHLST scheme. The robust system allows the experiment to run continuously for over 50 h in order to show high data-locking efficiency for the FHS scheme. In addition, a comprehensive simulation with an experimentally determined single-photon transmittance and bit-error rate e_b is performed to optimize the parameters of the FHS scheme. Our experimental results solidly demonstrate data locking in a variety of experimental settings, suggesting that quantum data locking has promising applications in secure communication and secure storage. In the following, we present data-locking schemes and our experimental results.

Data-locking schemes. In the DHLST scheme, Alice encodes messages with a set of orthonormal bases and then encrypts the messages by applying a unitary operation, an identity or Hadamard transform depending on whether the key bit is 0 or 1, to each of the qubits. In quantum information, it can be shown that the maximum amount of accessible mutual information is $n/2$ without the one-bit key, while the n-bit message can be completely recovered with the one-bit key.

The DHLST scheme cannot scale up as Eve may get more information than Bob when the system efficiency is less than 50%. The FHS scheme solves this problem by using a longer key to constrain Eve's information to be arbitrarily small. This scheme is the first explicit loss-tolerant locking scheme. Central to this scheme is combining mutually unbiased bases and permutation extractors in the preparation of a set of unitaries. The implementation of the former bounds the probability that Eve may guess the outcome of the associated measurement, and the implementation of the latter is to further distill the randomness into almost uniform bits [11]. A random draw from the set of unitaries is used as the key to encrypt the messages. The implementation of this scheme consists of two encoding stages. In the first stage, a block of the message is converted to the eigenstates of the Z (denoted as 0) or Y basis (denoted as 1). The basis is set according to a Reed-Solomon code concatenated with a Hadamard code. By doing so, the Hamming distance between different messages after encryption is pairwisely maximal. In the second stage, the produced qubit sequence is transformed with a strong permutation extractor to further optimize its difference from the original message statistically. The decoding process is a time reversal of the encoding process. Note that the classical permutation may be performed prior to the partial Hadamard transform. (See the Supplemental Material for details about the realization of the FHS scheme [25].)

In the FHS scheme, the basis choices consume a secret key of length $\log(2/\epsilon^2)$, and the permutation extractor consumes a key of length $40\,000\log(24n^2/\epsilon)$. As shown in the Supplemental Material, the mutual information is $6\epsilon n/16.12 + H(\epsilon)$ if the key is unknown and expands to $\eta \times n/16.12[1 - H(e_b)]$ if the secret key is known. Here $H(\cdot)$ is the binary Shannon entropy, and the information is calculated excluding the key. All the Logarithms are in base 2.

Experiment setup. We experimentally demonstrate quantum data-locking schemes with single photons. As shown in Fig. 1, we pass single-spatial-mode 780-nm laser light through a 10-mm, periodically poled potassium titanyl phosphate (PPKTP) crystal, which converts the pump photons into pairs of daughter photons at 1560 nm via a type-II spontaneous parametric down-conversion process [26]. The pair of correlated, orthogonally polarized daughter photons is separated by a polarizing beam splitter (PBS) and then coupled into single-mode optical fibers. We remove the residual pump photons by dichroic mirrors. We herald the presence of single photons by detecting their twin partners. With the beam waists set to be 180 and 85 μm for the pump and collection beams at the center of the crystal, respectively, the single-photon heralding efficiency is determined to be 87%, including all losses in the photon-pair source setup [27–29].

The experimental implementations of the two data-locking schemes are similar. Because the DHLST scheme uses only a 1-bit preshared key to choose basis Z or Y, we use one Pockels cell to encode the messages in the experiment. In the FHS scheme, a time-varying basis sequence is required. We modulate the messages and bases using two successive Pockels cells. As shown in Fig. 1, Alice first brings the single photons to free space and passes them through a PBS. Then she encodes the message by setting the first Pockels cell to zero or $\lambda/2$ voltage and chooses the bases by setting the second Pockels cell to zero or $\lambda/4$ voltage. Both Pockels cells are initially oriented at 45° with respect to the vertical axis. When applied with $\lambda/2$ or $\lambda/4$ voltage, the first Pockels cell functions as a half-wave plate oriented at 45°, and the second Pockels cell functions as a quarter-wave plate oriented at 45°. After encoding, the photons are coupled into single-mode fibers for delivery. Bob uses a Pockels cell to set his bases similarly by applying zero or $\lambda/4$ voltage. The loss in the encoding (decoding) process is determined to be 7%, which is mainly due to the mismatch between the free-space optical mode and the fiber optical mode.

We use a SNSPD with a timing jitter of $\tau \sim 70$ ps as the heralding detector. The fast timing response allows us to orient Pockels cells appropriately to encode or decode messages in real time, and the relatively high detection efficiency (50%) helps us to create a good rate of single photons to reduce the running time of the experiment. We use a TES to detect the signal photons at the receiver. The single-photon detection efficiency of the TES is determined to be 75% when it is held at $\sim$100 mK.

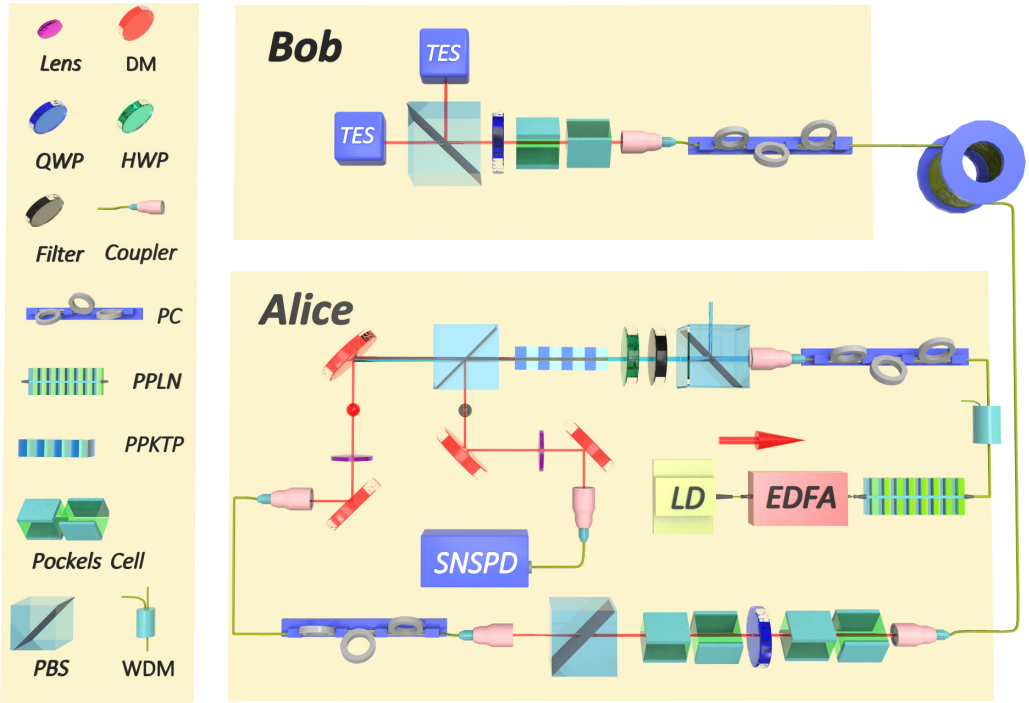

FIG. 1. Schematic of experimental quantum data locking. Alice pulses a distributed feedback laser diode (LD) at $\lambda = 1560$ nm with a pulse width of 10 ns at 100 kHz. After passing through an erbium-doped fiber amplifier (EDFA), the laser pulses are up converted to 780 nm via second-harmonic generation (SHG) in an in-line periodically poled lithium niobate (PPLN) waveguide. The residual long wavelengths are removed with a wavelength-division multiplexer (WDM) and a 945-nm low-pass (LP) filter. Alice focuses the pump pulses at 780 nm into a periodically poled potassium titanyl phosphate (PPKTP) crystal to create pairs of orthogonally polarized photons that are degenerated at 1560 nm via spontaneous parametric down conversion. The photon pairs are separated by a polarizing beam splitter (PBS). Alice uses dichroic mirrors (DMs) to remove the residual pump light at 780 nm and fluorescence. The pairs of signal and idler photons are collected into single-mode optical fibers. Alice detects the idler photons with a superconducting nanowire single-photon detector (SNSPD) to herald the presence of signal photons. The heralded signal photons are encoded by Pockels cells. After encoding, the single photons are sent to Bob via a fiber spool. In the meantime, a control signal is sent to Bob to prepare his bases accordingly to decode the incoming single-photon signals, which are received by two transition-edge sensors (TES) after a PBS. A polarization controller (PC) is applied wherever it is needed to maximize transmittance of photons in the right polarization and the extinction ratio. System synchronization is controlled by a field-programmable gate array (FPGA).

A field-programmable gate array (FPGA) provides a 100-kHz signal to pulse the pump laser. Upon receiving the heralding signals, the FPGA sends signals to Pockels cells (to prepare bases and unitary operations) to encode the heralded single photons with quantum states according to the preprogrammed data-locking scheme. The FPGA also sends signals to prepare Bob's Pockels cell to decrypt the message according to the preshared key, such that the received single photons are detected in the correct bases by TES.

We note that the permutation step is a classical algorithm and does not affect the performance of the data-locking schemes. The full realization is left for future work. We have nevertheless taken into account the seed consumption of this permutation step in the data analysis.

Experimental results. We first realize the DHLST scheme. We set the basis to be Z (Y) if the key is 0 (1) and send more than 8 Mbits of data in each basis. As shown in Table I, for both bases, single-photon transmittance, from preparation in Alice's station to detection in Bob's station, is determined to be greater than 55%, and the measured error rate is less than 0.4%. The accessible mutual information $I_{\rm acc}(A:B)$ between Alice and Bob is greater than the maximum amount of information $(n/2)$ that can be obtained by a receiver who does not have the key, which clearly exhibits data locking.

To experimentally demonstrate the loss-tolerant FHS scheme, the single-photon transmittance is tailored to be 54%, 41%, and 33% by setting the fiber length accordingly to be 0, 5, and 11 km. For each length, we vary the data size from 64 to 640 Mbits to examine the data locking. By setting $\epsilon = 10^{-9}$, Eve's accessible information $I_{\rm acc}(A:E)$ is bounded by 1, while $I_{\rm acc}(A:B)$ is proportional to n (see the Supplemental Material for details).

We define the data-locking efficiency as

$$\kappa = \frac{I_{\rm acc}(A:B) - I_{\rm acc}(A:E) - r}{r}, \tag{1}$$

where r is the key length and $I_{\rm acc}(A:E)$ and $I_{\rm acc}(A:B)$ are the mutual information before and after reconciliation between Alice and Bob.

TABLE I. Experimental results of data locking with the DHLST scheme (σ represents one standard deviation).

	e_b	η	$I_{\rm acc}(A:B)/n \pm \sigma$
Z basis	0.4%	55.2%	$53.1\% \pm 0.4\%$
Y basis	0.3%	56.6%	$54.9\% \pm 1.4\%$

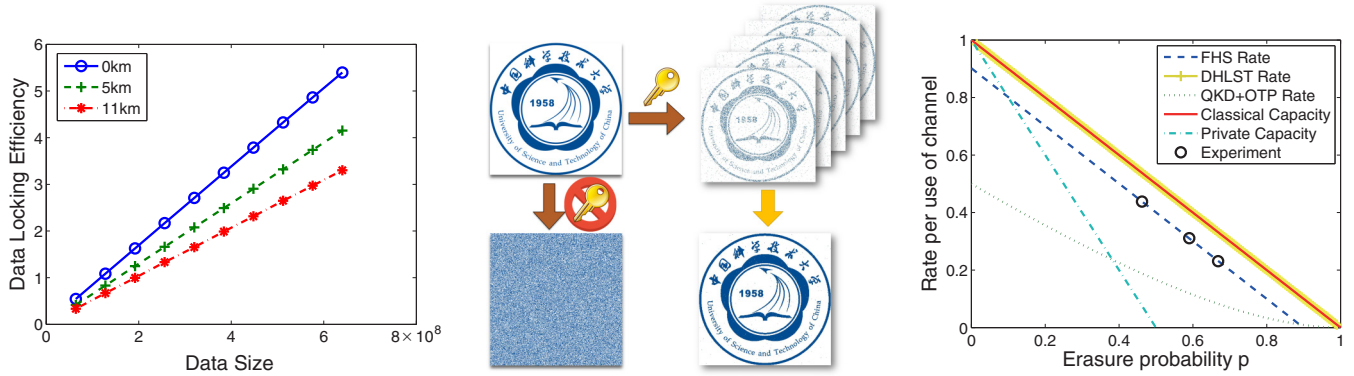

FIG. 2. (a) Data-locking efficiency of the FHS scheme with tailored single-photon transmittance. (b) Sending a photo with data (un)locking and error correction. (c) Communication rate in a quantum erasure channel.

The data-locking efficiency grows linearly with data size, as shown in Fig. 2(a). It requires the larger data size to surpass the performance of one-time pad encryption (with $\kappa = 1$) as the system loss increases. For our experiment, the data-locking efficiency beats the performance of one-time pad encryption when data size is larger than 128, 192, and 256 Mbits for $\eta = 54\%$,41%, and 33%, respectively.

Information integrity is also critical in secure applications. Here, we realize forward error correction (FEC) with erasure coding in the experimental implementation of quantum data locking. As an example, we send a photo of the logo of the University of Science and Technology of China with quantum data (un)locking through a lossy channel. We repeat each encoded qubit $50/\eta$ times. As such, we can recover each qubit with a probability of $1-(1-\eta)^{50/\eta} \geqslant 1-\exp(-50)$, while Eve's information increases only by $50/\eta$ times. As shown in Fig. 2 (b), with the key, the photo of the logo at the receiver is sharp with the error correction code compared to the blurred one without using the error correction code. Without the key, what is received is simply a set of random data.

An important application of data locking is the quantum locked key distribution. We estimate the performance of key distribution based on our experimental results (open circles) with $\epsilon = 10^{-9}$ and compare it with classical capacity and private capacity. Here, the classical capacity is the maximum amount of information that can be sent through the channel regardless of security. The private capacity is the secure part of the information when sending the information directly through the channel without any encoding. For a qubit erasure channel, the private capacity is $1-2p$, and the classical capacity is $1-p$, where p is the erasure probability. As shown in Fig. 2(c), the secure communication rate of data locking (long-dashed line) is well above the private capacity (dot-dashed line) and is close to the classical capacity (solid line). We also plot the estimated secure key rate based on the DHLST scheme (thick solid line) in Fig. 2(c), which basically overlaps with the classical capacity by consuming only one additional bit. For comparison, we plot the secure key rate of the most used quantum key distribution (QKD) + one-time pad encryption (OTP) combination (short-dashed line; see Supplemental Material). We consider the biased basis-choice method [30] and infinite-size limit in QKD, the conditions under which almost all the signal pulses are used to generate secure keys. The secure communication rate using QKD is less than one half of the rate based on data locking. The difference will be even larger when transmitting a longer random-number sequence using quantum locked key distribution. However, we note that in terms of security, QKD+OTP is better than the quantum locked key distribution using the FHS scheme. (The DHLST scheme has the lowest security; Eve may obtain more information than Bob when the erasure probability is larger than 0.5.) Yet the security of quantum locked key distribution using the FHS scheme with the bounded quantum storage assumption can be as good as QKD.

Conclusion. In conclusion, we have experimentally shown data locking with single photons in a variety of experimental settings. Our analysis shows its potential in key distribution. As an example for future applications, we successfully transmitted a photo with data (un)locking and an error correction code. Our experimental results suggest that quantum data locking has potential in many resource-limited secure information applications.

Note added. Recently, we become aware of a related work [31].

Acknowledgments. The authors would like to thank J.-Y. Guan, L.-K. Chen, X. Yuan, Y.-H. Li, and Q.-C. Sun for enlightening discussions. This work has been supported by the National Fundamental Research Program (under Grant No. 2013CB336800), the National Natural Science Foundation of China, the Chinese Academy of Science, and the 1000 Youth Fellowship program in China.

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

[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. Elliott, New J. Phys. **4**, 46 (2002).
[5] M. Peev, C. Pacher, R. Allaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati *et al.*, New J. Phys. **11**, 075001 (2009).
[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang *et al.*, Opt. Express **19**, 10387 (2011).
[7] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang *et al.*, Phys. Rev. X **6**, 011024 (2016).
[8] J. Qiu, Nature (London) **508**, 441 (2014).
[9] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).
[10] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
[11] O. Fawzi, P. Hayden, and P. Sen, J. ACM **60**, 44 (2013).
[12] S. Lloyd, arXiv:1307.0380.
[13] C. Lupo, M. M. Wilde, and S. Lloyd, Phys. Rev. A **90**, 022326 (2014).
[14] D. Leung, J. Phys.: Conf. Ser. **143**, 012008 (2009).
[15] F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung, Proc. Royal Soc. A **469**, 20130289 (2013).
[16] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, Phys. Rev. X **4**, 011016 (2014).
[17] C. Lupo and S. Lloyd, New J. Phys. **17**, 033022 (2015).
[18] C. Lupo and S. Lloyd, Phys. Rev. Lett. **113**, 160502 (2014).
[19] I. Devetak, IEEE Trans. Inf. Theor. **51**, 44 (2005).
[20] R. König, R. Renner, A. Bariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502 (2007).
[21] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat. Photon. **7**, 210 (2013).
[22] S. Chen, L. You, W. Zhang, X. Yang, H. Li, L. Zhang, Z. Wang, and X. Xie, Opt. Express **23**, 10786 (2015).
[23] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).
[24] D. Fukuda, G. Fujii, T. Numata, K. Amemiya, A. Yoshizawa, H. Tsuchida, H. Fujino, H. Ishii, T. Itatani, S. Inoue, and T. Zama, Opt. Express **19**, 870 (2011).
[25] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.94.020301 for more details about the realization of the data locking schemes.
[26] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, Opt. Express **15**, 15377 (2007).
[27] R. S. Bennink, Phys. Rev. A **81**, 053805 (2010).
[28] M. D. C. Pereira, F. E. Becerra, B. L. Glebov, J. Fan, S. W. Nam, and A. Migdall, Opt. Lett. **38**, 1609 (2013).
[29] P. B. Dixon, D. Rosenberg, V. Stelmakh, M. E. Grein, R. S. Bennink, E. A. Dauler, A. J. Kerman, R. J. Molnar, and F. N. C. Wong, Phys. Rev. A **90**, 043804 (2014).
[30] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).
[31] D. J. Lum, J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, Phys. Rev. A **94**, 022315 (2016).