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, P. R. 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, P. R. China*

[3] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, P. R. China*

[4] *Quantum Optical Measurement Group, Research Institute for Physical Measurement National Metrology Institute of Japan(NMIJ), National Institute of Advanced Industrial Science and Technology(AIST) 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, P. R. China*

[6] *Purple Mountain Observatory and Key Laboratory of Radio Astronomy, Chinese Academy of Sciences, 2 West Beijing Road, Nanjing, Jiangsu 210008, P. R. China*

Quantum data locking is a special quantum effect that can lock classical correlation. One can lock an exponentially large amount of information using a short secret key, making it inaccessible to unauthorized users without the key. Here we report experimental demonstrations of quantum data locking scheme originally proposed by DiVincenzo *et al.* [Phys. Rev. Lett. 92, 067902(2004)] and a loss-tolerant scheme developed by Fawzi, Hayde, and Sen [J. ACM. 60, 44(2013)]. In both experiments we verify that the unlocked amount of information can be larger than the key size, exhibiting data locking effect not shown in classical information theory. We successfully transmit of a photo over a lossy channel with quantum data (un)locking and error correction as an application example.

Information security continuously remains the research frontier, driven by both scientific curiosity and the increasing demand from practical applications in secure communication and secure data storage. Classical information security is based on computation complexity, the security can be broken if equipped with enough computational capacity. Quantum key distribution (QKD), on the other hand, allows two parties to generate secure keys with the security based on quantum mechanics. Now QKD has been demonstrated in metropolitan networks and is ready to commercialize. By generating secret keys using QKD and encrypting message with one-time pad, the security of information transmission can be guaranteed. The one-time pad method offers the highest security but acquires the length of key size the same as the information size. Quantum data locking [1–4] allows to lock information in quantum states with exponentially shorter key, presenting an efficient solution to many resource-limited secure applications.

In classical information theory, the mutual information is a measure for the correlation between two parties. The increase of mutual information is proportional to the messages communicated between two parties. 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 codeword 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)[1] found that a k-bit key can increase the mutual information by an amount more than k via quantum means. In the DHLST scheme, Alice encodes messages with a set of orthonormal bases and then encrypt the messages by applying a unitary operation, Identity or Hadamard transform depending on the key bit 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.

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 [4–6].

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 [2], 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 [7]. This makes quantum data locking appealing for realistic applications such as

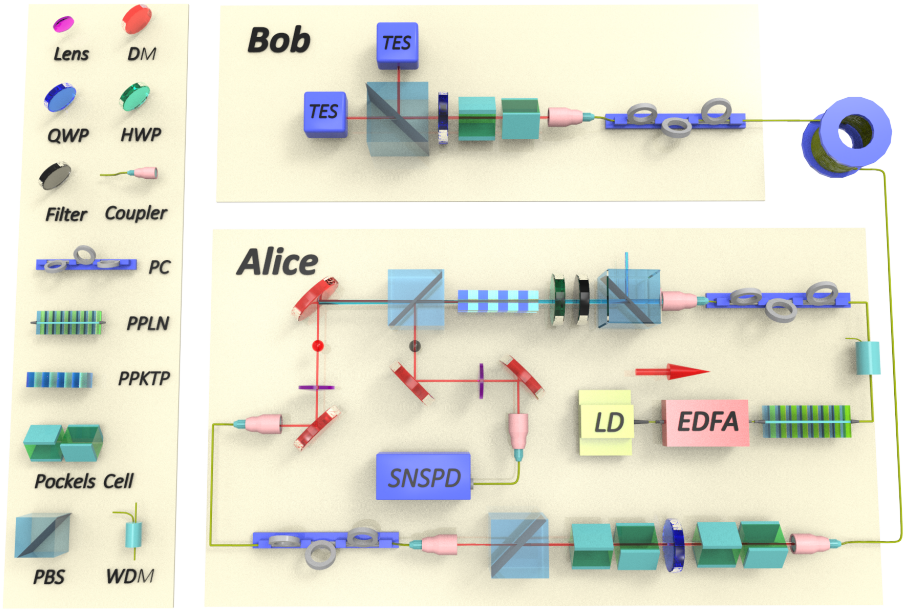


FIG. 1. Schematic of experimental quantum data-locking

secure communication [3, 4]. The implementation of FHS scheme [2] includes the mutually unbiased bases and permutation extractors. The detailed scheme is complicated so will not be shown in this extended abstract. The secret key consumption includes the basis choices consumption of length $\log(2/\epsilon^2)$, and the permutation extractor consumption of length $40000\log(24n^2/\epsilon)$. The mutual information is $6\epsilon n/16.12 + H(\epsilon)$ without knowing the key, and expands to $\eta \times n/16.12(1 - H(e_b))$ given the secret key. Here $H(\cdot)$ is the binary Shannon entropy, and the information is calculated excluding the key.

Experimental realization of quantum data locking was considered to be a severe technical challenge [4]. Here, we report experimental demonstrations of both DHLST scheme and FHS scheme. As shown in Fig. 1, we generate heralded single photons by detect one of the correlated photon pairs using a superconducting nano-wire single photon detector (SNSPD) [8, 9]. Then the message is encoded using two successive pockels cells. After transmitting in fiber spools, Bob uses a pockels cell to set his bases and detects the message using superconducting Transition-edge-sensors (TESs) [10, 11].

In the experimental demonstration, daughter photons at 1560 nm are generated via type-II spontaneous parametric down-conversion process using a periodically-poled potassium titanyl phosphate (PPKTP) crystal. After optimizing the collection parameters, the single photon heralding efficiency is determined to be 87%, including all losses in the photon pair source setup [12–14]. We use a SNSPD with a rising edge of τ ∼70 ps and detection efficiency ∼50% as the heralding detector for fast heralding photon generation; We use a TES with detection efficiency ∼70% to detect the signal photons at the receiver.

The first result is the realization of DHLST scheme. We set the basis to be $Z(Y)$ if the key is 0(1), and send more than 8 Mb data in each basis. The whole transmittance in our setup is greater than 55%. With the measured error rate less than 0.4%, we calculate the accessible mutual between Alice and Bob is greater than $n/2$, which is greater than the maximum amount of information $(n/2)$ Eavesdropper might have (detail not shown in this extended abstract). From informational theoretical view, this locking effect is a non-classical behavior, thus clearly demonstrate the quantum data locking effect.

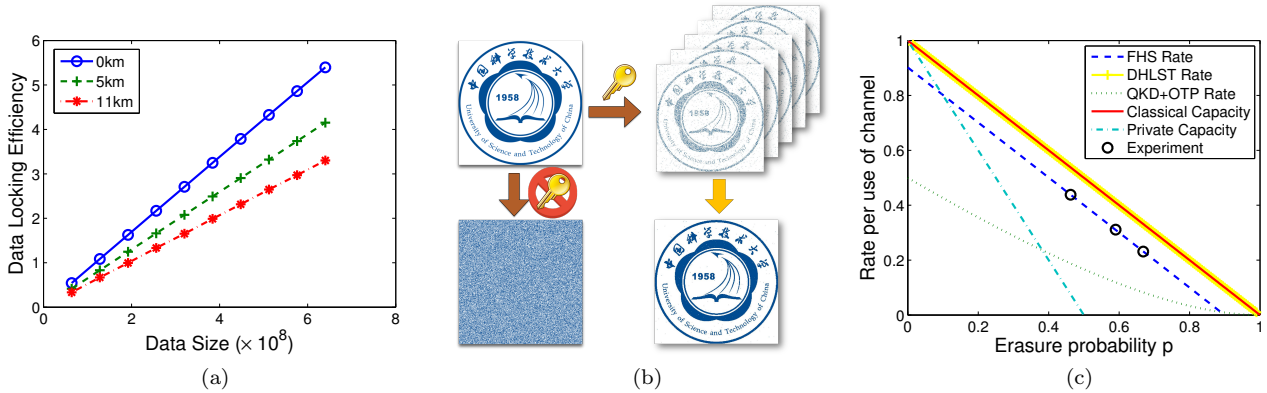
In a lossy channel, the FHS protocol is more suitable since it's loss tolerant. To verify this, we sent the single photons through fiber spools from 0 km to 11 km where the transmittance is tailored to be 54%, 41% and 33%. Eve's accessible information $I_{acc}(A:E)$ is bounded by at most 1 bit by setting $\epsilon = 10^{-9}$. (The detail is not shown in the extended abstract)

We define the data locking efficiency as

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

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

Fig. 2(a) shows the result data locking efficiency grows linearly with data size. The performance of data locking surpasses that of of one time pad (with $\kappa = 1$) when the data size is large enough. Note that the nonclassical quantum data locking effect appears when $\kappa > 0$.



(a) (b) (c)

FIG. 2. (color online) (a) Data locking efficiency of 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.

From practical view, we need to keep information integrity when transmit message. A forward error correction (FEC) with erasure coding can help. As an example, we send a photo with quantum data (un)locking through a lossy channel, and we simply repeat each encoded qubit by $50/\eta$ times as a FEC code. As shown in Fig. 2(b), although the recovered photo is lossy each time, we can recover the original message with high probability by decode using the repeat photos. Using this method, Eve's information only increases $50/\eta$ times.

An important application of data locking is quantum-locked key distribution. We estimate the performance of key-distribution based on our experimental results (open circle) with $\epsilon = 10^{-9}$, and compare it with the classical capacity and private capacity. As shown in Fig. 2(c), the secure communication rate of data locking (long dashed line) is well above the private capacity (dotted-dashed line) and is close to the classical capacity (solid line). For comparison, we plot the secure key rate of the most-used QKD+one time pad combination, which 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+one time pad is better than quantum locked key distribution using the FHS scheme (which is much higher than using DHLST scheme). Yet, the security of quantum locked key distribution using the FHS scheme with bounded quantum storage assumption can be as good as QKD.

[1] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
[2] O. Fawzi, P. Hayden, and P. Sen, Journal of the Acm **60**, 44 (2013).
[3] S. Lloyd, arXiv.org (2013), 1307.0380v1.
[4] C. Lupo, M. M. Wilde, and S. Lloyd, Physical Review A **90**, 022326 (2014).
[5] D. Leung, Journal of Physics: Conference Series **143**, 012008 (2009).
[6] F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **469** (2013), 10.1098/rspa.2013.0289.
[7] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, Physical Review X **4**, 011016 (2014).
[8] 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).
[9] S. Chen, L. You, W. Zhang, X. Yang, H. Li, L. Zhang, Z. Wang, and X. Xie, Opt. Express **23**, 10786 (2015).
[10] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).
[11] 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).
[12] R. S. Bennink, Phys. Rev. A **81**, 053805 (2010).
[13] M. D. C. Pereira, F. E. Becerra, B. L. Glebov, J. Fan, S. W. Nam, and A. Migdall, Opt. Lett. **38**, 1609 (2013).
[14] 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).