SCIENTIFIC REPORTS

OPEN

Experimental Quantum-enhanced Cryptographic Remote Control

Xiao-Ling Pang[1,2], Lu-Feng Qiao[1,2], Ke Sun[1,3], Yu Liu[1,3], Ai-lin Yang[1,2] & Xian-Min Jin[1,2]

Received: 18 October 2018
Accepted: 27 March 2019
Published online: 09 April 2019

The Internet of Things (IoT), as a cutting-edge integrated cross-technology, promises to informationize people's daily lives, while being threatened by continuous challenges of eavesdropping and tampering. The emerging quantum cryptography, harnessing the random nature of quantum mechanics, may also enable unconditionally secure control network, beyond the applications in secure communications. Here, we present a quantum-enhanced cryptographic remote control scheme that combines quantum randomness and one-time pad algorithm for delivering commands remotely. We experimentally demonstrate this on an unmanned aircraft vehicle (UAV) control system. We precharge quantum random numbers (QRN) into controller and controlee before launching UAV, instead of distributing QRN like standard quantum communication during flight. We statistically verify the randomness of both quantum keys and the converted ciphertexts to check the security capability. All commands in the air are found to be completely chaotic after encryption, and only matched keys on UAV can decipher those commands precisely. In addition, the controlee does not response to the commands that are not or incorrectly encrypted, showing the immunity against interference and decoy. Our work adds true randomness and quantum enhancement into the realm of secure control algorithm in a straightforward and practical fashion, providing a promoted solution for the security of artificial intelligence and IoT.

With the rapid development of artificial intelligence and IoT, greater demands are being placed on the security by growing hacking incidents. To implement cryptographic remote control, two general types of key-based algorithms, public-key and symmetric, are being widely investigated. Public-key algorithms use two different keys for encryption and decryption, and are often based on computational complexity; while they are imperfect in the real world for being slow, and vulnerable to chosen-plaintext attacks[1]. Conventional symmetric algorithms require that communication parties share matched and secret keys in advance; while the security of such algorithms relies on the shared keys. One-time pad[2], as a powerful symmetric algorithm, has been proved by Claude Shannon to be impossible to crack[3], as long as crucial problems of generating and sharing real random sequences are settled.

Randomness is a fundamental resource with significant applications in cryptography and numerical simulation. Real random sequences, however, are hard to generate mathematically[4], but have to rely on unpredictable physical processes[5–9]. Although different mechanics, such as chaotic effects[10,11], thermal noise[12], biometric parameters[13] and free-running oscillators[14] are employed in the generation of physical random number, they are faced with some problems like hard to detect failure[15]. The inherent uncertainty of quantum mechanics makes quantum systems an excellent stochastic source, with the fact that a single photon incident on a 50:50 beam splitter be transmitted or reflected is intrinsically random. More importantly, the randomness is precisely balanced and immune to environmental perturbations.

Sharing randomness is another crucial problem to be settled for realizing symmetric algorithms. One best-known scheme is quantum key distribution (QKD), which is quite mature so far for applications, with enormous progresses[16–19] and is even ready for constructing secure networks[20–24]. Nevertheless, many situations of IoT control are not compatible with QKD schemes. For example, sensor networks require low cost, low power and miniature devices, which is hard to be met by QKD systems[25], especially for large-scale and distributed sensor networks.

Interestingly, in many situations, real-time sharing of randomness is not really necessary in practice. For instance, UAVs or satellites are essentially well identified before being launched, and are well isolated with other parties during their missions. For all these situations, we could precharge quantum keys into controllers and

[1]State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Physics and Astronomy, Shanghai Jiao Tong University, Shanghai, 200240, China. [2]Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui, 230026, China. [3]Zhiyuan Innovative Research Center, Shanghai Jiao Tong University, Shanghai, 200240, China. Correspondence and requests for materials should be addressed to X.-M.J. (email: xianmin.jin@sjtu.edu.cn)

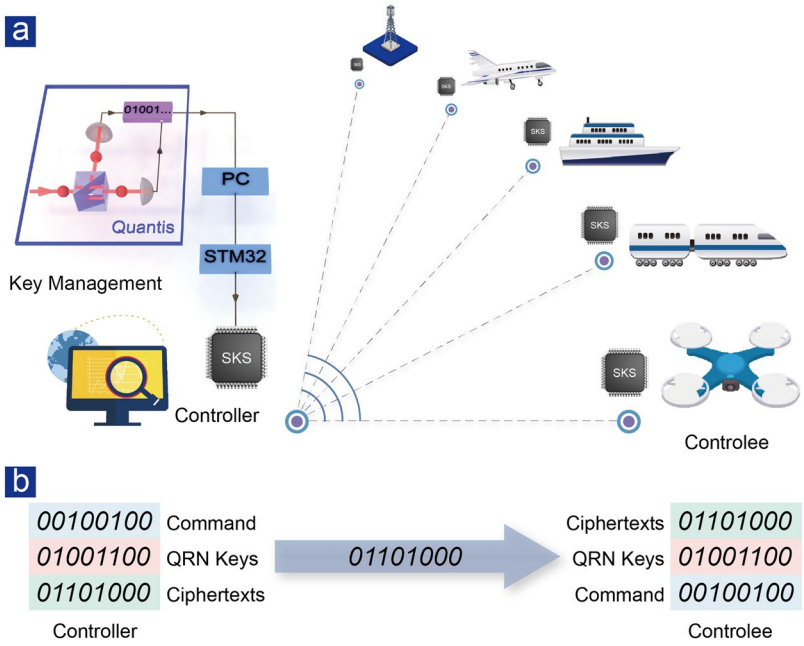

Figure 1. Quantum-enhanced cryptographic remote control. (**a**) A schematic diagram of quantum-enhanced cryptographic remote control system and the potential applications. The quantum random number generator utilized here is the "Quantis USB" of ID Quantique company. Scenarios applicable to our direct-charging scheme: remote control of UAV, high-speed rail scheduling, vessel movement, airport dispatch and smart grid control. (**b**) A specific example that combines QRN keys and one-time pad algorithm for delivering commands remotely.

controlees, and implement cryptographic remote control with quantum enhancement in a straightforward and practical way. In this work, we present this quantum-enhanced cryptographic remote control scheme that combines quantum randomness and one-time pad algorithm for delivering commands remotely, and experimentally demonstrate this on a UAV control system.

The cryptographic system is composed of three subsystems: key management unit, controller unit and controlee unit, as is shown in Fig. 1(a). The randomness derived from quantum nature of single photons is charged into IoT devices through secure key storage (SKS) chips to perform one-time pad encryption and decryption. The connection of flexible small-scale SKS chips to QRN generator is realized by a home-built key management unit. SKS chips are planted into controllers and controlees before they are detached. Commands are encrypted by one-time pad algorithm with a certain section of keys, which can only be decrypted correctly by the controlee with corresponding keys. On the controller side, with QRN keys, a bitwise exclusive OR is performed on commands before being sent; and conversely, with identical keys, commands can be deciphered and executed on the controlee's side, as is shown in Fig. 1(b).

The data transmission diagram of our UAV control system is illustrated in Fig. 2(a). Encryption keys are generated by Quantis, which is a reliable QRN generator, employing a quantum process as the source of randomness, and producing random sequences at a bit rate of 4 Mb/s. To be specific, a photon incident on a semi-transparent mirror will be reflected with half the probability, leading to a "0"; or transmitted with half the probability, leading to an "1". A microcontroller is dedicated for charging or updating quantum keys into SKS chips.

The successful execution of one-time pad algorithm depends on the synchronization of keys. Unfortunately, it happens that commands get lost or make mistakes, leading to key mismatch between controllers and controlees. Any minor key mismatch may cause control system failure. To solve this problem, we assign unique address information to each command, so that each command with quantum keys is independent and well labeled. Once error happens, the corresponding command will be discarded directly together with its encryption and decryption keys to maintain the synchronization. Such address information doesn't have to be encrypted, because they include no information about commands.

The randomness of quantum keys is a crucial parameter that determines system security. Quantum random number based on the uncertainty principle of quantum mechanics provides the honest-to-goodness randomness in the world, with the properties of unpredictable and unreproducible[1]. We use NIST suites to perform statistical tests[26], and the final results are shown in Fig. 2(b). The results are *P–values* of all 15 tests: indicating how a sequence is identical to purely random number, ideally *P–values* equal to one. The results of NIST tests prove an excellent statistical randomness of our quantum keys.

Furthermore, according to one-time pad algorithm, where ciphertexts are the XOR values of quantum keys and plaintexts, the randomness of quantum keys determines that of ciphertexts. We intercept a section of commands in the air sent by the controller, and test them with three characteristics of random binary sequences proposed by Gobomb: balance property, runs property and auto-correlation property[27]. The good properties of

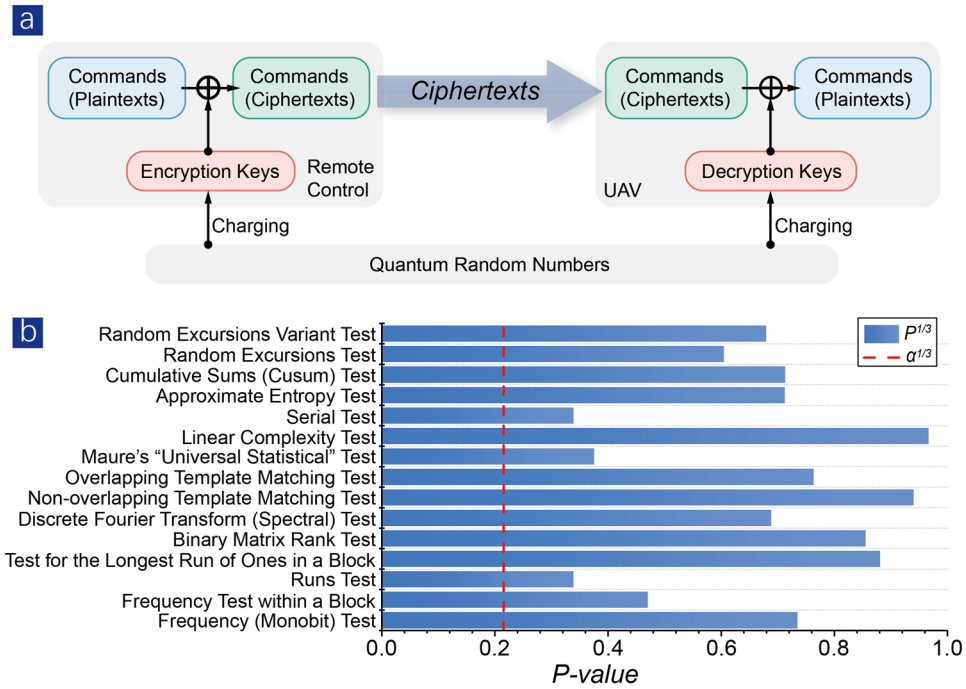

Figure 2. Signal flow diagram and NIST tests of quantum randomness. (**a**) Signal flow diagram of the quantum-enhanced cryptographic control system. (**b**) NIST statistical randomness tests performance of quantum keys. The experimental results are obtained from 1,638,400 bits samples with a significance level of $\alpha = 0.01$. In the histogram, the value of each test that exceeds the red dashed line turns out a successful pass.

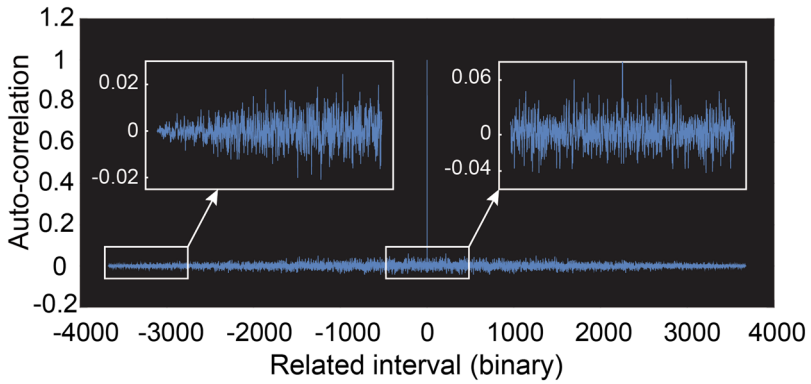

Figure 3. The auto-correlation function measured among long commands ciphertexts. The auto-correlation function of ideal random sequence is close to delta function. The sharp auto-correlation peak in the center indicates that the encrypted binary sequence has excellent independence on each part. The insets show auto-correlation details in the near- and far-field regime.

Test Index	*P–value*	Proportion	Result
Frequency	0.4861	1	SUCCESS
Runs	0.4719	1	SUCCESS

Table 1. Balance and runs properties. *P–values* for uniformity check, and proportions for examination of the sequences that pass a certain statistical test (Success Rate). 20 pieces of commands are tested.

balance, runs (see Table 1), and auto-correlation (see Fig. 3) indicate that our ciphertexts are statistically random. Meanwhile, since the quantum keys are unpredictable and unrepeatable, the ciphertexts intercepted here are expected and experimentally observed to be truly random, which is impossible to be deciphered without matched quantum keys.

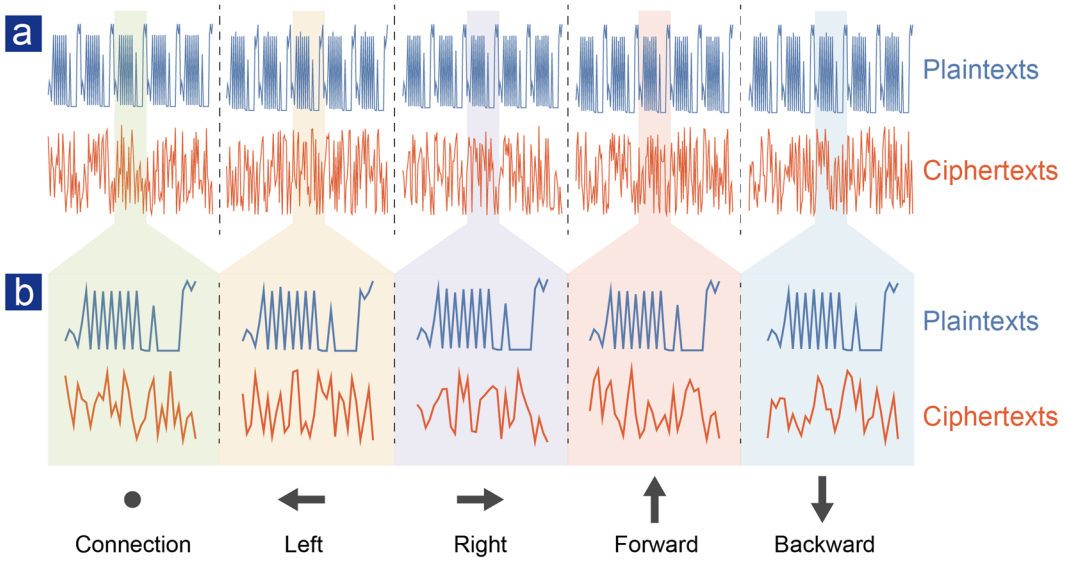

Figure 4. Experimental results of intercepted commands. (**a**) Intercepted five pieces of typical commands both with (blue lines) and without (red lines) one-time pad encryption for comparison. (**b**) Details of each functional command. The last four bytes of ciphertexts represent the assigned address information of quantum keys. One command is combined with 32 bytes, and each byte represents for an integer whose value ranges from 0 to 255, stored with eight binaries. See Supplementary Materials for details.

Experimental commands between the remote control and the aircraft are shown in Fig. 4. We intercept five pieces of different functional commands, both with and without one-time pad encryption for comparison. For plaintexts, we can see that five repeating commands share exactly identical values; while for ciphertexts, five repeating commands are bought into chaos, and there is no correlation between any two commands or even any two bytes, which guarantees the security as have been proved statistically in Table 1 and Fig. 3, according to three postulates proposed by Golomb[27].

Since the security of the commands depends on the one-time pad, the communication capacity in this cryptographic control scheme is mainly limited by the number of precharged QRNs. To extend the key updating period, on one hand, the capacity of secure key storage device should be large enough, while it might take more bytes in the commands for storing keys' address information. On the other hand, the encryption commands can be optimized according to different structures, and some trivial information in a certain command could be ignored to save keys, as well as to increase decryption speed.

In summary, we have proposed and experimentally demonstrated a quantum-enhanced cryptographic remote control scheme that combines quantum randomness and one-time pad algorithm for delivering commands remotely. The quantum-enhanced cryptographic scheme is expected to be generalized to bidirectional systems: controlees can be securely controlled and also be able to send encrypted recorded flight data back to controllers, such as position, direction and speed. Besides, the point-to-point solution can be extended to point-to-multipoint or distributed networks. More importantly, such scheme can be combined with fixed QKD channels[23,28–30] for long-distance quantum keys charging, providing a flexible solution for control security of artificial intelligence and IoT in large scale.

References

1. Schneier, B. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C* (John Wiley & Sons, Inc, 1996).
2. Gingerich, O. The Codebreakers: The Codebreakers. The Story of Secret Writing, by David Kahn. *Isis* (1996).
3. Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).
4. Knuth, D. E. *The art of computer programming Volume 2: Seminumerical algorithms Reading* (And Searching, 1981).
5. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
6. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47**, 595–598 (2000).
7. Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **93**, 910 (2008).
8. Uchida, A. *et al.* Fast physical random bit generation with chaotic semiconductor lasers. *Nature Photon.* **2**, 728–732 (2008).
9. Fiorentino, M., Santori, C., Spillane, S. M., Beausoleil, R. G. & Munro, W. J. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A* **75**, 723–727 (2006).
10. Stojanovski, T. & Kocarev, L. Chaos-based random number generators-part I: analysis. *IEEE Trans. Circ. Syst. I: Fund. Theory Appl.* **48**, 281–288 (2001).
11. Stojanovski, T., Pihl, J. & Kocarev, L. Chaos-based random number generators-part II: practical realization. *IEEE Trans. Circ. Syst. I: Fund. Theory Appl.* **48**, 382–385 (2001).
12. Petrie, C. S. & Connelly, J. A. A noise-based IC random number generator for applications in cryptography. *IEEE Trans. Circ. Syst. I: Fund. Theory Appl.* **47**, 615–621 (2000).

13. Szczepanski, J., Wajnryb, E., Amigó, J. M., Sanchez-Vives, M. V. & Slater, M. Biometric random number generators. *Computers & Security* **23**, 77–84 (2004).
14. Kohlbrenner, P. & Gaj, K. An Embedded True Random Number Generator for FPGAs. in *Proc. of the 12th Int. Symp. on Field Programmable Gate Arrays*. 71–78 (2004).
15. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004 (2017).
16. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theoretical Computer Science* **560**, 7–11 (2014).
17. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
18. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nature Photonics* **8**, 595–604 (2014).
19. Ji, L. *et al*. Towards quantum communication in free-space seawater. *Opt. Express* **25** (2016).
20. Qiu & Jane. Quantum communications leap out of the lab. *Nature* **508**, 441–442 (2014).
21. Elliott, C. The DARPA quantum network. *Quantum Communications and cryptography* 83–102 (2006).
22. Fujiwara, M. *et al*. Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19**, 10387–409 (2011).
23. Fröhlich, B. *et al*. A quantum access network. *Nature* **501**, 69–72 (2013).
24. Tang, Y. L. *et al*. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X* **6**, 011024 (2016).
25. Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* **29**, 1645–1660 (2012).
26. Rukhin, A. *et al*. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *Appl. Phys. Lett.* **22**, 1645–179 (2015).
27. Golomb, S. W. *Shift Register Sequences* (Holden-Day, 1967).
28. Ursin, R. *et al*. Entanglement-based quantum communication over 144 km. *Nature Physics* **3**, 481–486 (2007).
29. Marsili, F. *et al*. Detecting single infrared photons with 93% system efficiency. *Nature Photonics* **7**, 210–214 (2013).
30. Wang, J. Y. *et al*. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photonics* **7**, 387–393 (2013).

Acknowledgements

This work was supported by National Key R&D Program of China (2017YFA0303700), the National Natural Science Foundation of China (NSFC) (61734005, 11761141014, 11690033), the Science and Technology Commission of Shanghai Municipality (STCSM) (15QA1402200, 16JC1400405, 17JC1400403), the Shanghai Municipal Education Commission (SMEC) (16SG09, 2017-01-07-00-02-E00049), and the Zhiyuan Scholar Program (ZIRC2016-01). X.-M.J. acknowledges support from the National Young 1000 Talents Plan.

Author Contributions

X.-M.J. conceived the work and supervised the project. X.-L.P., K.S. and Y.L. developed the electronic system. X.-L.P., L.-F.Q., K.S., Y.L., A.-L.Y. and X.-M.J. all contributed to setting up the experiment. X.-L.P. and X.-M.J. analyzed the data and wrote the paper.

Additional Information

Supplementary information accompanies this paper at https://doi.org/10.1038/s41598-019-42278-8.

Competing Interests: The authors declare no competing interests.

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