Zero-Trust Security Protection Technology in Internet of Things - Research Article

International Journal of
Distributed
Sensor Networks

International Journal of Distributed Sensor Networks
2022, Vol. 18(11)
© The Author(s) 2022
DOI: 10.1177/15501329221136978
journals.sagepub.com/home/dsn
SAGE

A flexible continuous-wave quantum cryptography scheme with zero-trust security for Internet of Things

Yong Shen*, Xiaokang Tang*, Xiang Zhang, Yongzhuang Zhou and Hongxin Zou

Abstract
As quantum computing techniques develop rapidly, the security of classical communication, which is usually based on public key encryption algorithm, is under great threat. Therefore, a key establishment method with physics base is demanding, especially for Internet of Things devices, where energy and computational power is quite limited. In this article, we present a flexible continuous-wave quantum cryptography scheme for Internet of Things systems. In this configuration, the IoT controller contains a narrow linewidth laser as a real local oscillator. Thus, it is capable of working as either a host or a client in quantum key distribution with remote servers, and efficiently generating quantum random numbers for quantum key distribution, as well as one time pad communication with deployed sensors. The security of the scheme is analyzed under the assumption of collective attacks in the asymptotic regime, and feasibility is theoretically verified with typical channel and commercial device parameters.

Keywords
Zero trust, quantum cryptography, continuous-variable, quantum random number generator, quantum key distribution

Date received: 30 May 2022; accepted: 7 October 2022

Handling Editor: Peio Lopez Iturri

Introduction

The scale of Internet of Things (IoT) is growing rapidly with the development of information science and technology, and it is estimated that there will be 75 billion IoT devices operating by 2025.[1,2] As increasingly sensitive and large amount of data is being transferred via IoT, its security problem emerges and has drawn a lot of attention.[3–5] Due to the mobility, dynamicity, and flexibility of IoT devices, the traditional security paradigm based on perimeter is inevitably being threatened, and a zero trust hierarchy of IoT needs to be established. Classical solution for IoT security is typically based on asymmetric cryptosystems, where a public key is used for encryption and a private key for decryption. Thus, key distribution process can be avoided in these systems.[2] However, most of the public key algorithms, such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), will be easily broken by quantum computing with Shor's algorithm.[2,6,7] Although there are a lot of studies on quantum-resistive public key cryptosystems,[8–12] only a few researches for IoT systems have been carried out due to their constrained computational resources.[13,14] Therefore, in this scenario, it is reasonable to resort to

Department of Physics, The National University of Defense Technology, Changsha, P.R. China

*These authors contributed equally to this work.

Corresponding author:
Hongxin Zou, Department of Physics, The National University of Defense Technology, Changsha 410073, P.R. China.
Email: hxzou@nudt.edu.cn

quantum cryptography (QC), whose security is based on the fundamental laws of quantum physics rather than on the complexity of computing.[2–18]

To implement the perfect secure one time pad (OTP)[19] with QC, one needs to generate a truly random raw key based on the random nature of quantum physics[20,21] and distribute it with quantum key distribution QKD.[22,23] Unlike the original QKD protocol based on modulation and detection of discrete variables of single photons,[22] an alternative continuous-variable (CV) QKD protocol is based on homodyne or heterodyne detection of the amplitude and phase of coherent optical fields.[23] Since this protocol is highly compatible with the classical coherent optical communication,[24] its application in IoT systems is quite convenient and straightforward. Moreover, due to the mode selection nature of homodyne and heterodyne detection, noise in modes other than the signal mode will be filtered out automatically, which leads to a high signal-to-noise ratio (SNR).

To perform homodyne and heterodyne detection, a local oscillator (LO) is required as a phase reference, which is a strong laser field coherent with the signal. Since the final secret key rate is extremely sensitive to the phase noise between the signal and the LO,[23] originally they are prepared from the same laser at the host (normally referred to as Alice).[25–27] In addition, in order to reduce phase difference and cross talk in the channel, they are sent to the client (Bob) via the same fiber link using time and polarization multiplexing.[27–29] However, this configuration has two main drawbacks. One is a potential loophole of exposing both the signal and LO to the eavesdropper (Eve).[30] The other is the need of a high-power LO due to the channel loss, especially for long-distance communication.[31] To avoid these problems, a scheme with "locally" generated LO has been proposed and demonstrated.[31,32] In this scheme, the phase difference between the signal and LO is monitored and processed dynamically. Nevertheless, since the LO runs freely in this scheme, it may compromise the long-term stability and security of the system.

In this article, we propose a CV-QC scheme for IoT systems, where the LO is locked to the reference signal via a phase lock loop (PLL). By modulating the signal within a frequency region away from DC and performing heterodyne detection, the classical excess noise of the LO can be sufficiently suppressed. In this configuration, the phase tracking and data processing procedure are eliminated, so as to increase the communication speed and alleviate power and computation requirements on IoT controllers. In addition, in this scheme, the IoT controllers are capable of serving as either Alice or Bob, and generating quantum random numbers by measuring shot noise of vacuum states with the LO, which makes them more flexible for complex application scenarios.

Related works

The Gaussian-modulated CV-QKD protocol

Unlike the protocols based on non-classical states, such as single photons[22] and entangled states,[33,34] Grangier's group proposed a protocol where only optical coherent states are required.[28] In this protocol, Alice modulates the amplitude and phase of the laser field to generate a coherent state $|\alpha_A\rangle$, where $\alpha_A = X_A + iP_A$. X_A and P_A are the amplitudes of the two orthogonal quadratures of $|\alpha_A\rangle$, and their probabilities are Gaussian distributed. The coherent state is sent to Bob along with a phase reference LO via a lossy and noisy channel. Thus, at Bob's site, the state is usually a mixed rather than pure. By performing heterodyne detection, Bob can obtain two variables X_B and P_B, which can be written as

$$\begin{aligned} X_B &= X_A + \sqrt{\tfrac{2-T}{T}}X_0 + \delta X \\ P_B &= P_A + \sqrt{\tfrac{2-T}{T}}P_0 + \delta P \end{aligned} \tag{1}$$

where T is the transmittance of the channel, X_0 (P_0) and δX (δP) are the shot noise and excess noise of the X (P) quadrature, respectively. Then, Alice and Bob perform information reconciliation to establish a raw key. Since reconciliation is after the measurement, the raw key rate can be described by the classical Shannon mutual information $I(a:b)$, where a is the variable Alice modulated on a quadrature and b is the variable Bob measured on the same quadrature.

In the security analysis of QKD, the eavesdropper Eve is supposed to be capable of making any operation so long as not to violate the physics principle. Thus, Eve can replace the normal channel with a perfect lossless and noiseless one, and an ancilla to interact with each state Alice sent. After eavesdropping, the state Bob receives becomes lossy and noisy, just the same as being transmitted through the normal channel. Since Eve can store the entangled state in a quantum memory, and perform the optimal measurement after reconciliation between Alice and Bob, the mutual information with Alice (Bob) she can extract is described by the Holevo bound $\chi(a(b):E)$, where E denotes the state Eve stores. To eliminate the information Eve obtained, Alice and Bob need to perform privacy amplification. When the transmittance of the channel is larger than 0.5, $I(a:b)$ is larger than $\chi(a:E)$. In this case, Alice and Bob can use direct reconciliation, and the secret key rate is

$$K = I(a:b) - \chi(a:E) \tag{2}$$

When the transmittance of the channel is less than 0.5, $I(a:b)$ is always less than $\chi(a:E)$. Thus, there is no secure key for direct reconciliation. However, in this case, $I(a:b)$ may be larger than $\chi(b:E)$. Therefore, Alice and Bob can perform reverse reconciliation, and the secret key rate is

$$K = I(a:b) - \chi(b:E) \tag{3}$$

When the channel is quite lossy, the SNR is quite low, leading to poor reconciliation efficiency and laborious computation. In classical communication, when the SNR is low, one can send the same signal several times to promote the effective SNR. However, this method cannot be applied to CV-QKD, since it will induce loopholes.

Discretely modulated CV-QKD

To extend CV-QKD to long-distance communication, in 2009, Grangier's group proposed a sophisticated discretely modulated CV-QKD protocol[35] which can be implemented as an effective repetition code scheme without compromising the security. In this protocol, instead of Gaussian modulation, Alice randomly prepares one of the four coherent states

$$|\alpha_k\rangle = \left|\alpha e^{\mathbb{i}(2k+1)\pi/4}\right\rangle \tag{4}$$

where α is a positive real number, $k \in \{0,1,2,3\}$, $\mathbb{i}$ is the imaginary unit. In this case, the X and P quadratures are actually binarily modulated with $X_A(P_A) = \pm \frac{\alpha}{\sqrt{2}}$. To implement a N-bit repetition code scheme, Alice sends N states with the modulated variables denoted as $\{a_1, a_2, \ldots, a_N\}$. Bob's measurement results are denoted as $\{b_1, b_2, \ldots, b_N\}$. Then, through public channel, Bob reveals side information $\{|b_1|, |b_2|, \ldots, |b_N|\}$ and $\{\mathrm{sign}(b_1 \times b_1), \mathrm{sign}(b_1 \times b_2), \ldots, \mathrm{sign}(b_1 \times b_N)\}$. With the side information, Alice can infer b_1 with an enhancement of $\sqrt{N}$ in SNR. This protocol had been experimentally demonstrated[36] and adopted in IoT systems.[16] However, in this protocol, the LO should be prepared by host and sent to client together with the signal, which may induce crosstalk and loopholes.

The real LO CV-QKD scheme

To avoid the loophole induced by sending the LO and alleviate the power required for the LO, in 2015, Qi's group proposed a scheme to use a locally generated LO for CV-QKD.[31] To provide a phase reference, Alice inserts a pilot pulse between two signal pulses. At Bob's site, the relative phase ϕ between the signal and LO is monitored by measuring two quadratures X_R and P_R of the pilot pulse, which can be written as

$$\phi = -\tan^{-1}\frac{P_R}{X_R} \tag{5}$$

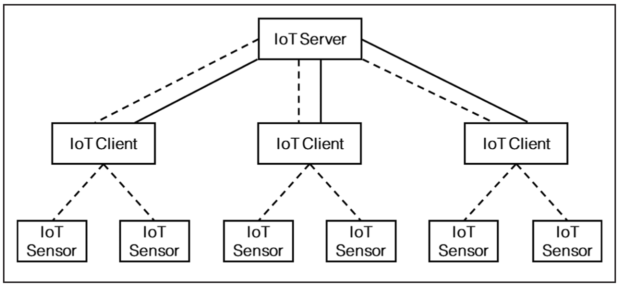

Figure 1. The hierarchy of the IoT system with quantum channels (solid lines) and classical channels (dashed lines).

Then, Alice and Bob can establish a relation between their variables as

$$\begin{aligned} X_B &= X_A\cos\phi + P_A\sin\phi + \sqrt{\tfrac{2-T}{T}}X_0 + \delta X \\ P_B &= -X_A\sin\phi + P_A\cos\phi + \sqrt{\tfrac{2-T}{T}}P_0 + \delta P \end{aligned} \tag{6}$$

In this scheme, the slow frequency drift of the LO is only monitored but not compensated, which means the drift will be accumulated and even run out of the bandwidth of the detector. It may lead to the breakdown of the system and compromise the long-term stability. In addition, high-frequency phase noise accumulated between the signal and pilot pulses is not taken into account and is fully mixed into the signal, leading to an underestimation of the channel noise and therefore resulting in loopholes of the security.

The CV-QC scheme with a locked LO

System configuration

A typical IoT system is illustrated in Figure 1. The server and the controller can perform QKD via quantum channels, which are usually fiber links. The classical information for reconciliation and privacy amplification is transferred via classical channels, which can be fiber links or wireless channels. While the sensors can only obtain keys from the controller via classical channels due to their size and power limitations.[17]

The setups of the server and the controller are depicted in Figure 2. Since the IoT controller is capable of working as either the host or the client, the IoT server can adopt the identical configuration. Therefore, for the sake of simplicity, we omit the details in the server. The optical signals are shown with solid lines and arrows indicating the propagation direction, while the electric signals are shown with dashed lines. At the controller site, there is a local laser with the linewidth of about 150 kHz.[32] Its output is splitted into 32 beams with a 1 × 32 beamsplitter. The first 30 beams are sent to a fiber-coupled photodiode array (FCPA) to perform 15 sets of homodyne detection. The measurement outputs are converted to digital signals with 15 analogue-to-digital converters (ADCs), and their least significant bits are stored as quantum random numbers.

When the controller works as a client, the server takes turns to send a weak signal pulse and a relatively strong reference pulse, with the pulse width of 30 ns, and the separation of 30 ns. The signal pulse has modulated information X_A and P_A on X and P quadratures, respectively, while the reference pulse only has a constant large DC component on the X quadrature. At the controller site, the optical switch is turned to the upper route. A heterodyne detection is performed with a portion from the local laser. By mixing the $\omega_0 = 2\pi \times 200$ MHz cosinusoidal signal and 10 MHz low-pass filtering, a beat frequency locking error signal of the reference pulse and the LO is obtained. With a properly tuned proportional integral derivative controller, the error signal is converted to a feedback signal and added to the local laser. Usually, the locking bandwidth is at megahertz level. By mixing with the cosinusoidal (sinusoidal) signal and 50 MHz high-pass filtering, X_B (P_B) are extracted from the signal pulse.

When the controller works as a host, the optical switch at the controller site is turned to the lower route. The controller also takes turns to generate signal and reference pulses. The proportional integral derivative (PID) controller is disabled when the local laser works in a free running mode. A portion from the local laser is splitted by the beam splitter (BS) and modulated in amplitude and phase. To generate a reference pulse, the amplitude is not attenuated and the phase is set to 0. To generate a signal pulse, the amplitude is strongly attenuated, and the phase is randomly modulated to $i\pi/2$, where $i = 0, 1, 2, 3$ is a two-bit quantum random number stored in the memory.

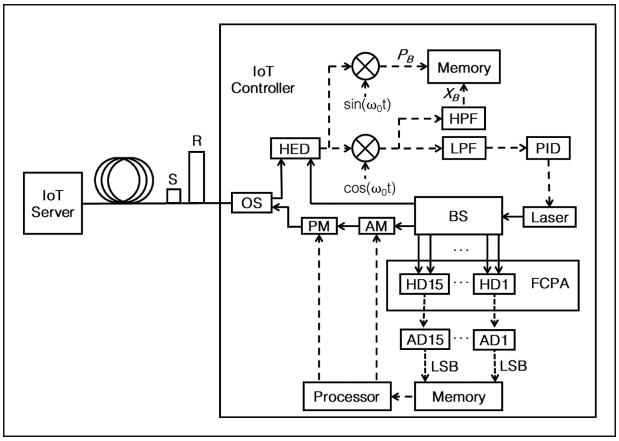

Figure 2. The schematic of the locked LO CV-QC scheme. S: the signal pulse; R: the reference pulse; OS: optical switch; HED: heterodyne detector; LPF: low pass filter; HPF: high pass filter; PID: proportional integral derivative controller; BS: beam splitter; AM: amplitude modulator; PM: phase modulator; FCPA: fiber coupled photodiode array; HD: homodyne detector; AD: analogue to digital converter; LSB: least significant bit.

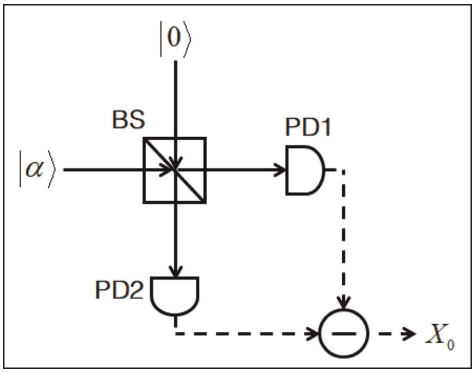

Figure 3. The equivalent homodyne detection on the vacuum state. BS: 50/50 beam splitter; PD: photodiode.

Quantum random number generation with homodyne detection

Quantum random numbers can be generated by performing homodyne detection on vacuum states.[37] The Wigner function of a vacuum state can be written as[38]

$$W_0(x, p) = \frac{1}{\pi} \exp\left(-x^2 - p^2\right) \tag{7}$$

Since the function is isotropic in phase space, without loss of generality, we can suppose it is the X quadrature being measured when performing homodyne detection on vacuum states.

The homodyne detection in Figure 2 is equivalent of measuring a quadrature of a vacuum state, as shown in Figure 3. $|\alpha\rangle$ is a coherent state, which is a portion of the local laser beam. It interferes with a vacuum state $|0\rangle$ at a 50/50 beam splitter. The two transmitted beams are detected by two identical photodiodes. One output is then subtracted by the other, giving the measurement result of the X quadrature of the vacuum state. Considering the quasi-probability distribution nature of the Wigner function, the measurement result probability is

$$P(x) = |\psi_0(x)|^2 = \int_{-\infty}^{\infty} W_0(x, p) dp = \pi^{-1/2} \exp\left(-x^2\right) \tag{8}$$

where $\psi_0(x)$ is the wave function of a vacuum state in the X representation. According to postulates of quantum mechanics, when the X quadrature of the vacuum state is measured, the result is a Gaussian random variable with the mean of 0 and the variance of $1/2$, which is known as the shot noise.

However, besides the shot noise, the realistic measurement result also contains other classical noise, such as electric noise in the circuit and pickups from the environment. This noise source may alter the statistic property of the measurement result and make it less random. To get rid of the influence of the classical noise, we can use the least significant bit (LSB) of the output of the AD as the random number.[26] It is worth to notice that, although the truly random bits may be more than 1, for the sake of simplicity and compactness of the IoT devices, we prefer to keep only the LSB. Let N_t, N_s, and N_c be the total noise, the shot noise, and the classical noise, respectively, we have

$$N_t = N_s + N_c \tag{9}$$

Then, the relationship of their LSB can be written as

$$n_t = n_s \oplus n_c \tag{10}$$

where n_t, n_s, and n_c are the LSB of N_t, N_s, and N_c, respectively, and $\oplus$ is the exclusive OR operation. Equation (10) is formally one time pad encryption, where n_t, n_s, and n_c are the ciphertext, the key, and the plaintext, respectively. The ciphertext is random only if the key is truly random, regardless of the plaintext. Therefore, when we keep n_t as the random number, classical noise will not compromise its randomness. These random numbers can be used to modulate the signal pulses when the controller works as a host. Also, they can be used to establish a key with corresponding sensors using traditional key distribution techniques.[17]

Security analysis of the CV-QKD scheme with a locked LO

When the local laser is locked to the reference pulses with beat frequency locking, the low frequency noise is compensated all the time and the linewidth of the beat signal can be suppressed to sub-hertz level. However, the bandwidth of the locking module is usually at megahertz level. Only the noise within the locking bandwidth can be sufficiently suppressed. While outside the locking bandwidth, power spectrum density of the beat signal is still in Lorentzian lineshape, which can be written as

$$P(f) = \frac{1}{\pi}\frac{1}{1 + (2f/f_0)^2} \tag{11}$$

where f_0 is the linewidth. The typical power spectrum density curves of free running and locked beat signal are shown in Figure 4. Therefore, the uncompensated laser noise needs to be taken into account.

To decrease the influence of the uncompensated noise, the signal should be shifted from DC to where the noise is at an acceptable level. Suppose the frequency range of modulated signal ranges from f_a to f_b, the noise induced by the laser ε_0 is proportional to the area of the shaded region, as shown in Figure 5. It is straightforward to obtain

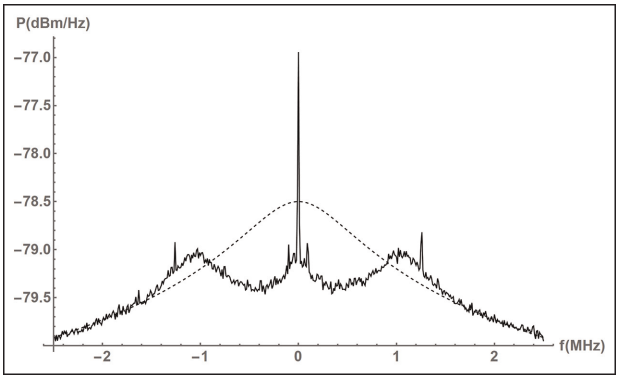

Figure 4. The power spectrum density curve of the beat signal between the signal and the LO, with LO unlocked (dashed line) and locked (solid line).

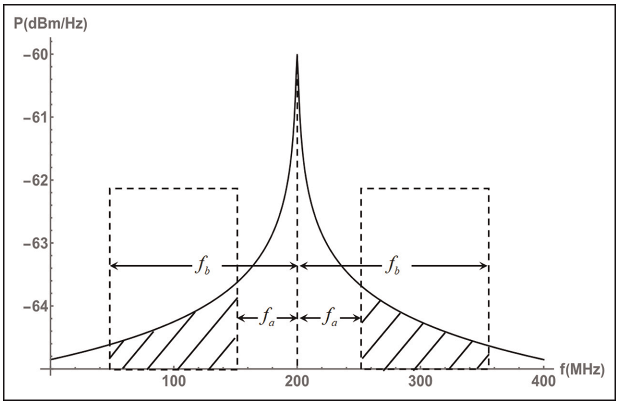

Figure 5. Illustration of the power spectrum density of the noise and frequency range of the signal, which starts from f_a and stops at f_b. The shaded area is the noise to be considered in security analysis.

$$\varepsilon_0 = 2\alpha^2\left[\frac{\arctan(2f_b/f_0) - \arctan(2f_a/f_0)}{\pi}\right] \tag{12}$$

For $f_0 = 150$ kHz, let $f_a = 50$ MHz, we have $\varepsilon_0 \approx 10^{-3}\alpha^2$.

The secret key rate of the discretely modulated CV-QKD under the collective attack can be calculated in the asymptotic limit.[25] When Alice sends the states defined in equation (4), the modulation variance is $V_A = 2\alpha^2$. The total variance of the states is then $V = V_A + 1$, including the shot noise. For a 50-km standard telecom fiber with 0.2 dB/km loss, the transmittance $T_0 = 0.1$. Considering the deviation of discrete modulation to the ideal Gaussian modulation, the effective channel loss T and source excess noise ε should be modified to

$$\begin{aligned} T &= T_0 \frac{Z^2}{Z_E^2} \\ \varepsilon &= \frac{Z_E^2}{Z^2}(V_A + \varepsilon_0) - V_A \end{aligned} \tag{13}$$

where

$$\begin{aligned} Z &= 2\alpha^2\left(\xi_0^{\frac{3}{2}}\xi_1^{-\frac{1}{2}} + \xi_1^{\frac{3}{2}}\xi_2^{-\frac{1}{2}} + \xi_2^{\frac{3}{2}}\xi_3^{-\frac{1}{2}} + \xi_3^{\frac{3}{2}}\xi_0^{-\frac{1}{2}}\right) \\ Z_E &= \sqrt{V_A^2 + 2V_A} \end{aligned} \tag{14}$$

with

$$\begin{aligned} \xi_{0,2} &= \tfrac{1}{2}\exp(-\alpha^2)(\cosh(\alpha^2 \pm \cos(\alpha^2)) \\ \xi_{1,3} &= \tfrac{1}{2}\exp(-\alpha^2)(\sinh(\alpha^2 \pm \sin(\alpha^2)) \end{aligned} \tag{15}$$

Then, channel noise is $\chi_c = 1/T - 1 + \varepsilon$. At Bob's site, suppose a typical heterodyne detector is adopted, whose quantum efficiency is 0.8, electronic noise is 0.1 in shot noise unit, and bandwidth is 350 MHz. The heterodyne detection noise is then $\chi_d = 2(1 + \upsilon)/\eta - 1$, and the total noise is $\chi_t = \chi_c + \chi_d/T$. For the sake of simplicity, we define the following variables

$$\begin{aligned} &a = V, \quad b = T(V + \chi_c), \quad c = \sqrt{T(V^2 - 1)} \\ &A = a^2 + b^2 - 2c^2, \quad B = (ab - c^2)^2 \\ &C = \tfrac{A\chi_d^2 + 2\chi_d\left(a\sqrt{B} + T(V + \chi_c)\right) + 2c^2 + B + 1}{(b + \chi_d)^2} \\ &D = \left(\tfrac{a + \sqrt{B}\chi_d}{b + \chi_d}\right)^2 \\ &\lambda_{1,2} = \sqrt{\tfrac{1}{2}\left(A + \sqrt{A^2 - 4B}\right)} \\ &\lambda_{3,4} = \sqrt{\tfrac{1}{2}\left(C + \sqrt{C^2 - 4D}\right)} \end{aligned} \tag{16}$$

and a function

$$g(x) = \frac{x+1}{2}\log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right) \tag{17}$$

Therefore, the secret key rate is

$$K = \beta \log_2\left(\frac{V + \chi_t}{1 + \chi_t}\right) - g(\lambda_1) - g(\lambda_2) + g(\lambda_3) + g(\lambda_4) \tag{18}$$

where β is the reconciliation efficiency, which can reach 0.95.[39] The relation between the modulation variance V_A and the secret key rate K is shown in Figure 6. From Figure 6, we can find the optimal modulation variance to be 0.29, and the maximum secret key rate to be 4.71×10^{-3}. For a modulation bandwidth of 100 MHz, and considering that a half of the signal is used for channel parameter estimation, the final key rate is about 59 kb/s. It is worth to note that the state of the art homodyne/heterodyne detector has a bandwidth of over 900 MHz.[40] Thus, the final key rate can be further increased when a larger bandwidth homodyne/heterodyne detector is adopted.

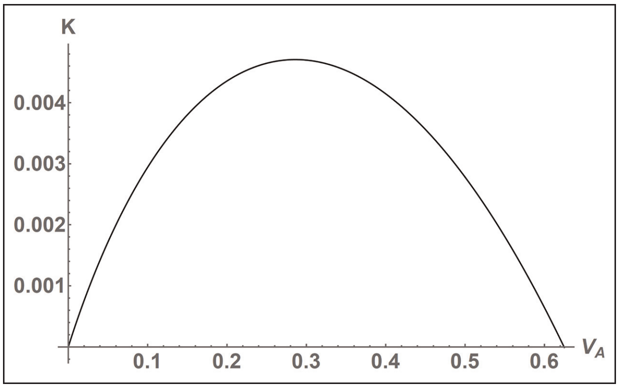

Figure 6. The relation between the modulation variance V_A and the secret key rate K.

Conclusion

In this article, we proposed a flexible CV-QC scheme for IoT systems with zero-trust security. The IoT controller with a local laser can generate quantum random numbers for CV-QKD and share keys with related IoT sensors using traditional key distribution techniques. To perform CV-QKD, both the server and the controller can be configured as either the host or the client. When the controller works as a client, the local laser is locked to reference pulses from the server using beat frequency locking. In this way, the slow frequency drift of the local laser is compensated, ensuring the long-term stability of the system. Also, since dynamic phase difference monitoring and data processing are not needed, the complexity of the system can be reduced. The security of the scheme is analyzed taking into account the residual phase noise between the signal and LO. When the signal is modulated in 50 MHz away from DC, the excess noise of the signal can be sufficiently suppressed. A final key rate of 59 kb/s can be established over a 50-km fiber link with the modulation bandwidth of 100 MHz. Considering this scheme is highly compatible with the classical coherent optical communication system, it will offer a lot of potential applications for the IoT networks when information security is of concern.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the National Natural Science Foundation of China (62105368).

ORCID iD

Hongxin Zou https://orcid.org/0000-0002-4172-5214

References

1. HIS. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), 2019, https://www.statista.com/statistics/471264/iotnumber-of-connected-devices-worldwide/
2. Fernndez-Caramés TM. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet Things* 2020; 7: 6457–6480.
3. Chrysostomou AC and Hadjichristofi G. Internet of Things: security vulnerabilities and challenges. In: *2015 IEEE symposium on computers and communication (ISCC)*, Larnaca, Cyprus, 6–9 July 2015, pp.180–187. New York: IEEE.
4. Lin J, Yu W, Zhang V, et al. A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things* 2017; 4: 1125–1142.
5. Samaniego M and Deters R. 2018 Zero-trust hierarchical management in IoT. In: *2018 IEEE international congress on Internet of Things (ICIOT)*, San Francisco, CA, 2–7 July 2018, pp.88–95. New York: IEEE.
6. Committee on National Security Systems (CNSS). *CNSS Advisory Memorandum Information Assurance 02-15: use of public standards for the secure sharing of information among national security systems*. Fort Meade, MD: CNSS, 2015.
7. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J Comput* 1997; 26: 1484–1509.
8. Lee W, No J-S and Kim Y-S. Punctured ReedCMuller codebased McEliece cryptosystems. *IET Commun* 2017; 11: 1543–1548.
9. Bernstein DJ, Buchman J and Dahmen E. *Post-quantum cryptography*. Berlin: Springer, 2009.
10. Aujla GS, Chaudhary R, Kaur K, et al. SAFE: SDN-assisted framework for edge-cloud interplay in secure healthcare ecosystem. *IEEE T Ind Inform* 2019; 15: 469–480.
11. De Feo L, Jao D and Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J Math Cryptol* 2014; 8: 209–247.
12. Cheng C, Lu R, Petzoldt A, et al. Securing the Internet of Things in a quantum world. *IEEE Commun Mag* 2017; 55: 116–120.
13. Guillen OM, Pöppelmann T, Mera JMB, et al. Towards post-quantum security for IoT endpoints with NTRU. In: *Design, automation & test in Europe conference & exhibition (DATE), 2017*, Lausanne, 27–31 March 2017, pp.698–703. New York: IEEE.
14. Bailey DV, Coffin D, Elbirt A, et al. NTRU in constrained devices. In: Koç ÇK, Naccache D and Paar C (eds) *Cryptographic Hardware and Embedded Systems—CHES 2001*. Berlin: Springer, 2001, pp.262–272.
15. Wen X, Wang G, Chen Y, et al. Quantum solution for secure information transmission of wearable devices. *Int J Distrib Sens N* 2018; 14: 79678.
16. Li M and Wang T. Optimized coherent state based quantum cryptography with high robust for networks deployment. *IEEE Access* 2019; 7: 109628–109634.
17. Al-Mohammed HA, Al-Ali A, Yaacoub E, et al. Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios. *IEEE Access* 2021; 9: 136994–137004.
18. Rivero-Angeles ME. Quantum-based wireless sensor networks: a review and open questions. *Int J Distrib Sens N* 2021; 17: 52210.
19. Shannon CE. Communication theory of secrecy systems. *Bell Labs Tech J* 1998; 15: 57.
20. Wei W and Guo H. Bias-free true random-number generator. *Opt Let* 2009; 34: 1876.
21. Qi B, Chi YM, Lo HK, et al. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt Lett* 2010; 35: 312.
22. Bennett Ch and Brassard G. Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of the IEEE international conference on computers, systems, and signal processing*, Bangalore, India, 9–12 December 1984, pp.175–179. New York: IEEE.
23. Grosshans F and Grangier P. Continuous variable quantum cryptography using coherent states. *Phys Rev Lett* 2022; 88: 057902.
24. Ke X and Wu P.Coherent optical communication. In: Ke X and Wu P (eds) *Adaptive optics theory and its application in optical wireless communication. Optical wireless communication theory and technology*. Singapore: Springer, 2022, pp.21–45.
25. Lodewyck J, Bloch M, Garcia-Patron R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys Rev A* 2007; 76: 042305.
26. Shen Y, Zou H, Tian L, et al. Experimental study on discretely modulated continuous-variable quantum key distribution. *Phys Rev A* 2010; 82: 022317.
27. Jouguet P, Kunz-Jacques S, Leverrier A, et al. Experimental demonstration of long-distance continuous variable quantum key distribution. *Nat Photonics* 2013; 7: 378–381.
28. Fossier S, Diamanti E, Debuisschert T, et al. Field test of a continuous-variable quantum key distribution prototype. *New J Phys* 2009; 11: 045023.
29. Shen Y, Chen Y, Zou H, et al. A fiber-based quasi-continuous-wave quantum key distribution system. *Sci Rep* 2014; 4: 4563.
30. Ma X-C, Sun S-H, Jiang M-S, et al. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys Rev A* 2013; 87: 052309.
31. Qi B, Lougovski P, Pooser R, et al. Generating the local oscillator locally in continuous-variable quantum key distribution based on coherent detection. *Phys Rev X* 2015; 5: 041009.

32. Wang T, Huang P, Zhou Y, et al. High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt Express* 2018; 26: 2794–2806.
33. Li L, Li H, Li C, et al. 2018 The security analysis of E91 protocol in collective-rotation noise channel. *Int J Distrib Sens N*; 14: 78192.
34. Chen Y, Wen X, Sun Z, et al. A sensitive information protection scheme in wearable devices based on quantum entanglement. *Int J Distrib Sens N* 2018; 14: 08487.
35. Leverrier A and Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys Rev Lett* 2009; 102: 180504.
36. Shen Y, Zou H, Tian L, et al. Experimental study on discretely modulated continuous-variable quantum key distribution. *Phys Rev A* 2010; 82: 022317.
37. Shen Y, Tian L and Zou H. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys Rev A* 2010; 81: 063814.
38. Leonhardt U. *Measuring the quantum state of light*. Cambridge: Cambridge University Press, 1997.
39. Leverrier A, Alléaume R, Boutros J, et al. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys Rev A* 2008; 77: 042325.
40. Zhang X, Zhang Y, Xu B, et al. Experimental implementation of high-speed balanced homodyne detector. In: *Frontiers in optics / Laser science, OSA technical digest*, paper JW3A.85. Washington, DC: Optica Publishing Group, 2018. https://opg.optica.org/abstract.cfm?uri=FiO-2018-JW3A.85)