PAPER • OPEN ACCESS

Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme

View the article online for updates and enhancements.

Quantum Science and Technology

Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme

Shuang Wang[1,2,3], Zhen-Qiang Yin[1,2,3] ⓘ, H F Chau[4], Wei Chen[1,2,3,5], Chao Wang[1,2,3], Guang-Can Guo[1,2,3] and Zheng-Fu Han[1,2,3,5]

1   CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, People's Republic of China
2   Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China
3   State Key Laboratory of Cryptology, PO Box 5159, Beijing 100878, People's Republic of China
4   Department of Physics and Center of Theoretical and Computational Physics, Pokfulam Road, Hong Kong
5   Authors to whom any correspondence should be addressed.

E-mail: weich@ustc.edu.cn and zfhan@ustc.edu.cn

Abstract

In comparison to qubit-based protocols, qudit-based quantum key distribution ones generally allow two cooperative parties to share unconditionally secure keys under a higher channel noise. However, it is very hard to prepare and measure the required quantum states in qudit-based protocols in general. One exception is the recently proposed highly error tolerant qudit-based protocol known as the Chau15 (Chau 2015 *Phys. Rev.* A **92** 062324). Remarkably, the state preparation and measurement in this protocol can be done relatively easily since the required states are phase encoded almost like the diagonal basis states of a qubit. Here we report the first proof-of-principle demonstration of the Chau15 protocol. One highlight of our experiment is that its post-processing is based on practical one-way manner, while the original proposal in Chau (2015 *Phys. Rev.* A **92** 062324) relies on complicated two-way post-processing, which is a great challenge in experiment. In addition, by manipulating time-bin qudit and measurement with a variable delay interferometer, our realization is extensible to qudit with high-dimensionality and confirms the experimental feasibility of the Chau15 protocol.

Introduction

Quantum key distribution (QKD) allows two distant peers Alice and Bob to share secret key bits through a quantum channel which is accessed by a malicious eavesdropper Eve [1, 2]. In a typical QKD protocol, Alice encodes random classical bits into quantum states, and sends them to Bob, who measures the incoming quantum states to decode Alice's classical bits. Then by classical communications and random sampling, Alice and Bob can obtain raw key bits, whose error rate can be also estimated. Finally, by classical post-processing, Alice and Bob can generate secret key bits. The most commonly used QKD protocol is the Bennett–Brassard 1984 (BB84) protocol [1] combined with the decoy states method [3–5]. In the past decade, tremendous progresses in experimental decoy states BB84 have been achieved [6–12]. Lately, several novel QKD protocols have been proposed [13, 14–16]. Among these protocols, measurement-device-independent-QKD [14] is immune to all detector-side-channel attacks and have been proven to be a feasible QKD scheme [17–21]. And the round-Robin-differential-phase-shift (RRDPS) protocol features that monitoring signal disturbance can be bypassed [16], thus becomes another hot topic. In the RRDPS protocol, Alice has to prepare trains of pulses each consisting of L pulses. In the simple case that each train contains only one photon, the secret key rate R of the RRDPS protocol in the one-way classical communication setting equals $1 - h_2(e_{bit}) - h_2(1/(L-1))$, where e_{bit} is the bit error rate of the raw key [16]. In other words, the RRDPS protocol can tolerate much higher bit error rate of the raw key than the BB84 protocol when L is sufficiently large. However, implementing the RRDPS

protocol for large L posts a great experimental challenge. In spite of the experimental difficulty, several experimental demonstrations of RRDPS protocol have been reported [22–25].

Inspired by the RRDPS protocol, Chau recently proposed a novel QKD protocol [13], called the Chau15 protocol, which can tolerate very high error rate and has a simpler implementation than the RRDPS protocol. In the Chau15 protocol, for each trial Alice randomly picks two distinct numbers i, j from the set $\{1, \ldots, L\}$ and a raw key bit $k \in \{0 \equiv +, 1 \equiv -\}$, then prepares a quantum state $|\psi_{ij}^{\pm}\rangle = (|i\rangle \pm |j\rangle)/\sqrt{2}$ according to the value of k used. That is to say, Alice encodes each raw bit in the phase between the two time bins $|i\rangle$ and $|j\rangle$. Alice sends $|\psi_{ij}^{k}\rangle$ to Bob, who then randomly picks two distinct numbers m, n in $\{1, \ldots, L\}$ and measures the incoming photon along $\{|\psi_{mn}^{\pm}\rangle\}$. Bob records his raw key bit as 0 or 1 according to the measurement result should the detector clicks. Repeating above steps for sufficient times, Alice and Bob announce their i, j and m, n for each trial and only retain the raw key bits correspond to the cases that $\{i, j\} = \{m, n\}$ as their sifted key bits. In [13], Chau proved that secret key bits can be generated when the error rate of sifted key bits is very high. It is remarkable that this scheme can tolerate up to 50% error rate provided that $L = 2^p$ for some integer $p \geqslant 2$.

It is instructive to realize the Chau15 protocol experimentally. One challenge is that one must prepare and measure certain high-dimensional quantum states, namely, qudits, in the Chau15 protocol although preparing and measuring these special qudit states are less complicated that those for a general qudit state. Another challenge is that the two-way classical communication post-processing method reported in [13] is both rather complicated and of low yield. Here, we first present a new security proof of the Chau15 protocol based on standard one-way communication plus a simple secret key rate formula for any integer $L \geqslant 4$ rather than only for L in the form 2^p. Then, we report a proof-of-principle experimental demonstration of the Chau15 protocol. In this experiment, we encode the qudit based on quantum superposition of time-bin and measurement is performed with the help of a variable delay interferometer [24]. As far as we know, this is the first experiment of the Chau15 protocol.

Security proof of the Chau15 protocol for arbitrary $L \geqslant 4$ with one-way communication

We first consider the case of an ideal single photon source and ideal detectors. Since the protocol is permutationally symmetric, quantum de Finetti theorem [26] implies that we only need to consider the security under Eve's general collective attack in the form

$$U_{\text{Eve}}|i\rangle |E_{00}\rangle = \sum_{j=0}^{L} c_{ij}|j\rangle |E_{ij}\rangle, \tag{1}$$

where $|E_{ij}\rangle$ is the quantum state of Eve's ancilla, $\{|E_{ij}\rangle\}$ is a set of basis for Eve's ancilla, $\langle E_{ij}|E_{il}\rangle = \delta_{jl}$. Without loss of generality, we assume $c_{ij} \geqslant 0$ and $\sum_{j=0}^{N} c_{ij}^2 = 1$.

Denote the probability that Bob obtains $|\psi_{mn}^{\pm}\rangle$ conditioned on the facts that Alice prepares her state as $|\psi_{ij}^{\pm}\rangle$ and Bob tried to project the state along $|\psi_{mn}^{\pm}\rangle$ by $p(m, n|i, j)$. In other words, $p(m, n|i, j)$ is the chance that a quantum state in Hilbert space spanned by $\{|i\rangle, |j\rangle\}$ is transformed into a space spanned by $\{|m\rangle, |n\rangle\}$.

In the supplemental material is available online at stacks.iop.org/QST/3/025006/mmedia, we show that Eve's information on all sifted key bits is given by

$$I_{AE} \leqslant h_2\left(\frac{\sum_{i<j, m<n:i, j\notin\{m,n\}} p(m, n|i, j)}{(L-2)(L-3)\sum_{i<j} p(i, j|i, j)}\right), \tag{2}$$

where $h_2(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. For easy use by experimentalists, we define the mean counting rate $Q = \sum_{i<j} p(i, j|i, j) / \binom{L}{2}$ and $Q' = \sum_{i<j, m<n:i, j\notin\{m,n\}} p(m, n|i, j) / \left(\binom{L}{2}\binom{L-2}{2}\right)$ (where $\binom{x}{y}$ is the binomial coefficient), then we have

$$I_{AE} \leqslant h_2\left(\frac{Q'}{2Q}\right). \tag{3}$$

Finally, the secret key rate per sifted key bit is given by

$$R = 1 - h_2(E) - I_{AE} \geqslant 1 - h_2(E) - h_2\left(\frac{Q'}{2Q}\right), \tag{4}$$

where E is the bit error rate of the sifted key bit.

We remark that our asymptotic bound of I_{AE} holds even when (i, j) is biased distributed. As long as the probability for Bob to measure any one of the (i, j) pairs is non-zero, we could then estimate $p(m, n|i, j)$ to arbitrarily good precision given a sufficiently long key [27]. In fact, Bob uses biased basis selection in our proof-of-principle

experiment. With the help of decoy states [3–5], this security proof can be adapted in real-life implementations with weak coherent sources. And in the supplementary material, we give an intuitive analysis to the case of finite key length with decoy states.

Demonstration of the superiority of the Chau15 protocol over the BB84 protocol

We give an example to demonstrate the superiority of the Chau15 protocol over the BB84 protocol in terms of the key rate. Suppose $L = 4$ and consider the situation that Alice and Bob use ideal apparatus. The only source of error is the quantum channel linking Alice to Bob. Suppose further that this quantum channel $\mathcal{E}$ is four-dimensional depolarizing. In other words, for any four-dimensional qudit, this channel keeps the state of the qudit unchanged with probability $1 - p$, and with probability p, the qudit is replaced by the four-dimensional completely mixed state. Thus, to each photon in the Chau15 scheme using time-bin presentation, this is just a depolarizing channel. But to the BB84 scheme using the same time-bin presentation, the situation is more complicated because the photon arrival times may change to the extend that sometimes Bob may detect multiple photons in the time window assigned to the detection of a particular photon. And sometimes, he does not detect a photon at all in that time window. In the supplementary material, we show that by sending photons in time-bin representation through this channel $\mathcal{E}$, the key rates per sifted key bit send by Alice for the Chau15 scheme with $L = 4$ and the BB84 protocols are given by

$$R_{\text{Chau15}}[\mathcal{E}] = 1 - h_2\left(\frac{p}{2}\right) - h_2\left(\frac{p}{2(2 - p)}\right) \tag{5}$$

and

$$R_{\text{BB84}}[\mathcal{E}] = 1 - 2h_2\left(\frac{p(8 - p)}{4(p^2 - 2p + 4)}\right), \tag{6}$$
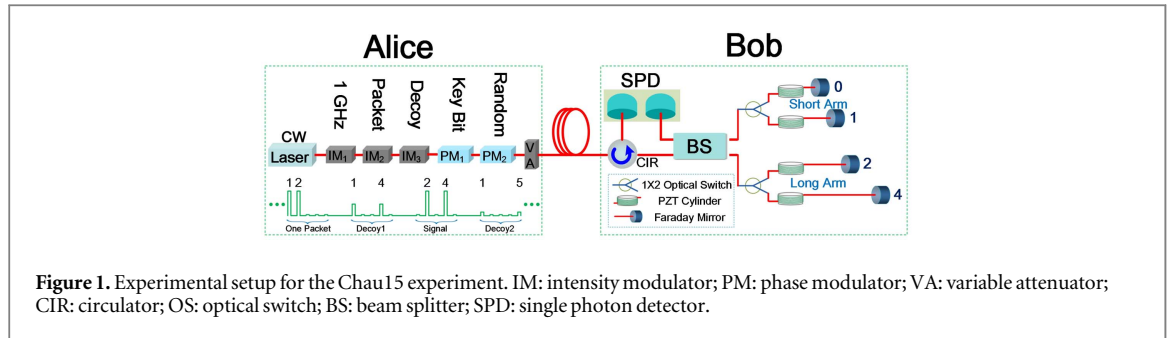
respectively. This means the supremum depolarizing probability p below which a secret key can be distilled equals 0.2835 and 0.2051 for the Chau15 and BB84 schemes, respectively. This shows the superiority of the Chau15 scheme with $L = 4$ over the BB84 protocol when p is in [0.2051, 0.2835].

Let us further analysis the situation. We show in the supplementary material that $R_{\text{Chau15}} > R_{\text{BB84}}$ for all $0 < p < 0.2051$ so that if we measure the key rate per sifted key bit, the Chau15 scheme is always better than the BB84 protocol. Nevertheless, more realistic and fair comparisons should be made which takes into account the following factors: 1. Photons wasted due to mismatch in preparation and measurement bases; 2. Photons wasted due to multiple detector clicks or null detection; 3. Difference in the actual time during per photon pulse send.

In the supplementary material, we show that in BB84, for those photons prepared and measured in the same basis, the average rate of detection equals $T_{\text{BB84}} = (p^2 - 2p + 4)/4$. And note that in the time-bin representation, the average time interval between successive photon pulse send by Alice in the Chau15 scheme for $L = 4$ is twice as long as that of the BB84 if we assume that the arrival time corresponding to $|i\rangle$ and $|i + 1\rangle$ are the same in both schemes. Taking these factors into account, the key rate per pulse to send one photon for the BB84 scheme is $\eta_{\text{BB84}} T_{\text{BB84}} R_{\text{BB84}}/2$ where $\eta_{\text{BB84}} = 1/2$ and 1 is the probability that the preparation and measurement bases agree for unbiased and extremely biased basis selection, respectively. (By extremely biased, we mean a single basis is chosen with probability arbitrarily close to 1.) The corresponding key rate for the Chau15 scheme with $L = 4$ equals $\eta_{\text{Chau15}} R_{\text{Chau15}}/4$, where $\eta_{\text{Chau15}} = 1/6$ and 1 for unbiased and extremely biased basis selection, respectively. Using the both two key rates per pulse, we conclude that for the four-dimensional depolarizing channel, the Chau15 scheme has a higher key rate than the BB84 protocol provided that $p > 0.1923$ ($p > 0.1512$) for the unbiased (extremely biased) basis selection. This further demonstrates the superiority of the Chau15 scheme over the BB84 protocol at least for the four-dimensional depolarizing channel $\mathcal{E}$ provided that it is sufficiently noisy.

Experimental setup and results

We performed the experiment using the setup in figure 1. Alice consists of a continuous wave (CW) laser at 1550.12 nm, three intensity modulators (IMs) and two phase modulators (PMs). IM_1 modulates the CW light into a coherent pulse train with a temporal width of 96 ps and a repetition rate of 1 GHz. IM_2 chops this pulse train into packets of 5 time slots (5 ns), in which only two random pulses indexed by i and j ($i, j \in \{1, 2, 3, 4, 5\}$ and $i < j$) are allowed to pass. IM_3 is employed to implement the decoy states method [3–5], in which each packet is randomly modulated into signal, decoy1, or decoy2 states. PM_1 encodes key bits by modulating phase $\left\{-\frac{\pi}{2}, \frac{\pi}{2}\right\}$ on pulses for each packet, and PM_2 adds random global phase on each packet. Finally, the variable

Figure 1. Experimental setup for the Chau15 experiment. IM: intensity modulator; PM: phase modulator; VA: variable attenuator; CIR: circulator; OS: optical switch; BS: beam splitter; SPD: single photon detector.

attenuator (VA) attenuates the average photon numbers per packet to the single photon level. The output quantum state prepared by Alice can be expressed as $|\psi_{ij}\rangle = (|i\rangle + e^{i\phi}|j\rangle)/\sqrt{2}$, where $\phi \in \{0, \pi\}$ is the phase difference between the ith and jth pulses.

Bob mainly consists of a 1 GHz, 1–4 bit variable-delay Faraday–Michelson interferometer (FMI) and a double-channel single-photon detector (SPD). By setting the delay to r, the variable-delay FMI makes the ith pulse interfere with the jth pulse if $j = i + r$. (Since no pulse will be picked to interfere with pulse i whenever $i + r > 5$, Bob is in effect biased in measurement basis selection in our demonstrative experiment.) Two channels of the SPD are connected to each of the output ports of the FMI, and which channel records a detection event depends on the phase difference ϕ. Through recording a click event in the interference slot, Bob fulfills the quantum projection into $|\psi_{ij}^{\pm}\rangle$.

To realize the variable-delay interferometer, the same structure as in [24] is employed here. Each of the two arms of this interferometer has two fiber delays, and the delay is chosen by a bidirectional NanoSpeed 1×2 optical switch (OS). The arm with the $\{0, 1\}$ delays is named the short arm, and the arm with the $\{2, 4\}$ delays is named the long arm. The chosen delays of the long and short arms are denoted as $x \in \{2, 4\}$ and $y \in \{0, 1\}$ respectively. Then, the delay of the interferometer is $r = x - y$. In total, the variable-delay FMI can achieve fast switch among 1–4 ns delay values. The piezoelectric transducer cylinder wrapped with 2 m fiber was used to obtain high precision of each delay, and also to compensate the phase shift of the interferometer. The insertion loss (IL) of the interferometer (including the IL of the circulator) is about 2.0 dB, and the values of each delay are almost the same. This variable-delay interferometer is polarization insensitive owning to Faraday mirrors and features an average extinction ratio of 23 dB.

Photons from the variable-delay FMI were detected by the double-channel SPD, and finally recorded by a time-to-digital converter (TDC). Both channels of SPD are based on InGaAs/InP avalanche photodiodes and employ the sine-wave filtering method [28]. The first channel features a detection efficiency of 22.1% (down to 20.8% if including $2 \rightarrow 3$ IL of CIR), a dark count rate of 1.5×10^{-6} per gate, and after-pulse probability of 0.8%. The second channel features a detection efficiency of 20.9%, a dark count rate of 1.1×10^{-6} per gate, and after-pulse probability of 1.1%. The TDC not only recorded signals but also set measurement time window. The value of the time window was set to 800 ps during the experiment, and this setting reduced the average effective detection efficiency of two channels of the SPD to 20.4%, while the total dark count was just a little less than 2.6×10^{-6} per gate.

Based on the experimental parameters listed above, the performance of Chau15 system was estimated and all parameters were optimized by maximizing the secret key rate. Setting the intensity and probability of one signal (μ) and two decoy states (ν_1 and ν_2) close to the optimal ones, we measured the mean yield Q and Q', and error rate of the signal state E_μ at four fiber lengths: 50, 100, 130 and 150 km. When Alice prepares laser pulse at time slots i and j, Bob gets the mean yield $Q = \sum_{i<j} p(i, j|i, j) / \binom{5}{2}$ if he also gets interference output between these two time slots, and Bob gets the mean yield $Q' = \sum_{i<j, m<n:i,j\notin\{m,n\}} p(m, n|i, j) / \left(\binom{5}{2}\binom{3}{2}\right)$ if he obtains interference output between time slots m, $n \notin \{i, j\}$. The experimental results are listed in table 1. The last set of data over 50 km length fiber is obtained in high error rate case, which may happen in the ultrahigh speed case or harsher environment. In the experiment, we intentionally distorted the modulating signal on PM_1 to get error rate over 20%.

Secret keys can still be extracted at a transmission distance of 150 km, which is comparable with the commonly used BB84 protocol. The secret key rate per packet is at 10^{-3} level over 50 km length fiber, which is lower than BB84 protocol. Note that in the absence of Eve, our experimental setup with this 50 km fiber causes mostly phase error σ_z rather than spin-flip error σ_x to our qudit in time-bin representation. Actually, the σ_x error rate is of order of 10^{-3}, which is only about 10% of that of σ_z error rate. With such a small σ_x error rate, we may use the biased-basis method by preferentially select the preparation and measurement basis in the Chau15 protocol to be $(|0\rangle| \pm |1\rangle)/\sqrt{2}$. In doing so, its secret key rate per packet is asymptotically equal to that of the biased BB84 in time-bin representation for they have essentially the same setup in this limit. In addition, when the error rate exceeds 20%, Chau15 protocol can still get secret key rate at 10^{-5} level over 50 km length fiber. Therefore, Chau15 protocol can outperform BB84, especially in the high error rate case. And, Chau15 protocol can also
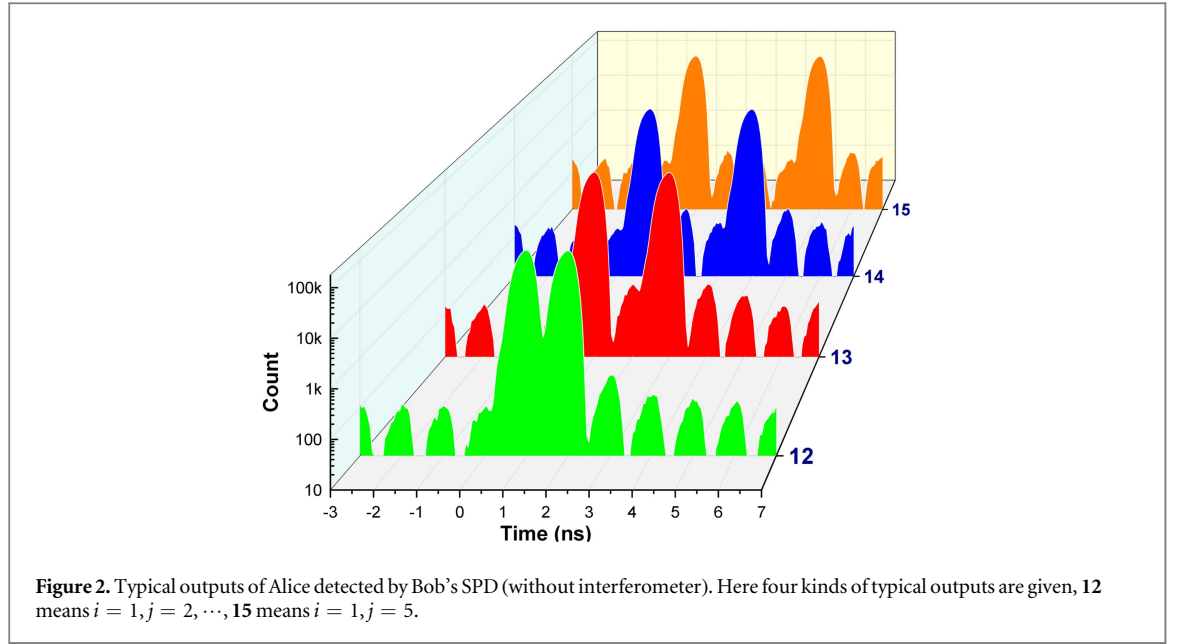
Figure 2. Typical outputs of Alice detected by Bob's SPD (without interferometer). Here four kinds of typical outputs are given, **12** means $i = 1, j = 2, \cdots$, **15** means $i = 1, j = 5$.

Table 1. Experimental results. The length of fiber (l), intensity (Int.) and probability (P) of one signal (μ) and two decoy states (ν_1 and ν_2), the mean yield (Q and Q'), error rate of the signal state (E_μ), and the secret key rate per packet(R_{inf} for infinite packet number and R_f for finite packet number). The last set of data over 50 km fiber is obtained in high error rate case. The total number of packets sent from Alice is $N = 3 \times 10^{11}$, the failure probability is set to be 10^{-10}, and parameters are optimized. The detailed formulae for calculating key rate are given in supplementary file.

l(km)	Int. (ph/packet)		P(%)	Q	Q'	E_μ(%)	R_{inf}	R_f
50	μ	0.66	97.81	4.36×10^{-3}	1.10×10^{-5}	1.83	1.48×10^{-3}	1.43×10^{-3}
	ν_1	0.05	1.40	3.33×10^{-4}	3.23×10^{-6}			
	ν_2	0.0016	0.79	1.34×10^{-5}	2.61×10^{-6}			
100	μ	0.62	94.64	4.05×10^{-4}	3.36×10^{-6}	2.16	1.25×10^{-4}	1.15×10^{-4}
	ν_1	0.10	3.36	6.75×10^{-5}	2.71×10^{-6}			
	ν_2	0.0015	2.00	3.58×10^{-6}	2.60×10^{-6}			
130	μ	0.57	87.74	9.04×10^{-5}	2.76×10^{-6}	3.21	1.99×10^{-5}	1.66×10^{-5}
	ν_1	0.14	7.52	2.42×10^{-5}	2.63×10^{-6}			
	ν_2	0.0014	4.74	2.81×10^{-6}	2.60×10^{-6}			
150	μ	0.50	36.12	3.31×10^{-5}	2.64×10^{-6}	5.68	1.19×10^{-6}	7.06×10^{-7}
	ν_1	0.14	37.76	1.11×10^{-5}	2.61×10^{-6}			
	ν_2	0.0012	26.12	2.67×10^{-6}	2.60×10^{-6}			
50	μ	0.07	84.45	4.65×10^{-4}	3.47×10^{-6}	20.32	2.80×10^{-5}	2.24×10^{-5}
	ν_1	0.035	10.40	2.34×10^{-4}	3.03×10^{-6}			
	ν_2	0.0002	5.15	3.73×10^{-6}	2.60×10^{-6}			

outperform RRDPS. The maximum transmission distance of the $L = 5$ RRDPS experiment system is less than 50 km using superconducting SPDs [23], while in our $L = 5$ Chau15 system, the transmission distance could reach 150 km with InGaAs/InP SPD. The tolerant error rate of the $L = 65$ RRDPS experiment system with the weak coherent source is less than 17% [24], while the value can exceed 20% in Chau15 system even $L = 5$. These results verified that Chau15 protocol has good comprehensive performances on maximum transmission distance, secret key rate and tolerant error rate with small L.

Nevertheless, the secret key rate per second of our proof-of-principle experimental realization is limited by the OS, whose switching speed in the setup is about 100 ns. This limitation can be overcome by employing the passive scheme based on $1 \times (L - 1)$ BS (just like [23]), or slow basis choice method [29], or the development of OS techniques in the near future. The main drawback of using passive beam splitter is that more SPDs are needed, which may be very impractical when L is large. And the total dark count rate is also increased in this case.

Another difficulty to overcome is to obtain relatively small yield Q', which plays an important role to estimate Eve's information (see equation (3)). The smaller Q' Bob measures, the more key rate Alice and Bob can share.

Under ideal conditions, i.e. the second intensity modulator (IM_2) has perfect extinction ratio, the yield Q' should be equal to the dark count of the SPD. However, the experimental results show that the yield Q' is larger than the dark count rate of the SPD, especially at short transmission distance. To offer an intuitive impression, we define the count ratio C_m as the count at time slot i to the count at time slot $m \neq i, j$ for the output packets from Alice. Q' can be evaluated by the mean value of C_m. The sources contributing to relatively large Q' mainly include the limited extinction ratio of IM_2, the dark count, after pulses and time jitter of the SPD. Therefore, Bob's SPD (without interferometer) is employed to directly measure the outputs of Alice. Four kinds of typical outputs with $i = 1$ (**12**, **13**, **14**, and **15**) are shown in figure 2, the time window of TDC is not set for this measurement. The worst case corresponds to the outputs of $j = i + 2$. Taking **13** output of Alice for example, the count ratio C_2 is only 280.

Conclusion

In summary, we developed a security proof for the Chau15 protocol with one-way post-processing, which facilitates the secret key generation in real-life situation. We also illustrate the superiority of the Chau15 protocol over the BB84 protocol for a certain depolarizing channel. In our experiment, the qubit-like qudits are prepared by manipulating time-bin of photon and measured by a variable delay interferometer. Our demonstration exhibits the fine feasibility and high error-rate tolerance of the novel Chau15 protocol and sheds light on QKD experiments with high-dimensionality.

Acknowledgments

ORCID iDs

Zhen-Qiang Yin ⓘ https://orcid.org/0000-0002-3486-3934

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (New York: IEEE) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[4] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[5] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[6] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[7] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503
[8] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504
[9] Peng C-Z, Zhang J, Yang D, Gao W-B, Ma H-X, Yin H, Zeng H-P, Yang T, Wang X-B and Pan J-W 2007 *Phys. Rev. Lett.* **98** 010505
[10] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 *Proc.IEEE ISIT* (Piscataway, NJ: IEEE) p 2094
[11] Yuan Z L, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **90** 011118
[12] Frolich B, Dynes J F, Lucamarini M, Sharpe A W, Yuan Z and Shields A J 2013 *Nature* **501** 69
[13] Chau H F 2015 *Phys. Rev. A* **92** 062324
[14] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[15] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[16] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475
[17] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[18] Liu Y *et al* 2013 *Phys. Rev. Lett.* **111** 130502
[19] Ferreira da Silva T, Vitoreti D, Xavier G B, do Amaral G C, Temporão G P and von der Weid J P 2013 *Phys. Rev. A* **88** 052303
[20] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H-K 2014 *Phys. Rev. Lett.* **112** 190503
[21] Wang C, Song X-T, Yin Z-Q, Wang S, Chen W, Zhang C-M, Guo G-C and Han Z-F 2015 *Phys. Rev. Lett.* **115** 160502
[22] Guan J-Y, Cao Z, Liu Y, Shen-Tu G-L, Pelc J S, Fejer M M, Peng C-Z, Ma X, Zhang Q and Pan J-W 2015 *Phys. Rev. Lett.* **114** 180502
[23] Takesue H, Sasaki T, Tamaki K and Koashi M 2015 *Nat. Photon.* **9** 827
[24] Wang S, Yin Z-Q, Chen W, He D-Y, Song X-T, Li H-W, Zhang L-J, Zhou Z, Guo G-C and Han Z-F 2015 *Nat. Photon.* **9** 832
[25] Li Y-H *et al* 2016 *Phys. Rev. A* **93** 030302
[26] Fuchs C A, Schack R and Scudo P F 2004 *Phys. Rev. A* **69** 062305
[27] Lo H-K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133
[28] He D-Y, Wang S, Chen W, Yin Z-Q, Qian Y-J, Zhou Z, Guo G-C and Han Z-F 2017 *Appl. Phys. Lett.* **110** 111104
[29] Sasaki T, Tamaki K and Koashi M 2016 arXiv:1604.04460