Security of differential quadrature phase shift quantum key distribution

Shun Kawakami, Toshihiko Sasaki and Masato Koashi
Photon Science Center, Graduate School of Engineering,
The University of Tokyo, 2-11-16 Yayoi, Bunkyo-ku, Tokyo 113-8656, Japan

The differential phase shift (DPS) protocol is one of the simplest quantum key distribution protocols for implementation. Despite its practical advantage, current security proofs for the DPS protocol lead to much lower key generation rates compared to the BB84 protocol. We prove the security of a variant of the DPS protocol, called differential quadrature phase shift (DQPS) protocol. In addition to the fact that the DQPS protocol can be implemented with essentially the same hardware as the BB84 protocol with phase encoding (PE-BB84), our results show that the key generation rate of the DQPS protocol is eight thirds as high as that of the PE-BB84 protocol in the asymptotic key-size limit, and that the advantage still holds when the effect of finite-sized key is taken into account.

Introduction: From a practical viewpoint, it is desired that a quantum key distribution (QKD) protocol is implemented with a conventional laser as its light source, and with simple hardware for encoding, decoding and detection. The simplicity is desired not only for a lower cost and a higher clock rate, but also because complicated systems and procedures tend to impose severe restrictions on the model of the sender's and the receiver's apparatus, and to suffer from inefficiency in short-time communications due to a large overhead involved in statistical estimations. The differential-phase-shift (DPS) protocol, which uses two relative phases $\{0, \pi\}$ between every neighboring pair of pulses belonging to a long train of pulses, is one of the simplest QKD implementations suited for communication over optical fibers. In the DPS protocol, the sender only needs a phase modulator for encoding, while the receiver only needs a passive Mach-Zehnder interferometer with two detectors. Its feasibility was already demonstrated in an experiment with a high clock rate [1]. Although its security was proved, so far the key generation rate is much lower than the decoy-BB84 protocol [2]. A new approach to improve the key rate was also proposed [3] and demonstrated [4–7] recently, but it requires a variable delay in the receiver's apparatus to measure relative phases between pulses at different intervals.

In this work, we seek after the benefit of the DPS-type QKD in a different direction. We prove the security of the differential quadrature phase shift (DQPS) protocol [8], which uses four relative phases $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ between neighboring pulses belonging to a long pulse train. The setup of the DQPS protocol is essentially the same as the BB84 protocol with phase-encoding (PE-BB84 protocol) [9, 10], which uses four relative phases between two neighboring pulses. We show that the key generation rate of the DQPS protocol is 8/3 as high as the rate of the PE-BB84 protocol in the asymptotic limit of infinite key size [11]. We further show that the advantage of the DQPS protocol over the PE-BB84 protocol still holds considering the finite key effect, despite the fact that the security proof is not as straightforward as the BB84 protocol. Our technique for the security proof is unique in the following sense. Although it is expected that we may prove the security in a similar vein to BB84 protocol with weak laser pulses, namely, by using the tagging idea [12], its application to the DQPS protocol is not straightforward. This is because there are chains of coherence among successive pulses, which prohibits us from defining the total photon number in neighboring two pulses. We use an alternative approach to define the photon number indirectly, which enables us to reduce the proof into the one for the BB84 protocol. This is in sharp contrast with the fact that the security proof of the original DPS protocol was quite complicated and resulted in a low key generation rate.

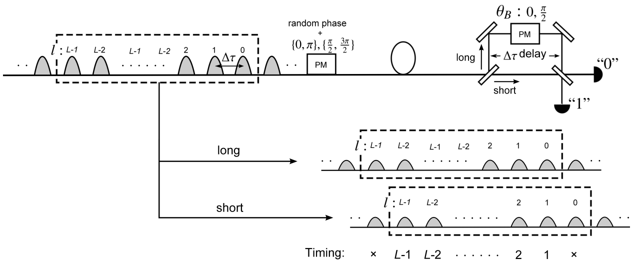
random phase
+
$\{0, \pi\}, \{\frac{\pi}{2}, \frac{3\pi}{2}\}$
PM
$\theta_B : 0, \frac{\pi}{2}$
PM
long
$\Delta\tau$ delay
short
"0"
"1"
l : L-1 L-2 L-1 L-2 2 1 0
$\Delta\tau$
long
short
l : L-1 L-2 L-1 L-2 2 1 0
l : L-1 L-2 2 1 0
Timing: × L-1 L-2 · · · · · · 2 1 ×

FIG. 1. Setup for the L-pulse DQPS protocol. The protocol regards a train of L pulses as a block, and the working basis is randomly chosen for each block. At Alice's site, pulses are modulated with phase $\{0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\}$ according to her random bits and basis choice. The randomization of the overall optical phase is also done for each block of L pulses. At Bob's site, each pulse train is fed to a delayed Mach-Zehnder interferometer with phase shift 0 or $\frac{\pi}{2}$ according to his basis choice. Valid timings of detection are labeled by integers $1, 2, .., L-1$, according to the index of the pulse from the short arm of the interferometer. Detection from interference between pulses from different blocks is regarded as invalid and ignored.

DQPS protocol: Here we introduce a DQPS protocol (See Fig. 1) which is slightly modified from the one [8] proposed by Inoue and Iwai. The protocol uses two bases, data basis for generating the final key and check basis for monitoring the leak of information.

1. Alice selects a bit $c \in \{0, 1\}$ with probability p_0 and p_1, which correspond to the choice of the data basis and the check basis, respectively. Bob also selects $d \in \{0, 1\}$ with probability p_0 and p_1.
2. Alice generates L random bits $a_l \in \{0, 1\}$ $(0, 1, .., L-1)$,

and prepares L optical pulses (system S) in the state

$$\bigotimes_{l=0}^{L-1} |e^{i\theta_l(a_l,c)}\sqrt{\mu}\rangle_{S,l}\,, \quad \theta_l(a_l,c) := a_l\pi + \frac{\pi}{2}lc, \tag{1}$$

where $|\sqrt{\mu}\rangle_{S,l}$ represents coherent state $e^{-\mu/2}\sum_k \frac{\mu^{k/2}}{\sqrt{k!}}|k\rangle_{S,l}$ of the l-th pulse mode. Alice randomizes the overall optical phase of the L-pulse train, and sends it to Bob.
3. If $d = 0$, Bob sets the amount of phase shift $\theta_B = 0$. If $d = 1$, he sets $\theta_B = \frac{\pi}{2}$.
4. If there is no detection of photons in the valid timings, Bob sets $j = 0$. If the detections have only occurred at a single valid timing, the variable j is set to the index of the timing. If there are detections at multiple timings, the smallest (earliest) index of them is assigned to j. If $j \neq 0$, Bob determines his raw key bit $b \in \{0,1\}$ depending on which detector has reported detection at the j-th timing. If both detectors have reported at the j-th timing, a random bit is assigned to b. Bob announces j through the public channel.
5. If $j \neq 0$, Alice determines her raw key bit as $a = a_{j-1} \oplus a_j$.
6. Alice and Bob repeat the above procedures $n_{\rm rep}$ times. They publicly disclose c and d for each of the $n_{\rm rep}$ rounds.
7-1. Alice and Bob define sifted keys $\boldsymbol{\kappa}_{A1}$ and $\boldsymbol{\kappa}_{B1}$, respectively, by concatenating their determined bits with $j \neq 0$ and $c = d = 1$. They publicly disclose $\boldsymbol{\kappa}_{A1}$ and $\boldsymbol{\kappa}_{B1}$.
7-2. Alice and Bob define sifted keys $\boldsymbol{\kappa}_{A0}$ and $\boldsymbol{\kappa}_{B0}$ by concatenating their determined bits with $j \neq 0$ and $c = d = 0$.
8. Bob corrects the errors in his sifted key $\boldsymbol{\kappa}_{B0}$ to make it coincide with Alice's key $\boldsymbol{\kappa}_{A0}$. Alice and Bob conduct privacy amplification to obtain the final keys.

Outline of security proof: In our proof, the tagging idea, which was proposed by Gottesman *et al.* [12], is used with a modification. Let us discuss the difference between the original tagging idea and ours. In the security proof of the PE-BB84 protocol, if a pair of pulses emitted from Alice contains more than a single photon, that signal is considered to be "tagged" and totally insecure. This is useful in the sense that as for untagged incidents, we can apply the proof for single-photon BB84 protocol, which is well established. Intuitively, we might want to use the same idea for the security proof of the DQPS protocol because a key bit is generated from a pair of pulses like in the PE-BB84 protocol. However, this turns out to be difficult. In the DQPS protocol, Alice generates a key bit $a = a_{j-1} \oplus a_j$ after Bob's announcement of detection timing j. If we are to define tagged incidents as the state in which Alice's $(j-1)$-th and j-th pulses contain more than a single photon like in the PE-BB84 protocol, these two pulses must be modulated with a common random phase shift. But such a modulation would disturb the relative phase between Alice's $(j-2)$-th and $(j-1)$-th as well as j-th and $(j+1)$-th pulse, undermining what is intended in the DQPS protocol.

An alternative way we took is to set the tagging rule through an equivalent entanglement-based version of the protocol. In the virtual version of the protocol, Alice prepares L auxiliary qubits (system A) and L optical pulses (system S) in state

$$|\Psi(c)\rangle_{AS} := \bigotimes_{l=0}^{L-1} |\psi(c)\rangle_{AS,l} \tag{2}$$

depending on her basis choice (c=0,1), where

$$|\psi(c)\rangle_{AS,l} := \frac{1}{\sqrt{2}}(|+\rangle_{A,l}|e^{i\frac{\pi}{2}lc}\sqrt{\mu}\rangle_{S,l} + |-\rangle_{A,l}|-e^{i\frac{\pi}{2}lc}\sqrt{\mu}\rangle_{S,l}). \tag{3}$$

It is easily seen that ${}_{A,l}\langle\pm|\psi(c)\rangle_{AS,l} = |\pm e^{i\frac{\pi}{2}lc}\sqrt{\mu}\rangle / \sqrt{2}$, which means that the state conditioned on the measurement result on $\{|+\rangle_{A,l}, |-\rangle_{A,l}\}$ basis is identical to the actual one defined in Eq.(1). To express Alice's key extraction process $(a_{j-1} \oplus a_j)$, we consider a CNOT gate on the $(j-1)$-th qubit as a target and the j-th qubit as a control, followed by $\{|+\rangle_{A,l}, |-\rangle_{A,l}\}$ basis measurement on the j-th qubit. An important property of $|\psi(c)\rangle_{AS,l}$ is that ${}_{A,l}\langle 0|\psi(c)\rangle_{AS,l}$ and ${}_{A,l}\langle 1|\psi(c)\rangle_{AS,l}$ are expressed as the superposition of odd- and even-photon number state, respectively. This suggests that we may, in principle, extract information on the photon number in each of the pulses through measurement on the remaining $(L-1)$ qubits. Let $\{z_l\}$ $(l \neq j)$ be the result of $\{|0\rangle_{A,l}, |1\rangle_{A,l}\}$ basis measurement on Alice's qubit system. We set the tagging rule as follows:

$$\sum_{l \neq j} z_l = m : \text{untagged}, \quad \sum_{l \neq j} z_l < m : \text{tagged}, \tag{4}$$

where m is the total photon number contained in the L-pulse block, which is well-defined thanks to the random phase shift on the whole pulse train. When the result is "untagged", the state of system S is projected to the subspace where the l-th pulse $(l \neq j-1, j)$ has no more than a single photon as well as $(j-1)$-th and j-th pulses (in total) have no more than a single photon. Roughly speaking, this situation is quite similar to untagged events in the PE-BB84 protocol. As a rigorous proof, we can prove that for untagged incidents, the errors in the check basis is regarded as a result of unbiased sampling, which means that the amount of privacy amplification is determined from the observed error rate in the same way as the BB84 protocol [11].

To obtain the secure key rate in the asymptotic limit ($n_{\rm rep} \to \infty$), we assume that the following observed parameters are fixed: $Q := |\boldsymbol{\kappa}_{A0}|/n_{\rm rep}p_0^2$, $E_0 := {\rm wt}(\boldsymbol{\kappa}_{B0} - \boldsymbol{\kappa}_{A0})/n_{\rm rep}p_0^2$, $E_1 := {\rm wt}(\boldsymbol{\kappa}_{B1} - \boldsymbol{\kappa}_{A1})/n_{\rm rep}p_1^2$, where $|\boldsymbol{\kappa}|$ represents the length of a bit sequence $\boldsymbol{\kappa}$, the minus sign is a bit-by-bit modulo-2 subtraction, and ${\rm wt}(\boldsymbol{\kappa})$ represents the weight, the number of 1's, of a bit sequence $\boldsymbol{\kappa}$. The asymptotic key rate per pulse is given by

$$R_L^{\rm (asy)} = \frac{p_0^2}{L}\Big((Q - r_{\rm tag})(1 - h\big(\frac{E_1}{Q - r_{\rm tag}}\big)) - Qfh(E_0/Q)\Big) \tag{5}$$

where $f > 1$ represents the inefficiency of error correction and $r_{\rm tag} = 1 - \sum_{m=0}^{\lceil L/2 \rceil} e^{-\mu L}\mu^m {}_{L+1-m}C_m$. Note that for $L = 2$, $r_{\rm tag}$ represents the probability that Alice emits more than a single photon in a pair of pulses, which is the ratio of tagged incidents in the PE-BB84. Although we have so far assumed that each pulse is in a coherent state, the proof can be easily extended to cover a general light source through a proper definition of $r_{\rm tag}$. It is also possible to determine $r_{\rm tag}$ through a simple off-line calibration setup like in the BB84 protocol.

Finite key analysis: For finite key analysis, let $n_0(\sim n_{\rm rep}p_0^2)$ be the number of rounds at which Alice and Bob have chosen $c = d = 0$ (regardless of the detection). In the framework of composable security definition [15], the protocol is $\epsilon :=$

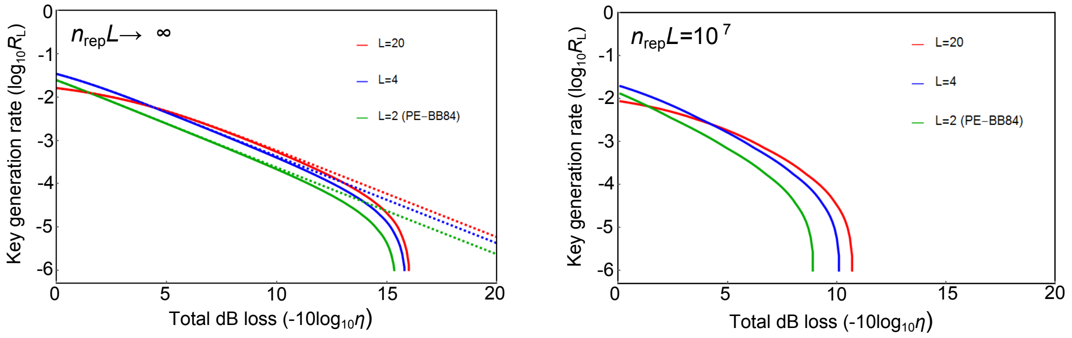

FIG. 2. Secure key rate per pulse R_L ($L = 2, 4, 20$) in the asymptotic limit (left) and for a finite total pulse number $n_{\rm rep}L = 10^7$ (right) as a function of the overall channel transmission η. Note that $L = 2$ corresponds to the PE-BB84 protocol and the other values to the DQPS protocol. Dotted lines represent the key rates assuming no dark count. We see a clear advantage of the DQPS protocol.

$\sqrt{2}\sqrt{\epsilon_1+\epsilon_3}+\epsilon_2+\epsilon_4$ secure [14] if the key rate is set to

$$R_L^{(\rm fin)} = \Bigg(\Big(|\boldsymbol{\kappa}_{A0}| - n_0(r_{\rm tag}+\delta)\Big)\Big(1 - h\Big(\frac{m_d(m_s)}{|\boldsymbol{\kappa}_{A0}| - n_0(r_{\rm tag}+\delta)}\Big)\Big) - |\boldsymbol{\kappa}_{A0}| f h(E_0/Q) - s_3 - s_4\Bigg)\frac{1}{n_{\rm rep}L} \quad (6)$$

where $m_d(m_s)$ is a function of observed error number $m_s :=$ wt$(\boldsymbol{\kappa}_{B1}-\boldsymbol{\kappa}_{A1})$ satisfying Pr(wt$(\boldsymbol{\kappa}_{B0,\rm untag}-\boldsymbol{\kappa}_{A0,\rm untag}) \geq m_d(m_s)) \leq \epsilon_1$. Here, $\boldsymbol{\kappa}_{A0,\rm untag}$ and $\boldsymbol{\kappa}_{B0,\rm untag}$ are the concatenations of all the untagged bits in $\boldsymbol{\kappa}_{A0}$ and $\boldsymbol{\kappa}_{B0}$, respectively. Furthermore, δ, s_3 and s_4 satisfy Pr$(|\boldsymbol{\kappa}_{A0,\rm untag}| \leq |\boldsymbol{\kappa}_{A0}| - n_0(r_{\rm tag}+\delta)) \leq \epsilon_2$, $2^{-s_3} \leq \epsilon_3$ and $2^{-s_4} \leq \epsilon_4$, respectively.

Numerical examples : In Fig. 2, we show results of numerical calculation of the key rates per pulse, $R_L^{(\rm asy)}$ and $R_L^{(\rm fin)}$, as a function of overall transmission η (including detector efficiency) for $L = 2$(PE-BB84), 4 and 20. We assumed a dark count probability of $p_{\rm dark} = 0.5\times10^{-5}$ per pulse per detector and a loss-independent bit error rate of 3%. We also assumed $Q = |\boldsymbol{\kappa}_{A0}|/n_0 = 1 - e^{-(L-1)\mu\eta} + 2p_{\rm dark}$, reflecting the fact that there are $(L-1)$ valid timings per block of pulses. The error correction efficiency was set to $f = 1.1$. For the asymptotic case, we have also shown the key rates when the dark counts are negligible and the error rate is fixed to be 3% (the dotted lines). For the asymptotic case, we see that R_L for different values of L are all proportional to η^2 in the limit of small η, but its coefficient increases as L gets larger. In the region of small η, we found that $R_{20}/R_2 \sim 8/3$. For the zero-error case, we have analytically found that $R_{L\to\infty}/R_2 \to 8/3$ for $\eta \to 0$. For the finite-key case, we chose the security parameter $\epsilon = 10^{-10}$, and the total pulse number $n_{\rm rep}L = 10^7$. We see that the advantage of the DQPS protocol ($L = 4, 20$) over the PE-BB84 protocol ($L = 2$) still holds even when the effect of finite-sized key is taken into account.

Summary: We proved the security of a DQPS protocol, which is a variant of the DPS protocol. By tailoring the definition of tagging in the entanglement-based version of the protocol, the security proof of the DQPS protocol is reduced to that of the BB84 protocol. In the asymptotic limit of infinite pulses, the key rate of the DQPS protocol with a large block size L is 8/3 as large as the one of the PE-BB84 protocol. Furthermore, we showed that the advantage still holds in a finite-key regime despite the fact that the security proof of DQPS protocol is not as straightforward as the BB84 protocol.

[1] H. Takesue *et al.*, Nat. Photonics **1**, 343 (2007).
[2] K. Tamaki, M. Koashi, and G. Kato, arXiv:1208.1995 (2012).
[3] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).
[4] J.-Y. Guan *et al.*, Phys. Rev. Lett. **114**, 180502 (2015).
[5] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nat. Photonics **9**, 827 (2015).
[6] Y.-H. Li *et al.*, arXiv:1505.08142 (2015).
[7] S. Wang *et al.*, Nat. Photonics **9**, 832 (2015).
[8] K. Inoue and Y. Iwai, Phys. Rev. A **79**, 022319 (2009).
[9] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE Press, New York, 1984), Vol. 175.
[10] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
[11] S. Kawakami, T. Sasaki, and K. Masato, arXiv:1512.08129 (2015).
[12] D. Gottesman, H.-K. Lo, J. Preskill, and N. Lütkenhaus, Quant. Info. Compu. **5**, 325 (2004).
[13] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[14] M. Hayashi and T. Tsurumaru, New Journal of Physics **14**, 93014 (2012-09-01T00:00:00).
[15] J. Muller-Quade and R. Renner, New Journal of Physics **11**, 085006 (2009).