# Adaptive Pulse-Position Modulation for High-Dimensional Quantum Key Distribution

Hongchao Zhou
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, MA
Email: hongchao@mit.edu

Gregory Wornell
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, MA
Email: gww@mit.edu

***Abstract*—High-dimensional quantum key distribution (QKD) systems that exploit temporal correlation among entangled photons are of growing practical interest. In such systems, the observation time is typically partitioned into frames of fixed duration, with pulse-position modulation (PPM) coding used within each frame, via which a secret key is established between the parties. Such schemes can be very inefficient in their use of photons, since only a fraction of the frames can be used. As an alternative, we describe an efficient class of schemes with adaptive frame size whose performance can converge to the fundamental limit much more quickly. We analyze and compare the performances of both fixed and adaptive PPM schemes, taking into account photon transmission and detection losses. Further numerical results reveal the significant performance gain of adaptive PPM relative to fixed PPM.**

## I. Introduction

Quantum key distribution (QKD) aims at establishing a secret key between two parities Alice and Bob with provably security and high bandwidth. Recently, there has been growing interest in QKD systems with high-dimensional quantum states, due to their increased sensitivity to eavesdropping and decreased sensitivity to noise [1], [3]. A system for high-dimensional QKD is demonstrated in Fig. 1, in which a photon-entanglement source, co-located with Alice, emits entangled photon pairs based on a Poisson process. In this system, the time is discretized, namely, the time is divided into small units called time-bins. The rate of the Poisson process for photon-pair emission is $\lambda$ photon-pairs per time-bin. Detectors at Alice or Bob can detect whether there are photons in each time-bin, but they can not determine the exact number of photons as well as their arriving times. The binary (time-pulse) sequences observed by Alice and Bob are different due to several factors including photon transmission losses, photon detection losses and dark current at detectors. Photon transmission losses happen when a photon is transmitted from the source to Bob, and we assume that each photon has a probability $\eta$ to be successfully transmitted. Photon detection losses happen at both the detectors of Alice and Bob, and each photon arriving at a detector has a probability $\eta_D$ to be detected. We call $\eta$ the transmission efficiency and $\eta_D$ the detection efficiency.

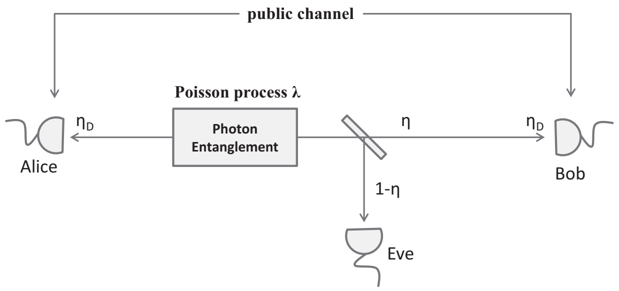

Fig. 1. A scenario for high-dimensional quantum key distribution.

In the key-distribution system, we assume that there is a third party Eve, who is trying to eavesdrop the quantum communications between Alice and Bob by placing a beam splitter on the path of photon transmission. [1] To guarantee the security of the system, we consider the worst case, i.e., all the lost photons in transmission are detected by Eve. In order to establish a secret key based on the correlated time-pulse observations, Alice and Bob communicate over a public channel. It is assumed that every message communicated between Alice and Bob over the public channel can be captured by Eve.

The problem of high-dimensional QKD is formulated as follows. Let $A \in \{0,1\}^n$ be the binary sequence observed by Alice. $A$ indicates whether there are photons detected by Alice in each time-bin. If $A_i = 1$, it means that there are at least one photons detected by Alice in the $i$th time-bin, and we call this time-bin a photon-bin; otherwise, $A_i = 0$, and we call it an empty-bin. Similarly, we let $B$ and $E$ be the binary sequences observed by Bob and Eve, respectively. The goal of QKD is to establish a secret key $S$ between Alice and Bob (based on their observations $A$ and $B$) such that $S$ is almost uniformly distributed and Eve knows little information about $S$. The difficulty of high-dimensional QKD comes from the sparsity of $A$ and $B$, hence traditional techniques such as Slepian-Wolf coding [6] cannot be directly applied for efficiently generating

This work was supported in part by AFOSR under Grant. No. FA9550-11-1-0183, and by the DARPA InPho program under Contract No. HR0011-10-C-0159.

[1] Eve may also perform nondemolition measurement on incoming photons. This activity, causing quantum collapse, can be observed by Alice and Bob in principle, e.g., by using Franson interferometer [1]. However, it is beyond the scope of the current paper.

978-1-4799-0446-4/13/$31.00 ©2013 IEEE

a secret key.

Pulse-position modulation (PPM) is a common technique that converts the binary time-pulse sequences into large-alphabet sequences of fixed alphabet size; hence it enables us to transfer the high-dimensional key-distribution problem into a studied problem named large-alphabet secret key distribution [7], for which near-optimal key-distribution schemes exist. Although simple PPM has been proposed [4], it is not efficient for preserving useful information. In this paper, we introduce a more efficient scheme, called adaptive PPM, which makes good use of the information discarded by the simple PPM. Compared to simple PPM, the performance of adaptive PPM can converge to the theoretical limit much more quickly. In addition, in contract to previous study on simple PPM, we analyze and evaluate the performances of both the schemes based on a more realistic model, i.e, taking into account photon transmission losses, detection losses and multi-pair events. Numerical results reveal the significant performance gain of adaptive PPM relative to simple PPM.

## II. Preliminary

Given a system described in the introduction, we define the key rate of a protocol as the expected number of secret key bits generated per time-bin. The maximal key rate of a key-distribution protocol was studied in [5]. Specifically, given a time-bin, we let $a = 1$ denote the event that Alice has non-zero photon detections in the time-bin; otherwise, $a = 0$. Similarly, $b$ indicates whether Bob has photon detections in the time-bin, and $e$ indicates whether Eve has photon detections in the time-bin. Let $r^*$ be the maximal key rate, according to Theorem 2 and Theorem 3 in [5] as well as the fact that $b$ and $e$ are independent, we get $r^* = I[a; b]$, where $I[a; b]$ is the mutual information between $a$ and $b$.

Given the photon-emission rate $\lambda$, transmission efficiency $\eta$ and detection efficiency $\eta_D$, the joint probability distribution of $a, b, e$, i.e., $P(a, b, e)$, can be uniquely determined. For the sake of simplicity, we use $p_{abe}$ to denote $P(a, b, e)$ and use $p_{ab}$ to denote $P(a, b)$. For instance,

$$p_{11} = \sum_{w \geq 1} P_{\text{emit}}(w)(1 - (1 - \eta_D)^w)(1 - (1 - \eta\eta_D)^w),$$

where $P_{\text{emit}}(w) = \frac{e^{-\lambda}\lambda^w}{w!}$ is the probability of emitting $w$ pairs in a time-bin. The details of calculating all $p_{ab}$ and $p_{abe}$ are omitted.

It is known that near-optimal protocols exist for large-alphabet secret key distribution [7]. Specifically, let $X^n \in \mathcal{X}^n, Y^n \in \mathcal{X}^n$ be two memoryless sequences observed by Alice and Bob respectively, and let $Z^n \in \mathcal{Z}^n$ be a memoryless sequence observed by Eve. According to Theorem 3 in [5], the lower bound on the maximal key rate is

$$\max(I[X; Y] - I[X; Z], I[X; Y] - I[Y; Z]).$$

In order to fairly evaluate and compare the performances of PPM schemes, we assume that large-alphabet secret-key-distribution protocols achieving this theoretical lower bound exist.

## III. PPM for Photon Transmission Losses

In this section, we consider the ideal case that the difference between $A$ and $B$ is purely caused by photon transmission losses, i.e., the detectors at Alice and Bob can detect all the incoming photons correctly and successfully. In this case, PPM schemes result in a common sequence between Alice and Bob, and no further error correction is required.

### A. Simple PPM

Simple PPM has been proposed to eliminate the effect of photon transmission losses in high-dimensional QKD [4]. In simple PPM, all the time-bins are divided into frames, each consists of $k$ time-bins. Given a frame, we let $N_A$ denote the number of photon-bins observed by Alice and $N_B$ denote the number of photon-bins observed by Bob. Only frames with $N_A = N_B = 1$ are used for key distribution, and we call them active frames. Note that if we only consider photon transmission losses, then given an active frame, the position of the photon-bin observed by Alice is the same as that observed by Bob in that frame. So based on the positions of photon-bins in active frames, Alice and Bob can get a common sequence of alphabet size $k$, where $k$ is the frame length.

The probability for a frame being active is $P(N_A = 1, N_B = 1) = \binom{k}{1} p_{11} p_{00}^{k-1}$, where $p_{ab}$ is the joint probability distribution of $a$ and $b$ observed Alice and Bob in a time-bin. In each active frame, there is a single photon-bin, and its position is uniformly distributed. So based on each active frame, Alice and Bob can share $\log_2 k$ common bits. However, they are not perfectly secure: It is possible that Alice, Bob and Eve all have photon detections in the same time-bin, when there are multiple photon-pairs emitted at the same time. In this case, Eve also knows the position of the photon-bin, which has been observed by Alice and Bob, so the common bits generated by this active frame is completely insecure. It is easy to calculate the probability that an active frame is secure, which is equal to

$$P(e = 0 | a = 1, b = 1) = e^{-\lambda(1-\eta)}.$$

In the simple PPM scheme, an optimal frame length $k$ can be selected to maximize the key rate. In this case, the key rate of the simple PPM scheme can be written as

$$r_s(\lambda, \eta) = \max_{k \geq 2} e^{-\lambda(1-\eta)} p_{11} p_{00}^{k-1} \log_2 k.$$

### B. Adaptive PPM

Simple PPM is not efficient for key distribution, since a big fraction of frames with useful information are discarded (only frames with $N_A = 1$ and $N_B = 1$ are used). In this subsection, we introduce a more efficient PPM scheme, called adaptive PPM, which uses all the frames with $N_A, N_B \geq 1$. The following procedure shows how to efficiently generate secret bits from a frame with $N_A \geq 1, N_B \geq 1$.

1) Alice randomly divide the frame into $N_A$ groups ($N_A$ is the number of photon-bins in the frame) such that each group includes exactly one photon-bin, then she sends this group information to Bob. Note that the time-bins

in the same group is not necessary to be adjacent. A way of determining the groups is described as follows: Let $i_1, i_2, ..., i_{N_A}$ be the photon-bins detected by Alice, and let $G_1, G_2, ..., G_{N_A}$ be the groups, i.e., the sets of bins without overlapping. At the beginning, Alice sets $G_j = \{i_j\}$ with $1 \leq j \leq N_A$, i.e., each group selects a photon-bin. After this step, each group randomly select one unassigned bin to add iteratively until all the bins have been assigned.

2) Bob replies the indices of the groups that he has photon detections back to Alice. Assume the groups $G_{j_1}, G_{j_2}, ..., G_{j_{N_B}}$ contain photon-bins detected by Bob, then those groups can be used to generate a secret key. For these groups, each includes exactly one photon-bin detected by Alice and exactly one photon-bin detected by Bob, at the same position. We call these groups as active groups.

According to our model, the $N_A$ photon-bins detected by Alice are uniformly distributed in the frame, and the $N_B$ photon-bins detected by Bob are uniformly distributed in these $N_A$ photon-bins. Based on this observation, we get the following result.

**Lemma 1.** *Let $G$ be an active group in the adaptive PPM scheme, if Eve does not have any photon detections in this group, then the position of the photon-bin observed by both Alice and Bob is uniformly distributed in $G$.*

Given a frame of length $k$, the number of photon-bins observed by Alice and the number of photon-bins observed by Bob have the following distribution,

$$P(N_A, N_B) = \binom{k}{N_A - N_B \quad N_B} p_{11}^{N_B} p_{10}^{N_A - N_B} p_{00}^{k - N_A}.$$

The size of each group is about $\frac{k}{N_A}$. From each group Alice and Bob can extract about $\log_2 \frac{k}{N_A}$ common bits. So the total number of common bits generated from this frame is

$$l(N_A, N_B) \simeq N_B \log_2 \frac{k}{N_A}.$$

However, as we discussed above, not all the groups are secure for generating secret bits; only the groups that Eve does not have any photon detections are secure. Following the same argument for the simple PPM scheme, we conclude that the probability for each active group being secure is $P(e = 0 | a = 1, b = 1) = e^{-\lambda(1-\eta)}$.

If we consider all the possible frames with $N_A, N_B \geq 1$, then we get the key rate of the adaptive PPM scheme,

$$r_a(\lambda, \eta) = \frac{1}{k} \sum_{N_A, N_B \geq 1} P(N_A, N_B) e^{-\lambda(1-\eta)} N_B \log_2 \frac{k}{N_A}. \tag{1}$$

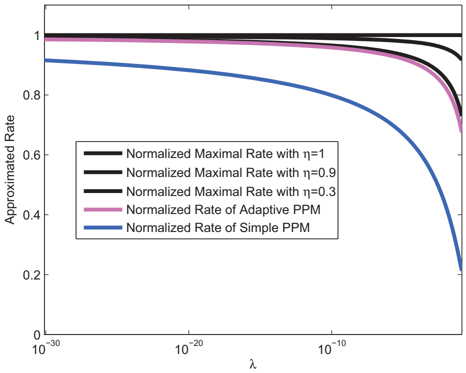

Fig. 2. The approximated normalized rates of the PPM schemes when $\eta_D = 1$, where $o(\lambda)$ terms are omitted.

### C. Analytical Approximations

Here, we compare the maximal key rate $r^*(\lambda, \eta)$, the key rate of the simple PPM scheme $r_s(\lambda, \eta)$, and the key rate of the adaptive PPM scheme $r_a(\lambda, \eta)$ when the photon density is low, i.e, $\lambda \ll 1$. In this case, the rates can be written as

$$r^* = \eta\lambda \log_2 \frac{1}{\lambda} + ((1-\eta)\log_2(1-\eta) + \log_2(e)\eta)\lambda + o(\lambda),$$

$$r_s = \eta\lambda \log_2 \frac{1}{\lambda} - \eta\lambda \log_2 \log \frac{1}{\lambda} - \eta\lambda + o(\lambda)$$

$$r_a = \eta\lambda \log_2 \frac{1}{\lambda} + o(\lambda).$$

We see that all the rates $r^*(\lambda, \eta), r_s(\lambda, \eta), r_a(\lambda, \eta)$ have the same first term. It implies that as $\lambda \to 0$, both $r_s(\lambda, \eta)$ and $r_a(\lambda, \eta)$ converge to $r^*(\lambda, \eta)$. However, the convergence rate strongly depends on the other terms, especially the second and the third terms.

We ignore the $o(\lambda)$ terms and normalize all the three rates by dividing them with $r^*(\lambda, \eta = 1)$. We see that the normalized key rates of the simple PPM scheme and the adaptive PPM scheme are independent of $\eta$, and the normalized maximal key rate is a non-increasing function of $\eta$. Fig. 2 compares the three approximated normalized rates. It shows that $r_a(\lambda, \eta)$ can quickly converge to $r^*(\lambda, \eta)$, while the convergence rate of $r_s(\lambda, \eta)$ is extremely slow.

## IV. PPM with Photon Detection Losses

In this section, we consider a general case that both photon transmission losses and detection losses exist. In this case, the sequences yielded by the PPM schemes are different for Alice and Bob. Hence, we divide the problem of high-dimensional QKD into two separate tasks: pulse-position modulation and large-alphabet secret key distribution.

### A. Simple PPM

In this subsection, we study the key rate of the simple PPM scheme when $\eta_D < 1$. Given a frame of length $k$, we let $N_A$, $N_B$ and $N_E$ denote the numbers of photon-bins observed by Alice, Bob and Eve, respectively. The probability for a frame being active is

$$P(N_A = 1, N_B = 1) = \binom{k}{1} p_{11} p_{00}^{k-1} + \binom{k}{1 \quad 1} p_{10} p_{01} p_{00}^{k-2}.$$

The key question is that, if $a, b, e$ has a joint distribution $p_{abe}$, what is the expected number of secret key bits generated from an active frame of length $k$, denoted by $\rho_{\text{active}}(k)$? Based on $\rho_{\text{active}}(k)$, we can get the key rate of the simple PPM scheme

$$r_s(\lambda, \eta, \eta_D) = \max_k P(N_A = 1, N_B = 1) \frac{\rho_{\text{active}}(k)}{k}. \qquad (2)$$

According to our assumption that optimal large-alphabet key-distribution schemes exist, we can write $\rho_{\text{active}}(k)$ as

$$\begin{aligned}&\rho_{\text{active}}(k)\\ =&\max(H(A|E, N_A = N_B = 1) - H(A|B, N_A = N_B = 1),\\ &H(B|E, N_A = N_B = 1) - H(B|A, N_A = N_B = 1)). \quad (3)\end{aligned}$$

Given an active frame, where $N_A = N_B = 1$, we can write $A$ and $B$ as integers in $\{0, 1, ..., k-1\}$. The probability that $A \neq B$ is

$$\delta = \frac{\binom{k}{2} p_{10} p_{01} p_{00}^{k-2}}{\binom{k}{1} p_{11} p_{00}^{k-1} + \binom{k}{1\quad 1} p_{10} p_{01} p_{00}^{k-2}}.$$

Since photon-bins are uniformly distributed in each frame, given a frame,

$$\begin{aligned}&H(A|B, N_A = N_B = 1) = H(B|A, N_A = N_B = 1)\\ =&(1-\delta)\log_2 \frac{1}{1-\delta} + \delta \log_2 \frac{k-1}{\delta}.\end{aligned}$$

Here, we focus on the calculation of $H(A|E, N_A = 1, N_B = 1)$ for a frame of length $k$. First, we compute $\alpha(N_E) = P(N_E, N_A = 1, N_B = 1)$ based on

$$\begin{aligned}&P(N_E = w, N_A = 1, N_B = 1)\\ =&\binom{k}{1\quad w-1} p_{111}^1 p_{001}^{w-1} p_{000}^{k-w} + \binom{k}{1\quad w} p_{110}^1 p_{001}^{w} p_{000}^{k-w-1}\\ &+ \binom{k}{1\quad 1\quad w-2} p_{101} p_{011} p_{001}^{w-2} p_{000}^{k-w}\\ &+ \binom{k}{1\quad 1\quad w-1} p_{100} p_{011} p_{001}^{w-1} p_{000}^{k-w-1}\\ &+ \binom{k}{1\quad 1\quad w-1} p_{101} p_{010} p_{001}^{w-1} p_{000}^{k-w-1}\\ &+ \binom{k}{1\quad 1\quad w} p_{100} p_{010} p_{001}^{w} p_{000}^{k-w-2}.\end{aligned}$$

If $E_i = 1$ for all $i$ with $A_i = 1$, then we denote $A \subseteq E$. Similarly as above, we get

$$\begin{aligned}&P(A \subseteq E, N_E = w, N_A = 1, N_B = 1)\\ =&\binom{k}{1\quad w-1} p_{111}^1 p_{001}^{w-1} p_{000}^{k-w}\\ &+ \binom{k}{1\quad 1\quad w-2} p_{101} p_{011} p_{001}^{w-2} p_{000}^{k-w}\\ &+ \binom{k}{1\quad 1\quad w-1} p_{101} p_{010} p_{001}^{w-1} p_{000}^{k-w-1}.\end{aligned}$$

For simplicity, we denote $P(A \subseteq E | N_E, N_A = 1, N_B = 1)$ as $\beta(N_E)$.

Due to the symmetry of time-bin positions, when $A \subseteq E$, the position of the photon-bin in $A$ is uniformly distributed in $\{i | E_i = 1\}$. As a result,

$$\begin{aligned}&H(A|E, N_A = 1, N_B = 1) = \sum_{N_E} P(N_E | N_A = 1, N_B = 1)\\ &[\beta(N_E) \log_2 \frac{N_E}{\beta(N_E)} + (1 - \beta(N_E)) \log_2 \frac{k - N_E}{1 - \beta(N_E)}].\end{aligned}$$

Based on the same method, we can also compute $H(B|E, N_A = 1, N_B = 1)$. Finally, we can get the key rate $r_s(\lambda, \eta, \eta_D)$ of the simple PPM scheme based on (2) and (3).

### B. Adaptive PPM

When $\eta_D = 1$, the adaptive PPM scheme described in Section III-B divides a frame into groups such that each group includes at most one photon-bin detected by Alice and at most one photon-bin detected by Bob. However, this property does not always hold when $\eta_D < 1$. In order to make the adaptive PPM scheme working for the general case, our idea is to continue to divide each group into sub-groups randomly, such that each subgroup includes at most one photon-bin detected by Alice and at most one photon-bin detected by Bob.

1) Let $N_A$ be the number of photon-bins observed by Alice in the frame. Alice randomly divides the frame into $N_A$ groups such that each group includes exactly one photon-bin, then she sends this group information to Bob. The size of each group is about $\frac{k}{N_A}$.
2) For a group, if Bob has observed $M_B$ photon-bins in the group. He randomly divides the group into $M_B$ subgroups such that each subgroup includes exactly one photon-bin observed by him, then he sends the subgroup information to Alice.
3) Alice determines those subgroups in which Alice has photon detections (the number of photon-bins in the subgroup is exactly one), and replies the indices of these subgroups back to Bob. After this process, Alice and Bob can determine the subgroups with exactly one photon-bin observed by Alice and exactly one photon-bin observed by Bob, which are used for key distribution.

Given a frame of length $k$, the distribution of $N_A$ is given by $P(N_A) = \binom{k}{N_A} p_1^{N_A} p_0^{k-N_A}$. Let $h(k')$ be the expected number of secret bits generated from a group of size $k'$, then the expected number of secret bits generated per frame is

$$\sum_{N_A=1}^{k} P(N_A)[U_A \cdot h(\lceil \frac{k}{N_A} \rceil) + (N_A - U_A) \cdot h(\lfloor \frac{k}{N_A} \rfloor)],$$

where $U_A = \text{remainder}(k, N_A)$.

Let $M_B$ be the number of photon-bins observed by Bob in a group of size $k'$, then $P(M_B)$ is

$$\frac{\binom{k'}{1\quad M_B-1} p_{11}^1 p_{01}^{M_B-1} p_{00}^{k-M_B} + \binom{k'}{1\quad M_B} p_{10}^1 p_{01}^{M_B} p_{00}^{k-M_B-1}}{\binom{k'}{1} p_1 p_0^{k-1}}.$$

In this case, we get $h(k')$, which is equal to

$$\sum_{M_B=1}^{k'} P(M_B)[\frac{U_B}{M_B} \rho_{\text{active}}(\lceil \frac{k'}{M_B} \rceil) + \frac{M_B - U_B}{M_B} \rho_{\text{active}}(\lfloor \frac{k'}{M_B} \rfloor)],$$

where $U_B = \text{remainder}(k', M_B)$, and $\rho_{\text{active}}(k')$ is the expected number of secret bits generated from an active subgroup of size $k'$. It can be proved that $\rho_{\text{active}}(k')$ can be calculated based on formula (3).

Finally, we get the key rate $r_a(\lambda, \eta, \eta_D)$ of the adaptive PPM scheme, which is equal to

$$r_a = \frac{1}{k} \sum_{N_A=1}^{k} P(N_A)[U_A \cdot h(\lceil \frac{k}{N_A} \rceil) + (N_A - U_A) \cdot h(\lfloor \frac{k}{N_A} \rfloor)].$$

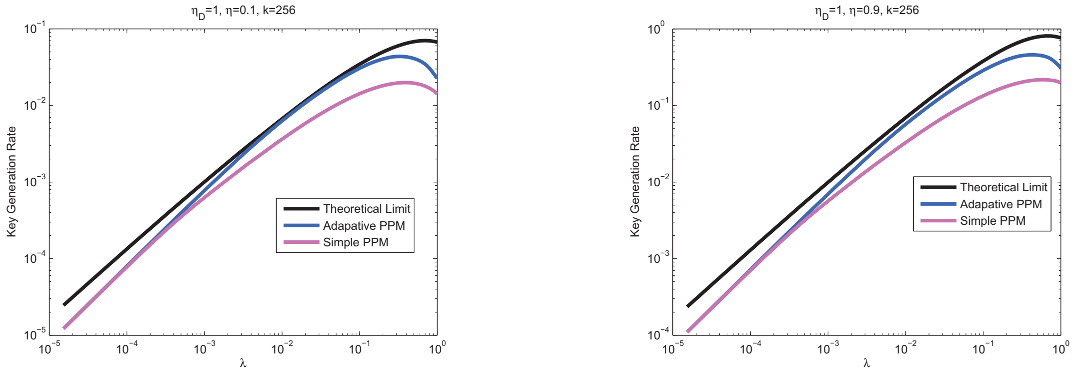

Fig. 3. The performance of the simple PPM scheme and the adaptive PPM scheme when $\eta_D = 1$ and $k = 256$.

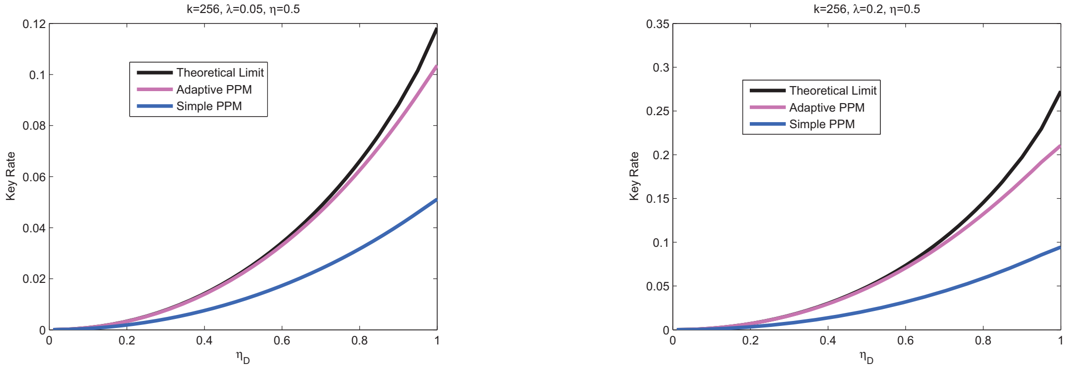

Fig. 4. The effect of $\eta_D$ to the performances of the PPM schemes.

## V. Numerical Results

In high-dimensional QKD, the frame length in a PPM scheme is usually limited by the coherence time of quantum states. It guarantees that the system cannot be attacked, since the randomness in the secret key only comes from the Heisenberg uncertainty principle [1]. In this section, given a maximal frame length, we compare the performance of the simple PPM scheme and the adaptive PPM scheme numerically.

Fig. 3 compares the key rates of the simple PPM scheme and the adaptive PPM scheme when $\eta_D = 1$ and $k = 256$. For the simple PPM scheme, $k = 256$ is the maximal frame length instead of the actual frame length selected. We see that when the photon density (emission rate) $\lambda$ is very small ($\lambda \ll \frac{1}{k}$), the adaptive PPM scheme has almost the same performance as the simple PPM scheme, since the number of frames is dominated by the frames with $N_A \leq 1, N_B \leq 1$ when $k$ is fixed and $\lambda \ll \frac{1}{k}$. When $\frac{1}{k} < \lambda < 0.1$, the performance of the adaptive PPM scheme is close to the theoretical upper bound. It is the region of practical interests. When $\lambda$ is not small, saying $\lambda > 0.1$, there is a certain gap between the key rate of the adaptive PPM scheme and the theoretical limit. But the performance gain of the adaptive PPM scheme compared to the simple PPM scheme is still significant.

Fig. 4 studies the effect of $\eta_D$ to the performances of the PPM schemes under two different groups of parameters. It is interesting to see that as $\eta_D$ decreases, the key rate of the adaptive PPM scheme converges to the theoretical limit. The intuition behind this phenomena is that the imperfectness of detectors at Alice and Bob makes it harder for Eve to predict Alice or Bob's observations. In contract to photon detection losses, where photons are lost at detectors, dark current has been observed in real quantum systems, and it causes independent photon detections at Alice or Bob even when there are no incoming photons. With further study, we found that both photon detection losses and dark current in systems do not hurt the performances of PPM schemes (relative to the theoretical maximal rate).

## References

[1] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," *Phys. Rev. Lett.* vol. 98, 060503 (2007).

[2] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, "Generation of hyperentangled photon pairs," *Phys. Rev. Lett.* vol. 95, 260501 (2005).

[3] N. J. Cerf, M. Bourennance, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems", *Phys. Rev. Lett.*, vol. 88, 127902 (2002).

[4] Y. Kochman and G. Wornell, " On high-efficiency optical communication and key distribution," in *Proceedings of Information Theory and Applications Worshop (ITA)*, 2012.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Info. Theory*, vol. 39, pp. 733–742, 1993.

[6] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources", *IEEE Trans. Info. Theory*, vol. 19, pp. 471–480, 1973.

[7] H. Zhou, L. Wang and G. Wornell, "Layered schemes for large-alphabet secret key distribution," in *Proceedings of Information Theory and Applications Worshop (ITA)*, 2013.