Fast QKD Using Array of Dead-Time Impaired Detectors

Shuangfeng Jiang, Majid Safari

Institute for Digital Communications, School of Engineering, The University of Edinburgh

Abstract *Detector dead time is a major limitation on the achievable key rate of QKD systems. We propose a dead-time compensated BB84 scheme using detector arrays and demonstrate that remarkable gains in sifted bit rate proportional to the size of array can be achieved. ©2023 The Author(s)*

Introduction

Quantum key distribution (QKD) is unconditionally secure in theory, but its security needs to be ensured under practical limitations[1]. In discrete-variable (DV) QKD protocols, practical photon counters such as single-photon avalanche diodes (SPADs)[2] are adopted as detectors. SPADs have precise time resolution, allowing for potential QKD transmission rates beyond GHz range. However, after each photon detection, SPADs should be quenched resulting in a finite dead time, τ, during which the detector is unable to respond to new incident photons[3]. With typical dead time in the range of tens of nanosecond, this causes a major limitation on secret key rates of DV-QKD systems.

There are limited investigations on the impact of detector dead time on QKD. For existing DV-QKD systems, to avoid dead-time issues, the transmission rate are commonly adjusted so that the received photon rate is less than $1/\tau$, limiting the maximum generation rate of sifted bits to less than $1/2\tau$[4]. Note that the sifted bits are formed by those encoded states where Alice and Bob select the same measurement basis, so theoretically the sifted bit rate (SBR) increases as the transmission rate increases[5].

Compensating for the detector dead time is crucial to go beyond the sift rate limit of $1/2\tau$[4],[6]. However, in such sub-dead-time transmission regime, a modified sifting scheme is required to avoid security issues caused by the possibility of closely spaced alternating photon detection events in the same basis. This leads to a potential security loophole for BB84 protocol, unless only one qubit is sifted during any sequence of alternating detection events, and this would significantly limit SBR[7]. To compensate for the dead time effect, in this paper, we propose the use of SPAD arrays that output the superposition of photon counts of their individual elements replacing single SPADs in the conventional BB84 scheme.

The SPAD array has already been utilized in quantum imaging and microscopy applications[8]–[10], owing to its fast response to single photons. Considering varying channel conditions, the SPAD array has been used in classical free-space optical (FSO) communication receivers[3] to produce adaptive sensitivity and its performance has been optimised against dead time[11],[12]. Moreover, the use of SPAD arrays is reported to develop large field-of-view QKD systems while limiting the collected background noise through post-processing[13].

To the best of our knowledge, the use of detector arrays for effective compensation of dead time effect in QKD systems has not been proposed before. Focusing on the BB84 protocol, we introduce a high-speed detection and sifting model using detector arrays instead of single-element detectors. We model the qubit sifting operation for the proposed QKD system and derive the probability of sifting analytically when the background noise is negligible, showing an excellent agreement with simulation results. We show that SBR significantly increases as detector array size grows.

BB84 QKD with Linked Array Detectors

In this paper, we focus on the polarization-encoded[14] BB84 protocol. The quantum bits (qubits) are encoded in two linear polarization bases[15]: rectilinear (0° and 90°) or diagonal (45° and -45°). On each transmission period or clock cycle, a single polarization encoded photon is sent to Bob via the quantum channel, which can be based on fibre or FSO. The total path gain γ is defined as the probability that an Alice's transmitted photon is collected by Bob's receiver. As Bob chooses the measurement bases randomly, 50% of the bits are compatible with Alice's, which contribute to the sifted key[16].

Unlike typical BB84 implementation[6] with single SPADs detecting photons at different polarizations, we consider an array of single-photon detectors per polarization. Note that the mentioned dead-time induced security loophole[7] happens regardless of using single or multiple elements at

the detector. For example, for single-element detectors, photon arrivals at an active detector (e.g., rectilinear polarisation $0°$) when the other detector in the same basis (i.e., rectilinear polarisation $90°$) is still in the quenching process would lead to alternating detection for the two detectors if the dead time is longer than interval between the two photon arrivals. This means that Eve can possibly extract all the information from such alternating detection sequence if she knows the first detector fired at the start of the sequence. Hence, inspired by the 'actively disabling' scheme proposed in[4],[17], we introduce our modified detection scheme for BB84 with array detectors where we link the corresponding elements of detector arrays of the two polarizations at the same basis such that a photon detection in an element of one detector array would also trigger a dead time in the linked element of the other detector array of the same basis, leading to both linked elements become inactive simultaneously. Therefore, after each photon detection the number of active elements of the two arrays remains the same.

Statistical Model of QKD with Detector Arrays

In order to analyze the performance of the proposed BB84 QKD system with detector arrays, we develop a Markov chain model to describe transition among the states of the linked array detectors in each basis. In this model, the states of the individual linked pairs of detector elements indicate whether they are already active now or the number of clock periods it takes to turn active. Here we define the quantity $K = \tau\rho_{\mathrm{TX}}$ which is the number of clock periods per dead time, and it is assumed to be an integer, where ρ_{TX} is the photon transmission rate. The number of elements per detector array is denoted by M. Note that the linked detector elements from the two arrays have equivalent states, so a single state can be used to represent the behavior of each linked pair. Thus, we define an M-dimensional Markov model to describes M linked pairs from the two arrays. Each detector element can take $K+1$ possible states representing the number of clock periods (0 to K) it takes to become active. In effect, the Markov model will be M-dimensional with $K+1$ states across each dimension, e.g., see Fig. 1 for 3-element detector arrays with $M = 3$ linked pairs. Note that the states are represented as an M-dimensional vector, $(k_1, k_2, \cdots, k_i, \cdots, k_M)$, where k_i denotes the numbers of clock periods left until the elements of the ith linked pair become active again so $k_i = 0$ means that the linked pair is already active.

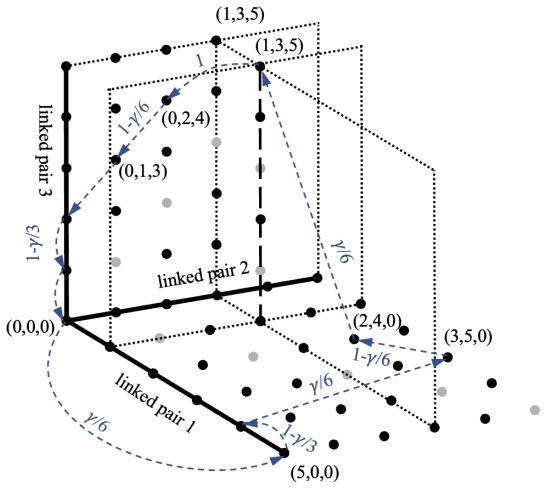

Fig. 1: Markov model of a Bob's basis with $M = 3$ and $K = 5$. Blue arrows show a transition cycle originating from state (0,0,0) with transition probabilities annotated.

Fig. 1 shows examples of transition probability between different states for the Markov model with $M = 3$ and $K = 5$. For example, the probability that a particular linked pair fires is $\gamma/6$ (i.e., $\frac{\gamma}{2M}$ for arbitrary M noting the 2 bases), leading to a possible transition from state $(0, 0, 0)$ to the state $(5, 0, 0)$. If there is no photon hitting the other two active linked pairs in the next clock cycle (which happens with probability is $1 - \gamma/3$, the basis would evolve to state $(4, 0, 0)$. Note that we cannot have states with identical non-zero entries since this would represents a simultaneous detection happened at some linked detector pairs, which are indicated by grey points in Fig. 1. However, in this work, we assume perfect single-photon sources and ignore background noise, i.e., there is maximum one signal photon arriving at the receiver per clock period. This analysis is extended to the noisy case in the extended version of this paper[18], where we also show that the proposed M-dimensional Markov model is irreducible and aperiodic with a unique stationary probability distribution.

Now, we determine the stationary probability distribution of the Markov chain model. Let $P(k_1, \cdots, k_{M-1}, k_M)$ denote the steady-state probability of the state $(k_1, \cdots, k_{M-1}, k_M)$. We also define $P_i(k_1, ..., k_i)$ as the probability of the state with i non-zero entries and $K - i$ zero entries. Note that, in this definition, the zero entries are eliminated, i.e., $P_i(k_1, ..., k_i) = P(0, ..., 0, k_1, ..., k_i)$. Due to the symmetry of the Markov model across different dimensions, any permutation of the entries will generate states with the same steady-state probability.

Lemma 1. *In the stationary probability distribution of the proposed M-dimensional Markov chain, the probability of all the states with i $(0 < i \leq M)$ nonzero entries are equal, that is*

$$P_i(k_1, \cdots, k_i) = P_i(k_1', \cdots, k_i') \triangleq P_i. \tag{1}$$

Lemma 1 is proved by writing the transition probability equations and considering the uniqueness of the solution for the linear set of transition equations as detailed in the extended version of the paper[18]. Applying this lemma, the general form of transition probability can be written for states with m non-zero entries ($1 \leq m \leq M$) as

$$P_m = \frac{\gamma}{2M} P_{m-1} + (M-m)\frac{\gamma}{2M} P_m \tag{2}$$

$$\begin{aligned} P_{m-1} &= [1 - (M-m+1)\frac{\gamma}{2M}]P_{m-1} \\ &+ (M-m+1)[1-(M-m)\frac{\gamma}{2M}]P_m, \end{aligned} \tag{3}$$

which result in the following recursive relationship

$$P_m = \frac{\frac{\gamma}{2M}}{1-(M-m)\frac{\gamma}{2M}} P_{m-1} \tag{4}$$

In addition, using lemma 1, the law of total probability of the steady-state Markov chain yields

$$P_0 + \sum_{m=1}^{M} \binom{M}{m} K(K-1)\cdots(K-m+1)P_m = 1.$$

where The term $\sum_{m=1}^{M} \binom{M}{m} K(K-1)\cdots(K-m+1)$ corresponds to the number of states with m nonzero entries in the M-dimensional Markov chain. Inserting (4) in the above equation, we get the analytical expression of P_0 as

$$\begin{aligned} P_0 =& [1 + \sum_{m=1}^{M} \binom{M}{m} [\prod_{m'=1}^{m} (K+1-m') \\ & \frac{\frac{\gamma}{2M}}{1-(M-m')\frac{\gamma}{2M}}]]^{-1}, \end{aligned} \tag{5}$$

while the expressions of $P_i, \forall 0 < i \leq M$ can be derived iteratively using (4).

SBR Performance Analysis

The QKD system can detect qubits when at least one linked pair is active, Hence SBR can be written considering probabilities $P_0, P_1, \ldots, P_{M-1}$ as

$$\begin{aligned} SBR =& \frac{1}{2}\rho_{TX}\gamma P_0 (1 + \sum_{m=1}^{M-1} \binom{M}{m} \frac{M-m}{M} \\ & (\prod_{m'=1}^{m} (K+1-m')\frac{\frac{\gamma}{2M}}{1-(M-m')\frac{\gamma}{2M}})). \end{aligned} \tag{6}$$

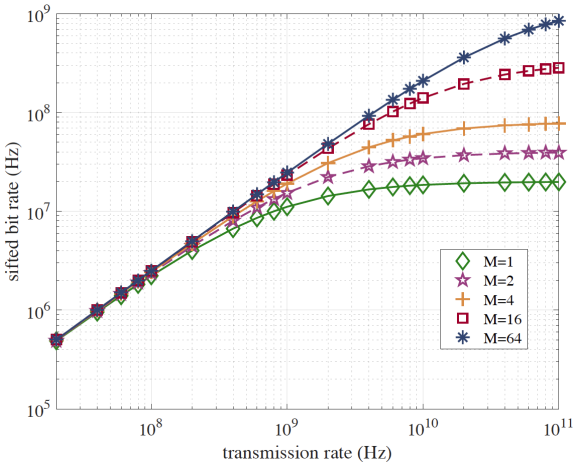

Fig. 2: The sifted bit rate versus qubit transmission rate for $\gamma = -13$ dB. Lines and markers of same colors show the corresponding analytical and simulation results respectively.

where (4) is used to write P_i's as P_0 and P_0 is given by (5). The term $\rho_{TX}\gamma$ denotes the photon arrival rate at the receiver, while the factor $\frac{1}{2}$ represents the compatibility probability of bases between Alice and Bob, and $\frac{M-m}{M}$ represents the probability that the incoming photon hits an active element of the partly active detector arrays. Inserting (5) into (6) and tending the transmission rate to infinity, it can be shown after some manipulation that SBR is asymptotically bounded as

$$\lim_{\rho_{TX}\to\infty} SBR = \frac{M}{\tau}. \tag{7}$$

This shows that a remarkable gain proportional to the size of array (M) is achievable in the SBR of the QKD system when using detector arrays instead of single-element detectors.

Fig. 2 depicts the SBR results of the optical QKD system with different M assuming $\gamma = -13$ dB. The figure shows an excellent agreement between the analytical (lines) and the simulation (markers) results. Compared with the green curve with the single SPAD, we can observe considerable gains in terms of SBR when ρ_{TX} is high enough. For example, using 4×4 detector arrays (i.e., $M = 16$) can provide a gain factor of approximately $SBR(16)/SBR(1) \approx 15$ at 100 GHz photon transmission rate. In general, the curves with different values of M approximately confirm the theoretical upper bound in equation (7).

Conclusions

A high-speed BB84 receiver based on detector arrays are proposed showing significant gains in SBR at high photon transmission rates almost proportional to the size of arrays. This is a remarkable finding showing potential significant gains for the achievable secret key rate.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[2] D. Chitnis and S. Collins, "A spad-based photon detecting system for optical communications", *Journal of Lightwave Technology*, vol. 32, no. 10, pp. 2028–2034, 2014.

[3] S. Huang and M. Safari, "Hybrid spad/pd receiver for reliable free-space optical communication", *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1364–1373, 2020.

[4] D. J. Rogers, J. C. Bienfang, A. Nakassis, H. Xu, and C. W. Clark, "Detector dead-time effects and paralyzability in high-speed quantum key distribution", *New Journal of Physics*, vol. 9, no. 9, p. 319, 2007.

[5] X. Tang, L. Ma, A. Mink, *et al.*, "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over mbit/s", *Optics Express*, vol. 14, no. 6, pp. 2062–2070, 2006.

[6] S. Jiang and M. Safari, "High-speed free-space qkd in the presence of spad dead time", in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, 2022, pp. 457–462.

[7] C. Kollmitzer and M. Pivk, *Applied quantum cryptography*. Springer, 2010, vol. 797.

[8] M. Zarghami, L. Gasparini, L. Parmesan, *et al.*, "A 32$\times$ 32-pixel CMOS imager for quantum optics with per-SPAD TDC, 19.48% fill-factor in a 44.64-μm pitch reaching 1-MHz observation rate", *IEEE Journal of Solid-State Circuits*, vol. 55, no. 10, pp. 2819–2830, 2020.

[9] A. Ghezzi, A. Farina, A. Bassi, *et al.*, "Multispectral compressive fluorescence lifetime imaging microscopy with a spad array detector", *Optics Letters*, vol. 46, no. 6, pp. 1353–1356, 2021.

[10] Y. Maruyama and E. Charbon, "A time-gated 128x128 cmos spad array for on-chip fluorescence detection", in *Proc. Intl. Image Sensor Workshop (IISW)*, 2011.

[11] S. Huang, S. M. Patanwala, J. Kosman, R. K. Henderson, and M. Safari, "Optimal photon counting receiver for sub-dead-time signal transmission", *Journal of Lightwave Technology*, vol. 38, no. 18, pp. 5225–5235, 2020.

[12] S. Huang, C. Chen, R. Bian, H. Haas, and M. Safari, "5 gbps optical wireless communication using commercial spad array receivers", *Optics Letters*, vol. 47, no. 9, pp. 2294–2297, 2022.

[13] A. T. Castillo and R. Donaldson, "Towards free-space quantum key distribution with a 2d single-photon sensor", in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, SPIE, vol. 11881, 2021, pp. 24–29.

[14] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution", *Physical Review A*, vol. 67, no. 2, p. 022 309, 2003.

[15] S. Jiang, W. O. Popoola, and M. Safari, "Quantum key distribution using time-gated spads over turbid underwater channels", in *CLEO: Science and Innovations*, Optical Society of America, 2021, JW1A–125.

[16] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[17] H. Xu, L. Ma, J. C. Bienfang, and X. Tang, "Influence of avalanche-photodiode dead time on the security of high-speed quantum-key distribution systems", in *Conference on Lasers and Electro-Optics*, Optica Publishing Group, 2006, JTuH3.

[18] S. Jiang and M. Safari, "High-speed quantum key distribution using dead-time compensated detector arrays", *Submitted to Optics Express*, 2023.