Conference materials
UDC 530.145
DOI: https://doi.org/10.18721/JPM.153.372

Phase-time-encoding MDI QKD tolerant to detector imperfections

I. V. Petrov [1]✉, D. D. Menskoy [1], A. S. Tayduganov [1]

[1] National University of Science and Technology MISiS, Moscow, Russia

✉ i.petrov@goqrate.com

Abstract. Measurement-device-independent quantum key distribution (MDI QKD) allows to eliminate the single-photon detector (SPD) vulnerabilities, increase the communication distance limits, and construct a multiple users key distribution network. Nevertheless, detector imperfections are able to decrease the secret key rate and maximum distance by orders of magnitude. In this work we propose a model of large SPD's dead time for the phase-time-encoding MDI QKD. We also propose a modified measurement device (Charlie) scheme with four detectors which is able to partially restore the sifted key loss caused by dead time.

Keywords: quantum cryptography, MDI QKD, single-photon detector, dead time

Funding: This research was ordered by JSCo "RZD".

Citation: Petrov I. V., Menskoy D. D., Tayduganov A. S., Phase-time-encoding MDI QKD tolerant to detector imperfections. St. Petersburg State Polytechnical University Journal. Physics and Mathematics, 15 (3.3) (2022) 365–370. DOI: https://doi.org/10.18721/JPM.153.372

Материалы конференции
УДК 530.145
DOI: https://doi.org/10.18721/JPM.153.372

Протокол КРК с НЦУ с фазово-временным кодированием, устойчивый к неидеальности детекторов

И. В. Петров [1]✉, Д. Д. Менской [1], А. С. Тайдуганов [1]

[1] Национальный исследовательский технологический университет МИСиС, Москва, Россия

✉ i.petrov@goqrate.com

Аннотация. Квантовое распределение ключа с независимым центральным узлом (КРК с НЦУ), позволяет устранить уязвимости детектора одиночных фотонов (ДОФ). Тем не менее, несовершенство детектора может снизить скорость секретного ключа и максимальное расстояние на порядки. В этой работе мы предлагаем модель большого мертвого времени ДОФ для фазово-временного кодирования КРК с НЦУ. Мы также предлагаем модифицированную схему измерительного устройства (Чарли) с четырьмя детекторами, которая способна частично восстановить потерю просеянного ключа, вызванную мертвым временем.

Ключевые слова: квантовая криптография, КРК с НЦУ, MDI QKD, однофотонный детектор, мертвое время

Финансирование: Исследовательская работа выполнена по заказу ОАО «РЖД».

Ссылка при цитировании: Петров И. В., Менской Д. Д., Тайдуганов А. С. Протокол КРК с НЦУ с фазово-временным кодированием, устойчивый к неидеальности детекторов // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2022. Т. 15. № 3.3. С. 365–370. DOI: https://doi.org/10.18721/JPM.153.372

Introduction

Similar to conventional prepare-and-measure QKD, dead time τ of a single-photon detectors (SPD) do not affect on the MDI QKD performance as long as τ is less than pulse-to-pulse time interval in a quantum channel. This condition imposes a severe limitation on the secret key rate: dead time limits the detection frequency from above by the $1/\tau$ value. Meanwhile, widely used gated-mode single-photon avalanche photodiodes (SPAD) are characterized by the large dead time $\tau \sim 0.1-10$ μs [1]. For typical pulse preparation frequency $f = 10^8$ Hz this means decrease in detection frequency by the 3 orders of magnitude ($1/\tau \sim 10^5$). This indicates the problem of practical MDI QKD with imperfect detectors, which we attempt to solve. In this work we consider the phase-time-encoding MDI QKD protocol with decoy-state technique and propose slight modifications to the measurement device, which improves the protocol performance. First, we explain how detectors' dead time affects the Bell state measurement. Second, we provide a theoretical model for the sifted key rate, which is useful for the optimal parameters search, and analyze the protocol performance.

Influence on Bell measurement output

In MDI QKD the untrusted node Charlie performs Bell measurement of the Alice-Bob joint quantum state and declares the result [2]. Events of the form $A_i \cap A_j$ are considered *successful*, where A_i and A_j denote detector's click in the corresponding time and space mode $i \in \{c_E, d_E\}$, $j \in \{c_L, d_L\}$ (c and d stand for space modes, E and L stand for time modes – see Fig. 1, *a*). As far as standard measurement scheme (see Fig. 1, *a*) contains only one SPD at each beam splitter (BS) output, the events $A_{c_E} \cap A_{c_L}$ and $A_{d_E} \cap A_{d_L}$ cannot be detected in the case, when dead time overlaps the second pulse in a time-encoded pair, i.e. $\tau \geq 1/f$. Using the theoretical formula of signal gain from [3], one can draw a simple conclusion: the loss of half of the events leads to double decrease in the gain, and hence the speed of the sifted key.

Alternative schemes:

1. We propose the *scheme with four detectors* (see Fig. 1, *b*) which contains two detectors at every BS output (*c*, *d*). As a result, one half of the previously discarded successful events can be detected, which for infinite key limit gives 25% restore of the sifted key rate in comparison with the two-detector scheme.

2. The scheme with four detectors can be upgraded in order to detect all the successful events with equal probabilities (see Fig. 1, *c*). One can send a pulse in each half of the time slots from previous schemes, provided that in each pair of detectors there is one that is gated in the first half of the time slot, while another is gated in the second half. Further we refer to this scheme as a *scheme with time-divided measurement*. Unfortunately, using passive beam splitters results in no profit in sifted key rate.

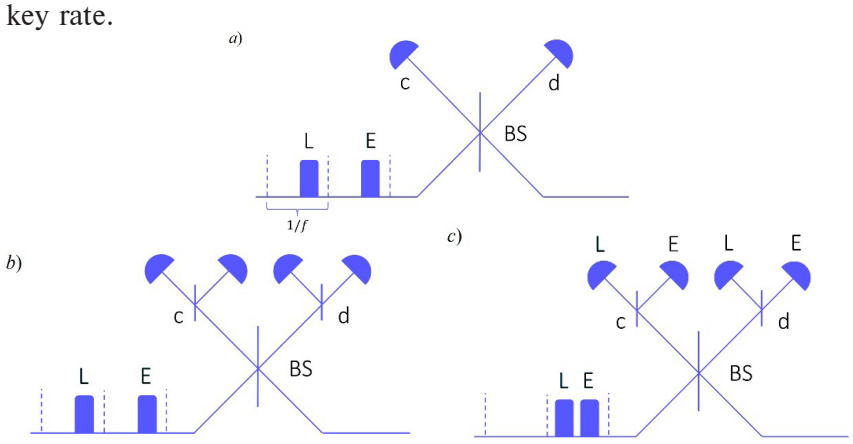

Fig. 1. Measurement schemes for phase-time-encoding MDI QKD: (*a*) – two detectors [3], (*b*) – four detectors, (*c*) – time-divided measurement. BS – beam splitter, (*c*, *d*) – output channels of BS, *E*, *L* – time slots of pulse preparation and detection gates

Sifted key rate model

The above result is valid for the sifted key rate estimation only in the case when the dead time overlaps every second pulse ($\tau \simeq 1/f$). Otherwise, the result obtained in the limit $\tau \gg 1/f$ and under conditions of synchronous dead time and infinite statistics is additionally applied [4]:

$$R_{sift}^{\tau \neq 0} = \frac{R_{sift}^{\tau=0}}{1+\tau R_{tot}} \tag{1}$$

where $R_{\text{sift}}^{\tau=0} = f p_Z^2 p_\mu^2 Q_{\mu_a \mu_b}^Z$ is sifted key rate for zero dead time (drawn out of signal gain $Q_{\mu_a \mu_b}^Z$ estimated in Z-basis for $\mu_{(a(b))}$ Alice (Bob) intensities [3]), $p_\mu = 0.5$ and $p_Z = 0.5$ are signal pulse and basis choice probabilities respectively, R_{tot} is the overall signal gain for BB84 protocol. In the case of MDI QKD, we have to estimate overall count rate when at least one detector clicks considering $\tau = 0$.

The simple estimation of Rtot that considers the two-detectors Charlie scheme, dark counts and multi-photon pulses is

$$R_{tot}^{(1)} = f\left(\Pr(n_{ph} > 0) + 2p_{dc}\right) \tag{2}$$

where

$$\Pr(n_{ph} > 0) = \left(1 - e^{-\mu_a \eta_a}\right) + \left(1 - e^{-\mu_b \eta_b}\right) - \left(1 - e^{-\mu_a \eta_a}\right)\left(1 - e^{-\mu_b \eta_b}\right) \simeq 4\mu\eta_{ch} \tag{3}$$

is a probability of nonzero-photon pulses pass through the channel, μ is mean photon number per pulse, η_{ch} is quantum channel transmittance. This prediction does not take into account Hong-Ou-Mandel interference on the beam splitter. Such a 'naïve' estimation close to the one from [4]. Note, when the decoy-state technique is used, the probability above must be summarized over all intensity pairs.

In general, for the decoy-state MDI protocol all detection events must be taken into account, and one has to sum up all click probabilities. We consider clicks from two incoming coherent states, prepared in different bases and of different intensities, and clicks due to dark counts. This estimation is referred to as $R_{tot}^{(2)}$:

$$\begin{gathered} R_{tot}^{(2)} = f \sum_{b_1, b_2, i, j, \mu_a, \mu_b} \Pr\left(n_{click} \geq 1 \,|\, \psi_{a,b}, \mu_a, \mu_b\right) \cdot p(\psi_{a,b}) \\ p(\psi_{a,b}) = p_{i,j} p_\mu p_{\text{basis}} = \frac{1}{4} p_{\mu_a} p_{\mu_b} p_{b_1} p_{b_2}, \\ \text{args}: b_1, b_2 \in \{X, Z\}; i, j \in \{0,1\}; \mu_a, \mu_b \in \{\mu, \nu, \omega\} \end{gathered} \tag{4}$$

Here every joint Alice-Bob quantum state $\psi_{a,b}$ is defined by the basis $\{p_{b_1}, p_{b_2}\}$ and intensity $\{p_{\mu_a}, p_{\mu_b}\}$ choice probabilities. General formula for $Pr(n_{click} \geq 1 \mid \psi_{a,b}, \mu_a, \mu_b)$ can be derived from a detector independent click probabilities D_i, averaged over the global phase:

$$\Pr(n_{\text{click}} \geq 1 \,|\, \psi_{a,b}, \mu_a, \mu_b) = 1 - \int_0^{2\pi} \frac{d\phi}{2\pi} \prod_i (1 - D_i) = 1 - p_{\text{no}}^{b_1 b_2} \tag{5}$$

where $i \in \{c_E, c_L, d_E, d_L\}$, $b_1, b_2 \in \{Z, X\}$. One can consider $p_{\text{no}}^{b_1 b_2}$ as a probability of '*no clicks*' on the detector. In the case of *XX* and *ZZ* basis choice (D_i^{ZZ}, D_i^{XX} are defined in [3])

$$\begin{aligned} p_{no}^{XX} &= (1 - p_{dc})^4 e^{-2\mu'}, \\ p_{no}^{ZZ} &= (1 - p_{dc})^4 e^{-\mu'}. \end{aligned} \tag{6}$$

Here $\mu' = \mu_a \eta_a + \mu_b \eta_b$.

It is left to calculate the probabilities for the cases *XZ* and *ZX* (it is worth noting that these

cases are connected through the replacing μ_a to μ_b and vice versa). One has to consider a state

$$\left|e^{i\phi_a}\sqrt{\mu_a}\right\rangle_{a_E}\left|e^{i(\phi_a+\theta_a)}\sqrt{\mu_a}\right\rangle_{a_L}\left|0\right\rangle_{b_E}\left|e^{i\phi_b}\sqrt{\mu_b}\right\rangle_{b_L} \tag{7}$$

After passing through the channel and beam splitter this state becomes

$$\begin{aligned}&\left|e^{i\phi_a}\sqrt{\frac{\eta_a\mu_a}{2}}\right\rangle_{c_E}\left|e^{i(\phi_a+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{2}}+e^{i\phi_b}\sqrt{\frac{\eta_b\mu_b}{2}}\right\rangle_{c_L}\otimes\\&\otimes\left|e^{i\phi_a}\sqrt{\frac{\eta_a\mu_a}{2}}\right\rangle_{d_E}\left|e^{i(\phi_a+\theta_a)}\sqrt{\frac{\eta_a\mu_a}{2}}-e^{i\phi_b}\sqrt{\frac{\eta_b\mu_b}{2}}\right\rangle_{d_L}\end{aligned} \tag{8}$$

In this case the detection probabilities are equal to

$$\begin{aligned}&D_{c_E}=D_{d_E}=1-(1-p_{dc})e^{-\frac{\eta_a\mu_a}{2}},\\&D_{c_L}=1-(1-p_{dc})e^{-1/2(\eta_a\mu_a+\eta_b\mu_b+2\sqrt{\eta_a\mu_a\eta_b\mu_b}\cos(\Delta_\phi+\theta_a))},\\&D_{d_L}=1-(1-p_{dc})e^{-1/2(\eta_a\mu_a+\eta_b\mu_b-2\sqrt{\eta_a\mu_a\eta_b\mu_b}\cos(\Delta_\phi+\theta_a))}.\end{aligned} \tag{9}$$

As a result, we derive that

$$p_{no}^{XZ}=(1-p_d)^4e^{-\mu_a}e^{-\mu'},\ p_{no}^{ZX}=(1-p_d)^4e^{-\mu_b}e^{-\mu'}. \tag{10}$$

Thus, we can accurately estimate $R_{sift}^{\tau\neq0}$ for a two-detector measurement scheme. To compare sifted key rate with proposed alternatives, consider $R_{sift}^{\tau=0}=r(\eta_d)$ as a function of an SPD quantum efficiency η_d.

Alternative schemes:

1. In the scheme with four detectors, when one detector in an arm of the first BS clicks, the left detector in the same arm and the second BS can be regarded together as a detector with $\eta_d/2$ efficiency. In order to predict the sifted key rate, we can use the same equations, but instead of $R_{\text{sift}}^{\tau=0}=r(\eta_d)$ we consider $R_{\text{sift}}^{\tau=0}=r(\eta_d)+r(\eta_d/2)$;

2. In the scheme with time-divided measurement one doesn't have to throw away the half of successful events in the Bell measurement, but all the detectors always have constant decrease in efficiency ($\eta_d/2$). Therefore, we consider $R_{\text{sift}}^{\tau=0}=r(\eta_d/2)$ and $R_{tot}=r'(\eta_d/2)$.

We note that $R_{sift}^{\tau\neq0}$ formulas for alternative schemes are numerically accurate only in single-photon approximation and the limit of $\tau\gg0$. Otherwise, they provide estimative results.

Simulation

In Fig. 2 we compare the computed secret key generation rate $R_{sift}^{\tau\neq0}$ for three presented detection schemes as a function of detector's dead time τ. Other model parameters are listed in Tab. 1. Four-detector scheme shows only partial restore, which is about 1.25 times of the measurement scheme with two detectors. Meanwhile, even considering double preparation frequency, time-divided scheme shows no restore of the key rate loss due to undetected successful events, as expected. Nevertheless, the dead time $\tau\leq10$ μs slows down MDI QKD by up to 3 times, regardless of the measurement scheme. One can also note the significant difference between 'naïve' sifted key rate estimation $R^{(1)}$ and accurate model $R^{(2)}$.

Table 1

Key model parameters

μ	ν	ω	p_z	p_μ	p_ν	L_{ab}, km	η_d	P_{dc}	f
0.3	μ/50	μ/100	0.5	0.5	0.25	160	10%	10^{-6}	3×10^8

Notations: {μ,ν,ω} are signal, week decoy and vacuum intensities (average number of photons per pulse), {p_Z, p_μ, p_ν} are basis and pulse intensity choice probabilities, Lab – total line length (0.2 dB/km fiber loss), η_d, p_{dc} – detector quantum efficiency and dark count probability, f – pulse repetition frequency.

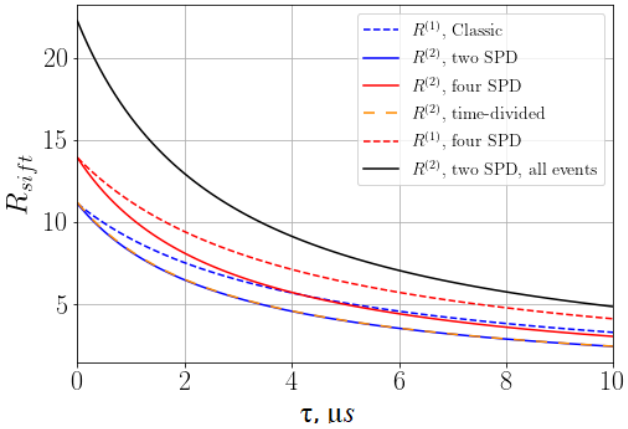

Fig. 2. Dependence of sifted key rate Rsift from dead time τ of a single photon detector (SPD). Three measurement schemes are compared (see Fig. 1). $R^{(1)}$ – 'naïve' estimation, $R^{(2)}$ – our general theoretical result

Conclusion

Dead time of a single-photon avalanche photodiode causes the dramatic decrease in the sifted key rate of a QKD setup. Phase-time-encoding MDI protocol is even more vulnerable for dead time $\tau \geq 1/f$, because it leads to the loss of a half of successful events in the Bell measurement. We proposed the theoretical model in order to predict the total number of detection events in the measurement scheme. We also proposed and compared measurement schemes with four detectors and with time-divided measurement, where the former is able to compensate for 25% of losses due to previously undetected events. This theoretical result needs further confirmation either by numerical or natural experiment. Meanwhile, the proposed sifted key model is applicable to accurate parameter optimization [5], compared to often used 'naïve' estimations of the total number of events.

Acknowledgments

This research was ordered by JSCo «RZD». The authors would also like to acknowledge Aleksander Duplinsky for thoughtful and productive discussions.

REFERENCES

1. **Hadfield R. H.,** Single-photon detectors for optical quantum information applications. Nature Photonics, 3 (12) (2009) 696–705.

2. **Lo H. K., Curty M., Qi B.,** Measurement-device-independent quantum key distribution. Physical review letters, 108 (13) (2012) 130503.

3. **Ma X., Razavi M.,** Alternative schemes for measurement-device-independent quantum key distribution. Phys. Rev. A, 86 (2012) 062319.

4. **Burenkov V., Qi B., Fortescue B., Lo H.-K.,** Security of high-speed quantum key distribution with finite detector dead time, 2010. DOI:10.48550/ARXIV.1005.0272

5. **Xu, F., Curty M., Qi B., Lo H.-K.,** Practical aspects of measurement-device-independent quantum key distribution. New Journal of Physics, 15 (11) (2013) 113007.

THE AUTHORS

PETROV Ivan V.
i.petrov@goqrate.com
ORCID: 0000-0002-5422-2886

TAYDUGANOV Andrey S.
a.tayduganov@goqrate.com

MENSKOY Daniil D.
d.meskoy@goqrate.com

Received 19.08.2022. Approved after reviewing 24.08.2022. Accepted 08.09.2022.