Conference materials
UDC 53
DOI: https://doi.org/10.18721/JPM.153.337

Posterior laser-locking technique for MDI-QKD

E. E. Mekhtiev [1, 2]✉, I. S. Gerasin [2, 3], N. V. Rudavin [3, 4],
A. V. Duplinsky [3, 4], Yu. V. Kurochkin [3]

[1] LLC "QRate", Moscow, Russia;

[2] Moscow Institute of Physics and Technology, Dolgoprudny, Russia;

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

[4] HSE University, Moscow, Russia

✉ mekhtiev@phystech.com

Abstract. We present a novel soft-ware based method to ensure independent lasers mutual coherence required for practical realization of advanced Measurement Device Independent Quantum Key Distribution (MDI-QKD) protocols. Proof of principle experiment has proved validity of the method, providing mutual coherence time while upper bound dictated by uncontrollable phase drift in optical fiber being ~ 100 μs.

Keywords: MDI-QKD, mode-pairing protocol, asynchronous protocols, mutual phase stabilization, mutual coherence

Funding: The study was commissioned by JSCo "RZD".

Citation: Mekhtiev E. E., Gerasin I. S., Rudavin N. V., Duplinsky A. V., Kurochkin Yu. V., Posterior laser-locking technique for MDI-QKD. St. Petersburg State Polytechnical University Journal. Physics and Mathematics, 15 (3.3) (2022) 194–197. DOI: https://doi.org/10.18721/JPM.153.337

Материалы конференции
УДК 53
DOI: https://doi.org/10.18721/JPM.153.337

Метод обеспечения взаимной когерентности двух независимых лазеров на этапе постобработки для реализации протоколов КРК с использованием НЦУ

Э. Э. Мехтиев [1, 2]✉, И. С. Герасин [2, 3], Н. В. Рудавин [3, 4],
А. В. Дуплинский [3, 4], Ю. В. Курочкин [3]

[1] ООО «КуРэйт», Москва, Россия;

[2] Московский физико-технический институт, Долгопрудный, Россия;

[3] Национальный исследовательский технологический университет «МИСиС», Москва, Россия;

[4] Национальный исследовательский университет «Высшая школа экономики», Москва, Россия

✉ mekhtiev@phystech.com

Аннотация. В работе описан метод обеспечения взаимной когерентности независимых лазерных источников, необходимой для практической реализации определенного класса протоколов Квантового Распределения Ключей (КРК) с использованием Недоверенного Центрального Узла (НЦУ). Экспериментальная проверка подтвердила эффективность предложенного метода, обеспечившего время взаимной когерентности ~ 10 мкс. Максимально достижимое время взаимной когерентности определяется фазовым шумом в оптическом волокне и составляет ~ 10 мкс.

Ключевые слова: КРК с НЦУ, асинхронные протоколы КРК с НЦУ, стабилизация относительно фазы, взаимная когерентность

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

Ссылка при цитировании: Мехтиев Э. Э., Герасин И. С., Рудавин Н. В. Дуплинский А. В., Курочкин Ю. В., Метод обеспечения взаимной когерентности двух независимых лазеров на этапе постобработки для реализации протоколов КРК с использованием НЦУ // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2022. Т. 15. № 3.3. С. 194–197. DOI: https://doi.org/10.18721/JPM.153.337

Introduction

Measurement device independent quantum key distribution (MDI-QKD) is a promising step towards secure quantum key distribution networks [1]. The motivation for developing device independent protocols arises from inevitable gap between theoretical description of a protocol and its real device realisation. This gap can be used by eavesdropper (Eve) to obtain additional information about secret key. The most vulnerable part of real-life QKD systems are single photon detectors, since they are exposed to the majority of quantum hacking attacks [2, 3]. MDI-QKD protocols allow Eve to control measurement device, still guaranteeing security of key distribution.

With all mentioned advantages, present experimental realizations of MDI protocols does not enjoy as high security key rate as prepare-and-measure protocols. Recently so-called asynchronous or mode-pairing MDI-QKD protocols have been proposed [4, 5] to make up for this shortcoming. The main feature of these protocols is a drastic improvement of the secure key rate over longer distances. However, Asynchronous MDI-QKD requires high degree of sender lasers mutual coherence. Usually this problem is solved via various hard-ware based laser locking techniques [6]. In this work we present easy soft-ware based approach to solve this problem. We refer to this approach as posterior laser-locking technique.

Problem statement

The mode-pairing MDI-QKD essentially is a generalization of time-bin encoding MDI-QKD. Namely, instead of two using fixed time bins to encode qbit, some pairing strategy between several time bins is applied to detection events at post-processing stage. This approach allows to achieve $O(\sqrt{\eta})$ instead of standard MDI asymptotic $O(\eta)$ for a secure key rate R, where $\eta \to +\infty$ is total channel transmittance [5].

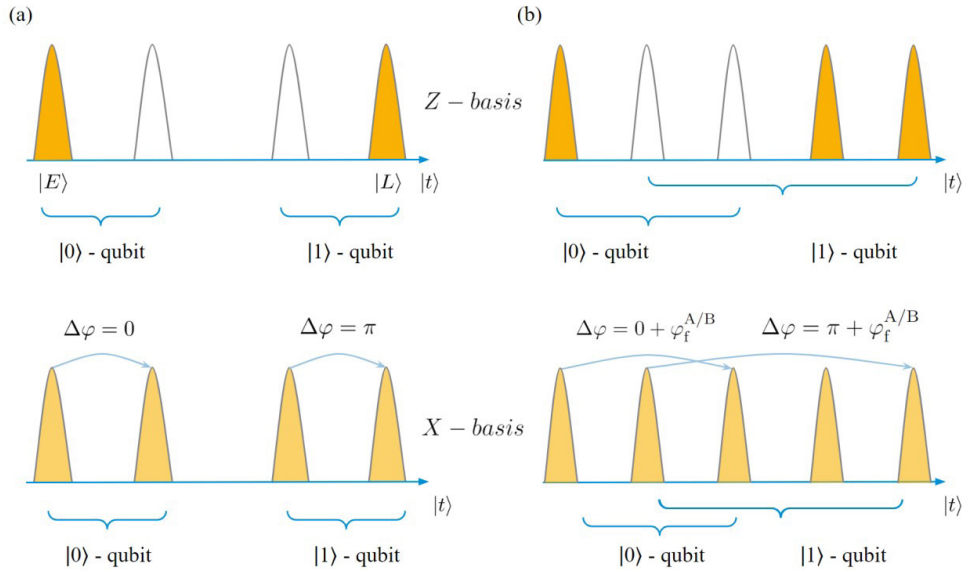

Fig. 1. MDI-QKD encoding schematics. Standard time-bin encoding (*a*). Mode-pairing encoding (*b*)

The schematic of mode-pairing encoding method is present on Fig. 1, *b*. The pairing time bin is chosen during post-processing which allow to efficiently use almost every detector "click", despite transmittance losses. However increasing the pairing time (blue-arrows) may lead to unexpected phase difference between chosen time bins induced by optical fiber $\varphi_f^{A/B}$. This phase term is totally random and may be different for sender A and B. This fact prevents senders from matching their encoding phases $\varphi \in \{0, \pi\}$ which is a must according to MDI- protocol. The next two sections describe our approach to overcome this problem.

Setup and Methods

1. Setup

Equations should be formatted in MathType (please AVOID MS Word Equation Editor). Equations are numbered consecutively beginning with (1) to the end of the paper, e.g.: We investigate interference of two independent continuous light beams. Fig. 2. represents experimental setup. Laser A is Keysight 81950A with spectral width < 100 kHz, Laser B is Keysight 81608A with spectral width < 100 kHz. Central wavelength of the two lasers adjusted so that their mean mutual beat frequency $\langle \Delta\omega_{AB} \rangle \sim 250$ MHz. Communication link is established with standard single-mode optical fibers. We use two fiber-coupled photodetectors at detection side to register lasers interference pattern. Signal photodetector PD_S is Thorlabs PDA8GS, compensating photodetector PDC_C is Thorlabs RXM40AF. Interference traces are captured by Teledyne LeCroy WaveMaster 808Zi-A oscilloscope. We investigate communication links of L = 0, 25, 50 and 75 km lengths to test robustness of a proposed method.

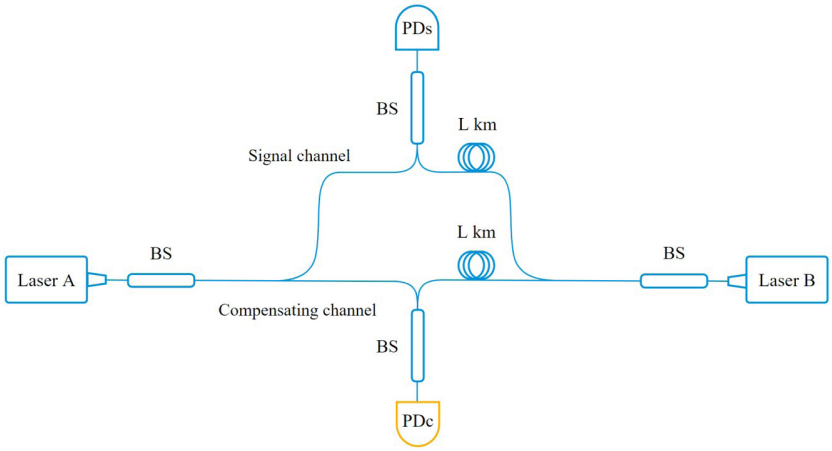

Fig. 2. Experimental setup. PD – photodetector, BS – 50:50 beamsplitter, L – optical fiber spool

2. Method

We aim to use frequency beat measured on PD_c to post-compensate phase difference on detector PDs arising from lasers wavelength difference. Intensities on PD_s andPD_c are respectively:

$$J_s(t) \sim e^{i[\Delta\varphi^0_{AB} + \Delta\varphi_{fs} + \Delta\omega_{AB}(t - t_s)\cdot t]} \quad (1)$$

$$J_c(t) \sim e^{i[\Delta\varphi^0_{AB} + \Delta\varphi_{fc} + \Delta\omega_{AB}(t - t_c)\cdot t]} \quad (2)$$

where $\Delta\varphi^0_{AB}$ is is initial phase difference between two laser sources; $\Delta\varphi_{fs}$, $\Delta\varphi_{fc}$ are random phase differences induced by optical fibers of signal and compensating channels; $\Delta\omega_{AB}(t-t_s)\cdot t$, $\Delta\omega_{AB}(t-t_c)\cdot t$ are phase differences on detectors PD_s and PD_c at time t due to lasers mutual incoherence; $|t_c - t_s|\cdot c$ path difference between signal and compensating channels. The proposed method works as follows:

1. Collect interference traces with detectors PD_s and PD_c;
2. Find $\Delta\omega_{AB}(t)$ from $J_c(t)$ with Fast Fourier Transform;
3. Subtract $\Delta\omega_{AB}(t)$ from the phase of $J_s(t)$;
4. Search to find delay $|t_c - t_s|\cdot c$ minimizing final phase error $\Delta\varphi_{err}(t)$.

Results and Discussion

Table 1 shows phase error rate of the two posteriorly-locked lasers. For detection node remote at 25 km mutual lasers coherence of ~ 100 μs is achieved with 0.15 rad certainty. We note that the upper time limit for Lasers A and B mutual coherence, imposed by random phase noise in optical fiber, ~ 100 μs [7].

Table 1

Phase error rate against communication link length

L, km	$\Delta\varphi_{err}$, $rad \cdot \mu s^{-1}$
0	0.004
25	0.015
50	0.027
75	0.059

Further improvement can be achieved with using higher sample rates on oscilloscope and greater lasers detuning. Also it should be noticed that proof-of-principle experiment does not require to send weak coherent laser pulses instead of continuous beam, since these pulses inherit the phase of continues wave from which they are "cut" with intensity modulator.

Conclusion

Altogether the degree of mutual coherence provided with new technique looks promising for effective realisation of asynchronous MDI-QKD protocols.

REFERENCES

1. **Lo H. K., Curty M., Qi B.,** Measurement-device-independent quantum key distribution. Physical review letters. 108 (13) (2012) 130503.
2. **Xu F., Ma X., Zhang Q., Lo H. K., Pan J. W.,** Secure quantum key distribution with realistic devices, Reviews of Modern Physics. 92 (2) (2020) 025002.
3. **Jain N., Stiller B., Khan I., Elser D., Marquardt C., Leuchs, G.,** Attacks on practical quantum key distribution systems (and how to prevent them), Contemporary Physics. 57 (3) (2016) 366–387.
4. **Xie Y. M., Lu Y. S., Weng C. X., Cao X. Y., Jia Z. Y., Bao Y., Chen Z. B.,** Breaking the Rate-Loss Relationship of Quantum Key Distribution with Asynchronous Two-Photon Interference, arXiv. (2021) preprint arXiv:2112.11635.
5. **Zeng P., Zhou H., Wu W., Ma X.,** Quantum key distribution surpassing the repeaterless rate-transmittance bound without global phase locking, arXiv. (2022) preprint arXiv:2201.04300.
6. **Khabarova K. Y., Kudeyarov K. S., Vishnyakova G. A., Kolachevsky N. N.,** Short-haul fibre-optic communication link with a phase noise compensation system for optical frequency signal transmission, Quantum Electronics. 47 (9) (2017) 794.
7. **Fang X. T., Zeng P., Liu H., Zou M., Wu W., Tang Y. L., Pan J. W.,** Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nature Photonics. 14 (7) (2020) 422–425.

THE AUTHORS

MEKHTIEV El E.
mekhtiev@phystech.edu
ORCID: 0000-0002-9756-7016

GERASIN Ilia S.
i.gerasin@goqrate.com
ORCID: 0000-0001-5084-7056

RUDAVIN Nikita V.
n.rudavin@goqrate.com
ORCID: 0000-0003-0264-5710

DUPLINSKY Alexander V.
a.duplinsky@goqrate.com
ORCID: 0000-0003-2222-0752

KUROCHKIN Yury V.
yk@goqrate.com
ORCID: 0000-0001-5376-6358

Received 12.08.2022. Approved after reviewing 18.08.2022. Accepted 24.08.2022.