Conference materials
UDC 535.8
DOI: https://doi.org/10.18721/JPM.163.151

# Passive optical scheme for BB84 protocol with polarization encoding on a silicon nitride platform

A.B. Sodnomay [1, 2, 3] ✉, V.F. Mayboroda [1, 3], V.V. Kovalyuk [2, 3, 4], A.D. Golikov [4], G.M. Chulkova [2, 4], G.N. Goltsman [2, 4, 5], R.A. Shakhovoy [1, 3, 5]

[1] QRate, Moscow, Russia;
[2] HSE University, Moscow, Russia;
[3] NTI Center for Quantum Communications, National University of Science and Technology MISIS, Moscow, Russia;
[4] Institute of Physics, Technology and Information Systems, Moscow State Pedagogical University, Russia;
[5] Russian Quantum Center, Skolkovo, Moscow, Russia
✉ a.sodnomay@goqrate.com

**Abstract.** Quantum key distribution is a technology that promises unconditional security for protecting data. However, despite being based on the laws of quantum physics, its practical implementation may have critical vulnerabilities. One way to address this is to passively prepare quantum states. In our work, we demonstrate a passive optical scheme for the BB84 protocol with polarization encoding. We use a finite-difference time-domain method to simulate the elements of this scheme on the silicon nitride platform. Our simulations suggest that the polarization extinction ratio will be more than 20 dB, which will allow for the generation of quantum states with a QBER (quantum bit error rate) of less than 1%.

**Keywords:** quantum key distribution, polarization encoding, integrated photonics

**Citation:** Sodnomay A.B., Mayboroda V.F., Kovalyuk V.V., Golikov A.D., Shakhovoy R.A., Chulkova G.M., Goltsman G.N., Passive optical scheme for BB84 protocol with polarization encoding on a silicon nitride platform, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 16 (3.1) (2023) 284–288. DOI: https://doi.org/10.18721/JPM.163.151



Материалы конференции
УДК 535.8
DOI: https://doi.org/10.18721/JPM.163.151

# Пассивная оптическая схема протокола BB84 с поляризационным кодированием на платформе нитрида кремния

А.Б. Содномай [1, 2, 3] ✉, В.Ф. Майборода [1, 3], В.В. Ковалюк [2, 3, 4], А.Д. Голиков [4], Г.М. Чулкова [2, 4], Г.Н. Гольцман [2, 4, 5], Р.А. Шаховой [1, 3, 5]

[1] ООО «КуРэйт», Москва, Россия;
[2] Национальный исследовательский университет «Высшая школа экономики», Москва, Россия;
[3] Национальный исследовательский технологический университет "МИСиС", Москва, Россия;
[4] Институт физики, технологии и информационных систем, Московский государственный педагогический университет, Москва, Россия;
[5] Российский Квантовый центр, Сколково, Москва, Россия
✉a.sodnomay@goqrate.com

**Abstract.** Квантовое распределение ключей – это технология, которая может обеспечить безусловную защиту данных. Однако, практическая реализация устройств, основанных

на законах квантовой физики, может иметь критические уязвимости. Одним из способов устранения уязвимостей является реализация пассивного приготовления квантовых состояний. В нашей работе мы предлагаем пассивную оптическую схему протокола BB84 с поляризационным кодированием. При помощи методов конечной разности во временной области, мы провели моделирование элементов схемы на платформе нитрид кремния. Результаты моделирования показали оценку поляризационной экстинкции более чем 20 дБ, что может обеспечить приготовление квантовых состояний с квантовым уровнем ошибок (QBER) менее чем 1%.

**Ключевые слова:** квантовое распределения ключа, поляризационное кодирование, интегральная фотоника

**Ссылка при цитировании:** Содномай А.Б., Майборода В.Ф., Ковалюк В.В., Голиков А.Д., Чулкова Г.М., Гольцман Г.Н., Шаховой Р.А. Пассивная оптическая схема протокола BB84 с поляризационным кодированием на платформе нитрид кремния // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2023. Т. 16. № 3.1. С. 284–288. DOI: https://doi.org/10.18721/JPM.163.151



## Introduction

Quantum Key Distribution (QKD) is a promising technology that takes a step towards unconditional security. The most widespread QKD protocol, the BB84-scheme, is generally implemented in two equivalents ways: polarization [1] and time-bin (phase) encoding [2]. Usually, each of these approaches uses optical phase and/or polarization modulators that allow preparing quantum states with high bitrate. However, these elements create the opportunity for eavesdropping. The other approach for preparing quantum states is a passive optical scheme [3], which requires only the light source and passive fiber or integrated photonics elements. In this work, we demonstrate our Photonics Integrated Circuits design for passive BB84 protocol with polarization encoding.

## Materials and Methods

The principle of the passive polarization encoding of BB84 consists in the following: Alice prepares weak coherent optical pulses with randomized phases and separates them in a beam splitter. One arm of the splitter rotates polarization of the optical pulse while the other arm has the optical delay line, whose time delay is agreed with the pulse repetition. Then different optical pulses combine in the polarization combiner. Finally, Alice prepares random polarization states since the phase difference between optical pulses is random.

We have designed a photonic chip on a 330 nm silicon nitride platform that includes a polarization converter to separate laser optical pulses with TE polarization and convert a portion of the light to TM polarization. The TE polarization then travels through a delay line of 58.78 mm in length, equivalent to a 400 ps delay for a 1550 nm wavelength. After that, the TM and TE polarization pulses are merged using a polarization beam combiner. Cross section of the silicon nitride wafer and the schematic representation are shown in Fig. 1.

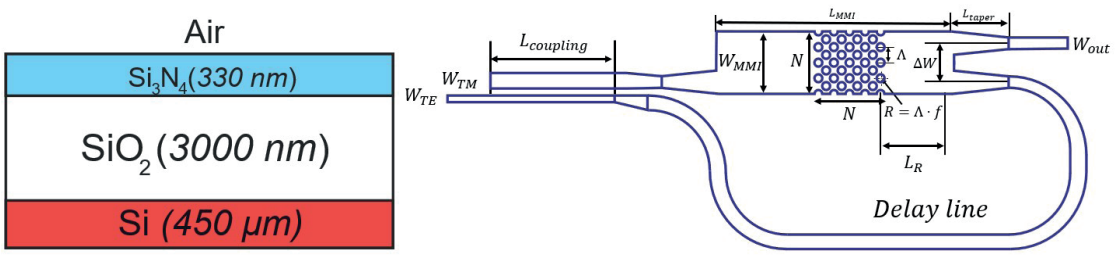


Fig. 1. Cross-section of the silicon nitride wafer (left image) and principal optical scheme (right image)

The polarization converter operates on the principle of matching the phase of TM and TE waves in different waveguides, in other words, it is necessary to fulfill the condition (1) [4]:

$$n_{eff}^{TM}\left(w_{TM}\right)=n_{eff}^{TE}\left(w_{TE}\right) \quad (1)$$

To achieve phase matching, specific dimensions have been chosen for the waveguide width of 0.78 μm for TE polarization and 1.4 μm for TM polarization, a coupling length of 84.5 μm, and a 0.21 μm gap between the two waveguides. The upper part of the waveguides is covered with air, the lower part is $SiO_2$. At the input and outputs of the polarization converter we add tapers with the length of 5 μm to conjugate with the waveguides with the width of 1 μm.

The polarization beam combiner (PBC) was constructed using a MMI coupler with a photonic crystal [5], which is etched out of silicon nitride and filled by around air. The full length of the MMI coupler ($L_{MMI}$) being 3 times the beat length of the TM wave, and the distance ($L_R$) between the photonic crystal and the common port of the MMI coupler being 1.5 times the beat length of the TE wave. To optimize the transparency for TM polarization and the reflective efficiency for TE polarization, a fill-factor ($f$) of 0.25, the number of rows and columns ($N$×$N$) is 13×13 and a photonic crystal period ($\Lambda$) of 0.5 μm have been chosen. The distance ($\Delta W$) between input and output interfaces of the PBC MMI is 4 μm. At the input and outputs of the MMI coupler we add tapers with the length of 5 μm to conjugate with the waveguides with the width of 1 μm. The detailed design of the PBC MMI is shown in Figure 2.

Table

**Parameters of MMI PBC**

| Parameter | $L_{taper}$ | $L_{MMI}$ | $L_R$ | $\Lambda$ | $W_{MMI}$ | $\Delta W$ | $f$ | $N$ |
|---|---|---|---|---|---|---|---|---|
| Value | 5 μm | 187.8 μm | 89.4 μm | 0.5 μm | 6.5 μm | 4 μm | 0.25 | 13 |

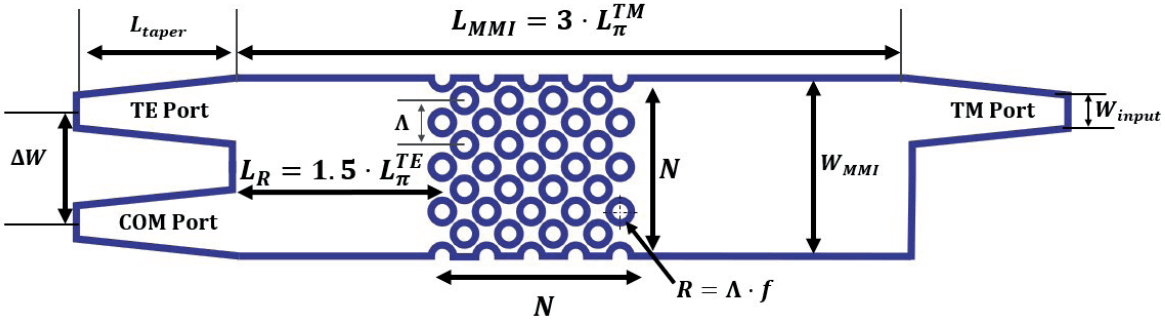


Fig. 2. PBC MMI design

## Results and Discussion

Using a finite-difference time-domain (FDTD) method, we simulated the photonics devices in our optical scheme. The polarization converter splits and transforms light at 1550 nm with levels of – 5.3 dB and – 3.4 dB for TM and TE polarization, respectively. The polarization extinction ratio (PER) was calculated as a ratio of TE and TM polarization power. Since the waveguides have a weak coupling, part of the light with TE and TM polarization can transmit into TM and TE waveguide respectively. It produces peaks in the wavelength dependence of polarization extinction ratio for TE polarization in the region of 1520 and 1580 nm, and one peak for the TM polarization at 1550 nm. For the 1550 nm, PER is 11 dB for TM-mode and 17 dB for TE-mode.

The insertion loss in the MMI region is 1.2 dB and 0.4 dB for TM and TE polarization, respectively, the polarization extinction is 15 dB for both type of polarizations. We expect additional losses in the delay line, which will equalize the polarization-dependent loss of the scheme. The simulation results of spectra are shown in Fig. 3, *d*.

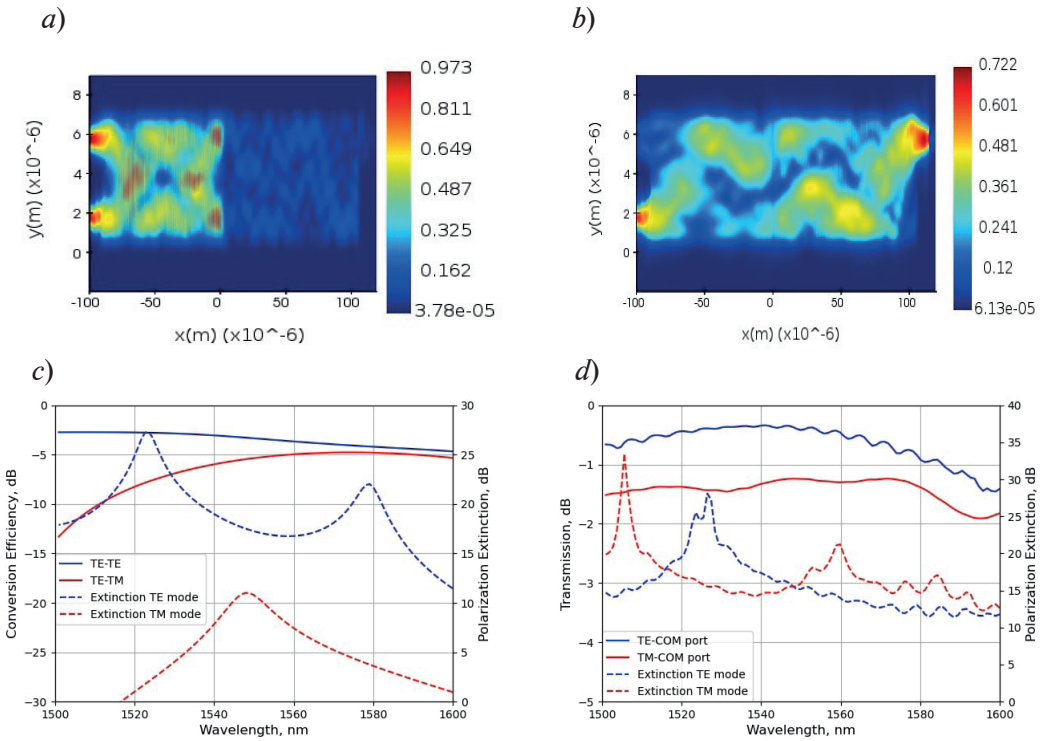


Fig. 3. Simulation results of TE-mode (*a*) and TM-mode (*b*) propagation through MMI PBS at 1550 nm wavelength, conversion efficiency and Polarization Extinction Ratio for TE and TM modes in polarization converter (*c*), transmission and PER of PBC MMI at different wavelengths (*d*)

## Conclusion

In this work we introduce the photonic chip for passive preparation of quantum states for BB84 protocol based on polarization encoding. This method enables the creation of quantum states without the use of any active components like phase or polarization modulators. As a result, it enhances the level of security against eavesdropping.

## REFERENCES

1. **Duplinskiy A., Ustimchik V., Kanapin A., Kurochkin V., Kurochkin Y.,** Low loss QKD optical scheme for fast polarization encoding. Optics express, 25 (23) (2017) 28886–28897.

2. **Paraiso T.K., Roger T., Marangon D.G., De Marco I., Sanzaro M., Woodward R.I., Shields A.J.,** A photonic integrated quantum secure communication system. Nature Photonics, 15 (11) (2021) 850–856.

3. **Curty M., Ma X., Lo H.K., Lütkenhaus N.,** Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals. Physical Review A, 82 (5) (2010) 052325.

4. **Liu L., Ding Y., Yvind K., Hvam J.M.,** Efficient and compact TE−TM polarization converter built on silicon-on-insulator platform with a simple fabrication process. Optics letters, 36 (7) (2011) 1059–1061.

5. **Xu L., Wang Y., El-Fiky E., Mao D., Kumar A., Xing Z., Plant D.V.,** Compact broadband polarization beam splitter based on multimode interference coupler with internal photonic crystal for the SOI platform. Journal of Lightwave Technology, 37(4) (2019) 1231–1240.

## THE AUTHORS

**SODNOMAY Amgalan B.**
a.sodnomay@goqrate.com

**MAYBORODA Vladimir F.**
v.mayboroda@goqrate.com

**KOVALYUK Vadim V.**
lpkgarage@yandex.ru

**GOLIKOV Alexander D.**
gad_92@inbox.ru

**CHULKOVA Galina M.**
gchulkova@hse.ru

**GOLTSMAN Grigoriy N.**
ggoltsman@hse.ru

**SHAKHOVOY Roman A.**
r.shakhovoy@goqrate.com

*Received 11.07.2023. Approved after reviewing 23.08.2023. Accepted 23.08.2023.*