Cross polarization-intensity correlations in chip-based QKD

Tianyi Xing,[1] Álvaro Navarrete,[2,3,4] Yongqiang Du,[5] Zhengeng Zhao,[5] Daniil Trefilov,[2,3,4] Xin Hua,[6] Xi Xiao,[6,7] Vadim Makarov,[8,2,9] Kejin Wei,[5,*] Marcos Curty,[2,3,4,†] and Anqi Huang[1,‡]

[1] *College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China*
[2] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[3] *School of Telecommunication Engineering, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[4] *atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*
[5] *Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning, 530004, China*
[6] *National Information Optoelectronics Innovation Center (NOEIC), Wuhan, 430074, China*
[7] *Peng Cheng Laboratory, Shenzhen, 518055, China*
[8] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[9] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*

(Dated: April 11, 2025)

Chip-based quantum key distribution (QKD) systems offer improved efficiency but may also introduce previously unrecognized security vulnerabilities. In this work, we identify and experimentally characterize cross-polarization-intensity (CPI) correlations in a real-world chip-based QKD system. Moreover, we introduce a security analysis that incorporates CPI correlations and apply it to evaluate the performance of an integrated high-speed QKD system. Our results emphasize the need for rigorous security assessments in chip-based QKD implementations.

Introduction. Quantum key distribution (QKD) [1] has become a cornerstone of secure communication technologies. Recent advancements have seen the integration of chip-based QKD systems [2], which offer increased key rates and more compact devices. However, practical implementations often diverge from idealized theoretical models, meaning that real-world systems remain susceptible to security vulnerabilities [3, 4]. In this context, the use of novel structures and materials in integrated QKD sources may further introduce previously unexplored threats.

In this work, we experimentally demonstrate the existence of cross polarization–intensity (CPI) modulation correlations in the source components of chip-based QKD systems. We further develop a security analysis that accounts for this type of correlations and apply it to evaluate the system's key rate based on the experimental data. These results offer critical insights into the practical security of integrated QKD systems and contribute to the advancement of more comprehensive and realistic security models.

Chip under test. The scheme of the source chip tested in our experiment is shown in [5] as illustrated in Fig. 1a. It comprises two pivotal elements: an intensity modulator (IM) and a polarization modulator. The IM is constructed with two multimode interferometers (MMIs), two thermal optical modulators (TOMs), and two carrier depletion modulators (CDMs). The Pol-M consists of two MMIs, four CDMs, and a two-dimensional grating coupler (2DGC). The 2DGC combines the light from two spatial modes into a single spatial mode with two mutually orthogonal polarizations. The TOM and the CDM serve as phase shifters to adjust the intensity and polarization states of the optical pulses emitted by the source chip. An electrical signal from an external source is converted into equally positive and negative voltages, which are then applied to a pair of upper and lower CDM/TOMs. An external electrical signal is split into equal positive and negative voltages and applied to a pair of upper and lower CDM/TOMs. The CDMs are driven by a radio frequency signal from an arbitrary waveform generator (AWG), while the TOMs are controlled by a direct current (DC) signal. The chip insertion loss is about 40 dB and the repetition frequency is 50 MHz. The IM is adjusted to produce signal states with a mean photon number of 0.5 during the constructive interference, and to produce decoy states with a mean photon number of 0.1.

Dependence of the pulse intensity on the polarization setting. First, we experimentally measure and characterize the dependence of the actual intensity of the emitted states on the polarization setting. The experimental setup is illustrated in Fig. 1a (Path 1). The variable optical attenuator (VOA) at the output of the encoder has an attenuation of 40 dB to ensure that the output optical energy is at the single-photon level. A superconducting nanowire single-photon detector (SNSPD) with ∼50% efficiency is used to monitor the photon count.

In the experiment, the photon count is initially recorded for 0 V at the IM's CDMs. Next, an AWG signal is applied to the first pair of Pol-M CDMs, sweeping the voltage from –3 V to 3 V in 0.05 V increments, and recording the detections at the SNSPD during 0.2 s for each voltage. The process is repeated for the decoy

* kjwei@gxu.edu.cn
† mcurty@vqcc.uvigo.es
‡ angelhuang.hn@gmail.com

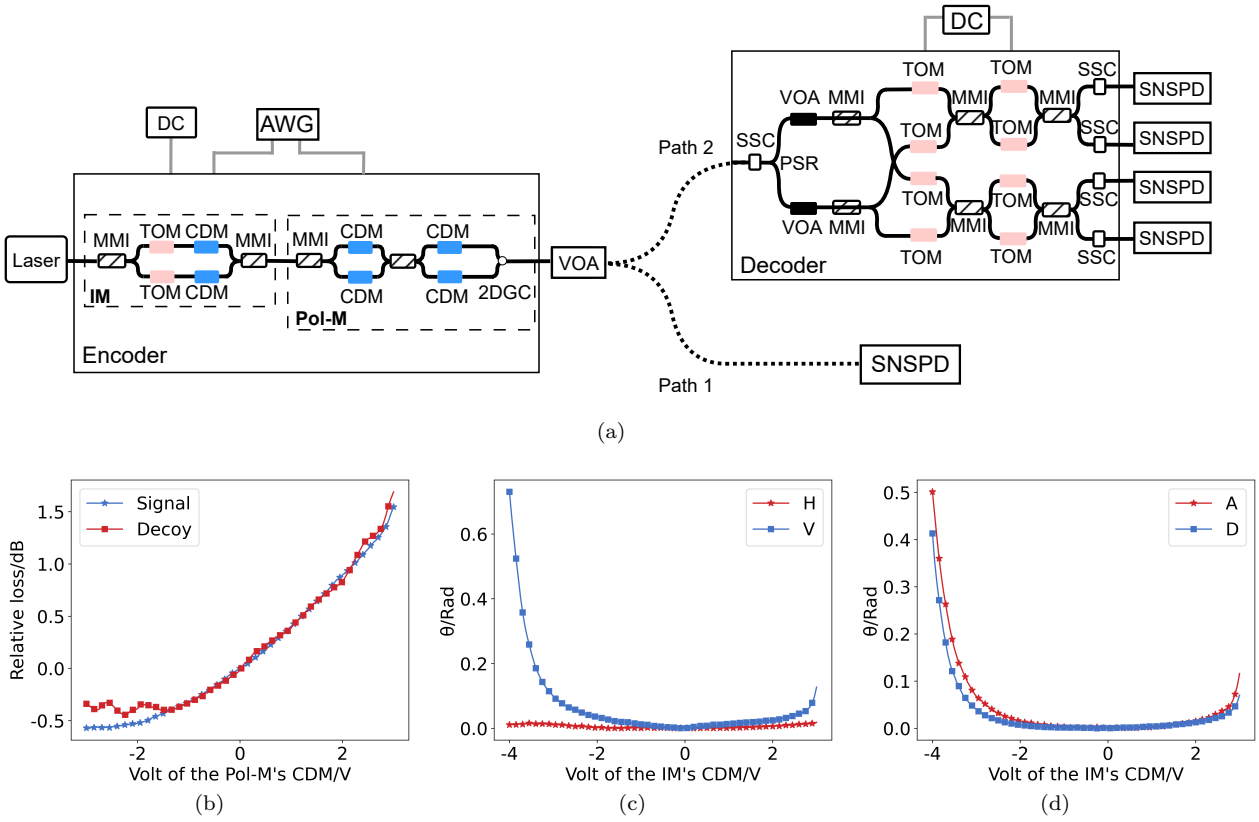

FIG. 1: **Experimental setup and results.** (a) The setup used to characterize the dependence of the pulse intensity on the polarization setting corresponds to Path 1, while that used to characterize dependence of the state polarization on the intensity setting corresponds to Path 2. (b) The experimental results for the signal/decoy intensities illustrate that the actual intensity of the emitted pulse depends on the polarization modulation, with noticeable fluctuations for the decoy state. (c) Polarization shift undergone by the Z-basis states $|H\rangle$ and $|V\rangle$ and (d) Polarization shift undergone by the X-basis states $|A\rangle$ and $|D\rangle$. To improve clarity, all curves are plotted using a 0.15 V step size.

intensity setting. Finally, we convert the photon counts into relative loss, defined as

$$loss(V_{Pol}) = -10\log_{10}\frac{N(V_{Pol})}{N(0)}, \tag{1}$$

where $N(V_{Pol})$ represents the number of detections when the Pol-M's CDMs are driven at V_{Pol}. The relative loss under the signal/decoy state is shown in Fig. 1b. These curves show that the relative loss of the chip varies with the voltage of the Pol-M's CDMs. As the voltage varies from -3 to 3 V, the relative loss of the source chip increases from -0.5 dB to 1.5 dB. For the decoy state, the relative loss experiences noticeable fluctuations when the voltage drops below -2 V due to the interference of the IM.

Dependence of the state polarization on the intensity setting. In the second experiment, we examine how the intensity setting affects the actual polarization of the emitted states. The experimental setup is shown in Fig. 1a (Path 2). A decoder chip [6] is employed to analyze the actual polarization of the quantum state. This decoder comprises spot size converters (SSC), a polarization splitter-rotator (PSR), VOAs, MMIs and TOMs. The loss of the decoder chip is ∼4 dB [6]. By adjusting the TOMs, one can measure the input light in the Z and the X bases.

In the experiment, the polarization setting is set to produce a particular polarization state $|\psi\rangle \in \{|H\rangle, |V\rangle, |D\rangle, |A\rangle\}$ for the signal intensity. Secondly, the signal from the AWG is applied to the IM's CDM, sweeping the voltage from -4 V to 3 V in increments of 0.05 V, and the clicks of the four SNSPDs for 0.2 seconds are recorded at each voltage. We repeat the procedure for the four polarizations. Note that the direct measurement results from the SNSPDs correspond to photon counts associated with the Z and X bases, and therefore these counts need to be converted into polarization states. We estimate the actual polarization state by calculating the normalized photon counts within the same basis. In particular, if N_H, N_V (N_D, N_A) denote the measured photon counts in the Z (X) basis, the estimated polarization state is computed as

$$|\psi\rangle = \begin{cases} (\frac{N_H}{N_H+N_V}, \frac{N_V}{N_H+N_V})^T & \text{if } |H\rangle \text{ or } |V\rangle \text{ is sent,} \\ (\frac{N_A}{N_A+N_D}, \frac{N_D}{N_A+N_D})^T & \text{if } |D\rangle \text{ or } |A\rangle \text{ is sent.} \end{cases} \tag{2}$$

Now, let $|\psi_0\rangle$ be the reference polarization state, *i.e.*, the state when the voltage of the IM's CDMs is 0 V. Then, we measure the difference between the polarization of the reference state $|\psi_0\rangle$ and the polarization of the state $|\psi\rangle$ associated with a particular voltage $V_{\rm IM}$ at the IM's CDMs as

$$\Delta\theta = \arccos\langle\psi|\psi_0\rangle. \tag{3}$$

As shown in the Figs. 1c and 1d, the observed polarization shifts significantly as $V_{\rm IM}$ deviates from 0 V. Furthermore, the magnitude of this shift depends on the voltage applied to the Pol-M. In particular, the horizontally polarized state $|H\rangle$ —which undergoes no modulation— suffers the smallest polarization shift, whereas the vertically polarized state $|V\rangle$ —which has the largest modulation voltage— exhibits the strongest polarization shift. These results demonstrate that the actual polarization changes with the voltage of the IM's CDMs.

Theoretical analysis and impact on the security. Let $x \equiv a_\alpha \in \{0_Z, 1_Z, 0_X, 1_X\}$ and $I \in \{I_0, I_1, I_2\}$ denote Alice's polarization and intensity settings, respectively. According to our experimental observations, the actual mean photon number μ of the generated optical pulse depends not only on the intensity setting I but also on the polarization setting x, and a similar effect has been observed for the actual polarization θ. This means that the transmitted states must be generally modeled as $\rho_{x,I} = \sum_{n=0}^{\infty} p_{n|\mu(x,I)} \, |n_{\theta(x,I)}\rangle\langle n_{\theta(x,I)}|$, where $p_{n|\mu(x,I)}$ represents the conditional probability of emitting n photons given that the actual intensity of the emitted pulse is $\mu(x,I)$, and $|n_{\theta(x,I)}\rangle$ is an n-photon state with polarization $\theta(x,I)$. Similarly, we have that $Q^{b_\beta}_{x,I} = \sum_{n=0}^{\infty} p_{n|\mu(x,I)} Y^n_{b_\beta,\theta(x,I)}$, where $Q^{b_\beta}_{x,I}$ ($Y^n_{b_\beta,\theta(x,I)}$) is the probability that Bob records the measurement outcome b given that he selects the basis β and Alice prepares the state $\rho_{x,I}$ ($|n_{\theta(x,I)}\rangle$).

In this scenario, the probability of emitting a single-photon state in a (Z, I_0)-round may differ for Alice's bits $a = 0$ and $a = 1$, as in general $p_{1|\mu(0_Z,I_0)} \neq p_{1|\mu(1_Z,I_0)}$. Besides, the single-photon yield can no longer be estimated using the standard decoy-state analysis, as $\theta(x,I)$ now depends on the intensity setting and therefore $Y^n_{b_\beta,\theta(x,I)} \neq Y^n_{b_\beta,\theta(x,J)}$ for $I \neq J$. Moreover, the single-photon states are now deviated from their ideal polarization state, and so the bit-averaged Z-basis and X-basis single-photon components are in general distinguishable.

To evaluate the impact of the cross CPI correlations on the security, we derived an asymptotic security analysis for decoy-state QKD that allows to estimate the single-photon yield and the phase-error rate in this scenario. For this, we establish loss-tolerant-type relations [7] among certain yields, as well as include additional fidelity-based constraints between yields with the same value of x but different I.

The rate vs distance performance of the decoy-state protocol is shown in Fig. 2. There, we consider two scenarios: one with an ideal transmitter that does not suffer from CPI correlations, and the real scenario with cross correlations. The results show that, with the considered security analysis, the CPI correlations slightly reduce the attainable secret-key rate in the two-decoy setup. Interestingly, in the one-decoy setup, CPI correlations enhance the secret-key rate. This occurs because these correlations introduce additional effective intensities that help to improve the yield and phase-error rate estimations. Importantly, we remark that applying a standard decoy-state analysis that disregards CPI correlations on the same set of protocol statistics could result in an insecure key rate.

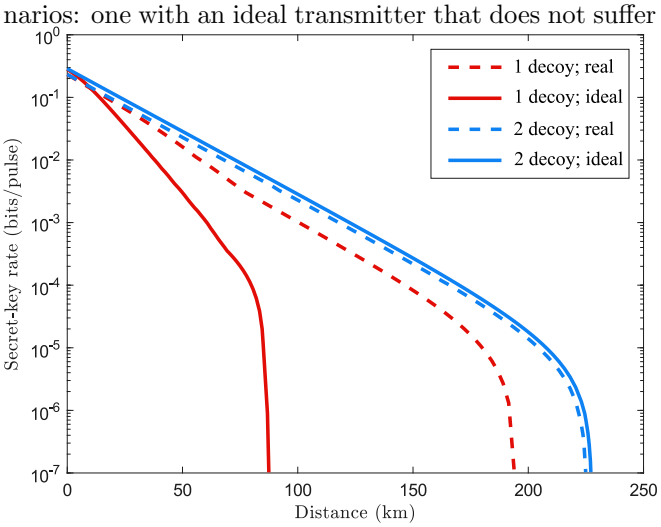

FIG. 2: Rate-distance performance for the decoy-state BB84 protocol with 1 (red lines) and 2 (blue lines) decoy intensities. The solid lines represent the ideal scenario where both the intensity and encoding perfectly match their ideal values. The dashed lines depict the realistic flawed scenario analyzed in this work. The intensities have been optimized for each distance.

[1] C. H. Bennett and G. Brassard, in *Proc of IEEE International Conference on Computers* (1984).

[2] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, *et al.*, Nature Photonics **17**, 416 (2023).

[3] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[4] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Phys. Rev. Appl **13**, 034017 (2020).

[5] K. Wei, X. Hu, Y. Du, X. Hua, Z. Zhao, Y. Chen, C. Huang, and X. Xiao, Photonics Research **11**, 1364 (2023).

[6] Y. Du, X. Zhu, X. Hua, Z. Zhao, X. Hu, Y. Qian, X. Xiao, and K. Wei, Chip **2**, 100039 (2023).

[7] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma,
Physical Review A **90**, 052314 (2014).