Hong-Ou-Mandel interference for plug-and-play measurement-device-independent QKD

Kai-Wen Chen[1,2], Simone Atzeni[1,2], Stéphane Clemmen[1,2,3,4], and Dries Van Thourhout[1,2]

[1]Photonics Research Group, INTEC Department, Ghent University-IMEC, 9052 Ghent, Belgium
[2]Center for Nano- and Biophotonics (NB-Photonics), Ghent University, 9052 Ghent, Belgium
[3]OPERA-Photonique CP 194/5, Université Libre de Bruxelles (ULB), 1000 Bruxelles, Belgium
[4]Laboratoire d'Information Quantique CP224, Université Libre de Bruxelles, 1050 Bruxelles, Belgium

Abstract

Plug-and-play Measurement-Device-Independent Quantum Key Distribution (MDI-QKD), where both the light source and measurement device are at an untrusted node, offers resilience against detector-side attacks and reduces the need for active stabilization. However, achieving high-visibility quantum interference remains essential for efficient Bell-state measurements. Here, combining a commercial gain-switched distributed feedback laser with a fiber Bragg grating filter, we demonstrate Hong–Ou–Mandel (HOM) interference with $47 \pm 1.6\%$ *visibility. Employing Faraday mirrors, our system achieves HOM visibility exceeding* 45% *and is insensitive to polarization variation in the quantum channel. Using off-the-shelf fiber components, it demonstrates high visibility and polarization insensitivity, representing a key step toward practical plug-and-play MDI-QKD.*

I. Introduction

Over the last few decades, quantum key distribution (QKD) has emerged as a promising technology to address the potential threat posed by quantum computing to classical encryption systems. To counter this threat, QKD leverages the fundamental principles of quantum mechanics and, in principle, ensures information-theoretic security for remote users [1]. However, in practical implementations, security loopholes arising from imperfect measurement systems can allow an eavesdropper to compromise the secret key shared between two users. Measurement-device-independent (MDI)-QKD addresses this issue by eliminating all detection-side loopholes, placing the detector at an untrusted node, Charlie, who performs Bell-state measurements (BSM) on the encoded photons sent by Alice and Bob [2].

For a reliable BSM, incoming photons must be identical in polarization, spectrum, and temporal profile. The Hong–Ou–Mandel (HOM) interference visibility quantifies this indistinguishability and serves as a key metric for BSM performance in MDI-QKD. Previous studies using single-photon sources or weak coherent pulses (WCPs) [3] have achieved high visibility, enabling secure key generation at high rates. However, maintaining high HOM visibility in MDI-QKD often requires active stabilization of the interfering photons, including spectral matching between independent sources [4] and polarization alignment to compensate for polarization rotation induced by environmental fluctuations in the two channels [5].

To address these challenges, a plug-and-play architecture for MDI-QKD has been proposed [2]. In this scheme, Charlie sends optical pulses to both users through separate optical channels. Then, Alice and Bob encode quantum information and return them to Charlie, where the BSM is subsequently performed. Sharing a common source ensures spectral indistinguishability, while Faraday mirrors at Alice's and Bob's nodes automatically compensate for polarization drifts in optical fibers [6]. This approach has been supported by both security analyses [2] and experimental demonstrations [7].

In this work, we experimentally demonstrate HOM interference in a plug-and-play MDI-QKD configuration, achieving a $47 \pm 1.6\%$ visibility. The system exhibits insensitivity to polarization drifts in the quantum channels connecting Alice and Bob to Charlie. Band-pass filters are employed at the source to generate Fourier-transform-limited pulses and to mitigate the timing jitter associated with gain-switched operation.

II. Preparation of Phase Randomized Weak Coherent Pulses (WCPs)

Practical QKD systems generally rely on WCPs generated from semiconductor lasers. However, phase randomization is required to eliminate residual coherence between adjacent pulses and to enable decoy-state protocols that satisfy security requirements against multi-photon components attack [8]. Several techniques have been developed to generate phase-randomized WCPs, including gain-switching, optical injection locking (OIL), and pulse carving [9]. Among these methods, gain-switched lasers offer the most efficient and practical solution.

Phase randomization in gain-switched operation is achieved by turning the laser off between pulses, allowing each new pulse to originate from spontaneous emission with a random phase. However, when gain-switched pulses are employed in MDI-QKD, effects such as time jitter, frequency chirp [10, 11], and relaxation oscillations [11] arise, which limit the achievable HOM interference visibility. Spectral filtering has been shown to effectively enhance HOM visibility by mitigating frequency chirp in short optical pulses [10].

We generate WCPs using a commercial DFB laser (D2502G, Lucent), driven by 200 MHz, 230 ps-wide RF pulsed signal from a pulse generator (8133A, Hewlett Packard) and DC biased below threshold to ensure gain-switching operation. Phase randomization of the generated pulses is verified by interfering adjacent pulses and recording the resulting intensity distribution on a high-speed sampling oscilloscope (DSA8300, Tektronix), which exhibited a characteristic double-peaked structure corresponding to dominant constructive and destructive interference events [12]. The spectral and temporal profiles of the generated pulses under different band-pass filtering conditions are reported in Fig. 1. A Finisar Waveshaper 1000S is employed to filter the pulses to 12.5 GHz, and a fiber Bragg grating (FBG) filter is subsequently used to further narrow the bandwidth to 4.6 GHz. As shown in Fig. 1 when the pulses are unfiltered, the spectral and temporal full widths at half maximum (FWHM) are 63 GHz and 37 ps, respectively, which are considerably broader than those of a transform-limited pulse (12 GHz and 37 ps FWHM, corresponding to a time-bandwidth product of 0.441 for a Gaussian profile). The broad spectral width results from frequency chirp induced by abrupt changes in carrier density and refractive index during gain-switching process [13]. When a 12.5 GHz band-pass filter is applied, the spectral FWHM decreases to 12.6 GHz, while the temporal FWHM remains nearly unchanged. Furthermore, with a 4.6 GHz FBG filter, the spectral FWHM reduces to 4.7 GHz, while the temporal FWHM is broaden to 121 ps. The 12.5 GHz and 4.6 GHz filters yield similar time-bandwidth products of 0.54 and 0.57, respectively, indicating that the pulses approach the transform limited condition.

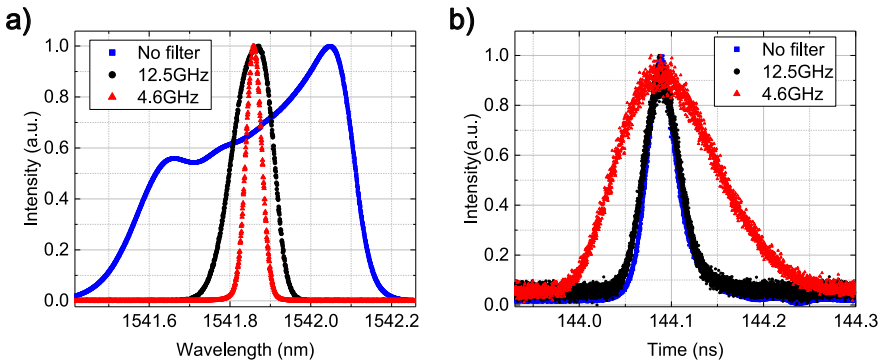

Fig. 1: (a) Optical spectrum and (b) temporal profile of phase-randomized gain-switched pulses generated by a DFB laser. A band-pass filter with 12.5 GHz or 4.6 GHz bandwidth is cascaded to the laser to reduce the pulse linewidth.

III. HOM Experimental Setup and Results

The HOM measurement for the plug-and-play MDI-QKD system is illustrated in Fig. 2. After WCPs preparation, a 50/50 beam splitter (BS1) divides the pulses and directs them to Alice's and Bob's nodes. A tunable optical delay line (ODL; ODL-650, OZoptics) is inserted in one of the node to compensate for the temporal delay between two subsequent pulses and synchronize the arrival time of Alice's WCPs with those of Bob at BS2. Polarization controllers (PC) are placed before BS2 in both Alice's and Bob's nodes to finely adjust the polarization of the WCPs, ensuring polarization indistinguishability at the interference point. Variable optical attenuators (VOAs) are employed to attenuate the laser power such that the mean photon number per pulse is within the single-photon regime, and eventually to balance the relative loss asymmetry between the two optical paths. The output ports of BS2 are connected to single-photon avalanche diodes (SPADs; SPD-OEM-NIR, Aurea Technology) operated in a 35 MHz gated mode with a 5 ns gate width, driven by a digital delay generator (DG645, Stanford Research System). The detection efficiency and dead time of the SPADs are set to 15 % and 10 μs, respectively. Detection events are recorded using a time tagger (ID1000, ID Quantique) with a temporal resolution of 100 ps. The coincidence histogram and HOM visibility are subsequently obtained using data acquisition software. The HOM visibility is measured by scanning the tunable delay line with picosecond precision and recording the coincidence counts from the two detectors at multiple delay settings.

Firstly, we investigate the effect of the filter bandwidth using the setup shown in Fig.2(a). In this configuration, two quantum channels are established between Charlie and Alice/Bob: one for transmitting strong optical pulses

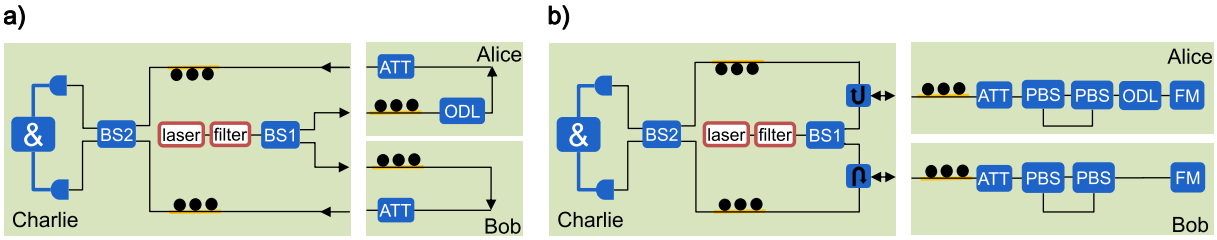

Fig. 2: Schematic of the HOM measurement setup for the plug-and-play MDI-QKD system. (a) Two quantum channels are established between Charlie and Alice/Bob for transmitting strong pulses and returning encoded weak coherent pulses (WCPs). (b) A single quantum channel configuration is implemented by introducing optical circulators at Charlie's node, with Faraday mirrors (FMs) at Alice's and Bob's nodes for automatic polarization compensation. BS, 50/50 beam splitter; ATT, variable optical attenuator; PBS, polarization beam splitter; ODL, tunable optical delay line.

from Charlie to the users, and the other for returning the encoded states back to Charlie. VOAs placed at Alice's and Bob's node are used to attenuate the pulses to WCPs level. Fig.3(a) presents the measured HOM visibilities obtained with different filter bandwidths. The visibility increases from 0.27 to 0.47 as the filter bandwidth is reduced from 62.4 GHz to 4.6 GHz, respectively. Since the HOM interference curve represents the convolution of the filtered pulses, a temporal broadening of the dip is observed for the 4.6 GHz case, consistent with the pulse trace shown in Fig.1(b).

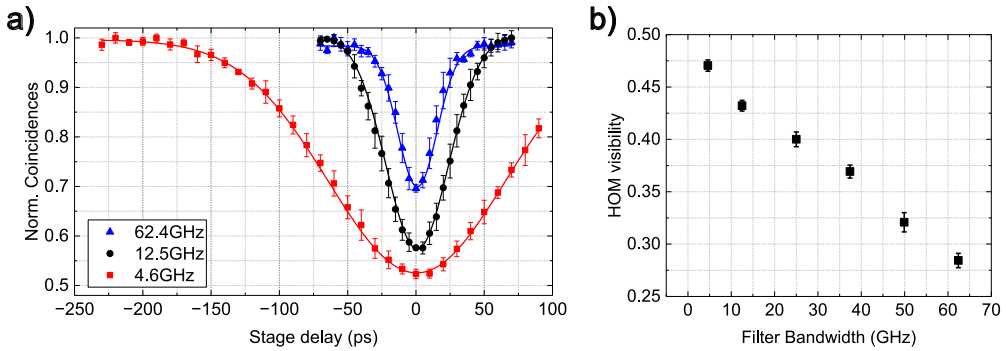

Fig. 3: HOM interference results using the setup in Fig. 2(a). (a) Normalized coincidences with delay line scanned for 200 ps, or 320 ps, range with filter bandwidths above 12.5 GHz, or 4.6 GHz, respectively. (b) Measured HOM visibility as a function of the filter bandwidth, showing an increase from 0.27 to 0.47 as the bandwidth is reduced from 62.4 GHz to 4.6 GHz.

Next, the plug-and-play MDI-QKD configuration incorporating Faraday mirrors is implemented, as illustrated in Fig.2(b). At Charlie's node, two optical circulators are placed after BS1, enabling Charlie to transmit strong optical pulses and receive encoded WCPs through a single quantum channel. Two polarization beam splitters (PBS) are connected back-to-back—an essential feature for future implementations where intensity modulators are placed between the PBSs for state encoding. A Faraday mirror is installed at the end of Alice's and Bob's node to reflect the pulse and rotate their polarization by 90°. Fig. 4(a) presents the HOM interference measurement, achieving a visibility of 0.47 using the plug-and-play configuration with a 4.6 GHz FBG filter applied to the laser pulses. Polarization drifts in the quantum channels is simulated by rotating the center waveplate of the polarization controllers (PCs) located at Alice's and Bob's nodes. Fig.4(b) shows that the HOM visibility remains above 0.45 for all waveplate rotation angles, indicating that the plug-and-play configuration in our system is robust against polarization drift in the quantum channel.

IV. Conclusions

In this work, we have demonstrated HOM interference with a visibility of $47 \pm 1.6\%$ in a plug-and-play MDI-QKD system. Photon indistinguishability was improved by reducing the linewidth of the WCPs through the use of narrow band-pass filters. Moreover, polarization insensitivity of the quantum channel was achieved through the use of Faraday mirrors at the user nodes, maintaining HOM interference visibility above 0.45 across all tested polarization states. Such visibility has been reported to support a sufficiently secure key rate in QKD systems [14].

In future work, high-speed intensity and phase modulators will be integrated at Alice's and Bob's nodes to enable quantum state encoding and to evaluate the quantum bit error rate (QBER) and key generation

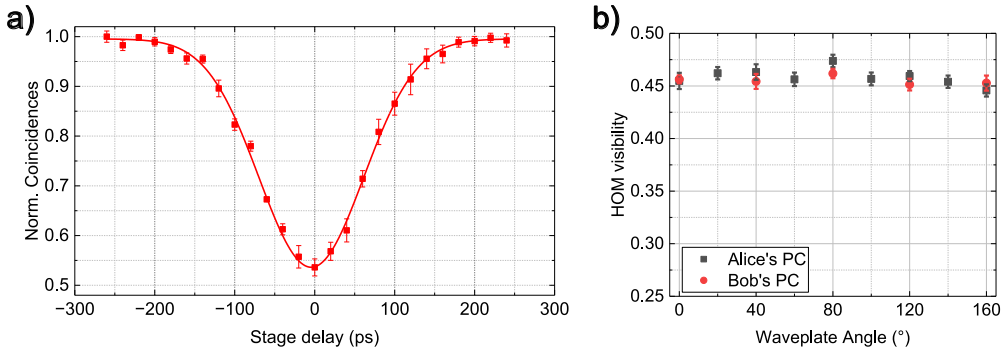

Fig. 4: HOM interference results using the setup in Fig. 2(b). (a) Normalized coincidences for delay line scanned over 250 ps, with effective optical path doubled by use of Faraday mirrors. (b) HOM visibility versus center waveplate angle in Alice's and Bob's polarization controller. HOM visibility remains above 0.45 across all settings, confirming robustness against polarization drift.

performance of the plug-and-play MDI-QKD system. Furthermore, the use of silicon photonic integrated circuits as transmitters [15], receivers [4], and heterogeneously integrated sources [16] will be investigated to increase integration density, enhance miniaturization, and reduce infrastructure costs.

Acknowledgements

This work is supported by EU Be-QCI (Grant agreement ID:101091625) and QU-Pilot (Grant agreement ID: 101113983). Stéphane Clemmen is a research associate of the FNRS.

References

[1] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[2] F. Xu, "Measurement-device-independent quantum communication with an untrusted source," *Physical Review A*, vol. 92, no. 1, p. 012333, 2015.

[3] E. Moschandreou, J. I. Garcia, B. J. Rollick, B. Qi, R. Pooser, and G. Siopsis, "Experimental study of hong–ou–mandel interference using independent phase randomized weak coherent states," *Journal of Lightwave Technology*, vol. 36, no. 17, pp. 3752–3759, 2018.

[4] X. Zheng, P. Zhang, R. Ge, L. Lu, G. He, Q. Chen, F. Qu, L. Zhang, X. Cai, Y. Lu *et al.*, "Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution," *Advanced Photonics*, vol. 3, no. 5, pp. 055 002–055 002, 2021.

[5] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Physical review letters*, vol. 111, no. 13, p. 130501, 2013.

[6] A. Kersey, M. Marrone, and M. Davis, "Polarisation-insensitive fibre optic michelson interferometer," *Electronics Letters*, vol. 27, pp. 518–520, 1991.

[7] G.-Z. Tang, S.-H. Sun, and C.-Y. Li, "Experimental point-to-multipoint plug-and-play measurement-device-independent quantum key distribution network," *Chinese Physics Letters*, vol. 36, no. 7, p. 070301, 2019.

[8] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, no. 23, p. 230504, 2005.

[9] T. K. Paraïso, R. I. Woodward, D. G. Marangon, V. Lovic, Z. Yuan, and A. J. Shields, "Advanced laser technology for quantum communications (tutorial review)," *Advanced Quantum Technologies*, vol. 4, no. 10, p. 2100062, 2021.

[10] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, M. Ward, and A. Shields, "Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications," *Physical Review Applied*, vol. 2, no. 6, p. 064006, 2014.

[11] L. Millet, A. Boaron, R. Thew, and G. Boso, "Influence of laser chirp and interferometer delay and imbalance on the performance of a time-bin bb84 quantum key distribution system," *Applied Physics Letters*, vol. 127, no. 4, 2025.

[12] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Applied Physics Letters*, vol. 104, no. 26, 2014.

[13] J. Wiesenfeld and J. Stone, "Picosecond pulse generation in optically pumped, ultrashort-cavity, ingaasp, inp, and ingaas film lasers," *IEEE journal of quantum electronics*, vol. 22, no. 1, pp. 119–132, 2003.

[14] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Practical aspects of measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 15, no. 11, p. 113007, 2013.

[15] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang *et al.*, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Physical Review X*, vol. 10, no. 3, p. 031030, 2020.

[16] C. Agnesi, B. Da Lio, D. Cozzolino, L. Cardi, B. Ben Bakir, K. Hassan, A. Della Frera, A. Ruggeri, A. Giudice, G. Vallone *et al.*, "Hong–ou–mandel interference between independent iii–v on silicon waveguide integrated lasers," *Optics letters*, vol. 44, no. 2, pp. 271–274, 2019.