Photon-Efficient High-Dimensional Quantum Key Distribution

Tian Zhong, Hongchao Zhou, Ligong Wang, Gregory Wornell, Zheshen Zhang, Jeffrey Shapiro, Franco N. C. Wong,
Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
Rob Horansky, Varun Verma, Adriana Lita, Richard P. Mirin, Thomas Gerrits, Sae Woo Nam
National Institute of Standards and Technology, 325 Broadway, MC 815.04, Boulder, Colorado 80305, USA
Alessandro Restelli, Joshua C. Bienfang
Joint Quantum Institute, National Institute of Standards and Technology and University of Maryland, 100 Bureau Dr., Gaithersburg, MD 20899, USA
Francesco Marsili and Matthew D. Shaw
Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, California 91109, USA
tzhong@mit.edu

Abstract: We demonstrate two high-dimensional QKD protocols — secure against collective Gaussian attacks — yielding up to 8.6 secure bits per photon and 6.7 Mb/s throughput, with 6.9 bits per photon after transmission through 20 km of fiber.

OCIS codes: (270.5565) Quantum communications; (270.5585) Quantum information and processing; (270.0270) Quantum optics.

The widespread use of quantum key distribution (QKD) has been hindered by low secure-key throughput due to the inherent loss and de-coherence of photons during transmission. Most existing protocols use a two-dimensional Hilbert space or two conjugate continuous variables for key encoding, with photon information efficiency (PIE) of at most 1 bit per photon and a key rate that is limited by the photon flux reaching the receiver. High-dimensional QKD (HDQKD) promises to significantly improve PIE and key throughput, however its implementation within a framework of proven security for multiple bits per photon has remained a long-standing challenge. We report the first full-protocol implementations of HDQKD, yielding high PIE up to 8.6 secure bits per photon and sustaining 6.9 bits per photon after 20 km of fiber transmission. With enhanced throughput as high as 6.7 Mb/s, our results represent a viable approach to high-capacity quantum communications by efficiently utilizing available photonic entanglement and detection resources.

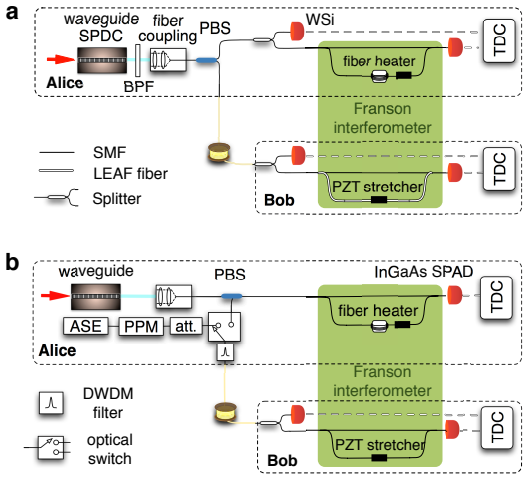

Table I. Optimal operating parameters of HDQKD

	Protocol (a)	Protocol (b)
α_{SPDC}	0.035 %	0.5 %
α_{PPM}	-	1.3
Franson visibility	99.7 %	99.5 %
βI_{AB}	7.6	3.0
χ^E	0.29	0.1
secure PIE	7.31	2.9
secure Mb/s	6.7	7.3

Fig. 1. (a) Experimental schematic for entanglement-based HDQKD using SPDC photons. (b) Schematic for PPM-based HDQKD using ASE and SPDC photons. 90-10 fiber beam splitters were used in (a), and 50-50 splitters in (b). PPM on ASE light was performed using a 10 Gb/s intensity modulator. In (b) the ASE and SPDC photons were randomly routed using an electro-optical switch driven by a pseudo-random bit sequence with a ratio of 7:3 between PPM frames and Franson frames. The path-length difference of the Franson interferometer was 9.5 ns in (a), and 793 ps in (b). BPF: band-pass filter, PBS: polarizing beam splitter, TDC: time-to-digital converter.

The two HDQKD implementations are shown schematically in Fig. 1. The protocol in 1(a) uses time-energy-entangled photon pairs generated from a continuous-wave spontaneous parametric downconversion (SPDC) source at Alice's location. Alice and Bob measure the photon arrival times at a resolution τ that defines a time bin. N consecutive bins form a frame. For each frame, Alice and Bob measure the arrival bin position of photons either directly, for extracting symbols of $k=\log_2 N$ bits, or after going through the Franson interferometer used to establish security. After the quantum communication, Alice and Bob post-select frames that contain exactly one detection, and perform error correction and privacy amplification. The system in 1(b) uses pulse-position modulation (PPM) of

a classical amplified spontaneous emission (ASE) photon source to generate multi-bit symbols. The thermal-state broadband ASE photons were filtered to mimic the spectrum of SPDC light. For each frame, Alice randomly chooses between the two sources to send a photon to Bob, whom then measures the photon arrival time either directly or after the Franson interferometer. This random switching prevents Eve from knowing when security check is performed. After the quantum communication, she publicly announces her choice of the photon sent, allowing Bob to sift the raw symbols before error correction and privacy amplification steps.

The secure PIE is $\Delta I_{AB} = \beta I_{AB} - \chi^{E}$, where β is the reconciliation efficiency, I_{AB} is the extractable mutual information (MI) between Alice and Bob, and χ^{E} is the Holevo information of Eve bounded by the measured Franson visibility considering collective Gaussian attacks in the asymptotic limit of infinitely long keys [1]. Error correction performed on the raw k-bit symbols was implemented using a custom code for large-alphabet QKD. The code uses a layered scheme that successively applies low density parity check (LDPC) binary error correction on every bit layer of the symbols.

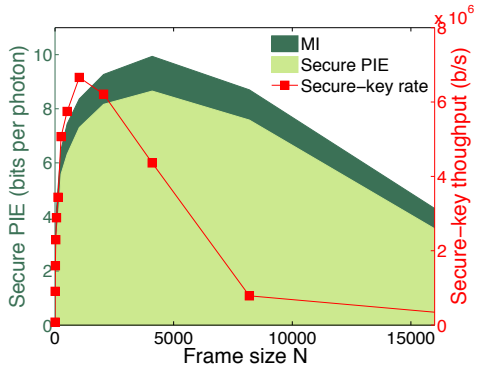

Fig. 2. Optimization of secure PIE and secure-key throughput for the HDQKD protocol using time-energy entangled photons.

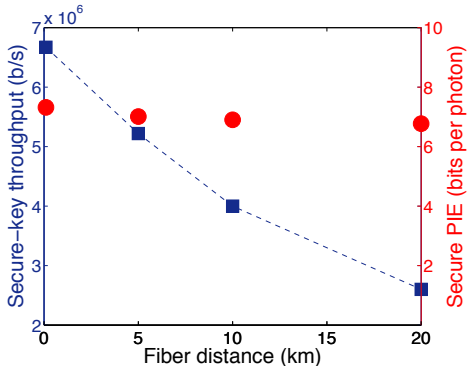

Fig. 3. Secure QKD throughput (solid squares) and PIE (solid circles) measured after up to 20 km of fiber.

We employed six ≈90 % efficient WSi superconducting nanowire single-photon detectors (SNSPDs) with an average timing jitter of ≈80 ps full-width at half-maximum (FWHM) and a maximum count rate of ≈1.5 ×10^6 s^{-1} [2]. To mitigate the ≈700 ns reset times of WSi SNSPDs, passive 50-50 splitters were used at both Alice and Bob to distribute photons evenly between two WSi SNSPDs, and their data were interleaved. Fig. 2 shows the results of optimizing the HDQKD throughput by varying the frame size while keeping the mean photon number per time bin α constant. The optimized parameters are summarized in Table I. The bin size was τ = 80 ps. Our layered LDPC code performed error correction efficiently for all symbol lengths. The measured raw Franson visibilities were consistently at $V/V^{th} \geq 99.8$ % (V^{th} is the theoretical visibility) as a result of complete non-local dispersion cancellation [3], leading to a tightly bounded $\chi^{E} \leq 0.39$ bits. With a fiber transmission distance of 100 m, the secure PIE peaked at 8.6 bits per photon for the frame size N = 4096 that is comparable with the pump coherence time ≈200 ns. This entanglement-based system achieved a maximum secure key rate of 6.7 Mb/s at 7.3 secure bits per coincident pair. Compared with binary encoding (N=2), such as the state-of-the-art implementation of BBM92 based on polarization entanglement [4] with a 12.5 kb/s rate, our result demonstrates an improvement in PIE by ≈20 times and QKD throughput by ≈500 times. More importantly, long-distance photon-efficient key distribution experiments were performed at 5 km, 10 km and 20 km of standard optical fiber distance as shown in Fig. 3. We were able to maintain 6.9 secure bits per photon despite broadening of the coincidence signals due to fiber chromatic dispersion.

The PPM implementation employed commercially available InGaAs single-photon avalanche photodiodes (SPADs) operated in the self-differencing mode at a 1.26 GHz gating frequency, with detection efficiencies of 18 % and effective detection gate width of ≈100 ps. Higher dark counts and afterpulsing of SPADs resulted in increased symbol error rates and lower PIE. However, the reset time of the high-speed gated SPADs is much shorter than that of the WSi SNSPDs, thus allowing much higher source generation rates without saturating the detectors. We achieved a peak PPM key generation of 7.3 Mb/s with a secure PIE 2.9 bits per photon at N=16. This key rate, which compares favorably with the highest QKD rate reported to date based on decoy-state BB84 protocol [5], could have been higher but is currently limited by the maximum count-recording rate of 12 ×10^6 s^{-1} of the TDCs.

References

[1] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, arXiv:1311.0825.
[2] F. Marsili *et al*., Nature Photon. **7**, 210 (2013).
[3] T. Zhong and F. N. C. Wong, Phys. Rev. A **88**, 020103(R) (2013).
[4] A. Treiber *et al*., New J. Phys. **11**, 045013 (2009).
[5] M. Lucamarini *et al*., Opt. Express **21**, 24550 (2013).