Mutual Information of a High-Dimensional Quantum Key Distribution Scheme using Time-Bin Encoding

Christoph F. Wildfeuer and Daniel J. Gauthier

Department of Physics, Duke University, Durham, NC 27708, USA

wildfeuer@phy.duke.edu

Abstract:
We derive the mutual information of a high-dimensional time-bin entangled quantum-key distribution system (QKD) when a spontaneous parametric down-conversion source (SPDC) is used.

OCIS codes: 270.0270, 270.5568

1. Introduction

Methods for high-dimensional QKD have been proposed that share information using the photon arrival time, thereby encoding over 10 bits of information per detected photon pair, albeit with large noise [1]. One possible photon source for this scheme is spontaneous parametric down-conversion which, in the case of no system loss, generates a random sequence of perfectly correlated photon pairs shared between the two parties Alice and Bob. Alice and Bob each use single-photon counter modules and synchronized time-tagging devices to obtain the timing information, which constitutes the key, as displayed in Fig.1. If loss is present, random deletion errors require error correcting codes and privacy amplification to generate a secret key, as previously considered by Kochman and Wornell [2] for the case of asymmetric losses. The concept of a frame, where n time-bins are grouped together, may be used to improve the efficiency of the error correction task. For instance, a frame where Alice and Bob share at most one photon pair ideally provides $\log_2(n)$ shared bits of information.

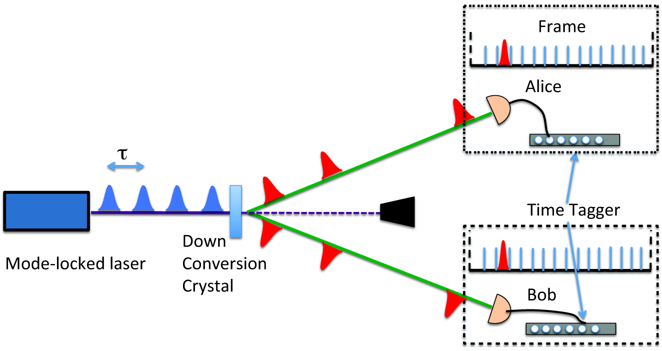

Fig. 1. Proof-of-principle experimental setup for the QKD system. A mode-locked laser with pulse period τ pumps a nonlinear crystal that produces photon pairs.

2. Conditional entropies and mutual information

As a first step, we investigate the situation of no channel loss, but allow for more than one photon in a frame, thereby extending the work of Kochman *et al.* [2]. We introduce conditional entropies [3, 4] and decompose the information contained in a frame encoding scheme into two parts: the information contained in the bit pattern conditioned on the photon number; and the information contained in the photon-number distribution. We find that the mutual information in the lossless case is bounded by Alice's or Bob's individual entropies and is given by

$$I(X_{\mathrm{A}}, X_{\mathrm{B}}) = -\sum_{k=0}^{n} P(k) \log_2 \left(\frac{P(k)}{\binom{n}{k}} \right). \tag{1}$$

Equation (1) holds for any photon-number probability distribution $P(k)$. We display the mutual information for a Poisson photon-number distribution of the photon pairs, i.e., $P(k) = (n\lambda)^k \exp(-n\lambda)/k!$, where λ is the mean photon-number per time-bin with time-bin width τ in Fig. 2. The figure displays the contribution to the mutual information for frames with zero, one, two, and three photons in a frame. We observe that one-photon frames provide the largest contribution to the mutual information. However, two-photon and three-photon frames give a substantial contribution except in the limit when $\lambda \to 0$.

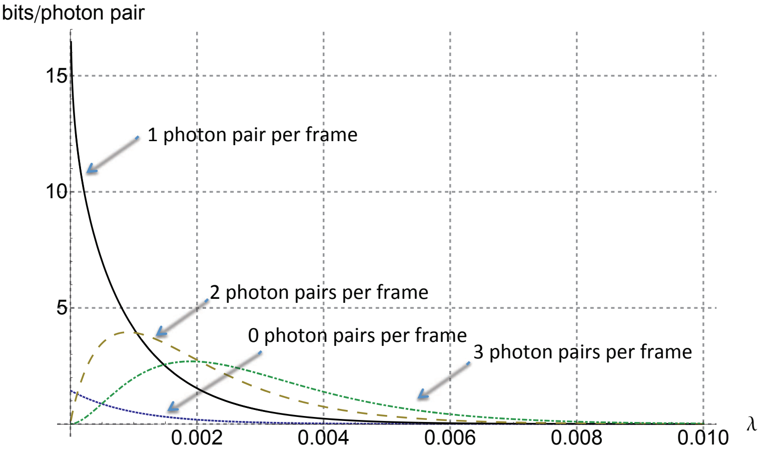

Fig. 2. Mutual information per photon pair detected $I(X_{\mathrm{A}}, X_{\mathrm{B}})$ as a function of the mean photon number per time-bin for $n = 1024$ time bins and no loss.

Next we investigate the general case of arbitrary loss for Alice and Bob by introducing the parameters $0 \leq \eta_{\mathrm{A}} \leq 1$ and $0 \leq \eta_{\mathrm{B}} \leq 1$, characterizing each channel. We construct the two-dimensional probability distribution that determine the probabilities for all measurement outcomes for Alice and Bob. We outline the formalism and show that, for an ideal single photon-pair source (exactly one photon pair per frame, $P(k=1) = 1$ and $P(k \neq 1) = 0$), the mutual information is given by $I(X_{\mathrm{A}}, X_{\mathrm{B}}) = \eta_{\mathrm{A}}\eta_{\mathrm{B}} \log_2(n)$. The mutual information per detected photon pair is given by $I_{\mathrm{d}}(X_{\mathrm{A}}, X_{\mathrm{B}}) = I(X_{\mathrm{A}}, X_{\mathrm{B}})/\eta_{\mathrm{A}}\eta_{\mathrm{B}} = \log_2(n)$. Hence, the photon efficiency becomes 10 bits per detected photon pair for a frame size of $n = 1024$ time bins.

We extend this approach to a Poisson photon-number distribution for the photon pairs, which describes very well the situation for a SPDC source, and show results for the mutual information. We finally discuss how the time frame scheme can be used in the first stage of error correcting schemes.

This project is supported by DARPA Information in a Photon (InPho), managed by the Army Research Office.

References

1. I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States," Phys. Rev. Lett. **98**, 060503 (2007).
2. Y. Kochman and G. W. Wornell, "On high-efficiency optical communication and key distribution," Information Theory and Applications Workshop (ITA), pp.172-179, 5-10 Feb. 2012.
3. S. M. Barnett and P. M. Radmore, "Methods in Theoretical Quantum Optics," Oxford University Press, Oxford (1997).
4. T. Brougham and S. M. Barnett, "Information communicated by entangled photon pairs," Phys. Rev. A **85**, 032322 (2012).