

# Enhancing performance and security of practical quantum communication using quantum frequency conversion

Nitin Jain,<sup>1</sup> Paritosh Manurkar,<sup>2</sup> Prem Kumar,<sup>3,4</sup> and Gregory S. Kanter<sup>3</sup>

<sup>1</sup>*Department of Physics, Technical University of Denmark, 2800 Lyngby, Denmark*

<sup>2</sup>*National Institute of Standards and Technology, Boulder, CO 80305, USA*

<sup>3</sup>*Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208, USA*

<sup>4</sup>*Department of Physics and Astronomy, Northwestern University, Evanston, IL 60208, USA*

Quantum frequency conversion (QFC) is a method whereby the quantum features of an input optical ‘signal’ are preserved while simultaneously changing the signal wavelength<sup>1</sup>. QFC is usually realized as a nonlinear interaction, for instance, sum-frequency generation (SFG) in a  $\chi^{(2)}$  waveguide, in which the signal field is combined with a strong classical ‘pump’ field. The basic idea of QFC is illustrated in Fig 1(a). Typically QFC is simply used to translate the wavelength of an input signal. For example, QFC can convert the wavelength of telecom-band photons to visible regime, where single-photon detection can be performed both with high efficiency and low noise, and without resorting to bulky expensive cryogenic technology.

The QFC efficiency  $\eta$  has a sine-squared relationship (under CW conditions) with the square root of the pump power<sup>1–3</sup>. As the pump power is increased from zero,  $\eta$  also increases and reaches a maximum. In case of an ideal SFG,  $\eta = 1$  (after neglecting optical loss), which implies all signal photons obtained at the output of the waveguide simply have their frequency *upconverted*. Practically speaking,  $\eta \lesssim 1$  and due to spurious nonlinear interactions etc., the upconverted photons are also accompanied with noise photons<sup>3</sup>.

**Multidimensional quantum communication:** By means of spectral engineering of the SFG process, which can be realized by tailoring the dispersion properties of the nonlinear medium<sup>4,5</sup> and/or modulation of the pump pulses<sup>6,7</sup>, multimode quantum signals can be made to undergo *mode-selective upconversion*. Depending on the shape and power of the pump pulse, a well-defined signal mode—from a set of orthogonal modes or their superpositions—can be ‘filtered out’, i.e., extracted with high fidelity. This provides the ability to synthesize and analyze arbitrary temporal modes (TMs), which can be used for implementing multidimensional quantum communication protocols and performing quantum information processing tasks<sup>4,8,9</sup>. Figure 1(b) shows the temporal profiles of four orthogonal signal modes  $S1$ – $S4$  that can be mode-selectively upconverted by the corresponding pumps  $P1$ – $P4$  (not shown to avoid cluttering).

**Optical waveform reshaping:** If the pump power is increased beyond the point where the maximum  $\eta$  is achieved, one reaches a stage where ideally all the upconverted light gets re-converted to the original signal wavelength<sup>10</sup>. This principle can be utilized for programmable reshaping of optical pulses without altering their wavelength. Figure 1(c) depicts a couple of examples of reshaped waveforms obtained using the first two

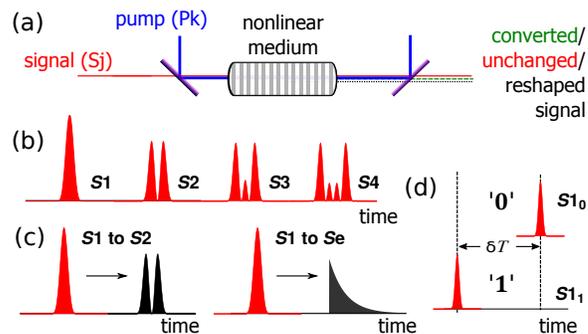


FIG. 1. (Color online) General QFC scheme and signal waveforms for various quantum information processing tasks. In the most basic QFC operation, the shape and power of the pump pulse is chosen so as to maximise the conversion of the signal pulse at the output of the waveguide. More broadly, one can also choose pump and signal modes  $Pk$  and  $Sj$ , respectively, so that for a given pump mode, only one from several ‘orthogonal’ signal modes is converted (green-dashed line), while others remain unchanged (red-solid line). (b) Temporal profiles of signal pulses in the first four Hermite-Gauss modes that form a TM basis. If  $j \neq k$ , the signal undergoes no wavelength conversion. However, if  $j = k$ , and the pump power is so that  $\eta$  is maximum, the signal undergoes only wavelength conversion. (c) Further increasing the pump power results in the output signal getting reshaped; see black-dotted line in (a). With appropriately tailored pumps (not shown), one can actuate  $S1 \rightarrow S2$  or  $S1 \rightarrow Se$  reshaping without a wavelength change. (d) Signal modes  $S1_0$  and  $S1_1$  encode bits ‘0’ and ‘1’, respectively, and form the basis of the time-bin qubit space. With a pair of pump pulses, the frequency-converted signal can be decoded interferometrically for QKD operation.

signal modes  $S1$  and  $S2$  of Fig. 1(b) and an exponentially decaying pulse  $Se$ . Typical applications where optical reshaping serves as a useful tool is interfacing of quantum emitters to the existing fiber infrastructure and pulse distortion compensation.

**Upconversion-protected (UcP) receiver:** With the telecom-band signal photon prepared as a superposition of two optical modes temporally separated by  $\delta T$ , as shown in Fig. 1(d), one can implement a time-mode interferometric quantum key distribution (QKD) scheme<sup>11</sup>. These signal photons, transmitted over the quantum channel, are combined with a pair of bright pump pulses (also separated by  $\delta T$ ) before undergoing upconversion and getting decoded, e.g., in an asymmetric Mach Zehnder interferometer. By adding spectral filters at carefully chosen locations in such a receiver, as well as by monitor-

ing the pump characteristics, one can restrict—in wavelength, time, and power—the light from the channel entering the receiver<sup>12</sup>. This can provide protection against many kinds of quantum hacking attacks<sup>13</sup> in which an eavesdropper actively injects optical radiation into the physical QKD implementation to exploit vulnerabilities, e.g., imperfections in the detection apparatus.

In this contribution, we review some recent results on mode-selective QFC for multidimensional quantum communication, temporal reshaping of optical waveforms on a picosecond timescale, and secure UcP receiver design<sup>9,10,12</sup>. Based on numerical simulations<sup>7</sup> that assume experimental advances in the actual realization of mode-selective QFC, we show that the communication throughput can be significantly increased while the error rate is decreased. Combining these results with some ideas from the UcP receiver, we propose a QKD scheme that can en-

able very high secret key rates over long distances.

- <sup>1</sup>P. Kumar, *Opt. Lett.* **15**, 1476–1478 (1990).
- <sup>2</sup>R. V. Roussev, C. Langrock, J. R. Kurz, and M. M. Fejer, *Opt. Lett.* **29**, 1518–1520 (2004).
- <sup>3</sup>M. A. Albota and F. N. C. Wong, *Opt. Lett.* **29**, 1449–1451 (2004).
- <sup>4</sup>A. Eckstein, B. Brecht, and C. Silberhorn, *Opt. Express* **19**, 13770 (2011).
- <sup>5</sup>D. V. Reddy, M. G. Raymer *et al.*, *Opt. Express* **21**, 13840 (2013).
- <sup>6</sup>Y.-P. Huang and P. Kumar, *Opt. Lett.* **38**, 468–70 (2013).
- <sup>7</sup>A. S. Kowligy, P. Manurkar *et al.*, *Opt. Express* **22**, 1–8 (2014).
- <sup>8</sup>B. Brecht, D. V. Reddy, C. Silberhorn, and M. G. Raymer, *Phys. Rev. X* **5**, 1–17 (2015).
- <sup>9</sup>P. Manurkar, N. Jain *et al.*, *Optica* **3**, 1300–1307 (2016).
- <sup>10</sup>P. Manurkar, N. Jain, P. Kumar, and G. S. Kanter, *Optics Letters* **42**, 951–954 (2017).
- <sup>11</sup>C. H. Bennett, *Physical Review Letters* **68**, 3121–3124 (1992).
- <sup>12</sup>N. Jain and G. S. Kanter, *Quantum Information Processing* **15**, 1–17 (2016).
- <sup>13</sup>N. Jain, B. Stiller *et al.*, *Contemp. Phys.* **57**, 366–387 (2016).