Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding

2015 New J. Phys. 17 022002

(http://iopscience.iop.org/1367-2630/17/2/022002)

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
30 September 2014

REVISED
10 December 2014

ACCEPTED FOR PUBLICATION
14 January 2015

PUBLISHED
4 February 2015

FAST TRACK COMMUNICATION

Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding

Tian Zhong[1], Hongchao Zhou[1], Robert D Horansky[2], Catherine Lee[1], Varun B Verma[2], Adriana E Lita[2], Alessandro Restelli[3], Joshua C Bienfang[3], Richard P Mirin[2], Thomas Gerrits[2], Sae Woo Nam[2], Francesco Marsili[4], Matthew D Shaw[4], Zheshen Zhang[1], Ligong Wang[1], Dirk Englund[1], Gregory W Wornell[1], Jeffrey H Shapiro[1] and Franco N C Wong[1]

[1] Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
[2] National Institute of Standards and Technology, 325 Broadway, MC 815.04, Boulder, CO 80305, USA
[3] Joint Quantum Institute, University of Maryland and National Institute of Standards and Technology, Gaithersburg, MD 20899, USA
[4] Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, CA 91109, USA

E-mail: tzhong@mit.edu **and** tzhong@alum.mit.edu

Keywords: quantum cryptography, quantum communications, quantum entanglement

Abstract

Conventional quantum key distribution (QKD) typically uses binary encoding based on photon polarization or time-bin degrees of freedom and achieves a key capacity of at most one bit per photon. Under photon-starved conditions the rate of detection events is much lower than the photon generation rate, because of losses in long distance propagation and the relatively long recovery times of available single-photon detectors. Multi-bit encoding in the photon arrival times can be beneficial in such photon-starved situations. Recent security proofs indicate high-dimensional encoding in the photon arrival times is robust and can be implemented to yield high secure throughput. In this work we demonstrate entanglement-based QKD with high-dimensional encoding whose security against collective Gaussian attacks is provided by a high-visibility Franson interferometer. We achieve unprecedented key capacity and throughput for an entanglement-based QKD system because of four principal factors: Franson interferometry that does not degrade with loss; error correction coding that can tolerate high error rates; optimized time–energy entanglement generation; and highly efficient WSi superconducting nanowire single-photon detectors. The secure key capacity yields as much as 8.7 bits per coincidence. When optimized for throughput we observe a secure key rate of 2.7 Mbit s^{-1} after 20 km fiber transmission with a key capacity of 6.9 bits per photon coincidence. Our results demonstrate a viable approach to high-rate QKD using practical photonic entanglement and single-photon detection technologies.

1. Introduction

Quantum communication and quantum cryptography enable provably secure transfer of information between distant parties. The ability to distribute photonic entanglement reliably and efficiently has been an essential ingredient in many quantum information applications, including quantum key distribution (QKD) [1, 2], quantum teleportation, and quantum repeaters [3]. Entangled photons are attractive carriers of secure information, with numerous information-bearing degrees of freedom and proven immunity against eavesdropping when used in suitable communication protocols [2, 4]. If swapped with high fidelity at quantum repeater nodes, photonic entanglement could be extended over long distances, possibly to a global scale [3]. However, entanglement is a costly and fragile resource that often requires a dedicated quantum channel and specification-demanding hardware for implementing quantum communication protocols. QKD systems based on polarization entanglement that use commonly available spontaneous parametric down-conversion (SPDC) sources and Geiger-mode avalanche photodiodes have so far delivered secure key rates on the order of 10 kbit s^{-1} at a distance no more than a few kilometers [5], which is not attractive for practical applications in which loss due to long fiber distance is inevitable. There are novel communication protocols that are tolerant to photon loss

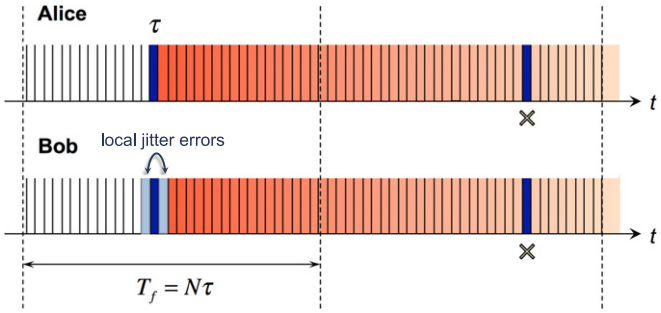

Figure 1. Large-alphabet temporal encoding using correlated photon pairs (in blue). Timing jitter errors are represented by gray slots, and red shadows indicate the reset time of the detectors combined with the dead time of the counting electronics, during which no additional detection can be registered (marked by crosses). To achieve both high PIE and throughput, an optimal frame size T_f and time bin duration τ should be chosen to fully utilize the available photon detection resource.

and entanglement degradation [6, 7], but it is still unknown whether these protocols can outperform existing QKD systems in terms of overall secure key rates and transmission distances.

One approach to significantly increase entanglement-based QKD throughput is to encode multiple bits per photon pair in their times of arrival, similar to the way pulse-position modulation is used in classical optical communication under photon-starved conditions. To date, most QKD protocols use binary encoding, corresponding to a key capacity, which we also call photon information efficiency (PIE), of $\leqslant 1$ bit per photon. Fundamentally this limits the secure bit rate to at most the photon flux reaching the receiver. Actual rates would be further reduced due to sifting, error correction, privacy amplification and other post-processing overheads for secure bit extraction. Therefore, to achieve higher throughput at a given photon flux (for a specific source and channel loss), increasing the bit-per-photon capacity or PIE to greater than one would provide a substantial improvement to QKD secure key rates. An obvious choice for high dimensional encoding is the arrival times of single photons, because of their excellent preservation after propagation through low-loss, minimal dispersion fiber, and their convenient detection with high timing resolution. Time binning the random arrival of a coincident photon pair in an N-bin time frame yields a symbol comprising $\log_2 N$ bits, as depicted in figure 1. This approach can provide a sizable benefit to the throughput of a QKD system in the photon-starved regime in which the (average) interval between photon detection events is much longer than the timing resolution of the detectors. As illustrated in figure 1, typical QKD systems operate under photon-starved conditions: photon pairs generated by SPDC suffer propagation losses and are detected at low rates, and single-photon detectors have long recovery times after each detection event [8]. In photon-starved situations, high-dimensional encoding with a frame size of N time bins yields a raw throughput given approximately by $R \propto \min\,[R_{\rm ph},\, R_{\rm det}] \cdot \log_2 N$, i.e., $\sim\log_2 N$ times better than binary QKD, where $R_{\rm ph}$ is the photon flux at the receiver and $R_{\rm det}$ is the maximum count rate of single-photon detectors.

Recently, there has been great interest to exploit the very high entropy (as many as $\approx$20 bits per photon from 10^6 temporal modes) of a time–energy entangled photon pair produced by continuous-wave (CW) SPDC for high-rate QKD [9–13]. But its implementation with proven security for multiple bits per photon has been a longstanding challenge. Proposals for such time–energy entanglement-based QKD have suggested security measures based on multiple Franson interferometers [10], Franson and conjugate-Franson interferometers [11], time-to-frequency conversion [12], dispersive optics [13], and recirculating Mach–Zehnder interferometers [14]. These different security checks highlight the complexity of implementing high-dimensional QKD (HDQKD) protocols. Recently, security proofs against collective attacks have been established for HDQKD based on Franson and conjugate-Franson interferometers [11] and on dispersive optics [13], using estimates of Alice and Bob's time-frequency covariance matrix (TFCM) to bound Eve's Holevo information. In particular, [11] shows that it is feasible to use a single Franson interferometer [15] to secure time–energy entanglement-based HDQKD. We should note that previous experiments involving Franson interferometry were limited to either demonstrations of immunity against individual attacks or feasibility studies of isolated components [16, 17]. As a result, they do not represent QKD implementations in which the security against collective attacks can be assured and the corresponding secure key rates determined.

In this work we report an experimental demonstration of photon-efficient HDQKD based on time–energy entanglement whose security against collective Gaussian attacks is achieved through a single Franson interferometer with near-unity visibility performance that does not degrade with fiber propagation loss. Eve's Holevo information is bounded by precise frequency correlation measurements via non-locally dispersion-canceled Franson quantum interference capable of operation over long fiber links. Using highly efficient WSi superconducting nanowire detectors [18] and an efficient error correction code designed specifically for high-dimensional encoding with tolerance to high symbol error rates (SERs), our HDQKD protocol yielded

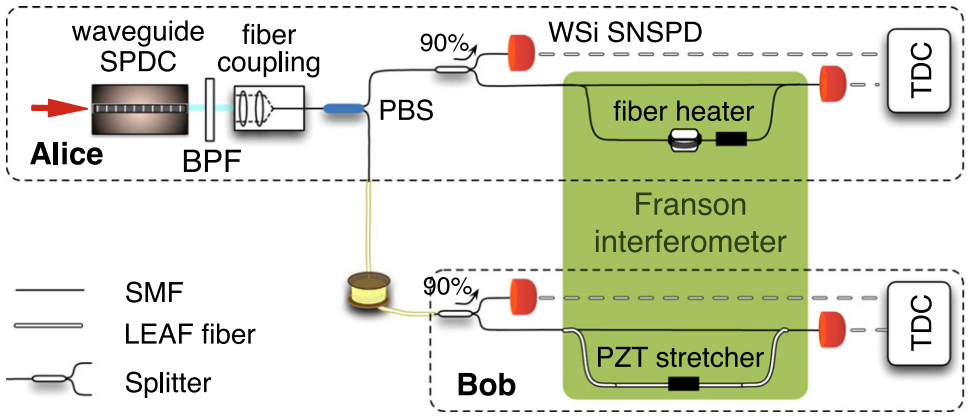

Figure 2. Schematic of entanglement-based HDQKD setup. Orthogonally polarized outputs from SPDC source at 1560 nm are separated using a polarizing beam splitter. Fiber beam splitters with a 90:10 ratio are used for key generation and Franson measurements. BPF: 10 nm bandpasss filter; PBS: polarizing beam splitter; SMF: single-mode fiber; TDC: time-to-digital converter.

up to 8.7 bits per photon coincidence if secure key capacity is maximized. When optimized for throughput, we obtained a secure key rate of 2.7 (7.0) Mbit s^{-1} through 20 km (100 m) of single-mode fiber with a PIE of 6.9 (7.4) bits per photon coincidence. These secure key rates significantly surpass previous entanglement-based QKD systems using polarization or time-bin entangled qubits. Our results demonstrate a viable approach to high-rate QKD using practical photonic entanglement and single-photon detection technologies.

2. QKD protocol

The photon-efficient HDQKD protocol is shown schematically in figure 2. The system uses time–energy entangled photon pairs generated from a CW SPDC source in Alice's possession. Alice sends one photon from each entangled pair to Bob through an optical fiber that is subject to Eve's attack, and retains the conjugate photon for measurements. Alice and Bob independently measure the photon arrival times at a resolution τ that defines a time bin. Both parties share a publicly synchronized clock to align their time bins, and they use N consecutive bins to form a time frame. For each frame, Alice and Bob randomly choose to measure the arrival time bin position of the photon either directly, for extracting a symbol of $k = \log_2 N$ bits, or after passing through their respective arms of the Franson interferometer, for establishing security. After the use of this quantum channel, Alice and Bob post-select frames that contain exactly one detection event by each party, and proceed to perform error correction and privacy amplification.

The secure PIE is given by $\Delta I_{AB} = \beta I_{AB} - \chi^E - \Delta_{FK}$ in bits per coincidence, where β is the reconciliation efficiency, I_{AB} is Alice and Bob's Shannon information (SI), χ^E is Eve's Holevo information for collective Gaussian attacks in the asymptotic limit of infinitely long keys [4], and Δ_{FK} accounts for penalties due to the finite key length [21, 22]. Error correction performed on the raw k-bit symbols is implemented using a custom code developed by Zhou *et al* [19] for large-alphabet QKD protocols. The code uses a layered scheme that successively applies low-density parity check (LDPC) binary error correction on all bit layers of the symbols, and has high reconciliation efficiency β even at high SERs.

3. Security of HDQKD using a single Franson interferometer

To bound Eve's Holevo information, Alice and Bob monitor the visibility V of a single Franson interferometer. It is long established that Franson quantum interference provides a measure of time–energy entanglement quality, and is routinely used as an equivalent Clauser–Horne–Shimony–Holt (CHSH) form of Bell's inequality measurement [23] for time-bin entanglement (a discrete case of time–energy entanglement with $N = 2$ in which a photon arrives either in an early or late time bin). However, it is less explicitly understood that the Franson visibility is directly linked to the two-photon frequency anti-correlation via $V = \langle \cos[(\hat{\omega}_A - \hat{\omega}_B)\Delta T] \rangle$ [15], where ΔT is the propagation delay between the interferometer's long and short paths, $\hat{\omega}_A$ ($\hat{\omega}_B$) is the frequency operator measuring the zero-mean detuning of Alice's (Bob's) photon at frequency $\omega_p/2 + \omega_A$ ($\omega_p/2 - \omega_B$), and ω_p is the SPDC pump frequency. Here we consider the interference visibility of a single photon pair emitted by Alice's source. Following the proof of lemma 1 in [11], we have the

following inequalities according to Taylor-series expansion,

$$V^{\mathrm{th}} = \left\langle \cos\left[\left(\hat{\omega}_{\mathrm{A0}} - \hat{\omega}_{\mathrm{B0}}\right)\Delta T\right]\right\rangle \geqslant 1 - \left\langle \left(\hat{\omega}_{\mathrm{A0}} - \hat{\omega}_{\mathrm{B0}}\right)^2\right\rangle \Delta T^2/2, \tag{1}$$

$$V = \left\langle \cos\left[\left(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}}\right)\Delta T\right]\right\rangle \leqslant 1 - \left\langle \left(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}}\right)^2\right\rangle \Delta T^2/2 + \left\langle \left(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}}\right)^2\right\rangle^2 \Delta T^4/8, \tag{2}$$

where V^{th} is the theoretical Franson visibility for an unperturbed entangled pair assuming a perfect measurement apparatus, $\langle(\hat{\omega}_{\mathrm{A0}} - \hat{\omega}_{\mathrm{B0}})^2\rangle$ is the undisturbed frequency correlation from the source (determined by the pump laser spectral linewidth), and a Gaussian attack has been assumed. Combining equations (1) and (2) gives

$$\left\langle \left(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}}\right)^2\right\rangle^2 - \frac{4}{\Delta T^2}\left\langle \left(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}}\right)^2\right\rangle + \frac{8}{\Delta T^4}\left(V^{\mathrm{th}} - V + \left\langle \left(\hat{\omega}_{\mathrm{A0}} - \hat{\omega}_{\mathrm{B0}}\right)^2\right\rangle \Delta T^2/2\right) \geqslant 0. \tag{3}$$

For the two distinct roots of the inequality (3), the root with a higher value results in $\langle(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}})^2\rangle$ being orders of magnitude larger than the experimental values, thus it is rejected. Using the lower value root as an upper bound, the inequality (3) reduces to

$$\left\langle \left(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}}\right)^2\right\rangle \leqslant \frac{2}{\Delta T^2}\left(1 - \sqrt{1 - 2\left(V^{\mathrm{th}} - V + \left\langle \left(\hat{\omega}_{\mathrm{A0}} - \hat{\omega}_{\mathrm{B0}}\right)^2\right\rangle \Delta T^2/2\right)}\right) \approx \frac{2}{\Delta T^2}\left(V^{\mathrm{th}} - V + \left\langle \left(\hat{\omega}_{\mathrm{A0}} - \hat{\omega}_{\mathrm{B0}}\right)^2\right\rangle \Delta T^2/2\right), \tag{4}$$

where we consider $V^{\mathrm{th}} - V \ll 1$ and $\langle(\hat{\omega}_{\mathrm{A0}} - \hat{\omega}_{\mathrm{B0}})^2\rangle \Delta T^2 \ll 1$. Rearranging the last term in the parentheses on the right-hand side and assuming, with no access to Alice's photon, Eve's interaction could only disturb Bob's variance $\langle\hat{\omega}_{\mathrm{B}}^2\rangle$ and the frequency covariance $\langle\hat{\omega}_{\mathrm{A}}\hat{\omega}_{\mathrm{B}}\rangle$, we obtain the following inequality to bound the total change in the mean-squared frequency difference $\langle(\hat{\omega}_{\mathrm{A}} - \hat{\omega}_{\mathrm{B}})^2\rangle$:

$$\Delta\langle\hat{\omega}_{\mathrm{B}}^2 - 2\hat{\omega}_{\mathrm{A}}\hat{\omega}_{\mathrm{B}}\rangle \leqslant 2\left(V^{\mathrm{th}} - V\right)/\Delta T^2. \tag{5}$$

The security analysis then follows the well-established proofs for Gaussian CV-QKD protocols based on the optimality of Eve's Gaussian collective attack for a given TFCM Γ [11, 24]. To start, we consider the undisturbed state of one signal-idler photon pair generated from CW SPDC

$$|\phi\rangle = \int\int \mathrm{d}t_{\mathrm{A}}\,\mathrm{d}t_{\mathrm{B}}\, \mathrm{e}^{-\frac{\left(t_{\mathrm{A}}+t_{\mathrm{B}}\right)^2}{16\sigma_{\mathrm{coh}}^2}} \mathrm{e}^{-\frac{\left(t_{\mathrm{A}}-t_{\mathrm{B}}\right)^2}{4\sigma_{\mathrm{cor}}^2}} \mathrm{e}^{-\mathrm{i}\omega_{\mathrm{p}}\frac{\left(t_{\mathrm{A}}+t_{\mathrm{B}}\right)}{2}} |t_{\mathrm{A}}\rangle_{\mathrm{A}}|t_{\mathrm{B}}\rangle_{\mathrm{B}}, \tag{6}$$

where σ_{coh} is the pump coherence time, and σ_{cor} is the biphoton correlation time. The two photons are correlated in the time domain, and anti-correlated in the frequency domain where time and frequency form a pair of conjugate bases. We thus introduce the arrival-time operator $\hat{t}_m$ and the frequency operator $\hat{\omega}_n$, where $m, n \in \{A, B\}$. The state $|\omega\rangle_{\mathrm{A}}$ ($|\omega\rangle_{\mathrm{B}}$) represents a single photon of the signal (idler) at frequency $\omega_{\mathrm{p}}/2 + \omega$ ($\omega_{\mathrm{p}}/2 - \omega$), so that with this convention the detunings, ω, from $\omega_{\mathrm{p}}/2$ are correlated, rather than anti-correlated. The TFCM for the above state is then

$$\Gamma^0 = \begin{bmatrix} \gamma_{\mathrm{AA}}^0 & \gamma_{\mathrm{AB}}^0 \\ \gamma_{\mathrm{BA}}^0 & \gamma_{\mathrm{BB}}^0 \end{bmatrix}, \tag{7}$$

where

$$\gamma_{\mathrm{AA}}^0 = \gamma_{\mathrm{BB}}^0 = \begin{bmatrix} \frac{1}{4}\sigma_{\mathrm{cor}}^2 + \sigma_{\mathrm{coh}}^2 & 0 \\ 0 & \frac{1}{4\sigma_{\mathrm{cor}}^2} + \frac{1}{16\sigma_{\mathrm{coh}}^2} \end{bmatrix},$$
$$\gamma_{\mathrm{AB}}^0 = \gamma_{\mathrm{BA}}^0 = \begin{bmatrix} -\frac{1}{4}\sigma_{\mathrm{cor}}^2 + \sigma_{\mathrm{coh}}^2 & 0 \\ 0 & \frac{1}{4\sigma_{\mathrm{cor}}^2} - \frac{1}{16\sigma_{\mathrm{coh}}^2} \end{bmatrix}. \tag{8}$$

Eve's presence disturbs Alice and Bob's initial TFCM to become

$$\gamma_{AA} = \gamma_{AA}^{0},$$
$$\gamma_{AB} = \gamma_{BA} = \begin{bmatrix} 1-\eta_t & 0 \\ 0 & 1-\eta_\omega \end{bmatrix} \gamma_{AB}^{0},$$
$$\gamma_{BB} = \begin{bmatrix} 1+\epsilon_t & 0 \\ 0 & 1+\epsilon_\omega \end{bmatrix} \gamma_{BB}^{0}, \tag{9}$$

where $\{\eta_t, \eta_\omega\}$ denotes the loss in time and frequency correlation, and $\{\epsilon_t, \epsilon_\omega\}$ denotes the excess noise in Bob's photon. The measured Franson visibility restricts the possible $\eta_\omega, \epsilon_\omega$ values via inequality (5). We note that any disturbance in the biphoton time correlation or Bob's arrival time variance (reflected by η_t and ϵ_t) cannot be bounded by our Franson interference measurement. Nevertheless, such disturbance by Eve does not afford her any benefit in gaining symbol information encoded in the time basis, thus it has negligible impact on χ^{E}. To ensure stronger security, we therefore take the mean-squared time arrival difference $\langle(\hat{t}_A - \hat{t}_B)^2\rangle$ to be square of the detector timing jitter (beyond which Eve's intrusion would have been readily detected by Alice and Bob), and $\langle \hat{t}_B^2 \rangle$ to be the time variance integrated over the entire frame duration.

For a given TFCM, a Gaussian attack maximizes Eve's Holevo information by assuming that she purifies the state to a joint Gaussian state between Alice, Bob and Eve. The Holevo information χ_Γ for covariance matrix Γ is

$$\chi_\Gamma = S\left(\hat{\rho}_E\right) - \int \mathrm{d}t\; p\left(t_A\right) S\left(\hat{\rho}_{E|t_A}\right), \tag{10}$$

where $S(\hat{\rho}) = -\mathrm{Tr}\,[\hat{\rho}\,\log_2(\hat{\rho})]$ is the von Neumann entropy of the quantum state $\hat{\rho}$. The inequality (5) constrains the set, $\mathcal{M}$, of physically allowed TFCMs with corresponding frequency variance and covariance elements. An upper bound on Eve's Holevo information is then calculated by maximizing $\chi_\Gamma = S(\hat{\rho}_E) - S(\hat{\rho}_{E|t_A}) = S(\hat{\rho}_{AB}) - S(\hat{\rho}_{B|t_A})$ over all TFCMs in $\mathcal{M}$, i.e.,

$$\chi^{E} = \sup_{\Gamma \in \mathcal{M}} \{\chi_\Gamma\}, \tag{11}$$

where $\hat{\rho}_{E|t_A}$ denotes the Eve's quantum state conditioned on Alice's arrival-time measurement, and we assume Eve, Alice, and Bob share a pure joint-Gaussian state.

Secret keys can in principle be encoded in both time and frequency conjugate bases. Keys encoded in the photon-arrival-time bins are secured by Franson interferometry, which measures two-photon frequency correlation. Additional bits can be encoded in multiple frequency bins that can be secured by the newly proposed conjugate-Franson interferometer [11], which measures the time correlation between photon pairs. However, frequency-bin encoding necessarily requires dense wavelength-division multiplexing (DWDM) components that incur substantial insertion loss given today's technology. (For instance, a typical four-channel 50 GHz DWDM filter has typical excess insertion loss of ≈3 dB, which leads to a 6 dB reduction in coincidence rates but gains only two extra bits in the most ideal scenario). Hence, in this work we choose an HDQKD implementation that favors a higher key rate and a simpler setup without DWDM by encoding only in the photon arrival times and securing it with a Franson interferometer. Here we should point out that in a TFCM, there are also time-correlation elements (e.g., $\langle(\hat{t}_A - \hat{t}_B)^2\rangle$) that could be disturbed by Eve's intrusion. Nevertheless, we find that the change in these elements has a negligible impact on χ^{E}, because Eve's attack on time correlations only gives her information encoded in frequency and therefore does not yield any knowledge about keys that are encoded in arrival time.

The ability to bound Eve's Holevo information, and thus to secure the multiple bits encoded in a coincident photon pair, depends critically on the measured Franson visibility by Alice and Bob. Although high visibility up to 96.5% has been routinely reported in prior Franson experiments [25], our numerical calculation shows that to bound $\chi^{E} \leqslant 1.0$ bit, visibility (without background subtraction) exceeding 99.5% is required (assuming $\Delta T = 5$ ns, pump laser linewidth of 1 MHz, SPDC phase matching bandwidth of 250 GHz). This result is in qualitative agreement with [10], which claimed that a 97% Franson visibility would lead to leakage of 5 out of 10 bits of information to Eve. To achieve and maintain the required near-unity visibility after long-distance fiber distribution of the photon pairs, our experiment used non-locally dispersion-canceled Franson interferometry, which we recently demonstrated to show a visibility of 99.6% [26]. It was pointed out in [26] that non-local dispersion compensation recovers the degradation of visibility due to group-velocity mismatch within each arm of the interferometer, and the visibility is not affected by any dispersion along the fiber connecting the source to Alice/Bob. Therefore, neglecting the detector dark counts, near-unity Franson visibility can be maintained, in principle, at arbitrarily long QKD distance.

4. Experimental implementation

The experimental setup in figure 2 was carefully optimized for achieving photon-efficient secure key distribution. We used a type-II phase-matched, single-spatial-mode periodically poled potassium titanyl phosphate (PPKTP) waveguide to generate high quality time–energy entangled photon pairs at 1560 nm with ≈80% spectral-spatial extraction efficiency into a single-mode fiber [27]. The pump coherence time was ≈250 ns, measured using a setup similar to self-homodyning but with the fiber loop path difference less than the laser coherence time so that only the intrinsic laser frequency noise was measured. For a crystal length of 15.6 mm, the SPDC phase-matching bandwidth was measured to be 1.6 nm (250 GHz), corresponding to a biphoton correlation time of ≈2 ps, with a source brightness of 10^7 pairs per second per mW of pump. The orthogonally-polarized photon pairs were separated with a fiber polarizing beam splitter, sending the signal photons to Bob through a single-mode fiber. In the experiment we used WSi superconducting nanowire single-photon detectors (SNSPDs) [18] with ≈90% detection efficiency at 1560 nm, dark-count rates of ≈1000 counts per second, an average timing jitter of ≈80 ps full-width at half-maximum, and a maximum count rate of $\approx 1.5 \times 10^6$ counts per second. A total of six WSi SNSPDs were used: two were used for the Franson-interferometric security check, and the other four detectors for key generation. To mitigate the long reset times of WSi SNSPDs in the key generation portion of the experiment, Alice (and Bob) used a passive 50:50 beam splitter to distribute incident photons equally between two WSi SNSPDs (not shown in figure 2), and their data were interleaved. Typical singles and coincidence count rates were 2–3 million, and 700 000 to 1 million counts per second, respectively.

To achieve higher key capacity, it is generally desirable to use small time bins, long frame durations and large Franson differential delays. In actual implementation, the optimal operating parameters are determined by factors including the pump coherence time, biphoton correlation time, and the detector timing jitter performance. Given the timing jitter of WSi SNSPDs being much larger than the SPDC biphoton correlation time, we chose a time bin size of 80 ps throughout our experiments. Accordingly, the 250 ns pump coherence time leads to an expected optimal frame size on the order of $N = 1000$ bins per frame. Large Franson differential delays up to 250 ns can be implemented in principle. However, in practice, we used a short delay of a few ns in the interferometer that allowed us to achieve excellent long-term phase stability.

As pointed out in the previous section, it is essential to have high visibility Franson interferometry in order to tightly bound Eve's Holevo information. Non-local dispersion cancellation [26] was incorporated into our fiber-based Franson interferometer by applying a negative differential dispersion (using low dispersion LEAF fiber) in Bob's arm of the interferometer to achieve near-unity Franson visibilities. The long-short fiber length difference of the Franson interferometer corresponded to a $\Delta T = 9.5$ ns differential delay. For long-term phase stability, we enclosed the interferometer in a multilayered thermally-insulated box with active temperature stabilization. Also, the fiber length differences in the two arms of the Franson interferometer were fine tuned to match their differential delays to within 1 ps by incorporating an additional closed-loop temperature control on one of the fiber paths. The variable phase shift of each arm was set by a piezoelectric transducer fiber stretcher. We implemented the random choice of measurements between key generation and Franson security check with a 90:10 fiber beam splitter. This asymmetric configuration maximizes the system key throughput while ensuring sufficient coincident count rates to establish Franson security. Detection events were time stamped by Alice and Bob with time-to-digital converters (PicoQuant HydraHarp 400). For long-distance QKD measurements, we inserted two spools of fiber with matched length L between the source and Alice and Bob's detectors to evaluate QKD performance at $2L$ distance. This matched-fiber configuration avoids the technical difficulty of aligning two timing records that are >10 μs apart. Without the matched fibers, Alice and Bob's detectors were separated by about 100 m of fiber.

After the quantum communication, Alice and Bob's raw timing data at a resolution of 1 ps were downloaded from the time-to-digital converters after every QKD session of 1 s, and were first parsed into $\log_2 N$ bit symbols for each coincident frame that had one detection by each party. Software error correction then proceeded with blocks of 4000 symbols each, resulting in an output stream of error-corrected symbols. After calculating the secure PIE, corrected symbols from the 1 s QKD sessions were fed into the privacy amplification algorithm to obtain the final keys. The key length for each session varied for different frame size N, but was on the order of 10^6 symbols. The information loss due to the finite key length Δ_{FK} takes into account the finite probabilities that error correction (ϵ_{EC}), privacy amplification (ϵ_{PA}), smooth min-entropy estimation ($\bar{\epsilon}$), or security parameter estimation (ϵ_{PE}) fail [22]. The finite key penalties due to error correction, privacy amplification and smooth min-entropy estimation were calculated in the same way as in [22], with $\epsilon_{\mathrm{EC}} = \epsilon_{\mathrm{PA}} = \bar{\epsilon} = 10^{-10}$ for optimal result. For the estimation of $\chi^{\mathrm{E}}_{\mathrm{FK}}$, Eve's Holevo information with finite key consideration, Alice and Bob calculate their normalized frequency correlation from measured Franson visibilities via equation (5), which has a χ^2 distribution:

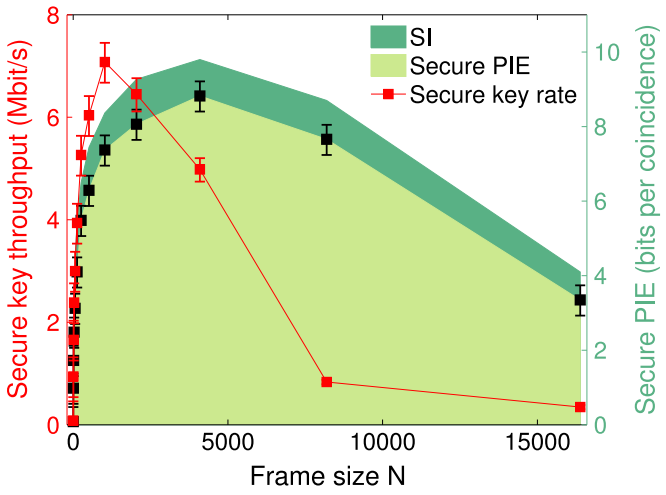

Figure 3. Entanglement-based HDQKD measurement results at various frame sizes. Plots of secure PIE (right axis) and the theoretical Shannon information (SI) show a gap that reflects the error correction efficiency and the effectiveness of using Franson visibility to bound Eve's Holevo information. Secure key throughputs (left axis) show a peak at $N = 1024$ which does not coincide with the location of the peak PIE. The error bars originate from experimental uncertainties of the Franson visibility measurement, and they are based on one standard deviation.

$$(m-1)\frac{\left\langle\left(\hat{\omega}_{\mathrm{A}}-\hat{\omega}_{\mathrm{B}}\right)^2\right\rangle}{\left\langle\left(\hat{\omega}_{\mathrm{A0}}-\hat{\omega}_{\mathrm{B0}}\right)^2\right\rangle}\sim\chi^2\left(1-\epsilon_{\mathrm{PE}},\,m-1\right), \tag{12}$$

where m is the number of Franson visibility measurements taken in each QKD session. An upper bound on $\langle(\hat{\omega}_{\mathrm{A}}-\hat{\omega}_{\mathrm{B}})^2\rangle$ with confidence interval $1-\epsilon_{\mathrm{PE}}$ is then given by:

$$\left\langle\left(\hat{\omega}_{\mathrm{A}}-\hat{\omega}_{\mathrm{B}}\right)^2\right\rangle_{\max}=\left\langle\left(\hat{\omega}_{\mathrm{A0}}-\hat{\omega}_{\mathrm{B0}}\right)^2\right\rangle+\frac{2}{\sqrt{m}}\,\mathrm{erf}^{-1}\left(1-\epsilon_{\mathrm{PE}}\right)\left\langle\left(\hat{\omega}_{\mathrm{A}}-\hat{\omega}_{\mathrm{B}}\right)^2\right\rangle. \tag{13}$$

This upper bound is then used to calculate the worst case χ^E and the most pessimistic secure PIE. In our experiment, $m = 100$, and we choose $\epsilon_{\mathrm{PE}} = 10^{-5}$. The overall failure probability of the entire protocol is thus $\epsilon_s = \epsilon_{\mathrm{EC}} + \epsilon_{\mathrm{PA}} + \bar{\epsilon} + \epsilon_{\mathrm{PE}} \approx 10^{-5}$. All data post-processing, if desired, can be implemented using a field programmable gate array to minimize the latency in key extraction.

5. Results

The high dimensional encoding scheme offers great flexibility to adjusting the dimensionality in order to optimize for the highest throughput. Without any change in hardware implementation, the frame size can be chosen in the data post-processing step by parsing the raw timing records into the desired symbol length [20]. In this way, secure key throughput can be easily optimized as operating conditions, such as transmission or fiber-coupling losses, change. For our setup without the matched fiber spools, figure 3 shows the secure PIE in bits per photon coincidence and the secure key rate in bits per second for different frame size N at a constant mean pair generation $\alpha = 0.03\%$ per time bin of 80 ps duration. We plot both the final secure PIE (filled black squares) and the theoretical SI (right axis of figure 3), with the gap between them reflecting the error correction efficiency and the effectiveness of using Franson visibility to bound Eve's Holevo information. We see that the secure PIE rises sharply as N increases, peaking at 8.7 bits per coincidence for $N = 4096$, where the mean pair generation was just over one pair per time frame. We note that for $N = 4096$ the frame duration of ≈ 330 ns is comparable to the average inter-arrival times between detection events produced by Alice's (and Bob's) pair of WSi SNSPDs. For longer time frames, the PIE decreases due primarily to the larger number of multi-pair events.

The more useful metric of the secure key rates (red filled squares) as N increases is also shown in figure 3 (left axis). As expected, the throughput rises sharply as the key capacity also rises rapidly at lower N. The peak secure key rate of 7.0 Mbit s^{-1} is reached at $N = 1024$ (10 bits per frame) where the secure PIE is 7.4 bits per coincidence. The peak key rate does not occur at the same frame size as that for the peak PIE. This is expected because the secure rate also depends on the number of frames per second, which decreases by a factor of two with each bit that is added to the symbol length of the frame. Indeed, one observes that the key rates drop rapidly for

Table 1. Operating parameters and QKD results for our HDQKD protocol, entanglement-based BBM92 protocol, and decoy-state BB84 protocol.

Parameter	HDQKD	BBM92 [5]	Decoy-BB84 [30]
α	0.03%	≈5%	42.5%
$N(\log_2 N)$	1024 (10)	2 (1)	2 (1)
SER	39.6%	3.2%	4.26%
βI_{AB} (PIE)	7.9	Unknown	Unknown
χ^{E}_{FK}	0.52	Unknown	Unknown
Secure PIE	7.38	≈0.35	0.26
Secure bit s^{-1}	7.0 M	14.5 k	1.09 M (at 50 km)

longer frame sizes. The ability to use software in the processing step to decide on the frame size makes it possible to dynamically optimize the system key rates as operating conditions change.

In table 1 we summarize the optimized throughput performance of our HDQKD protocol and compare it with state-of-the-art protocols. For our protocol, $\alpha = 0.03\%$ with a bin duration $\tau = 80$ ps. The total symbol errors indicated in table 1 consist of a constant amount of local errors (≈30%) due to detector timing jitter, plus uniform errors (<10%) due to the increase in the multi-pair probability for a frame that occurs with increased N. In examining the details of the error correction process we have identified the local errors as coincidences that occurred in neighboring time bins. They appear commonly as flipping a symbol's least significant bit, thus these local errors have a small effect on the extractable SI. The uniform errors are the main limiting factor to SI, especially at very large N. Because of high encoding dimensionality, our protocol can tolerate much higher symbol error rate than conventional binary QKD protocols can [29]. Our layered LDPC code performed error correction with high efficiency for all symbol lengths, ranging from $\beta = 83.8\%$ for $N = 2$ to 91.2% for $N = 16\,384$. The measured raw Franson visibilities (without dark-count subtraction) at all frame sizes were consistently at $V \geqslant 99.8\%$ as a result of complete non-local dispersion cancellation, leading to a tightly bounded $\chi^{E}_{FK} \leqslant 0.52$ bits per coincidence including the finite key length effect. To reduce Eve's information to an arbitrarily small amount, privacy amplification was applied using low-density random matrices [28]. Table 1 compares our entanglement-based HDQKD implementation with the state-of-the-art implementation of BBM92 protocol that uses binary encoding ($N = 2$) based on polarization entanglement to achieve a secure key rate of 14.5 kbit s^{-1} [5]. By using high dimensional encoding, efficient single-photon detection, and highly efficient error correction, our results show an increase in PIE by a factor of >20 and in QKD throughput by a factor of 500.

We also performed the HDQKD measurements ($\alpha = 0.03\%$ and $N = 1024$) at separations of 5, 10 and 20 km of standard optical fiber between Alice and Bob, obtaining the results shown in figure 4. Here, the total separation $2L$ was implemented by a pair of matched fiber of length L, each connecting Alice's or Bob's detector to the source. We assume that the fiber linking Alice's detector and the source is not accessible to Eve, thus mimicking the QKD configuration in figure 2 in which Alice possesses the source and the total distance to Bob equals the sum of the fiber lengths used in the experiment. We were able to maintain a minimum secure PIE (green filled circles) of 6.9 bits per coincidence at all three distances, which compares well with the 7.4 bits per coincidence that we obtained without the additional fiber. The PIE results clearly show no key capacity degradation over long distance fiber transmission, because we were able to maintain near-unity Franson visibility at long distances, but longer acquisition times were needed due to losses. In key generation, we observed a broadening of the two-photon coincidence measurements to ≈250 ps caused by chromatic dispersion in the 20 km of fiber. However, this broadening only contributed to increased local errors (in each symbol's least significant bit) that were reconciled efficiently with our error correction code. Moreover, it had no effect on the Franson measurement results because Franson visibility is only sensitive to the differential dispersion between the long and short paths inside each interferometer arm [26]. The secure-key throughputs (red filled squares) at different fiber transmission distances, plotted in figure 4 (left axis), show the decreasing key rates that are expected with fiber transmission loss. At 20 km we obtained a secure key rate of 2.7 Mbit s^{-1}, which compares favorably with the highest reported decoy-state QKD rate of over 1 Mbit s^{-1} at 50 km [30], as shown in table 1. Note that the decoy-state protocol does not use entangled photons, thus it is not compatible with the quantum repeater architecture that can extend quantum communications over much longer distances [3]. Lastly, it is worth mentioning that at currently measured fiber distances, the detector dark counts have negligible contribution to the accidental coincidences, thus affecting neither the Franson visibility nor the SER. With increasing fiber transmission loss, we expect the detector dark counts to eventually become the limiting factor to the secure key rate. Dark counts will begin to degrade the Franson visibility when Bob's singles rate becomes comparable to his detector's dark-count rate. Neglecting coupling losses and using our source's singles

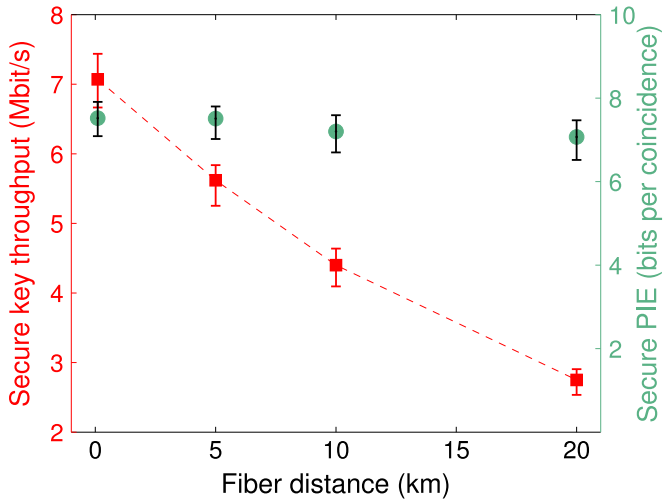

Figure 4. Secure PIE and throughput of HDQKD at various fiber distances. The time–energy entangled photon source was placed at equal distance from Alice and Bob, and secure PIE and QKD throughput were measured for various fiber separations between Alice and Bob. Measurements were made to optimize throughput with a frame size of 1024, bin duration of 80 ps, and mean pair generation of 0.03% per bin. The error bars are based on one standard deviation of the Franson visibility measurement.

rate, this will occur at a telecom-fiber distance of 175 km. Dark counts will increase the SER at shorter distances, and they will increase the proportion of harder-to-correct uniform errors relative to local errors. Thus 175 km is an optimistic upper bound on the maximum range of our protocol.

6. Conclusion

We have demonstrated a photon-efficient QKD protocol using high dimensional encoding of time–energy entangled photons with security against collective Gaussian attacks. High dimensional encoding in the photon arrival times is particularly advantageous under typical photon-starved conditions in which the rate of detection events is much lower than the photon generation rate, because of propagation losses, and the long recovery times of available single-photon detectors. We achieved a secure key capacity of as high as 8.7 bits per photon coincidence, indicating that much can be gained with high dimensional encoding relative to the binary encoding used in more conventional QKD protocols. When we optimized for key rates we obtained a peak QKD throughput of 7.0 Mbit s^{-1} with a secure PIE of 7.4 secure bits per coincidence at 100 m of fiber separation. With an additional fiber length of 20 km, we were able to maintain a high PIE of 6.9 bits per coincidence without degradation due to long distance fiber transmission and obtain a secure key rate of 2.7 Mbit s^{-1}. We achieved the record key capacity and throughput for an entanglement-based QKD system because of four principal factors: a PPKTP waveguide SPDC source with high extraction efficiency into a single-mode fiber; highly efficient WSi SNSPDs; Franson interferometry with near-unity visibility that does not degrade with fiber transmission loss; and efficient error correction coding that can tolerate high SERs.

The security against collective Gaussian attacks is based on a single Franson interferometer implemented with non-local dispersion cancellation in order to achieve near-unity visibility for bounding Eve's Holevo information. However, we are unable to theoretically show that the Franson interferometer alone is sufficient to provide security against non-Gaussian attacks. To be secure against the most general collective attacks would require the additional use of a conjugate-Franson interferometer, which is also needed if encoding of frequency bits is implemented [11]. Although a single Franson interferometer provides less comprehensive security, its simplicity allows for easy implementation in practical HDQKD systems. The simple configuration of our entanglement-based HDQKD protocol and the ability to change the frame size and bin duration in the processing step using software make it a robust QKD system to deploy with substantial performance improvement over today's binary encoded QKD technology. The use of entangled photons in the current HDQKD system is compatible with and of potential interest to future implementation of quantum repeater technology. Multi-bit encoding of time–energy entangled photons could be utilized in quantum repeater schemes with multi-mode capability [31], especially if high PIE can be maintained over long distances. We note that a quantum memory with a single photon storage capacity up to 64 temporal modes has been demonstrated using the atomic frequency combs protocol [32]. Future progress in quantum memory and repeater technology might lead to efficient relays for large-alphabet time–energy entanglement.

Acknowledgments

The authors acknowledge technical discussions with Yuval Kochman. This work was supported in part by the DARPA InPho program under Army Research Office Grant No. W911NF-10-1-0416. Part of this work was carried out at the Jet Propulsion Laboratory, under contract with the National Aeronautics and Space Administration.

References

[1] Bennett C and Brassard G 1984 Quantum cryptography: public-key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India* (New York: IEEE) 175–9
[2] Ekert A 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661
[3] Briegel H J, Dür W, Cirac J I and Zoller P 1998 Quantum repeaters: the role of imperfect local operations in quantum communication *Phys. Rev. Lett.* **81** 5932
[4] Grosshans F, van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 Quantum key distribution using Gaussian-modulated coherent states *Nature* **421** 238–41
[5] Treiber A, Poppe A, Hentschel M, Ferrini D, Lorünser T, Querasser E, Matyus T, Hübel H and Zeilinger A 2009 A fully automated entanglement-based quantum cryptography system for telecom fiber networks *New J. Phys.* **11** 045013
[6] Franson J D 2011 Sensitivity of entangled photon holes to loss and amplification *Phys. Rev.* A **81** 043831
[7] Zhang Z, Tengner M, Zhong T, Wong F N C and Shapiro J H 2013 Entanglement's benefits survives an entanglement-breaking channel *Phys. Rev. Lett.* **111** 010501
[8] Migdall A, Polyakov S V, Fan J and Bienfang J C (ed) 2013 Single-Photon Generation and Detection: Physics and Applications (*Experimental Methods in the Physical Sciences* vol 45) (New York: Academic)
[9] Ali Khan I and Howell J C 2006 Experimental demonstration of high two-photon-time–energy entanglement *Phys. Rev.* A **73** 031801(R)
[10] Brougham T, Barnett S M, McCusker K T, Kwiat P G and Gauthier D J 2013 Security of high-dimensional quantum key distribution protocols using Franson interferometers *J. Phys. B: At. Mol. Opt. Phys.* **46** 104010
[11] Zhang Z, Mower J, Englund D, Wong F N C and Shapiro J H 2014 Unconditional security of time–energy entanglement quantum key distribution using dual-basis interferometry *Phys. Rev. Lett.* **112** 120506
[12] Nunn J, Wright L, Söller C, Zhang L, Walmsley I A and Smith B J 2013 Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion *Opt. Express* **21** 15959–73
[13] Mower J, Zhang Z, Desjardins P, Lee C, Shapiro J H and Englund D 2013 High-dimensional quantum key distribution using dispersive optics *Phys. Rev.* A **87** 062322
[14] Brougham T and Barnett S M 2013 Mutually unbiased measurements for high-dimensional time-bin based photonic states *Europhys. Lett.* **104** 30003
[15] Franson J D 1989 Bell inequality for position and time *Phys. Rev. Lett.* **62** 2205–8
[16] Ali-Khan I, Broadbent C J and Howell J C 2007 Large-alphabet quantum key distribution using energy–time entangled bipartite states *Phys. Rev. Lett.* **98** 060503
[17] Thew R, Acín A, Zbinden H and Gisin N 2004 Experimental realization of entangled qutrits for quantum communication *Quantum Inf. Comput.* **4** 93–101
[18] Marsili F *et al* 2013 Detecting single infrared photons with 93% system efficiency *Nat. Photonics* **7** 210–4
[19] Zhou H, Wang L and Wornell G 2013 Layered schemes for large-alphabet secret key distribution *Proc. Information Theory and Applications Workshop* 1–10
[20] Kochman Y, Wang L and Wornell G 2014 Toward photon-efficient key distribution over optical channels *IEEE Trans. Inf. Theory* **60** 4958–72
[21] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev.* A **81** 062343
[22] Lee C, Mower J, Zhang Z, Shapiro J H and Englund D 2013 *Quantum Inf. Processing* (arXiv:1311.1233)
[23] Clauser J F, Horne M A, Shimony A and Holt R A 1969 *Phys. Rev. Lett.* **23** 880
[24] García-Patrón R and Cerf N J 2006 Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution *Phys. Rev. Lett.* **97** 190503
[25] Marcikic I, de Riedmatten H, Tittel W, Scarani V, Zbinden H and Gisin N 2002 *Phys. Rev.* A **66** 062308
[26] Zhong T and Wong F N C 2013 Nonlocal cancellation of dispersion in Franson interferometry *Phys. Rev.* A **88** 020103(R)
[27] Zhong T, Wong F N C, Restelli A and Bienfang J C 2012 Efficient single-spatial-mode periodically-poled $KTiOPO_4$ waveguide source for high-dimensional entanglement-based quantum key distribution *Opt. Express* **20** 26868–77
[28] Zhou H, Chandar V and Wornell G 2013 Low-density random matrices for secret key extraction *Proc. 2013 IEEE Int. Symp. on Information Theory* pp 2607–11
[29] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 Security of quantum key distribution using d-level systems *Phys. Rev. Lett.* **88** 127902
[30] Lucamarini M, Patel K A, Dynes J F, Fröhlich B, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2013 Efficient decoy-state quantum key distribution with quantified security *Opt. Express* **21** 24550–65
[31] Simon C, de Riedmatten H, Afzelius M, Sangouard N, Zbinden H and Gisin N 2007 Quantum repeaters with photon pair sources and multimode memories *Phys. Rev. Lett.* **98** 190503
[32] Usmani I, Afzelius M, de Riedmatten H and Gisin N 2010 Mapping multiple photonic qubits into and out of one solid-state atomic ensemble *Nat. Commun.* **1** 12