Hyperentangled Time-bin and Polarization Quantum Key Distribution

Joseph C. Chapman,[1,2,*] Charles C. W. Lim,[3,4] and Paul G. Kwiat[1,2]

[1]*Illinois Quantum Information Science and Technology Center,*

University of Illinois at Urbana-Champaign, Urbana, IL 61801

[2]*Department of Physics, University of Illinois at Urbana-Champaign, Urbana, IL 61801*

[3]*Department of Electrical & Computer Engineering,*

National University of Singapore, Singapore 117583

[4]*Centre for Quantum Technologies, National University of Singapore, Singapore 117583*

Fiber-based quantum key distribution (QKD) networks are currently limited without quantum repeaters. Satellite-based QKD links have been proposed to extend the network domain. We have developed a quantum communication system, suitable for realistic satellite-to-ground communication. With this system, we have executed an entanglement-based QKD protocol developed by Bennett, Brassard, and Mermin in 1992 (BBM92), achieving quantum bit error rates (QBER) below 2%. More importantly, we demonstrate low QBER execution of a higher dimensional hyperentanglement-based QKD protocol, using photons simultaneously entangled in polarization and time-bin, which has a distinct advantage over BBM92. We show that our protocol is suitable for a space-to-ground link, after incorporating Doppler shift compensation, and verify its security using a rigorous finite-key analysis.

I. MOTIVATION AND BACKGROUND

Implementing quantum key distribution (QKD) or other quantum communication protocols over long distances is a major goal and challenge for establishing a global quantum network. To lay dedicated dark fiber over long distances is expensive and non-reconfigurable, and, without quantum repeaters, such links have very low transmission, due to the exponential decrease in fiber transmission with distance. It has been proposed to instead use

[*] jchapmn2@illinois.edu

arXiv:1908.09018v3 [quant-ph] 3 Mar 2020

space-based links with free-space quantum channels between a ground station and an orbiting platform [1, 2], or to combine these with fiber links [3]. Such a channel has much lower loss than fiber over the same distance—transmission drops only quadratically, due to diffraction—allowing much more efficient protocol execution over comparable distances. For example, the recent achievement of entanglement distribution from a satellite to two ground stations realized a loss reduction of some 12 orders of magnitude [4]; the same satellite also demonstrated decoy-state QKD, realizing a 20 orders-of-magnitude enhancement in channel transmission [5, 6]. This satellite was used to implement the 1992 entanglement-based QKD protocol by Bennett, Brassard, and Mermin (BBM92) [7, 8], though the detection rate and signal-to-noise ratio were far too low to generate secret key of any substantial length (they did not account for finite key affects in their analysis). A number of other groups around the world are also working on similar endeavors [9–12]. To this same end, we have developed a single system to implement multiple quantum protocols relevant for satellite-based communication. We have previously characterized the performance of this system to implement superdense teleportation [13, 14], and have used it to demonstrate high-dimensional tests of nonlocality [15]. Given that our system already generates entanglement and hyperentanglement (simultaneous entanglement in multiple degrees of freedom [16]), here we consider only entanglement-based QKD protocols, which in any event offer advantages in terms of protection from side-channel attacks. In particular, we implement polarization-entanglement-based QKD (specifically, the BBM92 protocol [7]) as well as a novel higher dimensional, hyperentanglement-based QKD protocol (HEQKD). We include a finite-key security analysis and secret key rate simulation of both protocols (see Appendix A for full analysis) and characterize our lab-based implementation of both protocols under conditions relevant for a satellite-to-earth implementation. Finally, using our finite-key analysis, we simulate a currently feasible upgraded version of our system, to directly compare the projected performance of BBM92 and HEQKD in a space-to-earth channel.

While others have studied higher dimensional quantum key distribution [17–20], to the best of our knowledge no previous work has both used hyperentanglement and been able to make the full set of measurements required to implement higher dimensional QKD, i.e., measurements in a pair of fully mutually-unbiased bases. We chose to implement a hyperentangled system (as opposed to one using higher dimensional encoding in a single degree of freedom, e.g., time bins [17] or orbital angular momentum (OAM) [19–23]) to demonstrate

the feasibility and advantages of multiple photonic degrees of freedom in a single demonstration, as we discuss below. Polarization was chosen for its relative ease of manipulation, and both polarization and time-bins for their relative robustness in the atmospheric channel. In contrast, OAM modes are corrupted by turbulence; furthermore, the whole mode must be collected, not just part of it, or the OAM states cannot be reliably distinguished. In a satellite-based implementation, time bins are susceptible to the Doppler shift from the satellite's relative motion but we show that it is fairly straightforward to correct it. The hyperentanglement in polarization and energy-time setup used by Ecker et al. [18] relies on a post-selection-free measurement system (No time-bin filtering needed [24]) which precludes them from making the full mutually-unbiased basis measurement for their state. Due to our system's unique construction, we are able to make the full mutually-unbiased basis measurement required for secure QKD with polarization and time-bin hyperentangled photons, and use photons residing in all output time-bins. Finally, we note that energy-time entanglement with a continuous-wave pump or frequency entanglement are other possibilities for further research [25].

II.   PROTOCOL SUMMARY

A.   Polarization-Entangled BBM92

For our analysis of BBM92, Alice's and Bob's bases are written as $\{A_i\}_{i=1}^2$ and $\{B_i\}_{i=1}^2$, respectively. Assuming Alice and Bob are each operating in a two-dimensional Hilbert space with computational basis given by $Z = \{|i\rangle\}_{i=1}^2$, their measurement bases are defined as $A_1 \equiv Z$, $A_2 \equiv \{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$, and similarly for Bob, where $|0\rangle \equiv |H\rangle$, $|1\rangle \equiv |V\rangle$ for H, V representing horizontal and vertical polarization, respectively. We assume the bases are uniformly chosen with probability $1/2$ and the key is generated from both bases. Here, the size of the raw key is denoted by $m = n + k$, where $k = m(1 - r)$ is the amount of raw key used for parameter estimation, $n = mr$ is the amount of raw key left for key generation, and r is the parameter estimation ratio.

The BBM92 protocol ideally requires Alice and Bob to receive photons from a maximally entangled photon-pair source. In our case, the 1550-nm and 810-nm photons are entangled

in their polarization (Fig. 1), and the state shared between Alice and Bob is

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}|t_1 t_1\rangle \otimes (|HH\rangle + |VV\rangle). \tag{1}$$

B. HEQKD

For our analysis of HEQKD, Alice's and Bob's bases are written as $\{A_i\}_{i=1}^4$ and $\{B_i\}_{i=1}^4$, respectively. We assume that Alice and Bob are each operating in a four-dimensional Hilbert space with the computational basis given by $Z = \{|i\rangle\}_{i=1}^4$, their measurement bases are defined as $A_1 \equiv Z$, $A_2 \equiv \{(|0\rangle \pm |1\rangle)/\sqrt{2}, (|2\rangle \pm |3\rangle)/\sqrt{2}\}$, $A_3 \equiv \{(|0\rangle \pm |2\rangle)/\sqrt{2}, (|1\rangle \pm |3\rangle)/\sqrt{2}\}$, and $A_4 \equiv \{(|0\rangle + |1\rangle + |2\rangle - |3\rangle)/2, (|0\rangle + |1\rangle - |2\rangle + |3\rangle)/2, (|0\rangle - |1\rangle + |2\rangle + |3\rangle)/2, (|0\rangle - |1\rangle - |2\rangle - |3\rangle)/2\}$, and similarly for Bob, where $|0\rangle \equiv |Ht_1\rangle$, $|1\rangle \equiv |Vt_2\rangle$, $|2\rangle \equiv |Vt_1\rangle$, and $|3\rangle \equiv |Ht_2\rangle$ for H, V, t_1, and t_2 representing horizontal polarization, vertical polarization, time bin one, and time bin two, respectively. It can be easily checked that bases 1 and 4 and bases 2 and 3 are mutually unbiased. Bases 1 and 2 are each chosen with probability p, while bases 3 and 4 are each chosen with probability q. Hence, we have that $2p + 2q = 1$, or $q = 1/2 - p$.

Unlike BBM92, HEQKD requires the generation and distribution of hyperentangled photons[16]. As shown in Fig. 1, we prepare non-degenerate entangled photons (at 1550 nm and 810 nm) that are entangled in their polarization and time-bin degrees of freedom:

$$|\Psi_{AB}\rangle = \frac{1}{2}(|(Ht_1)_{810}(Ht_1)_{1550}\rangle + |(Vt_2)_{810}(Vt_2)_{1550}\rangle +$$
$$|(Vt_1)_{810}(Vt_1)_{1550}\rangle + |(Ht_2)_{810}(Ht_2)_{1550}\rangle). \tag{2}$$

III. SECURITY ANALYSIS AND SECRET KEY SIMULATION SUMMARY

In the following, we summarize the finite-key security of entanglement-based BB84 (also called BBM92) and a high-dimensional QKD protocol using two sets of two mutually unbiased bases. The security proof technique relies on the entropic uncertainty relation [26]; see appendix A for the full analysis. Hence, in our analysis, we trust the local measurements and the entanglement source is untrusted.

In both of the above protocols, we assume that entanglement is generated in Alice's laboratory using a non-deterministic photon pair source, e.g., a spontaneous parametric

down-conversion (SPDC) or four-wave mixing source. Using standard models for that type of source [27], if the probability of n photon-pairs being generated is P_n and the coincidence detection probability of n photon-pairs is Y_n, we calculate the overall coincidence detection probability per pump pulse using non-photon-number-resolving detectors for a given γ to be

$$R = \sum_{n=0}^{\infty} P_n Y_n = 1 - \frac{1 - \xi_A}{(1 + \eta_A \gamma)^2} - \frac{1 - \xi_B}{(1 + \eta_B \gamma)^2} + \frac{(1 - \xi_A)(1 - \xi_B)}{(1 + \eta_A \gamma + \eta_B \gamma - \eta_A \eta_B \gamma)^2}, \quad (3)$$

where γ is related to the pump power of the laser ($2\gamma = \mu$ is the mean number of pairs per pump pulse), ξ_A (ξ_B) is the probability of observing a noise or background count on Alice's (Bob's) side per pump pulse, and η_A (η_B) are the overall detection efficiencies for Alice (Bob). For a d-dimensional system, our estimated quantum bit error rate (QBER) per pump pulse is

$$Q_{d,\mathrm{obs}} = \frac{E_b + E_{|\Phi^n\rangle} + E_{\mathrm{MPE}}}{R}, \quad (4)$$

where $d = 2$ for BBM92, $d = 4$ for HEQKD, E_b is the probability of noise or a background count causing an error, $E_{|\Phi^n\rangle}$ is the probability of errors when all photons produced by SPDC are detected, and E_{MPE} is the estimated probability of errors when at least one pair of photons was detected from an n-photon-pair state.

In our analysis of both protocols we use the standard security definitions for QKD [28]: we say that the QKD protocol is ε-secure if it is both $\varepsilon_{\mathrm{sec}}$-secret and $\varepsilon_{\mathrm{cor}}$-correct, where $\varepsilon = \varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{cor}}$. Using the quantum leftover-hash lemma [29] and the entropic uncertainty relation [26], we can bound the min-entropy and, therefore, the secret key length of BBM92:

$$\ell^{2D} = \max_{\beta \in (0, \varepsilon_{\mathrm{sec}}/4)} \left\lfloor n(1 - h_2(Q_{2,\mathrm{obs}} + \Delta)) - \mathrm{Leak}_{\mathrm{EC}}^{2D} - \log_2 \frac{8}{\beta^4 \varepsilon_{\mathrm{cor}}} \right\rfloor, \quad (5)$$

where h_2 is the binary entropy, $\mathrm{Leak}_{\mathrm{EC}}^{2D}$ is the information leaked during error correction, Δ is the statistical noise due to finite statistics, and β is a constrained parameter to be optimised [29].

In our analysis of HEQKD, we focus on processing Alice's measurement data to extract her secret key; our analysis can easily be converted for Bob's measurement data. Specifically, we extract key when Alice measures in basis 1 (the random string of length $n_1 = m_{1,1} + m_{1,2} + m_{1,3}$, where, e.g., $m_{1,2}$ are the measurements in basis 1 for Alice and basis 2 for Bob) and basis 2 (the random string of length $n_2 = m_{2,1} + m_{2,2} + m_{2,4}$). The measurements in basis 3, $m_{3,3}$, and basis 4, $m_{4,4}$, are used for parameter estimation. Using the quantum leftover-hash

lemma [29] and a version of the entropic uncertainty relation for $d = 4$ mutually unbiased bases, after some simplification, we find the secret key length:

$$\ell^{4D} = \max_{\beta \in (0, \varepsilon_{\text{sec}}/4)} \lfloor n_{\text{ext}} + 4 \log_2 \beta - 2 \rfloor, \tag{6}$$

where

$$n_{\text{ext}} \equiv n_1 (2 - h_4(Q_{4,4,4,\text{obs}} + \nu(n_1, m_{4,4}, \bar{\varepsilon}))) + n_2 (2 - h_4(Q_{3,3,4,\text{obs}} + \nu(n_2, m_{3,3}, \bar{\varepsilon})))$$
$$- \text{Leak}_{\text{EC}}^{4D} - \log_2 \frac{2}{\varepsilon_{\text{cor}}}, \tag{7}$$

is the *extractable* key length, h_4 is the shannon entropy, $\text{Leak}_{\text{EC}}^{4D}$ is the information leaked during error correction, ν is the statistical noise due to finite statistics, $Q_{i,i',4,\text{obs}}$ is the observed error rate conditioned on Alice and Bob choosing basis i and i', and $\bar{\varepsilon} = \varepsilon_{\text{sec}}/6 - \beta/3$.

IV.   EXPERIMENTAL SETUP

To generate entangled photons in time-bin and polarization, we use an 80-MHz mode-locked, 532-nm laser (Spectra Physics Vanguard 2.5W 355 laser), frequency doubled from 1064 nm, with a ~7-ps pulse width. Each pulse of this beam is split into two time-bins using a ~2.4-ns delay (see Fig. 1). The beam is then used to pump a type-0 periodically poled lithium niobate crystal (poling period of 7.5 μm) inside a polarizing Sagnac interferometer. This Sagnac entangled photon source [30, 31], ignoring time bins, produces the state

$$\frac{\left(|H\rangle_{810} |H\rangle_{1550} + e^{i\phi} |V\rangle_{810} |V\rangle_{1550} \right)}{\sqrt{2}}. \tag{8}$$

The 532-nm pump has a bandwidth of 64 GHz full-width at half-maximum (FWHM). The peaks (FWHM bandwidths) of the downconversion photons are 809.7 nm (0.4 nm) and 1551 nm (1.5 nm). The downconversion bandwidths were measured using difference-frequency generation between the pump and a tunable ~1550-nm laser [32], whose wavelength was swept while the counts on the 810-nm side were recorded [33].

Avalanche photodiodes (Excelitas SPCM-AQ4C) with efficiency ~45% were used to detect the 810-nm photons. The 1550-nm photons were detected using four WSi superconducting nanowire detectors from NASA's Jet Propulsion Laboratory, optimized for 1550 nm with an efficiency of ~80% [34]. One detector had efficiency of ~40% due to cryostat fiber
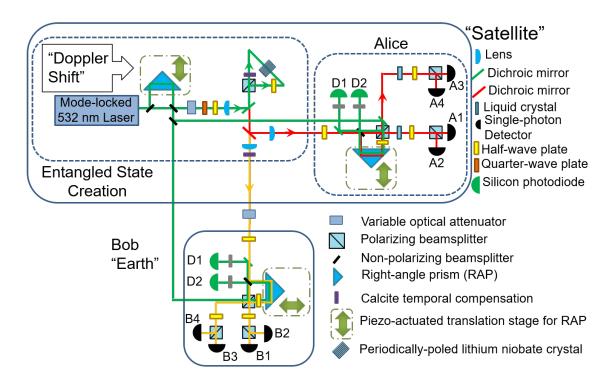
FIG. 1: BBM92 and HEQKD Optical Setup: Photonic "ququarts" hyperentangled in polarization and time-bin are generated via spontaneous parametric downconversion in periodically-poled lithium niobate. Green lines are the 532-nm pump (and stabilization) beam; red and yellow are the signal (810 nm) and idler (1550 nm) photons, respectively.

For BBM92, the pump right-angle prism was blocked so there was no time-bin entanglement. In both Alice's or Bob's analyzer, the short arm measured photons in the H/V basis and the long arm measured photons in the D/A basis. For HEQKD, both time-bin and polarization entanglement are used; see Tables III and IV for the measurement-to-detector mapping. The phase in the phase-sensitive bases (bases 2, 3, and 4) is tuned by tilting the quarter-wave plate before the Sagnac interferometer and/or actuating the liquid crystals after Alice's analyzer interferometer. All half-wave plates just before the detectors were set at 22.5° from horizontal. The half-wave plate before the analyzer interferometer was set at 0 (22.5°) from horizontal for measurements in bases 1,2 (3,4).

coupling misalignment after repair, so 3-dB attenuators were added to the fibers entering the other detectors to even out the detection efficiency for HEQKD measurements.

For BBM92, the measurement basis is randomly chosen by the 50/50 non-polarizing first

beamsplitter in Alice or Bob's delay interferometer: If the photon goes through the short path, it is analyzed in the H/V basis; if it travels the long path, it is analyzed in the D/A basis because of a half-wave plate (HWP) that effectively rotates the basis of that beamsplitter port from H/V to D/A. See Table III for a complete description of the mapping between the bases and measurements to the output time bins and detectors.

For HEQKD, the measurements of the four bases are made using an analyzer interferometer, polarization optics, and a time-bin sorting circuit. The analyzer interferometer allows for measurements of superpositions of the time bins, while the polarization optics allow for measurements of different combinations of polarization and time bin. Measurements in bases 1 and 2 (or 3 and 4) are distinguished by a time-bin sorting circuit that is, electrically, in between the detectors and the time taggers; see Appendix C for explanation of the necessity and operation of the time-bin sorting circuit. See Table IV for a complete description of the mapping between the bases and measurements to the output time bins and detectors.

In our system, the probability of basis 1 and basis 2 is split evenly, as is the probability between basis 3 and basis 4, because of the 50/50 non-polarizing beamsplitters in Alice's and Bob's analyzers. Additionally, we chose to measure in basis 1 and basis 2 $2p = 50\%$ of the time (controlled by rotating a HWP at the front of the analyzer interferometer), to measure an even sampling of all bases for the QBER characterization to follow; later in our analysis, however, we calculate the optimal value for this parameter as a function of channel loss and in a space-to-ground channel, assuming a fast electro-optic modulator is used to randomly choose the bases for each laser pulse.

V. RESULTS

A. Implementation Comparison

Fig. 2 shows the basic performance of our BBM92 and HEQKD implementations. The "crosstalk matrix" shows the expected correlations and anti-correlations when the same measurement basis is used by Alice and Bob and the uncorrelated results when they use different bases. Experimentally, we see QBER below 2% for BBM92 and below 5.5% for HEQKD. There are some imbalances in the matrix element probabilities between different bases and within bases due to transmission differences between different measurements and

bases.

In order to verify the ability of BBM92 and HEQKD to detect an eavesdropper, we inserted in the channel to Bob a 9-mm thick, a-cut calcite crystal oriented so that H and V polarizations are unaltered but travel at different speeds. The calcite is thick enough so the H and V polarizations can no longer interfere after exiting the calcite, because their wavepackets no longer overlap temporally. The calcite introduces a $\sim$ 5-ps relative delay, much larger than $\sim$ 1.7-ps coherence time of the 1.5-nm (0.4-nm) bandwidth 1550-nm (810-nm) photons. This simulates an eavesdropper that measures only in the H/V basis and simply records, then resends to Bob, what is measured. With this technique, the eavesdropper gains a significant amount of information at the necessary cost of introducing a significant amount of errors. Fig. 3 shows the expected and measured results of the eavesdropping. As expected, the results show a greatly increased QBER in all bases involving measurements using superpositions of polarizations.

The intrinsic QBER of the system can be measured accurately for all bases when the probability of producing an entangled pair is sufficiently low that the probability of producing multiple pairs (which can cause errors) is negligible. But since this also reduces the key rate, there is a trade-off, leading to an optimal pump power (mean pairs per pulse, μ) that produces the most secret key per use, when accounting for finite statistics. Fig. 4 shows the measured QBER vs mean pairs per pulse. For each dataset, the mean pairs per pulse were calculated from solving this system of equations:

$$S_i = \frac{RT(\eta_i\mu(4 + \eta_i\mu) + 4\xi_i)}{(2 + \eta_i\mu)^2},$$

(9)

$$C_{AB} = RT\Big(1 - \frac{4(1 - \xi_A)}{(2 + \eta_A\mu)^2} - \frac{4(1 - \xi_B)}{(2 + \eta_B\mu)^2} + \frac{4(1 - \xi_A)(1 - \xi_B)}{(2 + \eta_A\mu + \eta_B\mu - \eta_A\eta_B\mu)^2}\Big),$$

(10)

where S_i is the singles rates for Alice or Bob, C_{AB} is the total coincidence rate between Alice and Bob, T is the integration time, R is the repetition rate of the laser, η_i is the transmission for Alice or Bob, and ξ_i is the noise counts per laser pulse for Alice or Bob [27].

The data shows a significant variation in the intrinsic QBER of each basis, originating from the different physical processes that are present in the states and projections measured in each basis. The QBER in the H/V basis of BBM92, and basis 1 of HEQKD, is only affected by imperfect H/V basis alignment between Alice and Bob and imperfect polarizing beamsplitter extinction ratio, leading to only $\sim$ 1% QBER ($|HV\rangle$-type terms in our
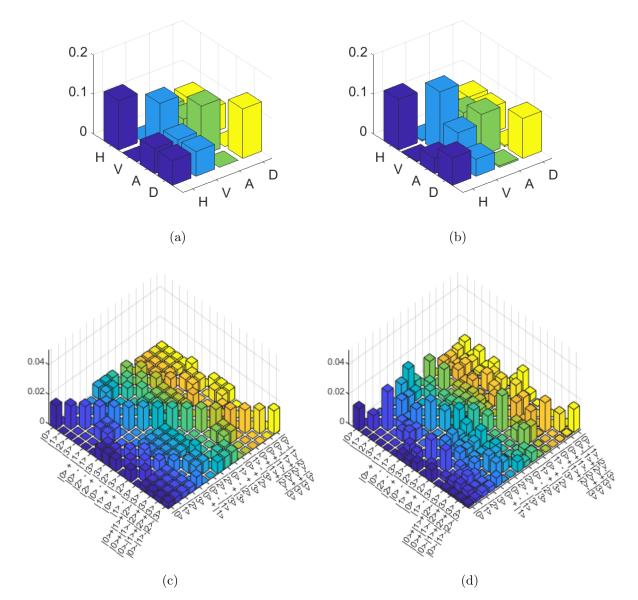
(a)

(b)

(c)

(d)
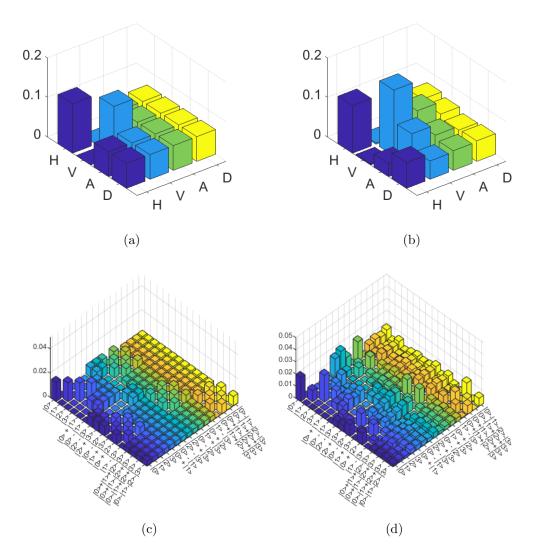
FIG. 2: Crosstalk Matrices: The x-axis (y-axis) shows Bob's (Alice's) projective measurement. (a) For the ideal BBM92 normalized crosstalk matrix, H/V QBER = 0 and D/A QBER = 0. (b) Measured BBM92 normalized crosstalk matrix, showing BBM92 QBER per basis for measured system (standard error in last digit calculated assuming poisson statistics): H/V QBER = 0.0088(3) and D/A QBER = 0.0185(6). (c) Ideal HEQKD normalized crosstalk matrix, where QBER ideally is zero in every basis, and $|0\rangle \equiv |Ht_1\rangle$, $|1\rangle \equiv |Vt_2\rangle$, $|2\rangle \equiv |Vt_1\rangle$, and $|3\rangle \equiv |Ht_2\rangle$. (d) Measured HEQKD normalized crosstalk matrix. The HEQKD QBER per basis for measured system (standard error in last digit calculated from seven measurement samples): $QBER_{11} = 0.010(3)$, $QBER_{12} = 0.013(3)$, $QBER_{13} = 0.002(1)$, $QBER_{21} = 0.008(2)$, $QBER_{22} = 0.036(7)$, $QBER_{24} = 0.044(6)$, $QBER_{31} = 0.003(2)$, $QBER_{33} = 0.029(5)$, $QBER_{34} = 0.029(7)$, $QBER_{42} = 0.04(1)$, $QBER_{43} = 0.025(9)$, and $QBER_{44} = 0.051(9)$.

FIG. 3: Crosstalk Matrices With Eavesdropper: The x-axis (y-axis) shows Bob's (Alice's) projective measurement. (a) Ideal BBM92 normalized crosstalk matrix when an eavesdropper performs an ideal intercept-resend attack on the H/V basis, yielding H/V QBER = 0 and D/A QBER = 0.5. (b) Measured BBM92 normalized crosstalk matrix with a birefringent crystal to decohere the polarization in the H/V basis, yielding H/V QBER = 0.028 and D/A QBER = 0.48. (c) Ideal HEQKD normalized crosstalk matrix when an eavesdropper performs an ideal intercept-resend attack on the polarization qubit, where $|0\rangle \equiv |Ht_1\rangle$, $|1\rangle \equiv |Vt_2\rangle$, $|2\rangle \equiv |Vt_1\rangle$, and $|3\rangle \equiv |Ht_2\rangle$. (d) Measured HEQKD normalized crosstalk matrix with a birefringent crystal to decohere the polarization in the H/V basis. QBER per basis for measured [ideal] system: $QBER_{11} = 0.02[0.00]$, $QBER_{12} = 0.02[0.00]$, $QBER_{13} = 0.01[0.00]$, $QBER_{21} = 0.02[0.00]$, $QBER_{22} = 0.52[0.50]$, $QBER_{24} = 0.49[0.50]$, $QBER_{31} = 0.01[0.00]$, $QBER_{33} = 0.50[0.50]$, $QBER_{34} = 0.50[0.50]$, $QBER_{42} = 0.47[0.50]$, $QBER_{43} = 0.50[0.50]$, and $QBER_{44} = 0.53[0.50]$.

state generation could also cause this same QBER, but are apparently negligible, since the basis 1 QBER matches our classical measurements of the basis alignment and polarizing beamsplitter). HEQKD Basis 2 is affected by the same influences as basis 1, but is also affected by the temporal entanglement visibility ($\sim 96\% \to 2\%$ QBER) and imbalances in the measured amplitudes of the terms in the superposition ($\sim 0.5\%$ QBER). The QBER in the D/A basis of BBM92, and HEQKD Basis 3, is also affected by the same error processes as basis 1, and is affected by imperfect polarization entanglement purity of the source (D/A visibility $\sim 98\% \to 1\%$ QBER) and imbalances in the measured amplitudes of the terms in the superposition ($\sim 0.5\%$ QBER). Finally, HEQKD basis 4 is affected by all previously mentioned error processes, and thus has the highest total QBER.

Since there would be a finite time-window during orbit when we could establish the required line-of-sight quantum channel of varying transmission (see link analysis below), it was important to characterize the system for various values of channel transmission. Errors from detector noise and background events will start to dominate the data when the channel transmission is too low. Fig. 5 shows the measured QBER for each basis in each protocol, for decreasing values of Bob's channel transmission. At the highest measured transmission in Fig. 5, our system (which was not optimized for key rate but QBER) produced $\sim$2k sifted events/s for BBM92 and $\sim$1k sifted events/s for HEQKD, correcting for the different μ used in each protocol for this measurement (see. Fig. 5).

B.   Doppler Shift

Since any transmitter in space will be moving rapidly, the interval between adjacent time bins in the ground station's reference frame initially will be reduced with respect to the interval measured in the transmitter's reference frame, as the transmitter is approaching. The intervals will match as the transmitter passes overhead, and as it moves away, the received interval will be longer (Fig. 6b)[1].

Assuming there is an adaptive optics system on the ground station to correct for turbulence (effectively a transverse variation in phase), the Doppler shift is the only source of time-bin phase change from the space-to-ground channel. The exact phase shift produced

---

[1] There is also a frequency shift on the photons, but since $\gamma \equiv \frac{1}{\sqrt{1-(\frac{V_{sat,long}}{c})^2}} = 1.00000000033$, assuming $V_{sat,long} = 7.7$ km/s (average velocity, e.g., of the ISS), the wavelength shift is negligible compared to the photon bandwidth of ~ 1 nm.
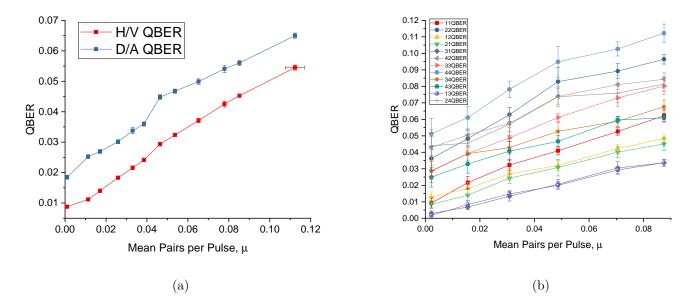
FIG. 4: QBER vs Mean Pairs per Pulse: (a) Measurement of QBER for each BBM92 basis as a function of mean pairs per pulse (adjusted by varying the pump-laser power). The total loss for Alice and Bob are 12 dB and 15 dB, respectively. The error bars, created from ten measurements, correspond to one standard deviation. (b) Measurement of QBER for each key-generating HEQKD basis combination as a function of mean pairs per pulse. In the legend, "12QBER" corresponds to QBER of Alice measuring in basis 1 and Bob measuring in basis 2. The total loss for Alice and Bob are 15 dB and 18 dB, respectively. The error bars, here created from seven measurements, correspond to one standard deviation.

through the Doppler effect is dependent on several parameters, including the maximum elevation angle of the orbit during a pass, which changes for subsequent passes and is at a maximum for passes directly overhead, i.e., the maximum elevation angle is 90°. For time bins separated by 1.5 ns and a $\sim 90°$-maximum elevation angle orbit, calculations of the relativistic longitudinal Doppler shift [35] using a simulation of a LEO (low-earth orbit) satellite with orbit inclination of 51° (angle between orbital plane and equator), 400-km altitude, i.e., the orbit of the International Space Station, and with the longitudinal velocity, $V_{sat,long}$, calculated along the beam path with respect to a ground station at 39° latitude

(a)   (b)

FIG. 5: QBER vs Bob's Channel Loss: (a) Measurement of QBER for each BBM92 basis as a function of the channel loss between the entangled photon source and Bob, with Alice's total loss fixed at 12 dB. Bob's minimum loss is 15 dB, without any channel loss. The mean pairs per pulse was $\mu = 0.026$. The error bars, created from at least ten measurements (up to 55 taken for higher loss data points), correspond to one standard deviation. (b) Measurement of QBER for each key-generating HEQKD basis combination as a function of the transmission of the channel between the entangled photon source and Bob, with Alice's total loss fixed at 15 dB. Bob's minimum loss is 18 dB, without any channel loss. The mean pairs per pulse was $\mu = 0.016$. The error bars, created from eight measurements, correspond to one standard deviation.

(e.g., continental United States) show an expected shift of

$$\Delta L(t) = \left(\sqrt{\frac{1 + \frac{V_{sat,long}(t)}{c}}{1 - \frac{V_{sat,long}(t)}{c}}} - 1 \right)(1.5 \text{x} 10^{-9} s)c, \tag{11}$$

as displayed in Fig. 6a. If acquisition starts and stops at a 20° elevation angle, then the total change in pulse separation during a pass of the satellite is $\Delta L(t_{stop}) - \Delta L(t_{start}) = 20\mu m$.

We implemented an in-lab simulation of this Doppler shift by moving smoothly varying a piezo-actuated translation stage that controlled the position of the pump's right-angle prism, using the same distance-vs-time profile as in Fig. 6a. To keep this Doppler shift

FIG. 6: Expected Doppler Shift: (a) Expected Doppler shift for an overhead orbit. (b) Pictorial explanation of effect of Doppler shift on time bins.

(and any other time-varying phase shifts) from adversely affecting the protocol's performance, we developed a phase stabilization system that uses a classical laser beam and proportional-integral feedback to track the path-length difference of the ground interferometer so it matches that of the emitted time bins throughout the pass (see Appendix B for more information). As seen in Fig. 7a, QKD is not possible without such phase stabilization because the QBER in some bases is too high, even though other bases are unaffected by the Doppler shift since their basis states, e.g., polarization, are time-bin phase insensitive. QBER in some bases starts high at Time = 0 s because there was no initial phase calibration done for this particular dataset. Fig. 7b shows the performance of HEQKD while a lab-simulated Doppler shift was occurring, with initial phase calibration done and the phase stabilization activated. During the Doppler shift the QBER was held stable to $< 1\%$ standard deviation. Since the quantum signal and classical-phase-stabilization pulses co-propagate with one another, we expect nearly all of the potential phase drift caused by satellite motion and vibration, to be common-mode except for phase drifts in the ground station analyzer. Therefore, we would expect similar performance of our lab-based phase stabilization system in an actual space-to-earth implementation.

FIG. 7: Doppler Shift Effect on HEQKD: Measured QBER for all basis combinations during an in-lab simulated Doppler shift (solid black curve) (a) without phase stabilization; (b) with phase stabilization active. The legend applies to both figure panels.

C.   Secret Key Rate Simulations

To perform a full finite-key optimization for the maximum secret key rate, we simultaneously optimized, via sequential quadratic programming, the mean pairs per pulse, μ (see Fig. 8a), the HEQKD basis probability, p, and the BBM92 parameter estimation ratio, r (see Fig. 8b), using only the first ten terms of Eqn. 4 due to computational difficulty in evaluating the infinite sums.

Because the QBERs in different bases vary significantly for our HEQKD implementation (c.f. Fig. 4b) it is not optimum to use a balanced analysis protocol (i.e., measure in all bases with equal likelihood); instead, in the asymptotic key regime (0-45 dB), one should give preference to bases used for key generation, and in the finite-key regime (45-56 dB) one should give preference to bases used for error-checking so the error estimate is tighter in the finite key analysis (see Fig. 8b). Similarly, the optimal parameter estimation ratio for BBM92 is high in the asymptotic key regime and decreases in the finite-key regime since more key is needed for parameter estimation when the raw key length is shorter.

Optimizing to obtain the longest final key for a long-distance HEQKD implementation,

we find the optimal μ in Fig. 8a rises as the loss increases, while for BBM92, μ decreased. We suspect the differing behavior in Fig. 8a and the higher average HEQKD QBER (0.07 for $\mu = 0.1$) over the average BBM92 QBER (0.036 for $\mu = 0.05$) is primarily due to the increased error tolerance of higher dimensional protocols [36] in general, which allows for a higher μ to be used. We think this leads to the 10-dB span in Fig. 8c where only HEQKD provides a non-zero secret key rate.

Notably, Fig. 8c shows that HEQKD can still yield useful secret keys ($\sim$ 10 kb/hr) in an overhead geo-stationary orbit (GEO). In contrast, a GEO implementation of BBM92 would require higher repetition rates and larger transmit and receive apertures. The left vertical dashed line in Fig. 8c is located at about 47 dB which we calculated using the Friis equation to estimate channel transmission η as a function of range: $\eta(r) = (\pi D_T D_R/(4\lambda r))^2$ [37, 38]. We set the range to 35,800 km, the transmitting telescope diameter to $D_T = 0.2$ m, receiving telescope diameter to $D_R = 3$ m, and wavelength to $\lambda = 1550$ nm, with the added assumptions of a 6-dB loss for receiver telescope and adaptive optics efficiency and 4-dB loss from the analysis/detection system, and used the system parameters listed in Table I. Similarly, the right vertical line at 57 dB was calculated using the Friis equation with a receiving telescope diameter to $D_R = 1$ m.

The instantaneous elevation angle of a LEO satellite with respect to some terrestrial observatory changes as it passes overhead, with a maximum elevation angle that varies from pass to pass (90° max elevation angle corresponding to a pass directly overhead). With that in mind, displayed in Fig. 9c, we show the predicted secret key length for HEQKD and BBM92, versus maximum elevation angle per pass, assuming the minimum acceptable elevation angle during a pass is 20° (below this we assume a reliable link cannot be established). This was calculated using the optimized μ, p, and r, as shown in Fig. 9a-b.

For these calculations, we used simulated orbit data for all orbital parameters, assuming a 400-km altitude and 51° inclination. The range was calculated from LEO to a ground station located at 39° N latitude. We used the Friis equation to estimate channel transmission, assuming a transmitting telescope diameter $D_T = 0.1$ m, receiving telescope diameter $D_R = 1$ m, and wavelength $\lambda = 1550$ nm, with the added assumptions of a 6-dB loss for receiver telescope and adaptive optics efficiency and 4-dB loss from the analysis/detection system, and other system parameters listed in Table I. We discretely integrated over the whole pass in 10-s increments; data acquisition was assumed to begin and end at 20° elevation
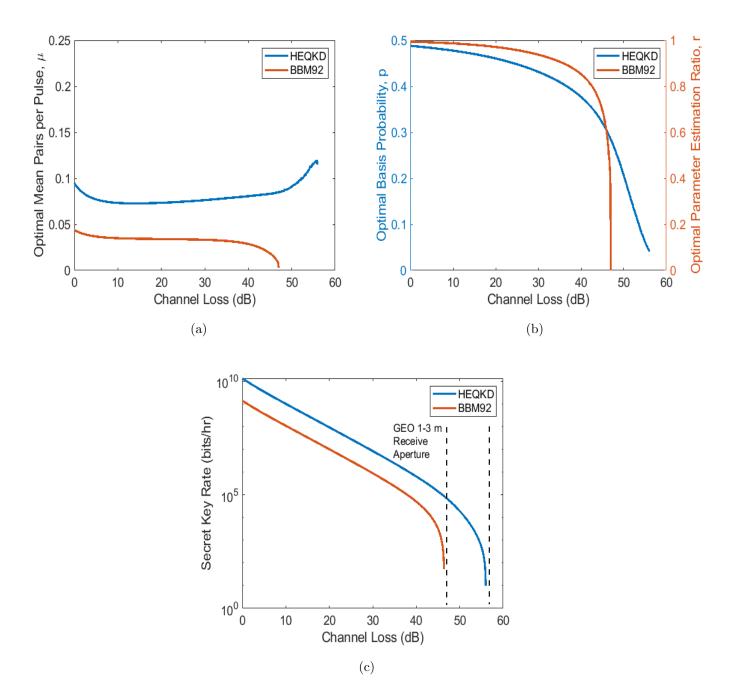
(a)

(b)

(c)

FIG. 8: Secret Key Length Optimization for HEQKD and BBM92: (a) Optimal mean pairs per pulse, μ, vs channel loss for 1 hour of key generation. (b) Optimal HEQKD basis probability, p, on the left vertical axis and Optimal BBM92 paremeter estimation ratio, r, on the right vertical axis vs channel loss for 1 hour of key generation. (c) Calculated secret key rate (bits/hr) vs Bob's channel loss calculated using the optimized values for μ and p and feasible future system parameters: 400-MHz laser repetition rate, 10^{-6} background noise, and Alice's total transmission including detection efficiency = 0.3. See Table I for more details. Assuming a 20-cm transmitter-aperture diameter and a GEO-altitude of 35,800 km, the channel loss for a 3-m (1-m) receiver-aperture diameter on the ground is 47 dB (57 dB) (see Secret Key Rate Simulations section).

(a)

(b)

(c)

FIG. 9: LEO Protocol Comparison: (a) Optimal mean pairs per pulse, μ, vs the maximum elevation angle per orbital pass. The channel loss (range) varied between 28 dB (400 km) and 36 dB (1000 km) in this simulation. Future system parameters used in simulations: 400-MHz laser repetition rate, 180-s orbital pass time, 10^{-6} background noise, and Alice's total transmission = 0.3, including detection efficiency. See Table I and Secret Key Rate Simulations section for more details. (b) Optimal HEQKD basis probability, p, on the left vertical axis and Optimal BBM92 paremeter estimation ratio, r, on the right vertical axis vs the maximum elevation angle per orbital pass. (c) Simulated secret key length per orbital pass for HEQKD and BBM92 vs the maximum elevation angle per orbital pass.

TABLE I: System Parameters: Current and expected future system parameters relevant to simulation.

	Current System	Simulated System
Laser Repetition Rate	80 MHz	400 MHz
Detector Efficiency A	0.45	0.6
Detector Efficiency B	0.4	0.9
Measurement System Transmission	0.6	0.7
Heralding Efficiency	0.15	0.7
Background Noise per Pump Pulse	10^{-5}	10^{-6}

angle, corresponding to a maximum range of about 1000 km with a minimum range of 400 km. For comparison, at those same distances, a fiber-optic cable (assuming 0.2 dB/km of attenuation) would have 80-200 dB of loss, much more than the 25-30 dB we expect in a free-space implementation leading to transmission rates lower by 17 orders of magnitude! With these assumptions, a future implementation of this system in LEO could generate a secret key of substantial length in a single pass with the secret key length generated by HEQKD exceeding that of BBM92 by an order of magnitude for all maximum elevation angles between 20° and 90°.

Thus, in a direct comparison between HEQKD and BBM92, using a finite-key analysis, we find that HEQKD allows for secret key generation at higher losses than does BBM92, including in geostationary orbit, and with much higher key rates than BBM92 when the losses are less extreme, e.g., in low-earth orbit or medium-earth orbit. This comparison was done with all system parameters being equal except choosing the optimal μ and p for HEQKD and the optimal μ and r for BBM92. We did not optimize the basis choice probability for BBM92 because our system uses a non-polarizing beamsplitter to set the ratio to 50% (which is important for our other protocol demonstrations with this system [13]). Additionally, the error rates of the two bases in BBM92 are very similar and our security analysis used data from both bases for key generation and error checking.

VI.   DISCUSSION

From these measurements and analyses, we project this system (with the same QBER but enhanced repetition rate and efficiency as we used in our simulations) would be suitable for operation in the channel between space and earth, and would be able to generate a sizable, usable secret key within a single orbital pass. Furthermore, we find that the use of time-bin qubits in general should be feasible for a channel that includes an orbiting platform, assuming one compensates for the adverse effect from the Doppler shift, as we have done. To successfully execute this protocol in a space-to-earth channel, active polarization compensation (to correct for rotations and phase shifts produced by the sending and receiving optics), an adaptive optics system at the ground station (to correct for wavefront distortions by the atmosphere and allow for single-mode fiber coupling of the received light), and phase stabilization (to phase stabilize the time bins from the Doppler shift and from other variations, e.g., satellite vibrations or laboratory temperature fluctuations) must be implemented in real time. Additionally, after the previous compensation systems have been activated, but prior to protocol execution, a phase calibration step is necessary for bases which include superpositions of time bins and/or polarizations, so that Alice and Bob are indeed measuring in the same bases. Implementing such systems with high precision is readily achievable with current technology and should enable QBER levels comparable with the values measured in our laboratory. Therefore, we conclude that useful quantum key distribution from a satellite in low-earth orbit should be feasible with existing technology.

VII.   ACKNOWLEDGMENTS

VIII.   AUTHOR CONTRIBUTIONS

All authors contributed to experiment design and wrote manuscript. J.C.C. carried out all experiments and data analysis, including upgrading the optical and detection system, and constructing the time-bin sorting circuit. C.W.L. carried out theoretical security analysis, and C.W.L and J.C.C wrote secret-key simulation.

Appendix A: HEQKD and BBM92 Finite Key Analysis

1.   Preliminaries: Models

In the following, we will analyze the finite-key security of entanglement-based BB84 (also called BBM92) and a high-dimensional QKD protocol using two sets of two mutually un-biased bases. The security proof technique relies on the entropic uncertainty relation [26]. In both of the above protocols, we assume that entanglement is generated in Alice's labora-tory using a non-deterministic pair source, e.g., a spontaneous parametric down-conversion (SPDC) or four-wave mixing source, where a non-linear crystal is used to split a strong laser beam into pairs of correlated photons [27]. Quantum mechanically, we can write the output state (using vector representation) of such a source as

$$|\Psi\rangle_{AB} \equiv \cosh^{-2}(\chi) \sum_{n=0}^{\infty} \sqrt{n+1} \tanh^n(\chi) |\psi_n\rangle_{AB}, \tag{A1}$$

where

$$|\psi_n\rangle_{AB} \equiv \frac{1}{n+1} \sum_{k=0}^{n} (-1)^k |n-i,i\rangle_A \otimes |k,n-k\rangle_B. \tag{A2}$$

Accordingly, the probability to get an n photon-pairs is

$$P_n \equiv \frac{(n+1)\gamma^n}{(1+\gamma)^{n+2}}, \tag{A3}$$

where $\gamma \equiv \sinh^2(\chi)$ is related to the pump power of the laser. $2\gamma = \mu$ is the mean number of pairs per pump pulse.

To model the detection rates (which are needed for the simulation), we define η_A and η_B to be the overall detection efficiencies for Alice and Bob, respectively. Note that η_A and η_B include all the losses due to the quantum channel, coupling loss, and detection inefficiency.

Using this definition, it is easy to see that the probability of observing a coincident detection (i.e., at least one click on each side) given the emission of an n photon-pairs, $|\psi_n\rangle$, is

$$\eta_n = [1 - (1 - \eta_A)^n][1 - (1 - \eta_B)^n]. \tag{A4}$$

In addition, we define the *yield* of an $n-$photon pair to be Y_n, which is the conditional probability that a coincident detection is observed if the source emits an $n-$photon pair:

$$Y_n = [1 - (1 - \xi_A)(1 - \eta_A)^n][1 - (1 - \xi_B)(1 - \eta_B)^n], \tag{A5}$$

where ξ_A (ξ_B) is the probability of observing a noise or background count on Alice's (Bob's) side per pump pulse. For example, in the case of zero photon emission, we have $Y_0 = \xi_A\xi_B$. Using the above models, the overall coincidence detection probability per pump pulse using non-photo-number-resolving detectors for a given γ is

$$R = \sum_{n=0}^{\infty} P_n Y_n = 1 - \frac{1 - \xi_A}{(1 + \eta_A\gamma)^2} - \frac{1 - \xi_B}{(1 + \eta_B\gamma)^2} + \frac{(1 - \xi_A)(1 - \xi_B)}{(1 + \eta_A\gamma + \eta_B\gamma - \eta_A\eta_B\gamma)^2}. \tag{A6}$$

To estimate the probability of detecting an error per pump pulse we look at the effects of measurement system errors, background light, and loss of the photons, including some effects from multiple-pair detection events (which require the assignment of a random bits if there are multiple detection events [39]). We needed to derive this estimate to have a rate formula that was suitable for $d = 4$ since the work of Ma et al. [27] was not easily generalized to higher dimensions. Here we derive an estimate for a d-dimensional system which gives an upper bound on the error rate, at least for the $d = 2$ case when compared to the formula for $E_\lambda Q_\lambda$, derived in [27] (which is an exact formula for the expected error rate for a system of that dimension).

We estimate the error from background events with 3 different cases: when Alice (Bob) loses all her (his) photons but detects a background event and Bob (Alice) detects at least one photon (assuming there is no error) and the case where both Alice and Bob lose all their photons and they both detect a background event. Conditional on these events happening and in the case that multiple photons are detected here, there is an error probability of e_0. Adding up all those different possibilities, we find the error probability for background

related errors to be

$$E_b = e_0 \sum_{n=0}^{\infty} P_n \left[\sum_{k=1}^{n} \left[\binom{n}{k} \eta_A^k (1 - \eta_A)^{n-k} \xi_B (1 - \eta_B)^n \right] \right.$$

$$+ \sum_{l=1}^{n} \left[\binom{n}{l} \eta_B^l (1 - \eta_B)^{n-l} \xi_A (1 - \eta_A)^n \right]$$

$$\left. + \xi_A \xi_B (1 - \eta_A)^n (1 - \eta_B)^n \right]. \tag{A7}$$

Assuming all photons produced are detected, some errors are dependent on the imperfections in the measurement system and others from the uncorrelated nature of certain terms in the higher-order photon pair wavefunction, $|\Psi^n\rangle$ [40] or from multiple photons being detected simultaneously on different detectors.

Correlated terms in $|\Psi^n\rangle$ occur with probability dN_n^2, where N_n is the normalization factor of $|\Psi^n\rangle$ (for $d = 2$, $N_n^2 = 1/(n!(n+1)!)$ [40]). To calculate N_n for HEQKD (d=4), we need to generalize the work of Kok et al. [40] to the case of four measurement outcomes instead of two. In this case,

$$H = i\kappa(a_0^\dagger b_0^\dagger + a_1^\dagger b_1^\dagger + a_2^\dagger b_2^\dagger + a_3^\dagger b_3^\dagger) + \text{H.c.}, \tag{A8}$$

where H.c. means Hermitian conjugate, κ is the product of the pump amplitude and the coupling constant between the electromagnetic field and the crystal. The operators $a_i^\dagger$, $b_i^\dagger$ and a_i, b_i are creation and annihilation operators for the 4 basis states in our measurement system, e.g., $a_0^\dagger|0\rangle = |Ht_1\rangle$, $a_1^\dagger|0\rangle = |Vt_2\rangle$, $a_2^\dagger|0\rangle = |Vt_1\rangle$, and $a_3^\dagger|0\rangle = |Ht_2\rangle$. Using the multinomial theorem, we find the state of n entangled photon pairs to be

$$|\Psi^n\rangle = N_n L_+^n |0\rangle = N_n \sum_{k_3=0}^{n} \sum_{k_2=0}^{n-k_3} \sum_{k_1=0}^{n-k_3-k_2} \left[n! \binom{n}{(n-k_3-k_2-k_1)k_1k_2k_3} \right.$$

$$\left. |k_0, k_1, k_2, k_3; k_0, k_1, k_2, k_3\rangle_{a_0,a_1,a_2,a_3,b_0,b_1,b_2,b_3} \right], \tag{A9}$$

where we define $L_+ = a_0^\dagger b_0^\dagger + a_1^\dagger b_1^\dagger + a_2^\dagger b_2^\dagger + a_3^\dagger b_3^\dagger = L_-^\dagger$, $k_0 = n - k_3 - k_2 - k_1$. N_n is a normalization factor so that $\langle \Psi^n | \Psi^n \rangle = 1$, where

$$\frac{1}{N_n^2} = (n!)^2 \sum_{k_3=0}^{n} \sum_{k_2=0}^{n-k_3} \sum_{k_1=0}^{n-k_3-k_2} \binom{n}{(n-k_3-k_2-k_1)k_1k_2k_3} = 2^{2n}(2n)!. \tag{A10}$$

For correlated terms, some measurement system errors happen when all the photons on 1 side are incorrectly sorted to the same wrong detector, which happens with probability $(e_d/(d-1))^n dN_n^2$, where we assume that errors are evenly distributed among all the states in a basis and e_d is the intrinsic error probability in that basis, conditional on a coincidence detection. The rest of the errors, which happen with probability $1 - (e_d/(d-1))^n dN_n^2$, have multiple photons being detected on each side, incurring an error probability of e_0. The total error probability when all photons produced are detected is

$$E_{|\Phi^n\rangle} = \sum_{n=1}^{\infty} P_n \eta_A^n \eta_B^n \left(\frac{e_d}{d-1}\right)^n dN_n^2 + \sum_{n=2}^{\infty} P_n \eta_A^n \eta_B^n \left(1 - \left(\frac{e_d}{d-1}\right)^n dN_n^2\right) e_0. \tag{A11}$$

Additionally, to further account for events where multiple photons are detected we include the cases where at least 2 photon pairs are created and at least 1 photon pair is detected and we assume that all events detected are either uncorrelated or have multiple detections so that we have to assign a random bit. The error probability for these events is

$$E_{\text{MPE}} = e_0 \sum_{n=2}^{\infty} P_n \left[\sum_{i=1}^{n} \left[\binom{n}{i} \eta_A^i (1-\eta_A)^{n-i} \right] \sum_{j=1}^{n} \left[\binom{n}{j} \eta_A^j (1-\eta_A)^{n-j} \right] - \eta_A^n \eta_B^n \right]. \tag{A12}$$

Thus, for a d-dimensional system, our estimated total quantum bit error rate (QBER) per pump pulse is

$$Q_{d,\text{obs}} = \frac{E_b + E_{|\Phi^n\rangle} + E_{\text{MPE}}}{R}. \tag{A13}$$

2. Security Bound for BBM92

Having defined the quantum channel and source models, we can derive a bound on the extractable key length (denoted by ℓ) for a given *post-processing block size* (the number of raw bits we collect in one execution of the protocol).

To further model the security of the QKD protocol, we consider a $(d = 2)$ QKD protocol with two mutually unbiased bases. Alice's and Bob's bases are written as $\{A_i\}_{i=1}^2$ and $\{B_i\}_{i=1}^2$, respectively. Assuming Alice and Bob are each operating in a two-dimensional Hilbert space with computational basis given by $Z = \{|i\rangle\}_{i=1}^2$, their measurement bases are defined as $A_1 \equiv Z$, $A_2 \equiv \{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$, and similarly for Bob. The bases are uniformly chosen (with $1/2$ probability each) and the raw key is generated from both bases. That is,

the raw key is randomly sampled from the measurement data (of size N); thus, the size of the raw key is fixed to some positive integer $m = n + k$, where $k = m(1-r)$ is the amount of raw key used for parameter estimation, $n = mr$ is the amount of raw key left for key generation, and r is the parameter estimation ratio. Following standard security definitions [28], we say that the QKD protocol is ε-secure if it is both ε_{sec}-secret and ε_{cor}-correct. For the first condition, the protocol is called ε_{sec}-secret if the joint state of the output secret key (say on Alice side) and the adversary's total quantum information is statistically indistinguishable from the ideal output state except with some small probability ε_{sec}. The ideal output state is an output key which is uniformly random (in the key space) and completely independent of the adversary's total information. For the second condition, the protocol is called ε_{cor}-correct if the output secret keys on Alice and Bob's sides are identical except with some small probability ε_{cor}.

The starting point of our security analysis is to ask how many secret bits can be extracted from Alice's raw key X (of size m) given E (Eve's total information about the QKD system). To this end, we use the quantum leftover-hash lemma [29] to bound the secret key length, ℓ, giving

$$\ell = \max_{\beta \in (0, \varepsilon_{\text{sec}}/2]} \left\lfloor H_{\min}^{\varepsilon_{\text{sec}}/2 - \beta}(X|E) + 4 \log_2 \beta - 2 \right\rfloor, \tag{A14}$$

where β is a constrained optimization parameter and and $H_{\min}^{\varepsilon_{\text{sec}}/2 - \beta}$ is the smooth min-entropy of X given E (see Ref. [41] for more details).

Using the fact that there exists a squashing model (a theoretical argument that maps higher photon number states to a qubit state) [42] for two mutually unbiased measurements (it applies regardless of whether the implementation uses active or passive basis choice), we can bound the min-entropy using the entropic uncertainty relation [26], assuming the measurements on Alice's side are mutually unbiased (e.g., no polarization misalignment at the measurement level). More specifically, we have

$$H_{\min}^{\varepsilon_{\text{sec}}/2 - \beta}(X|E) \geq n(1 - h_2(Q_{2,\text{obs}} + \Delta(n, k, \beta))) - \text{Leak}_{\text{EC}}^{2D} - \log_2 \frac{2}{\varepsilon_{\text{cor}}} \quad \text{and} \tag{A15}$$

$$\text{Leak}_{\text{EC}}^{2D} = 1.12 n h_2(Q_{2,\text{obs}}), \tag{A16}$$

where

$$\Delta(n, k, \beta) \equiv \sqrt{\frac{n+k}{nk} \frac{k+1}{k} \ln \frac{1}{\beta}}, \tag{A17}$$

$h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy, Δ is the statistical noise due to finite statistics, and $\text{Leak}_{\text{EC}}^{2D}$ and $\log_2 2/\varepsilon_{\text{cor}}$ are the information leakages due to error correction and verification, respectively. Putting everything together, we get

$$\ell^{2D} = \max_{\beta \in (0, \varepsilon_{\text{sec}}/4)} \left\lfloor n(1 - h_2(Q_{2,\text{obs}} + \Delta(n, k, \beta))) - \text{Leak}_{\text{EC}}^{2D} - \log_2 \frac{8}{\beta^4 \varepsilon_{\text{cor}}} \right\rfloor. \qquad (A18)$$

3. Security Bound for HEQKD

We consider an entanglement-based ($d = 4$) QKD protocol with four measurement bases. Alice's and Bob's bases are written as $\{A_i\}_{i=1}^4$ and $\{B_i\}_{i=1}^4$, respectively, and we suppose that their reference frames and measurements are aligned, i.e., $A_i = B_i$ for $i = 1, 2, 3, 4$. Assuming Alice and Bob are each operating in a four-dimensional Hilbert space with computational basis given by $Z = \{|i\rangle\}_{i=1}^4$, their measurement bases are defined as $A_1 \equiv Z$, $A_2 \equiv \{(|0\rangle \pm |1\rangle)/\sqrt{2}, (|2\rangle \pm |3\rangle)/\sqrt{2}\}$, $A_3 \equiv \{(|0\rangle \pm |2\rangle)/\sqrt{2}, (|1\rangle \pm |3\rangle)/\sqrt{2}\}$, and $A_4 \equiv \{(|0\rangle + |1\rangle + |2\rangle - |3\rangle)/2, (|0\rangle + |1\rangle - |2\rangle + |3\rangle)/2, (|0\rangle - |1\rangle + |2\rangle + |3\rangle)/2,$
$(|0\rangle - |1\rangle - |2\rangle - |3\rangle)/2\}$, and similarly for Bob. It can be easily checked that bases 1 and 4 and bases 2 and 3 are mutually unbiased. Bases 1 and 2 are each chosen with probability p, while bases 3 and 4 are each chosen with probability q. Hence, we have that $2p + 2q = 1$, or $q = 1/2 - p$.

After the measurement phase, Alice and Bob perform sifting (via public communication) to identify successful events according to their basis choices. We denote these sets by $\mathcal{S}_{i,i'}$ and their respective lengths by $m_{i,i'}$. For example, the data belonging to set $\mathcal{S}_{1,3}$ are the events in which Alice and Bob chose basis 1 and 3, respectively, and each detected one photon (though the results are not necessarily correct).

In our analysis, we focus on processing Alice's measurement data to extract her secret key; our analysis can easily be reversed for Bob's measurement data. We partition her data into four sets, namely, sets containing events in which Alice chooses either basis 1 or basis 2 (which data comprises the raw key) and sets containing events in which Alice chooses either basis 3 or basis 4 (used to determine Alice's QBER). Alice' data in basis 1 will be paired with Bob's data from basis 1, 2 and 3, and data in basis 2 will be paired with Bob's data from basis 1, 2 and 4. Note that common bases should ideally generate perfectly correlated data (2 bits per measurement) while bases that are not mutually unbiased and not common (e.g. basis 1 and basis 2) should ideally generate partially correlated data (1

TABLE II: HEQKD Bases: All basis combinations in the HEQKD protocol and their effect on key generation. MUB = mutually-unbaised basis, and Bits/Photon, in this case, means bits of raw key per sifted coincident photon pair detected.

Alice Basis	Bob Basis	MUB?	Bits/ Photon
1	1	N	2
1	2	N	1
1	3	N	1
1	4	Y	-
2	1	N	1
2	2	N	2
2	3	Y	-
2	4	N	1
3	1	N	1
3	2	Y	-
3	3	N	2
3	4	N	1
4	1	Y	-
4	2	N	1
4	3	N	1
4	4	N	2

bit per measurement). $\mathcal{S}_{3,3}$ and $\mathcal{S}_{4,4}$ are used for error estimation. $\mathcal{S}_{3,4}$ and $\mathcal{S}_{4,3}$ are unused. See Table II for the complete list of pairings.

To compute the finite-key security of Alice's data, we first need to introduce some random variables to capture the random behavior of the measurements. To that end, let $\mathbf{X}_1$ be the random string of length $n_1 = m_{1,1} + m_{1,2} + m_{1,3}$ describing Alice' measurement outcomes when she chooses basis 1. Likewise, for the case when Alice chooses basis 2 we write $\mathbf{X}_2$ to denote the random string of $n_2 = m_{2,1} + m_{2,2} + m_{2,4}$. Recall, the lengths of the sifted events when Alice measures in basis i and Bob measures in basis i' are denoted by $m_{i,i'}$. Our immediate goal now is to show that it is possible to extract a secret key of length $\ell > 0$ from $\mathbf{X}_1\mathbf{X}_2$ if certain experimental conditions are met.

The starting point of our security analysis is to ask how many secret bits can be extracted from Alice' raw key $\mathbf{X}$ (of size n) given $\mathbf{E}^+$ (Eve's total information about the overall joint state shared between Alice and Bob, including the classical communication sent by Alice to Bob). To this end, we use the quantum leftover-hash lemma [29] to determine the secret key length, ℓ, giving

$$\ell = \max_{\beta \in (0, \varepsilon_{\mathrm{sec}}/2]} \left\lfloor H_{\min}^{\varepsilon_{\mathrm{sec}}/2 - \beta}(\mathbf{X}_1 \mathbf{X}_2 | \mathbf{E}^+) + 4 \log_2 \beta - 2 \right\rfloor, \tag{A19}$$

where the left-hand term in the floor function is the smooth min-entropy of $\mathbf{X}_1 \mathbf{X}_2$ given $\mathbf{E}^+$ (see Ref. [41] for more details). We can further break up the min-entropy term into two parts by using a chain-rule inequality for smooth min-entropies,

$$H_{\min}^{\varepsilon_{\mathrm{sec}}/2 - \beta}(\mathbf{X}_1 \mathbf{X}_2 | \mathbf{E}^+) \geq H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_1 | \mathbf{X}_2 \mathbf{E}^+) + H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_2 | \mathbf{E}^+) + \log \left(1 - (1 - \bar{\varepsilon}^2)^{1/2} \right), \tag{A20}$$

where $\bar{\varepsilon} = \varepsilon_{\mathrm{sec}}/6 - \beta/3$. To further simplify the analysis, we assume that $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent. In the experiment, this assumption can be achieved by having Alice prepare highly entangled photon pairs (independent pairs), measure one half of each entangled photon pair, and send the other half to Bob via the quantum channel. This procedure in effect produces random outcomes in each run, which implies $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent variables. With this, we have that

$$H_{\min}^{\varepsilon_{\mathrm{sec}}/2 - \beta}(\mathbf{X}_1 \mathbf{X}_2 | \mathbf{E}^+) \geq H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_1 | \mathbf{E}^+) + H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_2 | \mathbf{E}^+) + \log \left(1 - (1 - \bar{\varepsilon}^2)^{1/2} \right), \tag{A21}$$

where now the smooth entropy terms $H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_1 | \mathbf{E}^+)$ and $H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_2 | \mathbf{E}^+)$ can be treated independently. To translate these terms into expressions that can be bounded using experimental data, we use a version of entropic uncertainty relations for two $d = 4$ mutually unbiased bases to get

$$H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_1 | \mathbf{E}^+) \geq 2n_1 - H_{\max}^{\bar{\varepsilon}}(\mathbf{T}_1 | \mathbf{T}_1'), \tag{A22}$$

$$H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_2 | \mathbf{E}^+) \geq 2n_2 - H_{\max}^{\bar{\varepsilon}}(\mathbf{T}_2 | \mathbf{T}_2'), \tag{A23}$$

where $\mathbf{T}_1$ and $\mathbf{T}_1'$ are Alice's and Bob's measurement outcomes corresponding to basis 4, and $\mathbf{T}_2$ and $\mathbf{T}_2'$ are the measurement outcomes corresponding to basis 3. Here, we suppose that the measurements are acting locally on a four-dimensional Hilbert space, which is a reasonable assumption since in practice Alice's light source, with relatively high probability, only produces independent entangled photon pairs. Assuming that Alice's and Bob's error

probabilities within a given basis are uniformly distributed (i.e., they can be modeled by a depolarizing channel), then we have that

$$H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_1|\mathbf{E}^+) \geq n_1(2 - h_4(Q_{4,4}^{4D} + \nu(n_1, m_{4,4}, \bar{\varepsilon}))), \tag{A24}$$

$$H_{\min}^{\bar{\varepsilon}}(\mathbf{X}_2|\mathbf{E}^+) \geq n_2(2 - h_4(Q_{3,3}^{4D} + \nu(n_2, m_{3,3}, \bar{\varepsilon}))), \tag{A25}$$

where $Q_{i,i',4,\mathrm{obs}}$ is the observed error rate conditioned on Alice and Bob choosing basis i and i', $h_4(x) = -x\log_2(x) - (1-x)\log_2(1-x) + x\log_2(3)$ is the shannon entropy, and

$$\nu(n, k, \varepsilon) = \sqrt{\frac{(n+k)(k+1)\ln(2/\varepsilon)}{nk^2}} \tag{A26}$$

is the statistical error due to finite sampling. Note that in the infinite key limit this term goes to zero.

Putting everything together, we can now establish a lower bound on $H_{\min}^{\varepsilon_{\sec}/2-\beta}(\mathbf{X}_1\mathbf{X}_2|\mathbf{E}^+) \geq n_{\mathrm{ext}}$:

$$n_{\mathrm{ext}} \equiv n_1(2 - h_4(Q_{4,4,4,\mathrm{obs}} + \nu(n_1, m_{4,4}, \bar{\varepsilon}))) + n_2(2 - h_4(Q_{3,3,4,\mathrm{obs}} + \nu(n_2, m_{3,3}, \bar{\varepsilon})))$$
$$- \mathrm{Leak}_{\mathrm{EC}}^{4D} - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}}, \tag{A27}$$

$$\mathrm{Leak}_{\mathrm{EC}}^{4D} = 1.2n_1 h_4(\min[0.75, p^2 Q_{1,1,4,\mathrm{obs}} + p^2 Q_{1,2,4,\mathrm{obs}} + pq Q_{1,3,4,\mathrm{obs}}]) +$$
$$1.2n_2 h_4(\min[0.75, p^2 Q_{2,1,4,\mathrm{obs}} + p^2 Q_{2,2,4,\mathrm{obs}} + pq Q_{2,4,4,\mathrm{obs}}]), \tag{A28}$$

where $\mathrm{Leak}_{\mathrm{EC}}^{4D}$ and $\log_2 2/\varepsilon_{\mathrm{cor}}$ are the leakages due to error correction and verification, respectively. Finally, we find

$$\ell^{4D} = \max_{\beta \in (0, \varepsilon_{\sec}/4)} \lfloor n_{\mathrm{ext}} + 4\log_2\beta - 2 \rfloor. \tag{A29}$$

Appendix B: Time-bin Phase Stabilization and Calibration

Due to natural environmental factors (vibration, temperature fluctuations), the phase between the time bins is prone to drift; to counteract this we stabilized the phase using an active proportional-integral (PI) feedback [43] system. The phase was measured using some

of the pump beam that was also sent (counter-propagating) through the analyzer interferometer in a mode that was vertically displaced from the single-photon beam. The output of the stabilization interferometer was measured using Detectors D1 and D2, low-bandwidth amplified Si photodiodes (Thorlabs PDA36A) and a DAQ (NI USB-6210) to interface with the computer. Due to the stabilization beam wavelength not matching the design specification of some of the components, and because the low-bandwidth detectors could not distinguish the interfering time bins (e.g., the short (long) path in the pump interferometer and the long (short) path in Alice or Bob's analyzer interferometer) from the non-interfering ones (short paths in both interferometers and long paths in both interferometers), the visibility was quite low ($< 10\%$) and also different for D1 and D2. This difference necessitated the use of a scaling factor γ to equalize the amplitude of oscillation between D1 and D2. With this scaling factor, the Error signal, E, used for the PI feedback algorithm was

$$E \equiv \frac{(I_{D1} - \gamma I_{D2})}{(I_{D1} + \gamma I_{D2})}, \text{ with } \gamma \sim 0.6. \tag{B1}$$

The feedback system was designed to keep E at zero by sending a signal to a piezo-actuated translation stage (Thorlabs 17.4-μm piezo AE0505D16F, Thorlabs TPZ001 piezo driver, and Newport 436 translation stage) under the analyzer interferometer's right-angle prism to adjust the phase, at an update rate of 100 Hz. Independent PI systems were implemented for the Pump-Alice combined interferometer and for the Pump-Bob combined interferometer.

Additionally, for QKD it is not only necessary that the phase is kept stable, but also that it is calibrated to the correct value. By changing the phase between $|H\rangle$ and $|V\rangle$, the liquid crystals after Alice's interferometer were used to adjust the phase of states in Basis 2 and 4 so that the photons were routed to the correct detector. For Basis 3 and Basis 4, it was necessary to tilt (about the vertical axes) a QWP before the source to adjust the phase of the polarization-entangled state so that $|D\rangle$ and $|A\rangle$ were routed to the correct detectors on each side.

Appendix C: Time-bin Sorting Circuit Operation

As displayed in Fig. 10, there are three time bins which exit Alice or Bob's time-bin analyzer interferometer, each with a different exit time with respect to the pulse which entered the pump delay interferometer. It is imperative to be able to distinguish all three

FIG. 10: Franson Time-Bin Qubit Preparation and Measurement: This diagram illustrates how the time bins are created and what possible combinations of them exit the second delay interferometer. Here we assume that $t_2 - t_1 = t_2^p - t_1^p$, i.e., that the path-length imbalances are matched. In this case, photons in either of the two middle time bins can interfere.

of these time bins for the HEQKD and BBM92 protocols implemented with this setup. The measurement of time-bin qubits using free-running, single-photon detectors alone lacks the ability to sort bases measurements when events from different time bins are routed to the same detector as in this experiment. It was therefore necessary to develop a circuit which could filter the events corresponding to different time bins into different electrical signals. We used the pump laser as a clock reference and filtered the signals from each detector based on their delay with respect to the laser clock, using an AND gate with a window width of ~ 1 ns. Each time bin has a unique delay with respect to the laser clock so this enabled complete filtering of the time bins.

In the time-bin sorting circuit, each detector output was copied (using ON Semi. NB7VQ14M) three times and was ANDed with a copy of the clock that was delayed by the correct amount so that only events from one of the time bins was successfully transmitted through the AND gate. This process was executed for all eight detectors (four for Alice and four for Bob) and for all three time bins, creating 24 unique output signals (12 for Alice and 12 for Bob).

To use an AND gate (Analog Devices HMC746LC3C) and adjustable delay chip (ON Semi. MC100EP195B) with low jitter (< 100 ps) and high bandwidth (> 1 GHz), it was necessary to transform the electrical signals from the detectors into signals compatible with high-speed differential logic standards like CML and PECL. This was done using a

FIG. 11: Time-bin Sorting Circuit: Descriptive schematic of pulse shaping, using the MAX9602 high-speed comparator, several NBSG53A high-speed D-flip flops with ~ 100 ns delay, and then a ~ 700 ps delay.

high-speed comparator (Maxim Int. MAX9602). Additionally, to achieve a subnanosecond pulse so the AND gate had ~ 1 ns acceptance window, the pulses from the detectors were shortened to < 1 ns using a cascade of 2 high-speed D flip-flops (ON Semi. NBSG53A). A pulse shortening effect was created by sending the comparator output into the CLK of the D flip-flop with Q (input) attached to logic HIGH and using a delayed copy of the output as a reset signal after the pulse was sent through the flip-flop. This long pulse was then sent through another D flip-flop with a short reset signal, producing a much shorter pulse (~ 1 ns) than the detector output pulses (~ 40 ns). See Fig. 11 for a pictorial description.

Appendix D: Event Timetagging

The detection events of Alice and Bob were recorded using separate time-tagging electronic devices (UQDevices UQD-Logic-16, time-bin width 156 ps), synchronized via a common 10-MHz sine-wave clock (Agilent 33250A Function Generator). Also, one channel on each time tagger was connected to a TTL pulse source (National Instruments DAQ USB-6210) through cables of the same length. This allowed the different time offsets of each time tagger to be measured accurately and subtracted out. The coincidence matrices for BBM92 and HEQKD are in Table III and Table IV, respectively, indicating what states are measured in a given time bin, by a given detector pair.

TABLE III: BBM92 Coincidence Matrix: Coincidence matrix of all detector and time-bin combinations used in the BBM92 protocol demonstration. See Fig. 10 for pictorial definition of time bins $t^p_1 + t_1$, $(t^p_1 + t_2$ & $t^p_2 + t_1)$, and $t^p_2 + t_2$.

Legend: H/V basis (green), D/A basis (pink), Different bases (blue).

		$(t^p_1+t_1)$				$(t^p_2+t_1)$ & $(t^p_1+t_2)$			
		A1	A2	A3	A4	A1	A2	A3	A4
$(t^p_1+t_1)$	B1	$\|Ht^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Ht^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Ht^p_1t_1\rangle\|Dt^p_1t_2\rangle$	$\|Ht^p_1t_1\rangle\|Dt^p_1t_2\rangle$
	B2	$\|Ht^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Ht^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Ht^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Ht^p_1t_1\rangle\|Dt^p_1t_2\rangle$	$\|Ht^p_1t_1\rangle\|Dt^p_1t_2\rangle$
	B3	$\|Vt^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Vt^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Vt^p_1t_1\rangle\|Dt^p_1t_2\rangle$	$\|Vt^p_1t_1\rangle\|Dt^p_1t_2\rangle$
	B4	$\|Vt^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|Ht^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|Vt^p_1t_1\rangle$	$\|Vt^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Vt^p_1t_1\rangle\|At^p_1t_2\rangle$	$\|Vt^p_1t_1\rangle\|Dt^p_1t_2\rangle$	$\|Vt^p_1t_1\rangle\|Dt^p_1t_2\rangle$
$(t^p_2+t_1$ & $t^p_1+t_2)$	B1	$\|At^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|At^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|At^p_1t_2\rangle\|Dt^p_1t_2\rangle$	$\|At^p_1t_2\rangle\|Dt^p_1t_2\rangle$
	B2	$\|At^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|At^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|At^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|At^p_1t_2\rangle\|Dt^p_1t_2\rangle$	$\|At^p_1t_2\rangle\|Dt^p_1t_2\rangle$
	B3	$\|Dt^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|Dt^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|Dt^p_1t_2\rangle\|Dt^p_1t_2\rangle$	$\|Dt^p_1t_2\rangle\|Dt^p_1t_2\rangle$
	B4	$\|Dt^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|Ht^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|Vt^p_1t_1\rangle$	$\|Dt^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|Dt^p_1t_2\rangle\|At^p_1t_2\rangle$	$\|Dt^p_1t_2\rangle\|Dt^p_1t_2\rangle$	$\|Dt^p_1t_2\rangle\|Dt^p_1t_2\rangle$

TABLE IV: HEQKD Coincidence Matrix: Coincidence matrix of all detector and time bin combinations used in the HEQKD protocol demonstration. See Fig. 10 for pictorial definition of time bins $t_1^p + t_1$, ($t_1^p + t_2$ & $t_2^p + t_1$), and $t_2^p + t_2$. (a) Measurements when Alice and Bob measure in bases 1 or 2. (b) Measurements when Alice measures in bases 3 or 4 and Bob measures in bases 1 or 2. (c) Measurements when Alice measures in bases 1 or 2 and Bob measures in bases 3 or 4. (d) Measurements when Alice and Bob measure in bases 3 or 4.

[1] Richard J Hughes, William T Buttler, Paul G Kwiat, SK Lamoreuax, GL Morgan, Jane E Nordholt, and Charles G Peterson, "Quantum cryptography for secure satellite communications," in *2000 IEEE Aerospace Conference. Proceedings (Cat. No. 00TH8484)*, Vol. 1 (IEEE, 2000) pp. 191–200.

[2] Markus Aspelmeyer, Thomas Jennewein, Martin Pfennigbauer, Walter R Leeb, and Anton Zeilinger, "Long-distance quantum communication with entangled photons using satellites," IEEE J. of Sel. Top. in Q. Elec. **9**, 1541–1551 (2003).

[3] Christoph Simon, "Towards a global quantum network," Nat. Phot. **11**, 678 (2017).

[4] Juan Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140–1144 (2017).

[5] Sheng-Kai Liao *et al.*, "Satellite-to-ground quantum key distribution," Nature **549**, 43 (2017).

[6] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, *et al.*, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).

[7] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).

[8] Juan Yin, Yuan Cao, Yu-Huai Li, Ji-Gang Ren, Sheng-Kai Liao, Liang Zhang, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, *et al.*, "Satellite-to-ground entanglement-based quantum key distribution," Phys. Rev. Lett. **119**, 200501 (2017).

[9] James A Grieve, Robert Bedington, Zhongkan Tang, Rakhitha CMRB Chandrasekara, and Alexander Ling, "Spooqysats: Cubesats to demonstrate quantum key distribution technologies," Acta Astronautica **151**, 103–106 (2018).

[10] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi, "Experimental satellite quantum communications," Phys. Rev. Lett. **115**, 040502 (2015).

[11] Christopher J Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Jeongwan Jin, Nigar Sultana, Sascha Agne, Elena Anisimova, Vadim Makarov, Eric Choi, Brendon L Higgins, *et al.*, "Airborne demonstration of a quantum key distribution receiver payload," Q. Sci. and Tech. **2**, 024009 (2017).

[12] Fabian Steinlechner, Sebastian Ecker, Matthias Fink, Bo Liu, Jessica Bavaresco, Marcus Huber, Thomas Scheidl, and Rupert Ursin, "Distribution of high-dimensional entanglement via an intra-city free-space link," Nat. Comm. **8**, 15971 (2017).

[13] Joseph C Chapman, Trent M Graham, Herbert J Bernstein, Christopher K Zeitler, and Paul G Kwiat, "Time-bin and polarization superdense teleportation for space applications," arXiv preprint arXiv:1901.07181 (2019).

[14] J. C. Chapman, H. Bernstein, K. Meier, C. Zeitler, and P. G. Kwiat, "Progress towards implementing superdense teleportation in space," in *Proc. SPIE 10547*, Vol. 10547 (2018).

[15] Christopher K. Zeitler, Joseph C. Chapman, Eric Chitambar, and Paul G. Kwiat, "Tests of nonlocality with hyperentangled photons," In Preparation.

[16] Julio T. Barreiro, Nathan K. Langford, Nicholas A. Peters, and Paul G. Kwiat, "Generation of hyperentangled photon pairs," Phys. Rev. Lett. **95**, 260501 (2005).

[17] Nurul T Islam, Charles Ci Wen Lim, Clinton Cahall, Jungsang Kim, and Daniel J Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Sci. Adv. **3**, e1701491 (2017).

[18] Sebastian Ecker, Fabian Steinlechner, Matthias Fink, Bo Liu, Jessica Bavaresco, Marcus Huber, Thomas Scheidl, and Rupert Ursin, "Towards high-dimensional quantum key distribution over long-distance free-space links (conference presentation)," in *Proc. SPIE 10799*, Vol. 10799 (2018).

[19] Mohammad Mirhosseini, Omar S Magaña-Loaiza, Malcolm N OSullivan, Brandon Rodenburg, Mehul Malik, Martin PJ Lavery, Miles J Padgett, Daniel J Gauthier, and Robert W Boyd, "High-dimensional quantum cryptography with twisted light," New J. of Phys. **17**, 033033 (2015).

[20] Frédéric Bouchard, Khabat Heshami, Duncan England, Robert Fickler, Robert W Boyd, Berthold-Georg Englert, Luis L Sánchez-Soto, and Ebrahim Karimi, "Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons," Quantum **2**, 111 (2018).

[21] Fang-Xiang Wang, Wei Chen, Zhen-Qiang Yin, Shuang Wang, Guang-Can Guo, and Zheng-Fu Han, "Characterizing high-quality high-dimensional quantum key distribution by state mapping between different degrees of freedom," Phys. Rev. Applied **11**, 024070 (2019).

[22] Vincenzo D'ambrosio, Eleonora Nagali, Stephen P Walborn, Leandro Aolita, Sergei Slussarenko, Lorenzo Marrucci, and Fabio Sciarrino, "Complete experimental toolbox for alignment-free quantum communication," Nat. commun. **3**, 961 (2012).

[23] Giuseppe Vallone, Vincenzo D'Ambrosio, Anna Sponselli, Sergei Slussarenko, Lorenzo Marrucci, Fabio Sciarrino, and Paolo Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," Phys. Rev. Lett. **113**, 060503 (2014).

[24] D. V. Strekalov, T. B. Pittman, A. V. Sergienko, Y. H. Shih, and P. G. Kwiat, "Postselection-free energy-time entanglement," Phys. Rev. A **54**, R1–R4 (1996).

[25] Poolad Imany, Jose A Jaramillo-Villegas, Ogaga D Odele, Kyunghun Han, Daniel E Leaird, Joseph M Lukens, Pavel Lougovski, Minghao Qi, and Andrew M Weiner, "50-ghz-spaced comb of high-dimensional frequency-bin entangled photons from an on-chip silicon nitride microresonator," Optics express **26**, 1825–1840 (2018).

[26] M. Tomamichel, C. C. W. Lim, N. Gisan, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nat. comm. **3** (2012).

[27] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo, "Quantum key distribution with entangled photon sources," Phys. Rev. A **76**, 012307 (2007).

[28] J. Mueller-Quade and R. Renner, "Composability in quantum cryptography," New J. of Phys. **11** (2009).

[29] M. Tomamichel and M. Hayashi, "A hierarchy of information quantities for finite block length analysis of quantum tasks," IEEE Trans. on Inf. Theory **59**, 7693–7710 (2013).

[30] B. S. Shi and A. Tomita, "Generation of a pulsed polarization entangled photon pair using a sagnac interferometer," Phys. Rev. A **69**, 013803 (2004).

[31] T. Kim, M. Fiorentino, and F. N. Wong, "Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer." Phys. Rev. A **73**, 012316 (2006).

[32] Kevin Zielnicki, Karina Garay-Palmett, Daniel Cruz-Delgado, Hector Cruz-Ramirez, Michael F OBoyle, Bin Fang, Virginia O Lorenz, Alfred B URen, and Paul G Kwiat, "Joint spectral characterization of photon-pair sources," J. of Mod. Opt. **65**, 1141–1160 (2018).

[33] T. M. Graham, *Using Hyperentanglement for advanced quantum communication*, Ph.D. thesis, University of Illinois at Urbana-Champaign (2016).

[34] F Marsili *et al.*, "Detecting single infrared photons with 93% system efficiency," Nat. Phot. **7**, 210 (2013).

[35] A. Einstein, "Zur elektrodynamik bewegter körper," Annalen der Physik **322**, 891–921 (1905).

[36] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," Phys. Rev. Lett. **88**, 127902 (2002).

[37] H. T. Friis, "Introduction to radio and radio antennas," IEEE Spectrum **8**, 55–61 (1971).

[38] S. B. Alexander, *Optical communication receiver design* (SPIE Optical engineering press, Bellingham, Washington, USA, 1997).

[39] Norbert Lütkenhaus, "Quantum key distribution: theory for application," App. Phys. B **69**, 395–400 (1999).

[40] Pieter Kok and Samuel L Braunstein, "Postselected versus nonpostselected quantum teleportation using parametric down-conversion," Phys. Rev. A **61**, 042304 (2000).

[41] R. Koenig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Trans. on Inf. Theory **55**, 4337–4347 (2009).

[42] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus, "Squashing models for optical measurements in quantum communication," Phys. Rev. Lett. **101**, 093601 (2008).

[43] N. Minorsky, "Directional stability of automatically steered bodies," J. Amer. Soc. Naval Eng. **34**, 280–309 (1922).