PHYSICAL REVIEW A **92**, 052339 (2015)

Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations

Jean-Philippe Bourgoin,[1,2,*] Nikolay Gigov,[1,2] Brendon L. Higgins,[1,2] Zhizhong Yan,[1,3] Evan Meyer-Scott,[1,2] Amir K. Khandani,[4] Norbert Lütkenhaus,[1,2] and Thomas Jennewein[1,2,†]

[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada N2L 3G1*

[2]*Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, Canada N2L 3G1*

[3]*Centre for Ultrahigh Bandwidth Devices for Optical Systems (CUDOS) & MQ Photonics Research Centre, Department of Physics & Astronomy, Macquarie University, Sydney, NSW 2109, Australia*

[4]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada N2L 3G1*

(Received 7 August 2015; published 30 November 2015)

Quantum key distribution (QKD) has the potential to improve communications security by offering cryptographic keys whose security relies on the fundamental properties of quantum physics. The use of a trusted quantum receiver on an orbiting satellite is the most practical near-term solution to the challenge of achieving long-distance (global-scale) QKD, currently limited to a few hundred kilometers on the ground. This scenario presents unique challenges, such as high photon losses and restricted classical data transmission and processing power due to the limitations of a typical satellite platform. Here we demonstrate the feasibility of such a system by implementing a QKD protocol, with optical transmission and full post-processing, in the high-loss regime using minimized computing hardware at the receiver. Employing weak coherent pulses with decoy states, we demonstrate the production of secure key bits at up to 56.5 dB of photon loss. We further illustrate the feasibility of a satellite uplink by generating a secure key while experimentally emulating the varying losses predicted for realistic low-Earth-orbit satellite passes at 600 km altitude. With a 76 MHz source and including finite-size analysis, we extract 3374 bits of a secure key from the best pass. We also illustrate the potential benefit of combining multiple passes together: while one suboptimal "upper-quartile" pass produces no finite-sized key with our source, the combination of three such passes allows us to extract 165 bits of a secure key. Alternatively, we find that by increasing the signal rate to 300 MHz it would be possible to extract 21 570 bits of a secure finite-sized key in just a single upper-quartile pass.

DOI: 10.1103/PhysRevA.92.052339 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex

I. INTRODUCTION

Quantum key distribution (QKD) offers communications security without reliance on computational presumptions by taking advantage of fundamental properties of quantum mechanics [1,2]. Despite reaching maturity that supports commercial implementation [3,4], QKD has yet to achieve widespread use, in large part owing to distance limitations, on the order of 200 km, inherent to lossy terrestrial transmissions [5–11]. Quantum repeaters [12] promise to overcome this shortcoming, but they require high-fidelity quantum memories which are still in the fundamental research stage [13,14] and are not yet viable for real-world application. Alternatively, quantum links to orbiting satellites can be implemented using existing technologies [15–19].

One near-term approach to satellite-based QKD is where a satellite, acting as a trusted node, performs two consecutive quantum key exchanges with two different ground stations. A combination of the two keys is then publicly revealed, allowing one ground station to extract the other's key, giving both locations a shared key in a way that no other party (except for the satellite) can surreptitiously intercept. This approach may be implemented with either uplink (photons sent from the ground station transmitter to the satellite receiver) or downlink (photons sent from the satellite transmitter to the ground station receiver). The feasibility of both of these has been extensively studied [18–21]. While a downlink benefits from lower transmission losses, allowing higher key rates, an uplink offers the advantage of a simpler satellite design, easier pointing, reduced on-board data collection requirements, and source flexibility, which makes an uplink the preferred scenario for scientific study [19,22].

A significant challenge in the uplink scenario is operating with the high photon loss experienced (40 to 60 dB). Previous work demonstrated that key extraction is possible, in principle, beyond 50 dB of loss in the infinite key limit [22]. However, this work did not perform all of the steps necessary to implement the QKD protocol and produce a secure key. (Indeed, experimental QKD demonstrations routinely go no further than calculate the expected length of the secure key based on observed parameters.) Here we experimentally demonstrate key extraction at various transmission loss levels, up to 56.5 dB, while including all the QKD processing steps required to finally extract a secure key. We also examine the effect of finite statistics, and assess the time required to achieve near-asymptotic key rates in the high-loss environment. Furthermore, we show the feasibility of ground-satellite QKD by experimentally recreating the varying losses of three realistic uplink satellite passes.

Our apparatus has the two parties involved in the high-loss QKD transmission operating independently, each party having separate event time taggers, global positioning system (GPS) receivers, and classical processing mediated by a classical communication channel. Because we focus on a future satellite

*jbourgoin@uwaterloo.ca

†thomas.jennewein@uwaterloo.ca

implantation, computational requirements are also a key aspect. The system we have developed attempts to reduce, as much as possible, these requirements at the receiver. We analyze the complexity of the classical processing functions, and demonstrate operation on low-power embedded hardware. We show that the requirements are feasible, making our overall design suitable for a satellite payload.

This paper is organized as follows. Section II details the steps of the QKD protocol and the approaches we have taken to optimize it for a satellite uplink. Section III describes the experimental apparatus we constructed to perform our demonstrations. Section IV presents the results in two parts: Sec. IV A shows the results of our computational analysis, while Sec. IV B shows the results of our experimental QKD demonstration. We close with discussion and conclusion in Sec. V.

II. IMPLEMENTING QKD WITH LIMITED RESOURCES

A. BB84 with decoy states

The seminal QKD protocol BB84 [1] encodes information in the polarization states of single photons. Ideally, at each time step Alice randomly selects one of four polarizations in two bases—horizontal (H), vertical (V), diagonal (D), or antidiagonal (A)—and sends a photon with this polarization to Bob. Bob randomly selects a basis, H/V or D/A, and measures the photon to obtain one of four outcomes. This procedure occurs for many time steps, and after revealing the bases used, Alice and Bob "sift" their events, discarding those which have mismatched bases. By defining H and D to correspond to a bit value of 0, and V and A to correspond to a bit value of 1, Alice and Bob retain a common string of random bits—the *sifted* key [2].

Practical implementations have extra complications: photons are lost in transmission, imperfections in photon source and detection devices introduce errors (which must be corrected), and weak coherent pulse sources, which are often used in place of true single-photon sources, exhibit potentially insecure multiphoton emission events. Decoy-state protocols [23], with error correction and privacy amplification as classical post-processing steps, have been developed to overcome these issues.

Theoretical QKD security proofs provide equations for the secure key rate based on experimentally measurable parameters such as the quantum bit error ratio (QBER), background noise counts, and decoy parameters. These allow us to make a statement about the security of the *final* key after the quantum transmission is complete. Most importantly, these equations determine the amount of privacy amplification required to be able to claim ϵ security [24,25]. Once the post-processing is complete and the final key deemed secure, it can then be used in a classical encryption protocol such as one-time pad.

We implement the vacuum+weak decoy-state protocol [23], in which Alice randomly emits signal states with average photon number μ, or decoy states that are either vacuum or have an average photon number $\nu < \mu$. In our implementation (Fig. 1), Alice employs polarization and intensity modulation [26] to prepare a random sequence of BB84 polarization encodings which are 92% signal and 8% decoy states. Our average photon numbers are $\mu \approx 0.5$ and $\nu \approx 0.05$, which

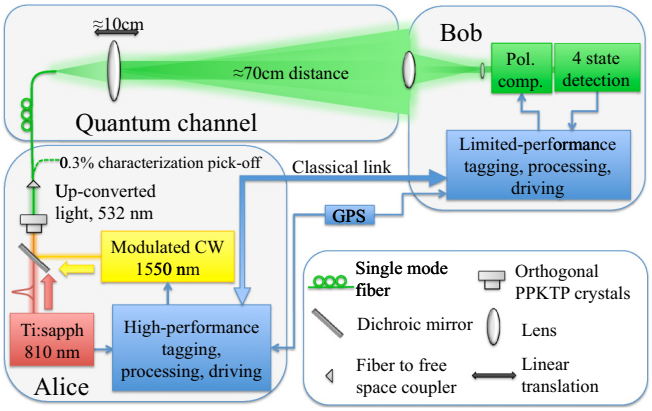

FIG. 1. (Color online) Schematic overview of our high-loss QKD apparatus. The source at Alice produces weak coherent pulses with wavelength 532 nm that possess both the short pulse length of the mode-locked 810 nm laser and the polarization state of the 1550 nm continuous wave laser. The quantum channel consists of a movable lens after the fixed output of an optical fiber to adjust the beam divergence over the free-space link. Computational performance of the tagging, processing, and driving in Bob is limited to simulate the available resources of a satellite-based QKD receiver payload.

are near the optimal for this protocol. (Further details of the apparatus are given in Sec. III.)

The lower bound for the final asymptotic secure key rate per laser pulse is [23]

$$R_\infty = qK_\mu\{-Q_\mu f_{\mathrm{EC}} H_2(E_\mu) + Q_1^{\mathrm{L}}[1 - H_2(E_1^{\mathrm{U}})]\}. \quad (1)$$

Here q is a basis reconciliation factor ($\frac{1}{2}$ for BB84), K_μ is the fraction of pulses that are signal states, f_{EC} is the efficiency parameter of the error correction algorithm, H_2 is the binary entropy function, $Q_{\mu/\nu}$ is the gain for signal/decoy states (the ratio of number of photons detected by Bob to number of pulses sent by Alice), $E_{\mu/\nu}$ is the QBER for signal/decoy states (ascertained in the error correction process), and Q_1^{L} and E_1^{U} are the lower bound of the gain and the upper bound of the QBER, respectively, for single-photon pulses.

The single-photon gain lower bound Q_1^{L} is calculated as

$$Q_1^{\mathrm{L}} = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \quad (2)$$

where Y_0 is the vacuum yield, determined by the cumulative probability of detector dark counts and background noise within the coincidence window. The single-photon QBER upper bound E_1^{U} is calculated as [23,27]

$$E_1^{\mathrm{U},\mu} = \frac{E_\mu Q_\mu}{Q_1^{\mathrm{L}}} - \frac{E_0 Y_0}{Q_1^{\mathrm{L}} e^\mu}, \quad (3)$$

$$E_1^{\mathrm{U},\nu} = \frac{E_\nu Q_\nu e^\nu - E_0 Y_0}{\nu Q_1^{\mathrm{L}}} \mu e^{-\mu}, \quad (4)$$

$$E_1^{\mathrm{U}} = \min\{E_1^{\mathrm{U},\mu}, E_1^{\mathrm{U},\nu}\}, \quad (5)$$

where E_0 is the vacuum error rate ($\frac{1}{2}$ in a perfect apparatus).

In the present work, the parameters in Eqs. (1)–(5) are determined from experimental data to obtain the asymptotic lower bound for the secret key rate per laser pulse R_∞. To

obtain the secure key rate in bits per second, R_∞ is multiplied by the pulse rate of the WCP source.

Proper generation of a secure key needs to incorporate the effects of statistical fluctuations due to finite-sized experimental data [28]. To account for this we use the common heuristic of adding or subtracting 10σ variation from the experimental parameters in such a way as to minimize the key rate [29]. (A recently proposed method may allow us to account for statistical fluctuation in a more rigorous fashion [30].) Finite-size security effects are captured [31] by the security parameter Δ, resulting in a key rate lower bound

$$R = qK_\mu\{-Q_\mu f_{\mathrm{EC}} H_2(E_\mu) + Q_1^{\mathrm{L}}[1 - H_2(E_1^{\mathrm{U}})] - Q_\mu \Delta/N_\mu\}, \quad (6)$$

where $\Delta = 7\sqrt{N_\mu \log_2[2/(\bar{\epsilon}-\bar{\epsilon}')]} - 2\log_2[2(\epsilon-\epsilon_{\mathrm{EC}}-\bar{\epsilon})]$, ϵ_{EC} is the error correction silent failure probability (we use 10^{-10}), N_μ is the raw key size, and $\bar{\epsilon}$ and $\bar{\epsilon}'$ are numerically optimized for R, constrained by $\epsilon - \epsilon_{\mathrm{EC}} > \bar{\epsilon} > \bar{\epsilon}' \geqslant 0$.

B. Distribution of post-processing tasks

The design of our classical post-processing software follows the principle that Alice should perform as many of the computationally intensive tasks as possible, as the ground station can be made rich in computing resources, compared to the limited capacity of a satellite payload. In our system, Alice, being the source of the optical signal over the high-loss link, is responsible for high-rate data readout. She also performs timing analysis (to match Bob's classically transmitted time-tagged photon detection events to her time-tagged source events) and basis sifting, afterwards sending simplified coincidence information back to Bob. We also choose a one-way error correction algorithm based on low-density parity-check codes [32], in which Alice performs the computationally expensive decoding algorithm while Bob only runs a linear algorithm to compute his syndromes (see Sec. II D). This scheme has the additional advantage of having low classical communication overhead. Finally, both parties perform a Toeplitz-matrix-based [33] privacy amplification routine suitable for low-power hardware implementation (see Sec. II E).

We separate Bob's software into two components: a driving control environment, and an embedded processing component. The driving control component is responsible for all platform-dependent tasks, e.g., loading time-tagger operating system drivers, configuring time taggers, reading out time tags, and displaying live statistics. To be suitable for implantation into a yet-to-be-designed satellite, Bob's embedded processing component is implemented in a platform-agnostic way using a portable low-level language (C). It is executed as a separate process on an x86-64 desktop computer, or on a low-power ARM development board, and performs the bulk of Bob's necessary processing tasks.

Because Bob's embedded component runs in a standalone process, its usage of computing resources can be accurately monitored. Moreover, the driving control component records the bandwidth used for classical communication. This design allows us to make an accurate assessment of the classical post-processing requirements and guides our analysis of the computing requirements of Bob's part of the QKD protocol.

C. Time synchronization and basis sifting

Several practical issues complicate the process of determining which time-tagged photon detections correspond to particular source events, including initial clock synchronization, drift over time, and variation in photon time-of-flight. For our apparatus, an extra complication is that our data acquisition hardware is not capable of operating at the high pulse frequency of the laser source (see Sec. III).

To reduce the heavy load on the time tagger at the source, only a subset of the laser's output pulses are time tagged. With Alice utilizing a predefined (known only to Alice) randomized sequence of pulse states, we assume that the laser's period is stable on the order of microseconds, and interpolate to reconstruct the transmitted states for timing analysis. The predefined sequence is not a requirement of the time tagger but is necessary due to limitations of the modulation electronics at the source, which require a preloaded sequence.

To reduce clock drift, we align the time-tagging units' internal clocks to a 10 MHz time-base signal provided by a GPS receiver at each site. Initial synchronization is achieved with the one pulse per second (1 PPS) signal provided by the GPS receivers. Position data are supplied with these signals, which can be used in conjunction with time data to estimate the distance between Alice and Bob, and hence, the time-of-flight of the photons between the source and the receiver.

In our system, photon detections are tagged with a resolution of 156.25 ps, but the 1 PPS signals are accurate to $\approx$100 ns. Additional analysis is required to identify corresponding emission and detection events to within a desired coincidence window of about 0.1 to 1.3 ns. The algorithm to achieve this synchronization utilizes the timing information from Bob's time tags, Alice's transmitted photon states, Alice's and Bob's GPS timing and position data, as well as a small subset ($\approx$5 %) of Bob's measured outcomes. Alice employs a histogram-based optimizing coincidence search within a predefined time span (about 100 ns). The subset of Bob's revealed measured outcomes (which are discarded from the final key) are also used to estimate the QBER to commence the error correction stage of the QKD protocol.

Once coincident events have been identified and noncoincident events removed, Alice performs basis sifting of her raw key to produce her sifted key and transmits a list of indices to Bob, which he utilizes to equivalently sift (for both time and basis, simultaneously) his photon detection events.

D. Error correction

Low-density parity-check (LDPC) codes are highly suitable for satellite-based QKD due to the low communication overhead required and the inherent asymmetry in the computational complexity at each site. First, Alice prepares an $M \times N$ irregular [34] parity-check matrix, where N is the sifted key block size, and M is based on the QBER estimate obtained during timing analysis. We use progressive-edge growth software [34] (modified from [35]), employing known optimal degree distribution profiles [36,37], to generate the parity-check matrix. Alice then transmits the matrix in a compact form to Bob over a classical channel. For each N-bit block of his sifted key, Bob runs an efficient linear algorithm to compute a syndrome using this matrix, and transmits it to Alice.

Alice then attempts to reconcile her sifted key assuming that Bob's sifted key is "correct" (it remains unchanged throughout this process). For each block of sifted key, Alice's goal is to resolve Bob's key vector $\mathbf{x}$, based on her key vector $\mathbf{y}$, Bob's syndrome $\mathbf{s}$, the parity-check matrix, and the estimated QBER. To accomplish this task, Alice employs *belief propagation*, an iterative message passing decoding algorithm, also known as the sum-product algorithm [38,39]. Our sum-product LDPC decoder is written in C# and is based on that found in [40]. Upon success, Alice and Bob both possess the N-bit error-corrected key block $\mathbf{k}_{\mathrm{EC}} = \mathbf{x}$ and obtain the exact QBER for the quantum transmission E_μ.

By Shannon's channel coding theorem [41] applied to the binary symmetric channel [42], we can deduce a closed-form estimate of the appropriate size of the LDPC matrix based on the (estimated, denoted by a tilde) QBER [43]: $M = N f_{\mathrm{EC}} H_2(\tilde{E}_\mu)$. The decoding step may yet terminate unsuccessfully with a given matrix and key block—the probability of this decreases as M (and thus f_{EC}) is increased. In the case of such a termination, we may either discard the key block or retry the algorithm with an augmented matrix containing all the rows of the previous matrix, similar to the "nested" LDPC codes proposed in [44]. In a satellite mission, the choice can be based on the availability of the classical communication channel. Our implementation exhibits efficiencies (f_{EC}) ranging from 1.1 to 1.5.

The silent failure probability of the belief propagation procedure—i.e., the probability that the process terminates successfully but there remains one or more uncorrected bits—is not well characterized in existing literature. While we have not observed any silent failures during our testing, we cannot be certain that $\epsilon_{\mathrm{EC}} = 10^{-10}$ is achieved. To ensure such certainty, one could calculate, reveal, and compare a fingerprint hash of $\mathbf{x}$ and $\mathbf{k}_{\mathrm{EC}}$. (Such an approach using 128-bit MD5 sums [45], for example, yields a collision probability, and thus a silent failure probability, of order $2^{-128} \approx 3 \times 10^{-39}$.) To account for the revealed bits, the final key length would need to be reduced by the same (constant) number of bits. Because the necessity of these extra steps and the specific method of implementation are unclear, we do not perform these steps here.

E. Privacy amplification

The error-corrected key block $\mathbf{k}_{\mathrm{EC}}$ is only partially secure, as some information may have leaked to an eavesdropper (Eve)—we attribute the observed QBER to Eve's interaction with the signal, and all parity information communicated during error correction is known to Eve as it was transmitted over a public channel. Privacy amplification is employed to create a new, final, key $\mathbf{k}_{\mathrm{F}}$ on which Eve no longer holds more than a negligible amount of information. The procedure consists of applying a *two-universal hash function* [2,46] to $\mathbf{k}_{\mathrm{EC}}$ to produce a provably secure key block $\mathbf{k}_{\mathrm{F}}$ of length $L < N$ (recall N is the sifted key block size). L is obtained by multiplying R of Eq. (6) by the number of pulses sent. For mitigating the nonlinear length reduction due to finite-size effects, N should be kept above a certain value, typically $\sim 10^5$, as finite-size effects heavily impact keys with lower N. This value is taken into consideration when selecting a hash function.

Privacy amplification is a symmetric operation which needs to be performed by both Alice and Bob. The choice of hash function dictates the computational complexity of the process and the amount of classical communication required. In our implementation, the privacy amplification procedure loosely follows the methodology outlined in [46]—however, we have made some alterations to their model and developed a different matrix multiplication procedure suitable for efficient implementation in hardware. Briefly, we employ the Toeplitz matrix [47] construction implemented using a shift register.

A Toeplitz matrix has constant descending left-to-right diagonal elements. An $L \times N$ Toeplitz matrix can be written as

$$T_{\mathbf{r}} = \begin{bmatrix} r_L & r_{L+1} & \cdots & & & & \cdots & r_{N+L-1} \\ r_{L-1} & r_L & r_{L+1} & \cdots & & & \cdots & r_{N+L-2} \\ \vdots & & \ddots & & & & & \vdots \\ r_2 & \cdots & r_{L-1} & r_L & r_{L+1} & \cdots & \cdots & r_{N+1} \\ r_1 & r_2 & \cdots & r_{L-1} & r_L & r_{L+1} & \cdots & r_N \end{bmatrix}. \tag{7}$$

A Toeplitz matrix is a two-universal hash function [33]. Note that a Toeplitz matrix $T_{\mathbf{r}}$ is completely defined by the $(N + L - 1)$-bit vector $\mathbf{r} = (r_1, r_2, \ldots, r_{N+L-1})$, thus its storage and transmission requirements are considerably reduced. Furthermore, an $L \times N$ matrix of the form $U_{\mathbf{r}} = (I_L | T_{\mathbf{r}})$, i.e., a concatenation of an L-dimensional identity matrix I_L and an $L \times (N - L)$ Toeplitz matrix $T_{\mathbf{r}}$, is also a two-universal hash function as we require, but requires only $N - 1$ bits to define [48,49].

Following error correction, Alice generates such a matrix by constructing a random binary string $\mathbf{r} = (r_1, r_2, \ldots, r_{N-1})$ of length $N - 1$, and then transmits $\mathbf{r}$ to Bob over the classical channel. Alice and Bob then use $\mathbf{r}$ and a shift register to apply the hash matrix $U_{\mathbf{r}}$, computing the final secure key, $\mathbf{k}_{\mathrm{F}} = U_{\mathbf{r}} \mathbf{k}_{\mathrm{EC}}$.

In our implementation, the identity portion of each row of $U_{\mathbf{r}}$ uses no space and can be accounted for with a simple logical AND operation. We represent $T_{\mathbf{r}}$ as an $(N - L)$-bit logical shift register. Initially, the shift register contains the last $N - L$ bits of $\mathbf{r}$ $(r_L, r_{L+1}, \ldots, r_{N-1})$. The remaining bits from $\mathbf{r}$ are used as input for the shift register. In this way we conserve memory by never needing to store full matrices.

The logical shift register is broken up into multiple 32-bit blocks, each of which is designed to fit inside a register on a processing unit. The register size of 32 bits is chosen for the support of multiple platforms, including our low-power ARM

test board. 64-bit platforms are also available, and with single instruction, multiple data (SIMD) extensions, commonplace in contemporary desktop processors, the register could be 256 bits or larger.

After privacy amplification, Alice and Bob are left with a secure key of L bits which can then be used to encrypt data transmitted on a classical channel through, e.g., one-time pad. We assume here that channel authentication is performed separately, possibly using some of the secure key (reducing the length available for encryption).

III. APPARATUS

Our QKD system, shown in Fig. 1, consists of a weak coherent pulse (WCP) source, a variable-loss free-space channel, and a compact four-outcome (two passively chosen measurement bases) quantum receiver. The source utilizes up-conversion (sum frequency generation) from two orthogonally oriented type-I periodically poled potassium titanyl phosphate (PPKTP) crystals to produce photon pulses at 532 nm wavelength from a mode-locked Ti:sapphire laser at 810 nm, operating at a rate of 76 MHz, and a continuous-wave laser at 1550 nm.

Diagonally polarized 810 nm laser pulses are combined with polarization- and intensity-modulated 1550 nm laser light (controlled by efficient telecom waveguide modulators [26]) to generate 532 nm pulses possessing the short pulse width and high repetition rate of the 810 nm laser, as well as the intensity and polarization of the 1550 nm light. Phase randomization between pulses, necessary to ensure security, is provided by the short coherence time of the 1550 nm laser (less than the pulsing period of the 810 nm laser, but much more than the pulse duration). Birefringent wedges precompensate the 810 nm light for temporal walk-off in the PPKTP crystals.

The photon pulses produced are coupled into a single-mode fiber. A fiber splitter sends ≈0.3 % of photons to a thick-silicon avalanche photodiode (Excelitas SPCM-AQ4C) to measure the average photon number per pulse. The remaining photons are sent to a free-space quantum channel consisting of a bare fiber output followed by a 3-in.-diameter lens on a longitudinal translation stage. The loss is adjusted by varying the position of the lens, changing the amount of light directed into the receiver by making the beam more or less divergent.

The quantum receiver, Fig. 2, is built using Thorlabs' cage system. The receiving telescope consists of a 5 cm diameter, 25 cm focal length collection lens followed by a 6.5 mm diameter, 11 mm focal length collimating lens. Passive measurement basis choice is implemented by coupling polarization discrimination apparatuses to two orthogonal outputs of a pentaprism beam splitter, each of which transmits approximately 47.5% of the injected power. (A pentaprism was chosen for potential application in future experiments—a 50:50 beam splitter would also suffice as we do not here use the pentaprism's third output.)

Polarization analysis is done by a 5 mm cubic polarizing beam splitter (PBS) in each arm, directing photons to one of four detector assemblies. Measurement in the diagonal basis is obtained by physically orienting (to 45°) the PBS and detectors around the beam path, relative to the other PBS (which defines the rectilinear basis). Following each analysis PBS, a second

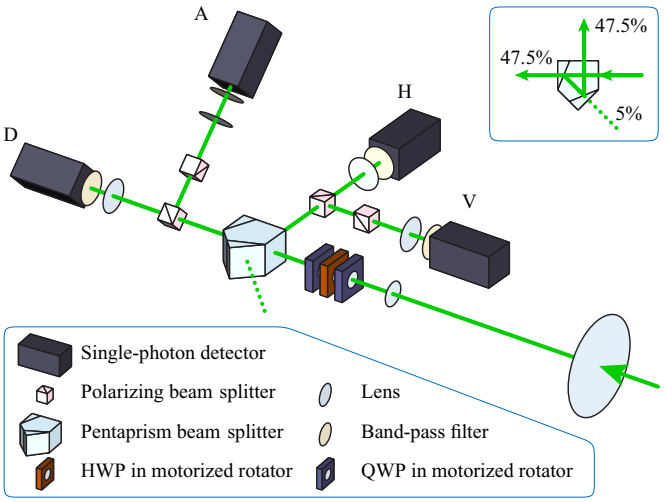

FIG. 2. (Color online) High-loss QKD receiver. Photons are captured by the telescope and pass through motorized-rotating half- and quarter-wave plates, correcting unwanted polarization rotations. The pentaprism beam splitter provides a passive basis choice between rectilinear and diagonal polarization bases. A polarizing beam splitter (PBS) in each basis arm discriminates H/V and D/A polarized photons, the latter by physically orienting the PBS 45° around the beam path. An extra PBS in each reflected arm reduces erroneous counts from device imperfections. Lenses focus the beams onto single-photon detectors, while band-pass filters reduce background light.

PBS, oriented at 90°, is used to suppress erroneous optical signal in the reflected path (owing to device imperfection).

Each detector assembly contains a spatial-filtering shield and a 2 nm band-pass filter to suppress background noise. Photons are focused by 6 cm focal length lenses and detected by thin-Si avalanche photodiodes from Micro Photon Devices, which feature good detection efficiency (≈50%), low dark counts (≈20 cps), and low jitter ($\leqslant$ 50 ps). Temporal filtering with a narrow (∼1 ns) time window allows us to accept signal photons while rejecting remaining background and dark counts with high fidelity. The background yield Y_0 is estimated by counting photon detections between pulses. Though this approach is known to be insecure, it suffices for our proof-of-concept demonstration.

Data are acquired by two time-tagger units, and processed by two x86-64 computers (and, when testing algorithmic performance, an ARM board) on a local-area network (LAN). Each time-tagger unit is connected to 10 MHz and 1 PPS signals coming from a GPS receiver. The signals from the source are connected to Alice's time tagger and the four outputs of Bob's detectors are connected to Bob's time tagger.

Our receiver also includes an arbitrary polarization rotation assembly, consisting of quarter-wave plates (QWPs) before and after a half-wave plate (HWP) mounted in motorized rotation stages, allowing the compensation of any unitary polarization change in the channel. We have developed an automated polarization alignment protocol which characterizes the effect of the channel on the known QKD polarization states, measuring the quantum signal directly, sufficient to then determine an optimal compensation implemented by the arbitrary polarization rotation assembly.

IV. RESULTS

A. Post-processing resource requirements

For a satellite uplink scenario, optical signals are sent from the ground when the satellite orbits over an optical ground station, while classical communication is performed—possibly at a later time—when the satellite orbits over one or more radio frequency (rf) ground stations. Hence, the satellite system must store all time tags accumulated during the optical station flyover, performing all classical steps of the QKD protocol during an rf station flyover when a classical communication link is present. Specifically, Bob must store: time tags, measurement bases, photon detections (bit values), and data defining the error correction LDPC matrix and privacy amplification Toeplitz matrix.

Our time-tagging hardware produces 64-bit time tags. To save on the limited memory and classical communications bandwidth available to a satellite, it is possible to reduce that number significantly, at the expense of additional computation steps. One simple scheme is to store the full time tag only at the beginning of every second of data collection, together with additional information provided by the GPS receiver (which outputs a data packet every second). In this way, the space required to store the time tag and measurement outcome information is 40 bits.

To further save memory and classical communications bandwidth, the sparse LDPC matrix for error correction can be efficiently transmitted and stored as an adjacency list where only the indices of each nonzero element in each row are recorded. If the decoding step fails, we must then retry with a larger matrix (or discard the block), implying an increase of f_{EC}, i.e., worse efficiency.

The embedded processing component of the satellite-side software is tested on an inexpensive (≈$150), low-power (2 W) Freescale i.MX53 QSB single-board computer featuring a 1 GHz single-core ARM processor and 1 GiB of RAM. The measured performance, Table I, illustrates successful operation within reasonable resource constraints. We have found that in our system the limiting factor for Bob is the privacy amplification step, which requires a relatively long processing time. For all other processes, the limiting factor is not Bob's computational power, but rather Alice's, and the 100 Mbit Ethernet link between them. A future implementation could have a far more powerful computer at Alice than what we have used for our demonstration.

TABLE I. Measured performance of the satellite-side QKD process running on a Freescale i.MX53 embedded ARM board processing 300 s of QKD data (28.8 dB loss data with rate-limiting applied; see text). Here privacy amplification is applied without incorporating finite-size effects which reduce secure key length, giving us upper bounds on resource usage. As expected, processing time scales quadratically with the photon detection rate—a least-squares quadratic fit gives a coefficient of determination $R^2 = 0.9992$.

Detection rate (Hz)	Sifted key rate (Hz)	QBER (percent)	Processing time (s)	RAM used (Mbyte)
500	229	3.43	0.5	11.19
1 000	457	3.44	1.1	20.42
5 000	2 326	3.53	14.5	70.09
10 000	4 647	3.57	56.3	71.70
20 000	9 286	3.55	772.1	75.47
30 000	13 924	3.54	2013.1	79.38
41 887	19 428	3.54	3969.4	84.52

For computational requirements analysis, we collect experimental data for 300 s at a receiver detection rate of about 42 kHz. Each 1-s chunk of this data is then truncated to produce various effective detection rates. Table I shows detailed memory and CPU usage for the embedded processing component. Privacy amplification complexity is asymptotically quadratic in the block size N due to the matrix multiplication process, while all other post-processing steps behave linearly. Hence, we expect the processing time of the QKD post-processing to overall scale quadratically with the detections, as is observed. Note that we do not expect the number of detections to exceed 1×10^7 over a single satellite pass using feasible quantum sources [19].

B. Experimental secure key extraction

We perform the experimental demonstration for losses ranging from 28.8 to almost 60 dB, determined from the photon detection rate (corrected for background) with respect to the transmitted optical power. The loss therefore includes both channel loss (variable) and receiver efficiency (fixed 1.5 dB for receiver optics and 3 dB for detector efficiency). The temporal filter window width is adjusted to improve the secure key rate for each value of loss, and ranges from 1.3 ns at low loss to 0.1 ns at high loss. The measured QBER of signal states ranges from 1.94% to 6.06%, with raw key rate (total detections within the temporal filter window, per second) ranging from 38211 Hz at 28.8 dB to 44.2 Hz at 56.5 dB, while the background detection rate ranges from 151 to 2.38 Hz (see Fig. 3).

Our experimental results incorporate the full error correction and privacy amplification post-processing. To limit computational time we artificially restricted the error correction block size to 600 000 (with the sifted key split into the necessary number of blocks). Privacy amplification was implemented over the full sifted-key length of error-corrected key bits in order to minimize finite size effects. We achieve error correction efficiencies between 1.12 and 1.50 (with better efficiencies at higher QBER, as predicted by [50]) and privacy amplification to $\epsilon = 10^{-9}$ security. The extracted secure key rate is shown in Fig. 4 for asymptotic extrapolations to the infinite limit of key length [Eq. (1)]. At the highest loss, 56.5 dB, our system is able to extract 0.5 bit/s of secure key in the asymptotic limit. This is comparable to the result of a previous high-loss demonstration [22] which reached 2 bit/s at 57 dB (the achievable rate there being inferred without implementing the complete QKD protocol). We note that the key rate can be readily improved by employing a faster source—QKD WCP sources have been demonstrated in the GHz range [5,51], more than an order of magnitude above our 76 MHz source rate.

Given that the apparatus remains sufficiently stable, the particular finite duration over which data are collected in this experiment is arbitrary. For our results, each data run lasts 5 to 10 min. With such times, when incorporating finite-size statistics [Eq. (6)] we find positive secure key rates for points up to 45.6 dB. For higher losses, there is insufficient statistics

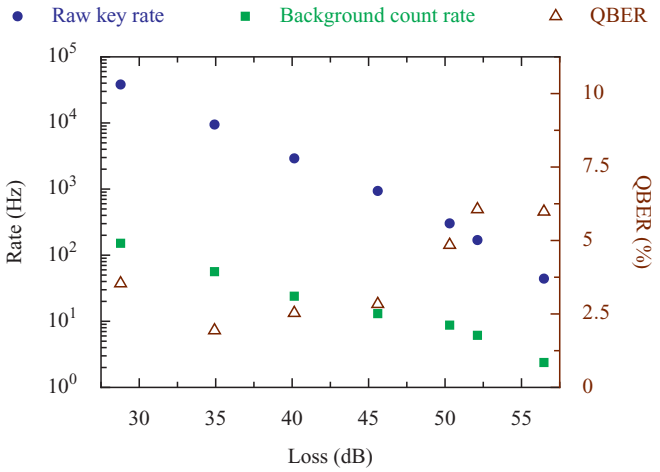

FIG. 3. (Color online) Measured raw key rate, background detection rate, and QBER obtained in different loss regimes, with a source pulsing at 76 MHz. The raw key and background rates include only detections that fall within the temporal filter window. The background rate (the product of the vacuum yield Y_0 and the pulsed laser frequency) is determined by measuring the counts received between laser pulses. At lower loss, the background term is dominated by light from the 1550 nm laser and some continuous wave component remaining in the pulsed 810 nm laser. Variations in QBER between runs are mainly due to laboratory temperature fluctuations which affected the birefringence of the optical fiber and the performance of the 1550 nm modulators. Loss includes both channel loss (variable) and receiver efficiency (fixed 4.5 dB).

to produce nonzero key under the condition of 10σ worst-case variation. As the detriment of finite-size effects is due to the limited number of photon counts, a faster source can also mitigate this.

Based on the measured experimental parameters, we can extrapolate the raw key rates and determine the achievable finite-size secure key rate if the apparatus was run for

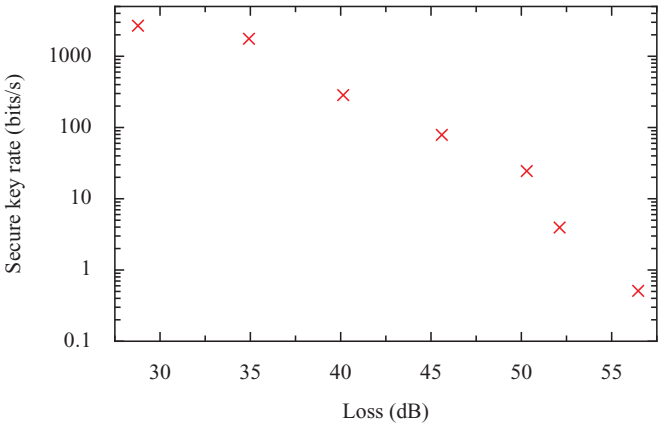

FIG. 4. (Color online) Secure key rate (lower bound) in the infinite limit for data measured in different loss regimes. The secure key rate tends to decrease as the loss increases, with some fluctuation about the trend due to variations in the source tuning and channel parameters throughout the data collection campaign. Loss includes both channel loss and receiver efficiency.

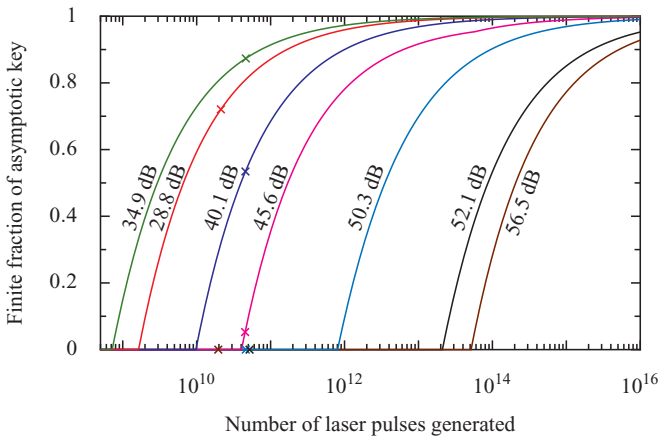

FIG. 5. (Color online) Finite-sized secure key rate as a fraction of the corresponding asymptotic secure key rate, given the total number of laser pulses transmitted. Curves are shown for experimental parameters corresponding to each of the loss conditions demonstrated, as indicated by labels beside each curve. Crosses indicate the value that was reached in the experiment. Lowest losses only require around 10^{10} pulses to exceed 80% of the asymptotic key rate. For the highest losses to reach this amount, significantly more pulses, 10^{14} to 10^{15}, must be transmitted due to the reduced signal-to-noise. Note these curves indicate secure key rates relative to those that could be achieved in the asymptotic limit, not absolute rates.

longer times or multiple runs under the same conditions were concatenated. Figure 5 shows the ratio of the asymptotic key rate that can be achieved by the finite secure key (R/R_∞), for a given total number of pulses transmitted, for each experimental loss condition we examine. For the lowest losses, only about 10^{10} pulses is necessary to reach over 80% of the asymptotic key rate, equating to a few minutes of collection time with our 76 MHz source. More time is required for higher losses: several weeks of continuous collection at 76 MHz, for the highest losses. Interestingly, we find that the 34.9 dB data produces nonzero secure key sooner than the 28.8 dB data—this is owing to the relatively high QBER at 28.8 dB. Our results consistently show a significantly higher decoy QBER compared to the signal QBER. This was caused by the intensity modulator which was found to produce a slight polarization shift that is dependent on the applied modulation, causing the two different intensity levels to have slightly different polarizations before being polarization modulated, leading to a difference in the optimal alignment for the two intensity levels. This polarization shift could be corrected by the addition of a polarizer after the intensity modulator, eliminating the polarization difference between the two states. Although this difference does not invalidate our proof-of-concept demonstration, removing it is crucial in a secure implementation as it leads to distinguishability between signal and decoy states which could be used by an eavesdropper to gain information. Removing this difference may also improve final key rates as it would reduce decoy QBER without affecting signal QBER. Our system alignment is optimized for the signal QBER.

The results presented here are comparable to the regime of a satellite uplink, where the usable part of a pass is expected to

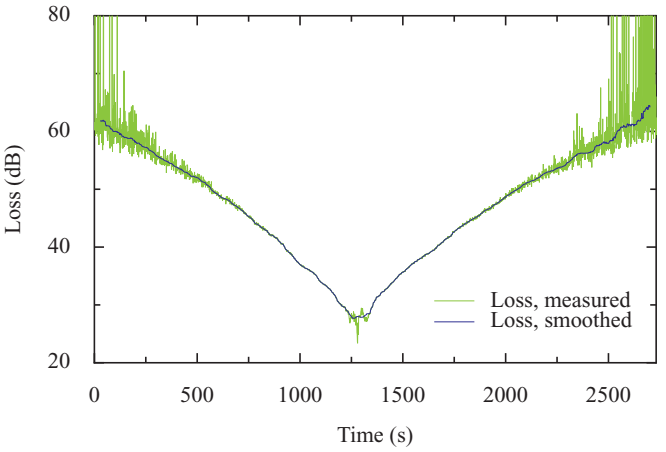

FIG. 6. (Color online) Experimentally measured loss over the 45 min data collection used to simulate the varying loss of a satellite pass. The data are smoothed by taking the median value of a 29 s moving window. These smoothed values are used to select experimental data that tracks the theoretical loss of a satellite pass while maintaining the natural statistical fluctuations.

vary typically between 40 and 55 dB loss [19], and help support the conclusion that our approach is suitable for eventual satellite implantation (though a faster source may be advised). To more closely examine the feasibility of our approach in the regime of a satellite uplink for QKD, we simulate several satellite passes by varying the position of the quantum-channel lens (thus varying the loss) during an experimental run. We do this once, the total run lasting approximately 45 min, with the loss changing smoothly from ≈63 dB to a minimum of ≈28 dB after about 21 min, and then back to ≈62 dB over the remaining time. The data accumulated are segmented into 1 s blocks, with the measured loss for each second over the duration of the experiment shown in Fig. 6.

We redistribute select 1 s blocks of raw key data in such a way that we obtain data sets that reproduce the statistics expected for real satellite uplink orbits [19]. The passes considered are the best, upper-quartile, and median passes (in terms of contact time) over a hypothetical ground station located at 45° latitude of a year-long 600 km circular Sun-synchronous low Earth orbit. The predicted losses are based on uplink at a wavelength of 785 nm, with a receiver diameter of 30 cm, a 2 μrad pointing error, and a rural sea-level atmosphere. The differences with our system (which has 532 nm wavelength and 5 cm receiver diameter) are necessary to mitigate the increased geometric losses over the long distance link of a satellite (requiring larger receiver diameter) and the effect of atmospheric turbulence and transmission (reduced at 785 nm compared to 532 nm). Both our 532 nm system and the expected 785 nm system utilize the same Si avalanche photodiode technology. Analyzing our experimental data possessing these theoretical losses is therefore a valid proof-of-concept demonstration.

The experimental data are smoothed by taking the median of a moving window of 29 s width, the result illustrated in Fig. 6. We use these smoothed data to select 1 s experimental data blocks to include in our analysis for each orbit by progressively scanning (from the center, in either direction) in 1 s steps for

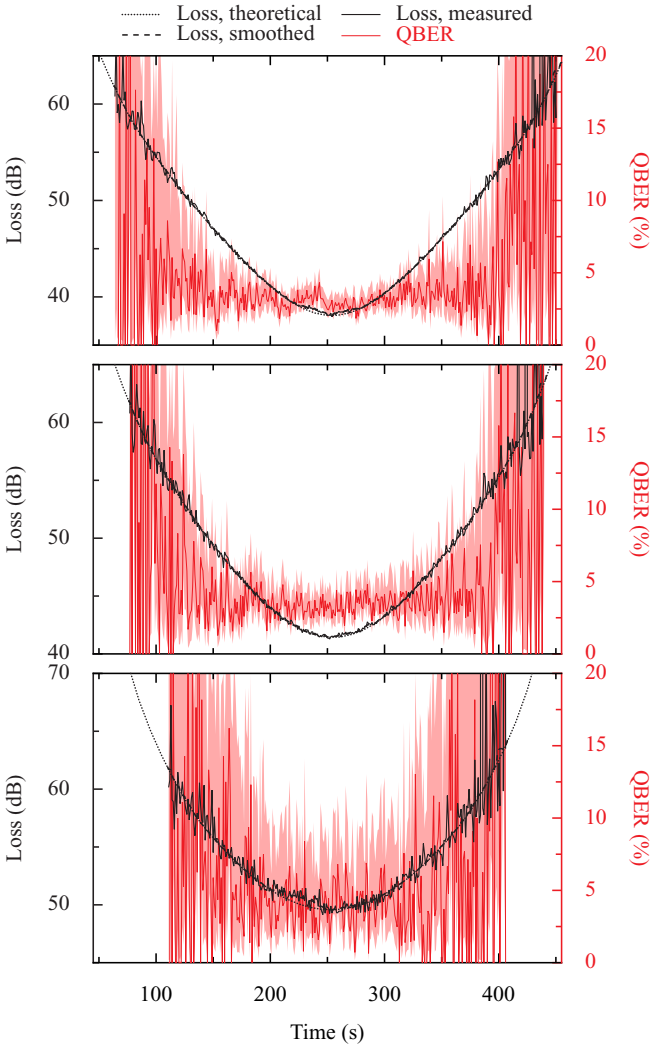

FIG. 7. (Color online) QBER and total loss of data sets reconstructed from measured data (shown in Fig. 5) for three representative satellite pass conditions: best pass (top), upper-quartile pass (middle), and median pass (bottom). The predicted loss is based on an uplink with a 600 km circular Sun-synchronous low-Earth-orbit satellite at a wavelength of 785 nm, with a receiver diameter of 30 cm, a 2 μrad pointing error, and a rural sea-level atmosphere. Smoothed loss follows the moving median determined at each 1 s experimental data block selected. Measured loss and QBER derive from the selected data, with shaded regions indicating the QBER 95% credible interval based on a uniform Bayesian prior. For the best pass, we obtain 3374 bit of secure key, including finite-size statistical effects.

the next 1 s data block that possesses smoothed loss matching or exceeding the theoretical orbit loss prediction. By selecting experimental data at points where the smoothed loss is matched to theoretical link predictions, we ensure that the data we sample are not biased by normal fluctuations in measured loss.

Figure 7 shows the three relevant losses—the theoretically predicted loss, the smoothed loss value at the sampled point, and the experimentally measured loss from the sampled point—and the estimated QBER for each representative pass. The measured losses of the sampled experimental data closely match the trend of the theoretical prediction, while maintaining realistic fluctuation. At higher losses the

TABLE II. Experimentally measured quantities for various loss conditions, including constant and varying losses simulating a satellite pass. Loss includes both channel loss and receiver efficiency. Except for rates extrapolated to a 300 MHz signal rate as indicated, all parameters are based on measurements with our 76 MHz pulsing laser source. Values here are incorporated into Eqs. (1) and (6) to determine the appropriate size of the privacy amplification matrix (Sec. II E), and thus the final secure key length. Where necessary for the finite-size heuristic, uncertainties (1σ) are also given.

Loss (dB)	28.8	34.9	40.1	45.6	50.3	52.1	56.5	Best	Upper-quartile	Median
Duration (s)	289	606	599	593	606	682	257	390	365	297
Mean detection rate (Hz)	41 926	10 464	3349	1167	427	301	186	1650	956	278
Signal detections, N_μ (10^3)	11 043	5 739	1746	556	184	116	11.4	544	279	43.4
Decoy detections, N_ν (10^3)	82.5	57.2	16.1	6.72	1.98	1.19	0.156	5.63	2.88	0.489
Vacuum detections, N_0 (10^3)	43.8	34.2	14.4	7.75	5.30	4.19	0.612	4.64	3.32	1.50
Signal photon number, μ	0.506	0.490	0.507	0.579	0.534	0.503	0.581	0.505	0.507	0.512
Decoy photon number, ν	0.0392	0.0419	0.0515	0.0723	0.0517	0.0486	0.0592	0.0568	0.0571	0.0507
Signal QBER, E_μ (%)	3.54	1.94	2.53	2.84	4.85	6.06	5.98	3.12	3.46	4.35
Uncertainty, σ (10^{-2} %)	0.566	0.581	1.20	2.26	5.14	7.24	22.4	2.15	3.52	10.0
Decoy QBER, E_ν (%)	38.8	13.0	19.0	7.28	11.5	14.9	23.9	14.1	14.2	17.7
Uncertainty, σ (10^{-1} %)	2.17	1.51	3.44	3.29	7.62	11.2	39.1	4.55	7.04	19.0
Signal vacuum QBER, E_0^μ (%)	50.8	52.0	50.4	50.6	50.3	50.4	50.5	50.6	50.7	50.7
Decoy vacuum QBER, E_0^ν (%)	42.0	32.6	42.5	44.7	47.4	47.2	48.2	45.9	45.5	44.6
Signal gain, Q_μ (10^{-6})	568	136	41.8	13.5	4.34	2.43	0.634	20.1	11.0	2.10
Uncertainty, σ (10^{-8} %)	17.1	5.67	3.16	1.81	1.01	0.715	0.595	3.00	2.08	1.01
Decoy gain, Q_ν (10^{-7})	496	158	45.0	19.0	5.48	2.92	1.02	24.3	13.3	2.77
Uncertainty, σ (10^{-8} %)	17.3	6.61	3.55	2.32	1.23	0.848	0.817	3.54	2.47	1.25
Single photon gain, Q_1^{L} (10^{-6})	370	111	24.5	7.70	2.65	1.31	0.400	12.1	6.35	1.10
Single photon QBER, E_1^{U} (%)	5.26	2.16	3.93	4.21	2.75	3.59	7.27	4.80	5.42	6.51
Vacuum yield, Y_0 (10^{-7})	20.6	7.39	3.14	1.71	1.15	0.806	0.312	1.56	1.19	0.665
Uncertainty, σ (10^{-9} %)	9.85	4.00	2.62	1.94	1.58	1.25	1.26	2.41	2.07	1.72
Error correction efficiency, f_{EC}	1.41	1.50	1.40	1.35	1.17	1.12	1.13	1.26	1.223	1.15
Raw rate (bits/s)	38 211	9 470	2915	938	303	169	44.2	1395	765	146
Sifted rate (bits/s)	19 298	3 802	1447	469	150	84.1	21.7	694	379	71.6
Secure rate (asymptotic) (bits/s)	2 684	1 761	285	79	24.5	3.95	0.510	120	49.1	2.96
Secure rate (finite-size) (bits/s)	1 935	1 539	152	5.39	–	–	–	8.65	–	–
At 300 MHz, projected (bits/s)	12 806	8 683	1190	234	–	–	–	372	59.1	–
Total finite-size key (kbits)	559	932	91.2	3.20	–	–	–	3.37	–	–
At 300 MHz, projected (kbits)	3 701	5 262	713	138	–	–	–	145	21.6	–

per-second QBER estimate has significant fluctuations due to the reduced sample size.

Performing the post-processing steps on these data sets and incorporating finite-sized statistics, we are able to extract a 3374 bit secure key from the best pass, out of a total of 544 056 bit raw key (643 521 detection events) with an average of 3.1% QBER in the signal. This result shows that even with our modest 76 MHz source a positive key rate can feasibly be generated from one pass (albeit a good one) of a typical low-Earth-orbit satellite receiver. In comparison, the upper-quartile pass receives 279 317 bit raw key (348 896 detections) with an average of 3.5% QBER, but this is insufficient to produce nonzero secure key with finite-sized effects considered (the asymptotic secure key is 17 916 bit). Similarly, the median pass with 43 375 bit raw key (82 470 detections) and average 4.4% QBER also cannot extract nonzero finite-sized secure key (asymptotic, 877 bit).

Improvements to the source could mitigate finite-sized statistical effects. By adjusting the photon and pulse count parameters, we can predict the performance of a 400 MHz source that produces $\frac{3}{4}$ signal (i.e., a 300 MHz signal rate, as per [19]), $\frac{1}{8}$ decoy, and $\frac{1}{8}$ vacuum pulses. With other measured parameters left unchanged, 21 570 bit secure key could be extracted from a single upper-quartile pass. This is directly comparable to the estimation of [19]—under better conditions (e.g., E_ν assumed equal to E_μ, intrinsic source QBER of 1%, $\nu = 0.1$, $f_{\mathrm{EC}} = 1.22$, and background estimate used only in calculation of E_μ while setting $Y_0 = 0$), a 111.3 kbit secure key was predicted.

Alternatively, finite-size effects could be reduced by combining the measurements of multiple passes. For example, we are able to combine the measurements of three upper-quartile passes—each independently unable to produce positive finite key—and thereby extract 165 bit of secure key with finite-sized statistics. (Significantly more median passes, around 215 combined, would be required to yield a positive finite-size secure key.) This might be a useful method to extract longer secure keys from the results of multiple marginal or individually unfruitful satellite passes.

The quantities measured in the experiment are summarized, in Table II, for each of the fixed loss cases and for each of the three varying-loss satellite-pass simulations. These are the values we use in Eqs. (1) and (6) to determine the secure key length.

V. DISCUSSION AND CONCLUSION

We have demonstrated the feasibility of satellite QKD using a quantum optical uplink by successfully performing QKD at losses up to 56.5 dB in the laboratory, with reduced computational requirements at the receiver, compatible with those that can be achieved on a satellite platform. We have improved over a previous high-loss demonstration [22] by implementing complete QKD protocols, including twin-basis measurements, error correction, and privacy amplification. We have also considered the effect of statistical fluctuations on the finite key length and have shown, by successfully performing full QKD and by extrapolation with varying losses that match those that would be experienced during representative passes of a satellite, that such a system is viable.

Several improvements to our system are possible as a next step, improving the key rate and moving our system towards being immediately deployable. One necessary modification to ensure secure QKD would be to employ a truly random source at Alice, rather than a fixed-length repeating pseudorandom sequence. Suitable high-speed electronics to implement this in tandem with a source with increased pulse rate could provide true security while significantly improving key rates above those reported here. While increased rates would necessitate more processing at the receiver, our analysis of computational requirements shows that detection rates could be increased by an order of magnitude or more over the demonstrated best-pass rate with processing at the receiver remaining feasible.

A particularly important challenge of satellite QKD yet to be addressed is the varying time-of-flight due to the changing distance between the satellite and ground station during a pass. For a 600 km orbit the distance between the satellite and ground station will vary by up to 7 km/s [19], leading to a time-of-flight varying by up to 23 μs per second. Correcting for such variation as part of the timing analysis is straightforward, in principle, but is beyond the scope of the present work. Notably, though not of the same magnitude, varying time-of-flight due to relative motion has been demonstrated in the context of QKD for moving transmitters [52,53] and, very recently, a moving receiver [54].

Additionally, our theoretical prediction of loss for a satellite pass is based on a 30 cm diameter receiver at 785 nm, while our system uses a 5 cm receiver and operates at 532 nm. These differences do not affect the proof-of-concept demonstrated in this paper nor the basic design of our apparatus as the operating principles are the same in either case. However, the optimal parameters will need to be satisfied to ensure success of a satellite uplink—the increased telescope diameter is necessary to reduce the geometric losses, and the 785 nm wavelength is necessary to provide the best balance between diffraction, atmospheric absorption and turbulence, and detector efficiency [19]. Together with a sufficiently accurate pointing mechanism, these engineering challenges for implementing a quantum receiver satellite payload are manifestly achievable in the near term.

ACKNOWLEDGMENTS

We thank Chris Erven for valuable input and NSERC, Canadian Space Agency, CFI, CIFAR, Industry Canada, FedDev Ontario, and Ontario Research Fund for funding. B.L.H. acknowledges support from NSERC Banting Postdoctoral Fellowships (Canada).

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India, 1984), pp. 175–179.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[3] idQuantique, http://www.idquantique.com/ (2015).

[4] MagiQ Technologies, http://www.magiqtech.com/ (2015).

[5] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, Nat. Photon. **1**, 343 (2007).

[6] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Free-space distribution of entanglement and single photons over 144 km, Nat. Phys. **3**, 481 (2007).

[7] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, Phys. Rev. Lett. **98**, 010504 (2007).

[8] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres, New J. Phys. **11**, 075003 (2009).

[9] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Decoy-state quantum key distribution with polarized photons over 200 km, Opt. Exp. **18**, 8587 (2010).

[10] Z. Yan, D. R. Hamel, A. K. Heinrichs, X. Jiang, M. A. Itzler, and T. Jennewein, An ultra low noise telecom wavelength free running single photon detector using negative feedback avalanche diode, Rev. Sci. Instrum. **83**, 073105 (2012).

[11] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre, Nat. Photon. **9**, 163 (2015).

[12] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, Phys. Rev. Lett. **81**, 5932 (1998).

[13] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup,

and R. J. Young, Quantum memories, Eur. Phys. J. D **58**, 1 (2010).

[14] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).

[15] G. Gilbert and M. Hamrick, Practical Quantum Cryptography: A Comprehensive Analysis (Part One), Tech. Rep. MTR00W0000052 (The MITRE Corporation, 2000), arXiv:quant-ph/0009027.

[16] J. E. Nordholt, R. J. Hughes, G. L. Morgan, C. G. Peterson, and C. C. Wipf, Present and future free-space quantum key distribution, in *Proceedings of SPIE on Free-Space Laser Communication Technologies XIV*, edited by G. S. Mecherle (SPIE, San Jose, USA, 2002), Vol. 4635, pp. 116–126.

[17] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lütkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, and A. Zeilinger, Space-QUEST, Experiments with quantum entanglement in space, Europhys. News **40**, 26 (2009).

[18] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, Feasibility of satellite quantum key distribution, New J. Phys. **11**, 045017 (2009).

[19] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, New J. Phys. **15**, 023006 (2013).

[20] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, Daylight quantum key distribution over 1.6 km, Phys. Rev. Lett. **84**, 5652 (2000).

[21] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, Ground to satellite secure key exchange using quantum cryptography, New J. Phys. **4**, 82 (2002).

[22] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein, How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss, Phys. Rev. A **84**, 062326 (2011).

[23] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[24] R. Renner, Security of quantum key distribution, Ph.D. thesis, ETH Zurich, 2005, arXiv:quant-ph/0512258.

[25] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[26] Z. Yan, E. Meyer-Scott, J.-P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. Hübel, and T. Jennewein, Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links, J. Lightwave Technol. **31**, 1399 (2013).

[27] R. Y. Q. Cai and V. Scarani, Finite-key analysis for practical implementations of quantum key distribution, New J. Phys. **11**, 045024 (2009).

[28] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Efficient decoy-state quantum key distribution with quantified security, Opt. Express **21**, 24550 (2013).

[29] S.-H. Sun, L.-M. Liang, and C.-Z. Li, Decoy state quantum key distribution with finite resources, Phys. Lett. A **373**, 2533 (2009).

[30] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[31] V. Scarani and R. Renner, Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing, Phys. Rev. Lett. **100**, 200501 (2008).

[32] D. J. C. MacKay and R. M. Neal, Near shannon limit performance of low density parity check codes, Electron. Lett. **33**, 457 (1997).

[33] H. Krawczyk, LFSR-based hashing and authentication, in *Advances in Cryptology—CRYPTO '94*, Lecture Notes in Computer Science, Vol. 839, edited by Y. Desmedt (Springer, Berlin, 1994), pp. 129–139.

[34] X.-Y. Hu, E. Eleftheriou, and D. Arnold, Regular and irregular progressive edge-growth Tanner graphs, IEEE Trans. Inform. Theory **51**, 386 (2005).

[35] X.-Y. Hu, E. Eletheriou, and D. Arnold, Source code for Progressive Edge Growth parity-check matrix construction (2003).

[36] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, Efficient reconciliation protocol for discrete-variable quantum key distribution, in *Proceedings of the 2009 IEEE International Conference on Symposium on Information Theory - Volume 3, ISIT'09* (IEEE, Washington, DC, 2009), pp. 1879–1883.

[37] J. Martinez Mateo, Efficient information reconciliation for quantum key distribution, Ph.D. thesis, Universidad Politecnica de Madrid, 2011.

[38] D. Pearson, High-speed QKD reconciliation using forward error correction, in *Proc. 7th International Conference on Quantum Communication, Measurement and Computing (QCMC), Glasgow, U.K,* AIP Conf. Proc. No. 734 (AIP, Melville, NY, 2004), pp. 299–302.

[39] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, Proof-of-concept of real-world quantum key distribution with quantum frames, New J. Phys. **11**, 095001 (2009).

[40] P. Chan, Low-density parity-check codes for quantum key distribution, Master's thesis, University of Calgary, 2009.

[41] C. E. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. **27**, 379 (1948).

[42] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications and Signal Processing (Wiley-Interscience, New York, 2006).

[43] D. Elkouss, J. Martinez-Mateo, and V. Martin, Information reconciliation for quantum key distribution, Quantum Info. Comput. **11**, 226 (2011).

[44] U. Raviteja and A. Thangaraj, Key reconciliation using nested LDPC Codes, in *14th National Conference on Communications* (Joint Telematics Groups, Bombay, India, 2008), pp. 79–83.

[45] Although MD5 is not cryptographically secure as methods to modify a file while preserving its hash value are known, this does not assist Eve's effort to reconstruct the *same* key as Alice and Bob.

[46] T. Tsurumaru, W. Matsumoto, and T. Asai, QKD Post-Processing Algorithms of Mitsubishi Electric Corporation, AIT QKD Post Processing Workshop 2011.

[47] R. M. Gray, Toeplitz and circulant matrices: A review, Found. Trends Commun. Inform. Theory **2**, 155 (2005).

[48] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 3rd ed. (The Johns Hopkins University Press, Baltimore, MD, 1996).

[49] M. Hayashi, Exponential decreasing rate of leaked information in universal random privacy amplification, IEEE Trans. Inform. Theory **57**, 3989 (2011).

[50] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, Fundamental finite key limits for information reconciliation in quantum key distribution, in *IEEE International Symposium on Information Theory (ISIT), 2014* (IEEE, Piscataway, NJ, 2014), pp. 1469–1473.

[51] H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, and Y. Yamamoto, 10-GHz clock differential phase shift quantum key distribution experiment, Opt. Express **14**, 9522 (2006).

[52] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Air-to-ground quantum communication, Nat. Photon. **7**, 382 (2013).

[53] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan, Direct and full-scale experimental verifications towards ground-satellite quantum key distribution, Nat. Photon. **7**, 387 (2013).

[54] J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, Free-space quantum key distribution to a moving receiver, arXiv:1505.00292.