Decoy-state quantum key distribution with direct modulated commercial off-the-shelf VCSEL lasers

Noel De La Cruz
Photonics Technology Department
The Aerospace Corporation
El Segundo, California
noel.delacruz@aero.org

Uttam Paudel
Photonics Technology Department
The Aerospace Corporation
El Segundo, California
uttam.paudel@aero.org

Pavel Ionov
Photonics Technology Department
The Aerospace Corporation
El Segundo, California
pavel.ionov@aero.org

Ethan H. Tucker
Photonics Technology Department
The Aerospace Corporation
El Segundo, California
ethan.tucker@aero.org

Andrew Mollner
Photonics Technology Department
The Aerospace Corporation
El Segundo, California
andrew.mollner@aero.org

Joseph Touch
ICSD Division
The Aerospace Corporation
El Segundo, California
joseph.touch@aero.org

Joseph Betser
Space System Architect
The Aerospace Corporation
El Segundo, California
joseph.betser@aero.org

Joshua Stoermer
Cloud Platforms & Architectures Department
The Aerospace Corporation
El Segundo, California
joshua.t.stoermer@aero.org

***Abstract*— We report on a BB84 decoy-state quantum key distribution (QKD) system constructed using commercial off-the-shelf (COTS) components. Four 794 nm vertical-cavity surface-emitting lasers (VCSELs) are current-modulated at 10 MHz rate with three power levels to form a decoy state transmitter. The COTS VCSELs exhibit long term stability with high polarization extinction ratio, narrow band operation (sub-nanometer bandwidth), and wavelength tunability and stability suitable for constructing four indistinguishable qubit channels. A 780 nm, 10 MHz time-transfer channel is used for transferring the timing information along with a start and end marker for the qubit transfer period. Internally-developed transmitter laser drivers and receiver detectors are controlled and read out with COTS system-on-chip (SoC) boards. We obtain a nominal bit-error-rate (BER) of ~4% for the system. We also report on the development of a synchronous (100 MHz) single photon detector for increasing the repetition rate of our QKD system. This work shows promise for building a COTS-based, small size, weight, and power hardware for space applications.**

Keywords — quantum key distribution, COTS, optical communications, BB84, VCSEL, APD, cryptography

I. INTRODUCTION

Conventional public-key cryptosystems, such as Diffie-Helman [1] or RSA [2] rely on the limited computational power of an eavesdropper. The advent of algorithms for quantum computers capable of breaking these cryptosystems (such as Shor's algorithm [3] for RSA) has motivated the development of quantum key distribution (QKD) as an alternative for public-key encryption that exploits principles of quantum mechanics to ensure its security [4][5]. Since its publication, QKD's foundational BB84 protocol [6] has seen proofs of its security in practical systems [7][8] and a variety of implementations in fiber, free-space and different network geometries [9][10][11].

The recent satellite-to-ground QKD demonstration [12] and plans from other groups (SAGA (ESA), SpooQySat (NUS), QEYSSat (CSA)) for new space-based network geometries has positioned the development of space-compatible QKD systems as an emerging interest for various civil, commercial, and defense applications. However, despite past and current initiatives, there remain several technical challenges to overcome in developing a robust space-based global QKD network [13][14].

Achieving continuous QKD coverage is deemed feasible using a constellation of small satellites in low earth orbit (LEO), as evaluated in [15] and [16]. The use of small-size satellites is a cost-effective alternative to larger platforms, but also introduces concerns regarding the cost-efficiency of deploying many satellites equipped with transceiver payloads. Thus, the development of systems optimized for small size, weight, power and cost (SWaP-C), and that are space-qualified (having undergone radiation, thermal, shock and vibration testing) are particularly vital. To this end, the hardware design described in this work prioritizes the use of low-cost and low-power COTS components with the potential for scalability to a small-satellite compatible design.

To enable a space-based QKD network, a suitable transceiver must be able to operate as a customizable and synchronous source with high data rates. Currently, the photon-generation rate and scalability of commercial entangled photon sources is limited. For free-space QKD systems, the low photon rate yields a reduction in the key rate, but also introduces more severe background light suppression requirements. Alternatively, decoy-based QKD implementations using a weak coherent pulse (WCP) source can attain high data rates and thus higher key generation rates than entangled sources [17]. Furthermore, the simpler architecture of WCP sources (attenuated laser sources) result in low-SWaP-C designs. Thus, a BB84 implementation using a WCP source presents as a likely candidate for enabling a small-satellite based QKD network.

The reliability and performance of VCSELs for space applications has been documented, with the noted advantages being small size, low power consumption and superior radiation tolerance when compared to edge-emitting lasers (EEL) [18][19][20]. Radiation hardness in

COTS VCSELs specifically has been demonstrated, as emphasized in [20]. In this work, we report on decoy-based BB84 QKD transmitter using COTS VCSELs driven by internally-designed driver boards. Other features include a classical optical channel for time-transfer and a space-qualified SoC for data capture and system control.

II. System Architecture

The system architecture, shown in Fig.1, is based on a typical BB84 configuration, except for the addition here of an optical control and time-transfer channel. Alongside this, is the normal classical channel for post-processing that starts equipped with classical authentication keys and ends with new, shared keys generated by QKD. The QKD transmitter is composed of four independent, linearly-polarized VCSEL lasers, each controlled by its own driver. Each polarization state is fixed with COTS polarizing optics and beam-splitters. The use of separate lasers requires precise wavelength control and stabilization to ensure all four channels are indistinguishable but removes the need for high-speed electro-optic modulators, which otherwise would add significant SWaP-C overhead to the design. The receiver architecture relies on passive basis randomization using 50:50 and polarizing beam-splitters to avoid the need for receive-side random number generation and corresponding optical polarization modulation.

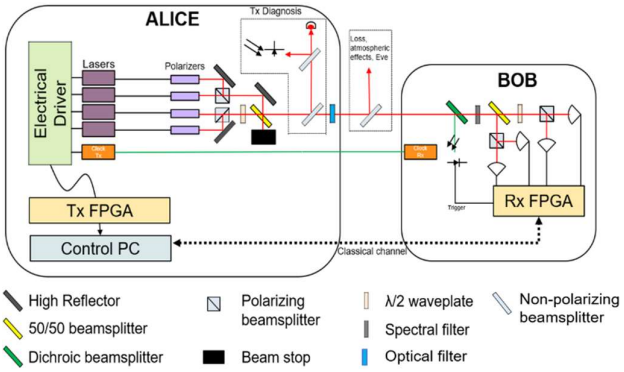


Figure 1 Decoy-state BB84 with dedicated clock transfer channel system architecture

The weak coherent quantum transmitter is implemented with four 794 nm VCSEL lasers, each generating one of the four BB84 polarization states. Polarization qubits are generated by modulating the drive current of each laser diode at a 10 MHz repetition rate and 50 ns on-time. The use of a weak coherent pulse source creates a vulnerability to the photon number splitting (PNS) attack [21], in the case of multi-photon pulses. To combat this, a three power-level (vacuum, low, and high power) based decoy-state BB84 protocol is used, where to detect an eavesdropper, the transmitter randomly chooses a subset of pulses to have a lower mean-photon number (μ) than the rest [22][23]. Thus, the lasers can output three optical power levels, $\langle vacuum \rangle$, $\langle \mu_1 \rangle$ *decoy state, and* $\langle \mu_2 \rangle$ *regular state* depending on the values of two digital inputs from the FPGA controller, with $\mu_2 : \mu_1 = 2$. This ratio able to be easily changed with the existing drivers. After optical attenuation, μ_1 and μ_2 become 0.1 and 0.2 photons per qubit period respectively.

To maintain unconditional security, the μ_1 and μ_2 states must be completely indistinguishable except for photon number [24]. Directly-modulating the VCSELs at two different pump current values can lead to spectral shift or differences in the time domain, violating a basic assumption of indistinguishability of the decoy state protocol and creating the potential for a PNS attack [25]. Huang, et al., showed in [25] that a timing mismatch between the decoy and signal states due to an imperfect source led to a reduction in secure key generation, even when the distinguishability of the states was considered in their security proof for robustness. In their paper, they propose to mitigate the reduction by calibrating the transmittance of the QKD receiver, a method also used to protect Bob's individual channels from a blinding attack [26][27].

To accurately assign received photon events to a qubit, the receiver needs to establish timing synchronous with the transmitter. Precise timing in combination with short transmission and reception time windows would also allow some reduction in the background light detection. Thus, we implemented a 780 nm optical time-transfer channel. The channel transfers both 10 MHz clock and symbols to indicate start and stop of key-generation session to the receiver.

In our current QKD demonstration system we use COTS single-photon SPCM-AQRH modules from Excelitas. The reach-through APD design offered by Excelitas delivers the highest quantum efficiency around 800 nm where an optimal combination of spectrally-accurate laser sources and good atmospheric transmission can be found. The reach-through devices require higher bias voltage, which is an acceptable tradeoff for better performance. However asynchronous quenching electronics of the COTS modules is performance-limiting in our system and determines our operation at 10 MHz qubit rate. Therefore we are also developing a custom single-photon APD (SPAD) driver utilizing periodic (clock-synchronous) quenching [28][29][30] at repetition rate of 100 MHz.

III. Transceiver Hardware

A. VCSEL Lasers as Weak Coherent Quantum Sources

The weak coherent source is composed of 4 vertical-cavity surface-emitting (VCSEL) lasers with a measured sub-nm bandwidth from Vixar, Inc (795S-0000-X006). The lasers are current-modulated to achieve pulsed operation per commands from the SoC control system. Each laser is equipped with an integrated thermo-electric cooler (TEC) and thermistor for precise temperature control. A custom board to control the TEC and modulate the laser drive current was constructed, see Fig. 2 The temperature control allows tuning of the laser wavelength between 790 and 796 nm, and we observe no significant wavelength drift when continuously modulated for approximately 2 hours each day for three consecutive days, see Fig. 3. For this demonstration, the lasers were tuned to a central wavelength of 793.8nm, a wavelength suitable for high atmospheric transmission. The characteristic performance of the transmitters is summarized in Fig. 3(a) and (b), demonstrating the tunability and indistinguishability in the output spectra of the VCSEL lasers.

We observed no more than 0.04% hourly power drift of all four lasers over a period of approximately 2 hours each day for three consecutive days. The modulation was also stable

over this period with a rise time of 100ps, see Fig. 3 (d). At low modulation current, the lasers emit with high polarization mode ratio of approximately 210:1. The observed spectral, polarization and power stability, and low power consumption make the directly-modulated VCSEL lasers very viable as weak coherent sources for BB84 QKD systems.

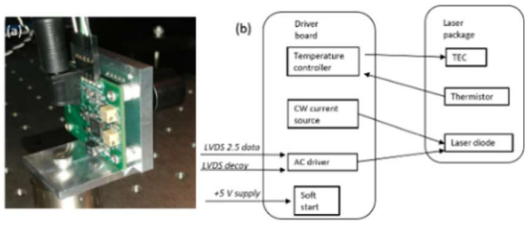


Figure 2 (a) VCSEL driver board for one polarization state transmitter. (b)The driver board's functional architecture.

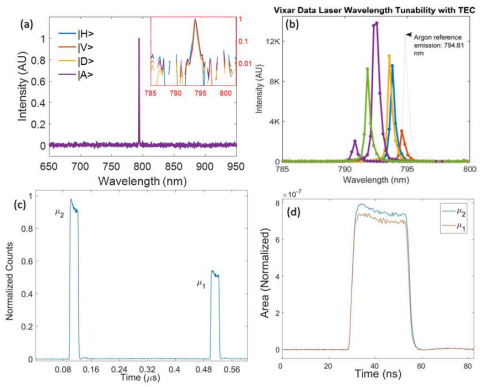


Figure 3 (a) Spectrum of the four COTS VCSEL lasers configured as QKD transmitters. All channels can be tuned to near indistinguishable wavelengths within sub-nm bandwidth. (b) Temperature tunability of the laser wavelength between 790 and 796nm. (c) Measured relative intensities of regular and decoy states with a ratio of 2:1. (d) Normalized temporal pulse profile.

B. Time-Transfer Laser Transmitter

For the optical clock transmitter, we use a directly modulated Eagleyard 780 nm DFB (distributed feedback) laser diode in a 14-pin package (PN: EYP-DFB-0780-00050-1500-BFW11-0005). The choice of a DFB laser was driven by the need for more power for the classical optical channel, as this type of laser is more suitable for current modulation in comparison to the other available single longitudinal mode laser alternatives. As with the VCSEL laser, the package includes TEC and thermistor, allowing for wavelength control and stabilization with temperature. The laser is driven by a pair of driver boards designed by us that implement temperature control and current modulation, see Fig. 4.

The laser was current-modulated at 10 MHz with 50% duty cycle, an extinction ratio of 13 dB and an average optical power of 22 mW. Under these operating conditions, the laser package produces a collimated beam of an average optical power of 22 mW. As can be seen in Fig. 4 (b), the laser operates on a single longitudinal mode under direct modulation. However, this performance is not guaranteed by the manufacturer as the laser is only specified for CW operation.

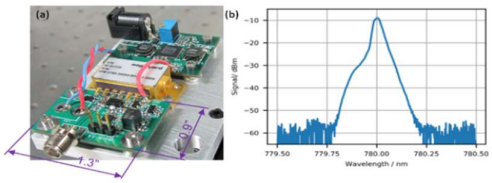


Figure 4 (a) The clock transmitter, comprised of an Eagleyard DFB package with custom driver boards. (b) Output optical spectrum of directly-modulated clock laser, operating in single mode.

C. Clock Receiver

The clock receiver was designed around an Excelitas C30737LH-230-80A APD (avalanche photodiode), Fig. 5. A custom driver board incorporating transimpedance amplifier, high-voltage (HV) APD bias source with temperature compensation, automatic gain control (AGC) and digital section including a comparator and phase-locked loop (PLL) for clock recovery (jitter reduction) with everything operating from a single external 5 V DC supply.

PLL achieves lock for average optical powers above 0.9 nW, which should be considered the receiver's minimum sensitivity limit. At the opposite end of the power range the receiver can lock up to optical power of 21 μW. However, above 0.5 μW there is an increasing delay of the recovered clock of several nanoseconds that is a function of the optical power. Thus, a correction is required between 0.5 μW and 21 μW. The PLL has a capture range of 9.1 MHz to 10.9 MHz.

At lower optical powers, measured Allan deviation for the optical time-transfer channel show inverse time dependence over a wide time-scale range, which corresponds to dominant white phase noise contribution [31]. This is consistent with the noise being dominated by the thermal noise of the transimpedance amplifier resistance and allows calculation of standard deviation (RMS jitter). At 2.1 nW average incident optical power on the receiver, the RMS jitter is 38 ps and decreases further with increase in received optical power and corresponding improvement in signal-to-noise ratio. This level of time-transfer precision will allow sub-nanosecond gbit time duration for background light suppression, if appropriately fast single photon detectors can be implemented.

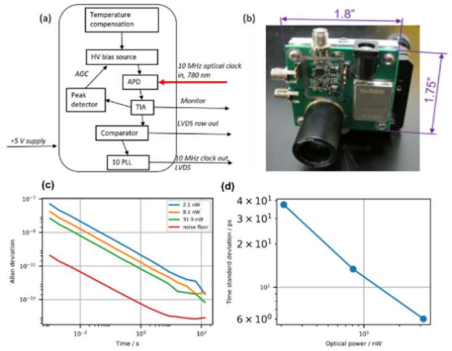


Figure 5 (a) Block diagram showing clock receiver board architecture. (b) Mounted clock receiver detector and board. (c) Allen deviation at and below 2.1 nW. (d)Time standard deviation with increasing power.

D. Single photon silicon avalanche detector periodically-gated at 100 MHz

Periodic gating of avalanche photodiodes for single photon detection [28][29][30] has emerged as a very viable technique for situations when periodic timing of measured signal can be accurately established. It has shown potential to improve the detector performance in terms of quantum efficiency and after-pulsing because of the reduction in the total charge of the avalanche needed for photoelectron detection [28][29][30]. Perhaps more importantly for free-space QKD systems it can reduce background light contribution to the total undesirable count rate by reducing the duty cycle of the detector sensitivity window. While this would not solve the background problem by itself, it eases requirements imposed on the spectral and spatial filtering (and, consequently, the system pointing) needed to achieve successful key generation in the presence of background light.

For this purpose, we designed and built a detector periodically-gated at 100 MHz around Excelitas Si reach-through APD, C30902SH-DTC. While the reach-through structure requires higher reverse voltage to achieve avalanche, it also exhibits higher quantum efficiency at around 800 nm where the transmitters operate. The APD has a 0.5 mm diameter active area and dual thermoelectric coolers. As in previously reported implementations [28][29][30], the diode is biased with a combination of DC high voltage (HV) and 100 MHz bias. As a result, the detector has reverse bias sufficient for non-negligible photon detection probability for only a small portion of the RF period. By the end of this time, the avalanche is unconditionally quenched. A single-board circuit (58 mm x 38 mm) was built to regulate the APD temperature at -25 ºC, provide DC HV and RF bias, and output detected photocount events in LVDS format, while being powered by single +5 V DC supply. The photon gating performance of the detector was characterized with a Coherent Mira 900 laser. The absolute quantum efficiency was not yet established, so only relative count rates at a fixed incident photon flux are given in Fig. 6 (left). As is seen from the figure, both detection probability and gate duration increase with increasing bias. This is accompanied by increasing after-pulsing, Fig. 6 (right). For the observed gate duration of 1.9 ns to 2.4 ns and the period of 10 ns, the expected reduction in optical background contribution to noise would be a factor of about 4 to 5.

.

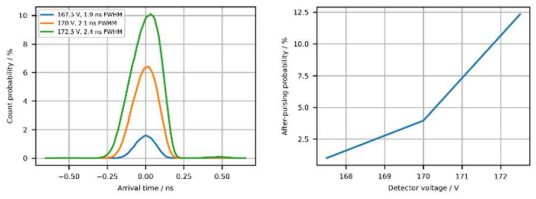
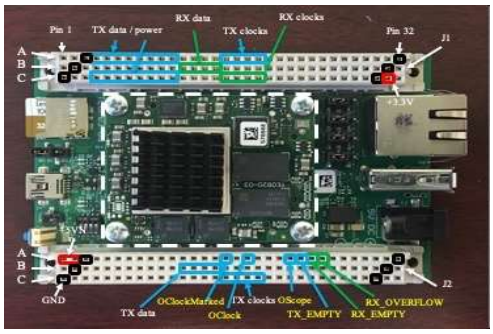


Figure 6 Left: Relative photon count probabilities versus DC bias voltage and photon arrival time at fixed photon flux. Right: After-pulsing probability versus DC bias voltage.

E. FPGA receiver and transmitter controller architecture

Both transmit and receive terminals of our QKD demonstration system implement FPGA-based controllers that interface with the hardware drivers. On the transmit side the FPGA provides decoy-state laser power level commands for the VCSEL laser drivers and clock with start/stop to the clock-transfer laser driver. On the receive side it captures qubit data, records the events, and provides buffering and start/stop symbol decoding.

The original design for both transmit and receive was based on Xilinx ML605 Virtex-6 FPGA prototyping boards connected over Ethernet to host computers. We recently transitioned to an SoC architecture based on a Xilinx Zynq Ultrascale+ that integrates an FPGA and an ARM-core on a single chip to reduce size and provide a path to flight (having been used on cubesats). The SoC board is shown in Fig. 7 and the FPGA interfaces are shown in Fig.8.



e

Figure 7 Annotated photo of the Zynq Ultrascale+.

The transmitter FPGA decodes 3 bits per clock cycle, which indicates polarization state (2 bits) and power level (1 bit); the transmission system assumes one polarization qubit is emitted at either full or decoy intensity levels every clock period during a QKD transfer. The transmitter FPGA also provides clock and start/stop symbols to the clock transmitter driver and serves as the master clock for the system.

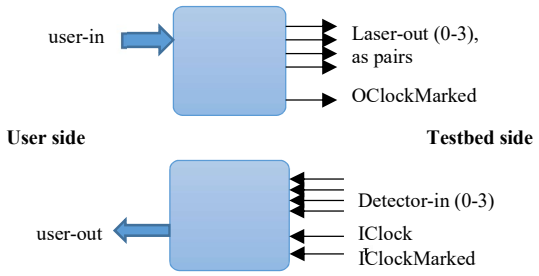


Figure 8 Diagram of the FPGA input and output digital interfaces.

The eventual intention is to run the receiver FPGA phase-locked to the clock recovered by the clock receiver. However, the current implementation supports only an on-board free-running 200 MHz clock. This provides adequate performance with our 50 ns photon detection window by sampling within 5 ns time slices. The receiver encodes 4 bits per qubit clock cycle to indicate received detection events. The encoding is as follows: no photons in any of the polarization states, one photon in one of 4 polarization states (a possibly valid qubit), multiple photons in the same

polarization state (indicating that polarization), and multiple photons spanning more than one polarization state (not indicating the polarizations).

Both transmit and receive FPGAs include additional signals used for debugging, monitoring, and loopback testing. The embedded ARM CPU implements user-level interface to the hardware utilizing these control signals. It allows hardware parameter configuration, measurement, and hardware test automation, including a separate test to validate the FPGA interface itself. The system is currently capable of transferring streams of up to 512 M qubits without interruption (input/output files of 128 MB, taking 27 s at 10 Mbaud); longer sequences can be transferred by staging data between SD memory cards and on-board memory.

IV. Post Processing Architecture

Raw received qubit data is post-processed to generate a secret key. This step is an important component of any practical QKD system, which is often omitted in discussion of QKD hardware implementations. Our post-processing implementation is informed by the single-photon protocol outlined in [32] and makes direct use of that in [23], with the analysis of the resultant security based on the latter article. Figure 9 indicates the protocol execution.

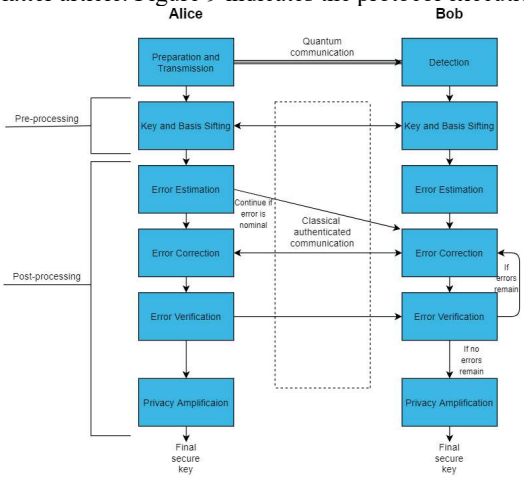


Figure 9 QKD pre and post-processing information flow.

A. Message Authentication

Almost Strongly Universal$_2$ (ASU$_2$) hashing (information-theoretically secure message authentication code) is used for the transmitter and receiver to verify the origin of messages exchanged on the classical channel. Specifically, a class of two-universal functions called Toeplitz matrices (constructed using a Linear Feedback Shift Register (LFSR) algorithm [33]) are used to make a tag from pre-shared secret key before being sent to the opposing party. The probability of a third party guessing the hash (ϵ_{Aut}) is set by the number of rows in the Toeplitz matrix, l: $\epsilon_{Aut} = 2^{-l}$. In the sattelite to ground optical communication scenario, this is further improved by the line-of-sight requirement on both transmitter and receiver.

B. Pre-processing

The transmitter and receiver exchange their basis selection information on the classical channel with encrypted tag authenticated messages, subsequently removing any bits for which they measured in different bases ("basis sifting"). The secure key cost for this procedure is 50% of the key for basis sifting (biased sifting [7] can substantially reduce this cost and may be added in the future), then the cost of authentication, $2k_{BS}$, where $k_{BS} = l_{BS}$, and a failure probability of $2\,\epsilon_{BS}$, where $\epsilon_{BS} = n2^{1-k_{BS}}$.

C. Error Estimation and Correction

After sifting, the phase error is estimated and if the error and raw key bits are below the expected bounds (as given in [37]) an authenticated message is sent to the receiver to continue the protocol.

To have a useable secret key, transmitter and receiver must share identical keys, but differences remain. A low-density parity check (LDPC) algorithm adjusted for QKD is used to remove these. Here, the transmitter multiplies its key by an LDPC matrix (LDPCM, a sparse quasi-random matrix) and encrypts the result using k_{ec} bits of pre-shared secret key before sending to the receiver. $k_{EC} = nfH(QBER)$, where n is the key length, f is the error correction efficiency [34] and H is the binary Shannon entropy. The receiver then uses the sum-product belief propagation algorithm [35] [36] to decode the error riddled key.

D. Error verification

Due to the probabilistic nature of the LDPC error correction, there is some chance that errors remain despite transmitter and receiver's parity check matrices matching. As a check, a proportion of the receiver's key, n is taken and a tag is created (as in message authentication). This tag is then encrypted, using $k_{EV} = 2l_{EV}$ bits of pre-generated secret key before being sent to the transmitter, which verifies no errors remain, or in the event that some do (a frame error), indicates that error correction must be reattempted. The failure probability for this step is: $\epsilon_{EV} = n2^{1-k_{EV}}$ (*i.e.*, errors pass through undetected) [32].

E. Privacy Amplification

Having reduced the security of their final keys due to a non-zero multiphoton pulse probability in the quantum communications, the transmitter and receiver amplify differences between their key and an eavesdropper's estimate by multiplying it with a Toeplitz matrix and in so doing, enhance its security. The failure probability is: $\epsilon_{PA} = (n + s - 1)2^{1-k_{PA}}$ [32]. Here, s is the length of the final key and n is the length of the error-corrected keys. Note, in this case, a fully-random Toeplitz matrix is used as opposed to the quasi-random Toeplitz used in previous steps.

F. Key Generation Rate and Security

With the post-processing as described in the preceding, the per block key generation rate is: $k_{QKD} = l - 2k_{BS} - k_{EE} - k_{EC} - k_{EV} - k_{PA}$.

Fig. 10 depicts the progression of a key through our pre/post processing program for a ~0.1 ms qubit transmission and detection where raw qubits with error are post-processed to generate error free key. The block size is reduced for clarity though it is normally greater than 10^5 in order to limit finite-size key security issues. Such post-processing algorithms allow generation of error-free secure key for engagements with BER below the security threshold but with an added computational cost and classical-communication overhead.

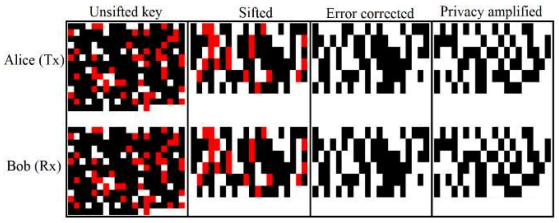


Figure 10 The polarization state qubit stream is folded and visualized as a matrix, where the transmitted and detected polarization states are color-coded by their assigned qubit (black – 0, white – 1, red – error).

V. System performance of the full QKD system

A 1-meter QKD test link was set up to evaluate the hardware performance. With the clock rate of 10 MHz, photon flux on the receiver of 0.2 (signal) and 0.1 (decoy) per qubit and no additional background light, we obtained a bit transmission rate of ~280 kHz (after basis sifting). The outgoing pulses were optically attenuated for measured mean photon numbers of 0.2 and 0.1 on the receiver for the signal and decoy states, respectively. We estimate a quantum bit error rate (QBER) of 3.96%±0.03% from the measurement. Fig. 11 summarizes these results, taken from an hour-long QKD exchange.

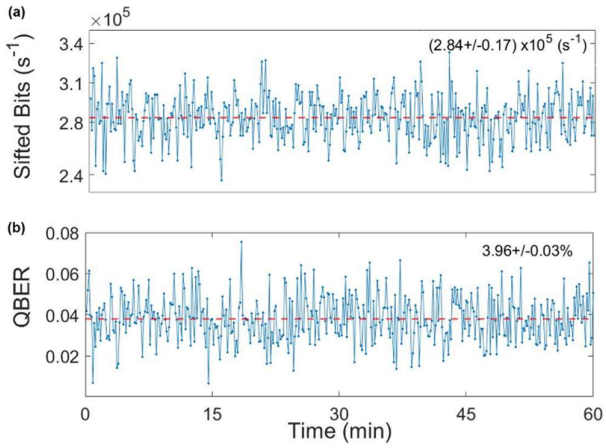


Figure 11 (a) The raw bit transmission rate per second after basis sifting. (b) The estimated QBER over an hour long QKD exchange.

The measured QBER approached the limit set by the polarization purity obtained in the current configuration. The polarization extinction varied across the four transmission channels and ranged between approximately 1% and 6% for both intensity states. Higher percent values were measured in the diagonal/anti-diagonal basis, from which the transmitted photons were more adversely affected by optics in the system with 90º incidence. Thus, the measured error for the overall system was dominated by imperfections in the prepared polarization states from that basis. The mean polarization extinction value measured across all channels was 3.50% and 3.95% for the signal and decoy state intensity levels, respectively.

VI. Conclusion and Lesson Learned

We demonstrated all component subsystems and algorithms necessary for constructing a low SWaP-C decoy-state BB84 QKD system utilizing COTS components and internally-developed electronics. Our bench-top system demonstration showed about 4% error rate, average across the polarization channels and is primarily determined by polarization errors in the system.

Using drive current modulation of COTS VCSELs and actively controlling their temperature we met the requirement for indistinguishability for individual BB84 polarization states. The lasers exhibited power, polarization and spectral stability over the course of approximately two hours each day for three consecutive days.

We implemented a dedicated optical time-transfer channel with 22 mW average transmit power and 0.9 nW receiver sensitivity. With 2.1 nW on the receiver, corresponding to 70 dB link margin, the channel achieves 38 ps RMS recovered clock time jitter. Additionally, the channel implements transmission of symbols to indicate start and stop of QKD session to the receiver terminal.

We also report on the development of a periodically-gated detector built around a commercially-available APD to reduce the contributions of background light to unwanted photon detections in a free-space QKD system. The single-board circuit design provides DC HV and RF biases and APD temperature control. When periodically-gated at 100MHz a gate duration of 1.9 ns to 2.4 ns is achieved. This corresponds to a reduction in expected background by a factor of 4-5. The 100 MHz repetition rate will also allow us to increase our system's operating rate and raw key rate as a result.

We further demonstrated compact data acquisition and control with a Xilinx SoC (FPGA plus CPU) chip, which has a history of space deployment. We also implemented the post-processing algorithms needed for complete system integration. Altogether, this work demonstrates the feasibility of building a space compatible QKD transmitter using COTS components. Further mechanical and optical design and integration work is still needed for a full outdoor system demonstration. Other planned improvements include implementing synchronous operation of the receiver SoC utilizing the recovered clock and transition to the 100 MHz qubit clock by taking advantage of our newly-developed synchronous APD receiver.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory* 22.6, 1976, pp. 644-654.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* 21.2, 1978, pp. 120-126.

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE, 1994.

[4] W. K. Wootters, and W. H. Zurek, "A single quantum cannot be cloned," *Nature* 299.5886, 1982, pp. 802-803.

[5] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review* 47.10, 1935, pp. 777.

[6] C. H. Bennett, and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, 1984, pp. 8.

[7] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology* 18.2, 2005, pp. 133-165.

[8] D. Gottesman, *et al*. "Security of quantum key distribution with imperfect devices," *Proc. International Symposium on Information Theory (ISIT),* IEEE, 2004.

[9] C. H. Bennett and G. Brassard, “Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working,” *ACM SIGACT News* 20.4, 1989, pp. 78-80.

[10] B. Korzh, *et al*. “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics* 9.3, 2015, pp. 163.

[11] C.J. Pugh, *et al*. “Airborne demonstration of a quantum key distribution receiver payload,” *Quantum Science and Technology* 2.2, 024009, 2017.

[12] S.-K. Liao, *et al*. “Satellite-to-ground quantum key distribution,” *Nature* 549.7670, 2017, pp. 43-47.

[13] O.L. Lee, and T. Vergoossen, “An updated analysis of satellite quantum-key distribution missions,” *arXiv preprint,* arXiv: Quantum Physics, 2019

[14] R. Bedington, J.M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” *npj Quantum Inf* **3,** 30, 2017.

[15] T. Vergoossen, *et al*., “Modelling of satellite constellations for trusted node QKD networks,” *Acta Astronautica*, 2020.

[16] L. Mazzarella, *et al*., “QUARC: Quantum Research Cubesat—a constellation for quantum communication,” *Cryptography*, 2020.

[17] J-P Bourgoin, *et al*., “A comprehensive design and performance analysis of low Earth orbit satellite quantum communication,” *New Journal of Physics,* Vol 15, 2013.

[18] R. Carson, *et al*., “Surface-emitting laser technology and its application to the space radiation environment,” *Proc. SPIE 10288, Advancement of Photonics for Space: A Critical Review*, 1028806, 1997.

[19] R. Morgan, *et al*., "Vertical-cavity surface-emitting lasers: the applications," *Proc. SPIE 3004, Fabrication, Testing, and Reliability of Semiconductor Lasers II*, 1997.

[20] L. Laforge, Moreland, J.R., Bryan, R.G., and Fadali, S., “Vertical cavity surface emitting lasers for spaceflight multi-processors,” *IEEE Aerospace Conference Proceedings*, 2006.

[21] G. Brassard, *et al*. "Limitations on practical quantum cryptography," *Physical Review Letters* 85.6, 1330, 2000.

[22] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Physical Review Letters* 94.23, 230504, 2005.

[23] Xi. Ma, *et al*. "Practical decoy state for quantum key distribution," *Physical Review A* 72.1, 012326, 2005.

[24] W. Hwang, “Quantum Key Distribution with high loss: toward global secure communication,” *Phyical. Revew* A 91, 057901, 2003.

[25] A. Huang, *et al*., “Quantum key distribution with distinguishable decoy states,” *Physical. Revew* A 98, 012330, 2018.

[26] Ø. Marøy, L. Lyderson, and J. Skaar, “Security of quantum key distribution with arbitrary individual imperfections,” *Physical Review* A 82, 032337, 2010.

[27] Ø. Marøy, V. Makarov, and J. Skaar, “Secure detection in quantum key distribution by real-time calibration of receiver,” *Quantum Sci. Technol*. 2, 044013, 2017.

[28] N. Namekata, S. Sasamori, and S. Inoue, “800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating,” *Optics Express* 14, no. 2, 10043-10049, 2006.

[29] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J Shields, “High speed single photon detection in the near infrared," *Applied Physics Letters* 91, no. 4, 041114, 2007.

[30] S. Suzuki, N. Namekata, K. Tsujino, and S. Inoue, “Highly enhanced avalanche probability using sinusoidally-gated silicon avalanche photodiode,” *Applied Physics Letters* 104, no. 4, 041105, 2014

[31] Riley, William J. "Handbook of frequency stability analysis.", 2008.

[32] C.-H. F. Fung, X. Ma, and H. F. Chau, “Practical issues in quantum-key-distribution postprocessing,” *Physical Review A* 81.1, 12318, 2010.

[33] H. Krawczyk, “LFSR-based hashing and authentication,” *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, 1994.

[34] J. Elkouss Martinez-Mateo, and V. Martin, “Information reconciliation for quantum key distribution,” *arXiv preprint arXiv:1007.1616*, 2010.

[35] D. MacKay, and R. Neal, “Near Shannon limit performance of low density parity check codes,” *Electronics Letters* 32.18, 1996, pp. 1645-1646.

[36] D. Pearson, “High-speed QKD reconciliation using Forward Error Correction,” *Proc. AIP Conference*, Vol. 734. No. 1. American Institute of Physics, 2004.

[37] Ma, Xiongfeng, et al. "Decoy-state quantum key distribution with two-way classical postprocessing." *Physical Review A* 74.3 (2006): 032330