

Free space quantum key distribution using modulating retro-reflectors

WILLIAM S. RABINOVICH,^{1,*} RITA MAHON,¹ MIKE S. FERRARO,¹ PETER G. GOETZ,¹ MARK BASHKANSKY,¹ RACHEL E. FREEMAN,¹ JOHN REINTJES,² AND JAMES L. MURPHY¹

¹Optical Science Division, US Naval Research Laboratory, 4555 Overlook Ave, Washington, DC 20375, USA

²KeyW, 7740 Milestone Parkway, Hanover, MD 21076, USA

*will.rabinovich@nrl.navy.mil

Abstract: Quantum key distribution (QKD) can be used to produce a cryptographic key whose security is guaranteed by quantum mechanics. The range of fiber-based QKD links is limited, by loss, to a few hundred kilometers, and cannot be used between mobile platforms. Free space QKD can, in principle, overcome these limitations. In practice, very narrow beam divergences must be used, requiring highly accurate pointing of the transmitting terminal to the receiver. This makes deployment very difficult. Here we describe the experimental implementation of a new type of free space QKD link, using modulating retro-reflectors (MRR). The MRR-QKD link eases the pointing requirements by more than three orders of magnitude, from microradians to degrees, while maintaining the narrow beam divergence necessary for long-range communication links. The system uses new, high extinction surface-normal multiple quantum well modulators with a modulation rate of 100 MHz. A laboratory-based BB84 QKD link using multiple quantum well MRRs is demonstrated, link budgets for possible applications are discussed, and security issues are considered.

© 2018 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

OCIS codes: (060.2605) Free-space optical communication; (060.5565) Quantum communications; (230.4110) Modulators; (230.5590) Quantum-well, -wire and -dot devices.

References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, (IEEE, 1984) pp. 175–179
2. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.* **5**(1), 3–28 (1992).
3. 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. Photonics* **1**(6), 343–348 (2007).
4. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-Device-Independent quantum key distribution Over a 404 km Optical Fiber," *Phys. Rev. Lett.* **117**(19), 190501 (2016).
5. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Nature Publishing Group* **2**(1), 1–12 (2017).
6. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photonics* **7**(5), 378–381 (2013).
7. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New J. Phys.* **4**(1), 43 (2002).
8. 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**(1), 010504 (2007).
9. H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O'Brien, and D. Bitauld, "Handheld free space quantum key distribution with dynamic motion compensation," *Opt. Express* **25**(6), 6784–6795 (2017).
10. B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, "Atmospheric continuous-variable quantum communication," *New J. Phys.* **16**(11), 1–14 (2018).
11. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H.

- Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nat. Phys.* **3**(7), 481–486 (2007).
12. 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**(1), 82 (2002).
 13. C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New J. Phys.* **11**(4), 045017 (2009).
 14. J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," *Phys. Rev. A* **92**(5), 052339 (2015).
 15. J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, "Free-space quantum key distribution to a moving receiver," *Opt. Express* **23**(26), 33437–33447 (2015).
 16. S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nat. Photonics* **7**(5), 382–386 (2013).
 17. S. K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J. G. Ren, J. Yin, Q. Shen, Y. Cao, Z. P. Li, F. Z. Li, X. W. Chen, L. H. Sun, J. J. Jia, J. C. Wu, X. J. Jiang, J. F. Wang, Y. M. Huang, Q. Wang, Y. L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y. A. Chen, N. L. Liu, X. B. Wang, Z. C. Zhu, C. Y. Lu, R. Shu, C. Z. Peng, J. Y. Wang, and J. W. Pan, "Satellite-to-ground quantum key distribution," *Nature* **549**(7670), 43–47 (2017).
 18. K. Günthner, I. Khan, D. Elser, B. Stiller, M. Bayraktar, C. R. M. Iler, K. Saucke, D. T. Ndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. R. G. tlich, S. Philipp-May, C. Marquardt, and G. Leuchs, "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica* **4**(6), 611 (2017).
 19. H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nat. Photonics* **11**(8), 502 (2017).
 20. H. Stockman, "Communications by Means of Reflected Power," *Proc. IRE* **36**(10), 1196–1204 (1948).
 21. G. J. Olson, H. W. Mocker, N. A. Demma, and J. B. Ross, "Coherent CO₂ Laser Communication System with Modulable Retroreflectors," *Appl. Opt.* **34**(12), 2033–2044 (1995).
 22. C. Swenson, C. Steed, I. De La Rue, and R. Fugate, "Low-power FLC-based retromodulator communications system," *Proc. SPIE* **2990**, 296–310 (1997).
 23. W. S. Rabinovich, R. Mahon, H. R. Burris, G. C. Gilbreath, P. G. Goetz, C. I. Moore, M. F. Steil, M. J. Vilcheck, J. L. Witkowski, L. Swingen, M. R. Suite, E. Oh, and J. Koplow, "Free-space optical communications link at 1550 nm using multiple-quantum-well modulating retroreflectors in a marine environment," *Opt. Eng.* **44**(5), 056001 (2005).
 24. P. G. Goetz, W. S. Rabinovich, R. Mahon, J. L. Murphy, M. S. Ferraro, M. R. Suite, W. R. Smith, H. R. Burris, C. I. Moore, W. W. Schultz, W. T. Freeman, S. J. Frawley, B. M. Mathieu, K. Hacker, and S. Reese, "Modulating retro-reflector lasercom systems for small unmanned vehicles," *IEEE J. Sel. Top. Commun.* **30**(5), 986–992 (2012).
 25. W. S. Rabinovich, C. I. Moore, R. Mahon, P. G. Goetz, H. R. Burris, M. S. Ferraro, J. L. Murphy, L. M. Thomas, G. C. Gilbreath, M. Vilcheck, and M. R. Suite, "Free-space optical communications research and demonstrations at the U.S. Naval Research Laboratory," *Appl. Opt.* **54**(31), F189–F200 (2015).
 26. T. Chan and J. Ford, "Retroreflecting optical modulator using a MEMS deformable micromirror array," *J. Lightwave Technol.* **24**(1), 516–525 (2006).
 27. G. C. Gilbreath, W. S. Rabinovich, T. J. Meehan, M. J. Vilcheck, R. Mahon, R. Burris, M. Ferraro, I. Solkolsky, J. A. Vasquez, C. S. Bovais, K. Cochrell, K. C. Goins, R. Barbehenn, D. S. Katzer, K. Ikossi-Anastasiou, and M. J. Montes, "Large-aperture multiple quantum well modulating retroreflector for free-space optical data transfer on unmanned aerial vehicles," *Opt. Eng.* **40**(7), 1348–1356 (2001).
 28. W. S. Rabinovich, P. G. Goetz, R. Mahon, L. Swingen, J. Murphy, M. Ferraro, H. R. J. Burris, C. I. Moore, M. Suite, G. C. Gilbreath, S. Binari, and D. Klotzkin, "45-Mbit/s cat's-eye modulating retroreflectors," *Opt. Eng.* **46**(10), 104001 (2007).
 29. C. Quintana, Q. Wang, D. Jakonis, X. Piao, G. Erry, D. Platt, Y. Thueux, A. Gomez, G. Faulkner, H. Chun, M. Salter, and D. O'Brien, "High speed electro-absorption modulator for long range retroreflective free space optics," *IEEE Photonics Technol. Lett.* **29**(9), 707–710 (2017).
 30. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**(23), 230504 (2005).
 31. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics* **8**(8), 1–10 (2017).
 32. N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**(1), 145–195 (2002).
 33. G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental Satellite Quantum Communications," *Phys. Rev. Lett.* **115**(4), 040502 (2015).
 34. 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**(1), 010504 (2007).
 35. W. S. Rabinovich, R. Mahon, P. G. Goetz, E. Waluschka, D. S. Katzer, S. C. Binari, and G. C. Gilbreath, "A cat's eye multiple quantum-well modulating retro-reflector," *IEEE Photonics Technol. Lett.* **15**(3), 461–463 (2003).
 36. T. H. Stievater, W. S. Rabinovich, P. G. Goetz, R. Mahon, and S. C. Binari, "A surface-normal coupled-quantum-well modulator at 1.55 μm ," *IEEE Photonics Technol. Lett.* **16**(9), 2036–2038 (2004).

37. P. G. Goetz, W. S. Rabinovich, S. C. Binari, and J. A. Mittereder, "High-Performance chirped electrode design for cat's eye retro-reflector modulators," *IEEE Photonics Technol. Lett.* **18**(21), 2278–2280 (2006).
38. W. S. Rabinovich, "Optical modulating retro-reflectors," in *Advanced Optical Wireless Communication Systems*, S. Arnon, J. Barry, G. Karagiannidis, R. Schober, and M. Uysal, eds. (Cambridge University, 2009).
39. M. Plett, W. S. Rabinovich, R. Mahon, M. S. Ferraro, P. G. Goetz, C. I. Moore, and W. Freeman, "Free-space optical communication link across 16 kilometers over the Chesapeake Bay to a modulated retroreflector array," *Opt. Eng.* **47**(4), 045001 (2008).
40. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Phys. Rev. Lett.* **91**(5), 057901 (2003).
41. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A* **72**(1), 012326 (2005).
42. J. J. Degnan, "Millimeter accuracy satellite laser ranging: a review," *Geodynamics* **25**, 133–162 (1993).
43. D. Rosenberg, A. J. Kerman, R. J. Molnar, and E. A. Dauler, "High-speed and high-efficiency superconducting nanowire single photon detector array," *Opt. Express* **21**(2), 1440–1447 (2013).
44. M. Shaw, K. Birnbaum, M. Cheng, M. Srinivasan, K. Quirk, J. Kovalik, A. Biswas, A. D. Beyer, F. Marsili, V. Verma, R. P. Mirin, S. W. Nam, J. A. Stern, and W. H. Farr, "A Receiver for the lunar laser communication demonstration using the optical communications telescope laboratory," in *Proceedings of CLEO: 2014 (OSA 2014)*, paper SM4J.2.
45. B. Moision, B. Erkmen, E. Keyes, T. Belt, O. Bowen, D. Brinkley, P. Csonka, M. Eglinton, A. Kazmierski, N.-H. Kim, J. Moody, T. Tu, and W. Vermeer, "Demonstration of free-space optical communication for long-range data links between balloons on Project Loon," *Proc. SPIE* **10096**, 100960Z (2017).
46. F. Fidler, M. Knapek, J. Horwath, and W. R. Leeb, "Optical communications for high-altitude platforms," *IEEE J. Sel. Top. Quantum Electron.* **16**(5), 1058–1070 (2010).
47. T. S. Rose, S. W. Janson, S. LaLumondiere, N. Werner, D. H. Hinkley, D. W. Rowen, R. A. Fields, and R. P. Welle, "LEO to ground optical communications from a small satellite platform," *Proc. SPIE* **9354**, 93540I (2015).
48. 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**(3), 1301–1350 (2009).
49. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," *Nat. Commun.* **2**, 349 (2011).
50. M. G. Tanner, V. Makarov, and R. H. Hadfield, "Optimised quantum hacking of superconducting nanowire single-photon detectors," *Opt. Express* **22**(6), 6734–6748 (2014).
51. M. S. Lee, M. K. Woo, J. Jung, Y.-S. Kim, S.-W. Han, and S. Moon, "Free-space QKD system hacking by wavelength control using an external laser," *Opt. Express* **25**(10), 11124–11131 (2017).
52. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A* **73**(2), 022320 (2006).
53. J. H. Shapiro, "Scintillation has minimal impact on far-field Bennett-Brassard 1984 protocol quantum key distribution," *Phys. Rev. A* **84**(3), 032340 (2011).
54. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play" systems for quantum cryptography," *Appl. Phys. Lett.* **70**(7), 793–795 (1997).
55. M. S. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, "Spatial mode side channels in free-space QKD implementations," *IEEE J. Sel. Top. Quantum Electron.* **21**(3), 187–191 (2015).
56. S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace BB84 quantum cryptography," *New J. Phys.* **11**(6), 065001 (2009).
57. W. S. Rabinovich, R. Mahon, M. Ferraro, P. G. Goetz, and J. L. Murphy, "Reduction of scintillation in optical modulating retro-reflector links," *Opt. Express* **22**(23), 28553–28565 (2014).
58. G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villorresi, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Phys. Rev. A* **91**(4), 042320 (2015).
59. C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, "Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere," *New J. Phys.* **14**(12), 123018 (2012).
60. W. S. Rabinovich, R. Mahon, M. Bashkansky, R. Freeman, and J. Reintjes, "A scintillation playback system for quantum links," *Proc. SPIE* **10096**, 1009604 (2017).

1. Introduction

Quantum key distribution (QKD) can be used to produce a cryptographic key with information-theoretical security guaranteed by quantum mechanics [1,2]. The maximum range of current fiber-based QKD links is a few hundred kilometers, limited by loss [3–6]. The key rates at these distances are very low, and fiber-based QKD cannot be used for mobile links. Free space QKD links can, in principle, overcome these limitations. Outdoor free space QKD links using weak coherent states have been demonstrated between fixed point nodes at

increasing distances [7–9]. Fixed-point free space QKD links have also been demonstrated using continuous variable QKD [10], and entangled states [11].

To avoid photon number splitting attacks, the QKD transmitter must ensure that the probability of emitting more than one photon per bit is low. In implementations using BB84 with weak coherent states, this means that the transmitter must limit the mean number of photons per bit to much less than one. As a result, producing a high key rate at long range requires a very narrow transmitter beam divergence, on the order of tens of microradians. As in all conventional free space optical systems, the requirements on the transmitter to know the location of the other end of the link, and to accurately point its beam there, are determined, in part, by the beam divergence. So a narrow divergence requires a very capable pointing system [12–14], posing a challenge for mobile links [15]. While there have been recent, very impressive, demonstrations of quantum links from aircraft [16] and low Earth orbit (LEO) spacecraft [17–19], deployment remains very challenging. For example, in the space to ground QKD link demonstrated by Liao et. al. [17], the low Earth orbit spacecraft carrying the QKD transmitter placed a 10-meter wide spot on its ground station from 1200 km away while moving at about 7 km/s. This required a multi-stage, high bandwidth system for determining the ground station location relative to the spacecraft, and both multi-axis gimbals and fast steering mirrors to aim the beam. Pointing and acquisition systems of this kind are very complex, weigh many kilograms, and can consume tens of watts of power. The success of this experiment decisively showed that space to ground QKD is possible, but the weight and power requirements limit this type of implementation to relatively large, complex, platforms.

Classical free space optical (FSO) links can also face pointing challenges. An approach to alleviate these problems, on one end of the link, is to use a modulating retro-reflector (MRR) [20–23]. In an MRR link one end consists of a conventional FSO terminal with a laser, optics, and a pointing system. The other end consists of a passive retro-reflector, for example a corner cube prism or a cat's eye optic, combined with an optical modulator.

In a classical MRR link, as shown in Fig. 1, the active end interrogates the MRR with a continuous wave (CW) beam. The retro-reflector will reflect the beam back to the interrogator as long as the MRR is pointed to within its field of view. This can be a few degrees to as much as 60 degrees. The optical modulator changes the strength of the reflected light, and is driven by a data signal. When the data signal consists of a binary one, the modulator is driven to its high transmission state, and when the data consists of a binary zero the modulator is driven to its low transmission state. Thus, the MRR imposes this signal on the retro-reflected beam, which is received by the interrogator. This allows a one-way link. Placing a receiver at the MRR end can allow a two-way link.

Unlike a conventional free space optical system, the pointing requirements of the retro-reflector are set by its field of view, not its reflected beam divergence. In most cases the reflected beam divergence is determined by diffraction from its aperture. An intuitive way to think of these kinds of links is to view the MRR as an FSO transmitter whose beam divergence is set by the diffraction limit of the retro-reflector aperture, and whose effective transmit power consists of the part of the interrogation beam that is intercepted by the MRR aperture. Thus, an MRR can have a beam divergence on the order of 100 microradians or less, but a pointing requirement of degrees.

However, in most cases, the interrogation beam overfills the retro-reflector aperture, so the effective transmit power of the MRR decreases with the square of the range. Because of this, a classical MRR link's strength drops off as $1/R^4$, with one factor of $1/R^2$ coming from the drop in effective transmit power and the other coming from the normal geometric propagation losses of the return link.

Since the 1990's, classical MRR links have been proven in many field experiments on a variety of platforms including ships, UAVs, balloons and small robots [22,24,25]. Several different kinds of modulators have been used including micro-electro-mechanical systems

(MEMS) [26], liquid crystals [22] and multiple quantum wells (MQW) [27]. The MQW MRRs have had the highest data rates with a 45 MHz [28], and a 200 MHz [29] MQW MRR demonstrated in pixelated cats' eye configurations.

Typically, while the beam divergence of an MRR is similar to a conventional FSO terminal, its effective output power is much less. An MRR terminal thus acts like a conventional FSO terminal with good beam divergence, but with a very under-powered source. This can seriously limit the performance of classical MRR links as compared to a conventional direct FSO link. However, it is not a disadvantage for quantum MRR links because the allowed transmit power of a QKD terminal is restricted to very low powers by the limitations imposed by the BB84 protocol.

In this work we experimentally demonstrate, for the first time, a free space QKD link that uses modulating retro-reflectors. We describe a new configuration for the system that overcomes the lack of high-speed, large area, surface normal polarization modulators, which would otherwise be needed to implement the BB84 protocol [1] using MRRs. We use a new design for MQW modulators for MRR links that offers the high extinction needed to maintain link security, and which has the bandwidth to run at rates of 100 MHz or higher. The laboratory demonstration of the link exhibits a quantum bit error rate low enough to maintain security. We show that systems using this approach can have a small size and function with a few watts of power.

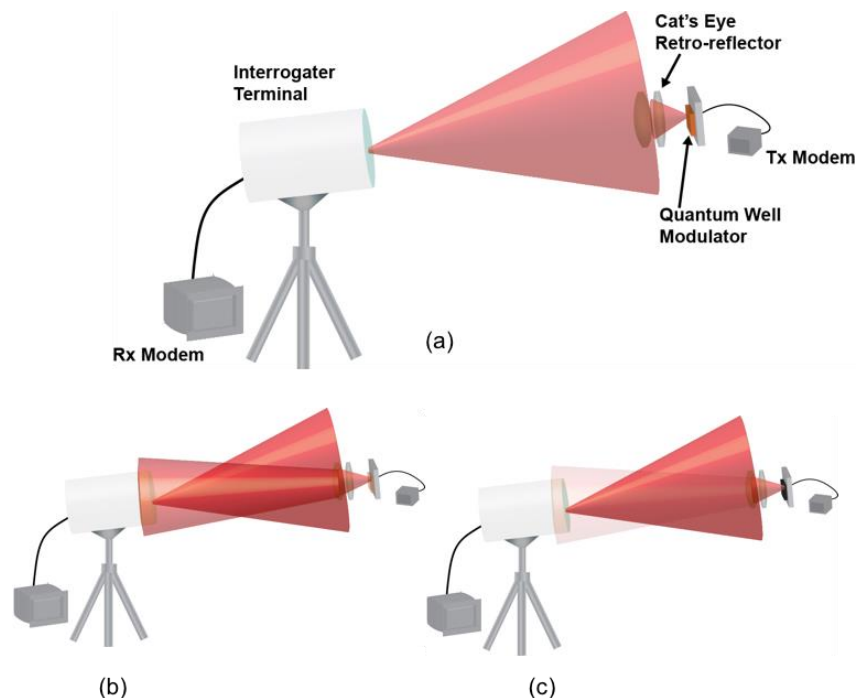


Fig. 1. Schematic of a classical modulating retro-reflector link using a cat's eye retro-reflector with a multiple quantum well modulator in its focal plane. (a) The interrogating laser uses active tracking to illuminate the MRR. (b) When the modulator is driven with a binary one the reflection is high. (c) When it is driven with a binary zero the reflection is low.

2. Quantum key distribution in a retro-reflecting configuration

A modulating retro-reflector QKD link using the BB84 protocol can be implemented with a ground station, Bob, that has a laser interrogator, which acts as a supply of photons for Alice, the mobile platform. Bob's interrogation laser emits many photons per bit. These photons are all circularly polarized, and are not encoded. Alice carries the MRR, and she is responsible

for transmitting the polarization-encoded bits that will be used to develop the quantum key. Bob actively tracks and illuminates Alice's MRR. Up to this point the link is classical. Also, up to this point, interception of the beam yields no information.

Alice's MRR must reflect back a weak coherent state that is in one of the four possible polarization states used by BB84. As usual, Alice chooses this state randomly for each bit. From this point on the link works exactly as a non-retro-reflecting free space QKD link. The normal rules for the average number of photons per bit in a QKD link apply. Thus Alice and Bob have to ensure that the rate of retro-reflected photons is at most 0.1 per bit for a link without decoy states, or higher if decoy states are used [30,31]. This can be achieved by Bob controlling the intensity of his interrogation beam, or Alice controlling the strength of retro-reflection, or some combination of both.

Some fraction of the retro-reflected photons is received at Bob's ground station. He analyzes them in a random basis, and the key is generated using a classical channel to select a common basis set, and using any of the techniques for error correction and privacy amplification that have been developed [31,32]. The classical channel could be an optical or RF link.

The idea of a QKD link using modulating retro-reflectors was proposed by Rarity in 2002 [12]. He suggested using a fast polarization modulator coupled to a single retro-reflector. In 2015 Vallone et. al. used a ground station to illuminate a satellite carrying a passive retro-reflector to show that ground to space QKD was possible [33]. Their work did not demonstrate a true MRR-QKD link because the encoding and reception of the bits were both done at the ground station. They also suggested that a retro-reflecting QKD link would be possible if a polarization rotator could be coupled to the retro-reflector.

In the 15 years since the idea of an MRR-QKD link was proposed there have been no experimental demonstrations. This is, in part, because there are no polarization modulators that have the combination of high speed, low power, large area, wide field of view, and compatibility with retro-reflection necessary for an efficient MRR-QKD link. Liquid crystals have most of these properties, but their maximum speed is in the tens of kilohertz. Pockel's cells require very high voltages, which limits high repetition rate operation, and consumes large amount of power.

Indeed the only MRR modulators that have been demonstrated that could achieve bandwidths of 100 MHz or greater are those based on surface-normal multiple quantum wells [28]. These devices are amplitude modulators and do not rotate polarization. However, there is another way to use them that allows them to act as BB84 encoders. A schematic of this approach is shown in Fig. 2.

Figure 2a shows an MRR-QKD array consisting of four MQW modulating retro-reflectors, each with a polarizer in front of it set to one of the BB84 bases. Figure 2b and 2c show the operation of the device. As before, Bob's interrogation beam contains no information. Bob's interrogation beam is circularly polarized. The MRR-QKD array is configured with a single input/output aperture to prevent Eve from distinguishing the reflection of the four MRRs by differences in their spatial mode patterns. Light enters through the input/output aperture and is divided up by a set of beam-splitters so that an equal amount falls on each of the MRRs. The input/output aperture can also, optionally, contain a variable attenuator to control the intensity of light that is retro-reflected. In operation three of the MRRs are left in the low transmitting, "closed" position so that they do not retro-reflect. For each bit, Alice randomly chooses one of the MRRs to be in a high transmission state. This MRR will retro-reflect light in the polarization corresponding to its internal polarizer back down to Bob.

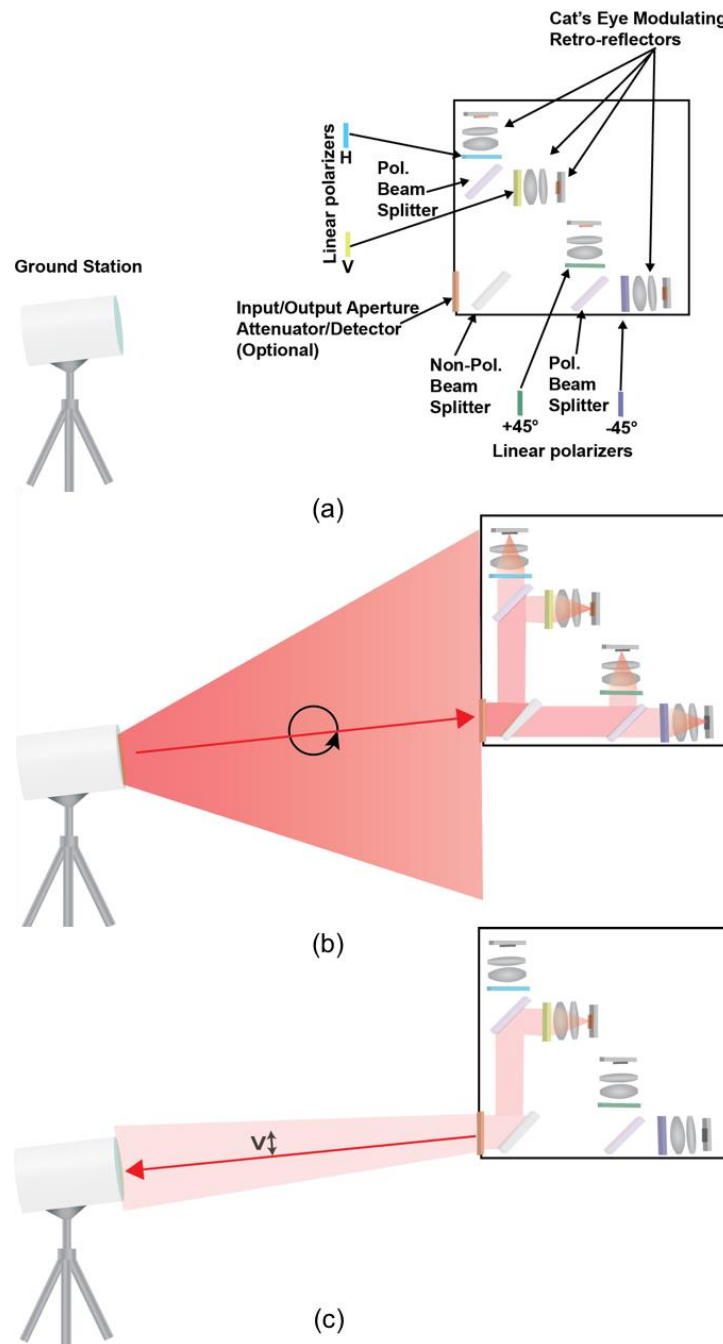


Fig. 2. Schematic of a quantum key distribution link using modulating retro-reflectors showing (a) the components. (b) An example of the interrogation of the MRR array from the ground station using a strong beam of unencoded circularly polarized light. (c) Three of the four modulators are in a low transmission state and one, the vertically polarized MRR in this example, is in a high transmission state. This MRR retro-reflects vertically polarized light. The interrogation steps and the retro-reflection step happen simultaneously, but are shown here sequentially for clarity.

Conceptually, this is very similar to conventional free space QKD transmitters that use four lasers, each set to one of the BB84 polarizations, except that in this case the photons are

supplied by the ground terminal [16,34]. This new configuration for an MRR-QKD links enables high performance amplitude modulators to be used, allowing the link performance to be very attractive.

An MRR-QKD link can have relaxed requirements on *both* ends. The effective transmit power of the MRR is limited to only a few picowatts, at 100 MHz rates, by the single photon requirement of the protocol. Even at ranges of a few hundred kilometers, supplying such a small amount of power to retro-reflect places a light burden on the ground station.

The mobile platform pointing requirements will be set by the field of view of the retro-reflector. Even for MRRs with relatively narrow fields of view, such as some of those based on cats's eye optics, this will be a few degrees [28].

Quantum MRR links have some advantages as well in comparison to classical MRR links. While a classical MRR link exhibits a $1/R^4$ dependence, in many cases a MRR-QKD link will exhibit an effective $1/R^2$ dependence. This is because the illumination power on the MRR will, in most cases, be limited by the single photon condition, rather than the interrogator's ability to put power on the aperture. As the range increases, the interrogator output power can be raised to keep the incident flux the same.

3. Experimental demonstration

A. Multiple quantum well retro-reflector array for BB84 encoding

Multiple quantum well modulators used for MRR links are large area PIN devices used in reverse bias, and illuminated in surface normal mode. For classical MRR links they have been implemented using two different architectures.

Corner cube based MRRs place a transmissive MQW modulator in front of the corner cube, or a reflecting MQW modulator as one of the sides of the cube [27]. The MRR can have a field of view as large as 60 degrees depending on the index of refraction of the corner cube material. The diameter of the modulator must be at least as large as the diameter of the corner cube. Electrically, the MQW modulator acts as a capacitor with a series resistance determined largely by the sheet resistance of the semiconductor contacts. Thus, the speed of the modulator scales inversely with its area, while the power consumption scales proportionally to its area. Corner cube MRRs must balance using a large aperture to return a strong signal with limitations on bandwidth from the electrical characteristics of the modulator.

The second MRR architecture is based on cat's eye retro-reflectors [35]. Cat's eye optics come in a wide variety of forms, but for MRR links are generally custom lens designs that return diffraction-limited beams. The MQW modulator is placed in the focal plane of the cat's eye. The size of the modulator depends on the diameter of the cat's eye, its numerical aperture, and the field of view over which it operates. This more complicated dependence allows more trade-offs between optical aperture, and hence return beam divergence, and the bandwidth of the MQW modulator. In addition cat's eye MQW MRRs can be operated in a pixelated fashion that, in principle, allows arbitrary scaling of the modulator bandwidth to hundreds of MHz or even GHz [28,29].

Either architecture could be used for a QKD link. Corner cubes would be most appropriate for short-range links, especially when no pointing of the MRR terminal is possible. The cat's eye configuration will likely be needed for long-range links, such as ground to space, where a large aperture and high bandwidth will be needed to generate a sufficiently high key rate (see section 4).

For both architectures, a principal challenge is the extinction ratio of the MQW modulator. The MQW modulators used for classical MRR links typically have about 80 pairs of multiple quantum wells and a total device thickness of about $3.5\ \mu\text{m}$ [36]. In operation, the MQW is traversed twice. The typical extinction ratios are about 3-4 dB, with a 5 V drive. These extinction ratios are acceptable because the detectors used in these links (large area PIN diodes or linear mode APDs) are not shot noise limited. Thicker MQW devices, which

would produce larger extinction ratio, are not used because they would also have larger on-state loss and, so, provide no advantage.

For an MRR-QKD link this low extinction is not acceptable. The extinction of the modulator will set a floor for the minimum quantum bit error rate (QBER) that is possible for the link. QBERs of greater than 11% render a QKD link insecure, and even values below this reduce the key rate.

To improve extinction ratio of the MQW we used two approaches. First, we developed a new MQW design with 160 pairs of strain-balanced InGaAs/InAlAs coupled quantum wells, designed to operate in the telecom c-band near 1550 nm. The epilayer structure of this design was similar to one we have previously reported [36], but the number of periods was doubled. This increased the total device thickness to about 5 microns, making fabrication more difficult and decreasing device yield.

Figure 3a shows the experimentally measured single-pass absorption spectrum of the multiple quantum well modulator for three different applied biases. The band-edge absorption of a MQW modulator is a continuous function of voltage.

At wavelengths between about 1525 nm and 1545 nm the absorption of the device decreases as voltage is applied, so the higher the applied voltage, the higher the transmission. We can define the extinction of the modulator as the ratio of the double pass transmission of the device at a given drive voltage to the double pass transmission at 0 V. We use the double pass transmission since, when used with a retro-reflector, the MQW is crossed twice. Figure 3b shows the experimentally measured double-pass extinction of the MQW modulator, driven with a 10 V bias, as a function of wavelength. The peak extinction is about 7.5 dB and occurs near the band-edge of the quantum well.

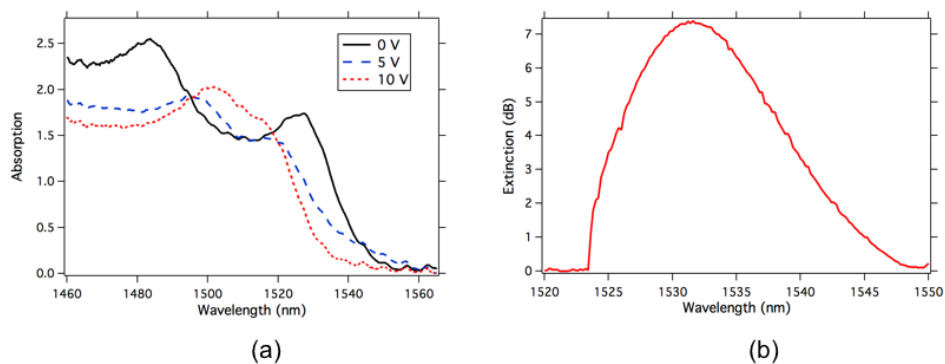


Fig. 3. (a) Exciton electro-absorption spectra and (b) Double-pass extinction of the MQW modulator measured at a 1 MHz modulation rate.

This extinction ratio would still yield an unacceptable QBER, but thicker devices would be impractical to fabricate. To increase the extinction further, a stack of two MQW modulators devices were packaged together in a single mount and driven with the same signal. This increased the peak extinction ratio to about 15 dB with 12 dB loss in the on-state. For classical MRR links this loss would negate the benefit of the higher extinction, but for a QKD link the extinction is required, and the loss is not a problem for most links (see section 4).

As shown in Fig. 4, the MQW modulators were fabricated as 6.5 mm diameter mesas. This is a very large size for MQW modulators, which can limit the modulation speed because of the high RC time constant. To provide high bandwidth we used a number of strategies that have been effective for classical links. Thick, highly doped contact layers help reduce the sheet resistance of the device, as does a web electrode on the top, p-type contact [37]. In addition, the device is divided into 4 pixels, each with its own MOSFET driver. All four pixels were driven with the same signal.

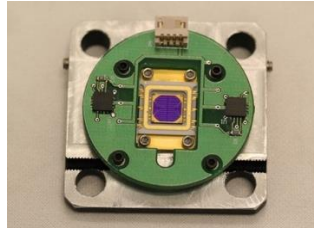


Fig. 4. A 6.5 mm diameter multiple quantum well modulator.

The modulator has a capacitance of about 2.5 nF/cm^2 and a sheet resistance of about 10 Ohms. Each quadrant of a 6.5 mm modulator thus had a capacitance of about 200 pF, and an RC time of 2 nanoseconds. The 10%-90% rise time of the MQW modulator was measured at 3.8 nanoseconds, limited by the minimum rise-time of the MOSFET driver, so a maximum modulation rate in excess of 100 MHz is possible. In the experiment, the modulators were opened for 25 nanoseconds and driven at a maximum repetition rate of 5 MHz, limited by the field programmable gate (FPGA) control electronics.

MQW modulators are capacitive devices and have a power consumption of:

$$CV^2 f \quad (1)$$

where C is the device capacitance, V is the drive voltage and f is the modulation rate.

Since, on average, a modulator is only open for one in four cycles, the power consumption of an individual modulator was 100 mW at the 5 MHz rate used in the experiment. The total power consumption of the entire MRR array was 800 mW at 5 MHz rate.

Faster control electronics could allow 100 MHz operation. However, at faster rates the modulator will self-heat substantially. Though the extinction will remain constant, up to the device bandwidth, the wavelength at which the peak extinction occurs will move to the red as the device heats. If we allow a 1 dB variation in the single device extinction, the allowable wavelength shift is $\pm 3 \text{ nm}$. The band-edge of InGaAs shifts at about $0.7 \text{ nm/}^\circ\text{C}$, so the allowable temperature variation is $\pm 4 \text{ }^\circ\text{C}$. Two approaches can be used to stabilize the response of the MQW modulator to temperature changes. For classical MQW MRR links a tunable interrogator has been used, so that the interrogation wavelength can follow the peak extinction [38]. For a laser operating with the range of typical Erbium fiber amplifiers, this allows about $50 \text{ }^\circ\text{C}$ of variation. An alternative is to use active stabilization of the modulator temperature, for example with a thermo-electric cooler. This type of temperature stabilization is straightforward, and is commonly used for temperature sensitive equipment on spacecraft and air platforms. In fact, compared to the temperature stabilization necessary for most lasers, the $\pm 4 \text{ }^\circ\text{C}$ stability needed for MRRs is relatively easy.

Each MRR consisted of a 6.3 mm diameter glass corner cube packaged with a linear polarizer and a stack of two multiple quantum well modulators placed in front of it. At 1550 nm the MRR has a diffraction-limited retro-reflected beam divergence of 630 microradians. The array consisted of four MRRs. An alternative arrangement, not used for this paper, but discussed section 4, could use the same 6.5 mm diameter MQW modulator combined with a 2.8 cm diameter cat's eye optic. In this case the beam divergence would be 140 microradians, and the field of view would be 5° .

For best performance, the MRR should have a retro-reflected beam divergence that is no larger than the diffraction limit for its aperture. In practice, this means using corner cubes or cat's eye retro-reflectors that do not introduce wavefront aberration. It also requires the MQW modulator to be optically flat. These are also considerations for classical MRR links, and we have, in past work, verified that both the corner cube and cat's eye MRRs we have developed return a diffraction-limited beam [28].

B. Laboratory demonstration of a free space quantum key distribution link using modulating metro-reflectors

A laboratory-based free space QKD link using a corner cube modulating retro-reflector array was set up. Figure 5a shows the schematic of the whole system. The interrogator consists of a transmitter and a receiver arranged in a bistatic configuration. The transmitter portion of the interrogator consisted of a linearly polarized, fiber-coupled cw semiconductor laser, tunable from 1530 to 1563 nm. A fiber collimator was used to bring the beam out into free space, and a waveplate was used to change the polarization to circular. Attenuators could be used to control the beam intensity that would hit the MRR array so that the retro-reflected beam intensity would be about 0.1 photons per bit. The beam was propagated 6 meters to the MRR-QKD array.

The MRR array is shown in detail in Fig. 5b. It is similar to the setup in Fig. 2 except for the use of corner cube retro-reflectors instead of cat's eyes, and some additional optics to maintain polarization states. The circularly polarized beam enters the system and is split by a non-polarizing beam splitter into two paths, one for each of the BB84 bases. In the path for the H-V basis, the circularly polarized beam is split into horizontal and vertical components by a polarizing beam-splitter. Each component then proceeds to a modulating retro-reflector, which has an additional polarizer to maintain polarization purity. If an MRR is set to a high transmission state, light will be retro-reflected in the appropriate polarization back through the polarizing beam-splitter and then through the non-polarizing beam-splitter to the interrogator.

The path for the 45° rotated +/− basis is similar, but a half wave plate is placed before the polarizing beam-splitter. For the incoming circularly polarized light, this waveplate acts to retard the phase by π but still leaves it circularly polarized, regardless of the waveplate's orientation. However, for the half wave plate oriented at 22.5 degrees to the H/V basis, the *retro-reflected* horizontal or vertically polarized beams are rotated 45 degrees, becoming the +/− basis pair on its return path through the system. The entire MRR array setup fit on a 40x40 cm optical breadboard.

The retro-reflected beam propagates back through free space to the receive section of the interrogator. The schematic for this section is shown in Fig. 5a, and is a conventional BB84 receiver. The incoming beam is split by a non-polarizing beam-splitter into an H/V and a +/− arm. In the +/− arm a half wave plate rotates the polarization into the H/V basis for convenience.

Polarizing beam-splitters in each arm send each polarization to Aurea multimode fiber coupled InGaAs Geiger mode avalanche photodiodes. The detectors were run at 10% quantum efficiency. The system was controlled by a custom field programmable gate array (FPGA). In each time slice, the FPGA sent a master sync pulse to a multichannel digital delay generator that was used to gate the Aurea detectors. The detectors were opened for 10 nanoseconds in each cycle. Detector dark counts averaged 7 s^{-1} when triggered at 5 MHz.

A second multichannel digital delay generator was connected to the drivers for the four MRRs. With no bias applied, the modulators were in a low transmission, closed, state. The MQW modulator pair for an MRR could be set to a high transmission state by applying a 10 V bias.

The system shown in Fig. 5 was used to demonstrate the generation of a sifted key using the standard BB84 protocol. The interrogator acted as Bob. Its CW laser supplied a stream of circularly polarized photons that were directed through free space to the input/output aperture of the MRR array, which acted as Alice.

In each time slice, one of the four MRRs was opened for 25 nanoseconds. This MRR was selected by the FPGA, which used a pre-generated file of 2^{15} random numbers to select which of the four channels to open, simulating Alice's random selection of which polarization state to transmit. The selected MRR reflected the BB84 polarization state corresponding to its

internal polarizer back to Bob's receiver. Attenuators in the return beam path were added to simulate link loss.

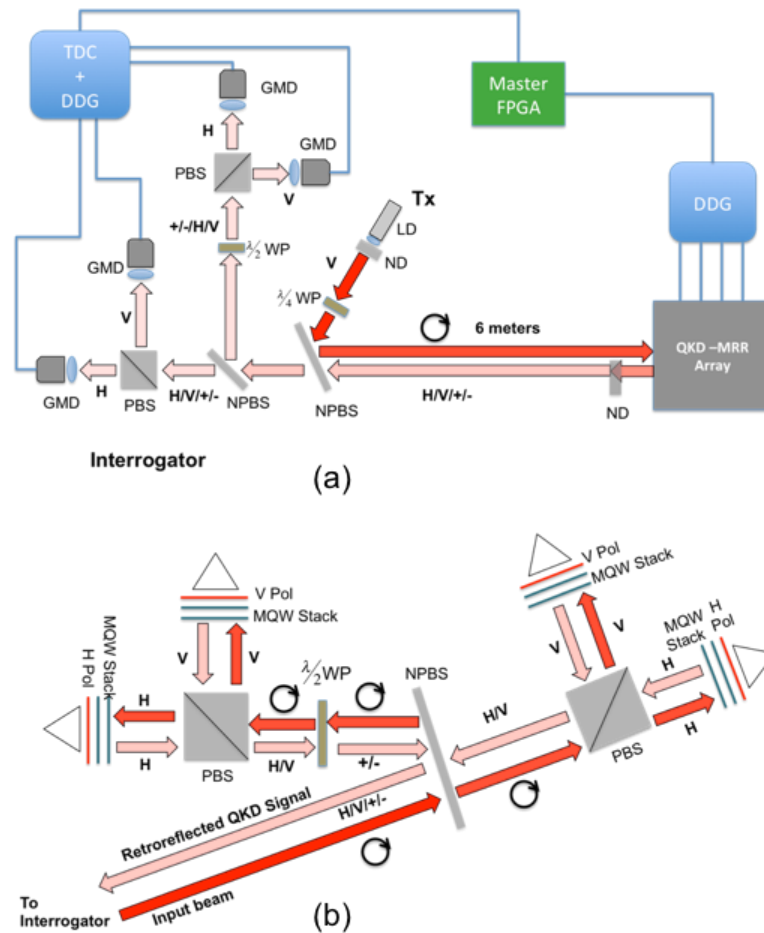


Fig. 5. Schematic of the MRR-QKD BB84 link experiment, showing (a) Details of the interrogator and the control electronics. TDC, time to digital converter; DDG, digital delay generator; GMD, Geiger mode photodetector; PBS, polarizing beam splitter; NPBS, non-polarizing beam splitter; WP, waveplate; ND, neutral density filter; LD, laser diode; FPGA, field programmable gate array; (b) Details of the MRR-QKD array. Beam dumps are not shown, for clarity.

In Bob's receiver, the non-polarizing beam-splitter at the entrance acted to provide the random selection of measurement basis, and the polarizing beam-splitters routed incoming photons to the appropriate single photon detector. For each time slice a multi-channel time to digital converter was used to record which of the single photon detectors fired. The time to digital converter also recorded the sync pulse sent from the FPGA at the beginning of a link to establish correct timing between the detector responses and the sequence of MRR states. A link lasted 10 seconds.

At the end of the link, the data was post-processed using the standard BB84 algorithm [1,2,32]. The data from the time to digital converters was used to determine which polarization state Bob measured in each time slice in which a detector fired. The random number file in the FPGA was used to determine which polarization state Alice transmitted in each time slice. The sifted key was developed using those time slices in which Bob measured a polarization state in the same basis that Alice transmitted. The QBER was determined by

comparing this sifted key to the sequence of polarization states transmitted by the MRR array. No additional error correction or privacy amplification was applied.

Sets of experiments with modulation rates of 1, 2.5 and 5 MHz were run. At each modulation rate runs were conducted for different interrogation laser wavelengths. MQW modulators have a wavelength dependent extinction, hence we expect the QBER to vary as the laser is tuned. In addition, MQW modulators can self-heat, which will shift the band-edge of the well material, and thus the optimum interrogation wavelength.

Figure 6 shows the QBER as a function of laser wavelength for the different modulation rates. Errors could be caused by dark counts in the detectors, background light, or leakage of light through the modulators that were set to their off-state. We were interested in quantifying the effects of leakage. The attenuation was set to simulate a link in which the retro-reflected rate of signal photons was 0.1 photons per bit and the propagation loss was about 15 dB. The sifted key rate was then about 1000/s, well above the dark counts of the detectors. The experiments were conducted in the dark so background flux was not significant. As a result, the QBER was determined by leakage from the three modulators set to their off state. This leakage was determined by the extinction ratio of the modulators and the polarization purity of the system as a whole. The minimum QBER seen in Fig. 6 is about 5%. The wavelength of this minimum shifts to the red for higher modulation rates, reflecting self-heating in the modulator. As the laser wavelength moves away from the minimum, the QBER climbs, eventually reaching the point at which link security cannot be maintained. We show the variation in QBER to exhibit the wavelength dependence of the modulator. In a real link the interrogation wavelength or the device temperature would be controlled so that the system would function at its minimum QBER of 5%.

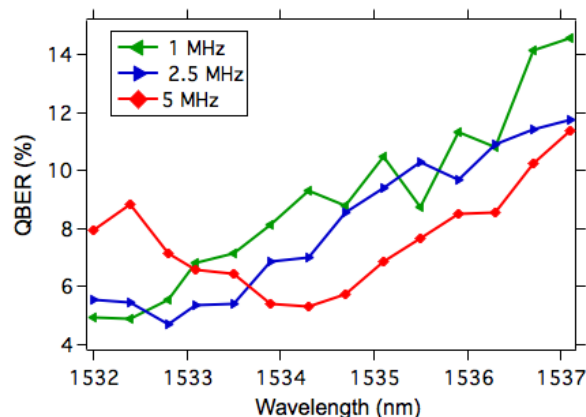


Fig. 6. Quantum bit error rate for three different modulation rates as a function of laser interrogation wavelength.

While a QBER of 5% can allow the development of a secure key, a lower error rate would be desirable to maximize the key rate. This could be achieved by adding a third MQW modulator to each stack. This would increase the extinction to around 23 dB, and drop the QBER due to extinction to about 1%. This would come at the cost of raising the insertion loss in the on-state, which would require the interrogating laser to be stronger, or its beam divergence to be tighter, or some combination of both. However, since the interrogator link budget for many MRR-QKD links is not very challenging, this may be an acceptable trade-off. We discuss this trade-off further in Section 4.

4. MRR-QKD link budgets

A. Link Budget Equations for QKD Links using Modulating Retro-reflectors

A modulating retro-reflector link can be split into two parts. In the uplink, the interrogating laser delivers optical power to the MRR, which acts as a receiver. The light passes through the modulator and, after some loss, is modulated. The wavefront is retro-reflected and a beam exits the aperture of the MRR. In the downlink, the MRR acts as a transmitter sending the modulated light back down to the interrogator.

The budget for the uplink is [23,38],

$$P_{\text{retro}} = P_{\text{las}} G_{\text{Tx}} L_{\text{Tx}} L_{\text{R}} L_{\text{atm}} G_{\text{MRR}} M \quad (2)$$

The budget for the downlink is,

$$P_{\text{sig}} = P_{\text{retro}} G_{\text{MRR}} L_{\text{atm}} L_{\text{VA}} G_{\text{Rx}} L_{\text{Rx}} \quad (3)$$

Table 1 . Definitions of Terms in MRR-QKD Link Budget

Symbol	Term	Definition
P_{retro}	Power at the MRR	
P_{las}	Transmit power	
G_{Tx}	Transmit antenna gain	$\left[\frac{32}{\theta_{\text{Div}}} \right]^2$
L_{Tx}	Transmit loss	
L_{R}	Propagation loss	$\left[\frac{\lambda}{4\pi R} \right]^2$
L_{atm}	Atmospheric loss	
G_{MRR}	Antenna gain of the MRR	$\left[\frac{\pi D_{\text{retro}}}{\lambda} \right]^2$
M	Modulation efficiency	
L_{VA}	Velocity aberration loss	
G_{Rx}	Receive antenna gain	$\left[\frac{\pi D_{\text{Rx}}}{\lambda} \right]^2$
L_{Rx}	Receive loss	
P_{sig}	Received signal power at the interrogator	
θ_{Div}	Transmit divergence	
D_{retro}	Diameter of the MRR	
D_{Rx}	Receiver diameter	
R	Link range	
λ	Laser wavelength	

The definitions of these terms are shown in Table 1. We assume a diffraction limited retro-reflector. We also define the parameter M , the modulation efficiency. For high extinction modulators, M is approximately equal to the on-state loss of the modulator. This link budget has been verified over many field tests of classical MRR links [24,25,39].

In a classical MRR link, the uplink budget is optimized to deliver the maximum possible power to the retro-reflector. In an MRR-QKD link we must limit the uplink power so that the retro-reflected signal does not violate any security protocols. The allowed retro-reflected power will vary but for BB84 using decoy states will be about 0.5 photons/bit [40,41].

In general, it is desirable to make the retro-reflector aperture as large as possible, since for a diffraction limited MRR this will increase its antenna gain. However, for links to rapidly

moving platforms, such as satellites, the effects of velocity aberration must be taken into account [12,42].

Velocity aberration is a relativistic effect that causes the beam to deviate from true retro-reflection, and is a well-known consideration in satellite laser ranging links. For satellites in low Earth orbit, the amount of velocity aberration varies, but can be as much as 50 microradians [42]. Thus, as the MRR diameter gets larger and the beam divergence narrows to approach this value, the returned power can drop. The term L_{VA} takes into account the loss due to velocity aberration by calculating the diffraction pattern of the retro-reflector, offsetting it by the velocity aberration, and integrating over the receive aperture of the interrogator. In practice, at a wavelength of 1550 nm, the point of diminishing returns in MRR aperture is about 3 cm.

A variety of approaches for dealing with velocity aberration, including spoiled corner cubes and biprisms [12] have been proposed and used, so future work may allow larger diameters.

B. Example link budgets for QKD-MRR links

A wide variety of QKD-MRR links are possible, from very short-ranges for encrypted consumer transactions [9], to space-based links [17]. Here we consider three possible examples. The first is relatively short-range fixed-point link, and the other two are long-range mobile links. These are simplified analyses. More realistic link budgets would require detailed analyses including background light, orbits, and other details. However, these links illustrate some of the unique features of QKD using MRRs.

We assume the use of a decoy state protocol [7] so that an average emission rate of 0.5 photons per bit may be used. We calculate the rate at which a sifted key can be created. That is, the key produced after Alice and Bob have eliminated all bits in which they did not share the same basis, but not including any reduction in the key length due to other error correction protocols or privacy amplification. For all links, we also assume a laser wavelength near 1550 nm, though other choices are possible.

First, we consider a link with an MRR array, similar to that described in the paper, using 6.3 mm diameter corner cubes each with a stack of two MQW modulators, but in this case running at 100 MHz. We consider a link range of 10 Km, as might occur in a metropolitan area. Such a link might be used if a dedicated fiber optic line was not available. The interrogator must control its output power and beam divergence such that the retro-reflected power is about 0.5 photons per bit. We allow for a 2 dB loss each way from atmospheric scattering. The double pass loss through the MRR arrays has a contribution of 9 dB from the beam-splitters, 12 dB from loss through the MQW in its high transmission state and 1 dB from residual loss after the anti-reflection coatings on the modulators. The total double pass loss through the MRR array is thus 22 dB. The required illuminating flux on the MRR can be produced using an interrogator with a 40 mW output power, and a 5 milliradian beam divergence. These are very easy transmitter requirements to meet. In fact, typical terrestrial FSO terminals operate with divergences below 1 milliradian.

If a stack of three MQW modulators in each MRR was used to lower the QBER, the double pass loss through the MRR array would go up by 6 dB. This could, again, be easily accommodated, either by raising the interrogating laser power to 240 mW, or decreasing the transmitter beam divergence to 2.5 milliradians. Thus, operating an MRR-QKD link at low QBER will not significantly increase its complexity.

An InGaAs Geiger-mode single photon avalanche detector (SPAD) is assumed with a detection efficiency of 20%, and an overall receiver efficiency of 10%. If the receive aperture is 10 cm, a key rate of 1000/s would be possible.

The assumed optical terminal parameters are easily met by many of the commercial building-to-building classical laser communication terminals that have been developed, by replacing their detectors with a SPAD.

For long range links, we assume a cat's eye MRR based on an existing diffraction limited design, with a 2.8 cm aperture and a 5° field of view [28,38], and the same MQW modulator stacks described in the paper. The modulation rate of the MQW modulator is again taken as 100 MHz. Here we assume the use of an efficient single photon detector such as a superconducting nanowire [43,44]. An overall receiver efficiency of 40% including optical and filter losses is assumed.

First, we consider a link to a stratospheric balloon. Recently Google's Project Loon has demonstrated classical free space optical links between pairs balloons operating at about 20 km altitude [45]. Ground to air links to these balloons are also possible. For example, two ground-based users separated by about 150 km could be connected by a balloon carrying two MRR-QKD arrays using two QKD exchanges. The link range from each user to the balloon would be 80 km, and the elevation angle would be 15 degrees.

On the balloon, the cat's eye MRRs would only need pointing to within 5° of the ground station, which can easily be met with a lightweight gimbal and a simple tracking system. The required illuminating flux on the MRRs could be achieved by a ground station with a 50 mW laser and transmitter beam divergence of 5 milliradians. When compared to a classical FSO communication system in which the laser power would typically be several watts and the beam divergence not wider than a few hundred micro-radians [46], these are very modest requirements. If a lower QBER MRR, with stacks of three multiple quantum well modulators, were used, the interrogator would require a beam divergence of 2.5 milliradians.

The requirements on the receiver at the ground station are more typical of a classical FSO link, and the ground station pointing requirements would be set by the receive field of view. If the interrogator's receive aperture were 0.5 meters, a key rate of 44,000/s would be possible. While the range for this link is possible for fiber based QKD, the potential key rate is much higher for the MRR-QKD link [3].

Next we consider a ground-to-space link with the MRR on a small satellite such as a cubesat [19,34]. If we assume an orbital height of 600 km, the range of the link would vary from 600 km with the cubesat at zenith to about 1075 km for an elevation angle of 30° . The uplink calculations are similar to those for the high altitude balloon. For example at zenith, assuming about 1 db of loss each way from atmospheric scattering, a ground station transmitter with a beam divergence of 2 milliradians and a 300 mW laser would illuminate the MRR on the cubesat with sufficient power for it to reflect back 0.5 photons/bit. For a pass at 30° degree elevation the range would increase and the atmospheric loss would be somewhat higher. In this case boosting the laser power to about 1 watt would provide sufficient illumination of the MRR.

As with the high altitude balloon links, the pointing burden on the spacecraft are enormously relaxed compared to conventional QKD link. The spacecraft must point the MRR array to within 5° (85 milliradians) of the ground station. This compares to pointing requirements of about 30 μ rad for a conventional QKD link, three orders of magnitude tighter. The impact of this reduced pointing requirement on the size and complexity of a rapidly moving low Earth orbit satellite is very significant, and one of the principle advantages of MRR-QKD links over conventional free space QKD links. The reduced pointing requirements would allow the spacecraft to dispense with the use of both gimbals and fast steering mirrors and use body-pointing systems with star-trackers and reaction wheels [47].

The downlink from the MRR is quite different from the balloon case because of velocity aberration [12,42]. For a 600 km orbit the amount of velocity aberration varies from about 25 μ rad to 50 μ rad, with the larger values appearing on zenith passes. The full angle $1/e^2$ beam width from a 2.8 cm retro-reflector at 1.55 micron wavelength is 140 μ rad, so the loss due to uncorrected velocity aberration can be large. The fact that the velocity aberration is largest for the passes with the shortest range does help even out its effect, but velocity aberration losses range from 3 to 12 dB. If we assume a one meter ground station receiver, a

key rate of about 500-700/s would be achievable for most of the passes above 30 degrees. Increasing the size of the MRR would not help, and in fact would decrease the key rate because of the effects of velocity aberration on the narrower beam. A larger receive telescope or a higher modulation rate at the MRR could increase the key rate, and both are certainly possible.

If an MRR with correction for velocity aberration could be created, the key rate could be an order of magnitude higher for the assumed 2.8 cm MRR. In fact, in this case a larger MRR could be used further increasing the rate.

5. Security of MRR-QKD links

A. General aspects of MRR-QKD link security

As with all QKD links, the vulnerability of the link to various kinds of attack must be considered [32,48]. A variety of quantum hacking attacks have been proposed and demonstrated, based on the vulnerabilities of components used in QKD systems [49–51]. An MRR-QKD link shares many characteristics of other kinds of QKD links, and as a result also shares many of the same attacks, counter-measures, and security analyses. In this section, we consider only those attacks that are unique to MRR-QKD links. Many of these attacks have similarities to other QKD implementations, and we can use earlier work as a guide in the analysis [52]. While MRR-QKD links have unique vulnerabilities, they also have some unique capabilities that allow countermeasures not available to other kinds of QKD links. First, we consider some physical aspects of MRR-QKD links that apply to all attacks.

1. If Eve intercepts Bob's interrogation beam before it strikes Alice's MRR array it yields no information. All photons at this point are circularly polarized.
2. If Eve illuminates the MRR array from an off-axis position, then the retro-reflected photons will not strike Bob's receiver unless Eve redirects them. Eve is off-axis if the angle between her position and Alice's MRR array differs from the angle between Bob's interrogator and Alice's MRR array by more than the divergence of the retro-reflected beam. This is a simple consequence of the physics of optical retro-reflection.
3. The double pass loss of an MRR-QKD array based on multiple quantum well modulator is high. As described in section 4 the loss for the array described in this paper, with a stack of two MQW modulators in each MRR, is 22 dB, while an array with a stack of three modulators would have a loss of 28 dB. This requires the light incident on the array to be much brighter than the desired retro-reflected intensity. For example, interrogating an array using two-modulator stacks operating at 100 MHz with sufficient intensity to reflect a mean intensity of 1 photon per bit would require a power of 2 nW incident on the entrance aperture of the array. For a three-modulator stack, the incident power would need to be 8 nW.
4. The transmission of the MQW modulators used in the MRR-QKD arrays is a continuous function of the applied bias. The MQW modulators have their minimum transmission at zero applied voltage (at the interrogation wavelengths used in this work). As the voltage is increased, their transmission increases. In this work, the modulators were operated at one of two voltages: 0 V for off, and 10 V for on. However, a lower on-voltage could be chosen to retro-reflect less light.
5. The MQW modulators used in this work are PIN diode structures operated in reverse bias at wavelengths near the band-edge of the semiconductor. As a result, in addition to acting as modulators, they also act as photodetectors. Thus, these devices can detect the amount of interrogating light falling on them. In addition, when used in high speed cat's eye MRRs, the MQW is pixelated. Since the MQW sits in the focal

plane of the cat's eye lens, the position of the focal spot on the pixelated MRR corresponds to the angle of incidence. So that, in addition to detecting the total amount of light falling on them, they can also determine the angle from which the light has come. In fact, this mode of operation can be used to allow high speed operation of cat's eye MRRs at low drive power [28], by detecting which pixel is illuminated by the interrogation beam and only driving that one with a modulation voltage.

B. Photon number splitting attacks

The essentials of the photon number splitting attack are the same for MRR-QKD links as for any other QKD links [32]: If more than one photon is transmitted, Eve can intercept one photon and let the others pass without introducing excess error into the link. To counter this, Alice must ensure that the chance of her emitting more than one photon per bit is low. For the MRR-QKD link, this requires that the mean number of photons that are retro-reflected is low; about 0.1 photons per bit without decoy state, and 0.5 with decoy states. There are two ways to accomplish this: Bob can limit his interrogation power, or Alice can adjust the double pass loss of her MRR array. In practice both approaches must be used. Bob, knowing the geometric propagation and approximate scattering losses of the interrogation link should adjust his laser power appropriately. However, Alice should also detect the amount of power incident on the MRR-QKD array and adjust its on-state transmission. This is for two reasons: First, to compensate for power fluctuations due to optical scintillation [53] and second, as we discuss below, to thwart attacks by Eve.

The photodetection capability of the MQW modulators makes the detection of the incident intensity simple, requiring no new components, just straightforward modification of the MQW's associated electronics [28]. Each MRR in the array can detect how much light is incident on it. Because, as described above, the interrogation beam must be quite bright, the photodetection sensitivity of the MQWs does not need to be particularly high.

The on-state loss of the MRR-QKD array can be adjusted in two ways. First, Alice can use a lower applied voltage for the on-state of the modulator. Again, this requires no new components. However, it does lower the extinction ratio of the array, increasing the QBER due to leakage. For MRR QKDs using stacks of three modulators, this may be acceptable, but for lower extinction systems there is another approach. A single additional MQW modulator stack can be placed at the entrance to the MRR-QKD array as shown in Fig. 2. This modulator stack can adjust the overall retro-reflected power without reducing the extinction ratio. It will increase the double pass loss of the array, requiring higher interrogation intensity, but as discussed in Section 4 this is not a problem as the interrogation links are relatively easy. This input stack can also be used to detect the incoming photon flux.

C. Intercept-resend attacks

Attacks in which Eve intercepts Alice's retro-reflected photon, measures it, and then resends it to Bob can be defeated in the same way as for any other BB84 link, by monitoring the QBER of the link, and ensuring it does not exceed a given level [32,48].

However, different variants of this attack are available to Eve due to the retro-reflecting nature of the link. Using a bright interrogator attack, Eve can intercept Bob's interrogation beam and replace it with her own much brighter beam designed to reflect back a much larger mean number of photons. She can then intercept the retro-reflected beam, measure one of the photons, attenuate the rest of the beam down to a low mean number, and let it propagate down to Bob. Effectively Eve creates the conditions that allow a photon number splitting attack.

As with fiber based plug and play links, these attacks can be defeated with active countermeasures [52]. First, since Alice should detect the incoming photon flux and adjust the on-state transmission of the array to retro-reflect a low mean photon number, Eve's bright

interrogation beam should automatically drive down the reflection of the array preventing the photon number splitting attack. If Eve's beam is so bright that Alice cannot reduce her reflectivity sufficiently then she can discard bits transmitted in these time slices.

A different variant of the intercept-resend attack, relies on how the MRR-QKD array produces a polarization state. In a weak polarized interrogator attack, Eve intercepts Bob's circularly polarized interrogation beam and substitutes a weak beam, but one that is linearly polarized in one of the four BB84 polarizations. In each time slice, Eve randomly selects one of the possible polarization states and illuminates Alice's MRR array. Because the beam is linearly polarized, Eve knows that the MRR array cannot retro-reflect the polarization orthogonal to the one she selected, since the polarized beam-splitters will not direct any light to that MRR. Half of the incident light will go to the MRR for Eve's selected polarization, and one quarter of the light will go to each of the MRRs in the basis that Eve did not select. Eve does not intercept the retro-reflected beam, but allows it to propagate back to Bob. Later, during the public communication between Bob and Alice, Eve can determine those time slices in which Bob picked the same measurement basis as Eve's linearly polarized interrogation beam. In those cases, she will know what bit Bob received. So, Eve gains a certain knowledge of half the bits in Alice and Bob's key.

Alice's countermeasure again uses the photodetection capability of the MQWs, and particularly the fact that all four MRRs can monitor the incoming power. If she sees an unequal amount of interrogation power falling on the MRRs she knows that the interrogation beam is not circularly polarized and she can discontinue the link, or ignore those bits with unequal power. Alice may also choose to use privacy amplification for those times when she detects this kind of attack. Bob can also detect this attack because his key rate will drop.

For both kinds of intercept resend attacks, in addition to optical power based detection schemes, Alice may be able to detect the fact that Eve has replaced Bob's interrogation beam if Eve uses off-axis illumination. Alice can use the angle of arrival sensing capability of the cat's eye MRR to determine that the interrogation beam is not coming from the proper location. In addition, if Eve uses off-axis illumination, then she can't simply allow her interrogation beam to retro-reflect to Bob because it will miss. She must send her own beam down to Bob. However, since Bob's receiver will have a narrow field of view aimed at Alice, Eve's beam may not enter Bob's receiver, and if it does it will be detectable as coming from the wrong angle. So, in practice, Eve must use an on-axis attack in which she positions herself directly along the line of incidence between Alice and Bob. In addition to the practical difficulties in doing this between moving platforms, for space-based platforms orbital dynamics may not allow this option except for a spacecraft using continuous powered flight.

D. Trojan horse attacks

In a Trojan horse attack, Eve does not attempt to intercept Bob's beam, but instead uses her own interrogation beam to probe the internal state of the MRR-QKD array and determine which polarization state Alice has picked for each bit. This kind of attack is well known in fiber based systems, and particularly in plug and play fiber based systems, which are similar to MRR-QKD links in that they reflect back an interrogating beam [52,54]. Since Eve can input her own circularly polarized beam into the MRR-QKD array and analyze the results she may gain knowledge of Bob and Alice's key without disturbing their link.

As with fiber based systems, several counter-measures exist [52]. Alice should use optical filters, to limit the range of wavelengths that enter the system. In addition, Alice can limit the range of angles that can enter or retro-reflect from the system through the optical design, balancing this with maintaining loose pointing requirements. The most useful countermeasures are again to detect the incoming optical power. If Eve is to gain knowledge of all of the key bits she must interrogate the MRR array with a power sufficient to reflect at least two photons per bit. Because of the double pass loss of the MRR-QKD array this is quite a large amount of power that is easily detected. It is also much larger than the power that

Bob's interrogation laser will have, which will trigger Alice to lower the transmission of the MQWs reducing Eve's information. This will also reduce Bob's key rate, which will be detectable to him. If Eve uses lower interrogation powers it will be less detectable, but also yield less information. Also, as with intercept-resend attacks, if Eve's interrogation beam is off-axis it can be detected as coming from the wrong angle.

E. Information leakage from other degrees of freedom

A side channel attack that can be used against some QKD systems is to measure other degrees of freedom of the photon that may be correlated with the degree of freedom used for the BB84 encoding [55,56]. For example, many QKD transmitters use four different lasers. Each laser is set to one of the polarization states. In each time slice one of the lasers is randomly turned on to transmit the bit. If the lasers are not matched in wavelength or if their pulse shapes are not identical, it may be possible to determine which state was sent. In addition, the spatial profiles of the lasers should be kept identical.

In fact, the MRR-QKD scheme described in this paper is very similar to the four-laser approach, with the MQW modulators playing the role of the lasers. One advantage of the MRR-QKD approach is that no information can leak out due to wavelength, because all the MRRs are illuminated with the same wavelength from the interrogation laser. However, as with the four-laser transmitter, care must be taken to match the rise and fall times of the modulators. It is also important to match the optical path lengths within the array.

The MRR-QKD array is configured with a single entrance and exit aperture so that the spatial mode profile cannot be used to determine the polarization state. However, it is also important to carefully align the optics so that there are no variations in the reflected light profile between the MRRs in the array.

6. Conclusions

This work has demonstrated the first free space QKD link using modulating retro-reflectors. Free space QKD with MRRs can allow links with a much lower pointing burden on the mobile end. This opens up the possibility of considering platforms that do not have the power and weight budget to carry high precision pointing gimbals and fast steering mirrors, such as drones, high altitude balloons and cubesats. It also has the potential to allow much lower cost links.

Running the system at rates up to 100 MHz or beyond is possible. Higher bandwidth MRR arrays will draw more power. However, in a cat's eye configuration this can be traded off against system field of view. Halving the diameter of the MQW modulators, while maintaining the same cat's eye diameter, will drop power consumption by a factor of four, at the cost of reducing the MRR field of view by a factor of two. Since the retro-reflector pointing tolerances are loose, this may be an advantageous system trade-off. For example, a 2.8 cm cat's eye MRR, could cover a 2° field of view with a 2 mm diameter MQW modulator. This is a loose enough pointing requirement to allow the use of lightweight coarse gimbals or spacecraft body-pointing. Such a system could work at 100 MHz at a power consumption of 1.5 watts. Rates to the GHz range are possible, at a modest increase in system complexity by using pixelated MRRs [28,29].

The approach of using an array of amplitude modulators to implement the link can be applied to other QKD encoding schemes. For example, phase encoding could be implemented by putting optical windows of varying thickness in each MRR in the array. The windows would each impose a fixed phase delay on the beam and as with the BB84 implementation, the modulators would select which MRR reflects in any time slice. The MRR-QKD approach is not however applicable to entangled-state QKD, but only to weak coherent states.

Short-range applications may also be attractive. This may also allow the use of very small retro-reflectors, and hence modulators. Since the modulations rate of MQWs is RC time limited up to GHz, this could enable very high rate links.

We have implemented the MRR-QKD link using modulators designed to work in the telecommunications band around 1550 nm. Other wavelengths can be used with MQW modulators based on other material systems. For example classical MRR links at 980 nm have been demonstrated using InGaAs/GaAs MQWs [27].

MRR-QKD links face a variety of attacks, as do all realistic QKD links. In most cases, these attacks can be defeated with countermeasures similar to those used for other varieties of QKD links. In some cases, unique countermeasures must be used. The class of attacks in which Eve intercepts the signal transmitted by the MRR array and replaces it with one of her own after measurement (intercept and resend) involve the same issues as in the one-way systems with the corresponding methods of mediation. For the class of attacks in which Eve illuminates the MRR array with her own signal, either as a replacement for Bob's interrogation signal or as a "Trojan horse" signal, an effective countermeasure is monitoring the incoming signal, as described by Gisin for plug and play systems [52]. The unique characteristics of the MQW devices allow them to act as both power and angle of arrival detectors without adding extra components to the system. Because of the high attenuation in the MRRs, Eve must use a strong classical-level illumination. This requirement ensures that incoming signal levels will be large enough to be easily detected.

Although this work has been done in a laboratory environment, our extensive previous field experimentation with classical MRR links [24,25] allows a confident extrapolation to longer range links because the optical propagation characteristics for both kinds of links are the same. Retro-reflector links, classical or quantum, have higher scintillation levels than one-way free space optical links [57]. The effects of scintillation, and mitigation techniques [58–60], will be important to determine in future work that takes these links out of the laboratory and into the field.

Funding

Office of Naval Research, Base program funding for the US Naval Research Laboratory.

Acknowledgments

We acknowledge the efforts of Byoung Don Kong, Doe Park and Brad Boos in fabrication of the multiple quantum well modulators.