Optimised quantum hacking of superconducting nanowire single-photon detectors

Michael G. Tanner,[1,2,*] **Vadim Makarov,**[3] **and Robert H. Hadfield**[1,2]

[1] *School of Engineering, University of Glasgow, Glasgow, G12 8QQ, Scotland, UK*
[2] *Institute of Photonics and Quantum Sciences, Scottish Universities Physics Alliance and School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, EH14 4AS, Scotland, UK*
[3] *Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

[*] *Michael.Tanner@glasgow.ac.uk*

Abstract: We explore bright-light control of superconducting nanowire single-photon detectors (SNSPDs) in the shunted configuration (a practical measure to avoid latching). In an experiment, we simulate an illumination pattern the SNSPD would receive in a typical quantum key distribution system under hacking attack. We show that it effectively blinds and controls the SNSPD. The transient blinding illumination lasts for a fraction of a microsecond and produces several deterministic fake clicks during this time. This attack does not lead to elevated timing jitter in the spoofed output pulse, and hence does not introduce significant errors. Five different SNSPD chip designs were tested. We consider possible countermeasures to this attack.

OCIS codes: (270.5568) Quantum cryptography; (270.5570) Quantum detectors; (030.5260) Photon counting.

References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in "Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing," (IEEE Press, New York, Bangalore, India, 1984), pp. 175–179.
2. QKD systems are available for purchase from several companies and research entities. Example commercial manufacturers are ID Quantique (Switzerland), http://www.idquantique.com, and SeQureNet (France), http://www.sequrenet.com/.
3. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," Nature **390**, 575–579 (1997).
4. S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," Science **335**, 303–308 (2012).
5. C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," Supercond. Sci. Tech. **25**, 063001 (2012).
6. R. H. Hadfield, J. L. Habif, J. Schlafer, R. E. Schwall, and S. W. Nam, "Quantum key distribution at 1550 nm with twin superconducting single-photon detectors," Appl. Phys. Lett. **89**, 241129 (2006).
7. R. J. Collins, R. H. Hadfield, V. Fernandez, S. W. Nam, and G. S. Buller, "Low timing jitter detector for gigahertz quantum key distribution," Electron. Lett. **43**, 180–182 (2007).
8. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121–3124 (1992).
9. 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**, 343–348 (2007).

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

10. K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” Phys. Rev. Lett. **89**, 037902 (2002).
11. C. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” Appl. Phys. Lett. **84**, 3762–3764 (2004).
12. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” New J. Phys. **11**, 075003 (2009).
13. D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, “Continuous high speed coherent one-way quantum key distribution,” Opt. Express **17**, 13326–13334 (2009).
14. S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, “2 GHz clock quantum key distribution over 260 km of standard telecom fiber,” Opt. Lett. **37**, 1008–1010 (2012).
15. H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Phys. Rev. Lett. **94**, 230504 (2005).
16. D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, “Practical long-distance quantum key distribution system using decoy levels,” New J. Phys. **11**, 045009 (2009).
17. Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, “Decoy-state quantum key distribution with polarized photons over 200 km,” Opt. Express **18**, 8587–8594 (2010).
18. T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, “Long-distance entanglement-based quantum key distribution over optical fiber,” Opt. Express **16**, 19118–19126 (2008).
19. A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, “Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization,” Opt. Express **16**, 11354–11360 (2008).
20. I. Choi, R. J. Young, and P. D. Townsend, “Quantum key distribution on a 10Gb/s WDM-PON,” Opt. Express **18**, 9600–9612 (2010).
21. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, “Field test of quantum key distribution in the Tokyo QKD Network,” Opt. Express **19**, 10387–10409 (2011).
22. P. J. Clarke, R. J. Collins, P. A. Hiskett, M. J. Garcia-Martinez, N. J. Krichel, A. McCarthy, M. G. Tanner, J. A. O’Connor, C. M. Natarajan, S. Miki, M. Sasaki, Z. Wang, M. Fujiwara, I. Rech, M. Ghioni, A. Gulinatti, R. H. Hadfield, P. D. Townsend, and G. S. Buller, “Analysis of detector performance in a gigahertz clock rate quantum key distribution system,” New J. Phys. **13**, 075008 (2011).
23. F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, “Detecting single infrared photons with 93% system efficiency,” Nat. Photonics **7**, 210–214 (2013).
24. F. Bussières, C. Clausen, A. Tiranov, B. Korzh, V. B. Verma, S. W. Nam, F. Marsili, A. Ferrier, P. Goldner, H. Herrmann, C. Silberhorn, W. Sohler, M. Afzelius, and N. Gisin, “Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory,” (2014). arXiv:1401.6958 [quant-ph].
25. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Continuous operation of high bit rate quantum key distribution,” Appl. Phys. Lett. **96**, 161102 (2010).
26. W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature **299**, 802–803 (1982).
27. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys. **81**, 1301 (2009).
28. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,” Phys. Rev. A **78**, 042333 (2008).
29. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” Nat. Photonics **4**, 686–689 (2010).
30. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Thermal blinding of gated detectors in quantum cryptography,” Opt. Express **18**, 27938–27954 (2010).
31. H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, “Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors,” New J. Phys. **13**, 073024 (2011).
32. M.-S. Jiang, S.-H. Sun, G.-Z. Tang, X.-C. Ma, C.-Y. Li, and L.-M. Liang, “Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems,” Phys. Rev. A **88**, 062335 (2013).
33. A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, “Laser damage helps the eavesdropper in quantum cryptography,” Phys. Rev. Lett. **112**, 070503 (2014).
34. L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, “Controlling a superconducting nanowire

single-photon detector using tailored bright illumination," New J. Phys. **13**, 113042 (2011).

35. M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, and M. Sasaki, "Characteristics of superconducting single photon detector in DPS-QKD system under bright illumination blinding attack," Opt. Express **21**, 6304–6312 (2013).
36. T. Honjo, M. Fujiwara, K. Shimizu, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Countermeasure against tailored bright illumination attack for DPS-QKD," Opt. Express **21**, 2667–2673 (2013).
37. M. Ejrnaes, R. Cristiano, O. Quaranta, S. Pagano, A. Gaggero, F. Mattioli, R. Leoni, B. Voronov, and G. Gol'tsman, "A cascade switching superconducting single photon detector," Appl. Phys. Lett. **91**, 262509 (2007).
38. F. Marsili, F. Najafi, E. Dauler, F. Bellei, X. L. Hu, M. Csete, R. J. Molnar, and K. K. Berggren, "Single-photon detectors based on ultranarrow superconducting nanowires," Nano Lett. **11**, 2048–2053 (2011).
39. M. G. Tanner, L. S. E. Alvarez, W. Jiang, R. J. Warburton, Z. H. Barber, and R. H. Hadfield, "A superconducting nanowire single photon detector on lithium niobate," Nanotechnology **23**, 505201 (2012).
40. R. M. Heath, M. G. Tanner, A. Casaburi, M. G. Webster, L. San Emeterio Alvarez, W. Jiang, Z. H. Barber, R. J. Warburton, and R. H. Hadfield, "Nano-optical observation of cascade switching in a parallel superconducting nanowire single photon detector," Appl. Phys. Lett. **104**, 063503 (2014).
41. M. Ejrnaes, A. Casaburi, R. Cristiano, O. Quaranta, S. Marchetti, N. Martucciello, S. Pagano, A. Gaggero, F. Mattioli, R. Leoni, P. Cavalier, and J.-C. Villégier, "Timing jitter of cascade switch superconducting nanowire single photon detectors," Appl. Phys. Lett. **95**, 132503 (2009).
42. M. G. Tanner, C. M. Natarajan, V. K. Pottapenjara, J. A. O'Connor, R. J. Warburton, R. H. Hadfield, B. Baek, S. Nam, S. N. Dorenbos, E. B. Ureña, T. Zijlstra, T. M. Klapwijk, and V. Zwiller, "Enhanced telecom wavelength single-photon detection with NbTiN superconducting nanowires on oxidized silicon," Appl. Phys. Lett. **96**, 221109 (2010).
43. R. H. Hadfield, A. J. Miller, S. W. Nam, R. L. Kautz, and R. E. Schwall, "Low-frequency phase locking in high-inductance superconducting nanowires," Appl. Phys. Lett. **87**, 203505 (2005).
44. J. A. O'Connor, M. G. Tanner, C. M. Natarajan, G. S. Buller, R. J. Warburton, S. Miki, Z. Wang, S. W. Nam, and R. H. Hadfield, "Spatial dependence of output pulse delay in a niobium nitride nanowire superconducting single-photon detector," Appl. Phys. Lett. **98**, 201116 (2011).
45. J. K. W. Yang, A. J. Kerman, E. A. Dauler, V. Anant, K. M. Rosfjord, and K. K. Berggren, "Modeling the electrical and thermal response of superconducting nanowire single-photon detectors," IEEE T. Appl. Supercon. **17**, 581–585 (2007).
46. F. Marsili, F. Najafi, C. Herder, and K. K. Berggren, "Electrothermal simulation of superconducting nanowire avalanche photodetectors," Appl. Phys. Lett. **98**, 093507 (2011).
47. V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Optic. **52**, 691–705 (2005).
48. V. Makarov, "Controlling passively quenched single photon detectors by bright light," New J. Phys. **11**, 065003 (2009).
49. L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," J. Mod. Opt. **58**, 680–685 (2011).
50. V. Burenkov, H. Xu, B. Qi, R. H. Hadfield, and H.-K. Lo, "Investigations of afterpulsing and detection efficiency recovery in superconducting nanowire single-photon detectors," J. Appl. Phys. **113**, 213102 (2013).
51. A. Kerckhoffs, "La cryptographie militaire," J. des Sciences Militaires **IX**, 5–38 (1883).
52. 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).
53. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
54. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
55. A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "A quantum key distribution system immune to detector attacks," (2012). arXiv:1204.0738v2 [quant-ph].
56. Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography," Appl. Phys. Lett. **98**, 231104 (2011).
57. L. Lydersen, V. Makarov, and J. Skaar, "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'," Appl. Phys. Lett. **99**, 196101 (2011).
58. Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Reply to "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'"," Appl. Phys. Lett. **99**, 196102 (2011).
59. M. Legré and G. Ribordy, "Apparatus and method for the detection of attacks taking control of the single photon detectors of a quantum cryptography apparatus by randomly changing their efficiency," intl. patent appl. WO 2012/046135 A2 (filed in 2010).
60. H. Terai, S. Miki, T. Yamashita, K. Makise, and Z. Wang, "Demonstration of single-flux-quantum readout operation for superconducting single-photon detectors," Appl. Phys. Lett. **97**, 112510 (2010).

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

1. Introduction

Quantum communication technologies offer information processing power having no analogues in the classical world. For example, quantum key distribution (QKD) [1] has been commercialised [2]; secret sharing, quantum teleportation [3], entanglement swapping, bit commitment, and blind quantum computation [4] have been demonstrated. To achieve quantum communications at high speed and over long distance, single-photon detectors with high timing resolution and low noise are essential. Superconducting nanowire single-photon detectors (SNSPDs) [5] achieve the best combination of these parameters at 1550 nm, the optimal wavelength for long distance transmission over optical fiber.

The first proof-of-principle demonstration using SNSPDs in QKD was carried out with a phase encoding system operating the Bennett-Brassard 1984 (BB84) protocol [1, 6]. A high bit rate, short wavelength ($\lambda = 850\,\mathrm{nm}$) demonstration was then reported based on the Bennett 1992 (B92) protocol with polarization encoding [7, 8]. A high bit rate long distance demonstration at $\lambda = 1550\,\mathrm{nm}$ was carried out at Stanford University [9] using the differential phase shift (DPS) QKD protocol [10]. This first QKD demonstration in excess of 200 km (40 dB transmission loss) was achieved using SNSPDs with 0.7% efficiency at 1550 nm, 10 Hz dark count rate and 60 ps full-width at half-magnitude (FWHM) jitter [9]. Record bit rates were also achieved at shorter distances, which was a significant improvement on the best QKD results achieved at that time with InGaAs single-photon avalanche photodiodes (SPADs) [11].

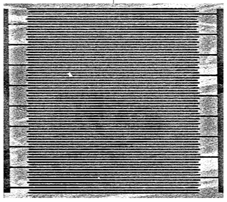
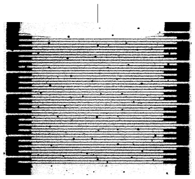
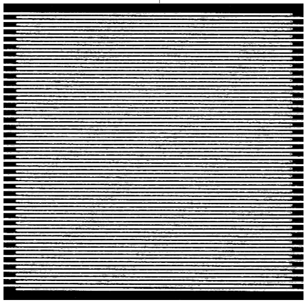
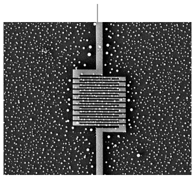
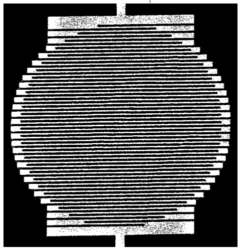
Since that study, many further QKD demonstrations have been reported using SNSPDs: the maximum range was extended to 250 km using low-loss fiber and implementing the coherent one-way (COW) protocol [12, 13], more recently extended to 260 km with DPS-QKD [14]; decoy-state protocols [15] have been demonstrated [16, 17]; entanglement-based QKD has been demonstrated over long distance [18]; SNSPDs have been implemented in QKD field trials in installed fiber networks [19–21]. A detailed comparison between SNSPDs and Si SPADs for short haul high bit rate QKD has also been published [22]. Since this time SNSPD technology has advanced rapidly [5] and near-unity efficiency coupled with low dark count rates is now achievable [23]. These new high-performance SNSPDs have recently been deployed in interfacing quantum networks with quantum memories via teleportation [24], and are likely to be employed in future QKD demonstrations. The 100-fold improvement in detection efficiency as compared to early demonstrations [9] in principle allows for 100 times more fiber attenuation, making QKD over up to 60 dB channel loss feasible. While the current record for highest QKD bit rate [25] has been achieved using SPADs, it is clear that SNSPDs are a vital technology in the advancement of fiber-based QKD systems and networks particularly with the advent of next generation SNSPDs with near-unity efficiency at telecom wavelengths [23].

Information security is an intrinsic feature of quantum communication protocols, guaranteed in principle by the underlying laws of physics [26, 27]. However, the limitations of components lead to vulnerability. Practical attacks breaking security of QKD have been proposed and successfully demonstrated, by exploiting imperfections and behavior of real hardware not accounted for in the theoretical treatment of security. Several of these attacks exploit imperfections of single-photon detectors, which have mostly been demonstrated on SPAD-based detectors [28–33]. It has been shown by Lydersen *et al.* [34] that an SNSPD also has exploitable imperfections, allowing bright-light blinding and deterministic control. A Japanese team has recently applied this technique to explore the vulnerability of DPS-QKD systems and test a countermeasure [35, 36]; however they have only investigated blinding of the detector but not optimisation and properties of the fake pulses.

Here we extend the basic technique of detector control by testing and demonstrating this vulnerability in several different SNSPD devices, using a realistic electronic bias and readout that has been employed in QKD demonstrations [6]. We demonstrate optimised on-demand

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

TABLE I. SNSPD devices tested, and their parameters.

Device number	1	2	3	4	5
Produced at	Cambridge	Cambridge	NICT	TU Delft	TU Delft
Substrate	Sapphire	Quartz	MgO	$\mathrm{SiO_2}$ layer on Si (simple optical cavity)	$\mathrm{SiO_2}$ layer on Si (simple optical cavity)
Nanowire material	NbN	NbN	NbN	NbTiN	NbTiN
Nanowire thickness, nm	8.8	8.8	4.2	6	6
Nanowire width, nm	70	100	100	100	80
Nanowire geometry	$9.5 \times 9.5\,\mu\mathrm{m}$, 17 sections in series each containing 4 parallel wires	$8 \times 8\,\mu\mathrm{m}$, 11 sections in series each containing 4 parallel wires	$15 \times 15\,\mu\mathrm{m}$ meander	$3 \times 3.5\,\mu\mathrm{m}$ meander	$\varnothing 11\,\mu\mathrm{m}$ meander
Scanning electron microscope image (contrast enhanced to emphasise nanowire geometry) 5 μm					
Critical current, μA[a]	65	27	21	66	7.5
Critical temperature, K	10.1	8.7	11.1	8.0	9.8
Minimum blinding power, dBm[a]	-9.65	-17.85	-17.35	-23.65	-25.07
Maximum blinding time τ_{recovery}, ns[a]	40	50	50	60	40

[a] Measured at the operating temperature of 3.5 K.

fake pulse generation. We also discuss and test non-ideal characteristics of the detector output during the fake pulse generation, and countermeasures to this attack. Although we have only tested stand-alone detectors, our findings reflect on the security of any QKD system that would employ them.

2. Experiment

We have tested five SNSPD devices, summarised in Table 1. The majority of data presented here was obtained from device 1. This detector is of the superconducting nanowire avalanche photon detector (SNAP) type with sections of nanowires connected in parallel [37–41]. This configuration is advantageous for reducing nanowire dimensions, in order to increase device efficiency while maintaining usable current levels in the detector and for reducing reset times for achieving higher count rates. This detector implementation is likely to be used in future high speed and detector efficiency QKD systems. However for completeness a representative range of detector types were tested. These included traditional meander-patterned devices on a variety of substrates, such as those used in several practical demonstrations of QKD (device 3) [21, 22]. Next-generation optical cavity enhanced detectors were included as well (devices 4

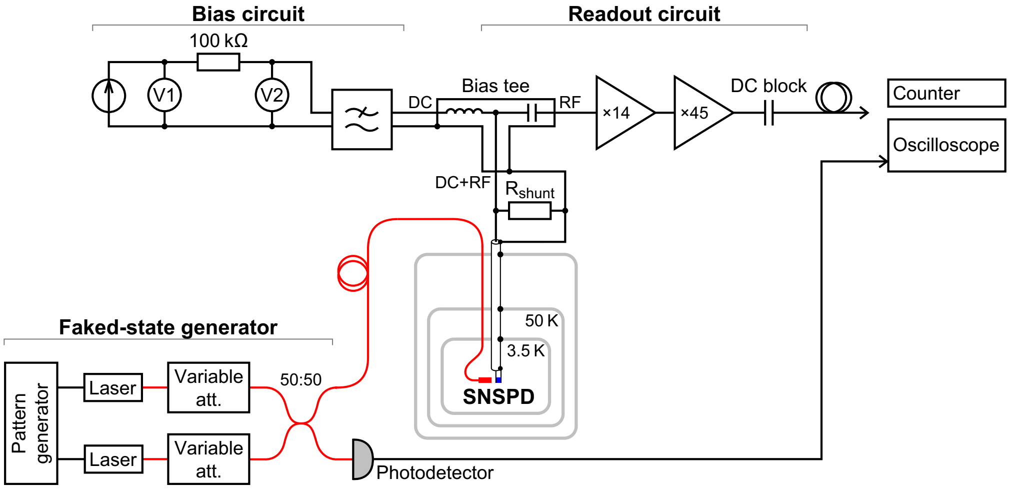


Fig. 1. Experimental setup. SNSPD is cooled to 3.5 K in a closed-cycle refrigerator, custom designed around a Cryomech PT-403 pulse tube cold head, and connected to room-temperature electronics via ~ 1 m long $50\,\Omega$ coaxial cable. The electronics consists of the bias and readout circuits. The bias circuit is composed of a battery-powered low-noise voltage source (Stanford Research Systems SIM928), $100\,\mathrm{k}\Omega$ resistor converting voltage into bias current, two voltmeters (Stanford Research Systems SIM970), and low-pass filter (Mini-Circuits BLP-1.9+). The bias current is applied to the SNSPD via the direct-current (DC) port of a bias tee (Picosecond Pulse Labs 5575A-104, 10 kHz–12 GHz radio-frequency (RF) port bandwidth). The readout circuit uses two radio-frequency amplifiers (RF Bay LNA-580, 23 dB gain 10–580 MHz bandwidth, and RF Bay LNA-1000, 33 dB gain 10 MHz–1 GHz bandwidth), and a DC block (Mini-Circuits BLK-18-S+, 10 MHz–18 GHz bandwidth). The pulses are registered by either a counter (Agilent 53131A) or an oscilloscope (Agilent Infiniium DSO80804A, 8 GHz 40 Gsamples/s). The SNSPD is illuminated via a single-mode fiber (Corning SMF28e) shown in red, by light formed by the faked-state generator. The latter consists of a pulse pattern generator (Agilent 81110A), two 1550 nm semiconductor laser diodes (one Thorlabs LPS-1550-FC and one Thorlabs LPSC-1550-FC), two optical variable attenuators (Hewlett-Packard 8156A) and a 50:50 ratio fiber beamsplitter providing two identical optical outputs. One output is connected to the SNSPD, while the other is monitored with a classical photodetector (Thorlabs DET01CFC, DC–1.2 GHz bandwidth).

& 5) [42], which are now becoming available for QKD implementations. The same blinding attack technique was successful with all detector types.

Our experimental setup (Fig. 1) represents a typical detector configuration used in QKD experiments [6]. The SNSPD device is biased at about 0.9 of its critical current (specific device properties such as critical current at the operating temperature are listed in Table 1). The bias is applied by a battery-powered low-noise current source connected via a bias tee. The important feature of the scheme is the presence of a shunt resistor R_{shunt} that prevents latching (typically a $50\,\Omega$ resistor) [43]. This resistor creates a low-impedance mismatch point ~ 1 m away from the SNSPD along the $50\,\Omega$ coaxial radio-frequency (RF) cable. A reverse-polarity pulse reflected from this impedance mismatch reaches the SNSPD about 10 ns after hotspot formation, and lowers the voltage across the device. If the hotspot has failed to dissipate and persists by Joule self-heating, this reflected pulse can remove electrical power from it aiding reset from the latched state. On longer timescales it is important that the shunt resistance is much lower than the SNSPD hotspot resistance. The shunt resistor provides an alternate current path, re-

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

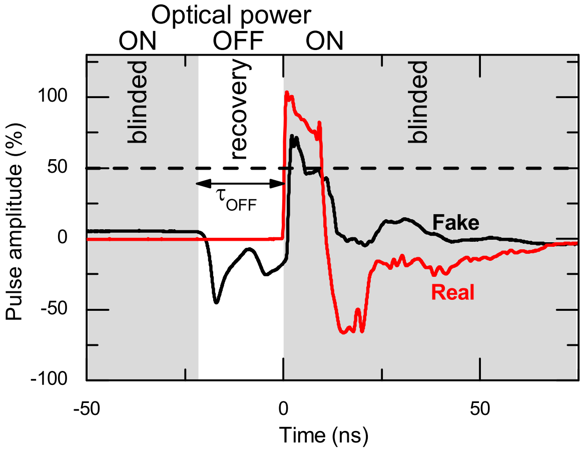


Fig. 2. Output pulses from the experimental setup described in Fig. 1 under normal single-photon illumination (red trace) and under bright-light illumination manipulating the detector (black trace). Laser illumination for the blinded case is illustrated by the plot shading. Time $t = 0$ns is the point at which the fake output pulse is triggered.

ducing current flow through the detector allowing cooling back to the superconducting state. The latter recovery mechanism is of particular importance to the detector blinding attack described in this paper. In this circuit configuration, SNSPD can be reliably operated at a higher bias current and higher photon detection efficiency than in the configuration without R_{shunt}. The pulse readout circuit consists of AC-coupled amplifiers with combined gain of 56 dB and 10–580 MHz frequency range. The detector output signal is observed with an electronic counter and an oscilloscope. The SNSPD is illuminated via single-mode fiber connected to the output of a faked-state generator. The faked-state generator allows the formation of arbitrary illumination diagrams with two distinct optical power levels at the SNSPD, in addition to zero power level. This is achieved with a pulse pattern generator powering two 1550 nm laser diodes, followed by optical variable attenuators to set the power levels. The output of the faked-state generator simulates illumination diagrams that the SNSPD would receive if it were a part of a QKD system under attack [34].

A typical output pulse from this setup is shown in Fig. 2, triggered by the incidence of a single photon. The normal character of an SNSPD output pulse includes a sharp leading edge as the detector becomes resistive and the current is forced out, followed by a slower recovery as the current returns to the detector. The shape of the observed recovery signal is highly dependent on amplifier bandwidths and reflections from components (such as the shunt resistor used in this setup). Note that this oscilloscope trace is not an accurate representation of the current flow returning to the device. The critical part of the pulse is the sharp clean leading edge on which counting electronics is normally triggered, providing the advantageous timing properties of SNSPDs. The observed leading edge is also dependent on amplifier bandwidth and hotspot resistance [44]. Hotspot growth time (typically < 100 ps [45, 46]) is normally short in comparison to the observed pulse rise time. In our experimental setup, the latter is limited by the first 580 MHz bandwidth amplifier (Fig. 1).

Lydersen *et al.* considered artificially generating pulses in SNSPDs through two methods [34]. The first involved latching the detector into the resistive state, through a short bright-light illumination, from which the detector does not recover. Fake detector pulses were generated through subsequent bright pulses causing variation of the device resistance. However, this at-

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

tack is effectively defeated by the inclusion of a shunt resistor [43] (or other reset circuit) as implemented in our standard experimental setup (Fig. 1), and also in some QKD demonstrations [6] in order to allow stable long-term detector operation. In this paper we describe the extension of the second method put forward by Lydersen *et al.* of blinding the detectors to incoming single photons through continuous bright-light illumination (of the order of 1 to 100 μW in this study depending on individual SNSPD characteristics). We find that with careful control it is possible to generate fake detector output signals reliably on-demand with timing properties better than in the single-photon case.

3. Detector control

3.1. Applicability to different QKD schemes

Since our testing was performed on a stand-alone detector, we need to briefly address the question how this applies to hacking a complete QKD system. In a detector control attack, Eve performs an intercept-resend in the transmission line. She uses a replica of Bob's setup to detect all quantum states emitted from Alice, then generates and sends bright-light faked states to Bob that attempt to replicate Eve's detection results in Bob's detectors [47, 48]. Note that Bob has two or more detectors. The simplest version of this attack requires that Eve can specify deterministically which detector in Bob clicks and when it clicks, at her will. To do so she needs to form bright-light pattern at the target detector that causes it to click with 100% probability, while all other detectors in Bob receive bright-light pattern that keeps them silent. The hacking method employed by Eve, and the sucess thereof, depends on the optical layout in Bob. For the purpose of the following analysis, we can broadly classify Bob's optical schemes into three categories.

The first category contains passive measurement schemes in which Eve can, by choosing appropriate polarization or phase of bright light, reduce light power at a selected detector by 20 dB (100 times) or more for an arbitrary time period, while keeping the other detectors illuminated [48]. Examples of such schemes are passive-basis-choice BB84 protocol and DPS-QKD protocol. The 20 dB figure is a typical extinction ratio of Bob's polarization- or phase-selective component, such as a polarizing beamsplitter or Mach-Zehnder interferometer. While the power at the selected detector is reduced greatly, other detectors in Bob may receive excess power in the form of a surge of up to 3 dB (a twofold increase in power) [34, 48]. Most QKD schemes so far tested with SNSPDs are of this type [7, 9, 14, 17, 18, 20, 22]. We thus base our stand-alone detector testing on a control diagram that alternates between 20 dB optical power drop and 3 dB surge around a steady blinding power level, as will be detailed in Section 3.2.

A second smaller category contains schemes where Bob uses a randomly-driven modulator for active basis choice in BB84 protocol [6, 16]. In these schemes Eve can drop power at the target detector by 20 dB conditional on a specific basis choice by Bob, while for other basis choices the power at all detectors will stay around the blinding level [29, 48]. The time duration for which Bob keeps one choice of basis applied to his modulator presents an additional constraint on Eve. If this time is greater than the time duration for which Eve needs to reduce the power delivered to the target detector, then her attack is in essence equivalent to the previous category. However in high-speed QKD implementations this condition may not hold and Eve's life becomes more complicated. In the latter case the devil is in the details: Eve may or may not be able to hack, depending on the exact particulars of the technical implementation. We do not consider the latter case, because there is no stable reference QKD implementation that we could obtain and examine in detail. Unfortunately all QKD implementations using SNSPDs have to date been laboratory prototypes – no complete commercial system yet exists.

A third, also smaller, category contains certain time-bin encoding schemes in which one or more detectors are essentially connected straight to the communication line and are not selective on any light parameter. These include implementations of COW protocol [12] and time-bin-encoded BB84 protocol [19]. In these schemes Eve will again be constrained by the exact details of the technical implementation (among other details, by the splitting ratio of the asymmetric beamsplitter [49]), and will have to analyse detector behavior beyond the level tested in this paper.

Looking beyond the optical layout in Bob, the readout circuitry can also affect Eve's attack strategy. The discriminator circuits used to convert the analog pulse shown in Fig. 2 into a digital detection signal vary, and are never described in sufficient detail in papers about QKD implementations. For example, it is usually not stated at what level the discriminator threshold is set. SNSPD pulse shape has the steepest and cleanest gradient mid-way through the leading edge, making 50% of the output peak height a sensible robust choice of discriminator level for-low jitter QKD operation. We thus assume in our testing that Bob uses a fast constant-level discriminator with threshold set at 50% of the single-photon pulse height. As will be obvious below, the attack works in a range of discriminator levels centered around 50%, and Section 3.3 discusses how fake pulse height can be varied during attack optimisation.

3.2. On-demand fake pulse generation

When illuminated with a bright 'blinding' pulse of light, the detector becomes resistive over a larger area than the single hotspot generated by single photon absorption. In the single-photon detection case the resistive region, or hotspot, grows due to Joule heating with the energy dependent upon I^2L, where I is the bias current and L is the kinetic inductance of the detector. Once the bias current is shunted out from the detector, the hotspot dissipates on a time scale determined by the rethermalisation of the nanowire with the substrate. This mechanism has been modelled in detail by others [45, 46].

In the bright-light case, we suggest that the resistive region is maintained through the direct absorption of the incident laser power in excess of the rethermalisation or cooling power of the SNSPD environment. It is interesting to note that very approximately, given bias current of the order of $10\,\mu$A, kinetic inductance of $1\,\mu$H and hotspot formation time of $100\,$ps, the power dissipated during hotspot formation is $\sim 1\,\mu$W. This power is sufficient to cause the hotspot to grow rather than rethermalise. This agrees well with the blinding powers required to maintain the devices in a resistive state ($> 1\,\mu$W or $-30\,$dBm, see Table 1).

Under blinding illumination, current is diverted from the detector causing an output pulse [see pulse at $t \sim -200\,$ns in Fig. 3(b) and 3(e)]. If the bright illumination continues, the detector remains in the resistive state and is no longer sensitive to incident photons. However, if the bright illumination is stopped (or its power is decreased sufficiently, 20 dB attenuation is shown to be sufficient in Fig. 3) for a short period of time (e.g., $< 50\,$ns), the nanowire rethermalises. It then once more becomes superconducting, and the current starts to return to the detector at a rate defined by the superconducting kinetic inductance of the SNSPD L and the circuit resistance. Recovery of the SNSPD after the blinding attack is somewhat different than recovery from single photon detection. Excess laser power has been absorbed into the detector, driving a large area resistive and causing a local rise in temperature. The need to rethermalise in addition to the normal return of current to the SNSPD extends recovery timescales dependent on the excess blinding energy deposited (or timescale of the attack). If enough of the bias current was allowed to return to the detector, it would once more become single-photon sensitive (after time τ_{recovery}), and would also exhibit dark counts. Note that it does not require the full bias current to have returned to the nanowire before the detector can exhibit a photoresponse or produce dark counts [23, 50]. However, if the bright illumination is re-applied before this time, after $\tau_{\text{OFF}} < \tau_{\text{recovery}}$ optimised experimentally in this work, the proportion of the current that had already returned to the detector is again forced out as the nanowire returns to the resistive

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

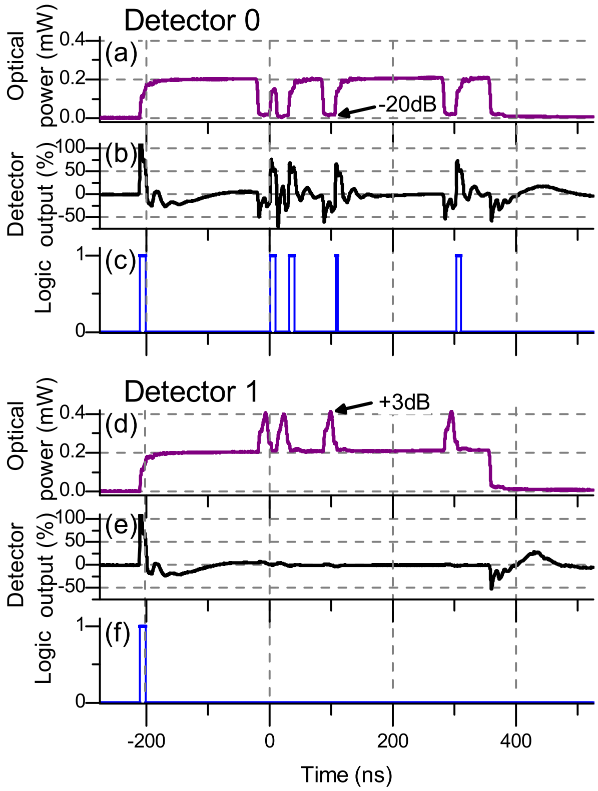


Fig. 3. Simulated control diagrams two detectors would receive inside Bob whose scheme allows to redistribute optical power between the detectors (i.e., measurement scheme of the first category in Section 3.1). Detectors are controlled through blinding with a bright laser pulse at time $t = -200\,$ns, followed by variation of the blinding laser power by $-20\,$dB on detector 0, and corresponding variation of $+3\,$dB on detector 1. Optical power at both detectors during the attack is shown in oscilloscope traces (a) and (d), while analog detector outputs are shown in oscilloscope traces (b) and (e). Corresponding logic pulses obtained by passing the analog signal through a 50% fixed-threshold discriminator are shown in (c) and (f).

state. This elicits another controlled fake output pulse from the detector while maintaining the SNSPD in a 'blinded' state. An example of this fake pulse is shown in Fig. 2. This is the basis of the detector attack described in this paper.

In the manner described above, an attacker can blind an SNSPD and elicit 'fake' output pulses on-demand. This is shown explicitly in the top half of Fig. 3. An initial output pulse occurs when the blinding illumination is initiated at $t \sim -200\,$ns, and subsequent controlled pulses are generated on-demand through brief reductions in the blinding illumination for time $\tau_{\mathrm{OFF}} < \tau_{\mathrm{recovery}}$ (in this case $\tau_{\mathrm{OFF}} = 20\,$ns). Once the control diagram was optimised, a fake output pulse occurred on every observed attempt in the authors' experiment with apparent 100% probability.

In order to achieve successful manipulation of the variety of SNSPDs tested in this work, some variation of parameters was needed, primarily blinding power and τ_{recovery} (see Table 1).

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

Devices were biased and operated as the authors would normally use them in experiments; only blinding attack parameters were optimised. While new generations of SNSPDs with near-unity detection efficiency using new materials such as tungsten silicide [23] were not tested in this study, their operating principle is the same. Variations in thermal and electrical properties are likely to require similar optimisation of the blinding parameters, but no change in the principle of the attack. In practice it may seem impractical to determine the correct blinding parameters to attack a system. However we assume, in accordance with Kerckhoffs' principle [51] (a cryptosystem should be secure even if everything about the system except the key is public knowledge), that the attacker knows all details of the devices, settings and protocols used. In practice, as detectors and commercial QKD systems develop, it is likely the detectors will have highly repeatable characteristics. It then becomes realistic to fully dismantle and analyse a sample of a commercial product to obtain starting values of these parameters in advance of attacking a QKD implementation. The attack may then begin to be applied intermittently while analysing the public communication between Alice and Bob and fine-tuning attack parameters [47, 52]. Eve would subsequently switch over to continuous attack with real-time adjustment of parameters, if necessary.

3.3. Pulse and recovery characteristics

The characteristics of the fake pulse seen in Fig. 2 are qualitatively similar to those of the real pulse: a sharp leading edge followed by a slow recovery. Amplitude of the fake pulse is reduced, because only a fraction of the full device current has returned to the detector before the fake pulse is triggered. If a longer pause is left before resuming the full blinding laser power, the fake pulse amplitude is increased. However, with pauses of duration closely approaching τ_{recovery}, there is a finite probability of a count occurring during the recovery from the blinded state, which is undesirable for full detector control. For the fake pulse outputs demonstrated in this paper, τ_{OFF} was kept sufficiently below τ_{recovery} (in this case $\tau_{\text{OFF}} = 20\,\text{ns}$). Then counts due to recovery from the blinded state did not occur during the attack, instead the fake pulse was generated returning the detector to the blinded state. This was confirmed in the good jitter characteristics of the fake pulses, discussed in Section 3.4. Fake pulse amplitude can be increased at the cost of a finite probability of a detector pulse occurring before the intended fake pulse.

However, counts during recovery from the blinded state are common if the blinding attack is stopped (e.g., $t > 400\,\text{ns}$ in Fig. 3), occurring with a probability 10–16% when the detector is blinded for 1–10 μs, see Fig. 4. The recovery of the detector from the blinded state is different from normal single-photon detection recovery (which can also stimulate afterpulsing [50]), as in the blinded case the detector must rethermalise to the base temperature before the system fully returns to normal operation. If carefully applied, the blinding power need not heat the detector excessively and the thermalisation time only slightly extends the recovery, which is still dominated by the current return time to the detector. However the dynamics of this recovery are affected by the temperature from which the SNSPD is rethermalising, hence the dependence of afterpulsing probability on blinding duty cycle as in Fig. 4. An additional contribution to afterpulses may be single-photon detection of photons delayed in the optical scheme via multiple back-and-forth reflections of the bright blinding pulse. The observed output signal during recovery from the blinded state is most clearly seen in Fig. 3(e) after $t = 350\,\text{ns}$.

The presence of afterpulses should not stop the attack. In Fig. 3(b) at $t = 0\,\text{ns}$ two fake pulses are generated at a repetition period of 30 ns. After the first pulse, 10 ns of bright light is required to return the detector to the blinded state before a second fake pulse can be generated with $\tau_{\text{OFF}} = 20\,\text{ns}$. In this manner, fake pulses can be generated at a repetition rate of 33 MHz. While these parameters vary between detectors (see last row in Table 1), by the very nature of the attack discussed above τ_{OFF} is kept well below τ_{recovery} (in this case at 50%). In normal QKD

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

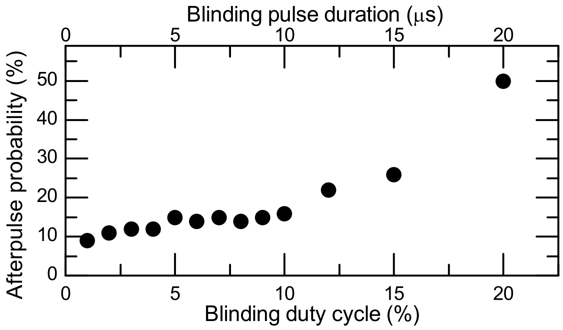


Fig. 4. Probability of an afterpulse occurring when the blinding pulse is stopped, dependent on the fraction of the time the detector is illuminated by the blinding pulse. Blinding attack repetition rate was kept constant at 10 kHz, while blinding pulse duration was varied. Since many fake pulses would be generated during each blinding cycle, fake detection rate would be much higher than 10 kHz.

operation, the maximum single-photon detection rate would be $1/\tau_{\text{recovery}}$ *with a unity efficiency detector.* The hacker can match or better this rate, with significant further gains available when compared to a non-unity efficiency single photon detector in Bob.

For the detector studied in detail in this paper, if kept under Eve's control for 10 µs every 100 µs, an afterpulse will occur 16% of the time (Fig. 4). In each 10 µs cycle the hacker can generate 333 fake pulses, or if matching the maximum single photon detection rate only 250 fake pulses, with an average of 0.16 afterpulses. As such, afterpulses per fake pulse occur at a rate of 0.06%, adding only a small contribution to the error rate.

3.4. Jitter

For good detector control, the timing jitter of the fake electrical output pulses must be comparable or better than that of the real response. This is shown in Fig. 5. As long as the pause in the blinding pulse is kept below τ_{recovery}, the jitter achieved is as good or better than for single-photon response, for all detectors tested. While normal SNSPDs suffer from some variation in timing response over the detector area due to varying hotspot resistance of $\sim 1\,\text{k}\Omega$ [44], in the

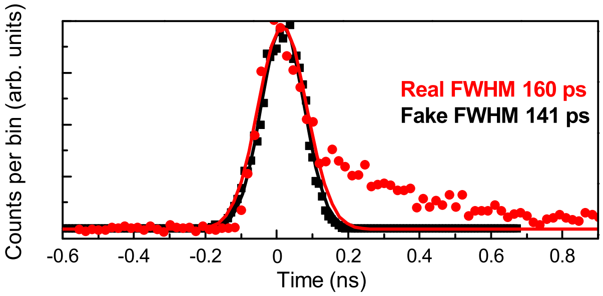


Fig. 5. Comparison of timing jitter measured in the experimental setup described in Fig. 1, for device 1. Timing distribution due to single-photon illumination (red circles) and manipulation through bright-light illumination (black squares) is shown, together with Gaussian fits. FWHM time widths are 160 and 141 ps, respectively. Jitter is measured at a fixed threshold level set at 50% of the amplitude of a single-photon detection pulse.

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

case of the blinding attack the SNSPD switches to a very high resistance every time, giving a sharper leading edge to the pulse and improved timing jitter.

Additionally, for the real single-photon case shown in Fig. 5 a tail is observed on the jitter histogram, characteristic of the avalanche process for parallel wire (SNAP) detectors [37–41] (devices 1 & 2). The tail is not observed for the standard meander SNSPDs (devices 3–5). This tail is not present in the fake jitter histogram for any of the five devices, as the higher power of the blinding pulse ensures immediate cascade of the detector into the resistive state. Improved FWHM characteristics of the faked detector response for all detectors tested offer Eve some leeway in her hacking attack: for example, improved error rate here may be used to compensate for any increased errors due to afterpulses.

3.5. Summary

Experimental results obtained with simulated control diagrams shown in Fig. 3 show that the detectors are successfully manipulated with only 20 dB variation in blinding power. These diagrams should be fully reproducible when attacking the majority of QKD schemes using SNSPDs [7, 9, 14, 17, 18, 20, 22], making these schemes vulnerable to the detector control attack. The control diagrams can be adapted to minor variations between individual detectors in the QKD system, such as different values of τ_{recovery} and minimum blinding power. For the remaining QKD schemes [6, 12, 16, 19] these control diagrams may not directly apply, yet should be good starting point for refining the attack. For the latter schemes, detailed investigation of the implementation details and a tailored advanced attack tactics would be required. For example, for an active basis choice scheme that switches measurement bases faster than τ_{recovery}, Eve could try to send faked states tailored to certain sequences of bases. We did not investigate these schemes owing to the lack of a stable reference implementation such as a commercial QKD system that uses SNSPDs.

4. Countermeasures

An attack such as that described in this paper will always be dependent on the exact configuration of the QKD system. This paper attempts to demonstrate that vulnerability to attack exists in stand-alone SNSPDs of all configurations available to the authors, with only minor adjustment of parameters (see last two rows in Table 1). A further investigation would have to target a complete QKD system containing SNSPDs. This would be a level of effort outside the scope of this paper, especially as no commercial QKD systems using SNSPDs are yet available as a benchmark. However, it is worth considering countermeasures that may remove this vulnerability in the future.

There are two main forms of countermeasure available to eliminate the security loophole demonstrated here. The preferred action is to include the equipment imperfections in the security model, as for example is done in the measurement-device-independent QKD scheme [53–55] where the detector system is moved outside of the security proof. However, in practice, patches to rule out already demonstrated attacks on existing systems are often considered first, while not offering any guarantee that the vulnerability can be eliminated [56–59]. Below we give some ideas for these latter kind of ‘band-aid’ countermeasures applicable to the attack described here.

As mentioned in section 2, the inclusion of R_{shunt} in the experimental design shown in Fig. 1 offers a countermeasure to the first attack described by Lydersen *et al.* [34]. Alternate reset circuits including systems which actively reset the bias to avoid detector latching may have significant implications for the operation of the attack and may form the basis of a countermeasure. It may be that such active reset circuits are once again vulnerable to the first type of attack described by Lydersen *et al.* [34]. Due to lack of availability to the authors, such active reset

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

circuits have not been investigated in this work.

For the passive reset circuit described here, a countermeasure uses the feature that if the detector under blinding attack from bright-light illumination is under DC electrical monitoring, a small increase in the average resistance can be observed, limited by R_{shunt}. This manifests itself as a measurable average voltage drop across the DC bias port (measured by voltmeter V2 in Fig. 1), dependent on the duty cycle of the blinding attack. The reading on V2 increased linearly from 0.2 mV to 0.5 mV with blinding duty cycle varying from 0 to 50%. This is at the limit of the resolution of the standard voltmeter used here. The fractional change in measured resistance was slight in this demonstration especially at short blinding pulse duration (or blinding duty cycle). It can be imagined that more sensitive device monitoring of the correct bandwidth may enable easier detection of attacks that put the detector into a resistive state for a greater time than expected in normal operation. However, it should be noted that in high bit rate QKD the detector will be running at close to its maximum count rate. After each count, during detector recovery, a finite resistance would also be measured on V2. The wise hacker injecting high bit rate fake detector pulses will be aware of this and may be able to keep the blinding duty cycle low, keeping variation on V2 comparable to that caused by high bit rate QKD. It can be imagined that attacks may be limited to short periods of detector blinding.

A further countermeasure could be implemented as follows: The shape of the fake output pulses in this attack are highly dependent on the amplifiers used in the system. The setup used here is the standard arrangement employed in the majority of the authors' work. Real and fake pulses demonstrated here have the same important features (see Fig. 2), suitable for triggering a discriminator in a QKD system. However, we also tested other configurations of amplifiers. The leading edge of the fake pulse is maintained with the range of amplifiers tested. However, if DC-coupled amplifiers are used (instead of the AC-coupled standard amplifier chain in Fig. 1 that has 10 MHz low frequency cut-off), a different characteristic is seen. While the detector is in the blinded state, a constant output level is observed, only relaxing during the recovery phase. A pulse is still observed when the detector is switched to the blinding state, but the recovery does not match that of a real pulse. This would still be suitable for triggering many types of discriminators. The situation may be further complicated by the use of cryogenic amplifiers, or complete superconducting readout circuits [60] currently being developed. If a fast analog-to-digital converter (ADC) is used after the analog electronics instead of a simple threshold discriminator, it may be possible to distinguish real and fake pulses via more detailed automated analysis of the signal shape.

Further countermeasures of this type may also be possible, trying to distinguish distorted pulse shape and other abnormalities. However the authors believe that the type of attack described here is less dependent on the precise electrical circuit than the latched-state attack originally described by Lydersen *et al.* [34], and could be developed further by potential hackers in response to simple countermeasures.

5. Conclusion

In this paper, we have demonstrated further vulnerabilities in SNSPDs used in QKD systems. The purpose of this study has been to demonstrate the detailed operation of an attack on SNSPDs and moreover to consider the weaknesses of such an attack. Although hacking of a real QKD system has not been demonstrated, this study nevertheless provides an important signposting for future QKD system development. This bright-light blinding and control has been successfully demonstrated on a range of currently available SNSPD devices of different types on a variety of substrates. The attack has been shown to produce fake pulses and pulse trains on-demand with timing characteristics better than the detector's normal response. It has been shown that for many QKD schemes, multiple detectors in Bob could be controlled indi-

#204736 - $15.00 USD Received 14 Jan 2014; revised 5 Mar 2014; accepted 5 Mar 2014; published 14 Mar 2014

vidually. As such, it is suggested that careful consideration of the full QKD system and security model including detectors is needed in the development of commercial apparatus, before robust security claims can be made.

Acknowledgments

The authors thank L. San Emerito Alverez, W. Jiang and Z. H. Barber at the University of Cambridge, UK, S. Miki, Z. Wang and M. Sasaki at NICT, Japan, and S. N. Dorenbos and V. Zwiller at TU Delft, Netherlands for supplying devices. V.M. thanks Industry Canada for support. R.H.H. acknowledges a Royal Society University Research Fellowship. R.H.H. and M.G.T. acknowledge support from the UK Engineering and Physical Sciences Research Council (EPSRC grants EP/F048041/1, EP/G022151/1 and EP/J007544/1).