Recent peer-reviewed quantum-attacks completely cracking existing quantum communicators by utilizing the physical non-idealities of their building elements. This is called quantum hacking.

Source: Science Citation Index

Record 1 of 14
Title: **Full-field implementation of a perfect eavesdropper on a quantum cryptography system**
Author(s): Gerhardt, I (Gerhardt, Ilja); Liu, Q (Liu, Qin); Lamas-Linares, A (Lamas-Linares, Anta); Skaar, J (Skaar, Johannes); Kurtsiefer, C (Kurtsiefer, Christian); Makarov, V (Makarov, Vadim)
Source: NATURE COMMUNICATIONS Volume: 2 Article Number: 349 DOI: 10.1038/ncomms1348 Published: JUN 2011
Abstract: Quantum key distribution (QKD) allows two remote parties to grow a shared secret key. Its security is founded on the principles of quantum mechanics, but in reality it significantly relies on the physical implementation. Technological imperfections of QKD systems have been previously explored, but no attack on an established QKD connection has been realized so far. Here we show the first full-field implementation of a complete attack on a running QKD connection. An installed eavesdropper obtains the entire 'secret' key, while none of the parameters monitored by the legitimate parties indicate a security breach. This confirms that non-idealities in physical implementations of QKD can be fully practically exploitable, and must be given increased scrutiny if quantum cryptography is to become highly secure.

Record 2 of 14
Title: **Hacking commercial quantum cryptography systems by tailored bright illumination**
Author(s): Lydersen, L (Lydersen, Lars); Wiechers, C (Wiechers, Carlos); Wittmann, C (Wittmann, Christoffer); Elser, D (Elser, Dominique); Skaar, J (Skaar, Johannes); Makarov, V (Makarov, Vadim)
Source: NATURE PHOTONICS Volume: 4 Issue: 10 Pages: 686-689 DOI: 10.1038/NPHOTON.2010.214 Published: OCT 2010
Abstract: The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics(1-4). So-called quantum key distribution (QKD) implementations always rely on detectors to measure the relevant quantum property of single photons(5). Here we demonstrate experimentally that the detectors in two commercially available QKD systems can be fully remote-controlled using specially tailored bright illumination. This makes it possible to tracelessly acquire the full secret key; we propose an eavesdropping apparatus built from off-the-shelf components. The loophole is likely to be present in most QKD systems using avalanche photodiodes to detect single photons. We believe that our findings are crucial for strengthening the security of practical QKD, by identifying and patching technological deficiencies.

Record 3 of 14
Title: **Experimentally Faking the Violation of Bell's Inequalities**
Author(s): Gerhardt, I (Gerhardt, Ilja); Liu, Q (Liu, Qin); Lamas-Linares, A (Lamas-Linares, Antia); Skaar, J (Skaar, Johannes); Scarani, V (Scarani, Valerio); Makarov, V (Makarov, Vadim); Kurtsiefer, C (Kurtsiefer, Christian)
Source: PHYSICAL REVIEW LETTERS Volume: 107 Issue: 17 Article Number: 170404 DOI: 10.1103/PhysRevLett.107.170404 Published: OCT 20 2011
Abstract: Entanglement witnesses such as Bell inequalities are frequently used to prove the nonclassicality of a light source and its suitability for further tasks. By demonstrating Bell inequality violations using classical light in common experimental arrangements, we highlight why strict locality and efficiency conditions are not optional, particularly in security-related scenarios.

Record 4 of 14
Title: **Fakes states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols**
Author(s): Makarov, V (Makarov, V.); Skaar, J (Skaar, J.)

Source: QUANTUM INFORMATION & COMPUTATION Volume: 8 Issue: 6-7 Pages: 622-635 Published: JUL 2008
Abstract: In quantum cryptosystems, variations in detector efficiency can be exploited to stage a successful attack. This happens when the efficiencies of Bob's two detectors are different functions of a control parameter accessible to Eve (e.g., timing of the incoming pulses). It has previously been shown that the Bennett-Brassard 1984 (BB84) protocol is vulnerable to this attack. In this paper, we show that several other protocols and encodings may also be vulnerable. We consider a faked states attack in the case of a partial efficiency mismatch on the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocol, and derive the quantum bit error rate as a function of detector efficiencies. Additionally, it is shown how faked states can in principle be constructed for quantum cryptosystems that use aphase-time encoding, the differential phase shift keying (DPSK) and the Ekert protocols.

Record 5 of 14
Title: **After-gate attack on a quantum cryptosystem**
Author(s): Wiechers, C (Wiechers, C.); Lydersen, L (Lydersen, L.); Wittmann, C (Wittmann, C.); Elser, D (Elser, D.); Skaar, J (Skaar, J.); Marquardt, C (Marquardt, Ch); Makarov, V (Makarov, V.); Leuchs, G (Leuchs, G.)
Source: NEW JOURNAL OF PHYSICS Volume: 13 Article Number: 013043 DOI: 10.1088/1367-2630/13/1/013043 Published: JAN 2011
Abstract: We present a method to control the detection events in quantum key distribution systems that use gated single-photon detectors. We employ bright pulses as faked states, timed to arrive at the avalanche photodiodes outside the activation time. The attack can remain unnoticed, since the faked states do not increase the error rate per se. This allows for an intercept-resend attack, where an eavesdropper transfers her detection events to the legitimate receiver without causing any errors. As a side effect, afterpulses, originating from accumulated charge carriers in the detectors, increase the error rate. We have experimentally tested detectors of the system id3110 (Clavis2) from ID Quantique. We identify the parameter regime in which the attack is feasible despite the side effect. Furthermore, we outline how simple modifications in the implementation can make the device immune to this attack.

Record 6 of 14
Title: **Thermal blinding of gated detectors in quantum cryptography**
Author(s): Lydersen, L (Lydersen, Lars); Wiechers, C (Wiechers, Carlos); Wittmann, C (Wittmann, Christoffer); Elser, D (Elser, Dominique); Skaar, J (Skaar, Johannes); Makarov, V (Makarov, Vadim)
Source: OPTICS EXPRESS Volume: 18 Issue: 26 Pages: 27938-27954 DOI: 10.1364/OE.18.027938 Published: DEC 20 2010
Abstract: It has previously been shown that the gated detectors of two commercially available quantum key distribution (QKD) systems are blindable and controllable by an eavesdropper using continuous-wave illumination and short bright trigger pulses, manipulating voltages in the circuit [Nat. Photonics 4, 686 (2010)]. This allows for an attack eavesdropping the full raw and secret key without increasing the quantum bit error rate (QBER). Here we show how thermal effects in detectors under bright illumination can lead to the same outcome. We demonstrate that the detectors in a commercial QKD system Clavis2 can be blinded by heating the avalanche photo diodes (APDs) using bright illumination, so-called thermal blinding. Further, the detectors can be triggered using short bright pulses once they are blind. For systems with pauses between packet transmission such as the plug-and-play systems, thermal inertia enables Eve to apply the bright blinding illumination before eavesdropping, making her more difficult to catch.

Record 7 of 14
Title: **Device Calibration Impacts Security of Quantum Key Distribution**
Author(s): Jain, N (Jain, Nitin); Wittmann, C (Wittmann, Christoffer); Lydersen, L (Lydersen, Lars); Wiechers, C (Wiechers, Carlos); Elser, D (Elser, Dominique); Marquardt, C (Marquardt, Christoph); Makarov, V (Makarov, Vadim); Leuchs, G (Leuchs, Gerd)
Source: PHYSICAL REVIEW LETTERS Volume: 107 Issue: 11 Article Number: 110501 DOI: 10.1103/PhysRevLett.107.110501 Published: SEP 9 2011

Abstract: Characterizing the physical channel and calibrating the cryptosystem hardware are prerequisites for establishing a quantum channel for quantum key distribution (QKD). Moreover, an inappropriately implemented calibration routine can open a fatal security loophole. We propose and experimentally demonstrate a method to induce a large temporal detector efficiency mismatch in a commercial QKD system by deceiving a channel length calibration routine. We then devise an optimal and realistic strategy using faked states to break the security of the cryptosystem. A fix for this loophole is also suggested.

Record 8 of 14
Title: **Tailored bright illumination attack on distributed-phase-reference protocols**
Author(s): Lydersen, L (Lydersen, L.); Skaar, J (Skaar, J.); Makarov, V (Makarov, V.)
Source: JOURNAL OF MODERN OPTICS Volume: 58 Issue: 8 Pages: 680-685 DOI: 10.1080/09500340.2011.565889 Published: 2011
Abstract: Detector control attacks on quantum key distribution systems exploit the linear mode of avalanche photodiode in single photon detectors. So far, the protocols under consideration have been the BB84 protocol and its derivatives. Here we present how bright tailored illumination exploiting the linear mode of detectors can be used to eavesdrop on distributed-phase-reference protocols, such as differential-phase-shift and coherent-one-way.

Record 9 of 14
Title: **Controlling a superconducting nanowire single-photon detector using tailored bright illumination**
Author(s): Lydersen, L (Lydersen, Lars); Akhlaghi, MK (Akhlaghi, Mohsen K.); Majedi, AH (Majedi, A. Hamed); Skaar, J (Skaar, Johannes); Makarov, V (Makarov, Vadim)
Source: NEW JOURNAL OF PHYSICS Volume: 13 Article Number: 113042 DOI: 10.1088/1367-2630/13/11/113042 Published: NOV 30 2011
Abstract: We experimentally demonstrate that a superconducting nanowire single-photon detector is deterministically controllable by bright illumination. We found that bright light can temporarily make a large fraction of the nanowire length normally conductive, can extend deadtime after a normal photon detection, and can cause a hotspot formation during the deadtime with a highly nonlinear sensitivity. As a result, although based on different physics, the superconducting detector turns out to be controllable by virtually the same techniques as avalanche photodiode detectors. As demonstrated earlier, when such detectors are used in a quantum key distribution system, this allows an eavesdropper to launch a detector control attack to capture the full secret key without this being revealed by too many errors in the key.

Record 10 of 14
Title: Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography" [Appl. Phys. Lett. 98, 231104 (2011)]
Author(s): Lydersen, L (Lydersen, Lars); Makarov, V (Makarov, Vadim); Skaar, J (Skaar, Johannes)
Source: APPLIED PHYSICS LETTERS Volume: 99 Issue: 19 Article Number: 196101 DOI: 10.1063/1.3658806 Published: NOV 7 2011

Record 11 of 14
Title: **Controlling an actively-quenched single photon detector with bright light**
Author(s): Sauge, S (Sauge, Sebastien); Lydersen, L (Lydersen, Lars); Anisimov, A (Anisimov, Andrey); Skaar, J (Skaar, Johannes); Makarov, V (Makarov, Vadim)
Source: OPTICS EXPRESS Volume: 19 Issue: 23 Pages: 23590-23600 Published: NOV 7 2011
Abstract: We control using bright light an actively-quenched avalanche single-photon detector. Actively-quenched detectors are commonly used for quantum key distribution (QKD) in the visible and near-infrared range. This study shows that these detectors are controllable by the same attack used to hack passively-quenched and gated detectors. This demonstrates the generality of our attack and its possible applicability to eavsdropping the full secret key of all QKD systems using avalanche photodiodes (APDs). Moreover, the commercial detector model we tested (Perkin-Elmer SPCM-AQR) exhibits two new blinding

mechanisms in addition to the previously observed thermal blinding of the APD, namely: malfunctioning of the bias voltage control circuit, and overload of the DC/DC converter biasing the APD. These two new technical loopholes found just in one detector model suggest that this problem must be solved in general, by incorporating generally imperfect detectors into the security proof for QKD. (C) 2011 Optical Society of America

Record 12 of 14
Title: **Superlinear threshold detectors in quantum cryptography**
Author(s): Lydersen, L (Lydersen, Lars); Jain, N (Jain, Nitin); Wittmann, C (Wittmann, Christoffer); Maroy, O (Maroy, Oystein); Skaar, J (Skaar, Johannes); Marquardt, C (Marquardt, Christoph); Makarov, V (Makarov, Vadim); Leuchs, G (Leuchs, Gerd)
Source: PHYSICAL REVIEW A Volume: 84 Issue: 3 Article Number: 032320 DOI: 10.1103/PhysRevA.84.032320 Published: SEP 15 2011
Abstract: We introduce the concept of a superlinear threshold detector, a detector that has a higher probability to detect multiple photons if it receives them simultaneously rather than at separate times. Highly superlinear threshold detectors in quantum key distribution systems allow eavesdropping the full secret key without being revealed. Here, we generalize the detector control attack, and analyze how it performs against quantum key distribution systems with moderately superlinear detectors. We quantify the superlinearity in superconducting single-photon detectors based on earlier published data, and gated avalanche photodiode detectors based on our own measurements. The analysis shows that quantum key distribution systems using detector(s) of either type can be vulnerable to eavesdropping. The avalanche photodiode detector becomes superlinear toward the end of the gate. For systems expecting substantial loss, or for systems not monitoring loss, this would allow eavesdropping using trigger pulses containing less than 120 photons per pulse. Such an attack would be virtually impossible to catch with an optical power meter at the receiver entrance.

Record 13 of 14
Title: **Avoiding the blinding attack in QKD; REPLY (COMMENT)**
Author(s): Lydersen, L (Lydersen, Lars); Wiechers, C (Wiechers, Carlos); Wittmann, C (Wittmann, Christoffer); Elser, D (Elser, Dominique); Skaar, J (Skaar, Johannes); Makarov, V (Makarov, Vadim)
Source: NATURE PHOTONICS Volume: 4 Issue: 12 Pages: 801-801 DOI: 10.1038/nphoton.2010.278 Published: DEC 2010
ISSN: 1749-4885

Record 14 of 14
Title: **Controlling passively quenched single photon detectors by bright light**
Author(s): Makarov, V (Makarov, Vadim)
Source: NEW JOURNAL OF PHYSICS Volume: 11 Article Number: 065003 DOI: 10.1088/1367-2630/11/6/065003 Published: JUN 12 2009
Abstract: Single photon detectors (SPDs) based on passively quenched avalanche photodiodes can be temporarily blinded by relatively bright light, of intensity less than 1 nW. A bright-light regime suitable for attacking a quantum key distribution system containing such detectors is described in this paper. In this regime, all SPDs in the receiver Bob are uniformly blinded by continuous illumination coming from the eavesdropper Eve. When Eve needs a certain detector in Bob to produce a click, she modifies the polarization (or other parameters used to encode quantum states) of the light she sends to Bob such that the target detector stops receiving light, while the other detector(s) continue to be illuminated. The target detector regains single photon sensitivity and, when Eve modifies the polarization again, produces a single click. Thus, Eve has full control of Bob and can perform a successful intercept-resend attack. To check the feasibility of the attack, three different models of passively quenched detectors have been tested. In the experiment, I have simulated the intensity diagrams the detectors would receive in a real QKD system under attack. Control parameters and side effects are considered. It appears that the attack could be practically possible.