Tampering with source harms the security of quantum cryptography

Shi-Hai Sun[1],* Feihu Xu[2,4],† Mu-Sheng Jiang[1], Xiang-Chun Ma[1], Hoi-Kwong Lo[2],‡ and Lin-Mei Liang[1,3]§
[1] *College of Science, National University of Defense Technology, Changsha 410073, P.R.China*
[2] *Center for Quantum Information and Quantum Control, Department of Electrical and Computer Enginnering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[3] *State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, P.R.China*
[4] *Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*
(Dated: June 1, 2015)

The security of source has become an increasingly important issue in quantum cryptography. Based on the framework of measurement-device-independent quantum-key-distribution (MDI-QKD), the source becomes the only region exploitable by a potential eavesdropper (Eve). Phase randomization is a cornerstone assumption in most discrete-variable (DV-) quantum communication protocols (e.g., QKD, quantum coin tossing, weak coherent state blind quantum computing, and so on), and the violation of such an assumption is thus fatal to the security of those protocols. In this letter, we show a simple quantum hacking strategy, with commercial and homemade pulsed lasers, by Eve that allows her to actively tamper with the source and violate such an assumption, without leaving a trace afterwards. Furthermore, our attack may also be valid for continuous-variable (CV-) QKD, which is another main class of QKD protocol, since, excepting the phase random assumption, other parameters (e.g., intensity) could also be changed, which directly determine the security of CV-QKD.

Since the detection system is widely regarded as the Achilles' heel of QKD , MDI-QKD is of great importance. Indeed, recently, MDI-QKD has been demonstrated both in the laboratory and in the field. Based on the framework of MDI-QKD, the source becomes the final battlefield for the legitimate parties and Eve. And the major flaw of source is that a semiconductor laser diode (S-LD), which generates a weak coherent state, is normally used as a single photon source in most commercial and research QKD systems. The security of MDI-QKD as well as BB84 based on S-LD has been proven with decoy state. Hence, it has been convinced that if the source can be well characterized (for example the source flaws could be taken care of with the loss-tolerant QKD protocol, perfect security can still be obtained.

However, we demonstrate a simple quantum hacking strategy, with both commercial and homemade pulsed laser based on S-LD, that allows Eve to actively violate the phase randomization assumption, without leaving a trace afterwards. Thus it is effective for most of DV-quantum communication protocols. Our attack may also be effective for CV-QKD, since other parameters of the source (e.g., intensity) could also be changed. For example, it had been proven that the local oscillator fluctuation will compromise the security of CV-QKD. Since S-LDs are widely used in most quantum information protocols (e.g., DV-QKD, CV-QKD, QCT, BQC, and so on), and the security of these protocols is closely related to S-LD's parameters, our work constitutes an important step towards secure quantum information processing.

Our attack differs from previous attacks. First, in our attack, Eve actively violate some basic assumptions required in the security proof by tampering with an initial perfect source. Second, unlike the laser damage attack in which Eve also actively creates loopholes for a perfect SPD, the created loopholes by our attack are temporary, this makes our attack impossible for Alice and Bob to detect during the off-time of the QKD system. Third, our attack also differs from the Trojan-horse attack. In our attack, Eve directly break some basic assumptions of QKD protocols, whereas in the Trojan horse attack, back-reflected light is measured to analyze Alice's information. And as the best we know, the Trojan horse attack is invalid for Alice with multi-lasers. But our attack remains applicable to such systems. Fourth and most importantly, our attack targets the source instead of SPD. This makes our attack to be a serious threat for most quantum information protocols (not only QKD, but also QCT and BQC).

Here we emphasize that the phase randomization is a cornerstone assumption in the security of many quantum communication protocols including QKD, QCT and BQC. It is important for not only weak coherent pulse based protocols, but also, for instance, parametric down conversion based protocols. And continuous or discrete phase randomization is also crucial for the loss-tolerant protocol. In fact, without the phase randomization, the performance of a quantum communication protocol will be dramatically reduced in distance and key rate. However, we demonstrate experimentally in a clear manner how easy it is for Eve to violate such a fundamental assumption in a practical setting. Thus our work is very generality for most of quantum information processing protocols. It works for most DV-QKD, with various en-

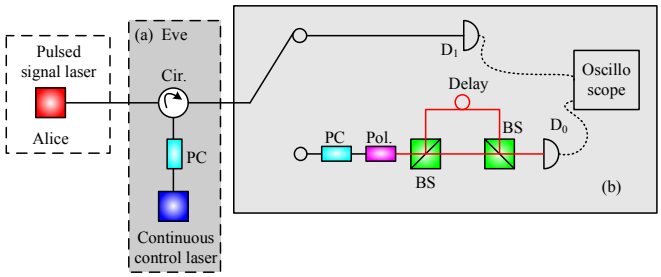

FIG. 1: (Color online) Schematic setup of our experiment. Part(a) shows Eve's control devices, in which Eve uses a continuous wave (cw) laser to tamper with the parameters of Alice's pulsed signal laser. Part(b) shows the experimental setups to measure the parameters of Alice's signal pulses. The phase of adjacent pulse is measured by an unbalanced Mach-Zehnder interferometer (lower arm of part(b)). And the waveform of Alice's signal pulse is directly measured with a photodiode (upper arm of part(b)). The output of photodiodes (D_0 and D_1) are recorded with an oscilloscope. Cir.: circulator; PC: polarization controller; Pol.: polarizer; BS: beam splitter. Solid lines are optical fibers (single-mode fiber for black color and polarization-maintaining fiber for red color), and dashed lines are electrical lines. Here we consider Eve's control laser working at continuous wave (cw) mode. However, in later parts of this paper, we will consider the possibility that Eve modulates her control laser into short photon pulses. This can make it harder for Alice to detect Eve's attack.

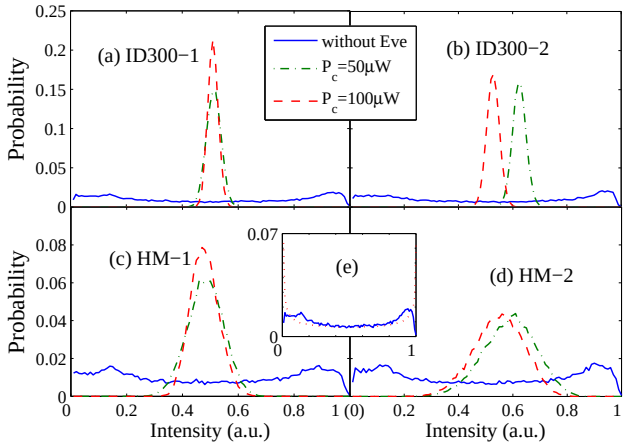

FIG. 2: (Color online) Experimental results for normalized intensity distribution of V_P^s. P_c is the power of Eve's control laser. Parts(a)-(d) show the intensity distribution of four S-LDs with Eve's different control intensities. Part(e) shows the theoretical simulation (dashed line) of the probability distribution when the phase of each pulse follows a uniform distribution from 0 to 2π, and the experimental results of ID300-1 (solid line) when Eve is absent. These results clearly show that when photons are injected into Alice's signal laser, the phase of the signal laser becomes correlated. Here P_c is not minimized for Eve, and a further experiment about the minimal power is discussed in the following text (see Fig.4).

coding schemes (polarization, phase and time-bin) and various kinds of lasers (pulsed laser and continuous wave (cw) laser). It is also possibly a serious threat for CV-QKD and other quantum information processing protocols (such as QCT and BQC).

The basic principle of our attack is as follows. In the inter-driven mode, the semiconductor medium of the S-LD is excited from loss to gain by each driving current pulse. A laser pulse is generated from *seed* photons originating from spontaneous emission. The phase of the laser pulse is determined by the seed photons. Since the phase of the seed photons is random, the phase of each laser pulse is random inherently. However, if a certain number of photons are injected from an external source into the semiconductor medium, these photons will also be amplified to generate laser pulses. Consequently, the seed photons consist of two parts: one from spontaneous emission and the other part from the external source. Both parts will affect the phase of the resulting laser pulse. If the injected photons greatly outnumber the photons from spontaneous emission, the phase of the output laser pulse is largely determined by the phase of the injected photons. Therefore, Eve can control the phase of Alice's signal laser by illuminating the S-LD from an external 'control source', and successfully violate the phase randomization assumption.

Figure 1 shows the schematic setup of our experiment. We test four sample S-LDs operating in inter-driven mode, two ID300 pulsed lasers from IdQuantique (numbers ID300-1 and ID300-2), and two homemade pulsed lasers with S-LDs from Sunstar Communication Technology CoLtd (model: SDLP55HMBIFPN, numbers HM-1 and HM-2). The phase between adjacent pulses is measured with an unbalanced Mach-Zehnder interferometer (lower arm of Fig.1(b). In theory, the output voltage after D_0 is $V_P \propto [1+\cos(\Delta\phi+\theta_0)]/2$, where $\Delta\phi$ is the phase difference between adjacent pulses, and θ_0 is the inherent phase difference between the two paths of the interferometer. By passively controlling the interferometer with temperature controller and vibration isolator, we can stabilize the interferometer within about 2 minute. Then we set $V_P^s \propto [1+\sin(\Delta\phi)]/2$ for $\theta_0 = \pi/2$.

A uniform distribution of $\Delta\phi$ from 0 to 2π will produce a U-type intensity distribution, owing to the fact that the mapping from phase to intensity is non-linear, $V_P \propto \sin(\Delta\phi)$. Indeed when Eve is absent, the same distributions (solid lines of Fig.2) are obtained in experimental with both ID-300 and the homemade pulsed laser. However, a bright light from Eve could correlate the phase of each pulse and violate the phase randomization assumption (dashed lines of Fig.2). In fact, when photons are injected into Alice's signal laser, the intensity distribution of V_P^s for both ID300 and the homemade signal laser becomes Gaussian. Consequently, various quantum hacking strategies can be applied to spy on the final key. Figure 3(a) shows a schematic setup to attack a complete QKD system.

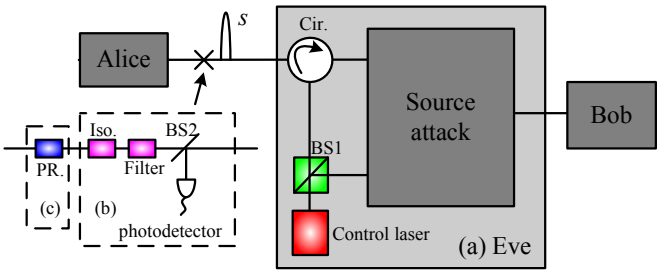

FIG. 3: (Color online) (a) Principle scheme to attack a complete QKD system by combining our attack with source attack. s is Alice's quantum signal pulse. Eve splits her bright control pulse into two parts with a beam splitter (BS1), one part serves as control laser to tamper with the parameters of Alice's signal pulse, while the other part serves as phase reference for Eve to perform the source attack. (b) A possible countermeasure for Alice to monitor our attack. Alice splits parts of the light with BS2 and monitors the power with a photodetector. The optical frequency filter is used to remove all wavelength-dependent flaw of Alice's source. The isolator (Iso.) is used to prevent light from entering Alice's lab from the quantum channel. (c) Active phase randomization scheme (PR.), which can guarantee the phase randomization assumption and partially reduce the risk of our attack, but it can not entirely remove our attack (see text for detail).

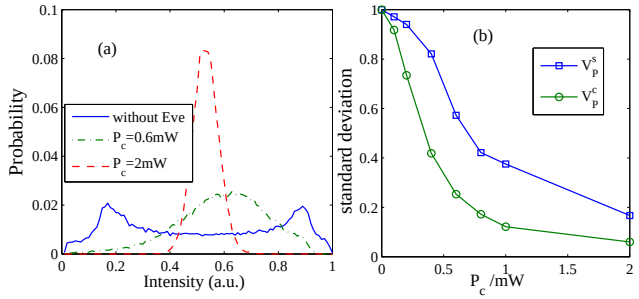

FIG. 4: (Color online) (a) Experimental results for V_P^s, when a 25dB isolator is placed after the signal laser ID300-1. (b) The standard deviation of $V_P^s \propto \sin(\Delta\phi)$ and $V_P^c \propto \cos(\Delta\phi)$ with different powers of control light. The standard deviation has been normalized by that of $P_c = 0$. The experimental results clearly show that, even if a 25dB isolator is used by Alice, the intensity distribution is still Gaussian-type but not U-type when Eve uses a cw laser with a power of $0.6mW$. It means that Eve could still ntroduce non-random phase in Alice's quantum signal. In the test, only a 25dB isolator is put after the output of Alice (the photodetector and the filter will be discussed in later). Other setups used here are the same as those for Fig.2.

Fig.5 shows that the pulse shape would also be changed by Eve's bright light. These changed parameters are also helpful. For example, the signal pulse is emitted earlier than that without Eve, and the time shift is different for each S-LDs. Furthermore, in the absence of an external field, the first oscillation is much stronger than the following oscillation, and a few oscillations appear. But when Eve is present, more oscillations are observed, and different laser diodes have different oscillation waveform. Thus it is possible for Eve to compromise the security of QKD systems with multi-lasers by measuring the characters of signal pules (e.g., time-shift, pulse width, optical frequency).

Here we remark that, generally speaking, the changes of pulse shape are helpful for both Eve and Alice. Although more imperfection could be exploited by Eve, more parameters could be monitored by Alice to discover the existence of Eve. In fact, both Eve and Alice must be very careful in the cat-and-mouse game. First, if Alice wants to completely monitor the changes of pulse shape, some advanced devices with high speed and bandwidth are required, which may dramatically increase the technology challenge and cost of a practical Alice. Second, Eve could carefully configure her attack to ensure that her attack could not increase the error rate and the changes of pulse shape could not be discovered by Alice. Third, generally speaking, the changed shape may actually benefit Eve more than Alice and Bob. This is because Eve could well be a spy or national security agency such as the NSA and so Eve has a much larger power and budget than Alice and Bob. Thus Eve is probably at a better position to exploit the imperfections that she has introduced in the quantum signal. Furthermore, note that even a tiny violation of the phase randomization assumption or other parameters of the source will undermine the very foundation of security proofs in QKD and it will no longer be fair for Alice and Bob to claim unconditional security.

Finally, in addition to using a laser, Eve can also attack the QKD system by using temperature, microwave radiation, and so on. At the same time, although most quantum hackers focus on the optical devices of the legitimate parties, Eve can also exploit imperfections in the electrical devices of the QKD system. For example, if the electromagnetic shielding of devices of Alice and Bob is imperfect, Eve could use microwave radiation from outside to control the parameters of these devices. These are the subjects for future investigations.

* shsun@nudt.edu.cn
† tigerfeihuxu@gmail.com
‡ hklo@ece.utoronto.ca
§ nmliang@nudt.edu.cn