Resilient Chip-Scale QKD with Integrated Hacking Prevention

Friederike Jöhlinger[1,2], Lawrence Rosenfeld[2], Henry Semenenko[1,2], Djeylan Aktas[2], John Rarity[2]

[1]Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1FD, UK
[2]Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1FD, UK

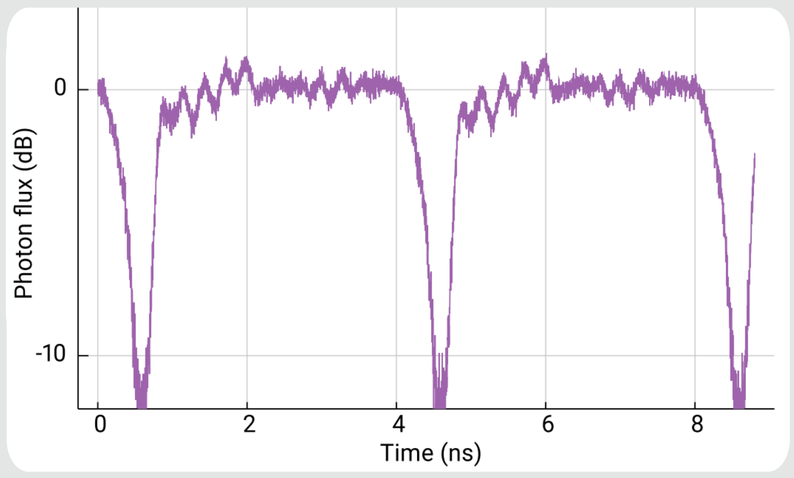
Abstract

Recently, the first integrated Measurement Device Independent Quantum Key Distribution (MDI QKD) system has been implemented here in Bristol [1]. To build on this result and achieve full system security and state-of-the-art key rates, a new indium phosphide (InP) transmitter chip has been designed and fabricated for a second-generation MDI QKD implementation. The new chip contains two laser sources, including a distributed feedback laser to allow for faster pulsing and high-speed phase modulators with a bandwidth of up to 30 GHz. With the new lasers and phase modulators a higher pulse rate will be achieved, leading to better key rates. Additionally, an on-chip photodiode can be used to monitor incoming light. This makes the chip much more resilient against hacking attacks on the receiver side. Since MDI QKD is intrinsically protected against detector attacks, this means that this new MDI QKD system will show great security overall.

Distributed Feedback Laser

To obtain phase randomised pulses from a laser, one can use gain switching: when the amplification medium is completely depleted, the next pulse will originate from spontaneous emission and therefore have a random phase w.r.t. the previous pulse.

The previous chip [1, 3] used a laser made of a semiconductor optical amplifier (SOA) surrounded by two distributed Bragg reflectors (DBRs). This worked very well when operated in a continuous wave (CW) mode, but the Distributed Feedback Laser (DFB) should allow faster gain switching.

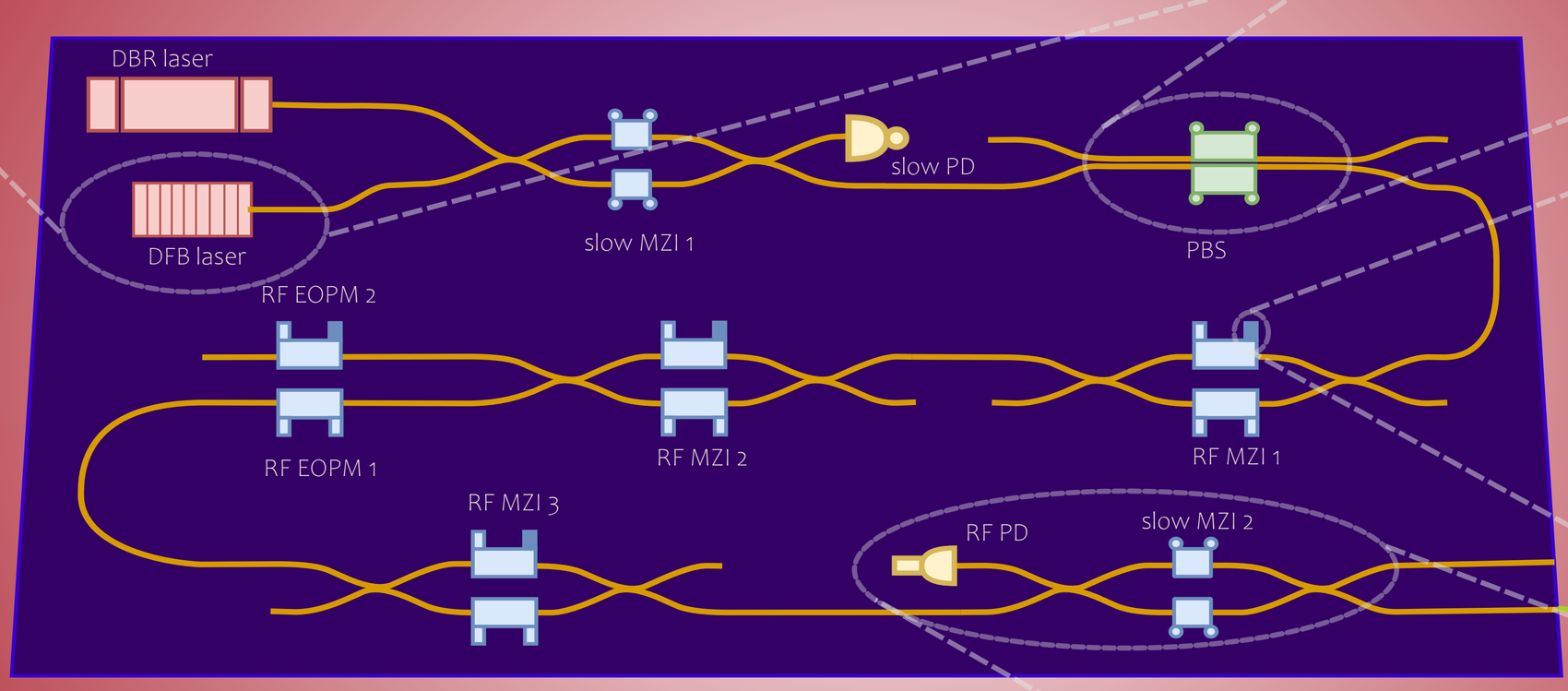


Photon flux of a DBR on-chip laser during switching measured by a Single Photon Detector (SPD). One can see strong oscillations at the start of the pulse, before settling after about 1.5 ns. A DFB laser is expected to settle more quickly increasing pulse and therefore key rate. Fig. reproduced from ref [2].

Polarising Beam Splitter

Active elements such as phase modulators and couplers often operate differently on TE and TM polarised light. Since on-chip lasers do not produce purely TE or TM light, this influences the precision other operations the chip will have.

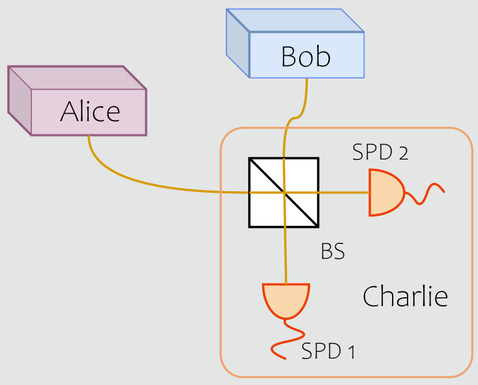
The addition of a polarising beam splitter (PBS) filters out one polarisation and leads to better extinction in the Mach-Zehnder interferometers (MZIs). The quantum signal produced will therefore be less noisy, reducing the overall quantum bit error rate (QBER).



On-Chip RF Termination

RF connections are terminated on chip to reduce electrical noise by avoiding wire bonds. The RF Electro-Optic Phase Modulators (EOPMs) should have a bandwidth of up to 30 GHz.

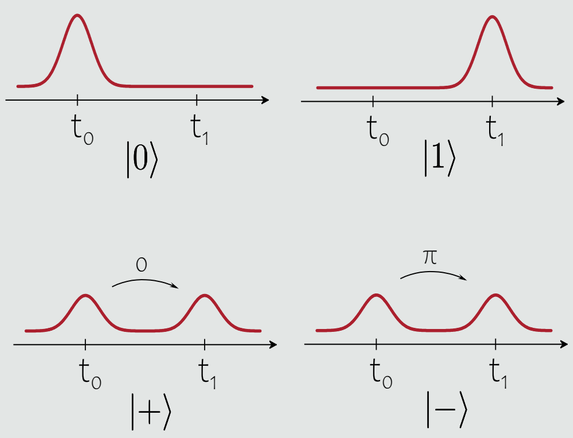
Time-Bin Encoded MDI QKD



In MDI QKD, both Alice and Bob send out a quantum state towards Charlie, an untrusted third party. Charlie interferes the two states on a beam splitter (BS), measuring in the Bell basis and publicly announces which of his two single photon detectors (SPDs) clicked, which indicates the correlation between the two received states. Since Alice and Bob know which state they have sent themselves, they can infer which state the other must have sent and therefore agree on a key bit.

In Time-Bin Encoded MDI QKD the state is divided over two time bins. In the $|0\rangle$ and $|1\rangle$ state the first or second time bin is filled, respectively. The $|+\rangle$ and $|-\rangle$ states have the same average photon number in total as the other two states, but spread over both time bins. The $|+\rangle$ state has no phase, the $|-\rangle$ state a π phase between time bins.

Additionally, decoy states should be used here as weak coherent states are used instead of single photons. The states are created using a combination of MZIs and individual phase modulators.



Hacking Prevention

MDI QKD is intrinsically protected against detection side-channel attacks. The transmitters, such as this chip, however, are still vulnerable. There are various attacks, many of which require the eavesdropper Eve to shine light into the receiver system via the quantum channel, such as the Trojan horse (THA) [4] and the laser damage attack (LDA) [5].

To monitor for such attacks, this chip contains a fast photodiode (RF PD) after an MZI as seen from Eve's direction. The MZI serves as a variable switch that determines the ratio of Eve's light reaching the RF PD and the optical encoding circuit. By choosing the right ratio, one can ensure that Eve's light is detected before she can receive any useful information about the encoding circuit during a THA. During a LDA attack, the RF PD could trigger an external switch to protect the chip from damage.

References

[1] Semenenko, H. *et al.* **Optica** 7(3), 238-242 (2020)
[2] Semenenko, H. (2019). Advances in Chip-Based Quantum Key Distribution [PhD thesis] University of Bristol
[3] Sibson, P. *et al.* **Nat. Commun.** 8, 13984 (2017)
[4] Jain, N. *et al.* **New J. Phys.** 16, 1230302 (2014)
[5] Makarov, V. *et al.* **Phys. Rev. A** 94, 030302(R) (2016)