Advances towards a Trojan Horse Attack on Chip Scale QKD

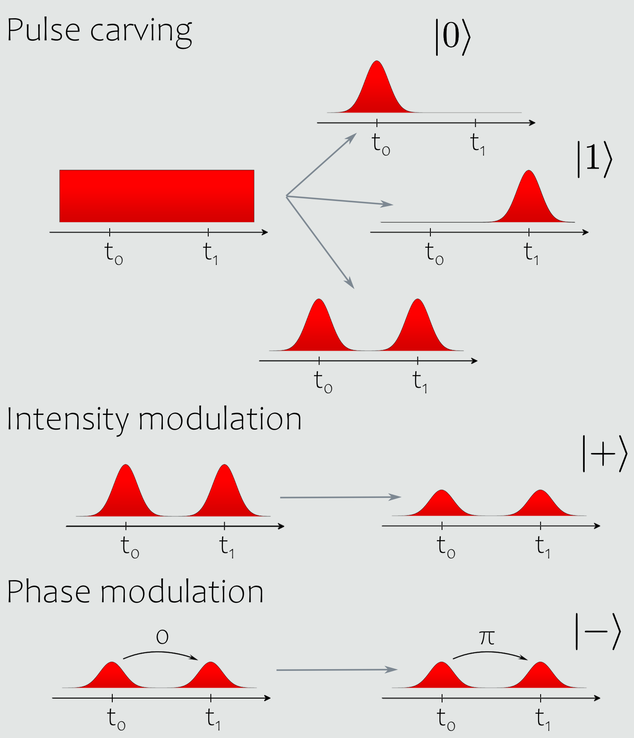
Friederike Jöhlinger[1,2], Henry Semenenko[1,2], Djeylan Aktas[2], Phil Sibson[3], Chris Erven[2,3], John Rarity[2]

[1]Centre for Doctoral Training in Quantum Engineering, University of Bristol, UK
[2]Quantum Engineering Technology Laboratories, University of Bristol, UK
[3]KETS Quantum Security Ltd., Bristol, UK

Abstract

Integrated optics offer a way for quantum key distribution (QKD) to become mainstream, due to its small size, excellent optical stability and the infrastructure for mass production available from standard telecom technology. However, there has been very little research into the security of chip-scale QKD systems, so far. In this poster the potential for a Trojan Horse Attack (THA) on an indium phosphide transmitter chip [1] is discussed. In a THA, Eve sends her own light into the QKD system and gains information about the state of the system and hence about the key from analysing the backscattered light. This attack has been successfully demonstrated on QKD systems using fibre optic components [2]. Here we will discuss how the attack can be adapted to a chip-scale system, including an analysis of reflections in the chip.

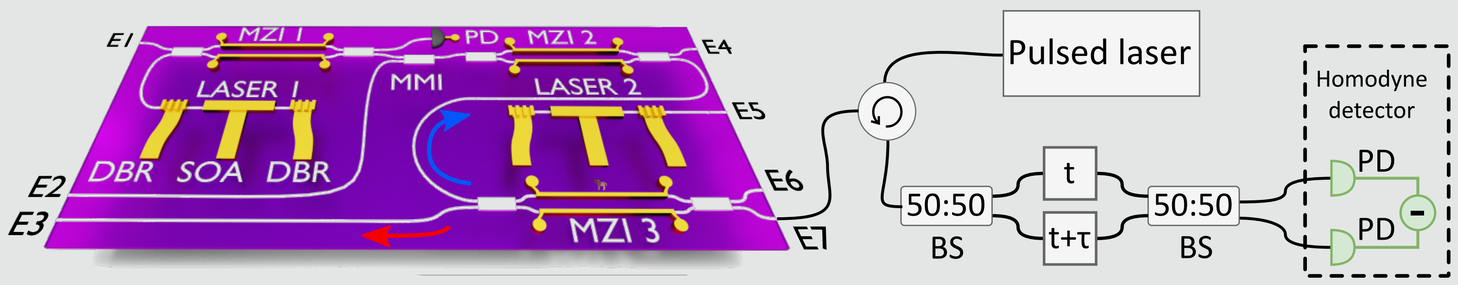
Encoding the key



The chip contains three Mach-Zehnder Interferometers (MZIs) and an electro-optic phase modulator (PH MOD) to pulse carve, intensity modulate, phase encode and phase randomise and can be used with various time-bin encoded protocols. All steps contain critical information about the key.

Trojan Horse Attack

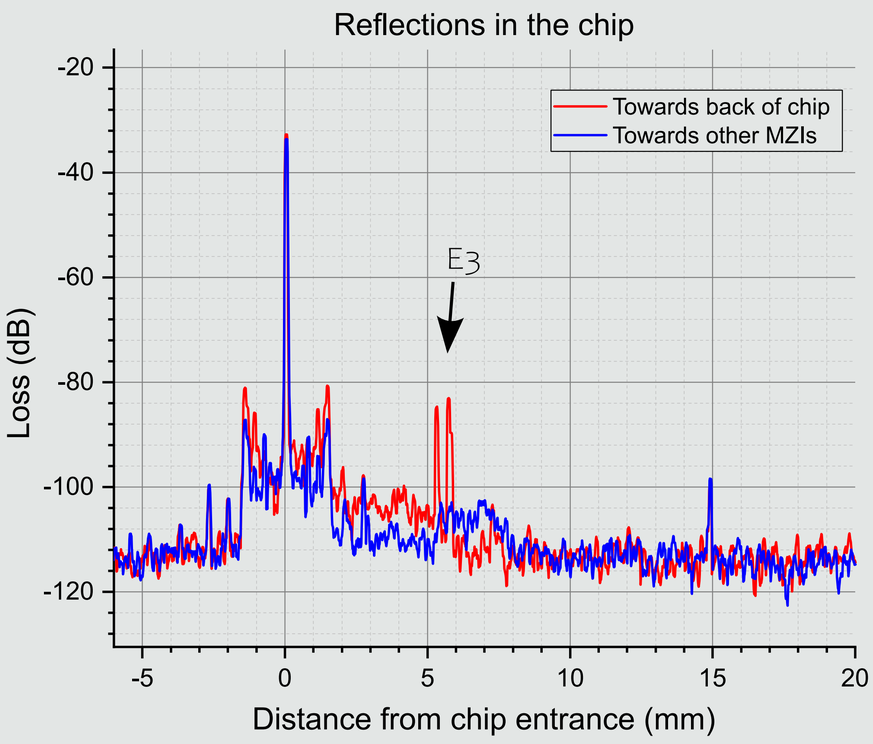
In the THA, Eve injects light into a QKD system and gains information about the key by analysing the backreflections, since her light has gone through elements used to encode the QKD signal states and will therefore contain partial or full information of the signal state produced at the same time.



One of the main requirements, is a significant and reliable point of reflection in the system after, from Eve's view, an encoding element. Such a reflection was found and the chip additionally shows a strong reflection where the light is coupled from the chip to the fibre.

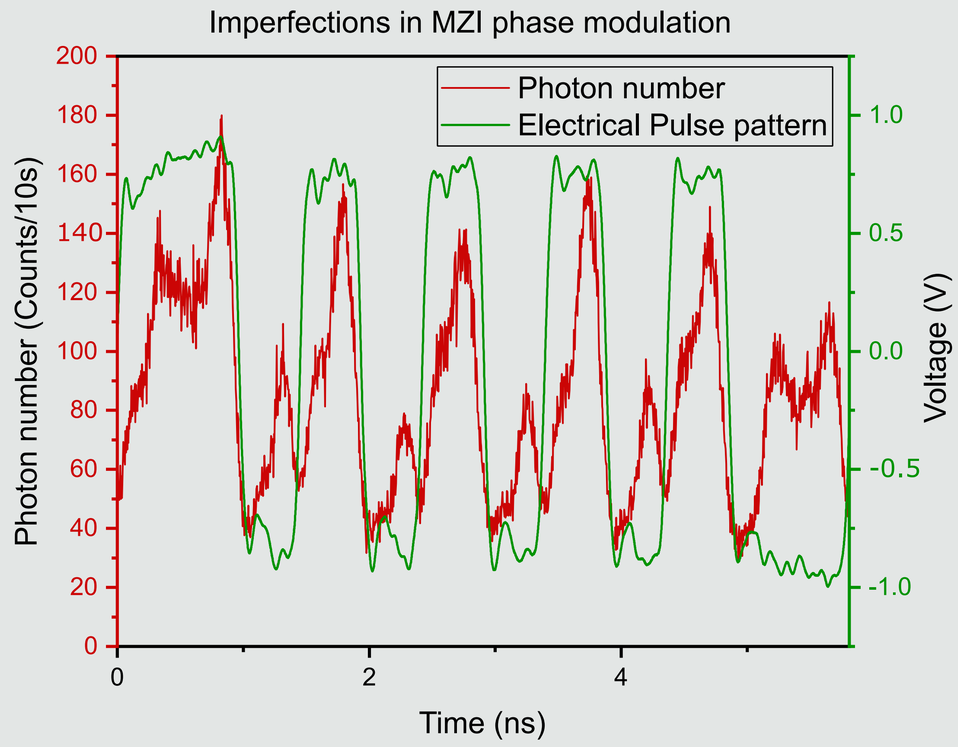
By interfering these two reflections, delaying the light reflected at E7 by τ, Eve can measure the phase encoded at MZI 3 using a homodyne detector.

Results



Reflections found at ~ 6mm from chip entrance E7
- Right distance for edge coupler E3
- Reflections dependent on setting of MZI 3

Challenges
- Small dimensions of system: entrance to back of the chip takes a pulse ~80 ps.
- Low reflection within the chip
- Not all chips show reflections, likely due to coating types used.
- Phases in protocol (0 and π) are the same if double, need to use further system imperfections



Conclusions

The prerequisites for a THA on a chip-scale QKD transmitter are met: there are distinct points of reflection in the chip that Eve can use to measure phase encoding.
However, the chip shows very few reflections and only such ones that could most likely be eliminated with careful design for future chips, for example by choosing anti-reflective coatings.

Find the Trojan Horse

The poster has been infiltrated by 4 Trojan Horses and 1 QCrypt sheep. Can you find them? The first one is easy.

References

[1] Sibson, P. et al. 2017 Nat. Commun. 8, 13984
[2] Jain, N. et al. 2014 New J. Phys. 16, 1230302