How to break Quantum Cryptography

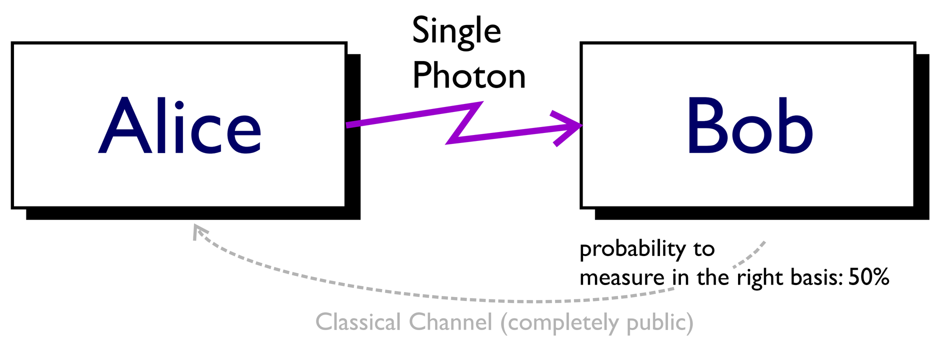
Qin Liu, Ilja Gerhardt, Vadim Makarov, Antía Lamas-Linares, Christian Kurtsiefer

In 1984 Charles Bennet and Gilles Brassard had the idea to use single quanta of light (photons) to transmit a random number from one location to another. Later this random number can be used to encrypt a message which can be sent from one side to the other in the clear (one-time pad).

The underlying principle was to use single photons, which have the intrinsic property that their quantum state cannot be copied with 100% fidelity (non-cloning theorem). So every copy process introduces errors and a legitimate receiver can estimate the knowledge of an eavesdropper and eventually retransmit the key.

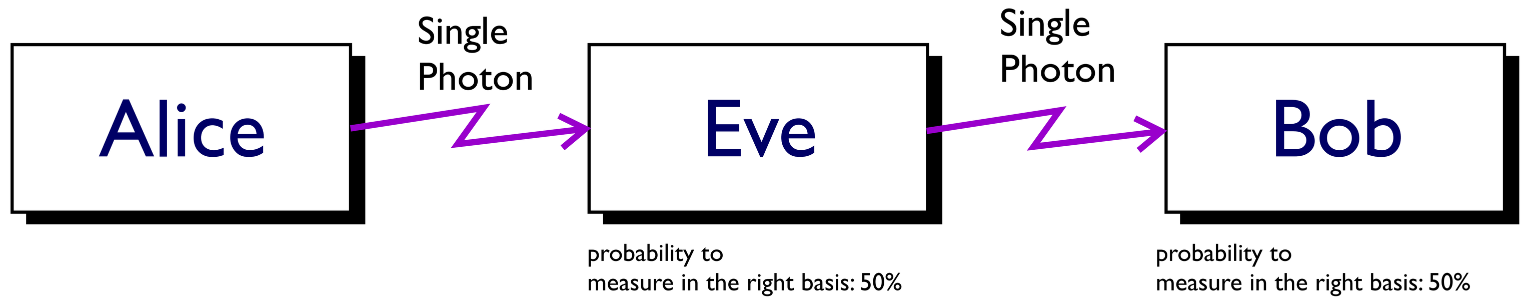
On paper, quantum cryptography (which is better described as quantum key distribution) is perfectly secure. In the real world, all implementations have certain constrains and issues. One is described below...

How does Quantum Cryptography work?



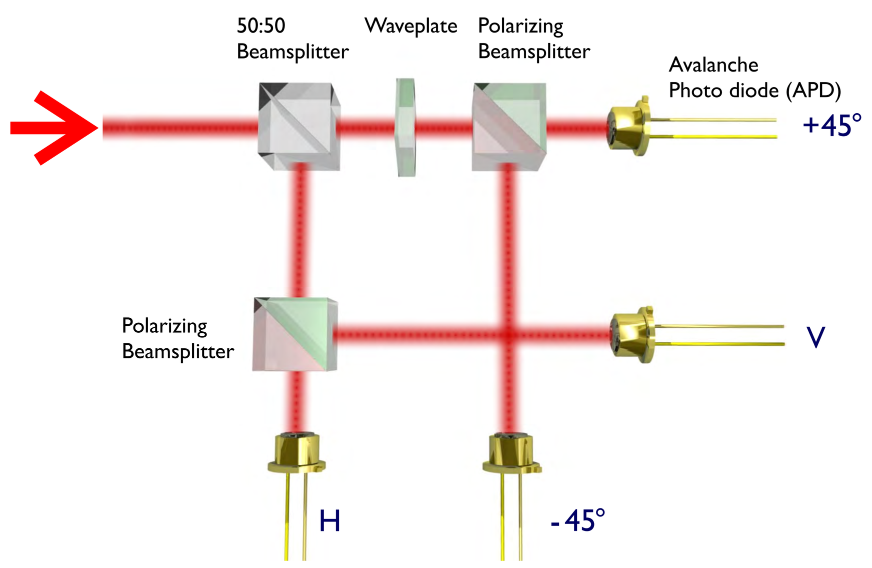
No errors between Alice and Bob

Why does a 'normal' attack not work?



25% errors between Alice and Bob

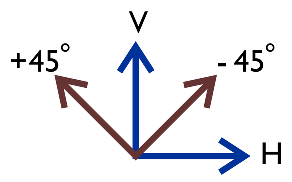
The Polarization Detection Unit with 4 APDs



Correlations between Alice and Bob

measurement with a certain input polarization:

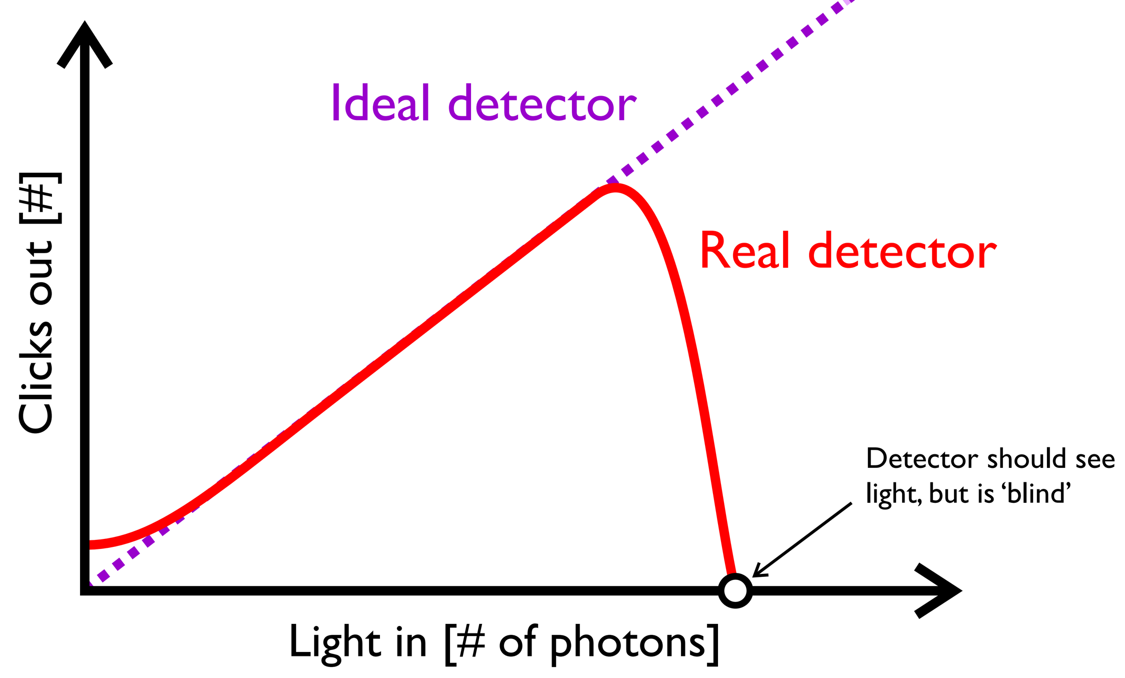
Transmitter \ Receiver	H	+45°	V	-45°
H	50%	25%	0%	25%
45°	25%	50%	25%	0%
V	0%	25%	50%	25%
-45°	25%	0%	25%	50%



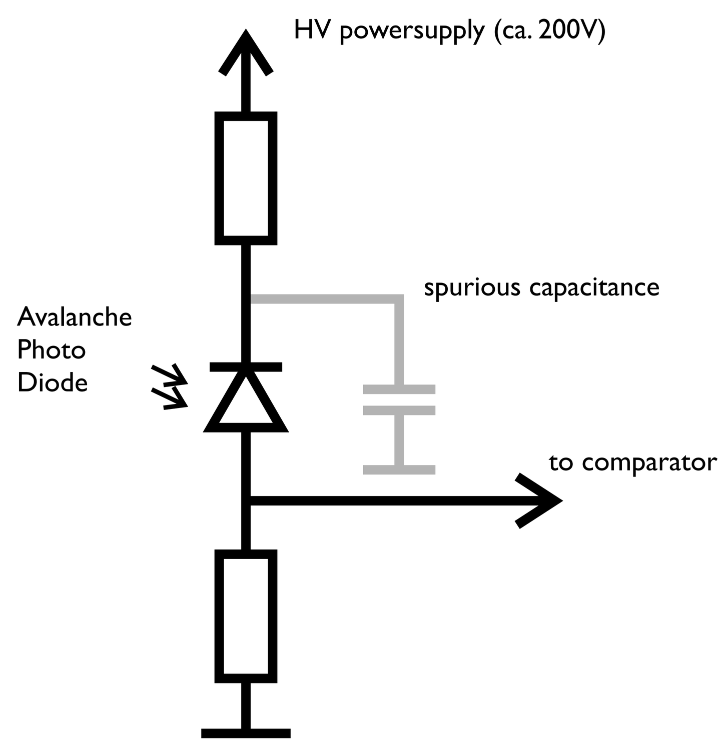
After all measurements the sender and the receiver can discuss on a public channel in which basis they have measured. First they discard all measurements which were not measured in the same basis and compare their number of detection events.
The public channel can be easily wiretapped with tools like *tcpdump* or *wireshark*, such that the measurement basis are know to an eavesdropper. Normally this would not be a problem, because the result of the quantum measurement is still unknown.

Real Detectors = Real Problems

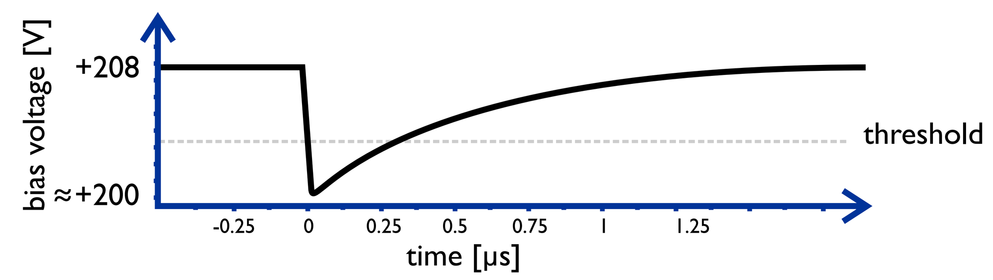
Ideal and Real Detector Response:



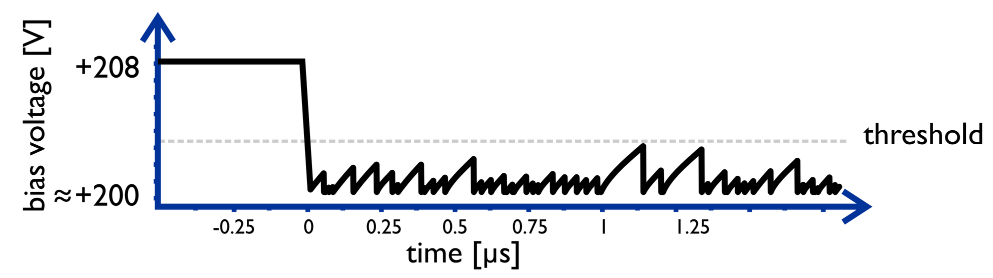
Basic Circuitry:



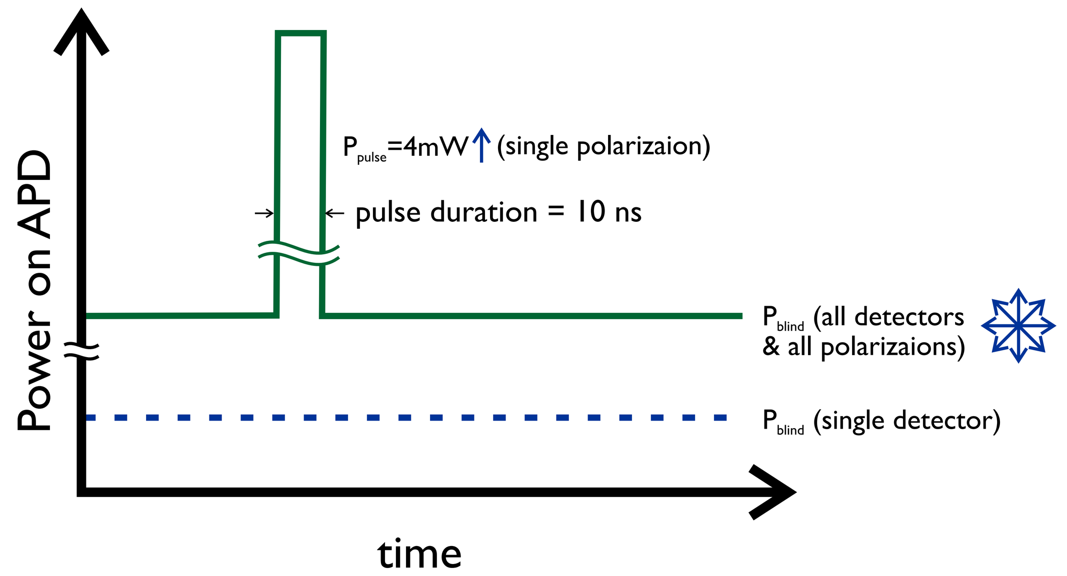
Avalanche Photo Diode - normal mode



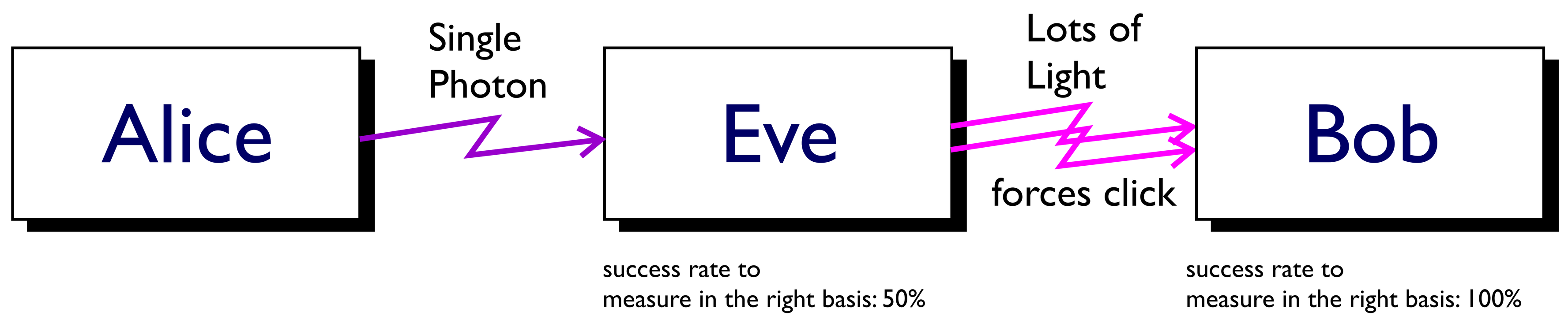
Avalanche Photo Diode - saturated, blind



How to generate a click in the receiver:



What our attack is doing:



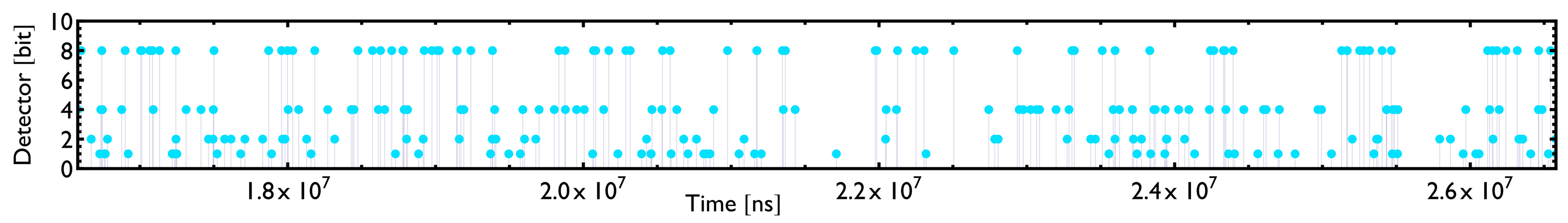
No errors between Alice and Bob - it looks like a normal transmission

A realistic scenario:

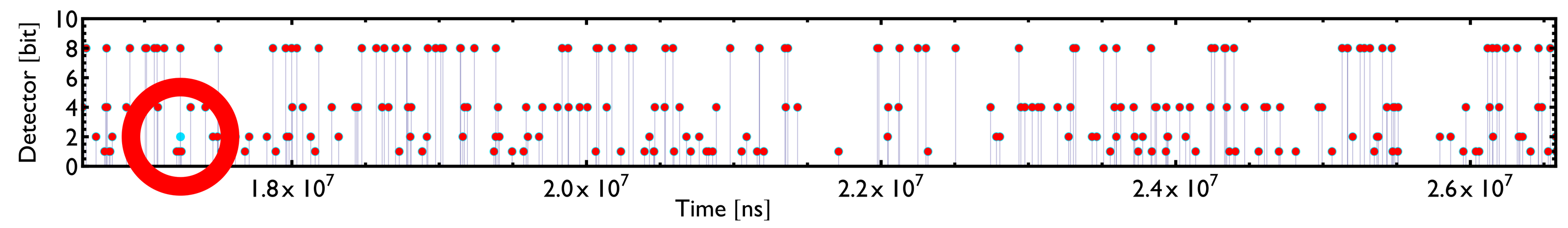
Recently we realized an attack on an established QKD line, spanning four different buildings with 290m optical fiber. A preliminary analysis shows that the eavesdropper is able to wiretap 100% of the secret transmission. The transmission channel is not changed significantly and it looks to the legitimate receiver as there would be nothing else but a little time delay which is introduced by our processing electronics.

[1] V. Makarov, New Journal of Physics, 11, (2009) 065003

Clicks captured by the eavesdropper:



Clicks generated in the legitimate receiver unit (red):



One click is missing: It looks like a tiny additional loss and still eve knows all bits of the secret key

NTNU
Norwegian University of Science and Technology

CQT Centre for Quantum Technologies, Singapore

http://quantumlah.org