Spying on practical QKD through a timing side channel

Antía Lamas-Linares and Christian Kurtsiefer
Department of Physics, National University of Singapore

Classical backdoors in QKD

The security of quantum key distribution (QKD) relies on the validity of quantum mechanics as a description of nature and on the non-existence of leaky degrees of freedom in the practical implementations. We experimentally demonstrate how, in some implementations, timing information revealed during public discussion between the communicating parties can be used by an eavesdropper to undetectably access a significant portion of the "secret" key.

All single photon counting implementations of QKD identify a single photon from background by measurement of the arrival time at detectors. This arrival time is then discussed (or encoded in a hardware signal) and discussed publicly for synchronization purposes. Ideally there should be no correlation between the timing information and the measurement results.

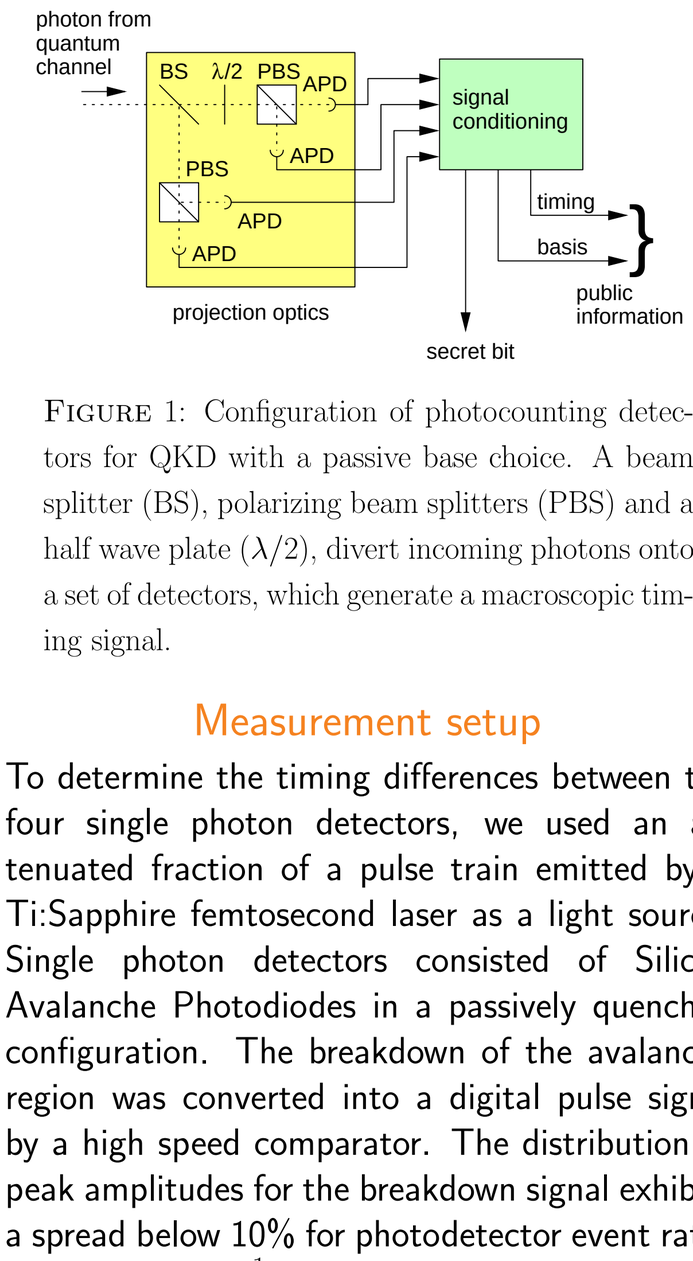

FIGURE 1: Configuration of photocounting detectors for QKD with a passive base choice. A beam splitter (BS), polarizing beam splitters (PBS) and a half wave plate ($\lambda/2$), divert incoming photons onto a set of detectors, which generate a macroscopic timing signal.

Measurement setup

To determine the timing differences between the four single photon detectors, we used an attenuated fraction of a pulse train emitted by a Ti:Sapphire femtosecond laser as a light source. Single photon detectors consisted of Silicon Avalanche Photodiodes in a passively quenched configuration. The breakdown of the avalanche region was converted into a digital pulse signal by a high speed comparator. The distribution of peak amplitudes for the breakdown signal exhibits a spread below 10% for photodetector event rates of 5000–6000 s^{-1}, and the pulse duration before the comparator is on the order of 2 ns.

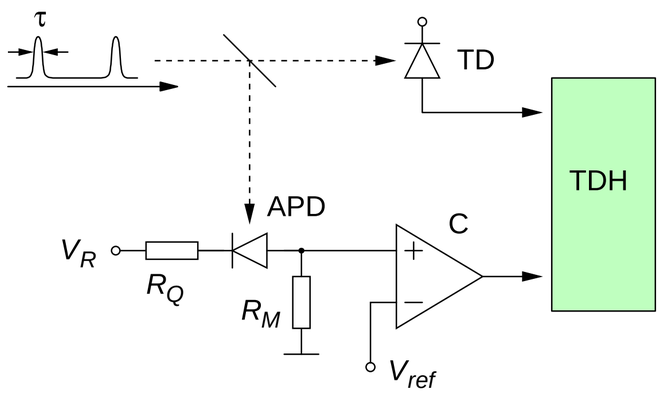

FIGURE 2: Experimental set-up to characterize the timing jitter of a single photon detector. A train of ultrashort light pulses from a mode-locked Ti:Sapphire laser is sent with strong attenuation into a passively quenched Si avalanche photodiode (APD). A histogram of timing differences (TDH) with respect to the signal of a trigger photodidode (TD) is recorded.

Detector response

A common detection topology for BB84-type schemes is shown in fig. 1. To determine the possible timing information we send a weak femtosecond light pulse to the input port and histogram the response time with respect to the trigger signal provided by a fast photodiode.

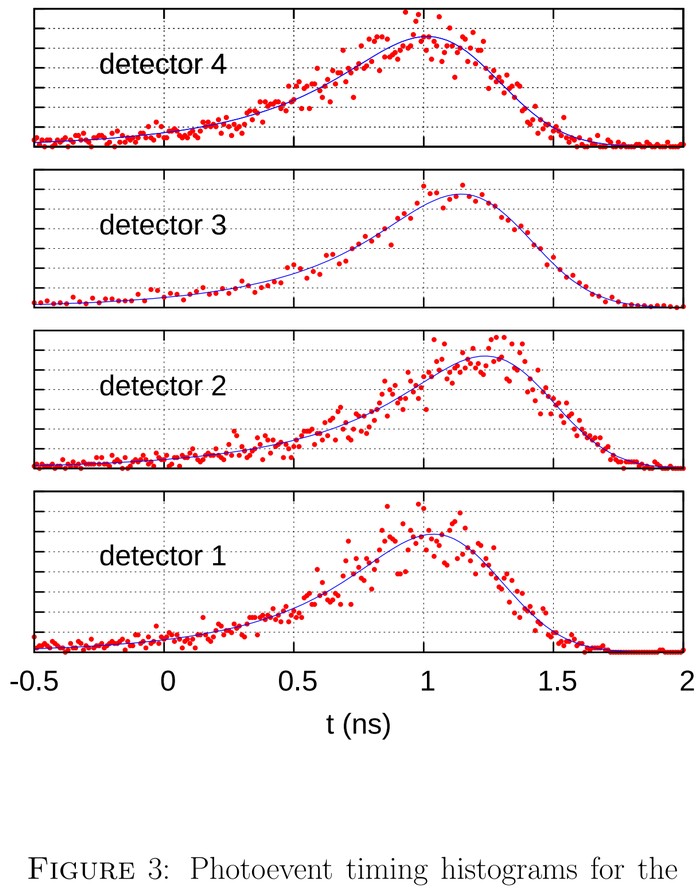

FIGURE 3: Photoevent timing histograms for the four detectors involved in a QKD receiver. The overall shape of the distributions is similar, but there is a distinction in the centroid of the histogram for different detectors.

The detector response was fitted to the convolution of an exponential decay with a Gaussian,

$$d_i(t) = \frac{1}{2\tau_e} e^{-\frac{\tau_G^2}{4\tau_e^2}} \cdot e^{\frac{t-t_0}{\tau_e}} \operatorname{erfc}\left(\frac{t-t_0}{\tau_G}\right). \qquad (1)$$

The fit values for the temporal offset t_0 and the exponential and Gaussian decay constants τ_e, τ_G for the four detectors $i = 1, 2, 3, 4$ are summarized in table 1. While the difference between τ_e and τ_G differ maximally by 38 ps and 20 ps, respectively, the time offsets t_0 can differ up to 240 ps between detectors 2 and 4. The physical origin of this difference could be attributed to differences in the electrical delays for the different detectors on the order of a few cm on the circuit board layouts, and to different absolute pulse heights of the detected breakdown currents due to different parasitic capacities for the different diodes.

Detector i	t_0 (ps)	τ_e (ps)	τ_G (ps)
1	1138 ± 7	395 ± 7	288 ± 4
2	1356 ± 6	433 ± 7	279 ± 4
3	1248 ± 4	409 ± 5	292 ± 3
4	1117 ± 7	415 ± 7	302 ± 4

TABLE 1: Extracted model parameters for the time distributions of the different photodetectors with their statistical uncertainties.

Mutual information

The knowledge in principle attainable by the eavesdropper is quantified by the mutual information $I(X;T)$ between the time distribution of detector clicks and the bits composing the secret key:

$$\begin{aligned} I(X;T) &= H(X) + H(T) - H(X,T) \\ H(T) &= -\int \bar{d}(t) \log_2[\bar{d}(t)]\, \mathrm{d}t \\ H(X) &= -\sum_x p^0(x) \log_2[p^0(x)] \\ H(X,T) &= -\sum_x \int p^0(x) d_x(t) \log_2[p^0(x) d_x(t)]\, \mathrm{d}t. \end{aligned}$$

where $\bar{d}(t) = \sum_x p^0(x) d_x(t)$ is the probability of a click occurring at time t for the ensemble of detectors, and $d_x(t)$ the probabilities of a click at a particular time t for a detector corresponding to logical value $x \in \{0, 1\}$. In most protocols, the prior distribution of logical values is balanced such that $p^0(0) = p^0(1) = 0.5$. For the detector timing distributions in fig. 3, this would reveal 3.8% of the secret key.

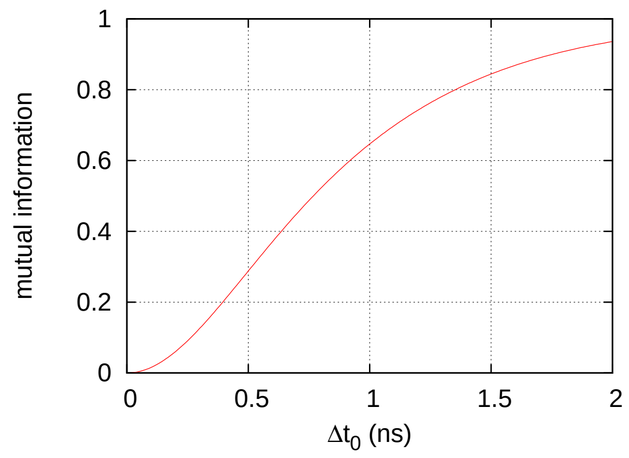

FIGURE 4: Eve's information as function of delay Δt_0 between detector timing distributions with identical shapes.

Figure 4 shows the eavesdropper's knowledge of the secret bit for two distributions $d_0(t), d_1(t)$ with the same $\tau_e = 400$ ps, $\tau_G = 290$ ps, but with different relative delays Δt_0. Detectors that are uncompensated by as little as $\Delta t_0 = 500$ ps will give the eavesdropper access to more than 25% of the "secret" key.

Conclusions

Quantum cryptography is slowly leaving the purely academic environment and starting to appear in commercial products. The theoretical aspects of its security are a very active research area, but comparatively little has been done in terms of scrutinizing the practical systems [1,2]. We have shown how some of the information publicly revealed by the communicating parties in some reasonable mature implementations, may lead to a large proportion of the key becoming insecure [3].

[1] V. Makarov, A. Anisimov and J. Skaar, PRA **74**, 022313 (2006).
[2] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, arXiv:0704.3253 (2007).
[3] A. Lamas-Linares and C. Kurtsiefer, arXiv:0704.3297 (2007).