Simple Side Channel Analysis on Plug-and-Play Quantum Key Distribution

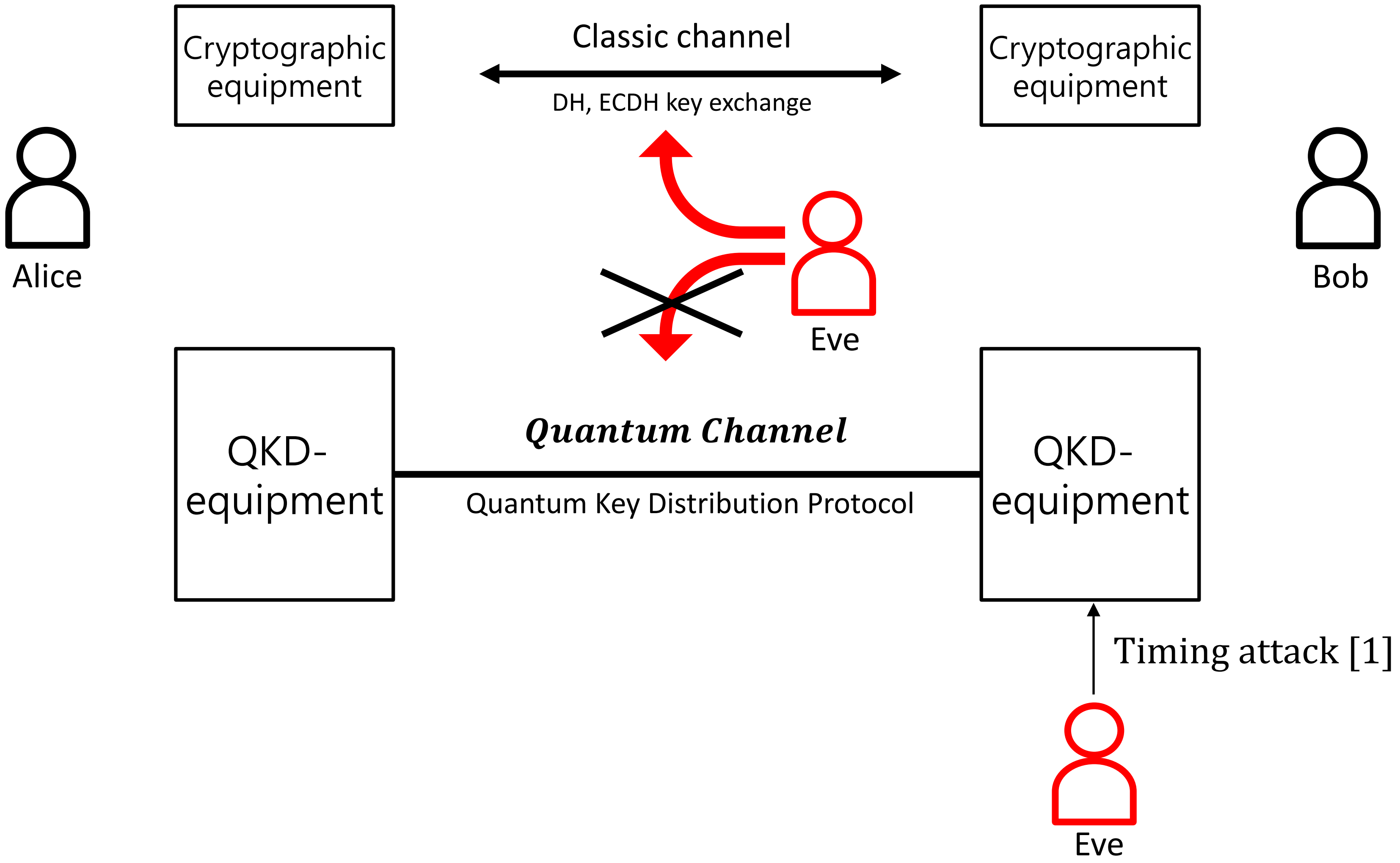
CHES 2018 Rump Session

2018. 09. 10

Suhri Kim, **Sunghyun Jin**, HanBit Kim, ByeongGyu Park, Seokhie Hong

Korea University

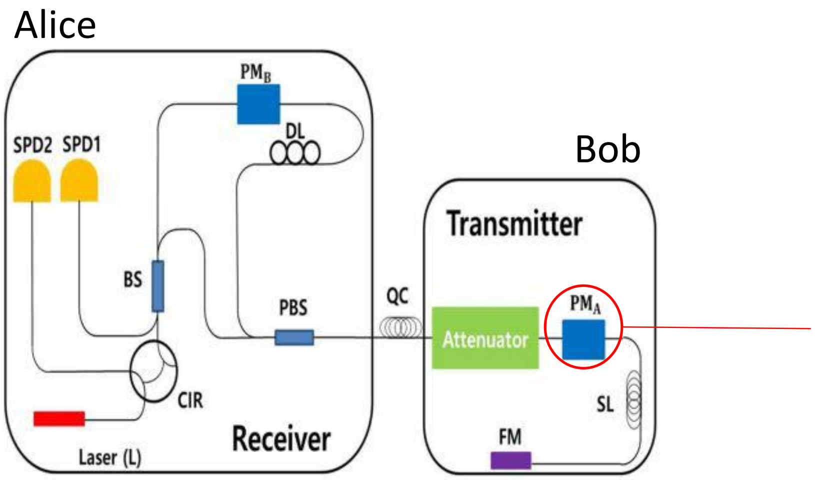
QKD(Quantum Key Distribution)



[1] Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. Opt. Express 15, 9388-9393 (2007).

Plug-and-Play QKD System

- Proposed by A. Muller
- Stable and Not required path having specific length ➔ No timing leakage

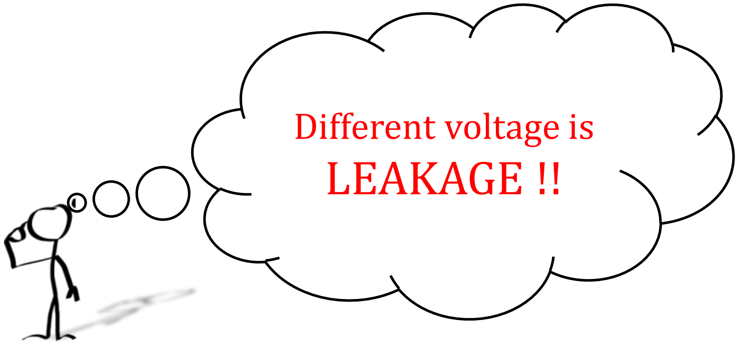


Block diagram of the P&P QKD system implemented in [2].

(BS: Beam Splitter, DL: Delay Line, PBS: Polarization Beam Splitter, CIR: Circulator, PMB: Phase Modulator in receiver, SPD: Single Photon Detector, FM: Faraday Mirror, PMA: Phase Modulator in transmitter, SL: Storage Line

(Bit, Bases) = (Voltage, Phase)

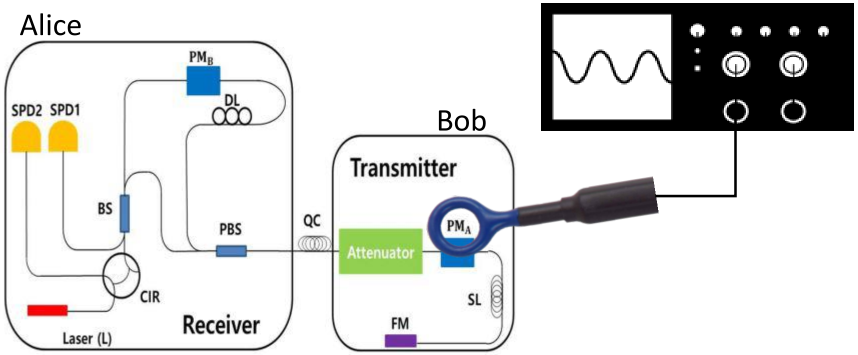
	0v	2.5v	5v	-2.5v
Bit	0	0	1	1
Bases	+	×	+	×
Phase	0	$\pi/2$	π	$3\pi/2$

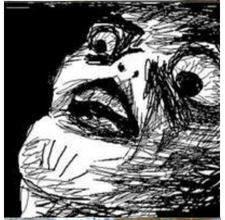


Different voltage is
LEAKAGE !!

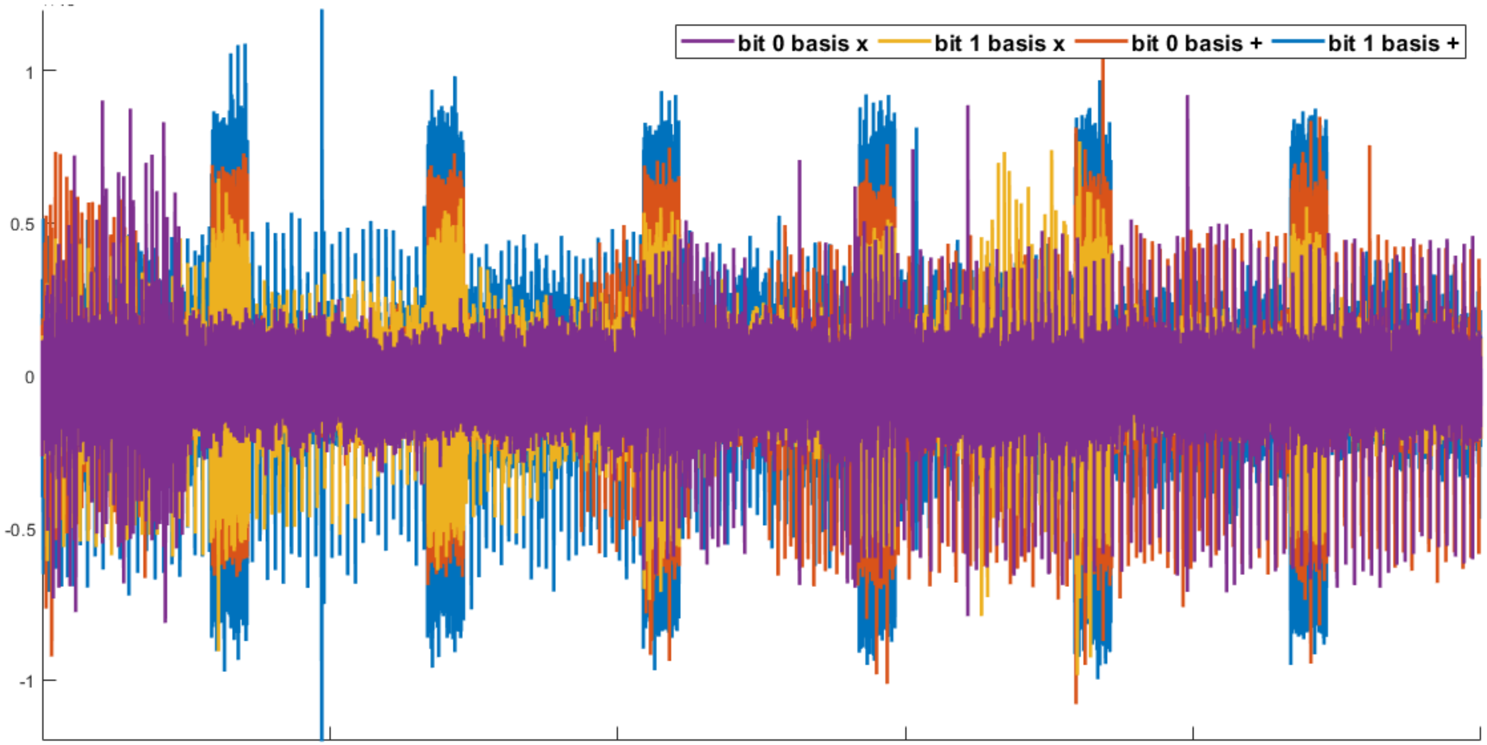
[2] B. Ahn, J. Ha, Y. Seo, J. Heo, J. Shin, and K. Lee, “Implementation of plug & play quantum key distribution protocol,” in 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, 2018, pp. 47–49.

Single Trace Attack on P&P QKD system





PLAINTEXT !



Thank you for your attention

sunghyunjin@korea.ac.kr

Cryptographic
Algorithm Laboratory