QKD

Quantum Key Distribution

Lai, Chia-Tso 3786011

Table of contents

01
Introduction

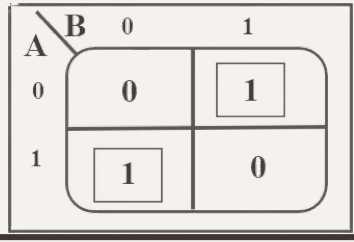
Classical Cryptography

	Secrecy	Challenge
Public Key Cryptography	Factorization of large numbers	Computational power of quantum computers
DES/AES	Lack of Information on decoding operation	Potential discovery of new classical algorithm
One-time Pad	Shared one-time secret keys	Only classical protocol proven to be secure

One-Time Pad

- Message *m* : a binary string of length n
- Secret key *k* : a binary sequence of equal length n

1. Alice computes the cipher text c = m⊕k
2. Alice sends the cipher text c to Bob over a public channel
3. Bob computes the XOR between cipher text c and key k to recover the message m= c⊕k=m⊕k⊕k



QKD Basis & Bits

Basis	Angle	Bit	Photon
+	0°	0	↔
+	90°	1	↕
✖	45°	0	↗
✖	135°	1	↖

02

BB84 Protocol

Attenuated Laser Pulses

- Laser pulses follows Poissonian distributions:

$$P(n) = \frac{\mu^n}{n!} e^{-\mu}$$

- Each pulse has on average less than 1 photon

- Conventionally, $\mu_s = 0.1$

Vacuum signals ≈ 90.5% Single photon ≈ 9% Multiphoton ≈ 0.5%

BB84 Protocol

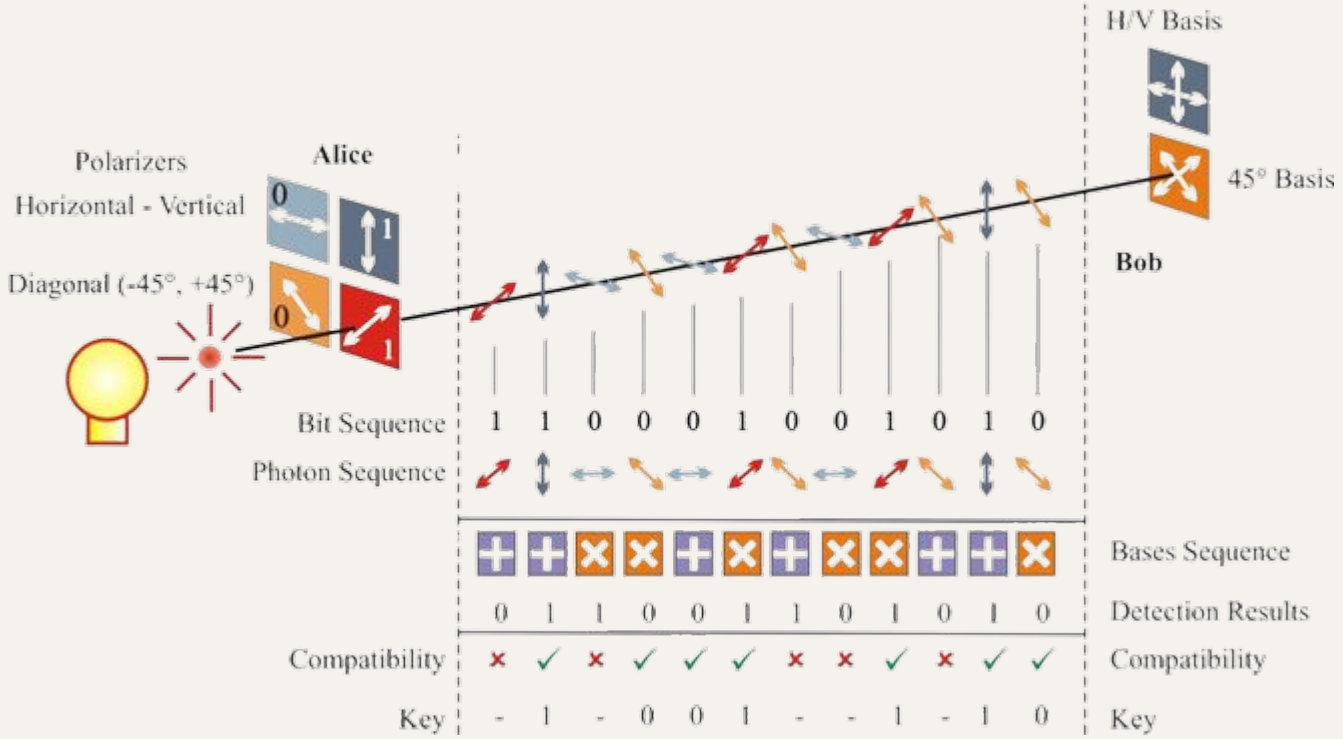
Phase 1 : Quantum Channel

- Alice sends random signals with varying polarization basis
- Bob performs measurement with random basis

Phase 2 : Classical Channel (Public Channel)

- Alice announces the basis she used for each signal. Bob announces the basis he used to perform measurement. They discard the signals where the basis are incongruent
- Alice randomly chooses half of the remaining bits and disclose them. Bob compares the signals with the measurement to check if more than a certain fraction of them agree.
- Identical bits are used as sifted keys

BB84 Protocol

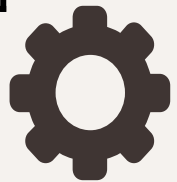


Mavroeidis et al.2018

Error & Correction

- Misalignment of devices, loss and noise of the quantum channel, dark counts in single photon detectors, etc.
- Classical linear correction code

Alice uses a linear correction code w, encodes it with her sifted key s and obtain a cipher text $c = w \oplus s$. Alice sends c to Bob
Bob has his sifted key $s' = s \oplus e$. Bob calculates his code $w' = c \oplus s' = w \oplus e$. From this relation, Bob can determine the error e



03

PNS Attack

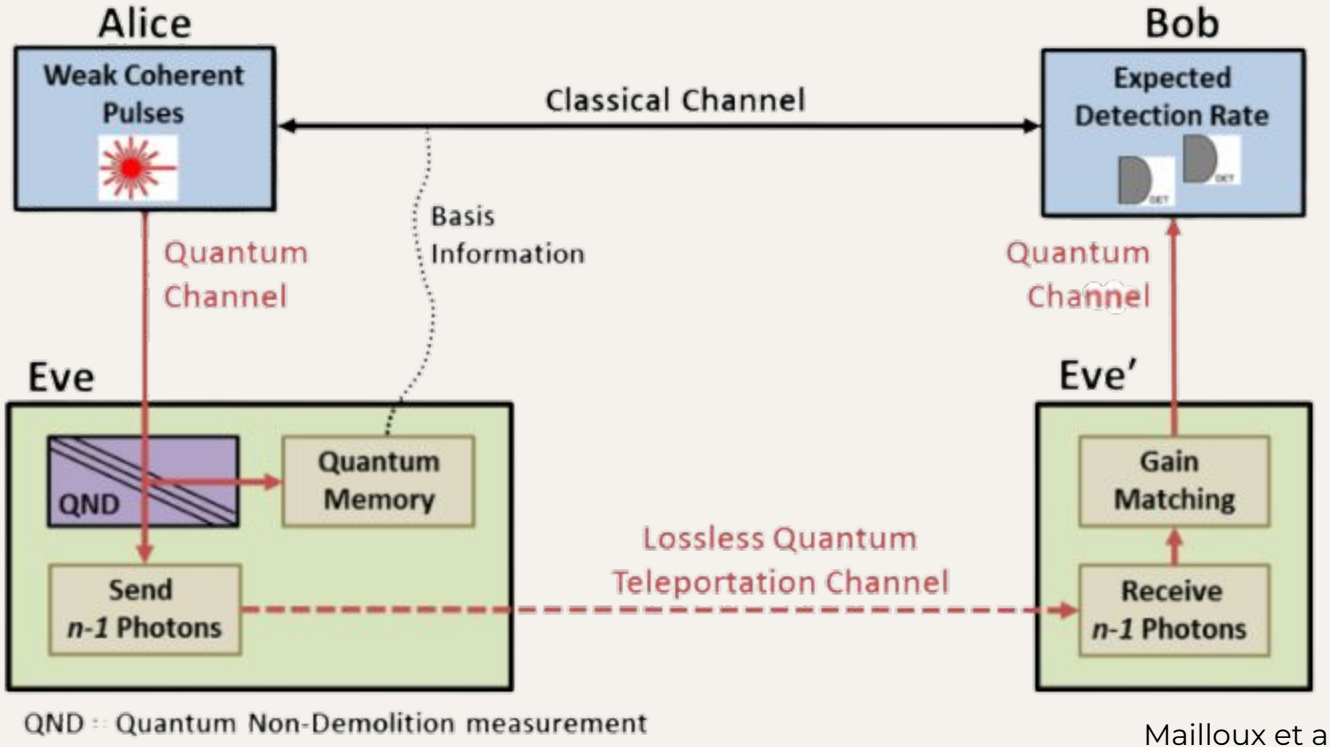
Photon Number Splitting Attack

Photon Number Splitting Attack

- Due to Poissonian nature of laser pulses, Alice might generate multi-photon pulses ➡ loophole!
- PNS attack is and ideal attack on lossy channel

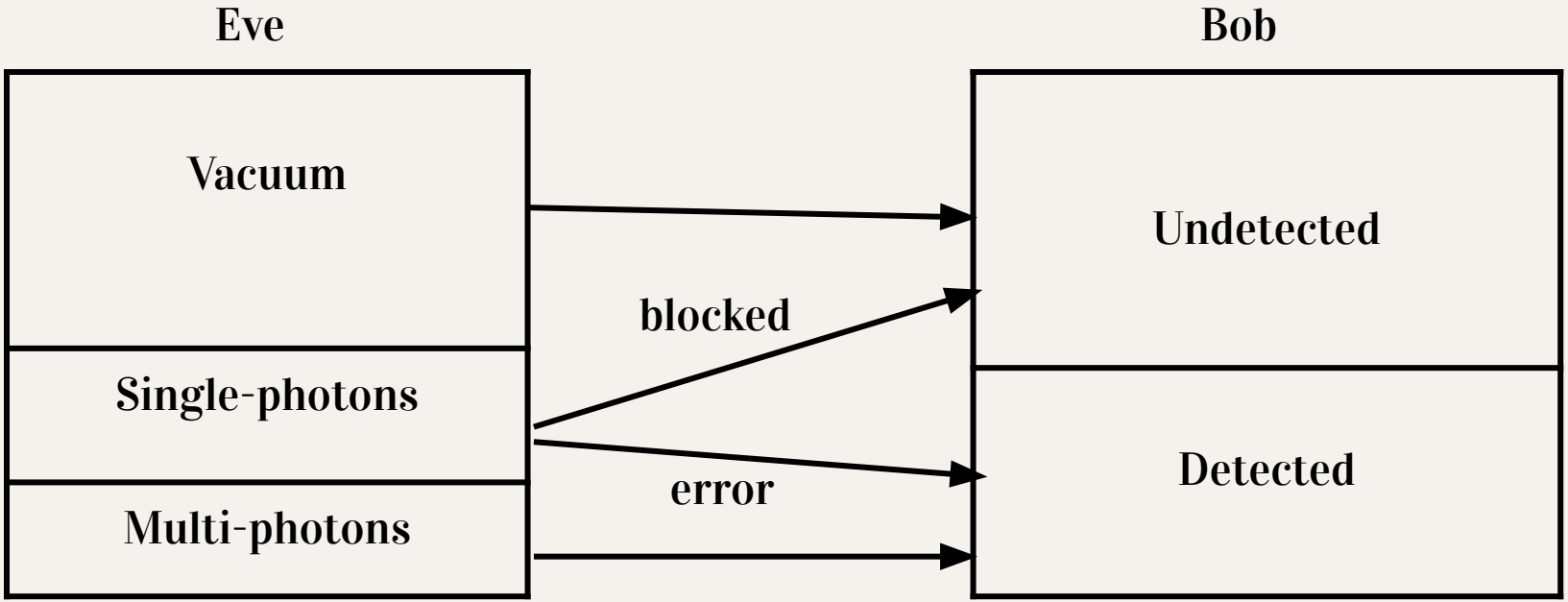
1. Eve replaces the lossy channel with a perfect channel
2. Perform a quantum nondemolition measurement on the total photon number of the pulses without disturbing the polarization
3. Split off one photon from the targeted pulses and make the measurement after Alice announces the polarization basis

Photon Number Splitting Attack



Mailloux et al. 2017

Selection Strategy



Mimicking the lossy channel

Back to Poisson distribution…

Transmittivity of the lossy channel = η ⇒ average photon number = μη

- Vacuum: $P(0) = e^{-\mu\eta}$
- Probability that Bob has a detection = $1 - e^{-\mu\eta}$

Goal: To mimic the detection rate with an ideal channel

⇒Eve has to measure and forward a fraction f of single photon back to Bob

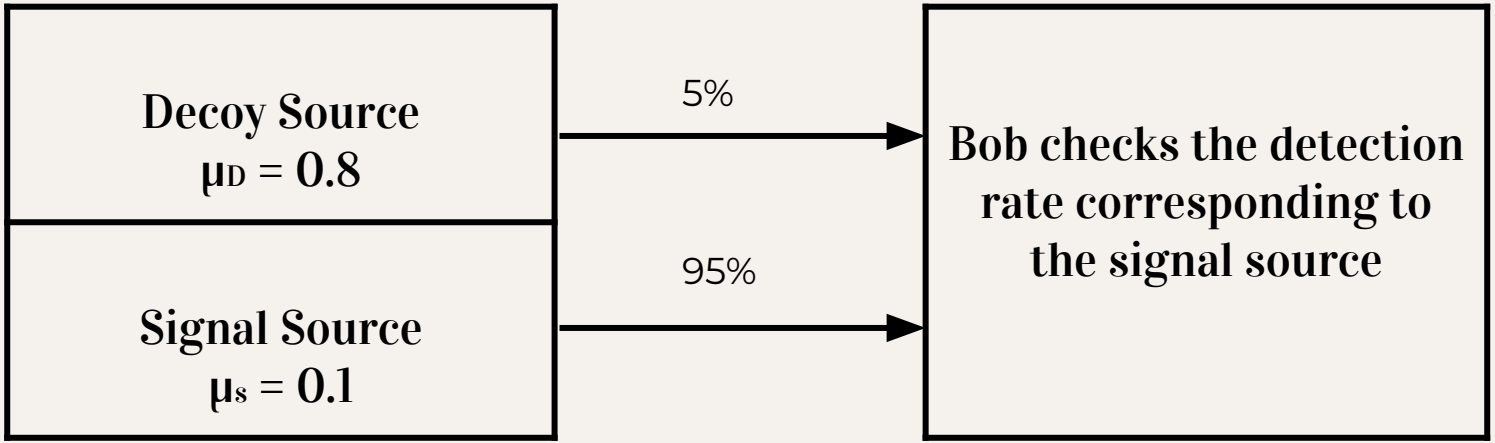
$$f = \frac{(1 - e^{-\mu\eta}) - P(n)}{P(1)}$$

04

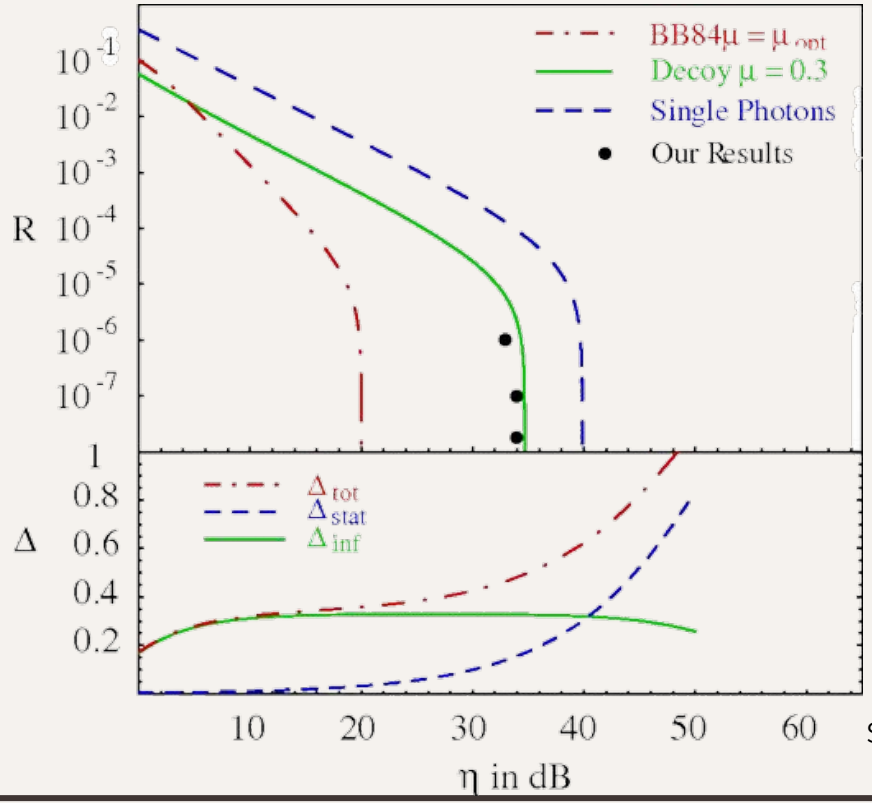
Decoy State Protocol

Counter-attack against PNS

- Alice chooses 2 sources with different average photon number μ
- Decoy source μ_D & Signal source μ_s
- Alice reveals the signal source so that Bob can check the detection rate



Different Protocols



Schmitt-Manderbach et al. 2007

References

1. Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/ijacsa.2018.090354

2. Bruss, D., & Leuchs, G. (2019). *Quantum Information, 2 Volume Set: From Foundations to Quantum Technology Applications* (2nd ed.). Wiley-VCH.

3. Mailloux, L., Grimaila, M., Hodson, D., Engle, R., McLaughlin, C., & Baumgartner, G. (2017). Modeling, Simulation, and Performance Analysis of Decoy State Enabled Quantum Key Distribution Systems. *Applied Sciences*, *7*(2), 212. https://doi.org/10.3390/app7020212

4. Schmitt-Manderbach, T., Weier, H., Furst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J., Zeilinger, A., & Weinfurter, H. (2007). Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *2007 European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference*. https://doi.org/10.1109/cleoe-iqec.2007.4386755