Security of Quantum Cryptography using Photons for Quantum Key Distribution

Karisa Daniels & Chris Marcellino
Physics C191C

Quantum Key Distribution

- QKD allows secure key distribution
- Keys are then used in classical cryptography
  - e.g. One-time pads (XOR with key ≥ length)

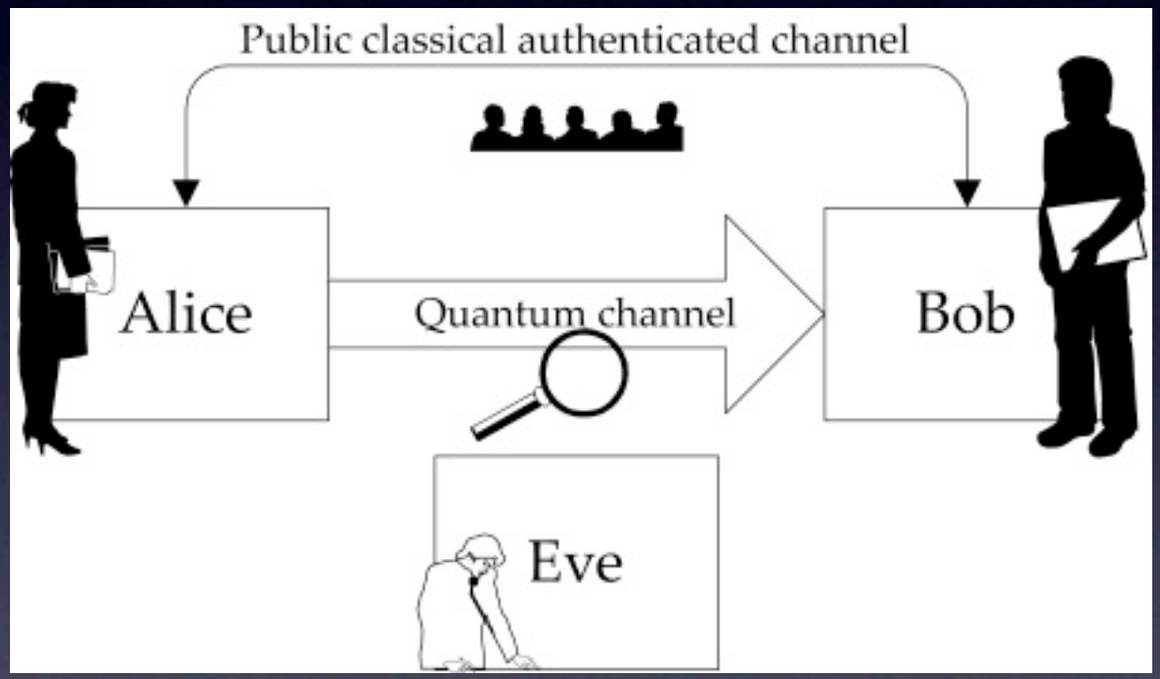
- QKD is all about distributing random keys
- Using the Laws of QM, an eavesdropper can be detected, and the key distribution aborted
- Otherwise, the key is guaranteed to be secure, and used as OTP

BB84

- First QKD algorithm
- Most of QKD/Quantum Cryptography is derived from BB84
- Proven secure given some assumptions
- Practically implementable!

BB84 Review

- Alice encodes random bits {0, 1} in random basis {0/1, +/−}, sends to Bob
- Bob receives bits and measures in random basis
- Alice reveals basis chosen, both compare to see which bits are viable
- Sacrifice portion of successfully sent bits to detect Eve



C. H. Bennet and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, p. 175 (1984).

BB84 Security Assumptions

- Physical security of encoding/decoding devices
- True source of random bits (e.g. Quantum)
- Authenticated classical channel to compare bits
- Reliable single photon emitters and detectors

These last two requirements are hard!

P.W. Shor and J. Preskill, Physical Review Letters 85, 441 (2000)

D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. 4, 325 (2004)

Attacks

- Practical photonic QKD implementations are vulnerable to imperfect assumptions
- Here we describe attacks that are result of difficulties in outputting single photons
  - Photon number splitting attack (PNS)
  - Beam-splitting attack (BS)

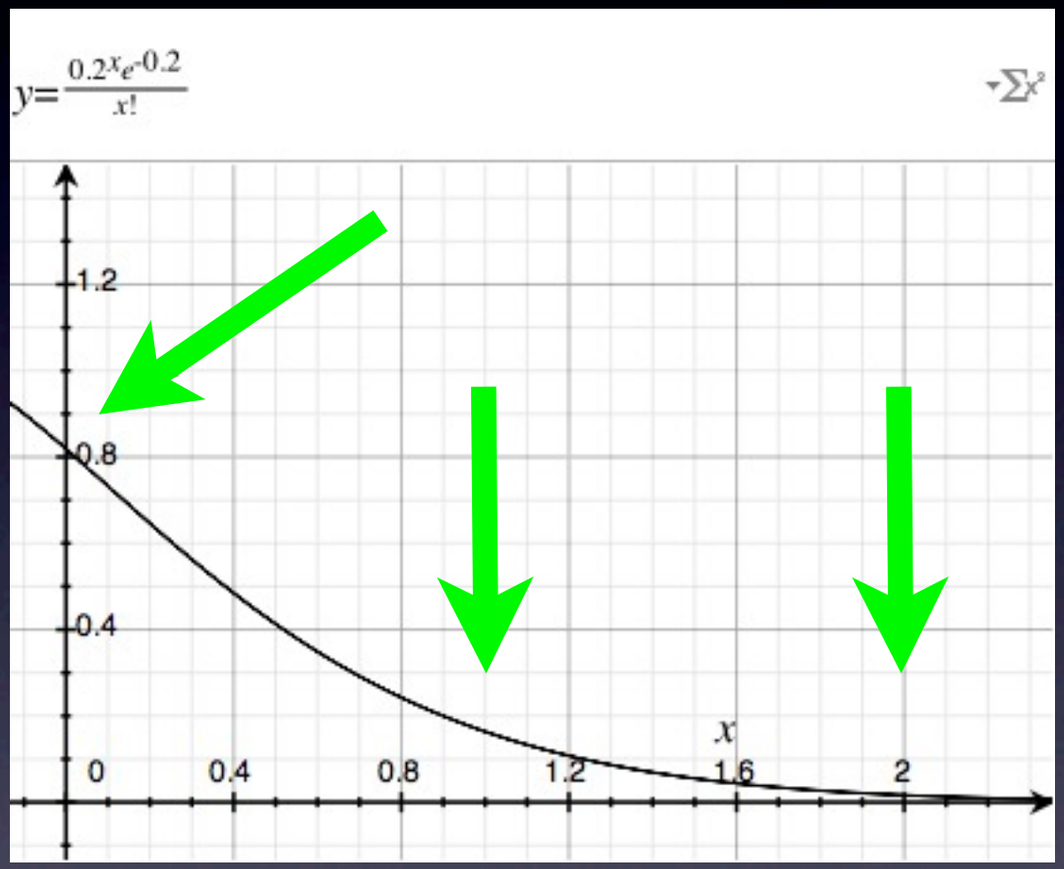
Poisson Approximation to Single Photon QKD

- First practical implementations of QKD (BB84) used attenuated laser light source
- Only option available at the time
- Still used as they are affordable and accessible
- But only an approximation to single-photon source

- The photon emission properties of a laser are described by the Poisson distribution

- We can control the mean of the distribution

- This is termed the ‘mean photon number’



Security aspects of quantum key distribution with sub-Poisson light. Edo Waks, Charles Santori, and Yoshihisa Yamamoto. Physical Review Letters, 66 (2002) 042315

Photon number splitting attack

- This small probability of sending multiple photons gives Eve an opportunity to capture the key
  - Eve captures one photon per each bit sent by Alice
  - She sends along n-1 photons through her ideal network to Bob, *storing* the remaining one for future measurement
  - Hence all transmissions of single photons to Bob get blocked

- During the discussion phase of BB84, Eve measures the captured photons in the basis that Alice reveals to Bob
- Hence, Eve has captured 100% of the key

How can we make this secure?

Potential Solutions

- Decoy Pulse QKD
- SARG04, a minor variation on BB84
- Differential phase shift QKD
- True single photon sources

Decoy Pulse QKD

- Two queues of random bits
  - Signal source typical sub-Poisson source
  - Decoy source is fixed multi-photon source
- Alice randomly interleaves signal bits with decoy bits and sends them to Bob
- Same classical comparison as BB84

Decoy State Quantum Key Distribution. Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen. Physical Review Letters, 94 (2005) 230504

Quantum Key Distribution with High Loss: Toward Global Secure Communication. Won-Young Hwang. Physical Review Letters, 91 (2003) 057901

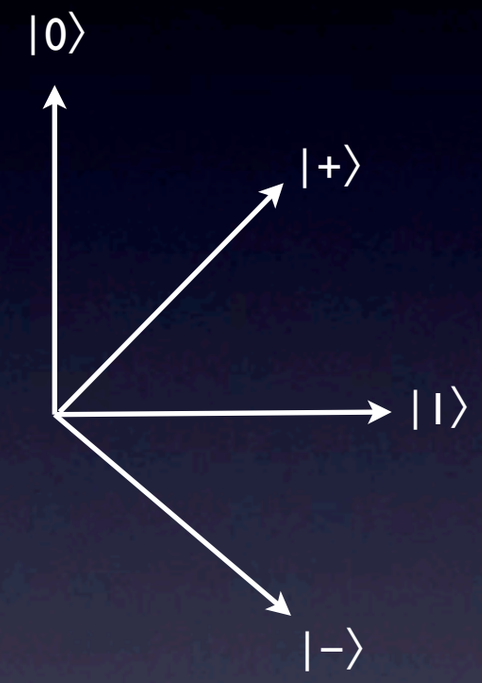
- During the revealing phase Alice looks at the decoy pulse and signal pulse loss
    - If loss of decoy pulse << signal pulse then the process aborted
        - This means that Eve was blocking single photon pulses and she has intercepted keys
    - Otherwise, majority of signal pulses were sent as single photon events and key was delivered securely

SARG04: BB84 with non-orthogonal states

- Just like BB84, Alice is sending one of $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$
- Bob measures in a random basis 0/1 or +/−
- Then, instead of announcing the basis Alice sent her random bit in, she announces the state she sent and one of the two states from the other basis at random

Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Physical Review Letters, 92(2004) 057901

- $|0\rangle$, $|1\rangle$ $\Longrightarrow$ classical bit "1"
- $|+\rangle$, $|-\rangle$ $\Longrightarrow$ classical bit "0"
  - This is the non-orthogonal nature of SARG04



- Bob only gains knowledge of Alice's qubit when he encounters a complete contradiction of his measurement basis and her broadcast pair

Example:
Alice sends $|+\rangle$ (“0” classical)

Bob measures in 0/1 basis and gets $|1\rangle$

Case 1:
Alice reveals $A_{+,1}$
Bob knows that he could have measured $|1\rangle$
either because Alice did or by chance
Result must be discarded

Case 2:
Alice reveals $A_{+,0}$
Bob sees that his result contradicts Alice’s statement, therefore he knows that Alice chose $|+\rangle$ which is classical “0”

SARG04 defeats the storage attack

- Since Alice no longer announces the basis used to transmit, Eve can't take advantage of the stored photons
- Now, she has only 50/50 odds of guessing the correct basis, since the classical values "0" and "1" lie in non-orthogonal bases, respectively.

Differential phase shift QKD

- Alice sends a coherent train of pulses all randomly modulated between {0,π} to Bob using a Poisson distribution
- Bob divides each pulse into two paths and then recombines them using a beam splitter
- When the beams are recombined the phase difference between the two pulses will either be 0 or π

Influence of multi-photon pulses on practical differential-phase-shift quantum key distribution. Zhao Feng, Fu Ming-Xing, Lu Yi-Qun and Liu Song-Hao. Chinese Physiscs, 16, 3402 (2007)

- When Eve applies the PNS attack, the possible number of photons found in each pulse changes to exactly 0 or 1, instead of a Poisson distribution

- This introduces bit errors into the recombined pulse that Bob receives, when Bob measures his states he can detect Eve

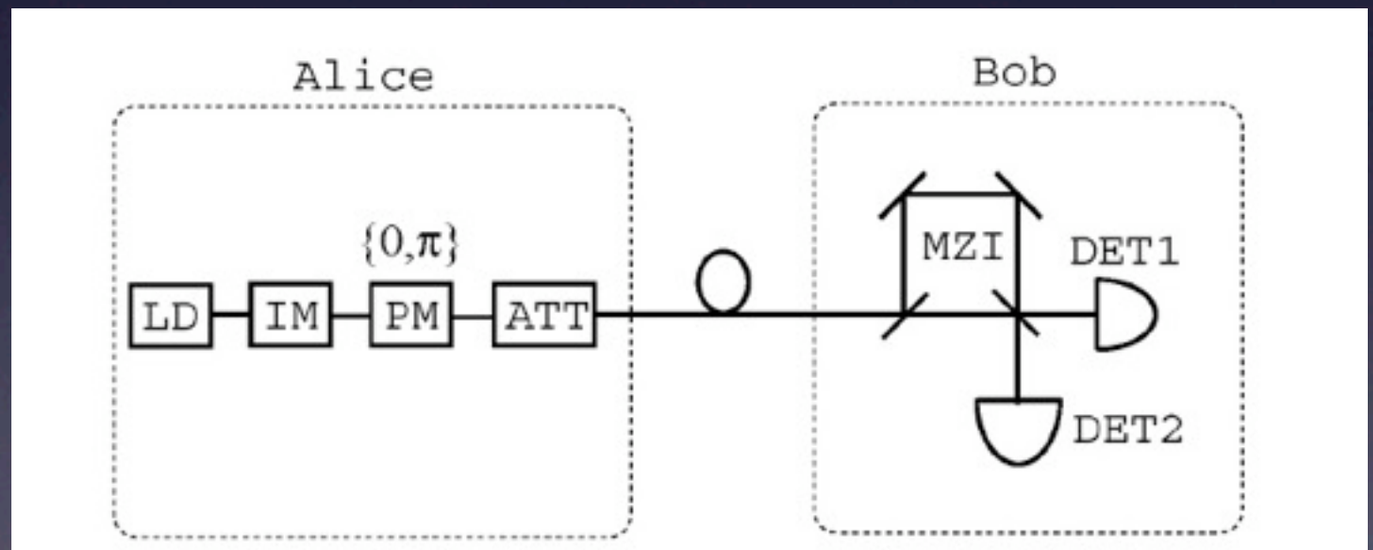


Fig. 1. Schematic diagram of differential-phase-shift QKD. LD, laser diode; IM, intensity modulator; PM, phase modulator; ATT, attenuator; MZI, Mach-Zehnder interferometer.

Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers. Toshimori Honjo, et al. Opt. Express 17, 9053-9061 (2009)

DPS-QKD still susceptible to Beam Splitting attack

- Eve takes advantage of the long distance that the photons have to travel between Alice and Bob
    - She inserts a beam splitter into Alice and Bob's path and diverts the photons
    - Eve keeps a portion of the beam and sends the rest on to Bob through a lossless channel (making the loss undetectable)
    - BS attacks do not introduce any errors to the system

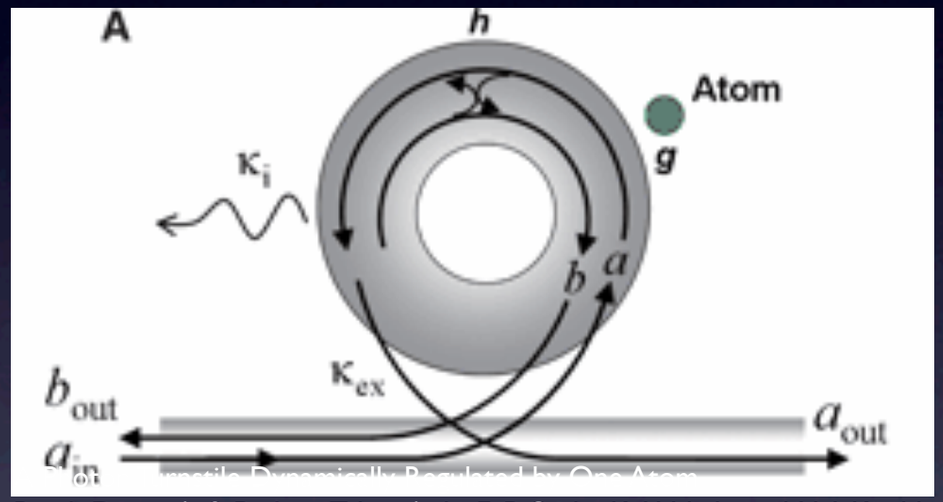
- Transmission distance is not limited by BS attacks in differential phase shift QKD
  - The probability that Eve intercepts information increase as the mean photon number increases, but remains the same for different transmission distances
- PNS and BS cannot limit the transmission distance as long as an appropriate mean photon number is selected

True single photon sources

- Research in this area is limited and recent
- Performance scales linearly as with DPS-QKD, except imperfect material properties limit throughput over long distances
- Even if a reliable single photon source were discovered there are still transmission/ throughput limits inherent in practical implementation

Example

- Single atom in turnstile controls the output of photons
  - Resonance controlled
- Other designs use quantum dots which have ~100% emission when excited



Barak Dayan, A. S. Parkins, Takao Aoki, E. P. Ostby, K. J. Vahala, and H. J. Kimble (22 February 2008) Science 319 (5866), 1062.

A Quantum Dot Single-Photon Turnstile Device. P. Michler, A. Kiraz, C. Becher, W.V. Schoenfeld, P. M. Petroff, Lidong Zhang, E. Hu, A. Imamog (22 December 2000). Science 290 (2282)