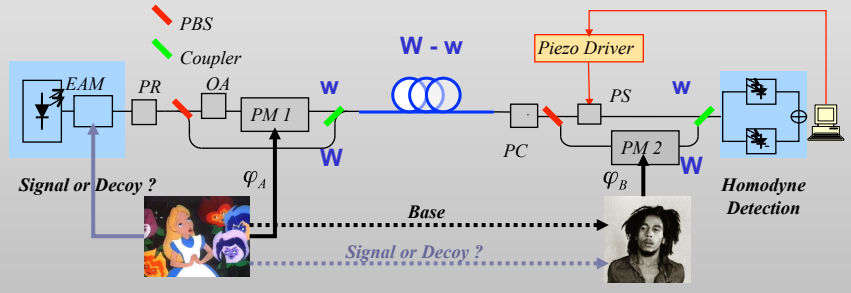
Application of the decoy-state (DS) technique in QKD using BHD



Bit rate of QKD system

- In general: $R = q.p_D.\eta_{pp}$

1) q depends on the QKD protocol
   - q = 0.5 standard 2&4-state BB84 (most QKD systems)
   - q = 1 extended BB84 protocol

2) P_D is the detection prob. of a single photon emitted from the source
   - $P_D = 1 - \exp(-\eta.\mu)$ weak coherent pulse (WKP)

3) η_{pp} is the post processing efficiency

- Post processing (η_{pp}) efficiency to be derived according to the security criterion.

2

Security threats against QKD

1. Individual Attacks (Lütkenhaus [1*])
   - Cause: channel loss
   - Including: intercept and resend attacks, beam-splitting attack, ...
   - a very loose bound on bit rate.

3. 3rd party attacks (Gottesman-Lo-Lütkenhaus-Preskill [3])
   - Cause: source and detector flaws
   - much tighter bound on the bit rate
   - GLLP formula

$$\eta_{pp} = -f(\delta)H(\delta) + (1-\Delta)[1-H(\delta)]$$

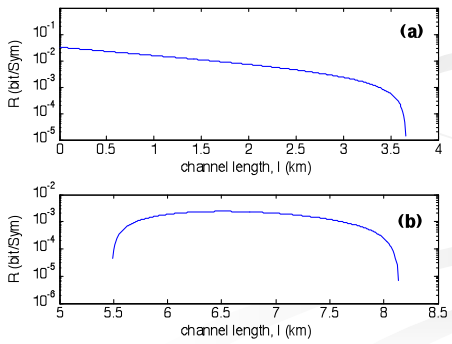
- $\delta = e$ — Quantum bit error rate (QBER)
- $\Delta = P_M / P_D$ — for Poissonian laser pulse
- $f(\ ) \approx 1.22$ — efficiency error correction code
- $H(\ )$ — binary entropy function

3

Secure Transmission Rate

- Adapting the GLLP formula to the BHD system

$$\eta_{pp} = (1-2a)\left[-f(e)H(e) + (1-\Delta)\left[1-H(e)\right]\right]$$



Simulation

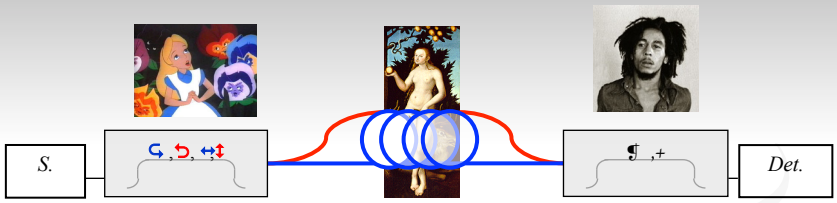
$\mu = 1.65$

a. *Threshold, x = 0.9*

b. *Threshold x = 2*

4

PNS Attack



Eve

1. counts the photon number.
   Quantum Non-Demolition (QND) photon counter
2. blocks all the single photon pulses.
3. splits up all multi-photon pulses, keeps one or several photons, allows the rest to pass
4. keeps μ at Bob's side unchanged
5. keeps the photon number distribution (PND) at Bob's side unchanged

5

Secure Transmission Rate (4/4)

3. PNS attack: (Lütkenhaus and Jahma [2])
   - Cause: non single photon sources
   - Result: extremely low bound on bit rate
   - Solution: Decoy State Technique (Hwang [4])
   - the bound only depends:
     channel length (l) and average photon number (μ)
   - feasible when:

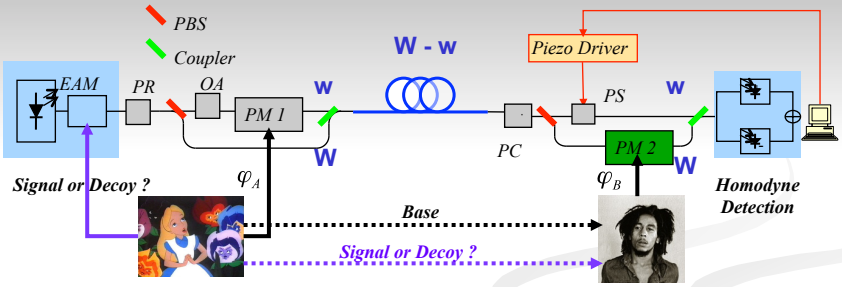
$$(1+\mu+\frac{\mu^2}{2}).e^{-\mu}-(1+\eta\mu).e^{-\eta\mu}\geq 0$$

   - For the case:
     - μ = 1.65
     - α = 0.21

   ⇒ l_{max} = 1.24 km !
   (Decoy State Technique is a must-have!)

6

Decoy State Technique



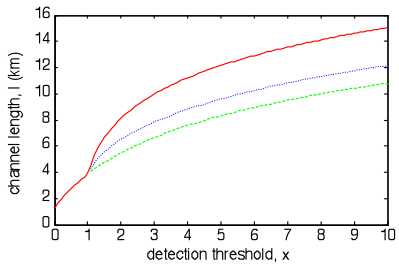
- Alice chooses at random: Decoy State (DS) / Signal State (SS)
- Two coherent states are indistinguishable.
  - So, Eve can not preserve the quantum bit error (QBER) for both of them.
- At the end of the transmission:
  - Alice announces publicly if she has used decoy state or signal state for each qubit.
  - Bob can detect the PNS attack by checking the QBERs.

7

Performance Analysis (simulations)

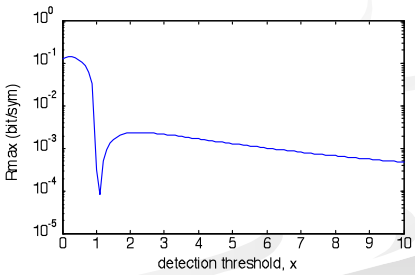
- Several DS's are possible.
- Performance improves by increasing the # of DS's
- We can use DS for the transmission or not.
- The following curves correspond to one coherent state
- In case of using several coherent states for the transmission:

$$R = p_1 . R_1 + p_2 . R_2 + \ldots$$



Simulation

Maximum (red), minimum (green) channel length and the channel length fives maximum bit rate (blue) for the values of thres hold: $0 < x < 10$



Simulation

Maximum transmission rate for the different values of thres hold

8

Performance Analysis (experiment)

- Changing μ is not equivalent to changing the channel length !
- μ is estimated using the Uncertainty Equation:

$$\Delta n.\Delta\varphi \geq \frac{1}{2}$$

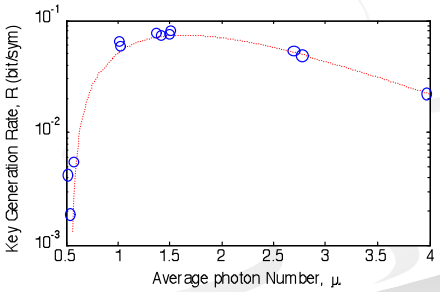
- For the Poissonian laser pulse:

$$(\Delta n)^2 = \mu$$

$$\Rightarrow \quad \mu = \sqrt{\frac{1}{2\Delta\varphi}}$$

- Expressing Δφ in respect to the output voltage:

$$\Delta\varphi = \Pi(\Delta V / V)$$



Simulation and Measurement

bit rate for different values of μ, x = 0.

9