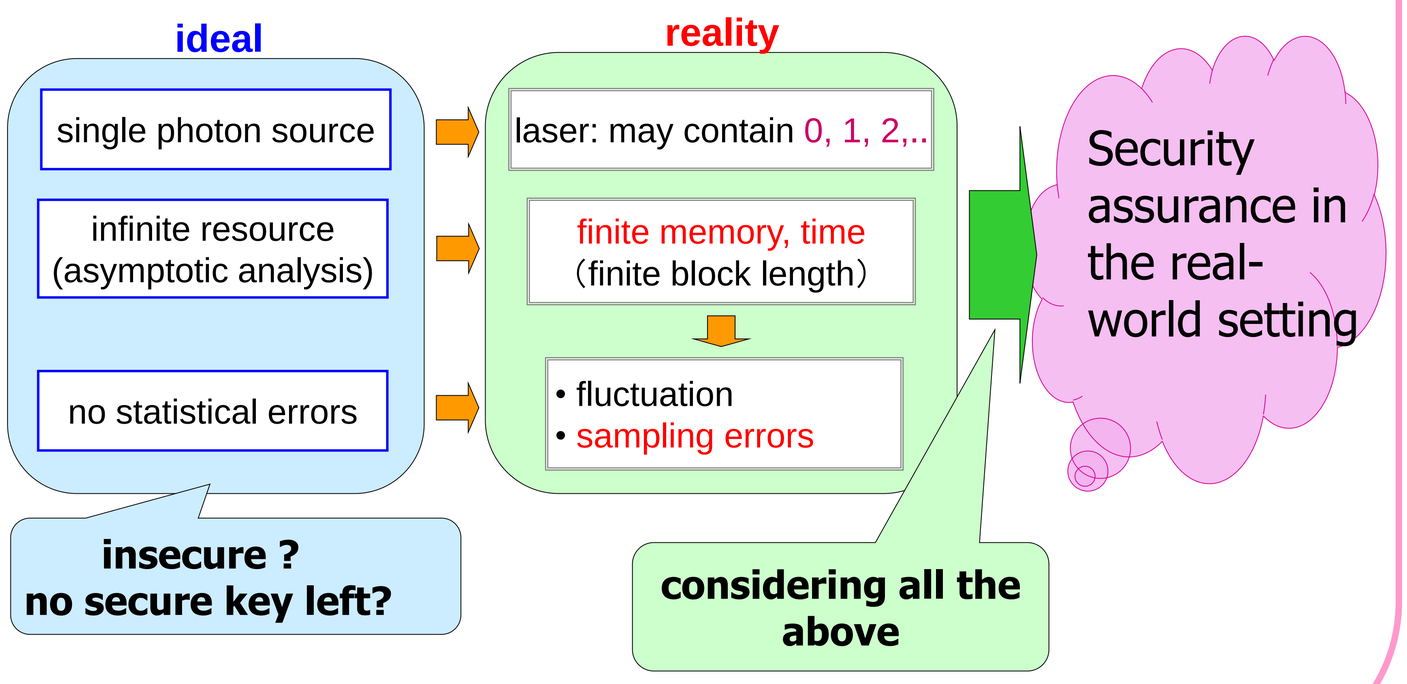
Experimental Decoy State Quantum Key Distribution with Unconditional Security Incorporating Finite Statistics

Jun Hasegawa
ERATO-SORST, JST

Introduction

- Quantum Key Distribution (QKD)
  - Provides a secret shared key between Alice and Bob
  - Eve's eavesdropping disturbs quantum states through quantum channel
  - The amount of leakage information can be estimated from the disturbance
- Asymptotic case (ideal)
  - Unconditional security was proved
  - Some errors can be negligible
- Finite case (reality)
  - Device fluctuation and sampling errors affect security of QKD
  - Useful asymptotic technique (GLLP's key generation rate) cannot be used

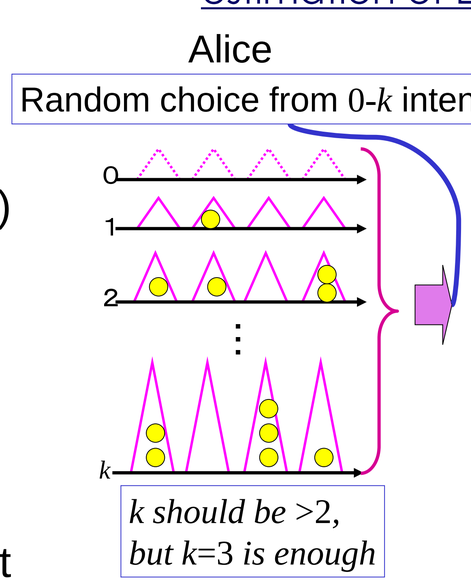
gap between ideal and reality in security analysis



Theory

- Estimation of Eve's information
  - Introduces a security parameter δ to evaluate Eve's information in finite case
  - Improves Eve's information theory with δ by using decoy method QKD (reference [2])
  - Investigate the characteristics of device fluctuation and sampling errors of the finite observed data
- Decoy method QKD [3]
  - Practical solutions with coherent state light pulses, in which several coherent state light pulses with different intensities are used.
  - Secure against PNS attack

Decoy method:
estimation of Eve's strategy



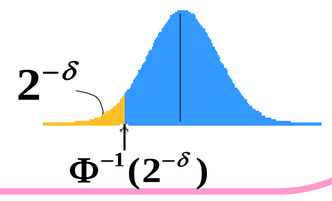
Sacrifice bits

$$m = \tilde{m} - \sqrt{v_r}\,\Phi^{-1}\left(2^{-\delta}\right)$$

$$\tilde{m} = h\left(e_p\right) n_{1,2} + n_{0,2} + n_{2,2} + \delta$$

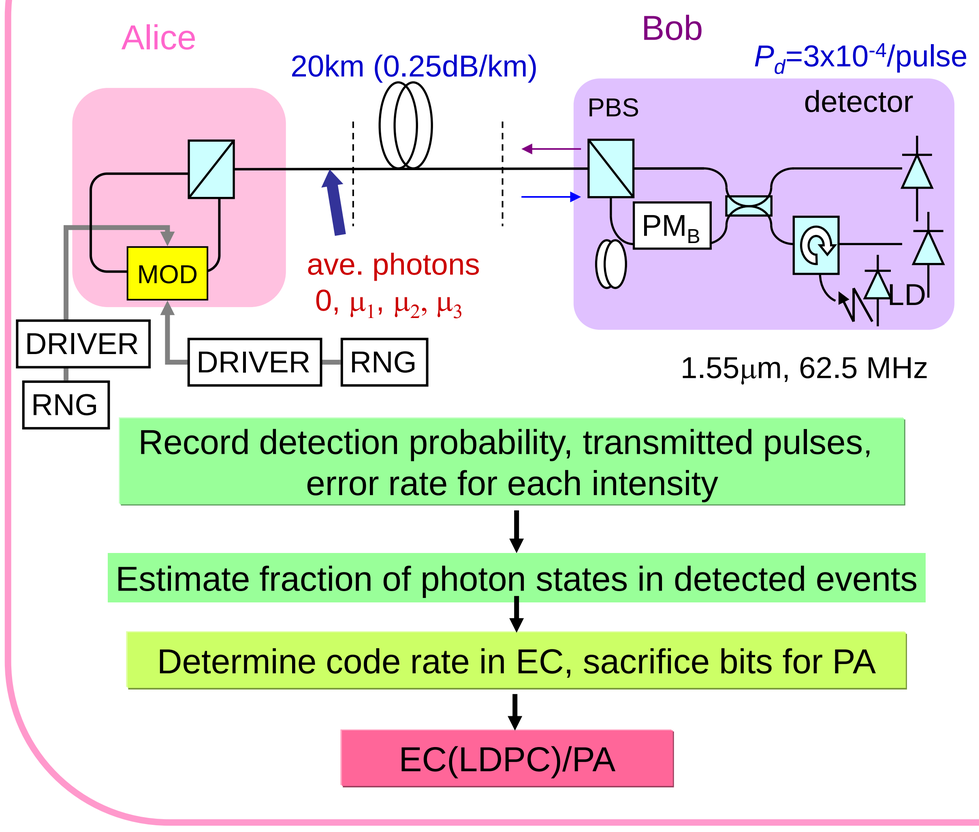
Eve's information on final key $\leq 2^{1-\delta}$

δ: security parameter
v_r: variance of estimated values



Experiment

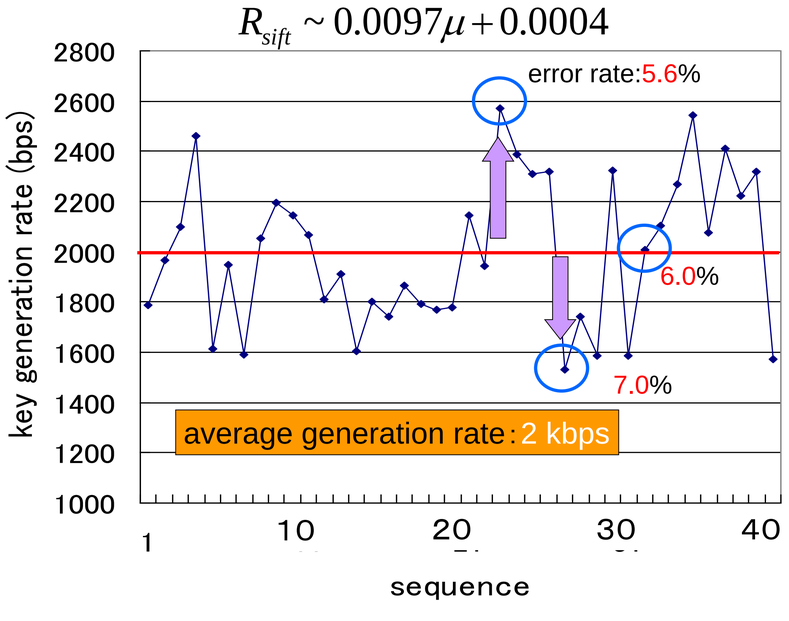
Implementation of decoy method



Final key rate

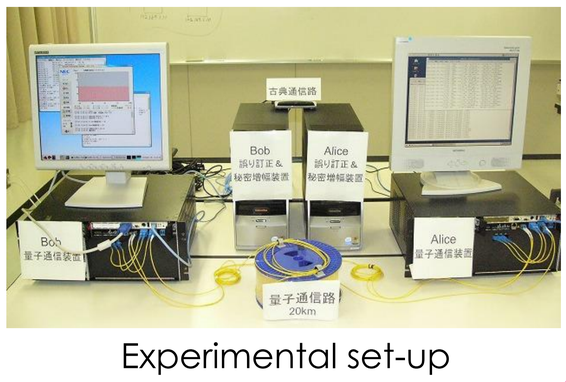
- μ_0,μ_1,μ_2,μ_3=0, 0.07, 0.35. 0.5
  μ_3=0.5 used for key generation
- code length 100,000 bits
- security parameter δ=8

$$R_{sift} \sim 0.0097\mu + 0.0004$$



Conclusion

- The **first secure** key generation with quantitative assurance
- The final key rate was 2 kbps after 20 km fiber transmission; the maximum leaked information on the final key : 2^{-7}
- Decoy method will also improve the final key rate with an imperfect single photon source



Experimental set-up

[1] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita, Proc.. of AQIS'07, 77-78 (2007).
[2] M. Hayashi, PRA**76**, 012329 (2007). [3] W.-Y. Hwang PRL**91**, 057901 (2003).