Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse

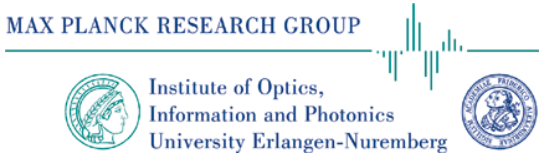
Reference: quant-ph/0607082

Kiyoshi Tamaki

(NTT Basic Research Laboratories, NTT corporation, & CREST, JAPAN)

Collaboration with

N. Lütkenhaus, M. Koashi, and J. Batuwantudawe



Talk at CQIQC II on August 8th, 2006

Outline of my talk

- Motivations for the study of the B92 with strong reference pulse
- Introduction of the B92 with SRP
- Outline of the security proof
- Security examples
- Summary

Motivations

For longer distances of QKD….

- Decoy state for BB84 W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

・In addition to the signal light, Alice and Bob use "decoy states" that has the same property except for the intensity of light.

→ Giving a good estimation of Ratio of event that Alice emits 1-photon & Bob detects 1-photon is well estimated!!

Data processing in practice is a bit tedious L

- B92 with strong reference pulse C. H. Bennett, Phys. Rev. Lett, **68**, 3121 (1992).

・ We use only the signal light. (data processing should not be tedious)

・ The simplest protocol (we use only two nonorthogonal states)

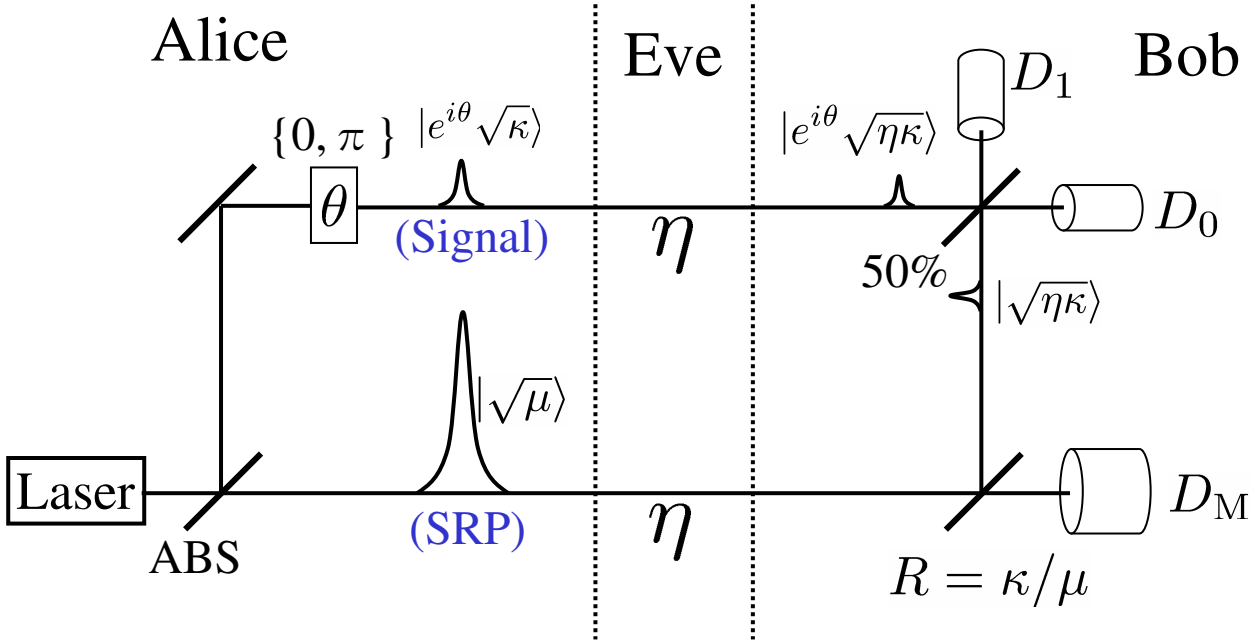
→ Other essencial points for the security is expected to obtain.

The security proof of the B92 with strong reference pulse is important, not only from practical viewpoint, but also from fundamental one.

B92 with strong reference pulse scheme

The essence of the B92 with SRP.

(In the experiment, we use double Mach-Zehnder interferometer)



Θ=0; D_0:$|\sqrt{2\eta\kappa}\rangle$ D_1: vac

$\Theta = \pi$; D_1 :$|\sqrt{2\eta\kappa}\rangle$ D_0 : vac

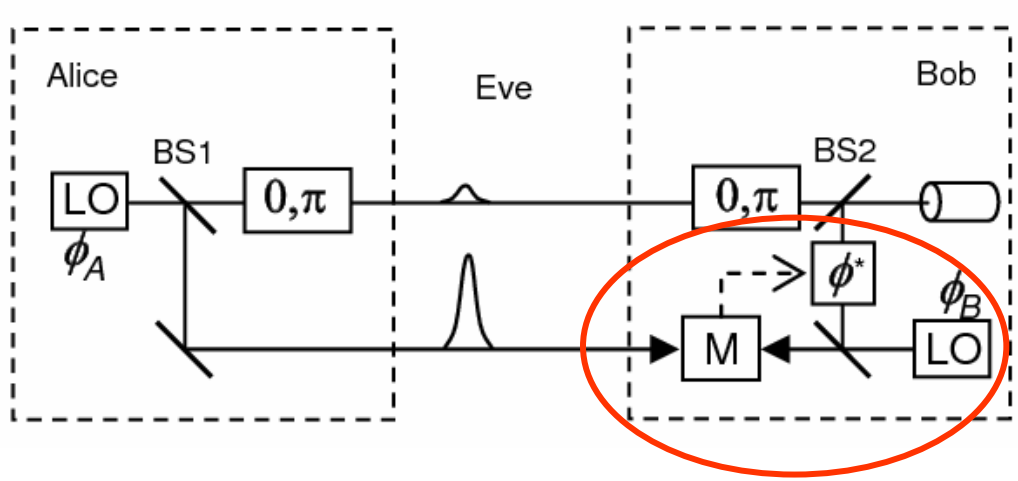
Click on one detector means conclusive

Bob has to broadcast if he got the conclusive event or not.

No click means inconclusive

Remark: Differences from Koashi's scheme

Koashi's scheme



Feed-forward control

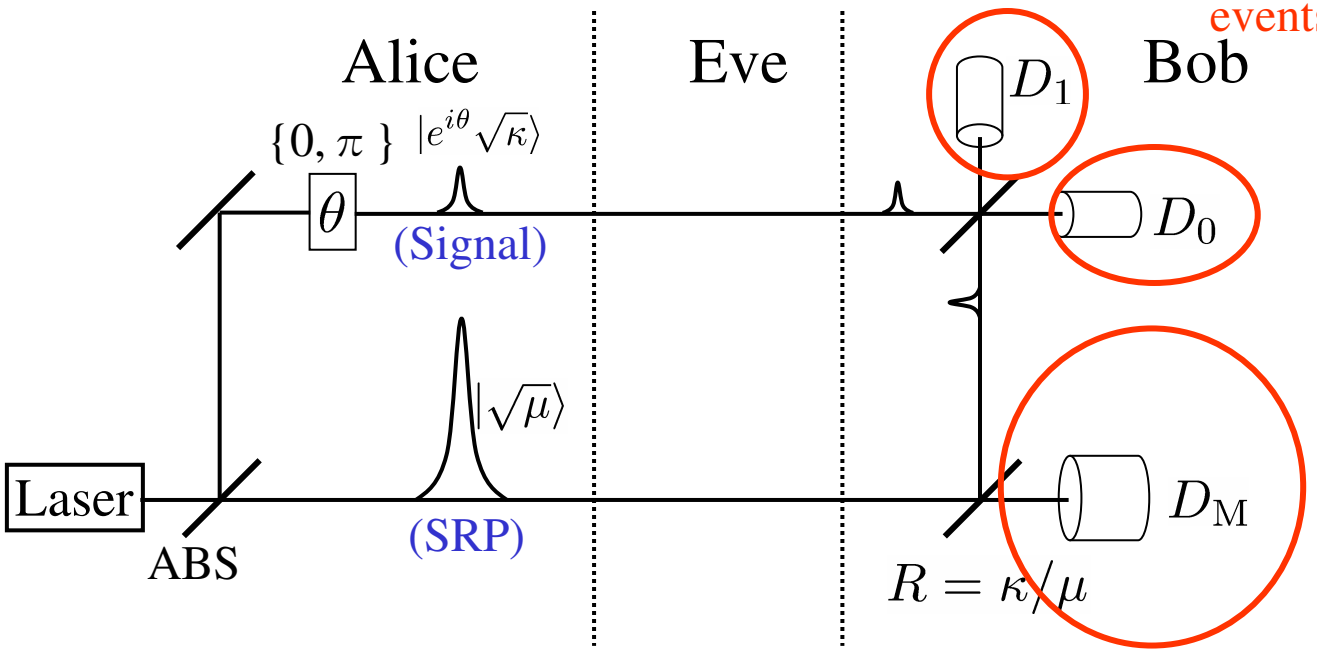
M. Koashi, *PRL*. **93**, 120501 (2004)

(1) Koashi's scheme requires a feed-forward control, while our scheme does *NOT* need it.

(2) In Koashi's scheme, we can use a *threshold* detector while our scheme requires detectors with assumptions that I mention later.

Assumptions

(2) Each of them discriminates among vacuum, single-photon, and multi-photon events.



(1) This detector resolves if the photon number is in a particular range or not, i.e. ,

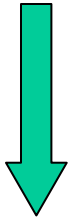
$$\nu \in [\nu_i, \nu_f - 1] \equiv \lambda^{(D_{\rm M})}$$

(3) All imperfections are under Eve's control.

Conclusive event: D_0 and D_1 detect a single-photon in total while $D_{\rm M}$ detects a photon number inside $\lambda^{(D_{\rm M})}$

Outline of the proof

The B92 is viewed as running many single-photon B92.



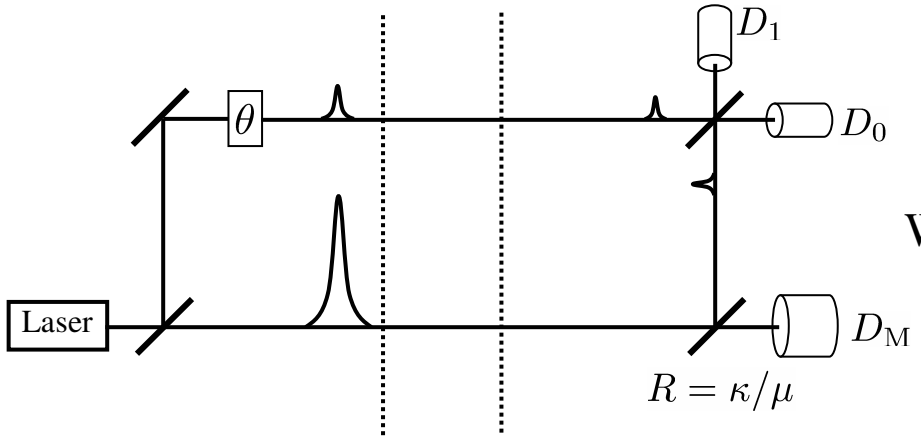
By applying the security proof of the single-photon B92 jointly, we are done.

Security proof for the single-photon B92

K. Tamaki, M. Koashi, N. Imoto, PRL. **90**, 167904 (2003)

K. Tamaki, and *N. Lütkenhaus*, PRA **69**, 032316 (2004)

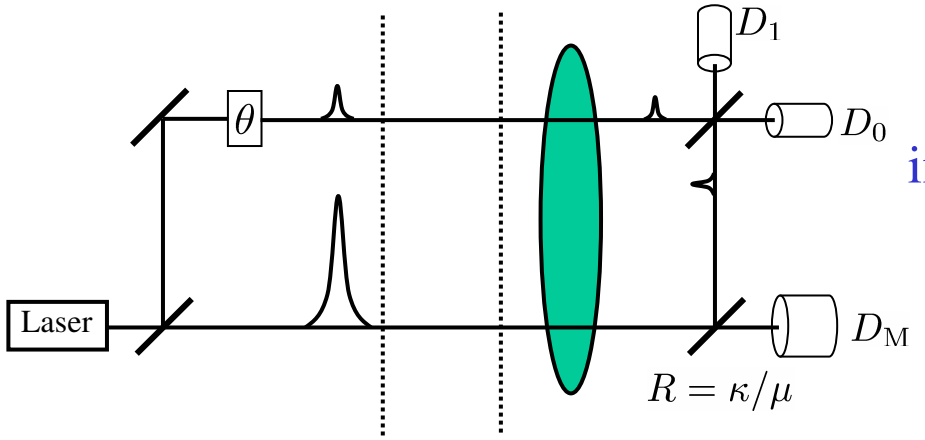
Observation I



We perform photon counting measurement in the end!!

Observe that a beam splitter conserves the total photon number

$U_{BS} = \oplus_{i=0}^{\infty} U_i$ U_i: an unitary operator working on the i-photon Fock space



in the sense that they have the same statistics for any input state!!

P_{j+k}: total photon number counting

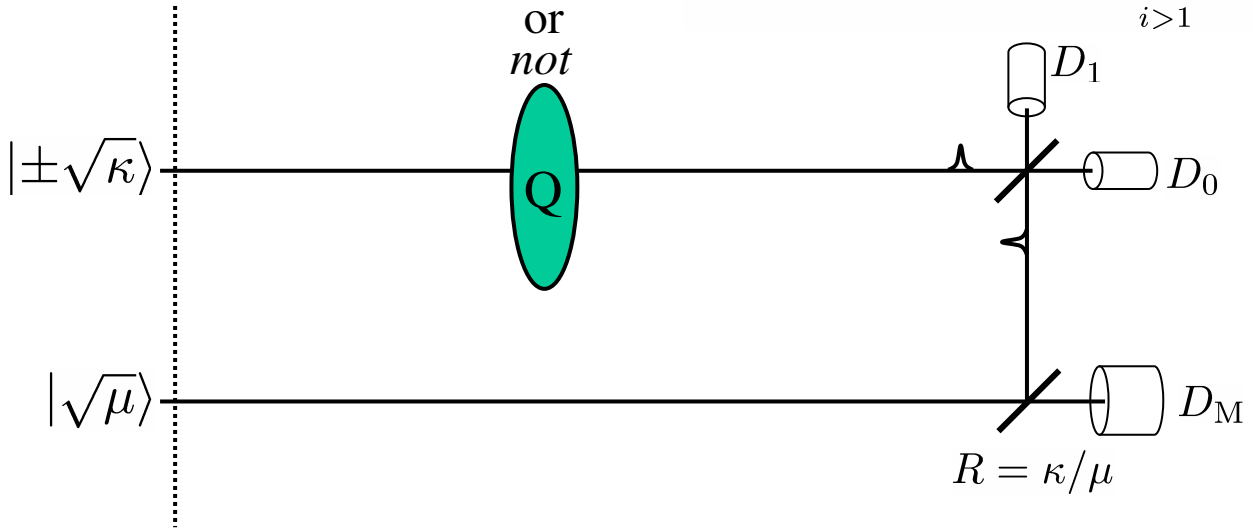
We can safely assume that we perform the projection, even if we do not so in practice!!

Observation II

Conclusive event: D_0 and D_1 detect a single-photon in total while $D_{\rm M}$ detects a photon number inside $\lambda^{(D_{\rm M})}$

Conclusive events do not contain more than 1photon

{Vac,Single} $Q = \{|vac\rangle\langle vac| + |1\rangle\langle 1|, \sum_{i>1} |i\rangle\langle i|\}$

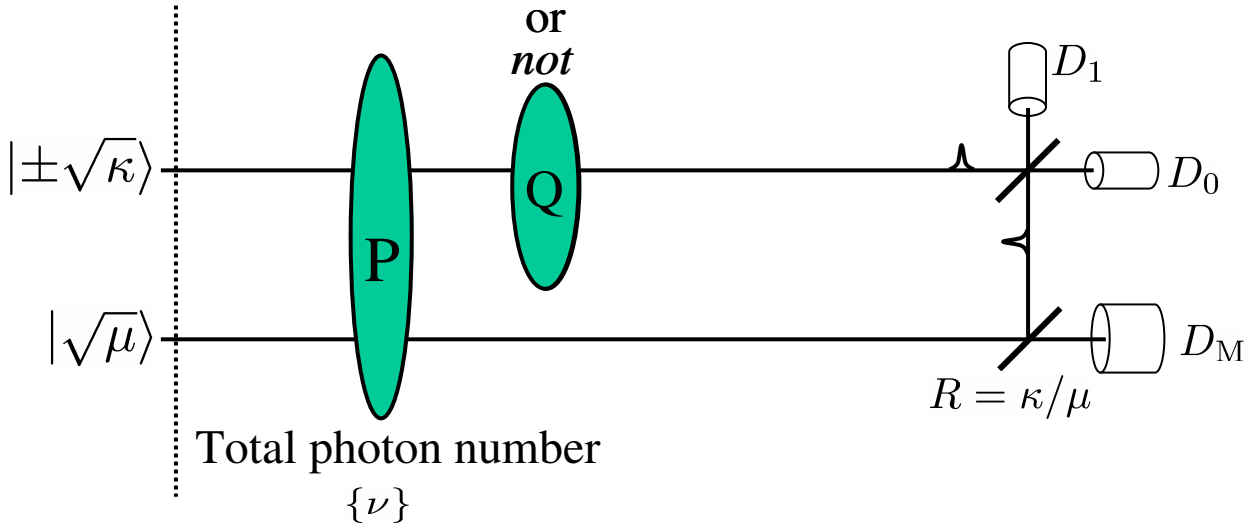


Q does ***not*** disturb the statistic of the conclusive events (distribution of "0" and "1") and the ratio of conclusive and inconclusive. Yes, Q ***does*** disturb the statistic of inside the inconclusive events (distribution of which of D0 or D1 clicks), but we do not care !!

Thus, as far as we distill a key from the conclusive events, we can safely assume that we perform Q, even if we do not do so in practice!!

Conversion of the B92 to an EDP protocol

Conclusive events contain
either 0 or 1-photon
$\{|0\rangle, |1\rangle\}$: Qubit

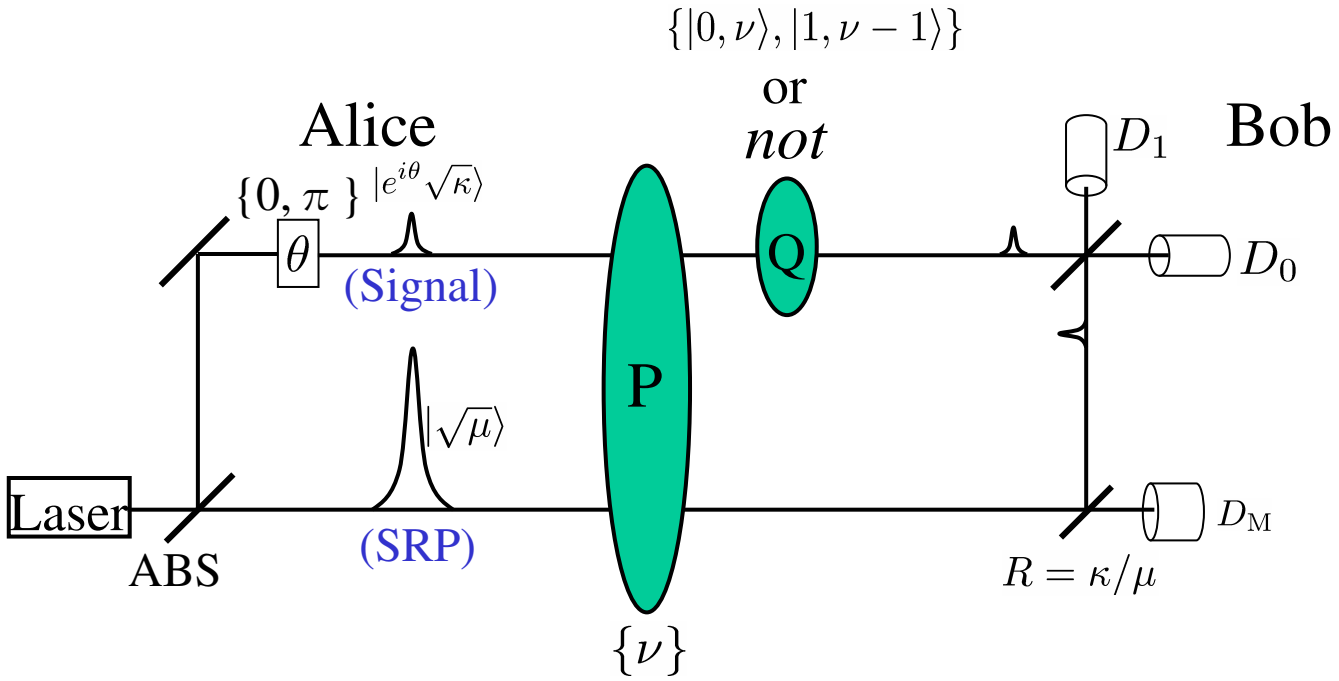


We know how to prove the security of B92 with single-photon.

K. Tamaki, M. Koashi, N. Imoto, PRL. **90**, 167904 (2003)
K. Tamaki, and *N. Lütkenhaus*, PRA **69**, 032316 (2004)

The security of the B92 is proven by considering how we treat many single-photon B92 jointly.

Remark

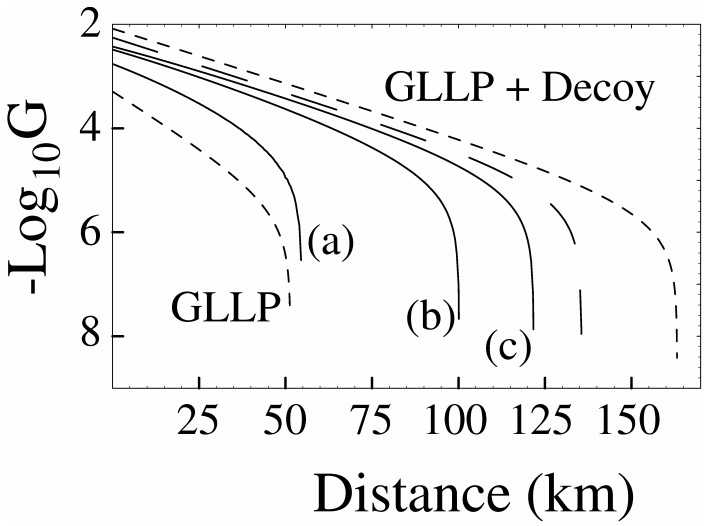


- A qubit contains vacuum & a single-photon state.

Even if the fiber is highly lossy, Bob is very likely to have a qubit!!

Big difference from the single-photon B92 !!

Security examples



Experimental data is taken from C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004).
(We neglect alignment errors.)

(a): 55km, μ =10^5, κ = 10^(-0.92), D_{M}= [260, 370] (at 55km) $\nu_{f/i} = \eta\nu \pm \sqrt{\eta\nu}$

(b): 100km, μ =10^(6.59), κ = 10^(-0.92), D_{M}= [1200, 1440] (at 100km)

(c): 122km, μ =10^(10), κ = 10^(-0.92), D_{M}= [1.230 10^6, 1.237 10^6] (at 122km)

GLLP: 51km

GLLP + Decoy: 163km G$\sim$ O(η)

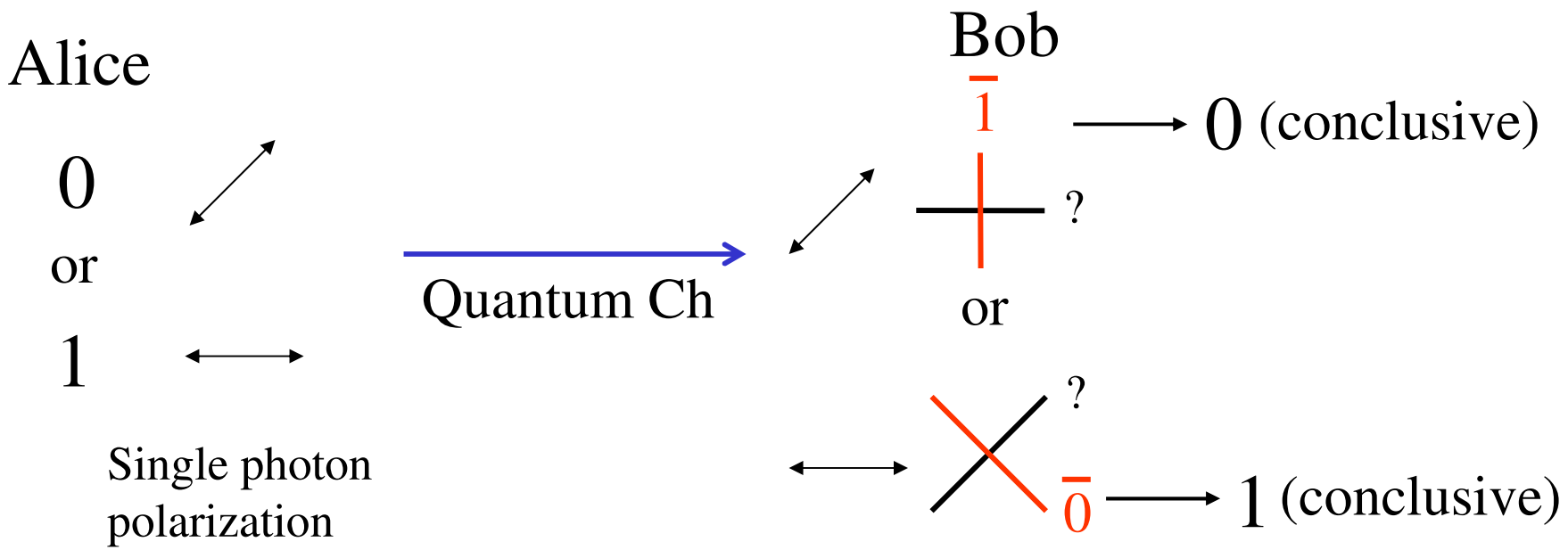
As we use stronger μ , G_{B92} approaches to O(η)

Summary of my talk

- We prove the unconditional security of the B92 with strong reference pulse.
- The B92 is viewed as running many single-photon B92 parallel.
- With proper choice of experimental parameters, the B92 achieves the key rate $\sim O(\eta)$
- It is interesting to consider how we replace the detectors with the discrimination among a vacuum, single-photon, and multi-photon to a threshold detector.

This talk is based on quant-ph/0607082

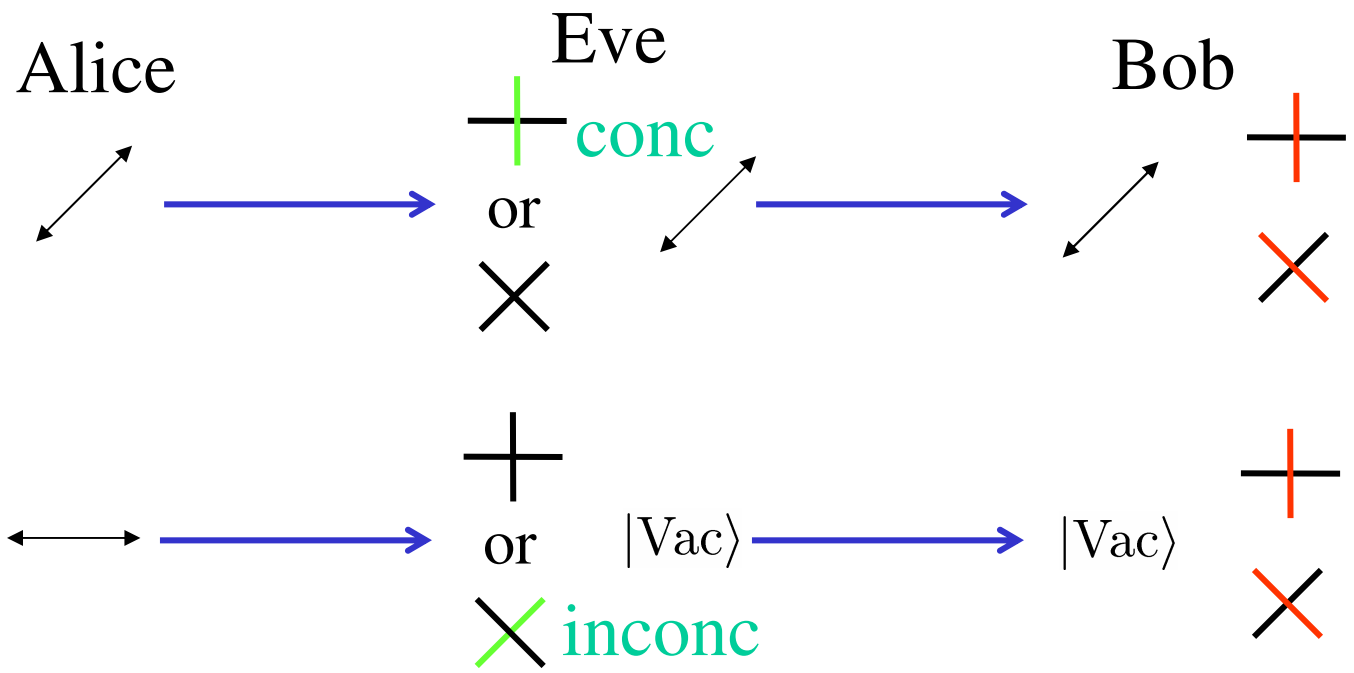
Introduction to polarization based B92 (No Eve, noises, and loss cases)



Bob broadcasts whether he got the conclusive result or not

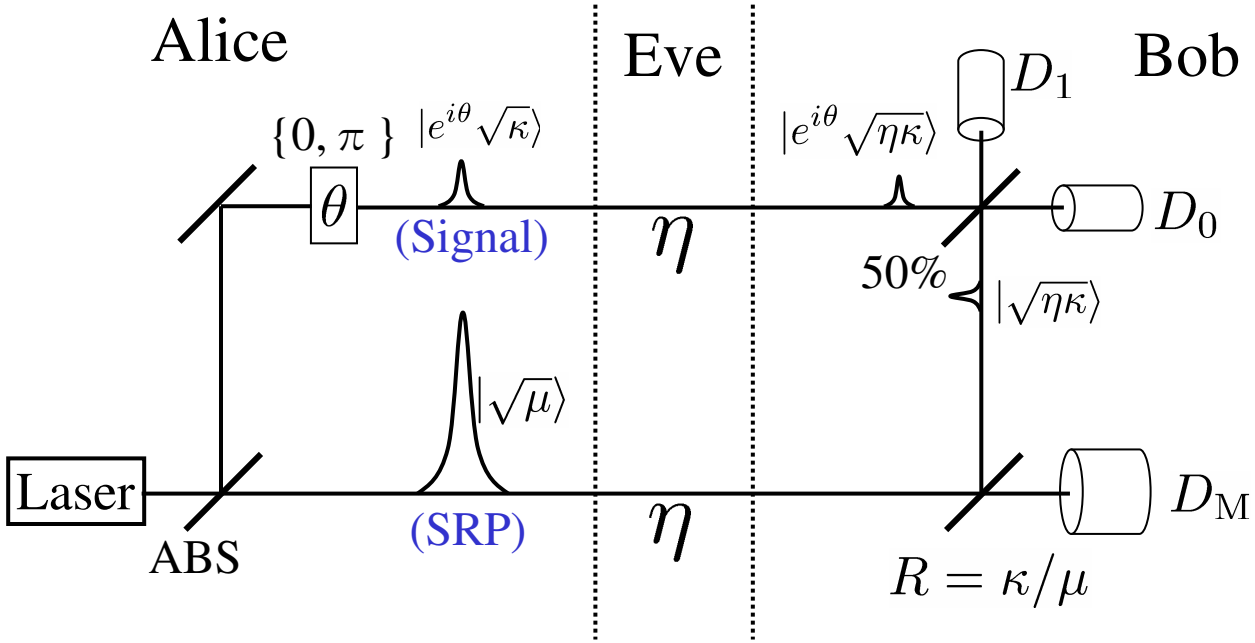
C. H. Bennett, Phys. Rev. Lett, **68**, 3121 (1992).

Defects of B92 (over lossy channel)



In the experiment with high loss rate, we cannot achieve long distance of communications.

A eavesdropping attack



1. Eve can employ a measurement that discriminates $|\sqrt{\kappa}\rangle$ and $|-\sqrt{\kappa}\rangle$

An USD attack on the signal light causes a random click (a bit error)

2. If she fails, then she sends the vacuum state.

➡ We expect that the B92 with SRP is robust against losses