Security of
Phase-encoded BB84 protocol

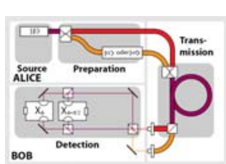
Agnes Ferenczi, Varun Narasimhachar, Norbert Lütkenhaus

Institute for Quantum Computing
University of Waterloo
Canada

Security and Modelling

Actual Device
e.g. reality based

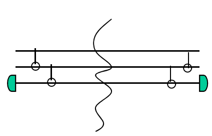
modelling



Quantum Optical Model
e.g. mode based

e.g. realistic sources (laser pulses)
threshold detector models

reduction to essentials
tagging, squashing



Securi Model
e.g. qu based

entanglement distillation (Bennett96,Deutsch et al, Lo)
information theoretic (Renner)

$||\rho_{ABE} - \rho_{AB} \otimes \rho_C||_1 \le \epsilon$

Security Proof

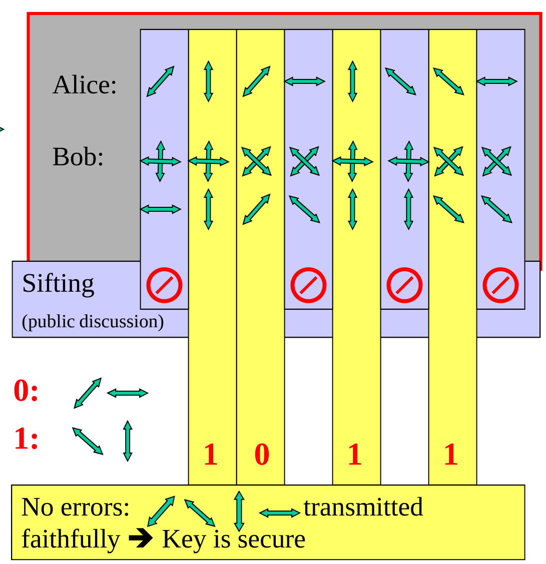
Universally composable security proof:
perfect key with exception of a probability ϵ

Basic Protocol

Bennett Brassard Protocol (1984)

Quantum Part:
Create random key:
➔random signals
➔random measurements

Public discussion over faithful classical channel: distinguish **deterministic** from **random processes**



General Key Formula

$$G(X_A, Y_B) = \min_{\rho_{AB} \in \Gamma_{AB}} \left\{ \underbrace{H(X_A) - H(X_A|Y_B)}_{\text{Shannon mutual information } I(A:B)} - \underbrace{\left(S(\rho_E) - \sum_{a \in X_A} p(a) S\left(\rho_E^{(a)}\right) \right)}_{\text{Holevo quantity } \chi(A:E)} \right\}$$

Shannon mutual information
I(A:B)

Holevo quantity
χ(A:E)

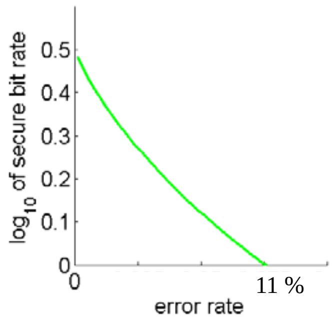
Evaluation for BB84 protocol:

[Mayers; Shor, Preskill;Renner]

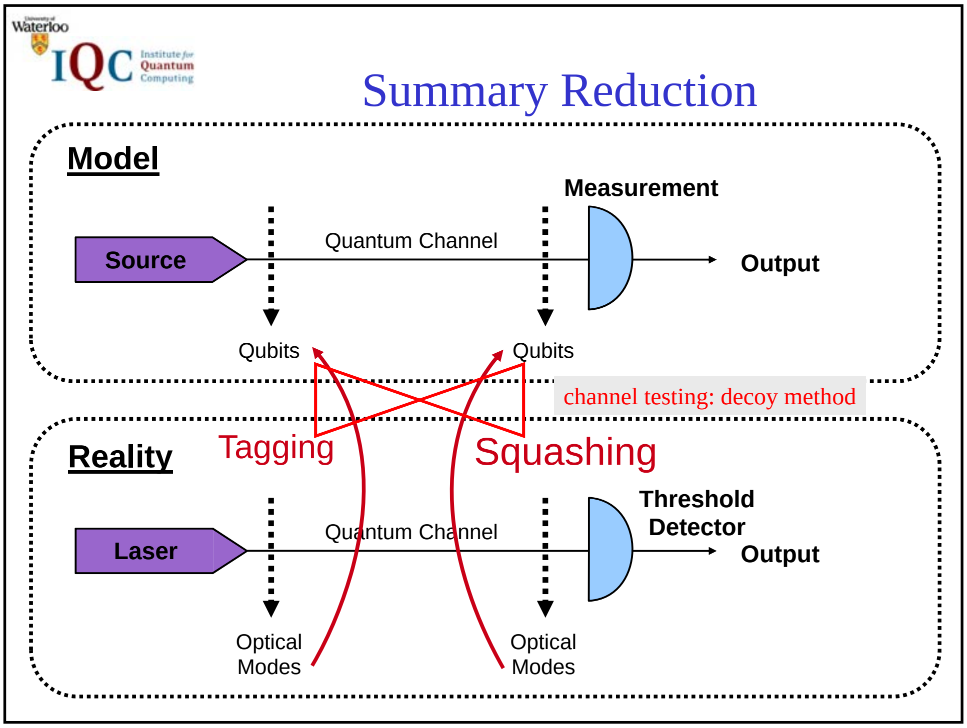
$$G = \frac{1}{2}\left(\underbrace{1 - h[e]} - h[e]\right)$$

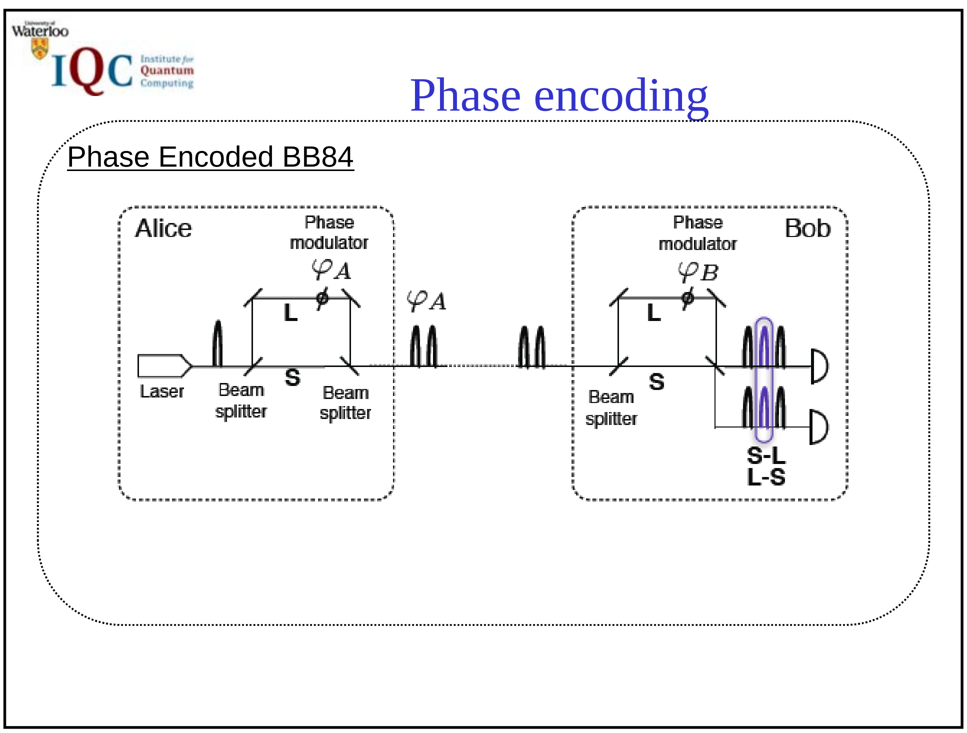
Shannon information
(error correction)

Holevo Quantity
(privacy amplification)

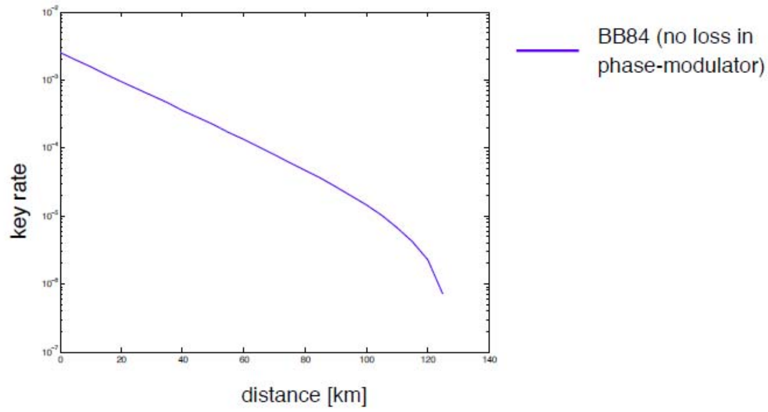


Quantum optical modeling & BB84 protocol


Waterloo
IQC Institute for Quantum Computing
Summary Reduction
Model
Measurement
Source
Quantum Channel
Output
Qubits
Qubits
channel testing: decoy method
Reality
Tagging
Squashing
Threshold
Detector
Laser
Quantum Channel
Output
Optical
Modes
Optical
Modes


Waterloo
IQC Institute for Quantum Computing
Phase encoding
Phase Encoded BB84
Alice
Phase
modulator
φA
L
Laser
Beam
splitter
S
Beam
splitter
φA
Phase
modulator
Bob
φB
L
Beam
splitter
S
S-L
L-S

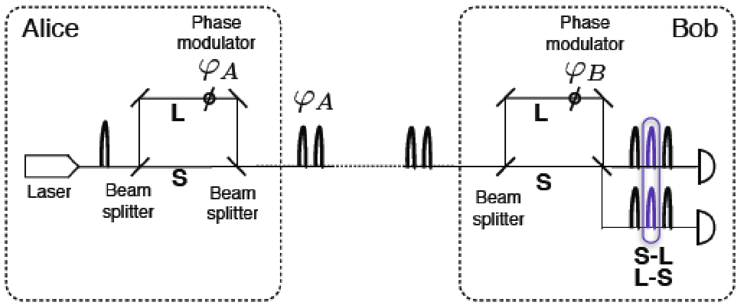
Results



Asymmetric Phase Encoding

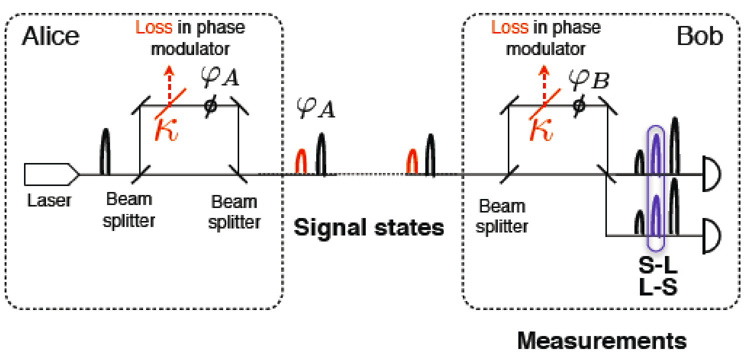
Phase encoding

Phase Encoded BB84



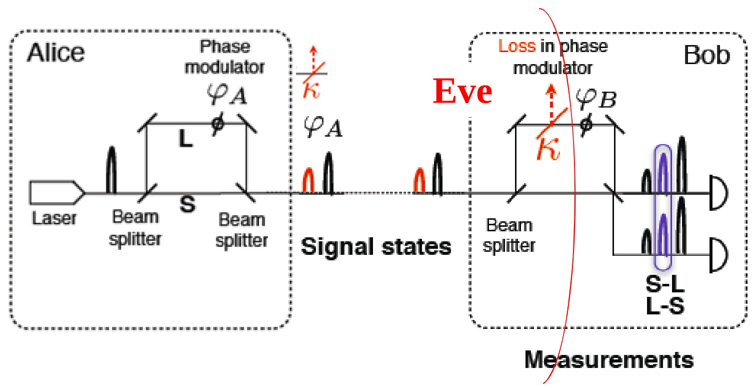
Phase encoding

Phase Encoded BB84



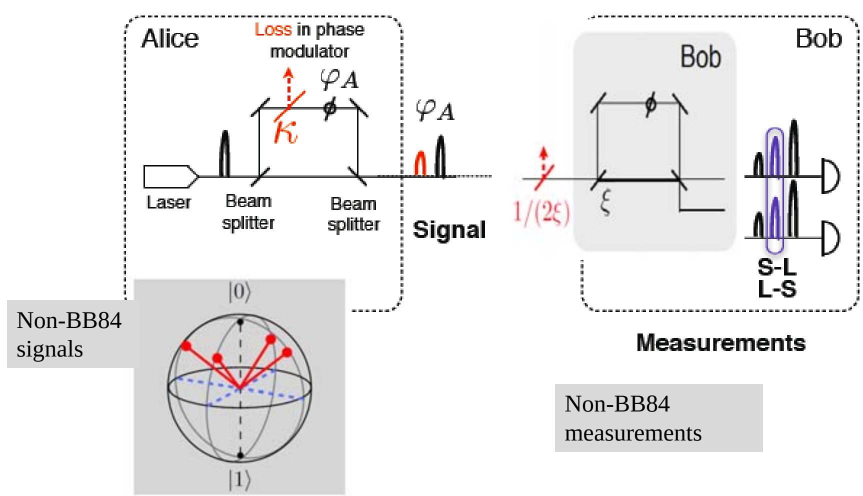
Asymmetric pulses: 1st attempt

[Li, Yin, Han, Bao, Guo, QIC 10, 771 (2010)]



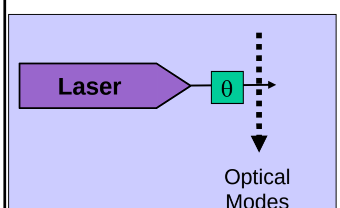
reduction to BB84 type protocol at cost:
source has security of μ_{high}, but signal throughput of μ_{low}

Asymmetric Pulses: Our Approach



Asymmetric Phase Encoding: Tagging

Source reduction: tagging



phase randomized laser pulse:

$\sum_n p(n) |n\rangle\langle n|$

+ signal encoding (polarization or phase encoding)

Tagging: consider all multi-photon signals known to Eve

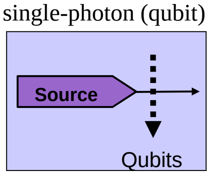
[Inamori, NL, Mayers, quant-ph/0107017 Eur.Phys.J.D **41**, 599 (2007)]
[Gottesman, Lo, NL, Preskill, QIC 2004]

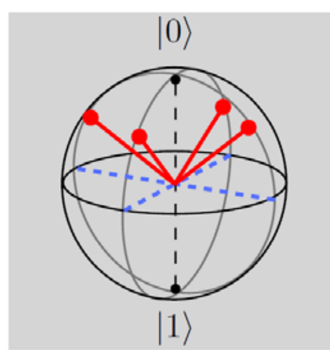
Example: BB84

$$G = \frac{1}{2}\left[R(1 - h[e_1]) - h[e]\right]$$

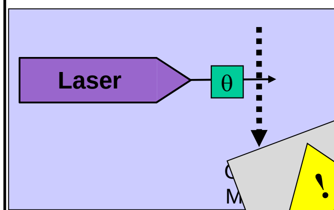
R Minimal fraction of contributing single photon signals

e_1: error rate within single-photon (qubit) signals





Source reduction: tagging



phase randomized la…

Σ_n p(n) …

+ … or phase encoding)

…-photon signals known to Eve

[Inamori, NL, Mayers, quant-ph/0107017 Eur.Phys.J.D **41**, 599 (2007)]
[Gottesman, Lo, NL, Preskill, QIC 2004]

Some systems with high clock rate use mode-locked lasers
→ argument does not apply!

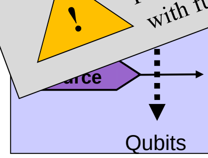
Example: BB84

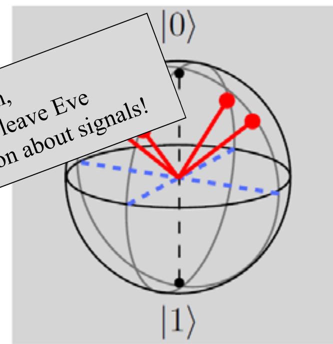
$$G = \frac{1}{2}\left[R\left(1 - h[e_1]\right) - h[e]\right]$$

R Minimal fraction of contributi… single photon signals…

e_1: error rate withi…

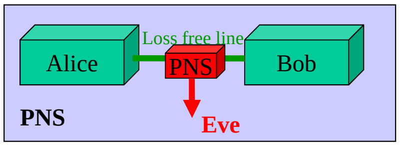
conservative approach,
PNS attack does not leave Eve
with full information about signals!



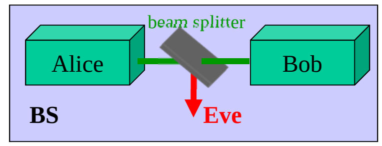


Asymmetric Phase Encoding: Decoy Method

Testing Channels: decoy method



$G \approx \eta^2$



$G \approx \eta$

Decoy state idea:[Hwang; Lo; Wang]

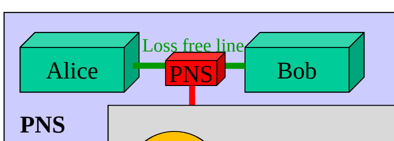
several input intensities μ_i

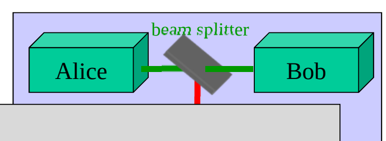
$$p_{det}^{(i)} = \sum_n p^{(i)}(n)\ Y(n)$$

observed detection probability for setting (i)
photon number distribution for setting (i)
Yield (probability that a n-photon signal triggers detectors)

yield Y(n) independent of choice of μ_i!
➔ can estimate Y(n) from few settings of μ_i

Testing Channels: decoy method





!

Decoy method:
Allows to estimate all observables as if they were conditioned on the photon number
➔ detected events from single photons p(det|n) = Y(n)
➔ error rate within detected single photons

Decoy state idea:[Hwang; Lo; Wang]

several input intensities μ_i

$$p_{det}^{(i)} = \sum_n p^{(i)}(n)\ Y(n)$$

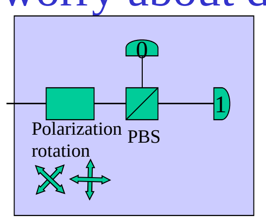
observed detection probability for setting (i)
photon number distribution for setting (i)
Yield (probability that a n-photon signal triggers detectors)

yield Y(n) independent of choice of μ_i!
➔ can estimate Y(n) from few settings of μ_i

Asymmetric Phase Encoding: Detectors

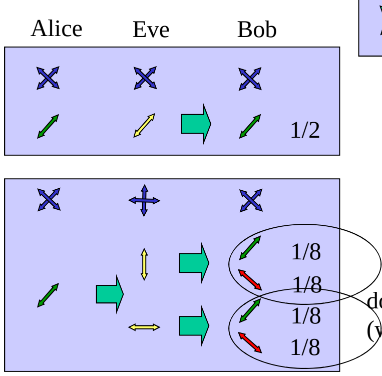
Why worry about detectors?

mode
ρ_M



events
no click
Det. '0'
Det. '1'
Double click

[N.L., Phys. Rev A 59, 3301 (1999)]



double clicks!
(when resending many photons)

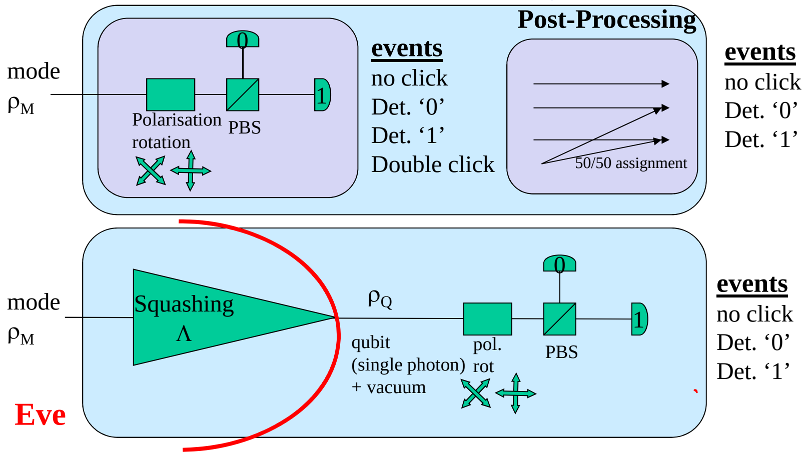
Discarding double clicks:
➔ Error rate: 0%
➔ Eve's information: 100%

Sifted key: Error rate: 25%
Eve's information: 50%

Discarding all double clicks can compromise QKD!

Finding Qubits in optical Modes

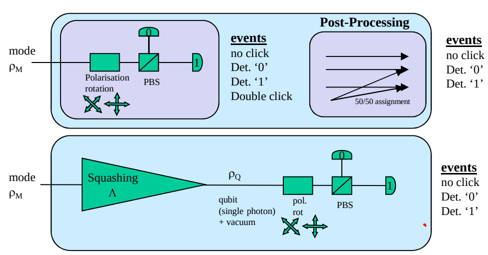
[Beaudry, Moroder, NL, PRL 101, 093601 (2008)]



With this post-processing we can assume without loss of generality that Eve forwards only single photons or vacuum!

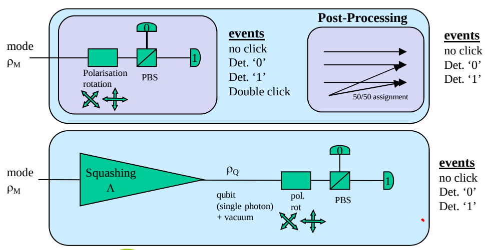
See also [Tsurumaru, Tamaki PRA 78, 032302 (2008)]]

Requirements



$$\mathrm{Tr}\left(\rho_{in} F_M^{(i)}\right) \stackrel{!}{=} \mathrm{Tr}\left(\Lambda(\rho_{in}) F_Q^{(i)}\right)$$

Requirements



$$\mathrm{Tr}\left(\rho_{in}F_M^{(i)}\right) \stackrel{!}{=} \mathrm{Tr}\left(\Lambda(\rho_{in})F_Q^{(i)}\right) = \mathrm{Tr}\left(\rho_{in}\Lambda^\dagger(F_Q^{(i)})\right) \quad \forall i$$

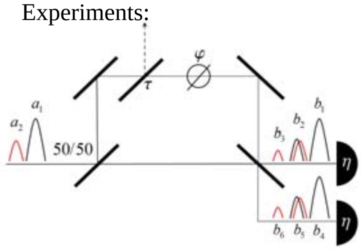
$$F_M^{(i)} = \Lambda^\dagger\left(F_Q^{(i)}\right)$$

Λ ⇔ Choi-Jamiolkowski matrix τ

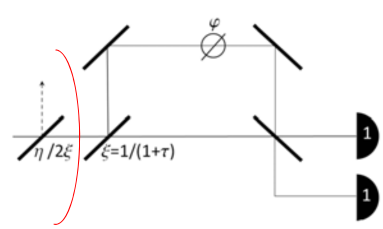
Λ completely positive
⇔ τ positive

Squash Model for Phase-Encoding

Experiments:



Experiment (Optical Model)



Experimental events:
no click
single click:
-Middle clicks (4 events)
- outside click
multi clicks:
- middle only
- outside only
- middle and outside

½ each

Target events:
no click
single click:
1/8 each -Middle clicks (4 events)
1/2 - outside click

Squashing Model exists!

Asymmetric Phase Encoding: Qubit Proof Technique

QKD Protocols: Security Analysis (Renner)

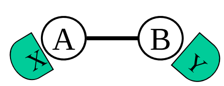
1) quantum phase

Alice and Bob exchange quantum signals and measure them

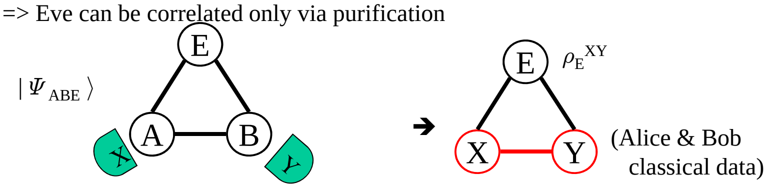
2) classical phase

a) Testing

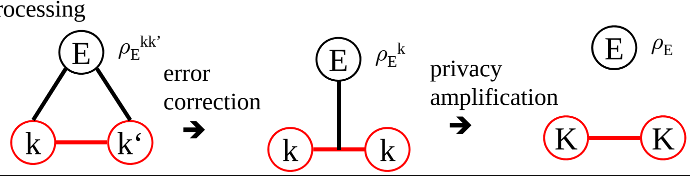
observation P(X,Y) ➔ $\rho_{AB} \in \Gamma$



=> Eve can be correlated only via purification

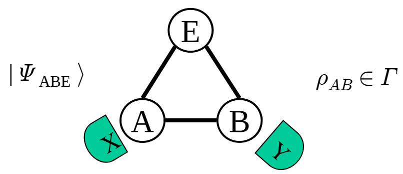


b) Processing

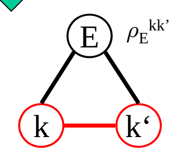


Using Symmetry

[Ferenczi, NL, Phys. Rev. A 85, 052310 (2012)]

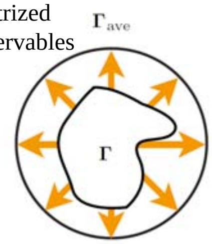


classical QKD protocol (sifting, bit assignment …)



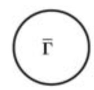
Symmetry:

Step 1: use only symmetrized (averaged) observables



Step 2: check that QKD protocol maintains symmetry

➔ convexity, equivalence under symmetry



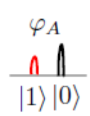
$$G = \min_{\Gamma} \left\{ H(k) - \delta_{leak} - \left(S(\rho_E) - \sum_k p(k) S\left(\rho_E^{(k)}\right) \right) \right\}$$

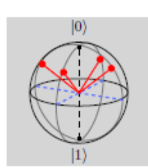
Security proof on the single-photon level

[A. Ferenczi, V. Narasimhachar, N. Lütkenhaus, arXiv:1206.6668v1]

Qubit-based security proof

- Identify $|0\rangle$ with advanced pulse, $|1\rangle$ with trailing pulse

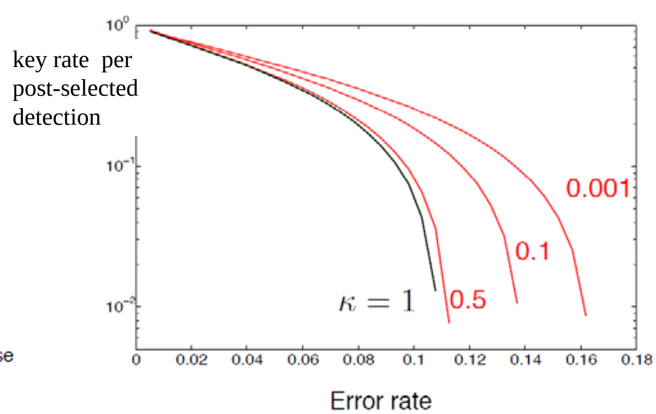




New signal states: With loss in the phase modulator

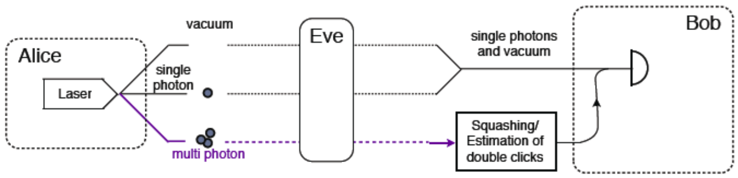
Protocols with asymmetric signal states

•No channel loss: tolerates a higher error rate than BB84 -> States less distinguishable than BB84 states.



Asymmetric Phase Encoding:
Full Results for Optical Model

QKD with practical devices



Qubit-based security proof ✗

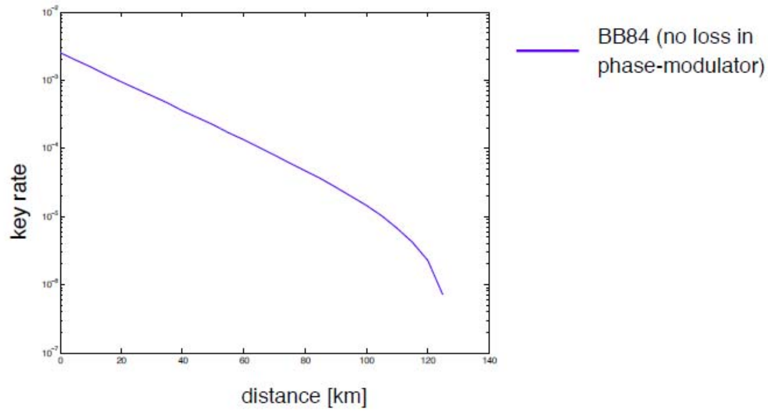
Practical devices not considered in qubit security proof
- Source: Laser -> Poissonian statistics
- Detector: Threshold detector (no photon number resolution)

Extend validity of qubit-based security proof ✓

Source
•Tagging: Eve is given full knowledge about multi-photon events.
•Decoy: Determine the fraction of single-photon events.

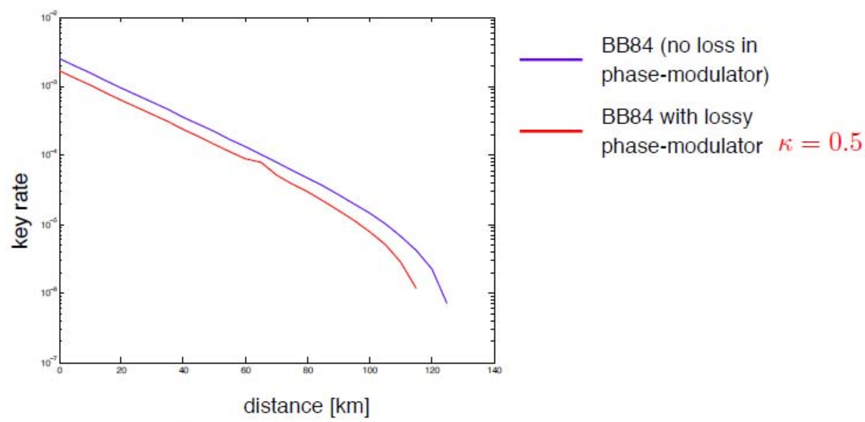
Detector
•Squashing: Justification that Bob receives a qubit or vacuum.
•Estimation of bounds on multi-photon contributions from double clicks.

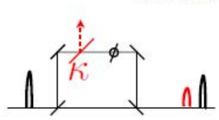
Results



[A. Ferenczi, V. Narasimhachar, N. Lütkenhaus, arXiv:1206.6668v1]

Results

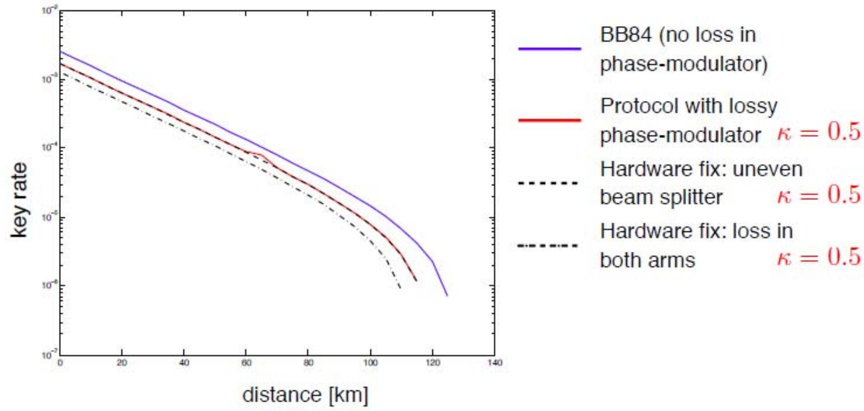


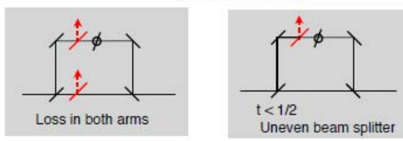


[A. Ferenczi, V. Narasimhachar, N. Lütkenhaus, arXiv:1206.6668v1]

Results

[A. Ferenczi, V. Narasimhachar, N. Lütkenhaus, arXiv:1206.6668v1]





Summary

Tool development for optical implementation:

- tagging
- squashing [Beaudry, Moroder, NL, PRL 101, 093601 (2008)]
- use of symmetry

Application to Asymmetric Phase-encoded BB84:

- reduced provable secure key rate
- identical to hardware fix
- room left for improvement (e.g. multi-photon pulses)

[A. Ferenczi, V. Narasimhachar, N. Lütkenhaus, arXiv:1206.6668v1]

Su... ary

Tool dev... ation:

- ta...

...093601 (2008)]

...symmetric Phase-...

- ...vable secure key rate
- ...cal to hardware fix
- room left for improveme...

[A. Ferenczi, V. Narasim... ...68v1]

Wanted:
Postdoc (Start Fall 2012)
Graduate Students (Fall 2013)

International QKD Summer School
Waterloo, July 29- August 2, 2013