Security of Practical QKD Links and Networks

R. Annabestani[1], A. Ferenczi[1], V. Narasimhachar[1], D. Pitkanen[1] , X.F. Ma[1], Ricardo Wickert[2], Peter van Loock[2],

Norbert Lütkenhaus[1]

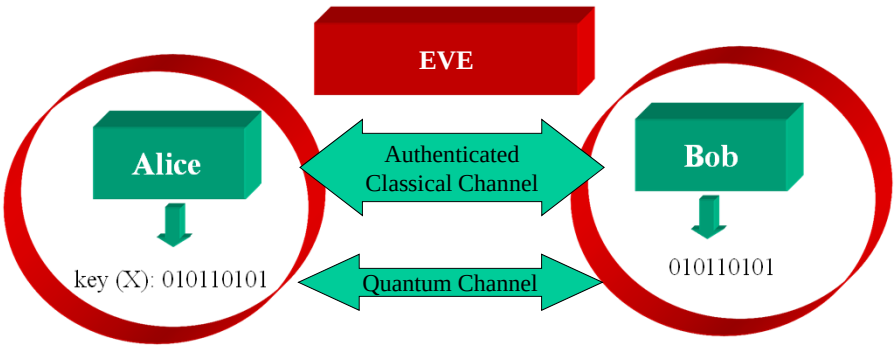
[1]Institute for Quantum Computing, Univ. Waterloo, Canada
[2]Max Planck Institute for the Science of Light, Erlangen, Germany

Discovery Grant
Strategic Project Grant FREQUENCY

Ontario Centres of Excellence

Ontario Research Fund

Quantum Key Distribution



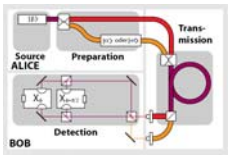
Alice/Bob devices/secure perimeters:

trusted devices (cannot be manipulated by Eve)
Device Models (either QM description, or Markovian Assumption …)
secure perimeter: Eve cannot read internal status of devices

Security and Modelling

Actual Device
e.g. reality based

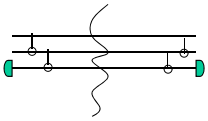
modelling



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)

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

Security Proof

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

Wha oof?

Boundary between scientific and acceptance can be moved (device independent security proofs) but never vanishes

Testing of Models
e.g. by embedding into larger models
- requires experience based cut-off
➔no scientific proof possible

Calib

-Model of Devices
-e.g. QM description
-quantum security perimeter

So what remains?
QKD provides secret key that is future-proof:
the key is as secure for all future as it is at its creation!

➔need to find common level of acceptance (ETSI standardization)
(testable/quantifyable or not)

-security parameters

Software and Hardware Implementation
-verified software
(development & execution)
-hardware security perimeter
- key management

- Scientific Security Proof
"perfect secret key with exception of probability ϵ"

Security proof defined by scientific standard

Structure

I. Security within quantum optical model

II. Security outside quantum optical model

III. Trusted Repeater Network

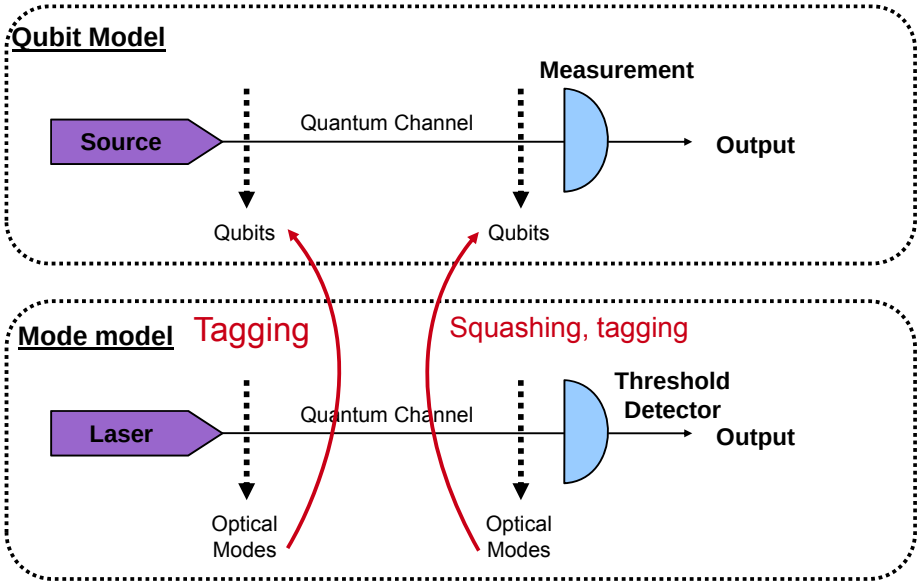
Structure

I. Security within quantum optical model

II. Security outside quantum optical model

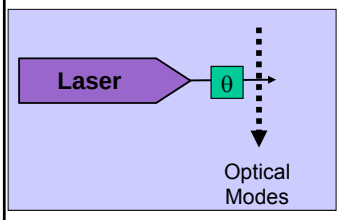
III. Trusted Repeater Network

Summary Reduction



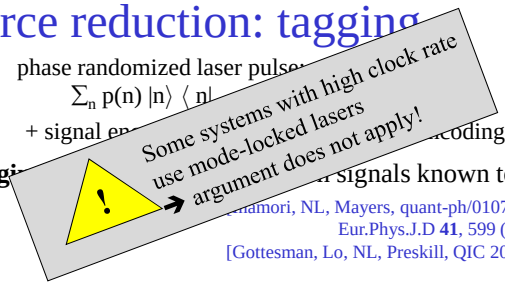
Source

Source reduction: tagging



phase randomized laser pulse
Σ_n p(n) |n⟩ ⟨ n|
+ signal en
coding)

Tagg
signals known to Eve



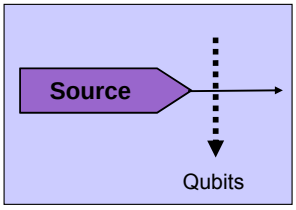
Inamori, NL, Mayers, quant-ph/0107017
Eur.Phys.J.D **41**, 599 (2007)]
[Gottesman, Lo, NL, Preskill, QIC 2004]

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

$R_{PNS} = \frac{p_{\text{exp}} - p_{\text{multi}}}{p_{\text{exp}}}$ Minimal fraction of contributing single photon signals

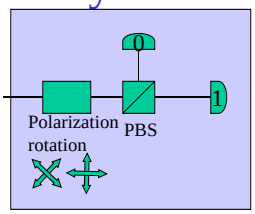
Secure key rate follows from qubit formula by simple rescaling!

Improvements on factor R: (decoy state method) $R_{decoy} = \frac{p(1)\,Y(1)}{p_{exp}}$



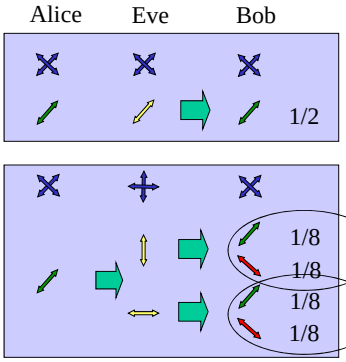
Detectors

Why worry about detectors?



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

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



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

double clicks!
(when resending many photons)

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

Discarding all double clicks can compromise QKD!

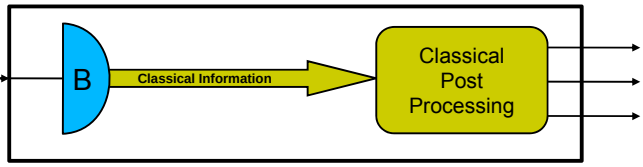
Squashing Model

Actual Measurement

General Optical Input State ρ_{in}

(Large Space)

Full Measurement $\mathbf{F_M}$

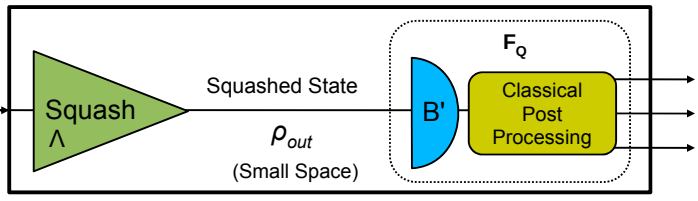


Theoretically Equivalent Measurement

General Optical Input State ρ_{in}

(Large Space)

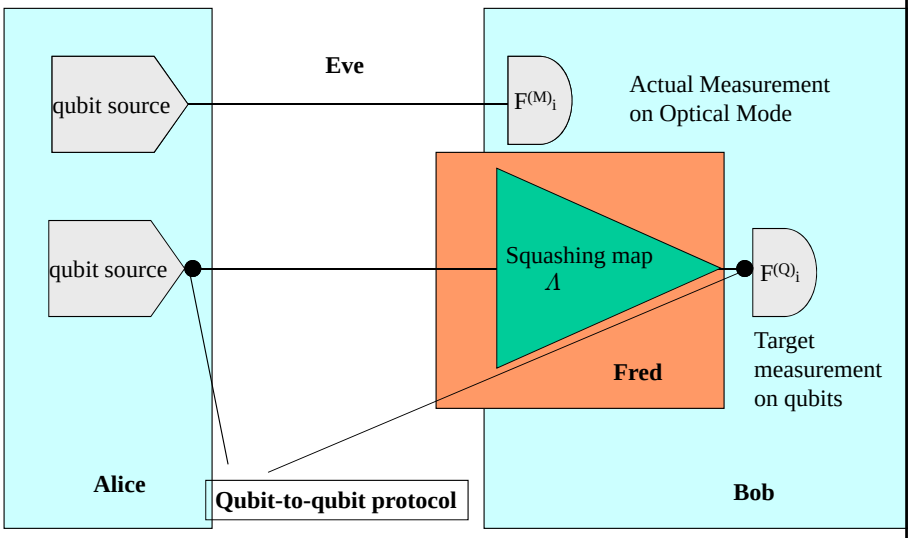
Squash Map Λ + Target Measurement $\mathbf{F_Q}$



Problem: Given F_M , F_Q , is there a physical squashing map Λ?

Already assumed in some QKD security proofs [Gottesman, Lo, NL, Preskill, QIC. 4, p 325 (2004)]

Squashing models and Security proofs



Generic Key Rate Enhancement

$$K = H(A) - H(A|B) - I_{PA}$$

$H(A) - H(A|B)$: Error correction

I_{PA}: privacy amplification

$H(A) - H(A|B) = I(A:B)$

Squashing Model requires tactical simplification of data:

e.g. random assignment of double-clicks

➔ necessary for simplified evaluation of privacy amplification

Coarse graining: B' ➔ B

For error correction refined data (knowledge of double clicks) can be used:
It suffices for Alice to send H(A|B') error correction information!

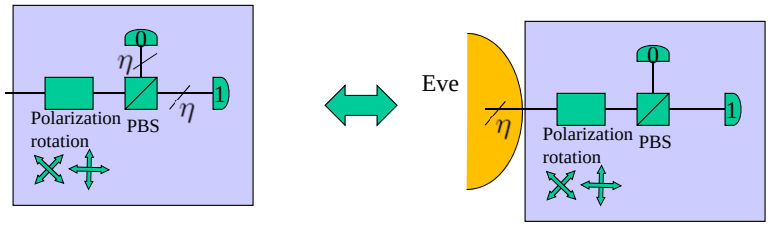
➔ privacy amplification component unaffected (for one-way error correction)

➔ key rate improved

[Ma, NL, Quant.Inf.Comp. 12, 203 (2012)]

Warning: unequal detection efficiency

For simplification reasons, we typically take out detection efficiencies and give it to Eve

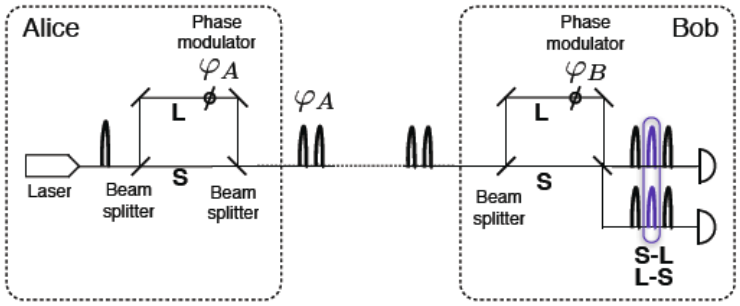


- overly conservative, but necessary to be able to complete proof
- relies on the both detector inefficiencies to be equal
- can be addressed, not trivial …

Phase Encoding Imperfections

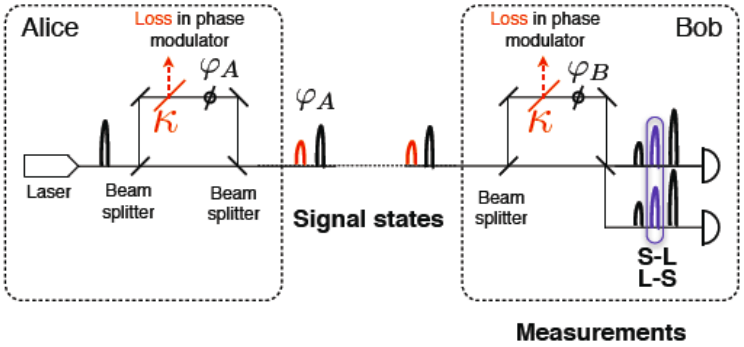
Phase encoding

Phase Encoded BB84



Asymmetric pulses

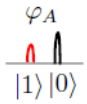
Phase Encoded BB84

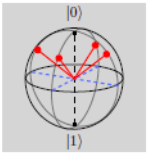


Security proof on the single-photon level

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

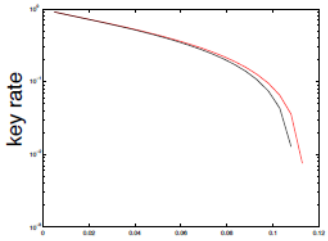
Qubit-based security proof
- Identify $|0\rangle$ with advanced pulse, $|1\rangle$ with trailing pulse





New signal states:
With loss in the phase modulator

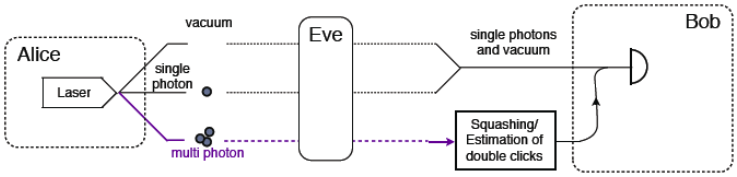
Protocols with asymmetric signal states
•No channel loss: tolerates a higher error rate than BB84 -> States less distinguishable than BB84 states.



With asymmetric states $\kappa = 0.5$

With BB84 states

QKD with practical devices



Qubit-based security proof

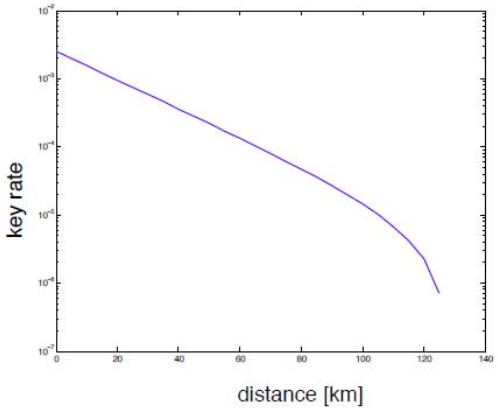
Practical devices not considered in qubit security proof
- Source: Laser -> Poissonian statistics
- Detector: Threshold detector (no photon number resolution)

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.

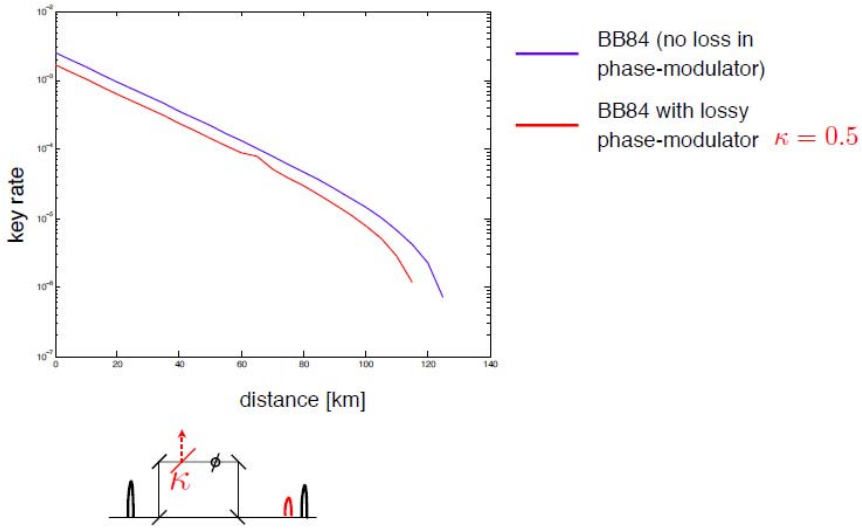
Detector
•Squashing: Justification that Bob receives a qubit or vacuum.
•Estimation of bounds on multi-photon contributions from double clicks.

Results



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

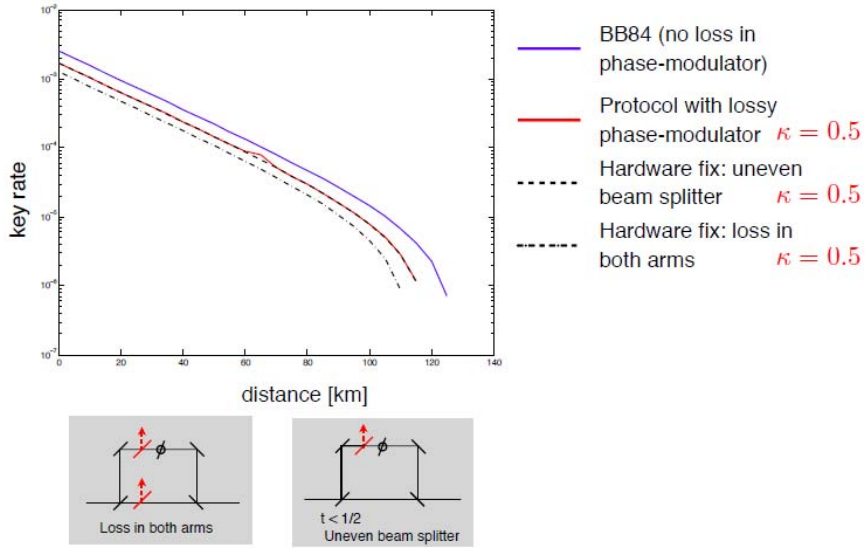
Results



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

Results

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



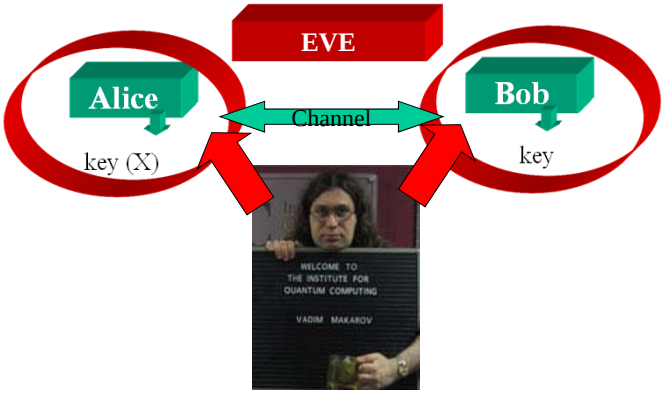
Structure

I. Security within quantum optical model

II. Security outside quantum optical model

III. Trusted Repeater Network

Not so friendly …



What Vadim Markarov (Trondheim, now Waterloo) does:

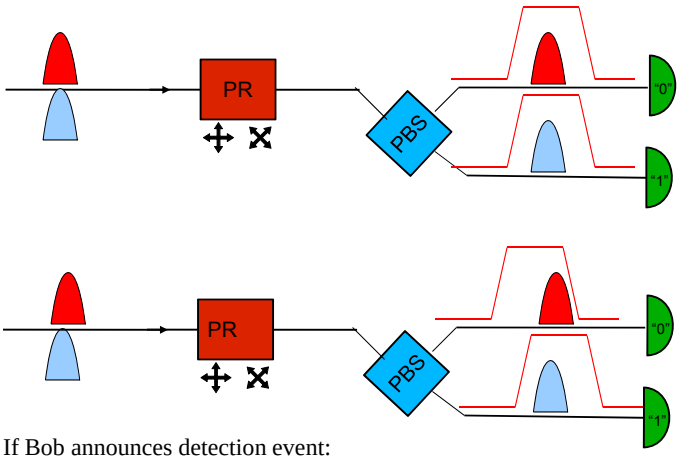
- find deviations of devices from model assumptions
- actively intrude devices via optical fibers!
- manipulate devices (blind, burn detectors)

Vadim's complices: Lo, Lamas-Linares, Kurtsiefer, Weinfurter, Leuchs' Erlangen Gang

Time Shift Attack

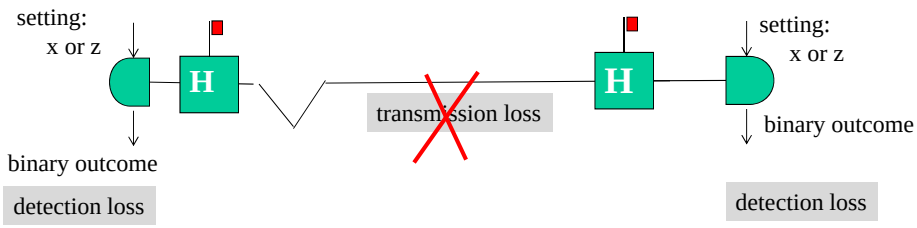
[Hoi-Kwong Lo's group]

Input from Eve



If Bob announces detection event:
➔ must have been the "0" detector!

Device Independence

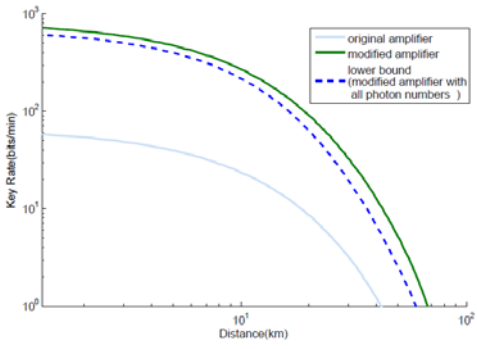


Heralding neutralizes effect of transmission loss!

(Heralding independent of setting, e.g. choose once signal passed heralding device …)

Detection-Device Independent QKD (BB84)

basis independent
average density matrix



combined detector/coupling efficiency $\eta_{cd} = 0.75$

$$K \geq \mu_{-c}\left(1 - h[Q_{-c}]\right) - h[\delta_b]$$

$$\delta_b = \mu_{-c}Q_{-c} + (1-\mu_{-c})\tfrac{1}{2}$$

Structure

I. Security within quantum optical model

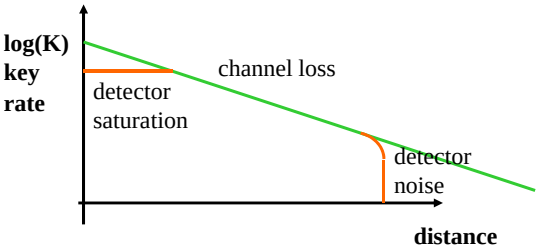
II. Security outside quantum optical model

III. Trusted Repeater Network
(The following slides have not been presented …)

Current Status: Point-to-Point Links

MagiQ™

Use fiber optics devices

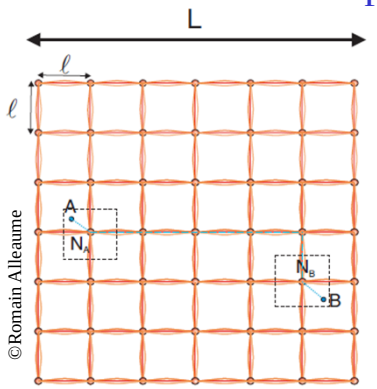


maximum distance: just under 200 km

scaling with distance (fiber): $K \sim \exp(-\alpha\, d/10)$ (no amplification possible!)

Example:
1 THz clockrate
0.17 dB/km
700 km = 120 dB
➔ 1 bit/sec over 700 km (infinite key limit)

Distance Problem: Trusted Repeater Networks



Realizations:

DARPA Network 2002-2005
SECOQC Network 2004-2008
Tokyo Network (2010)
South Africa
Geneva

use trusted classical nodes to propagate secrets through network

➔can cover metropolitan area networks at reasonable key rates

➔ stability against failure of individual links

Enlarged customer bases:

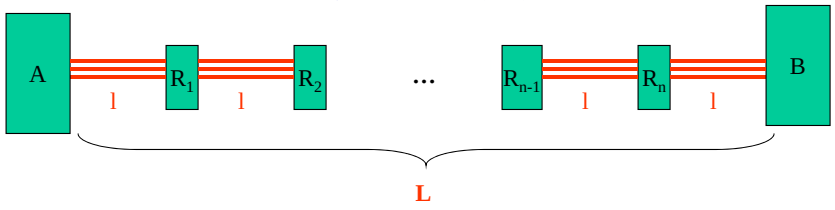
- intra-company metropolitan networks (financial institutions)
- government institutions

➔ automatic key management of many links

Note:
users of network should also be operators
➔ trust level must be high!

Cost Optimization: Linear Chain

[Alleaume, Roeff, Diamanti, NL, New J. Phys. Vol 11, 075002 (2009)]



User demand: rate G

QKD characteristics: secret key rate g(d)

Cost: $$C_{network} = C_{link}\,\frac{L}{l}\,\frac{K_{target}}{k(l)}$$

sequential links # parallel links

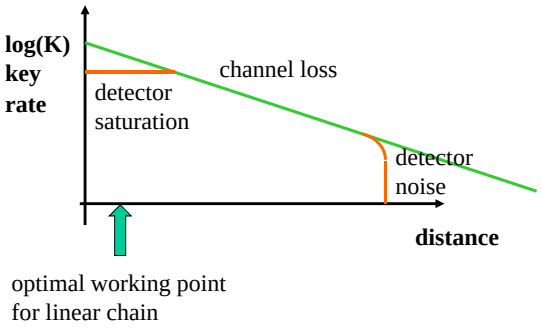
$$k(l) \sim \eta = 10^{-\alpha\, l/10}$$

➔ $$l_{opt} = \frac{10}{\alpha \ln(10)}$$

Optimal Loss:
4.3 dB ➔ ´ = 0.37

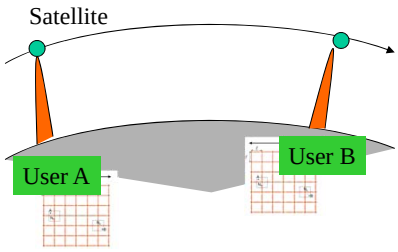
➔ α = 0.25 dB/km → l_{opt}=17.5 km

Working points for QKD



optimal working point
for linear chain

Distance Challenge: Moving Satellite



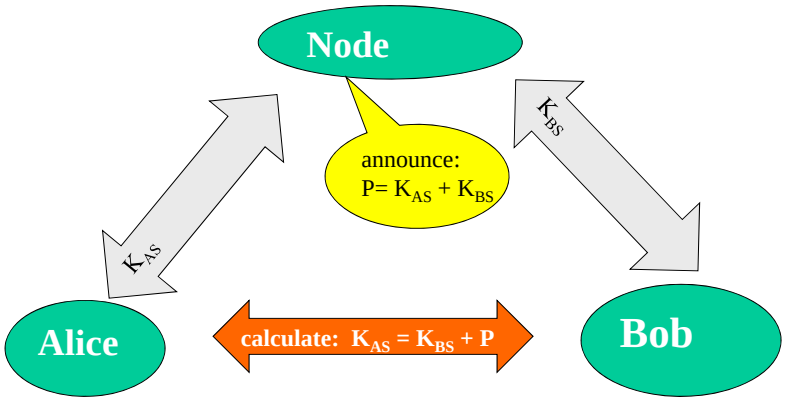
No distance limitation!

Can connect metropolitan area networks by satellites

Application Scenario:

- Commercial Enterprises operation on continental or intercontinental scale
- government
  - embassies
  - military applications

Propagation of Key along Network

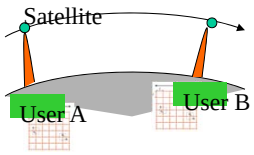


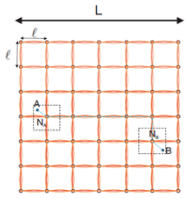
- Public announcement of P allows Alice and Bob to share a secret key
(Intermediate node/Satellite also knows that key)

Bottleneck

Intermediate nodes need to do quite heavy computational tasks:

- error correction close to Shannon limit
- privacy amplification on large block sizes





QKD Protocols

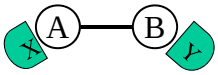
1) quantum phase

Alice and Bob exchange quantum signals and measure them

2) classical phase

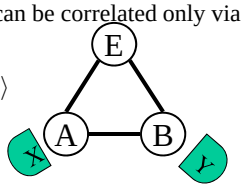
a) Testing

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

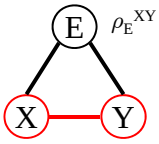


=> Eve can be correlated only via purification

$|\Psi_{ABE}\rangle$



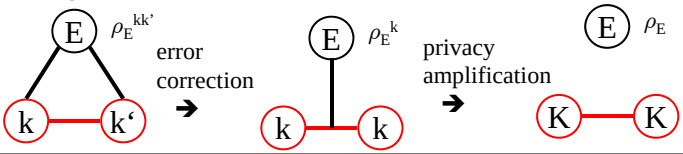
➔



ρ_E^{XY}

(Alice & Bob classical data)

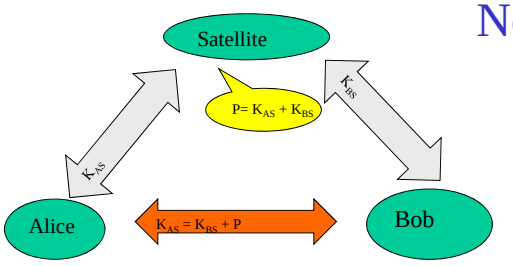
b) Processing



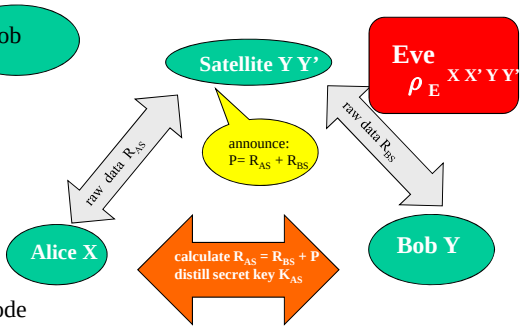
$\rho_E^{kk'}$ ρ_E^{k} ρ_E

Solution: Simplified Trusted Nodes

1) distribute quantum signals
2) create keys
3) connect keys



1) distribute quantum signals
2) connect data
3) create common key

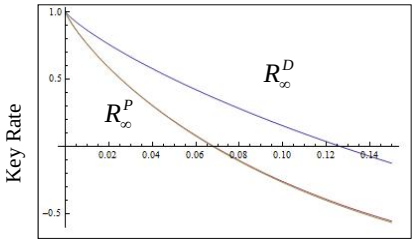


result:

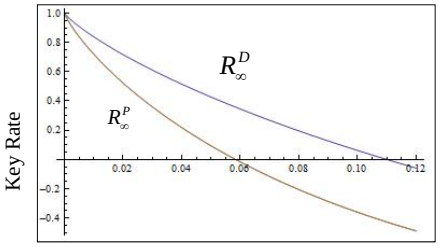
- reduced workload by intermediate node
- protection against passive eavesdropper:
  communication for classical key creation phase bypasses Satellite

Trusted node: parity announcement of data

6 State protocol:



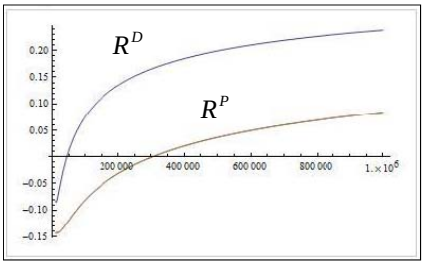
BB84 protocol:



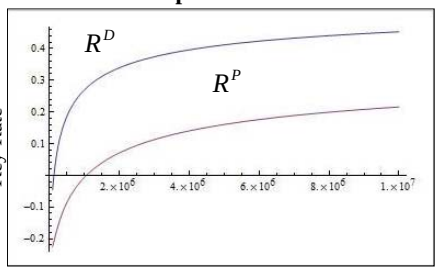
The key rate as a function of single link symmetric error rate Q.
Infinite key limit (no statistics issues)
D: direct link
P: via intermediate node with parity announcement

Non-Asymptotic Analysis:

6 State protocol:



BB84 protocol:



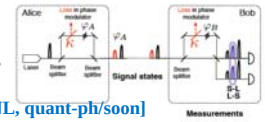
[1] R.Renner, PhD thesis, Diss. ETH NO 16242, quant_ph/0512258
[2] V. Scarani, R. Renner, Phys. Rev. Lett. **100**, 200501(2008)

Current work: improvement in order to work with smaller block sizes ...

Review

I. Security within quantum optical model

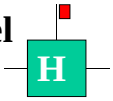
Example:
unbalanced phase encoding



[A. Ferenzi, V. Narasimhachar, NL, quant-ph/soon]
Tool of Squashing models: [N. Beaudry, NL, Phys. Rev. Lett. 101, 09301 (2008)]

II. Security outside quantum optical model

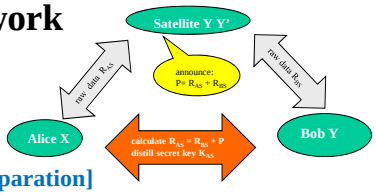
Linear optical heralding devices



[D. Pitkanen, X.F. Ma, R. Wicker, P. van Loock, NL, Phys. Rev. A 84, 022325 (2011)]
Tool of improved data processing: [Ma, NL, QIC 12, 203 (2012)]

III. Trusted Repeater Network

Simplified trusted nodes



[R. Annabestani, X.F. Ma, NL, in preparation]