Challenges and directions in quantum key distribution

Hauke Häseler, Matthias Heid, Tobias Moroder, Geir Ove Myhr, Norbert Lütkenhaus

Institute for Quantum Computing, University of Waterloo

Universität Erlangen-Nürnberg

Collaborations:

Marcos Curty, University of Zaragoza
Romain Alleaume, Francoise Roueff, ENST Paris
Kiyoshi Tamaki, NTT, Masato Koashi, Osaka
Hoi-Kwong Lo, Toronto
Valerio Scarani, Cyril Branciard, Nicolas Gisin, Geneva
Joe Renes, Darmstadt

Overview

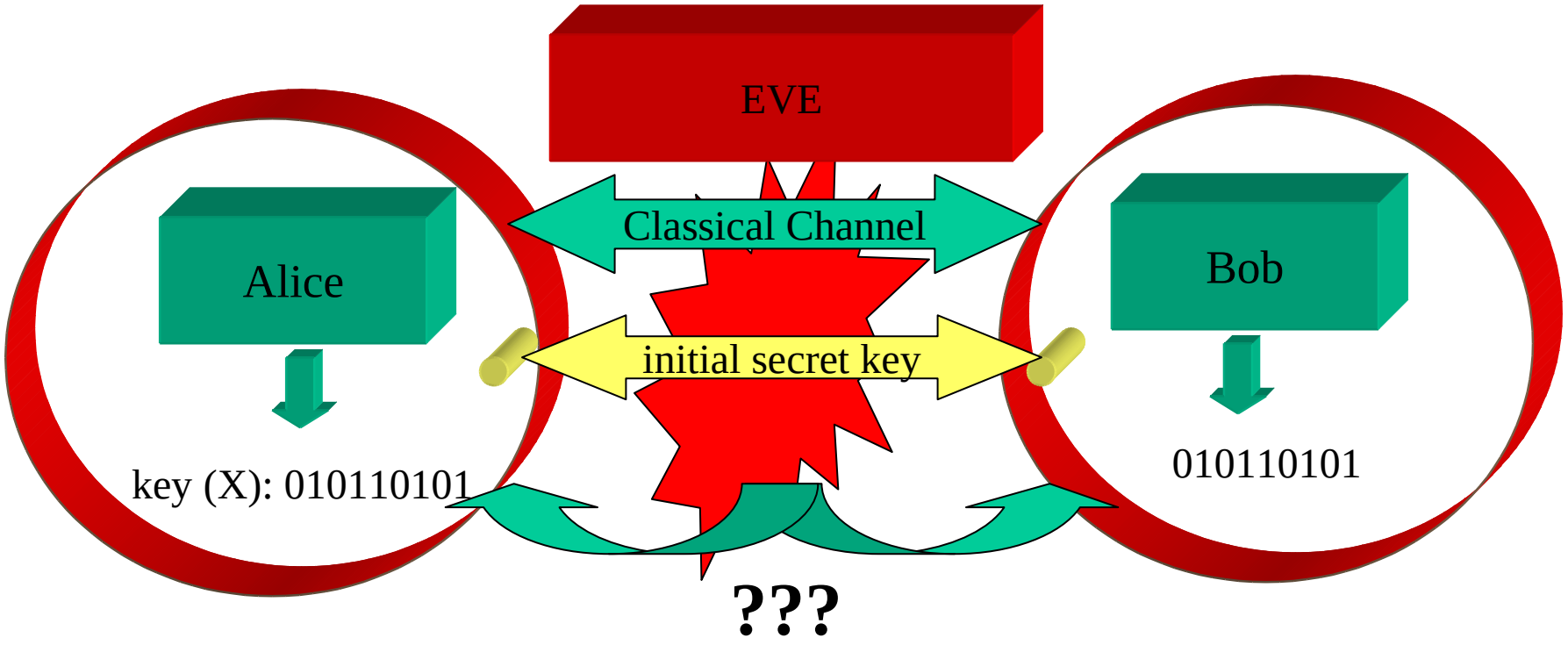
Reminder:
What the heck does QKD do anyway?

Improving the hardware:
Scaling of key rate with loss
Ł searching for good schemes

Improving the software:
basic ideas and limitations

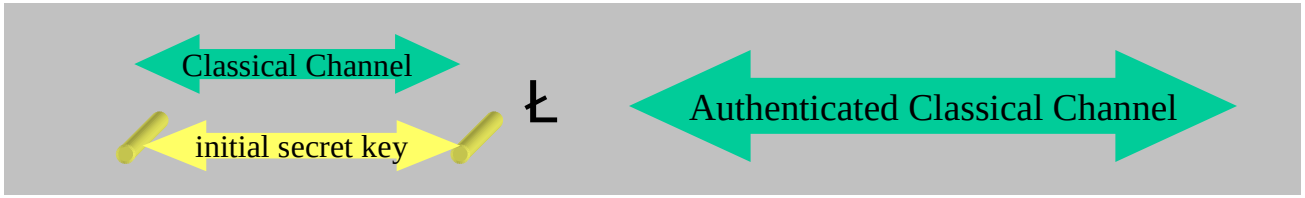
Beyond point-to-point connections:
networks to overcome distance limit

What is QKD about?

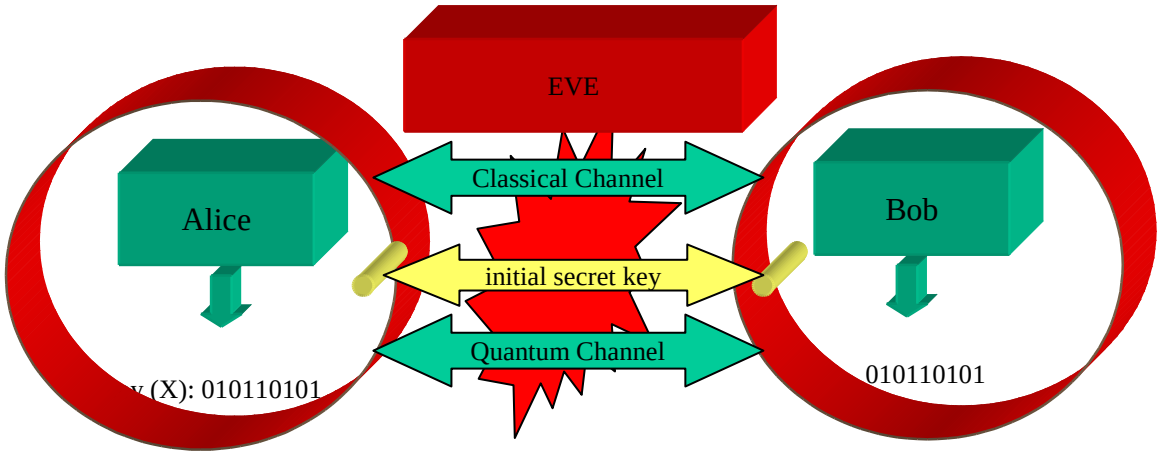


Task:
generate more secret key than initial key
Ł impossible (Shannon)

Additional resource:
quantum channel, non-orthogonal signal states



Security Model



Signal description:

- verification?

Measurements description:

- full modes with temporal behaviour?

Interior of sender and receiver isolated from Eve:
no side channels, Trojan Horse attacks

- added difficulty given optical nature of signals
  - optical path into the heart of the devices

On the channel: no assumption on Eve's power of computation, storage …

- **'Unconditional Security'** (à see Renato Renner's talk)

Obstacles on the Road to Widespread Use of QKD

1) Requirement for authentication:

How to initialize QKD?

Initial key only used to authenticate public channel of first round of QKD

- can be published after authentication
  - use short-term security of public key cryptography?
    - how about trust structure in public key crypto?

2) Key rate:

Secret key rate for point-to-point connections low

- new QKD hardware protocols adapted to high clock rates } Part I
- new QKD software protocols to increase key rate } Part II
- parallel QKD channels due to WDM

possibility to combine QKD with stream-ciphers or other symmetric ciphers in a meaningful way?

3) Topology:

Only point-to-point connection

- introduce network with trusted repeaters
  - loose unconditional security for end users
  - good tool to overcome distance problem

} Part III

4) Cost:

QKD devices too expensive

- not on a level of telecom provider, costs will decrease
  - but not as much as to Public Key Crypto level J

QKD needs dedicated fiber

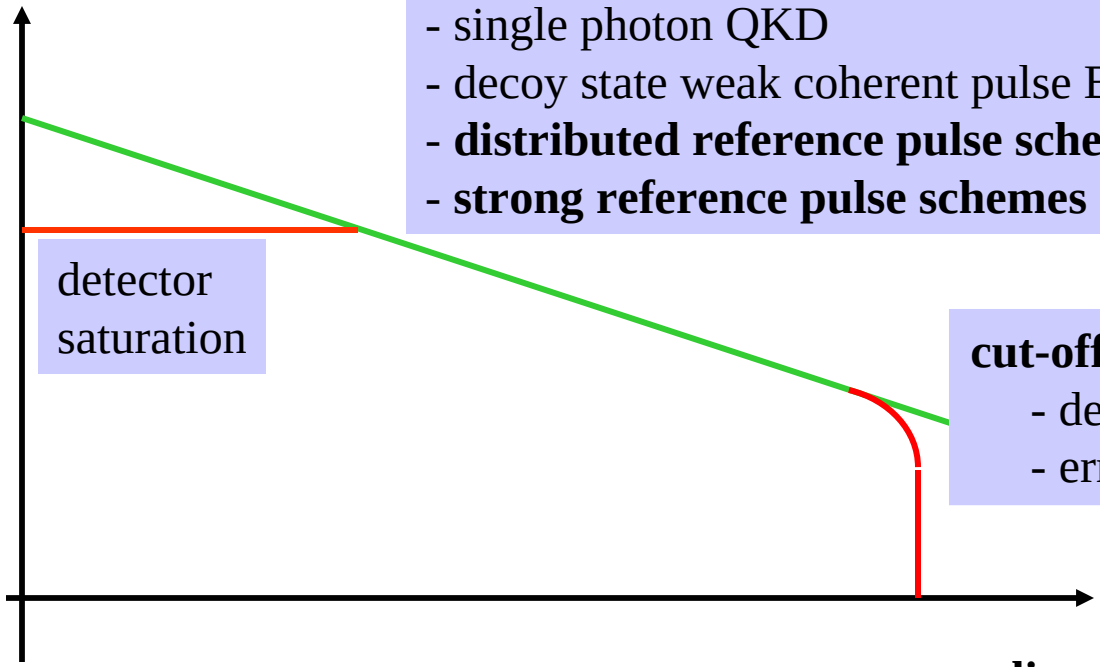
- currently, but that can change due to WDM techniques

University of Waterloo
IQC Institute for Quantum Computing

I. Improving the hardware

Limitations of Point-to-Point Links

Best loss performance G » η
- single photon QKD
- decoy state weak coherent pulse BB84
- **distributed reference pulse schemes (DPS, time-coding …)**
- **strong reference pulse schemes (original B92)**

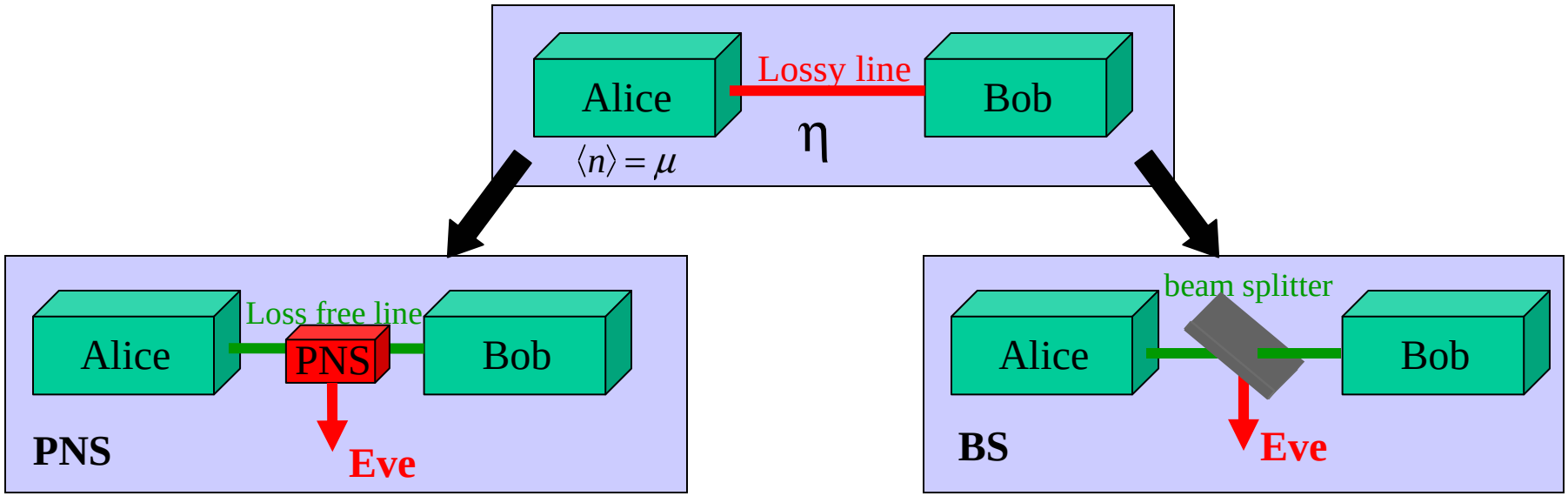


η: channel transmittivity

'Classical' Problems for higher clock rates:

Ł computational power for real time data processing
(LDPC error correction, privacy amplification, random permutations)
Ł synchronisation

Loss performance of WCP-BB84

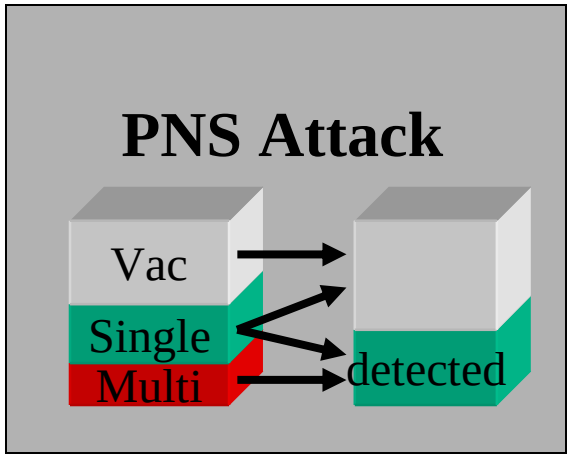


$$G \approx p_{exp} - p_{multi} \approx \left(1 - e^{-\mu\eta}\right) - \left(1 - (1+\mu)e^{-\mu}\right)$$

$$G \approx p_{exp} - p_{split} \approx \left(1 - e^{-\mu\eta}\right) e^{-(1-\eta)\mu}$$

μ_{opt} ¼ η

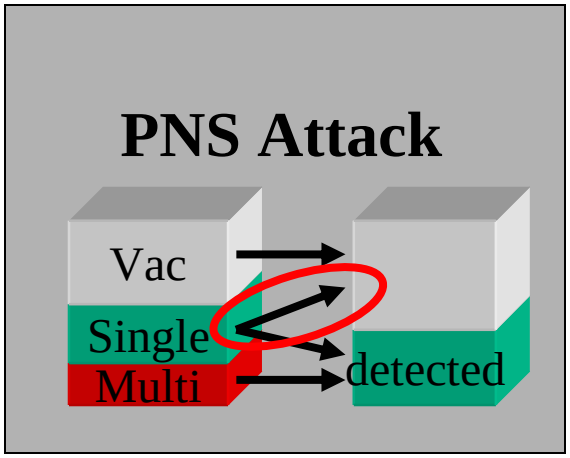
$G \approx \eta^2$

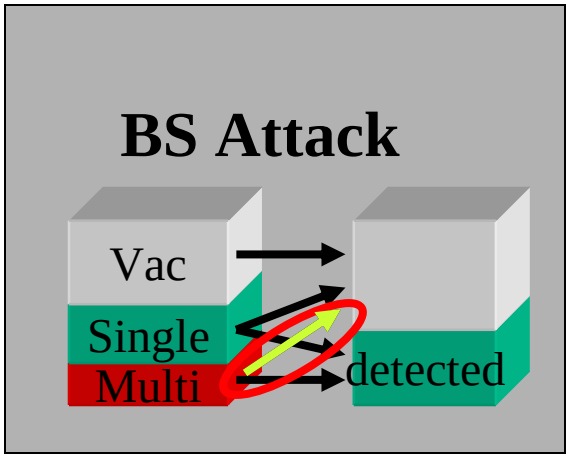


μ_{opt} ¼ 1

$G \approx \eta$

Ways out …





Hardware solutions:

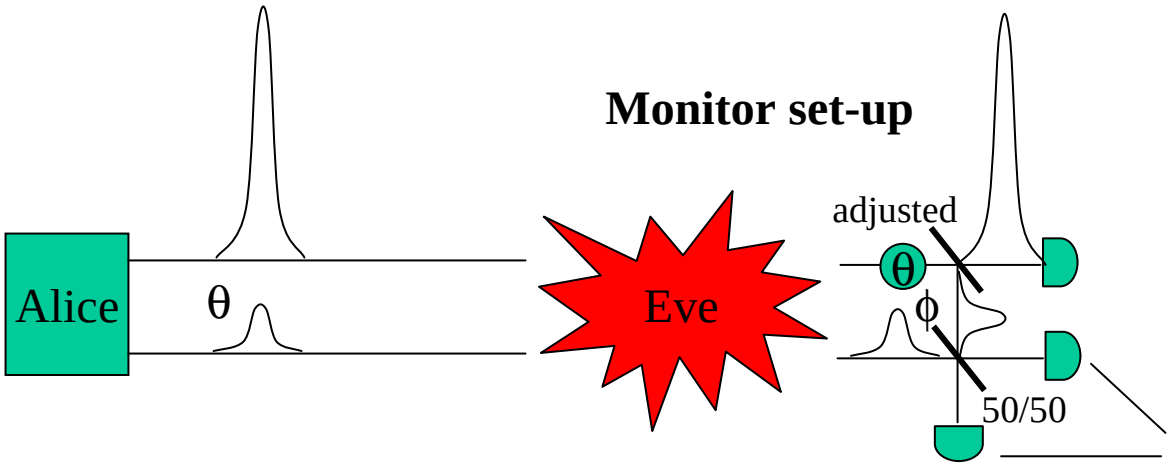
1) Use single photons … J

2) Test the channel better Ł decoy state (à see Hoi-Kwong Lo's talk)
measure (or bound) transfer coefficients Ł approach BS attack!

3) Deny Eve the possibility to block signals without penalty!
In PNS attack, Eve rules whether a signal is detected or not
Ł vacuum state is a 'neutral state'
Ł new schemes without 'neutral state'
- Strong reference pulse schemes
- Distributed reference pulse schemes

Strong Reference Pulse Scheme

Basic idea: **Eve cannot block signals [Bennett (1992)]**



No 'neutral' signal!

Classical photo-detector

Single-photon counter

Extension to BB84:

Huttner, Imoto, Gisin, Mor
PRA 51, 1863 (1995)

Security proofs:

modified receiver (phase estimation) **[M. Koashi]**

photon-number resolving detectors **[K. Tamaki, M. Koashi, NL]**

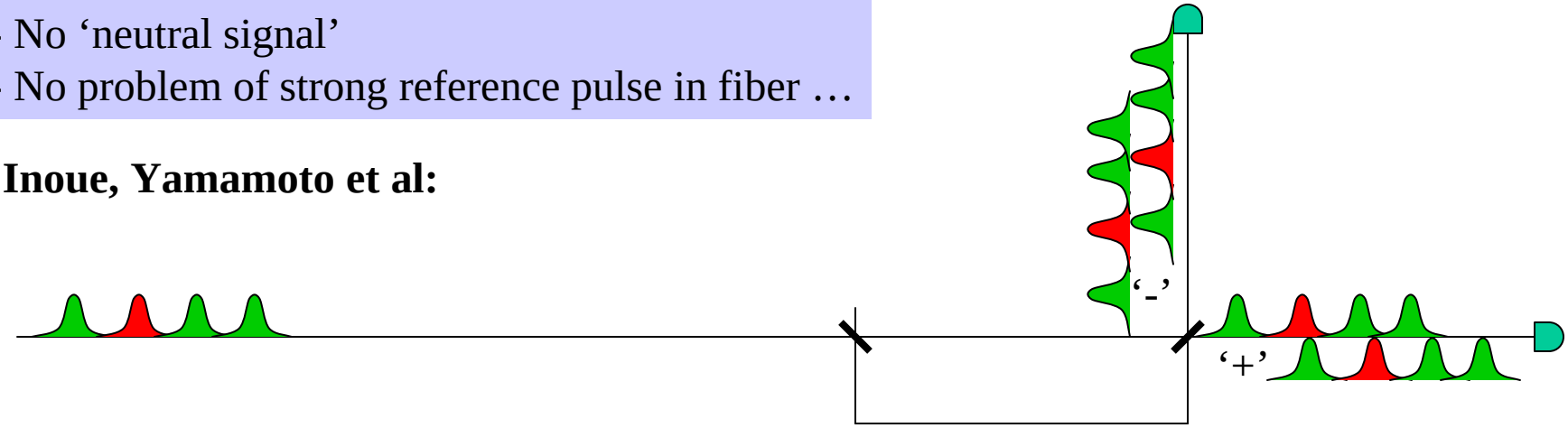
Confirms scaling G » η !

Not implemented yet! Problems of stray light from reference pulse!

Distributed phase reference

- No ‘neutral signal’
- No problem of strong reference pulse in fiber …

Inoue, Yamamoto et al:



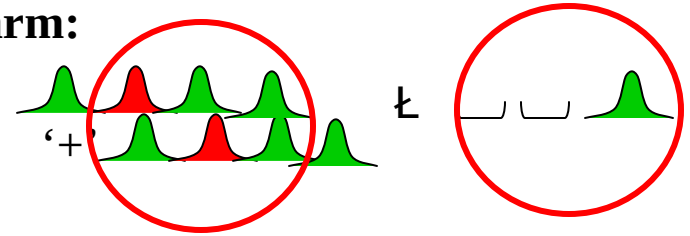
states: coherent states |§ α i

bits: relative phase of two pulses

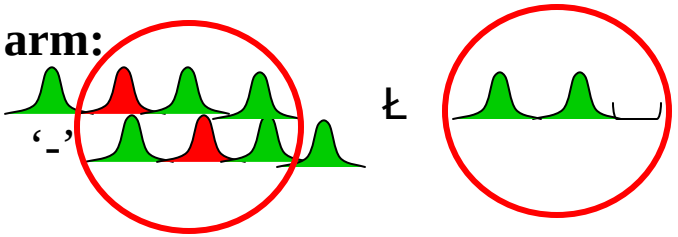
Ł non-orthogonal signal states!

Ł non-trivial POVM measurement!

lower arm:



upper arm:



Security proofs:

‘individual attack’ **[Waks et al]**

ultimate limitations:

[M. Curty, L.-L. Zhan, H.-K. Lo, N. L quant-ph/0609094]

Full security proof missing! No simple analogue of ‘collective attack’!

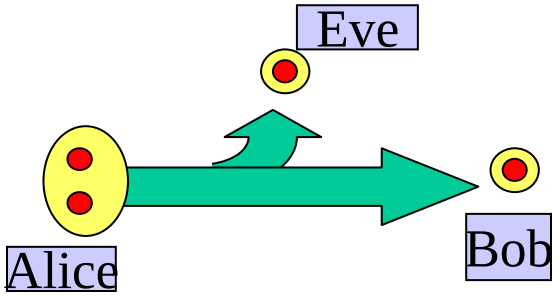
Related scheme (though not equivalent) using signals |0 α i |α 0 i |α α i: Geneva Group

University of Waterloo
IQC Institute for Quantum Computing

II. Improving the software

SARG protocol

[Scarani, Acin, Ribordy, Gisin]



Change public announcement:

Instead of basis ✕ or ✛

announce sets of neighbouring pairs:

{↗ ,↔} or {↔, ↘ } or { ↘ , ↕ } or { ↕ ,↗ }

Eve: splitting one photon off leaves task of discriminating two non-orthogonal signals

Bob: can with some probability identify signal error free

e.g. measurement ✛

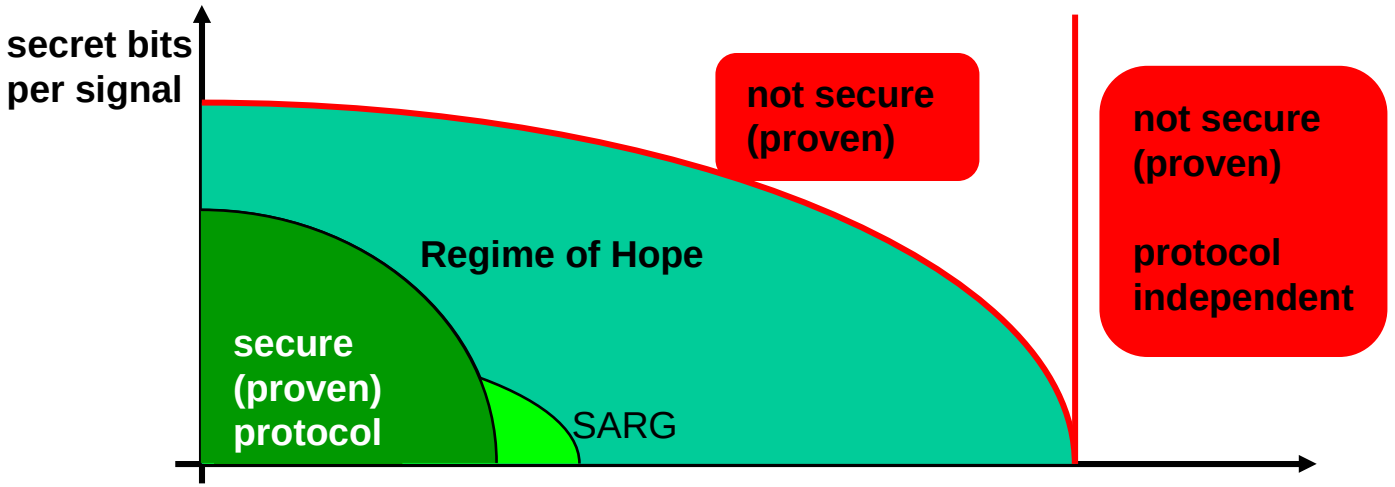
result ↕

announcement {↗ ,↔ }

Ł identifies ↗

SARG protocol reduces effect of multi-photons

Key rates for given apparatus



All lines depend on technology!

Upper bounds Ł **[Christandl, Ekert, Horodecki $^{-2}$, Oppenheim, Renner quant-ph/0608199]**

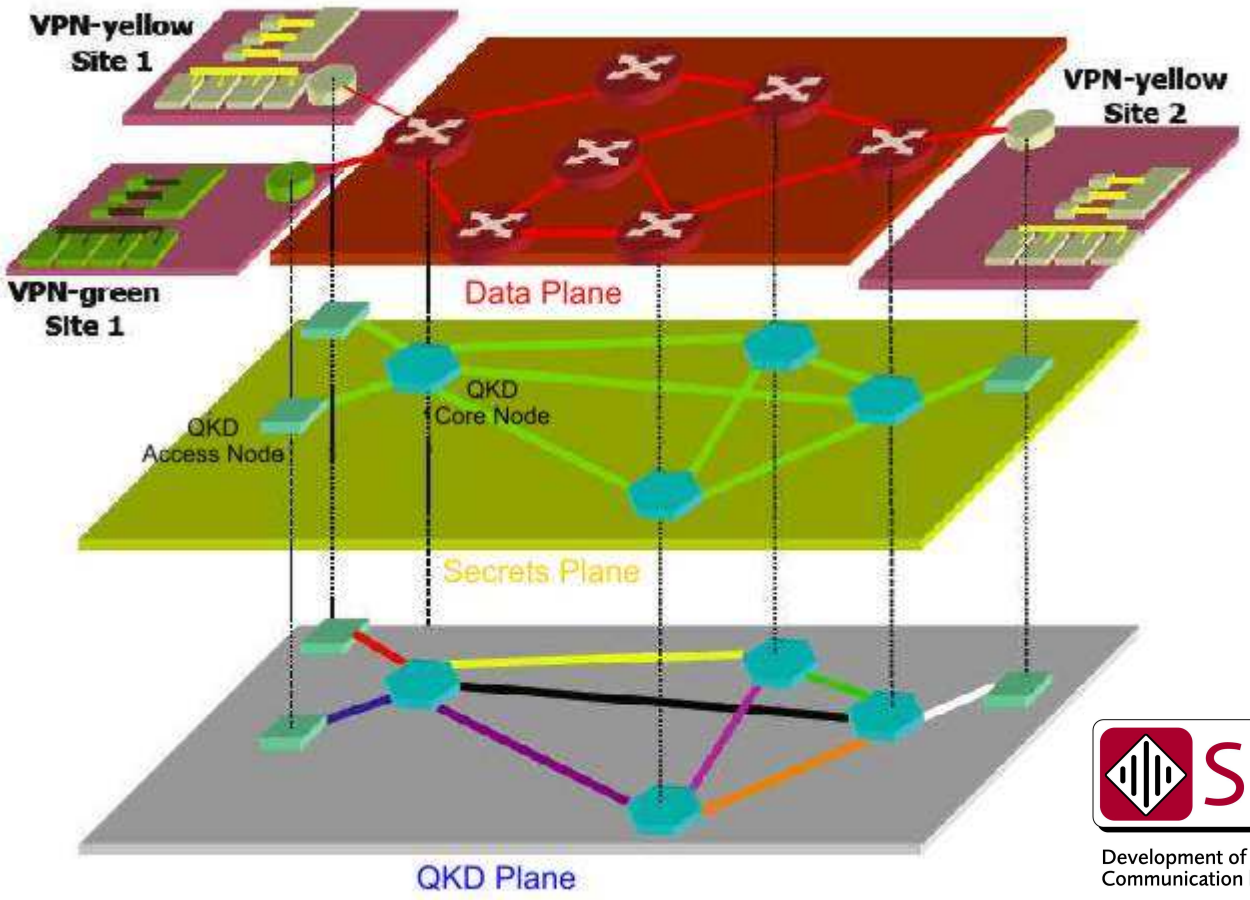
Upper bounds for simpler evaluation in trusted device scenario

Ł **[Moroder, Curty, NL, PRA 73, 012311 (2006)]**

Idea: $\rho_{AB} \,!\, \lambda\, \rho_{AB}^{sep} + (1-\lambda)\, \rho_{AB}^{ent}$ $\quad G \cdot (1-\lambda)\, I_{A;B}(\rho_{AB}^{ent})$

III. Networks

SECOQC Prototype Network



SECOQC

Development of a Global Network for Secure Communication based on Quantum Cryptography

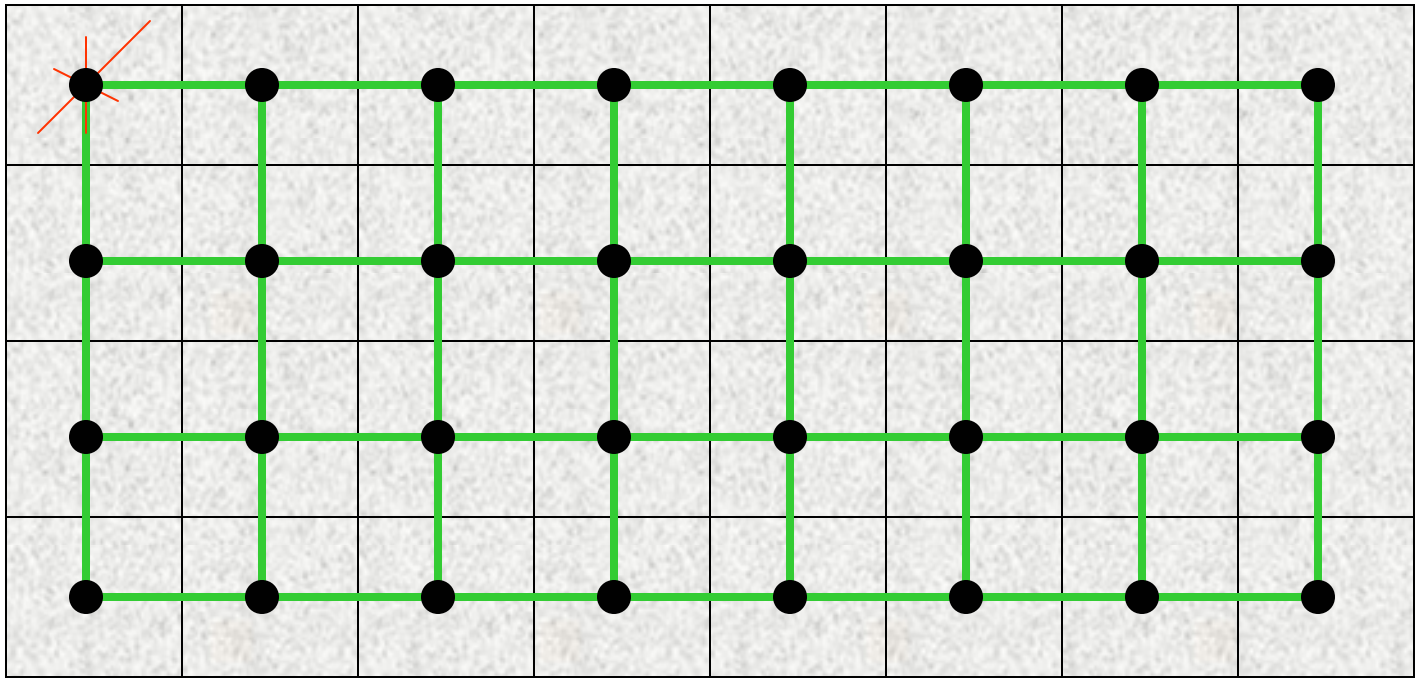
Trusted hub stations

- combine with classical tools to tolerate a few hubs in adversary's hand … Louis Salvail

Looking into the future …

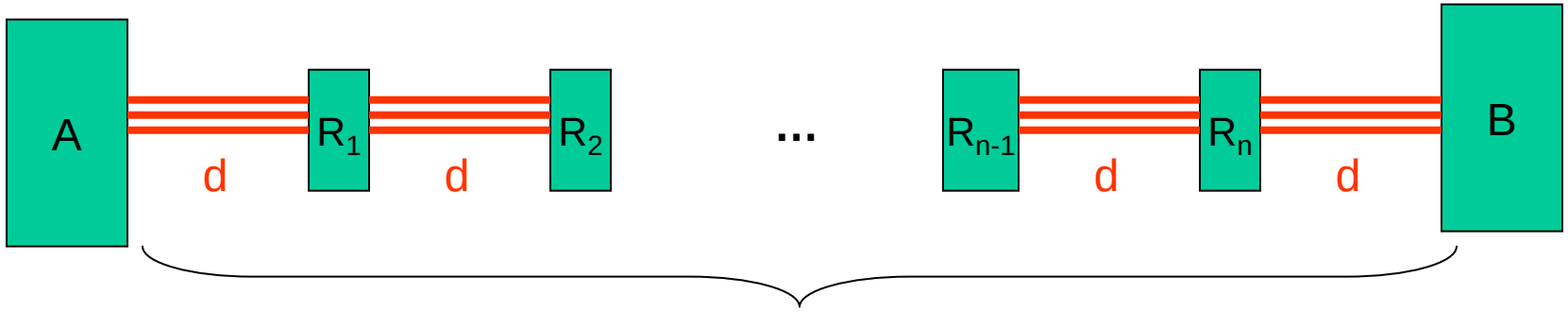
What if QKD would be standard telecommunication service, such as phone service?

- network structure with access network and backbone network



What is a suitable structure for authentication?
What should be the cell dimensions? (joint work with R. Alleaume and F. Roueff)

Network optimization: linear chain



User demand: rate G

QKD characteristics: secret key rate g(d)

Cost: $C_{network} = C_{link} \frac{D}{d} \frac{G}{g(d)}$

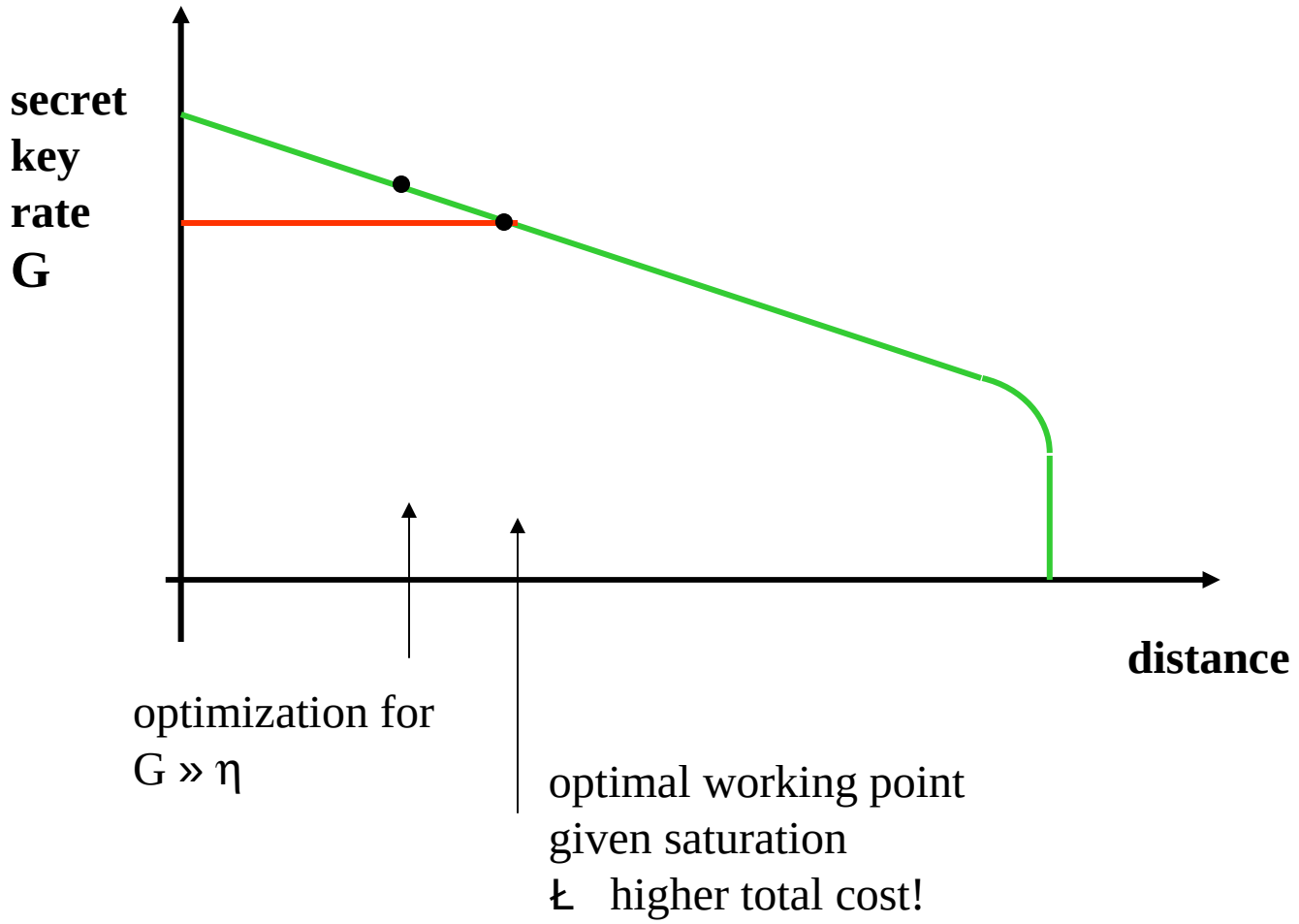
sequential links # parallel links

$g(d) \sim \eta = 10^{-\alpha\, d/10}$

➡ $d_{opt} = \frac{10}{\alpha \ln(10)}$

➡ α = 0.25 dB/km ! d_{opt}=17.5 km

Optimal working point



Optimize detectors: at d_{opt} we should be still in the regime of G » η!

Conclusion

QKD doesn't do miracles, but it can be a stepping stone in a broadening market.

QKD devices need to be properly engineered to match the model of security proofs.

- No secret key rate without security proof!

New schemes give relatively good scaling with loss (as for single photons sources)

New classical communication protocols can increase the key rate (software!)

True networks might solve some distance and application problems …

- they certainly provide some alternative optimization point, rather than maximum distance!