Integration of a commercial quantum cryptography appliance into metropolitan area networks

Alexandre Pauchard, Olivier Gay, Olivier Guinnard, Ralph Hoffmann, Antonio Matteo, Laurent Monnat, Gregoire Ribordy, Patrick Trinkler

Quantum Cryptography and Computing Workshop
October 2-6, 2006

id Quantique

Introduction

From a market perspective, the increase in network security is the key driver for the development of QC

ð Scientific community focuses mainly on improving and challenging it

For customers, other factors are also vital, sometimes even more important:

- Ø Simplicity – QC simplifies key management
- Ø Interoperability
- Ø Reliability
- Ø Redundancy
- ØTotal cost of ownership

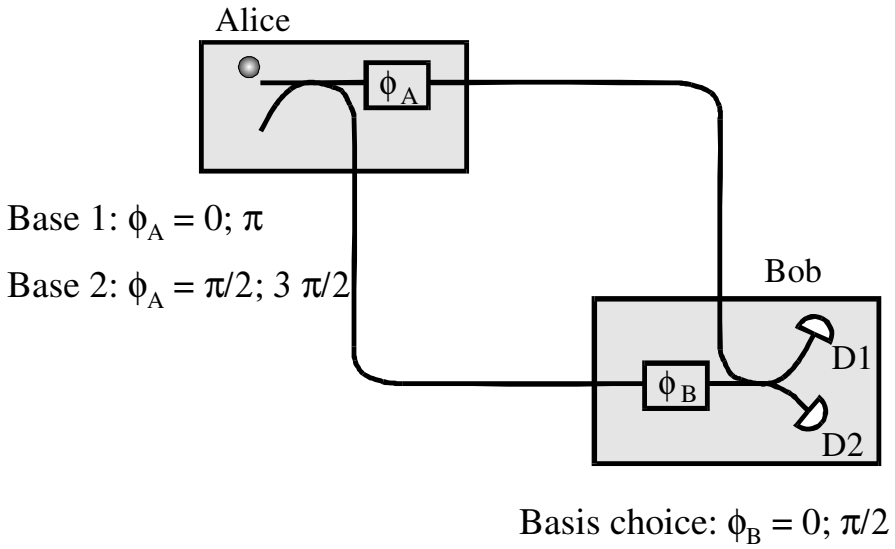
Outline

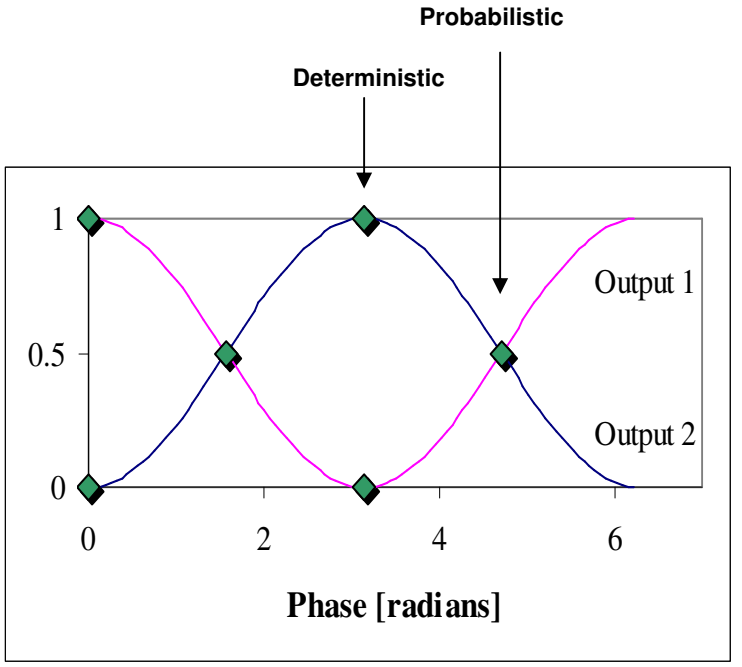
- Introduction
- Historical perspective on optical platforms and QKD experiments
- Vectis Link Encryptor – state-of-the-art encryption appliance
- Challenges facing the deployment in networks
- Future directions

Phase-Coding QKD Approach

Simple Mach-Zehnder implementation

Ø Mach-Zehnder Interferometer

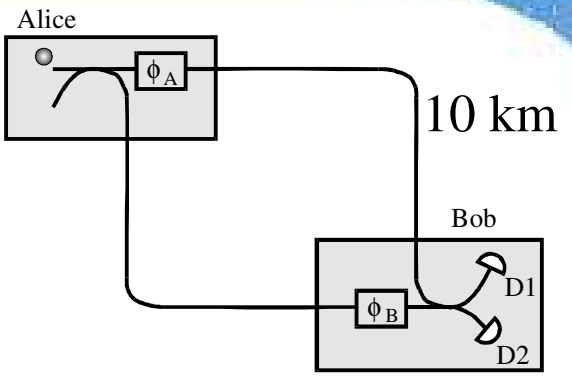




Phase-Coding QKD Approach

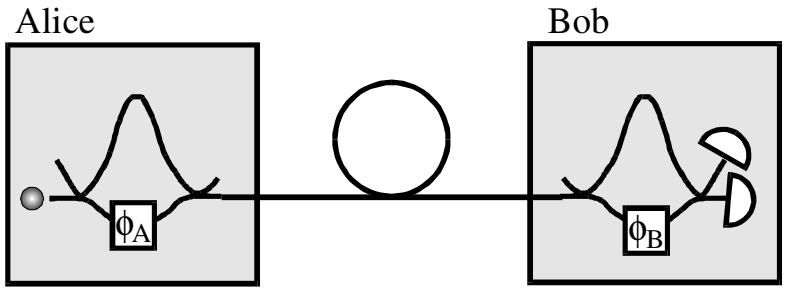
Mach-Zehnder implementation

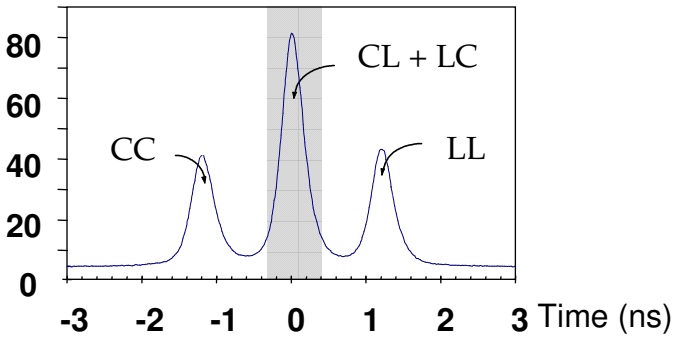
- Stability of such system is problematic



$$10\ \text{km} \pm \lambda/10\ (100\ \text{nm})$$

- In practice

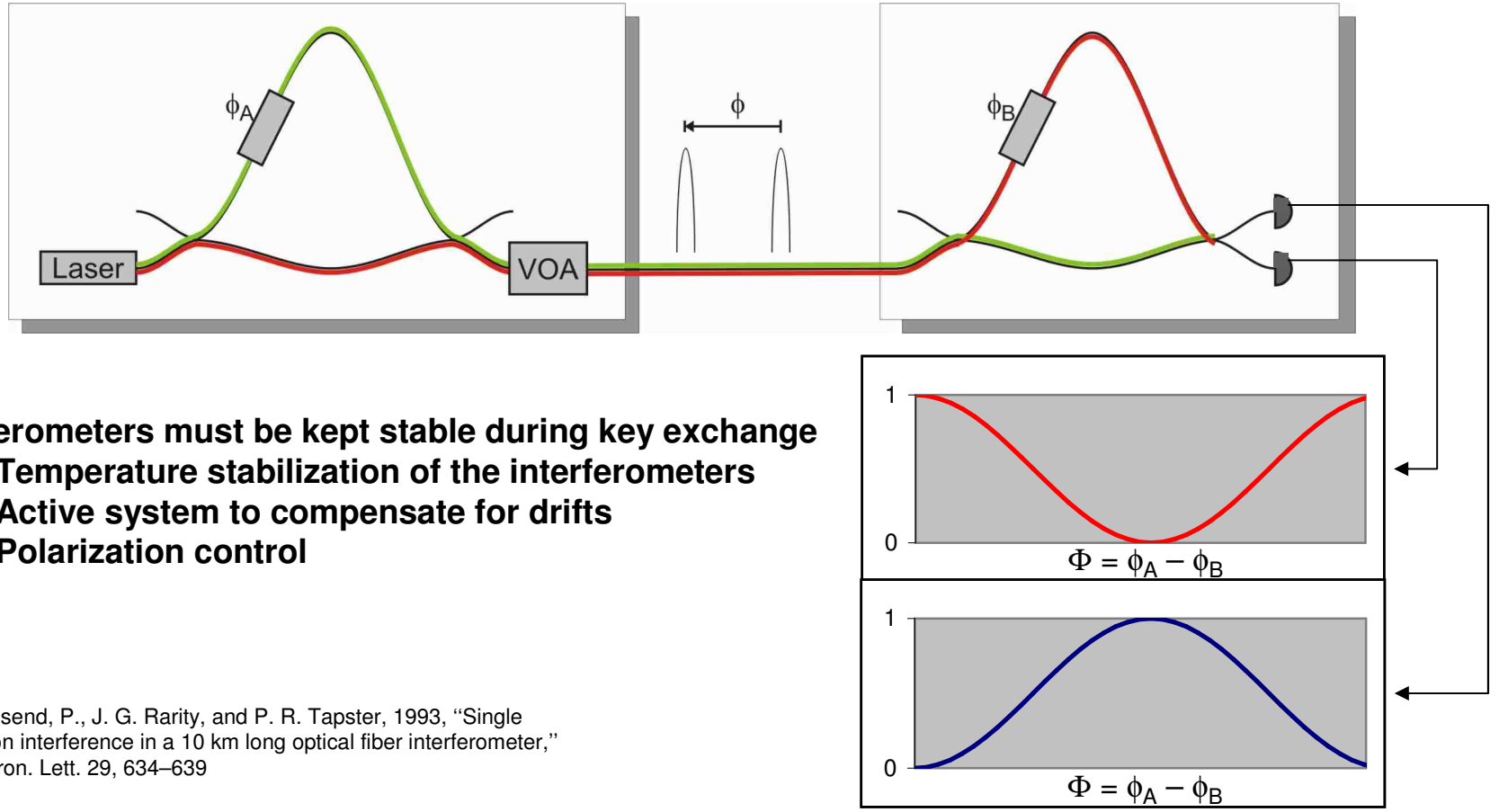




Phase-Coding QKD Approach

Double Mach-Zehnder implementation

Phase encoding between two time bins



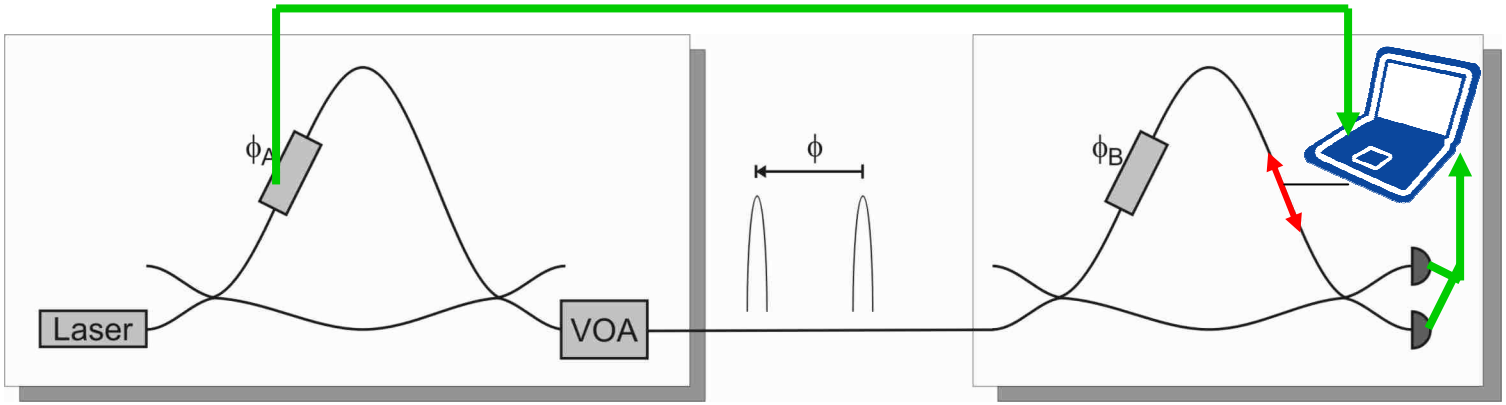
Interferometers must be kept stable during key exchange

- **Temperature stabilization of the interferometers**
- **Active system to compensate for drifts**
- **Polarization control**

Townsend, P., J. G. Rarity, and P. R. Tapster, 1993, "Single photon interference in a 10 km long optical fiber interferometer," Electron. Lett. 29, 634–639

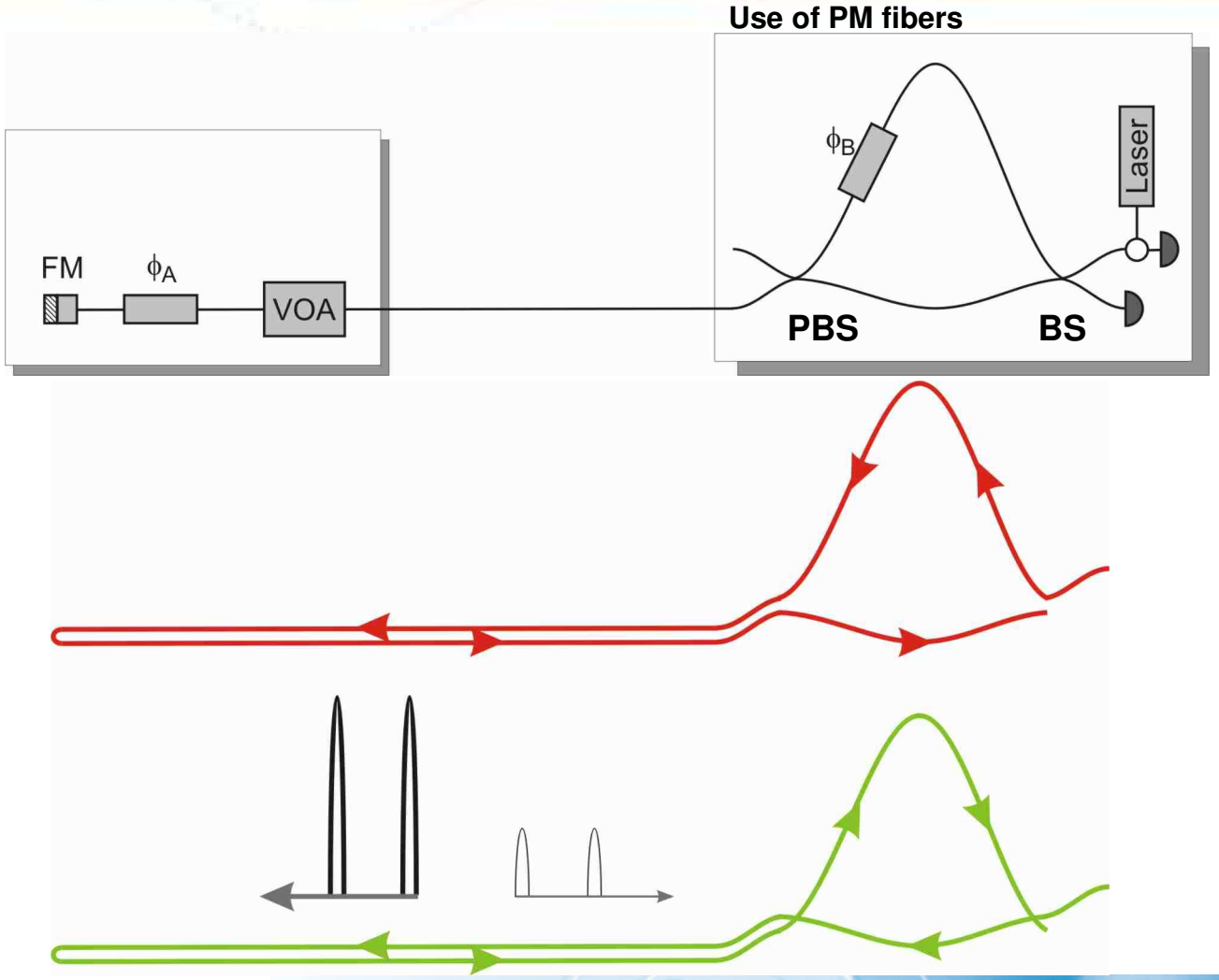
Motivation for autocompensating QKD

- Phase-coding scheme
  - Path length adjustment requires classical communication



- Autocompensating approach
  - Possibility to perform adjustment locally

Plug & Play Phase-Coding System

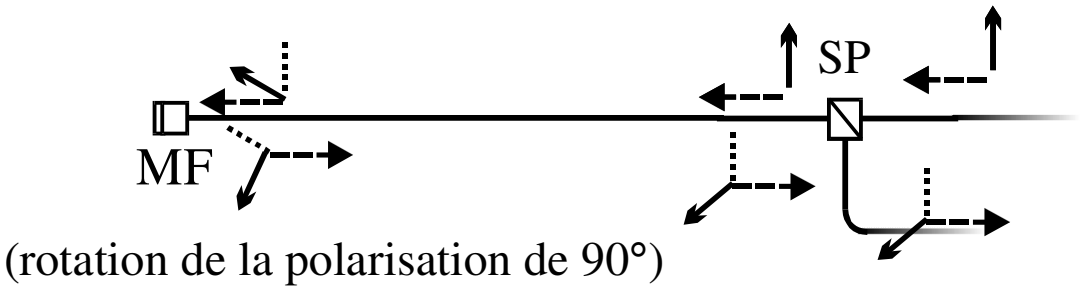


Source:
faint laser pulses

Gisin's group, Geneva

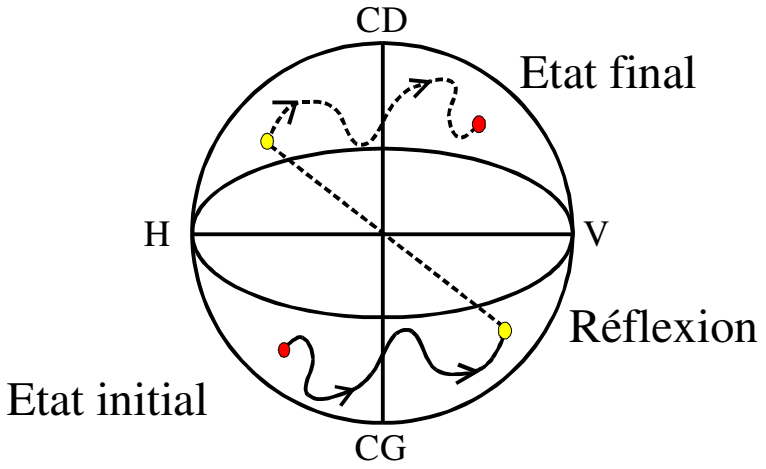
Plug & Play Phase-Coding System

Ø Birefringence compensation



(rotation de la polarisation de 90°)

Poincaré sphere representation



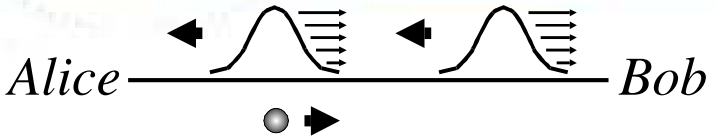
Main advantage:

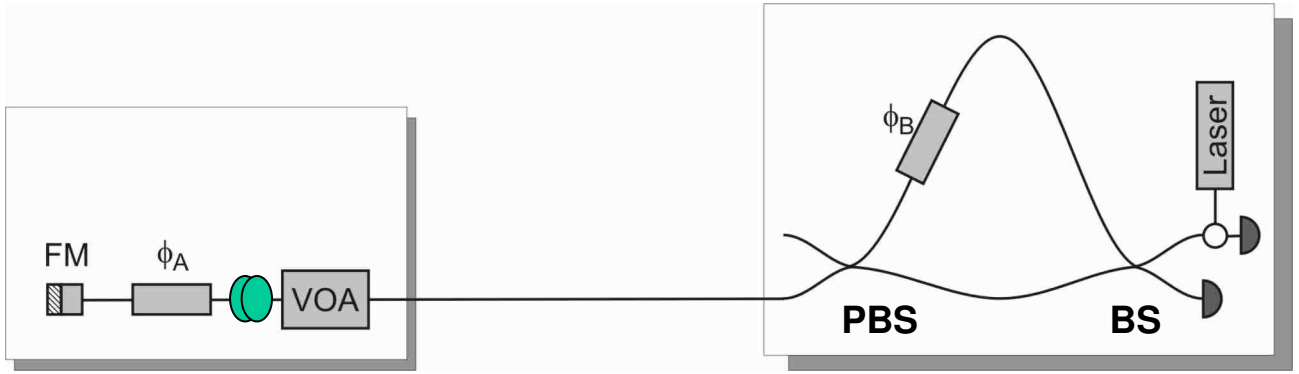
Output polarization state is orthogonal to the input state

ð Automatic and passive compensation for all polarization fluctuations in optical fibers

ð No adjustment necessary; stable system!

Plug & Play Phase-Coding System



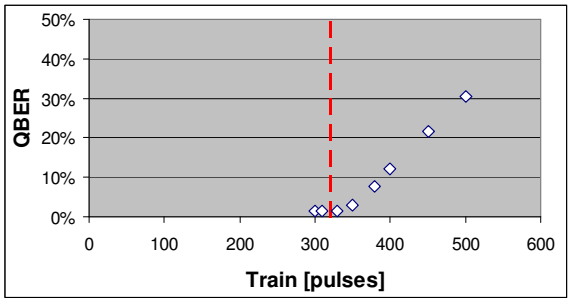


Source:
faint laser pulses

Use of PM fibers

Disadvantage #1:

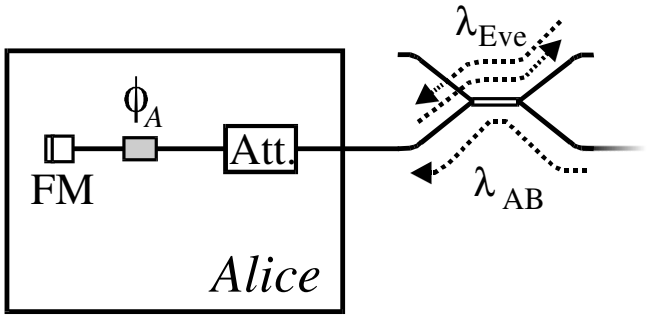
Rayleigh backscattering
ð requires optical delay line using fiber spool
ð Bob emits trains of pulses
ð bit rate reduction



Plug & Play Phase-Coding System

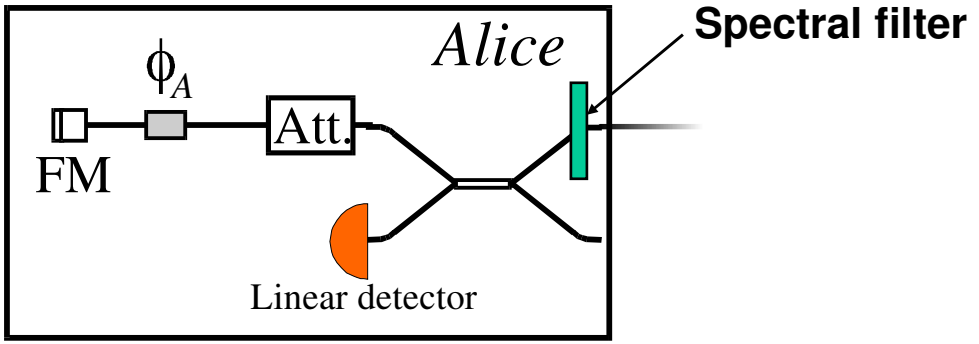
Disadvantage #2:

Eve could send probe beam and recover it through reflections at the mirror (Trojan horse attack)

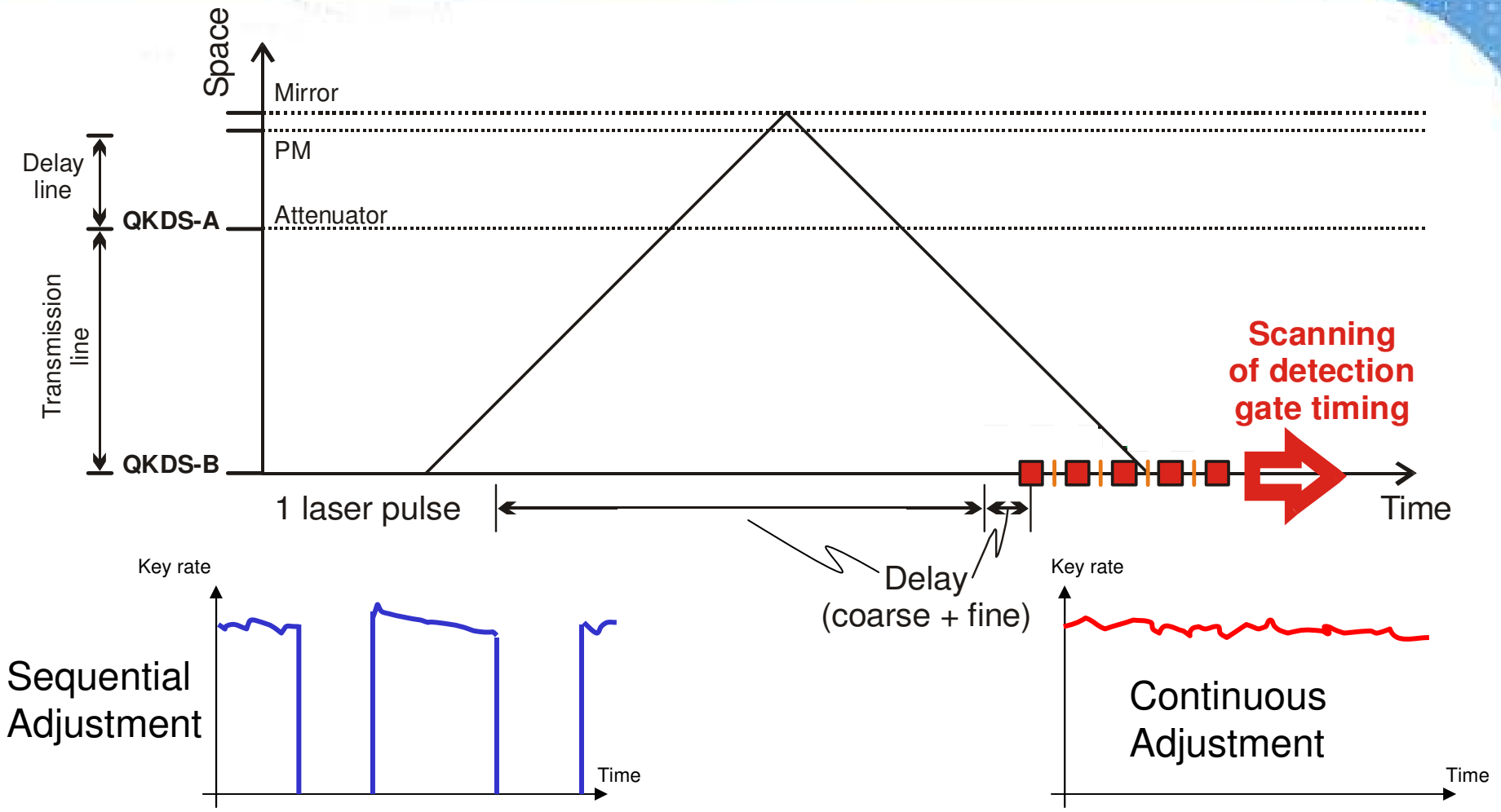


Solution:

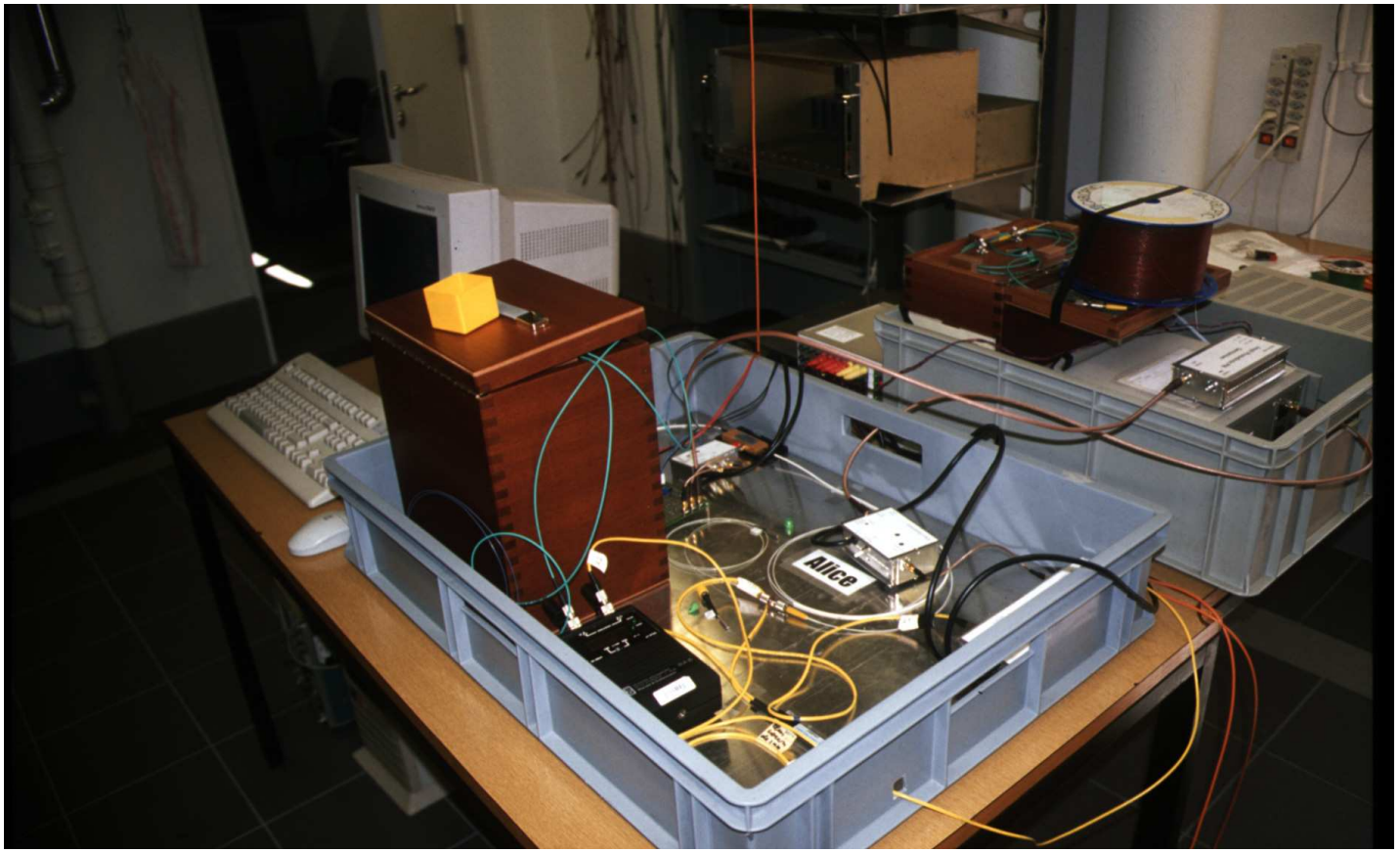
Add an attenuator in Alice to reduce amount of light through her system, and monitor incoming intensity using classical detector.



Time-of-flight Measurement



Initial experiments

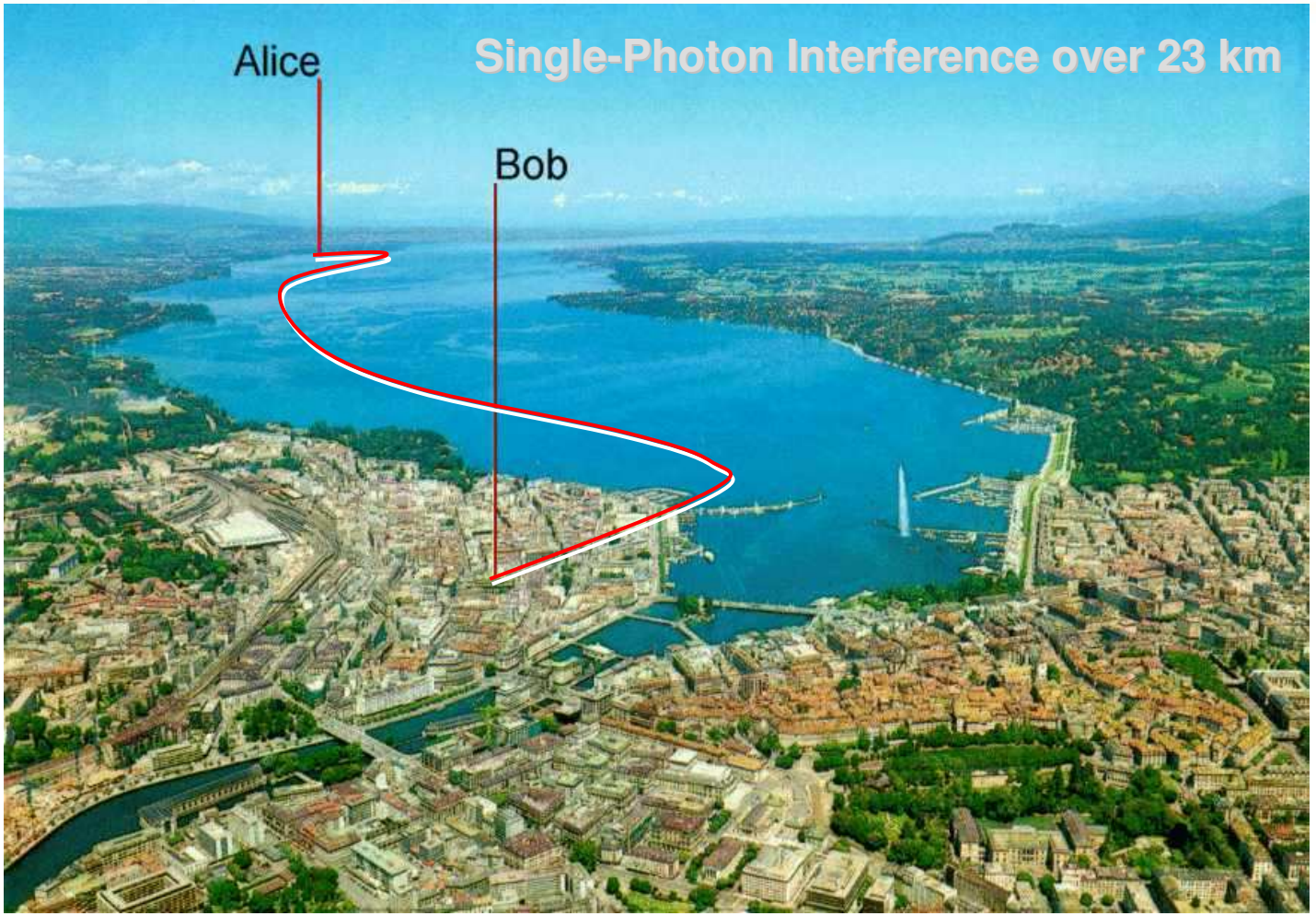


September 1996
August 1998

UNIVERSITÉ DE GENÈVE

id Quantique

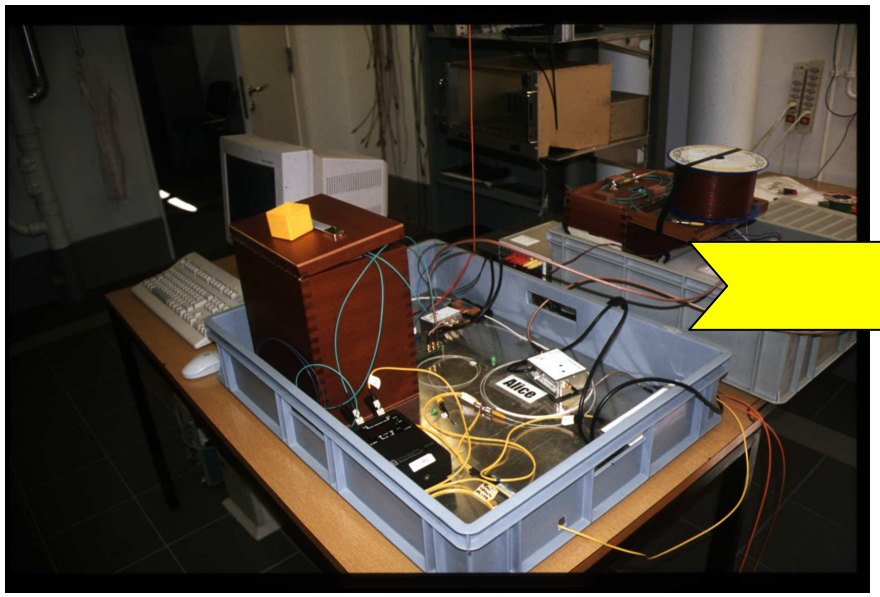
Extensively tested platform



id Quantique

1998 – 2002

From the breadboard…



to Clavis…

1998 – 2002

Ø Features of Clavis

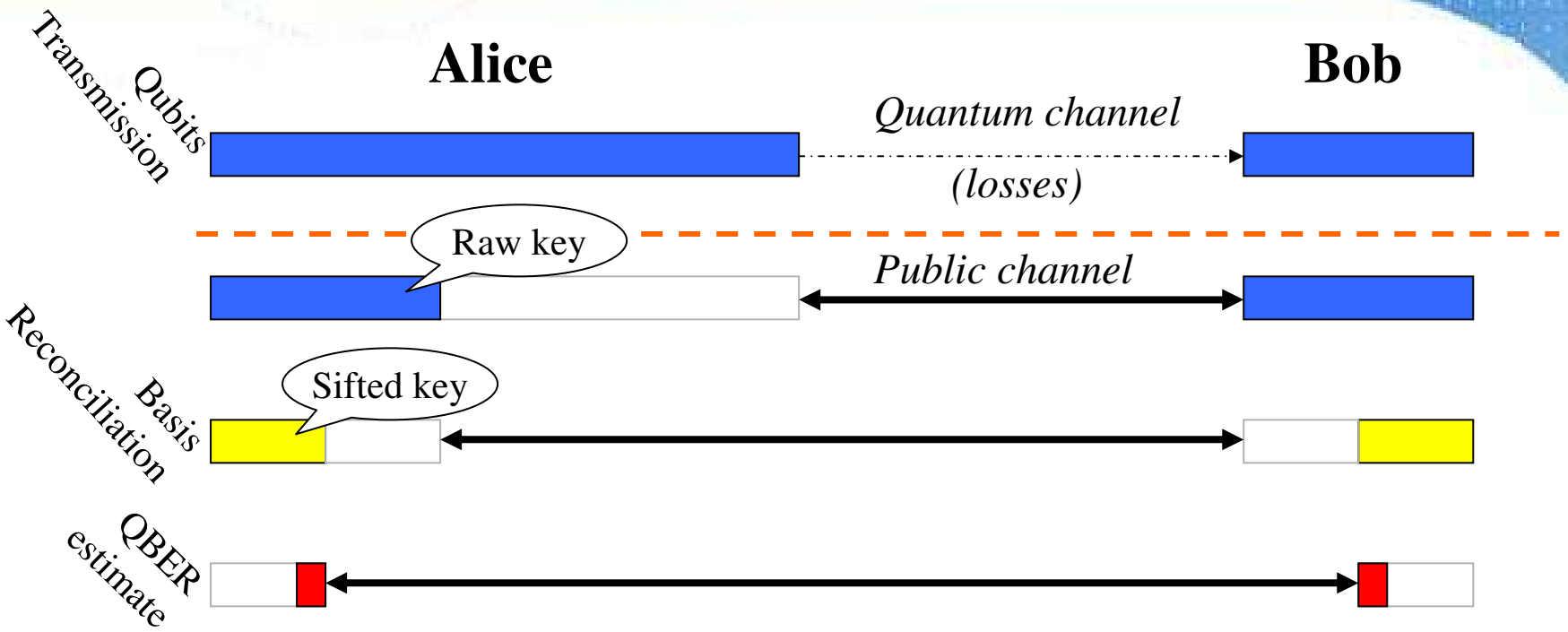
- Auto-compensating (patented) interferometric set-up
- Comprehensive software suite
- C++ library for system programming
- Encrypted file transfer

Technical Specifications

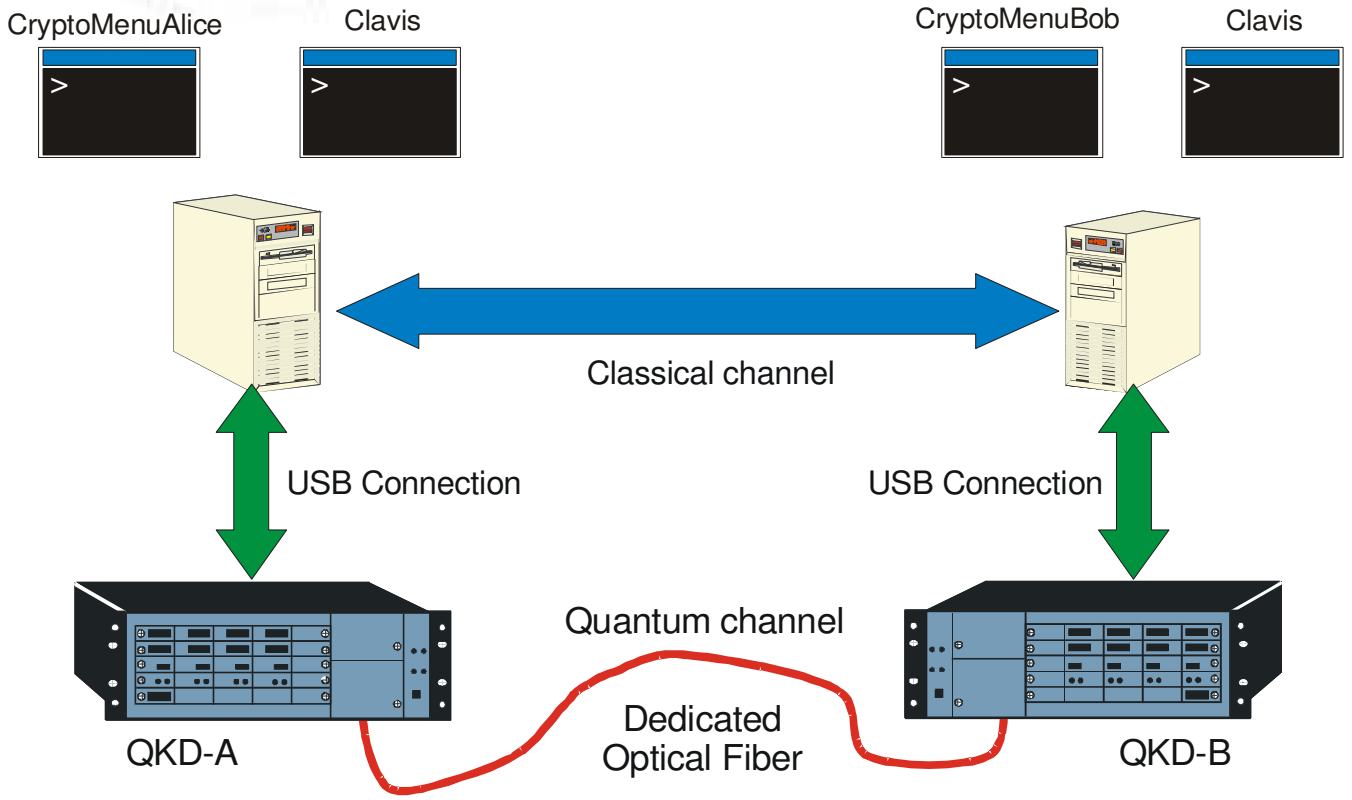
Key exchange		
Maximum transmission range	100	km
Raw key exchange rate[2]	> 1500	bits/s
[2] : over 25 km		
Key distillation		
BB84 and SARG protocols implemented		
Sifting		
Error correction (with confirmation)		
Privacy amplification		
Authentication		
Data encryption		
Automated key management		
Triple-DES (ANSI 9.52, 168 bits), AES 128-192-256 encryption		
Data authentication		
Interfaces and Inputs/outputs		
Optical connector (front panel)		FC/PC
Optical fiber type		SMF-28
USB interface (rear panel)		USB
Output Sync signals connectors		BNC
- QKDS-A		Classical detector, phase modulator
- QKDS-B		Laser source, phase modulator

id Quantique

Key distillation

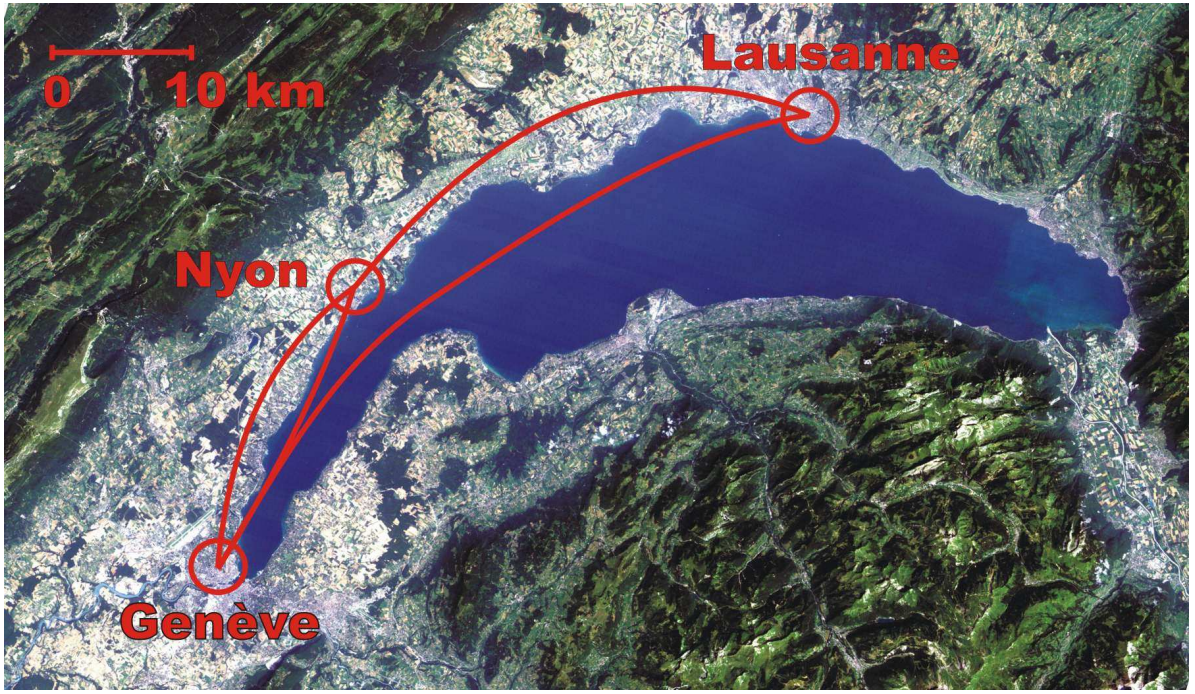


Clavis software



Versatile product: allows to change all important system parameters.

Extensively tested platform



RMP 74, 145-195, 2002,
Quant-ph/0101098

Raw Key Production over 67 km, QBER ≈ 5%

D. Stucki et al., New Journal of Physics
4, 41.1-41.8, 2002. Quant-ph/0203118

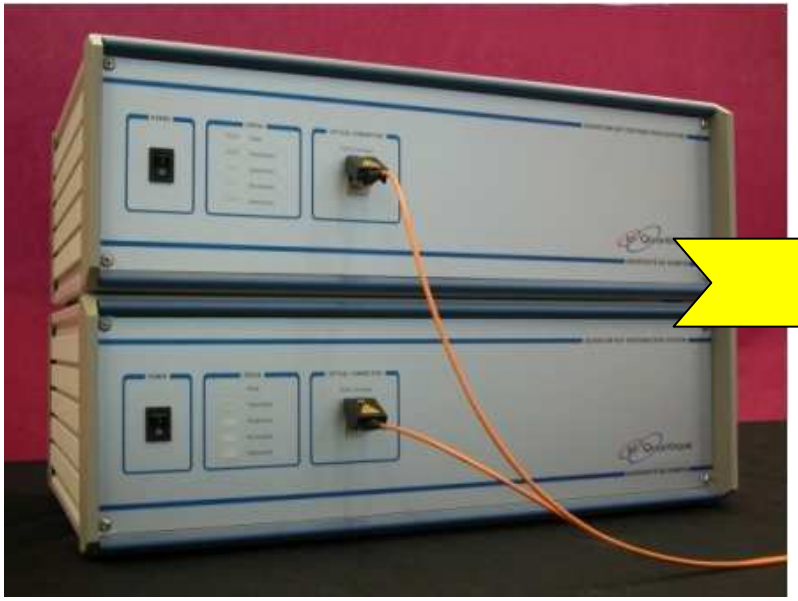
id Quantique

Outline

- Introduction
- Historical perspective on optical platforms and QKD experiments
- Vectis Link Encryptor – state-of-the-art encryption appliance
- Challenges facing the deployment in networks
- Future directions

2002 - 2006

From Clavis…



R&D Platform
Sifted key production

Users: physicist

To Vectis….

Network Appliance
Secret key exchange
Encryption engines
System management

Users: IT manager

Vectis Link Encryptor – key features

Ethernet 100Mbps link encryption (IEEE 802.3u)

- Encryption algorithms: AES 128-bit, 192-bit, 256-bit
- Authentication algorithms: HMAC-SHA-1, HMAC-SHA-256
- Layer 2 encryption
- RFC2544 compliant

Automated key management

QKD protocols: BB84 and SARG

Nondeterministic RNG: Quantis

Network management

- On-line monitoring: SNMP v3 MIB (RFC2274)
- Off-line management: web server; touch panel display
- Identity-based authentication

Intrusion detection

- Tamper detection system
- Tamper-evident chassis

Redundant power supply

Vectis Link Encryptor – Interfaces

LAN
full-duplex 100Mbps Ethernet port
RJ-45

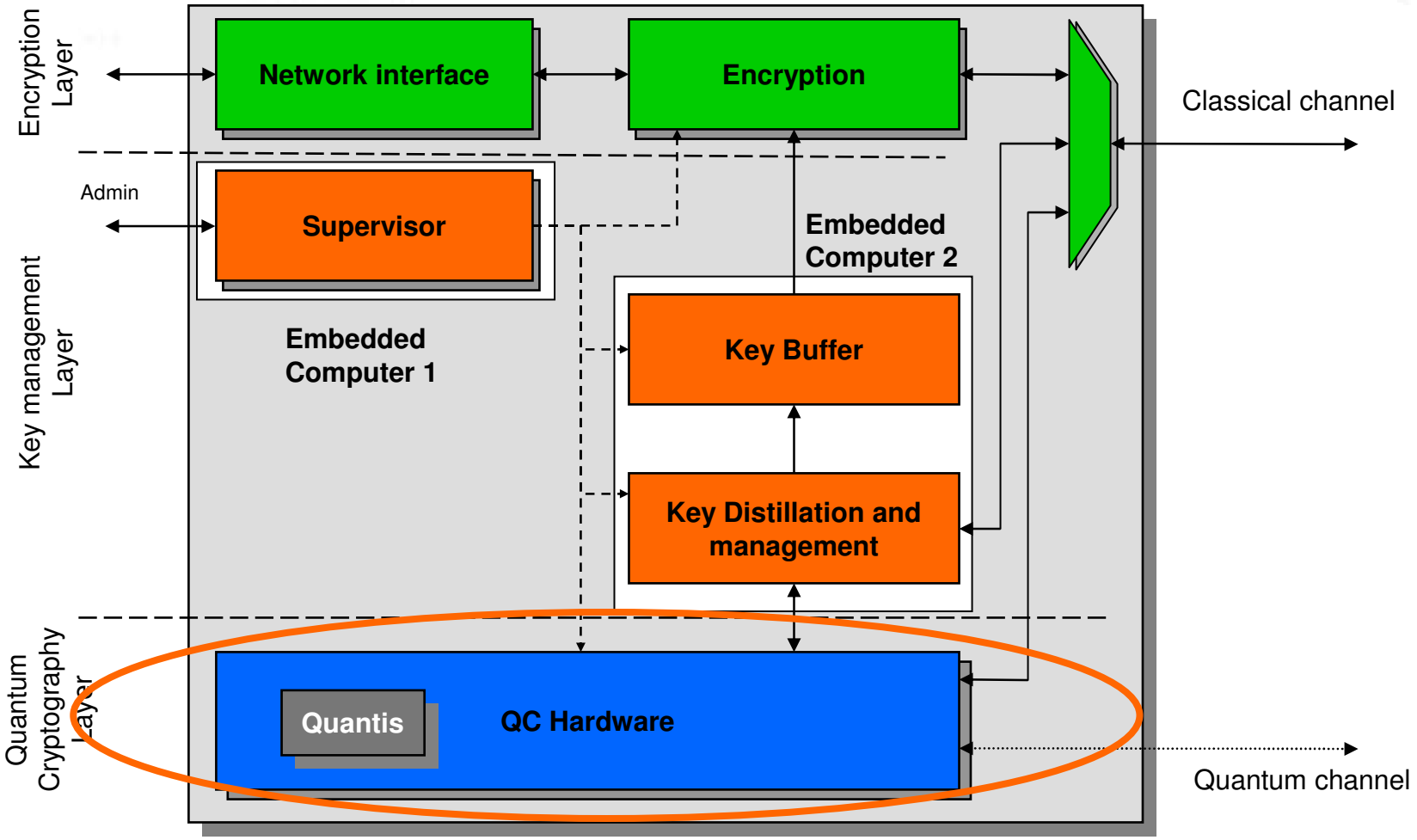
Secure Data Link
Bi-Di module for SMF
SC connector

Management
10/100 Ethernet (RJ-45)
RS-232
Indication LED

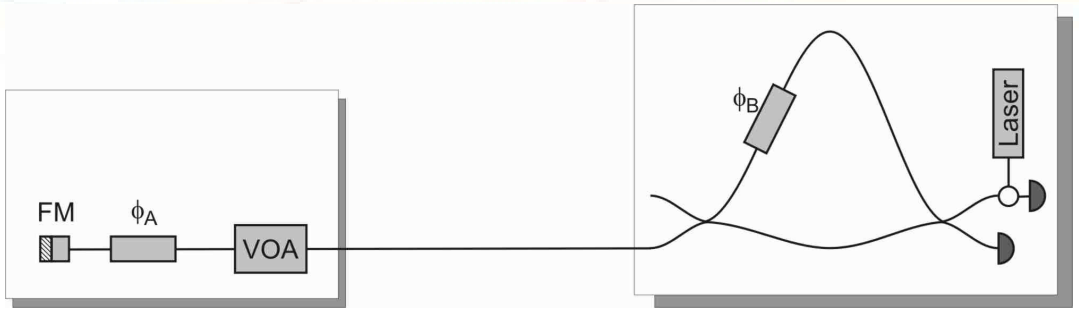
Quantum Channel Link
SMF, SC connector

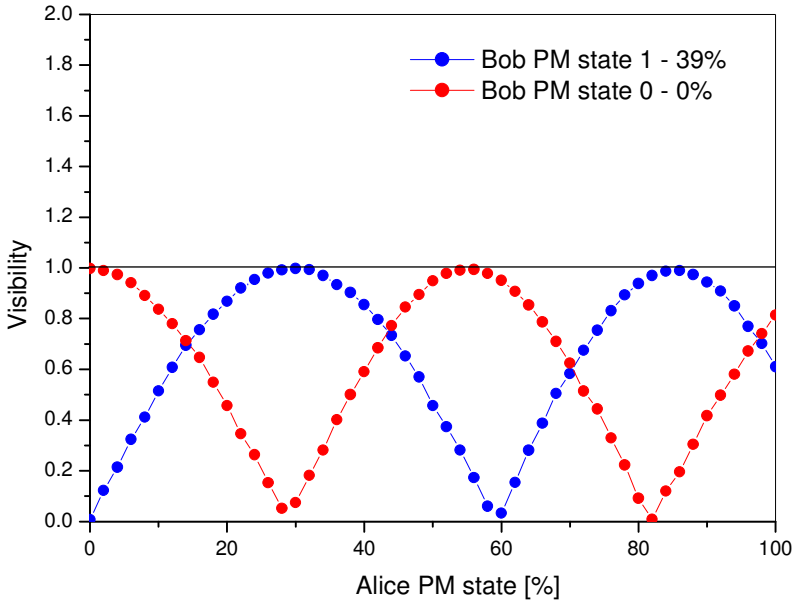
System Integration

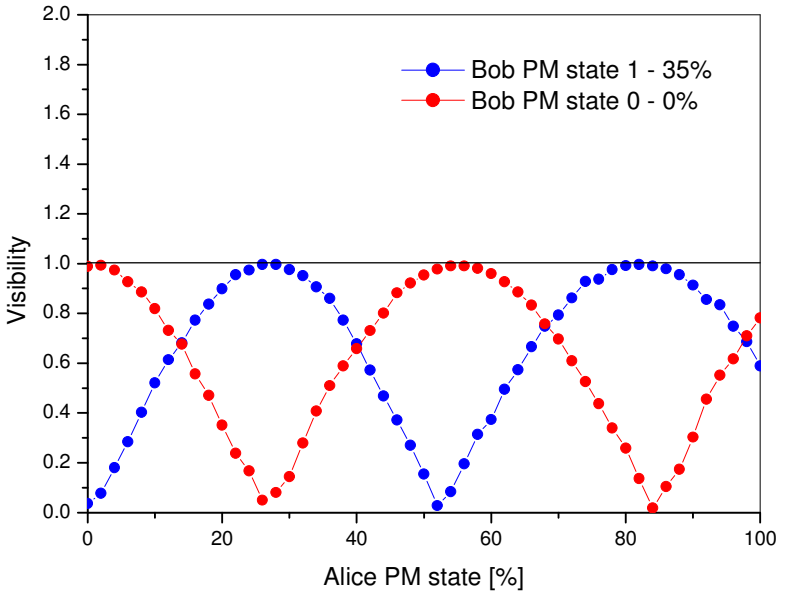
From customer's point of view, the system is completely symmetric.



Measured visibility of 2 appliances

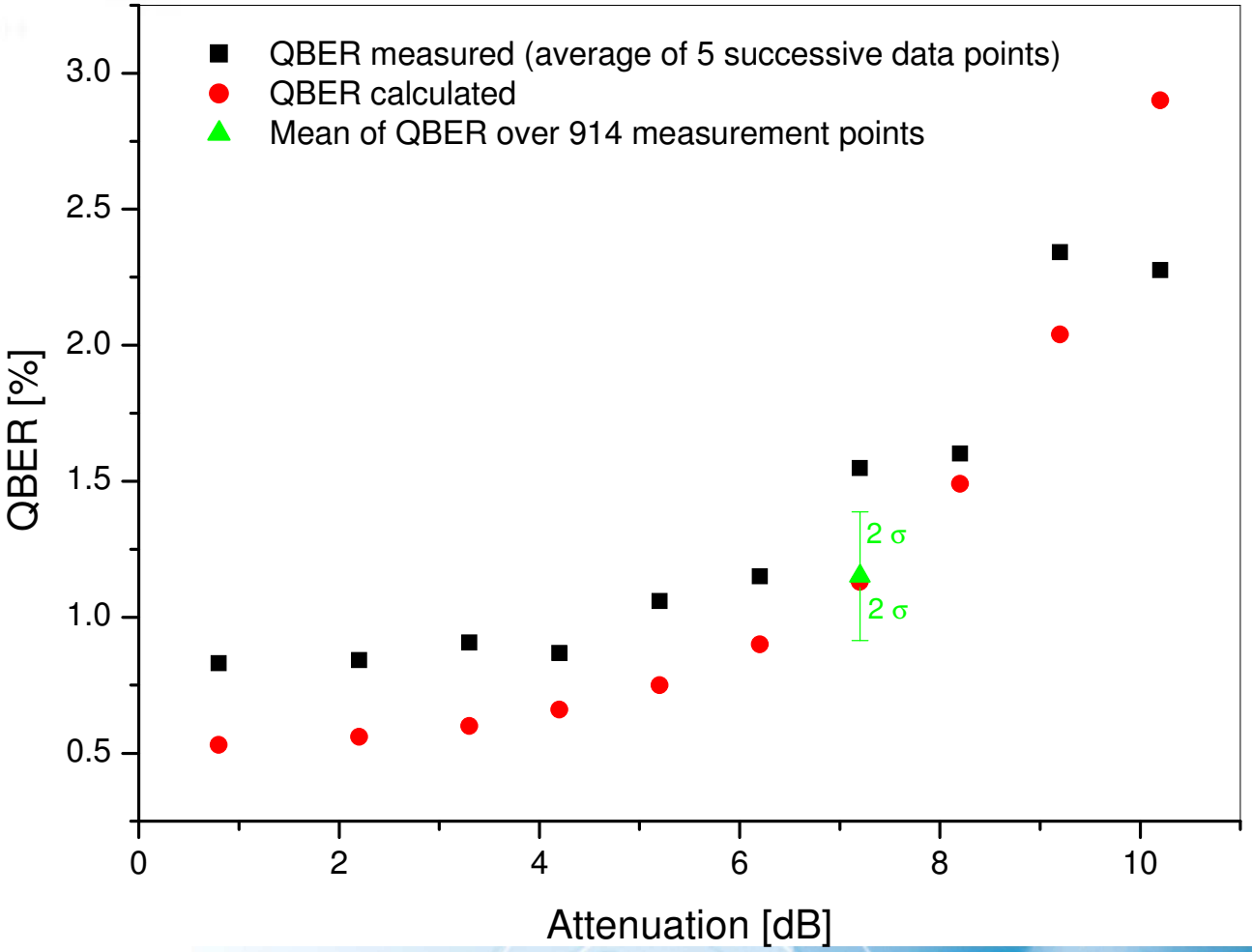




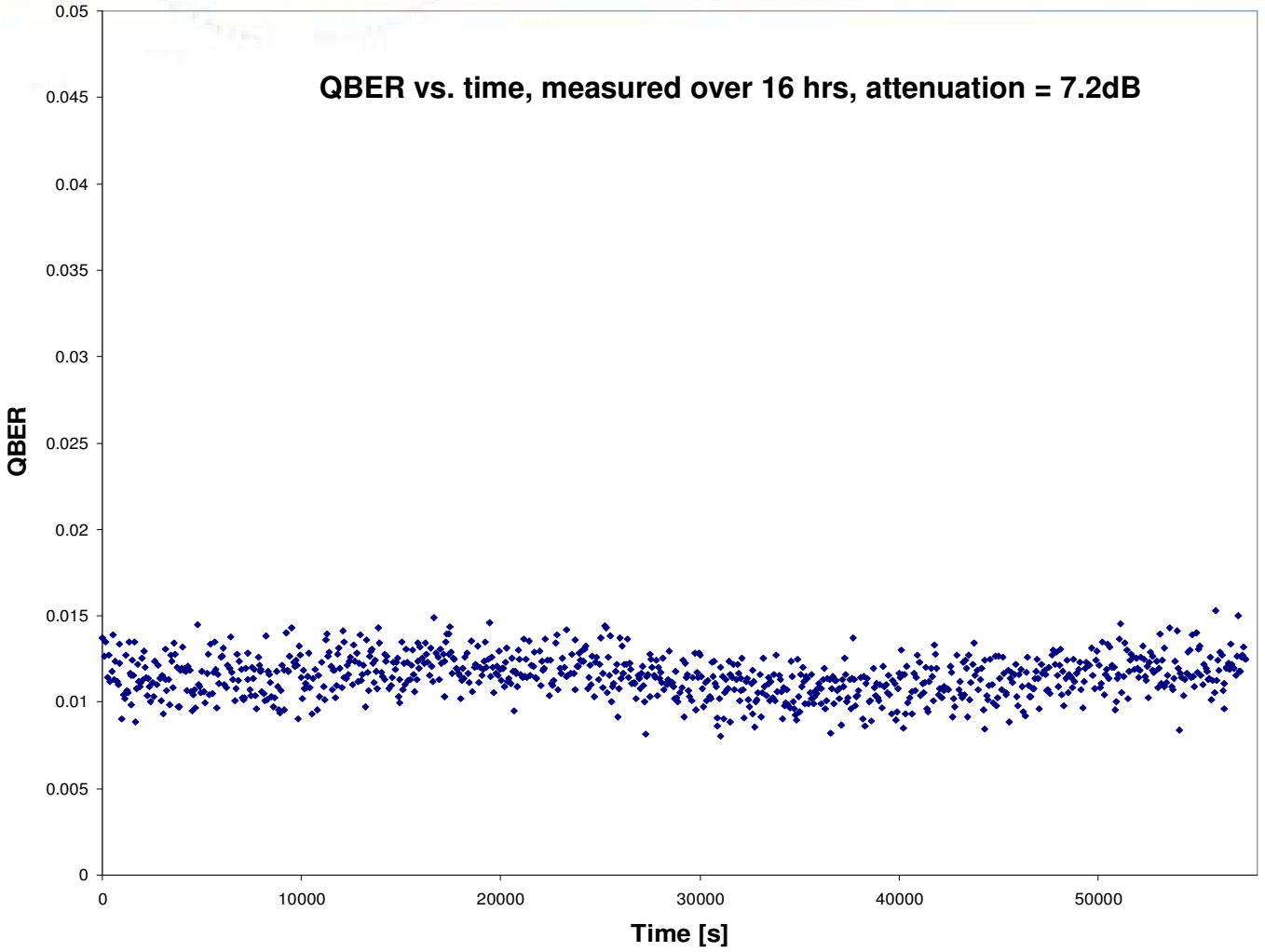


Visibility > 99.5% ð $QBER_{opt}$ < 0.4%

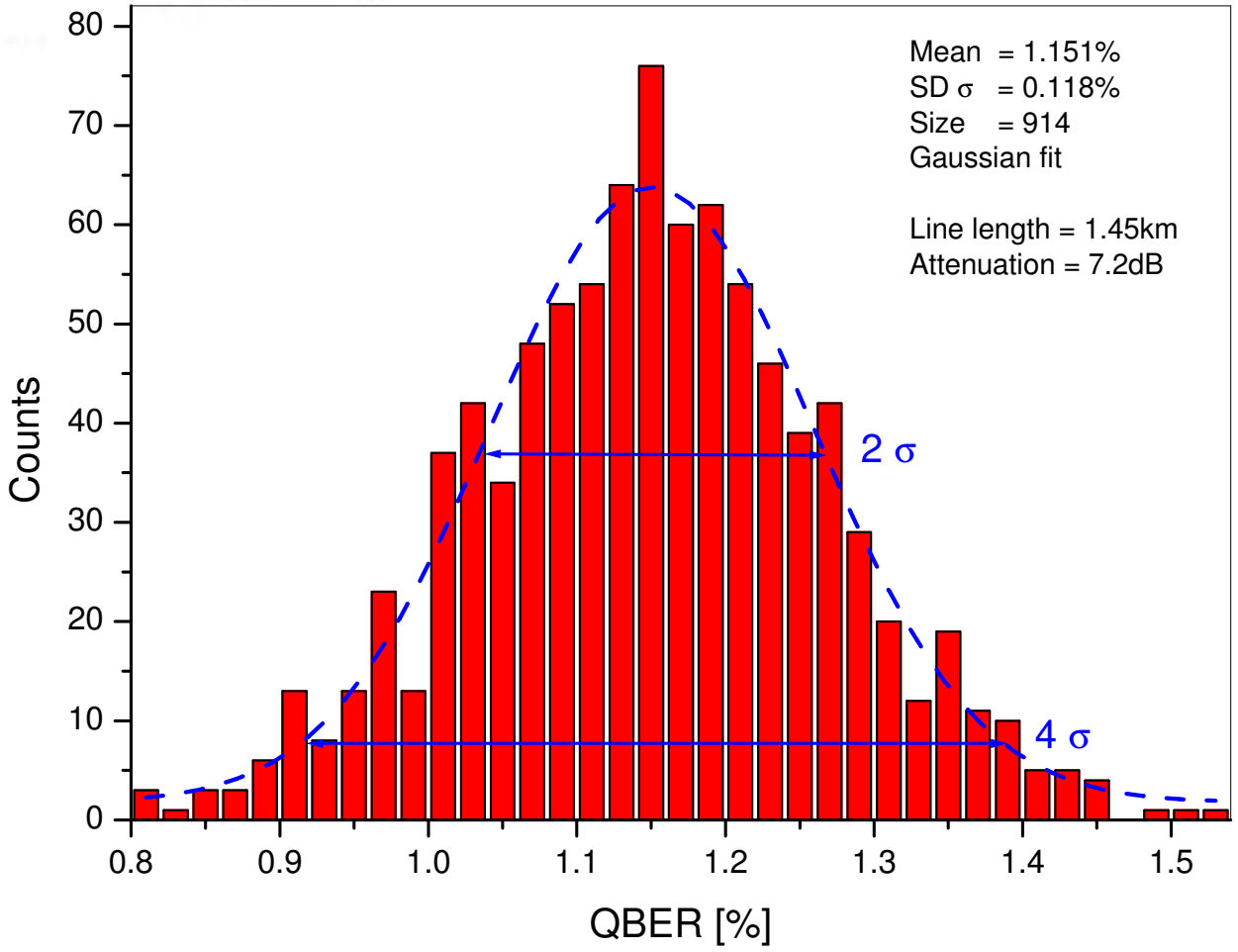
QBER vs. attenuation



Stability

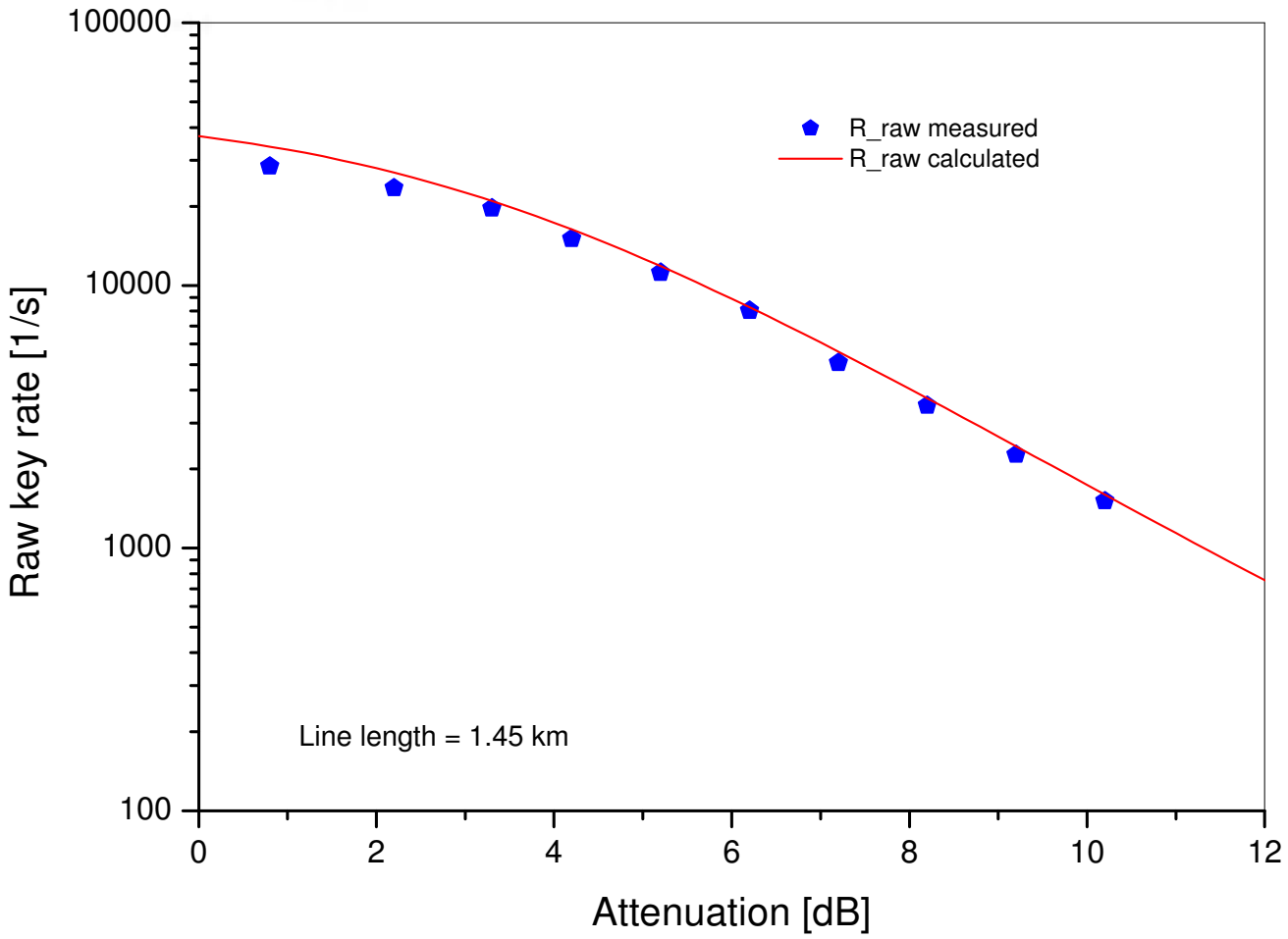

QBER vs. time, measured over 16 hrs, attenuation = 7.2dB
QBER
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
0
10000
20000
30000
40000
50000
Time [s]

Stability



id Quantique

Raw key rate



$$R_{raw} = q\, f_{rep}\, \mu\, t_{link}\, \eta$$

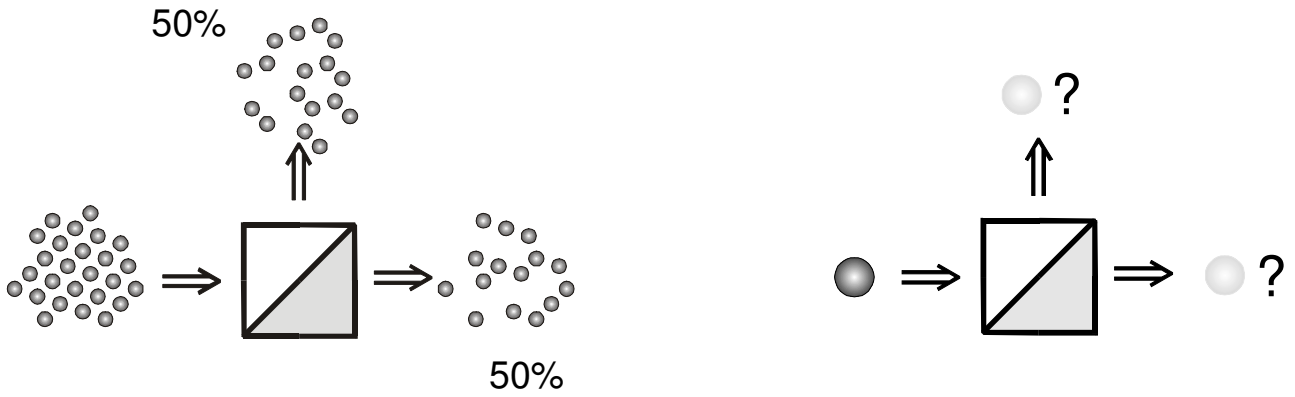
f_{rep} = pulse rate
μ = mean # photons / pulse
t_{link} = transmission
η = probability photon detection

Quantis RNG

- A single-photon constitutes an elementary quantum system

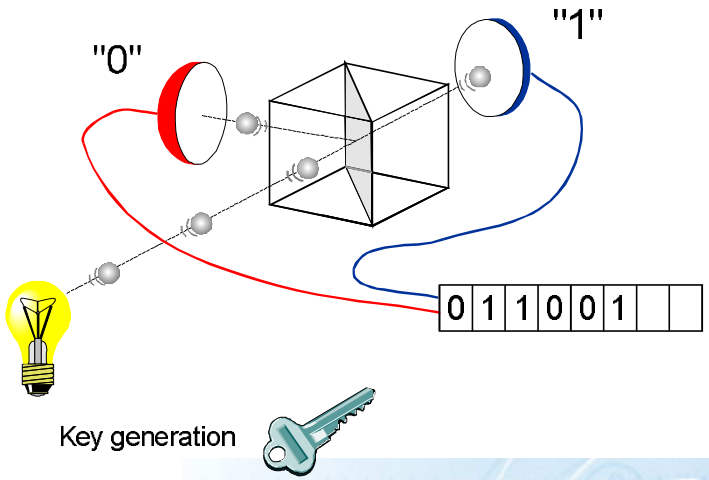
  It cannot be split

- Semi-transparent mirror

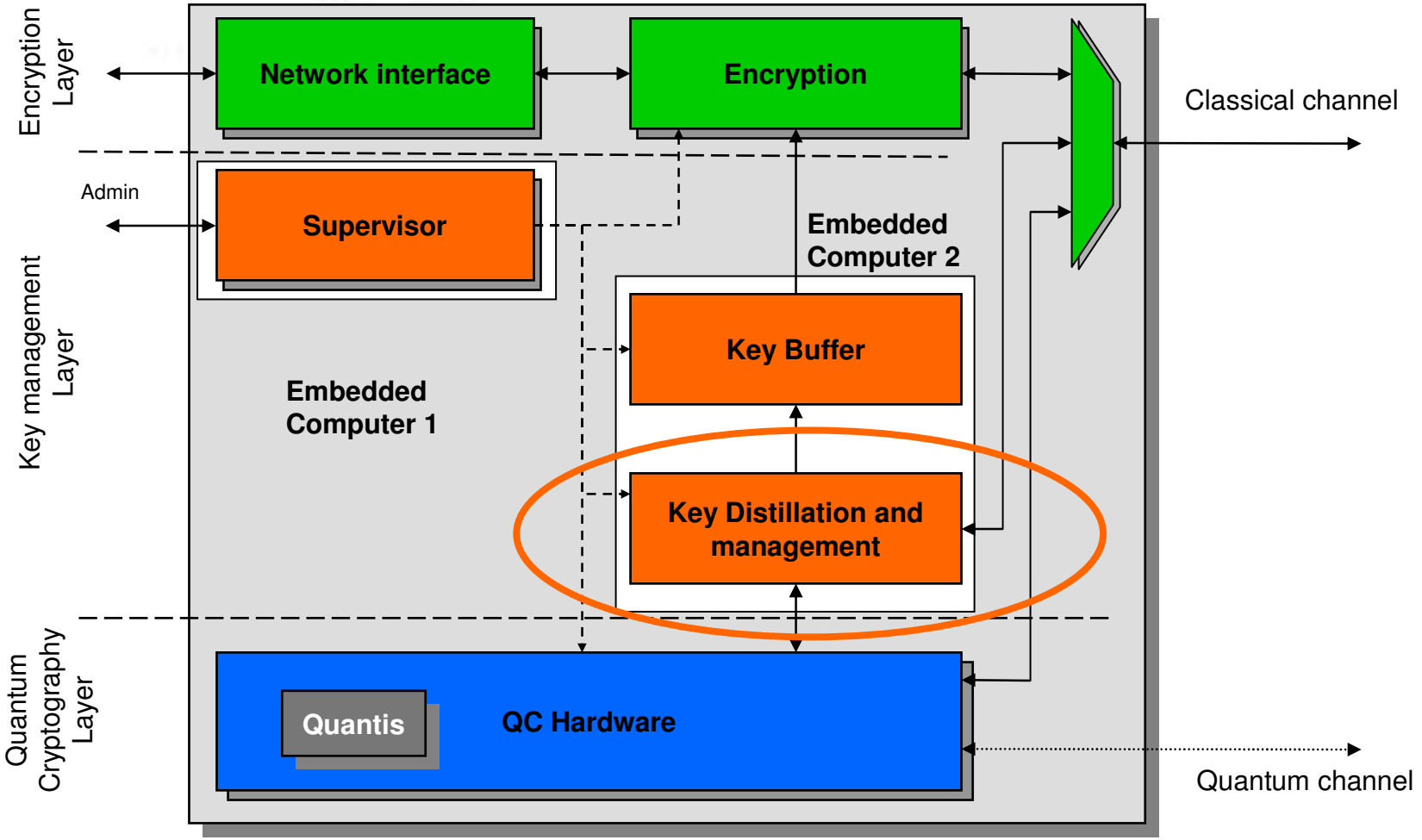


Quantis RNG

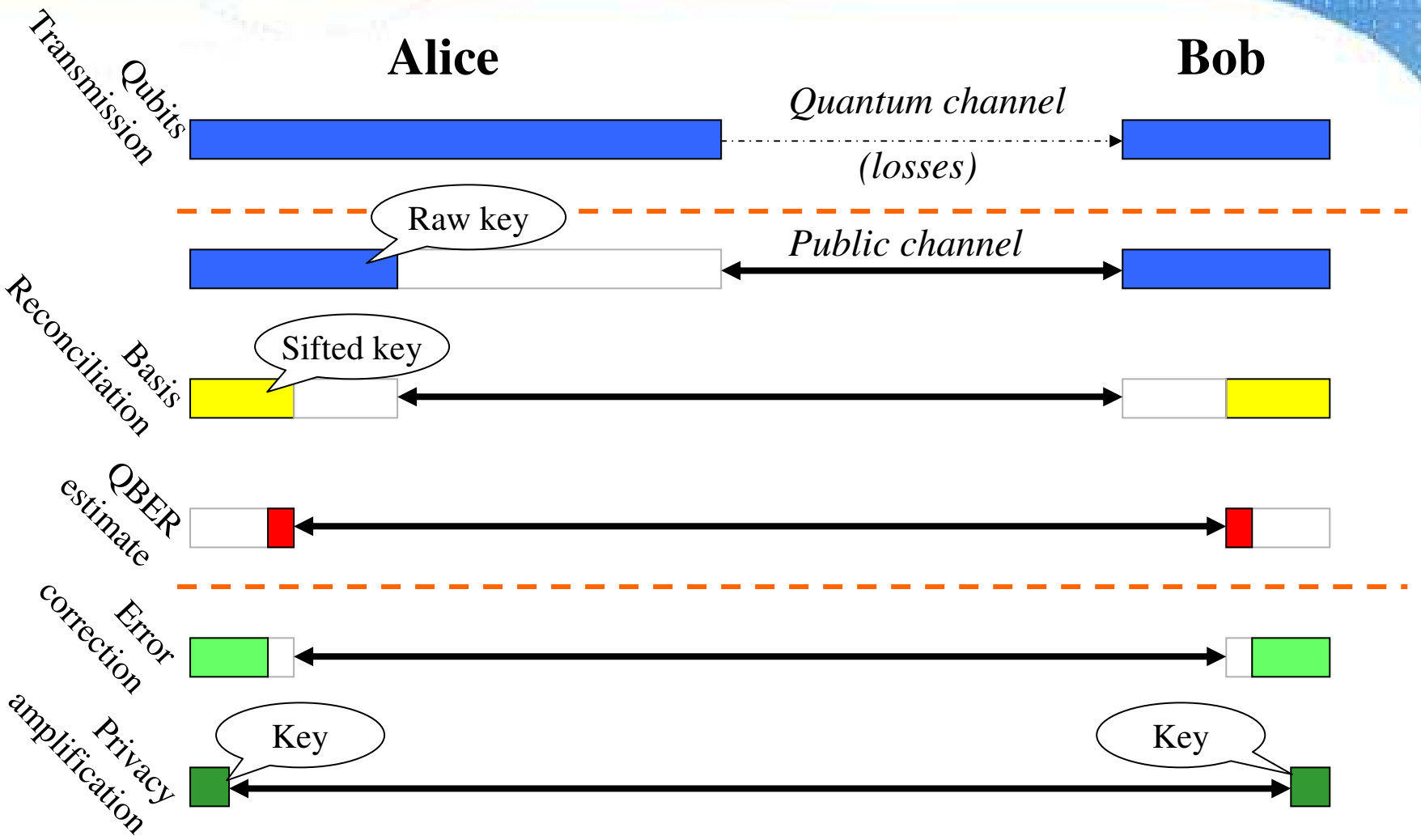
- Quantum physics is fundamentally random
- Cannot be influenced by any external parameters
- Output is completely unpredictable
- High bit rate
  - 4 or 16 Mbits/s



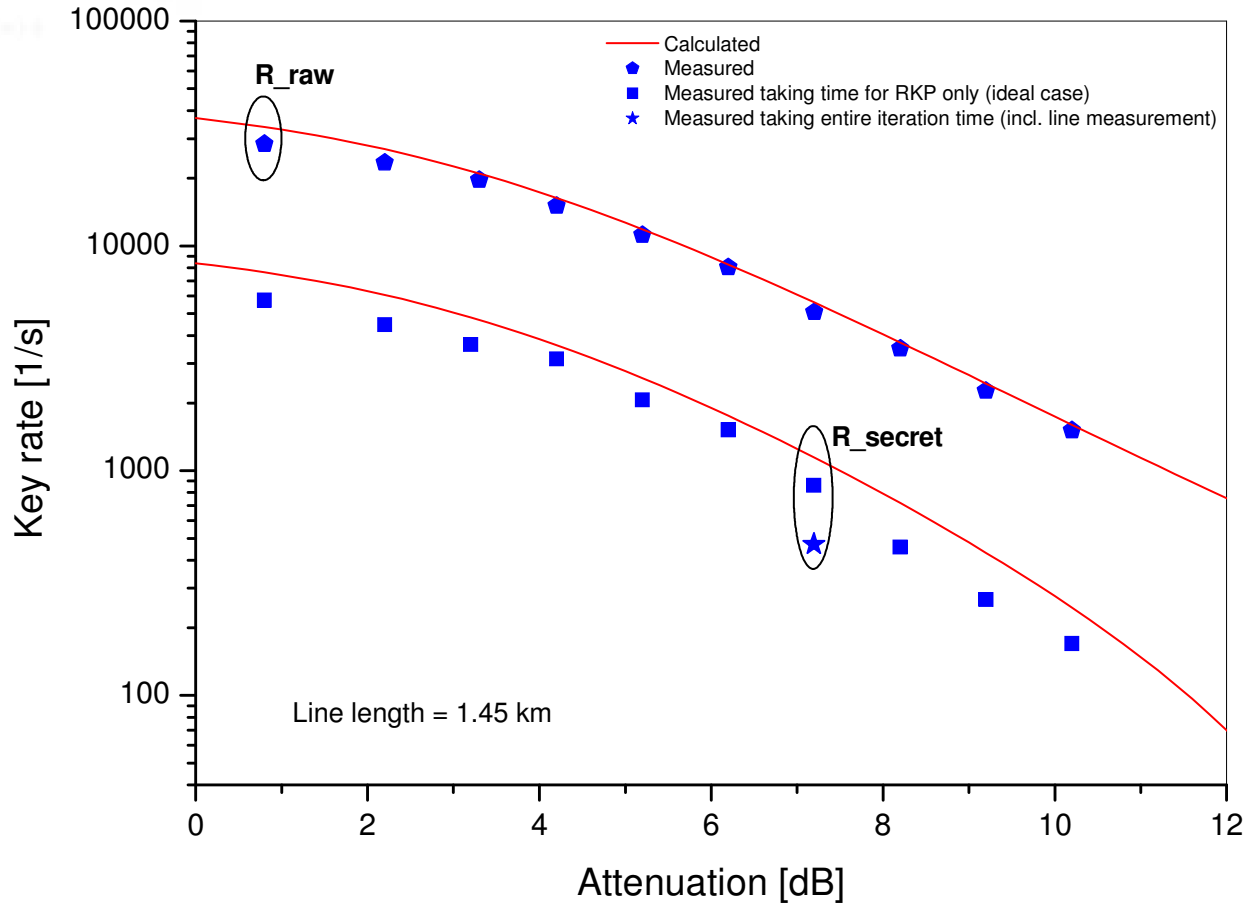
System Integration



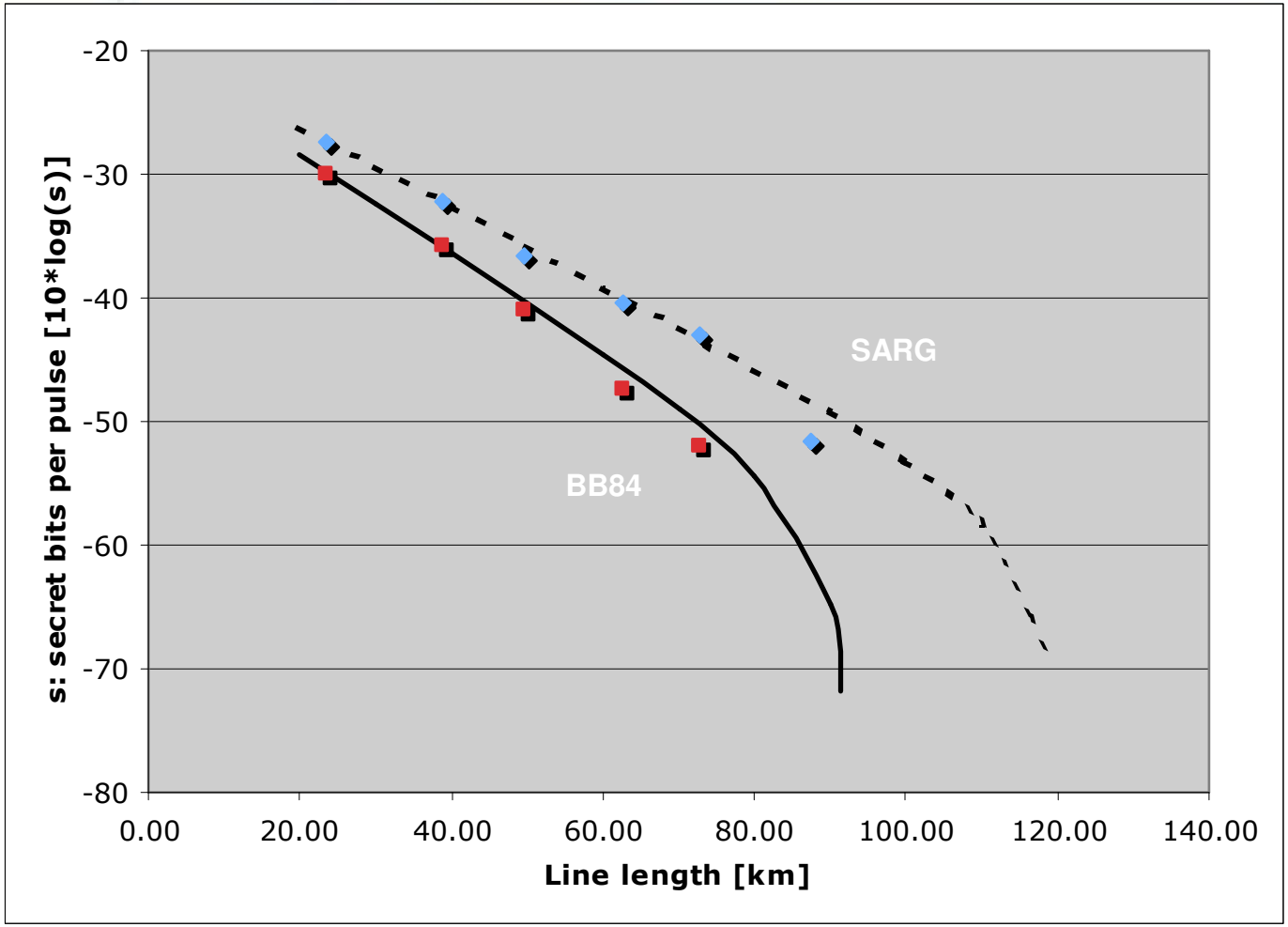
Key distillation



Secret key rate



BB84 vs. SARG


-20
-30
-40
-50
-60
-70
-80
s: secret bits per pulse [10*log(s)]
SARG
BB84
0.00
20.00
40.00
60.00
80.00
100.00
120.00
140.00
Line length [km]

Threat models taken into account

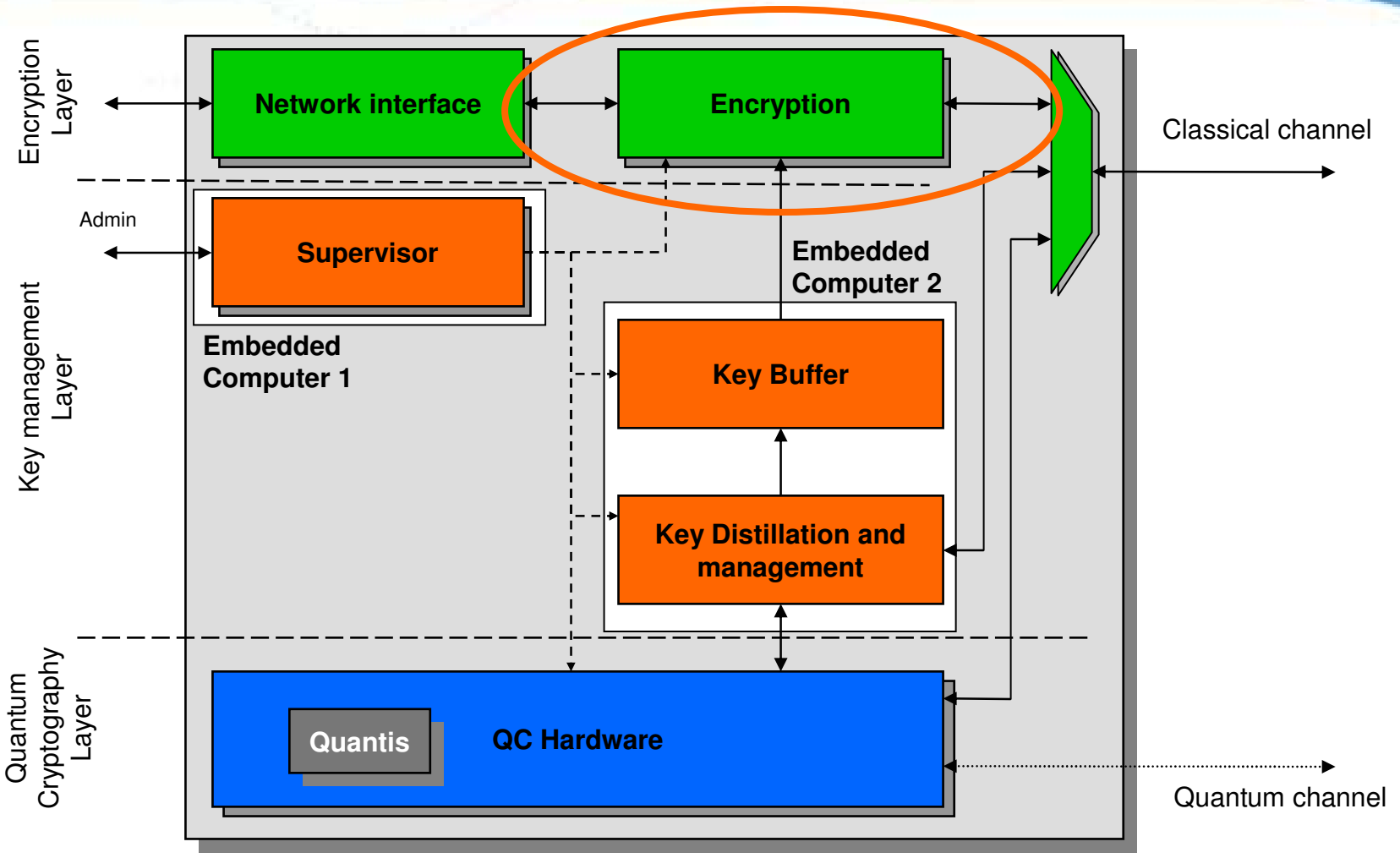
1. Optimal incoherent attacks for the pulses with n = 1 photon

2. Standard PNS attacks for the pulses with n >= 2 photons
3. Trojan horse attacks

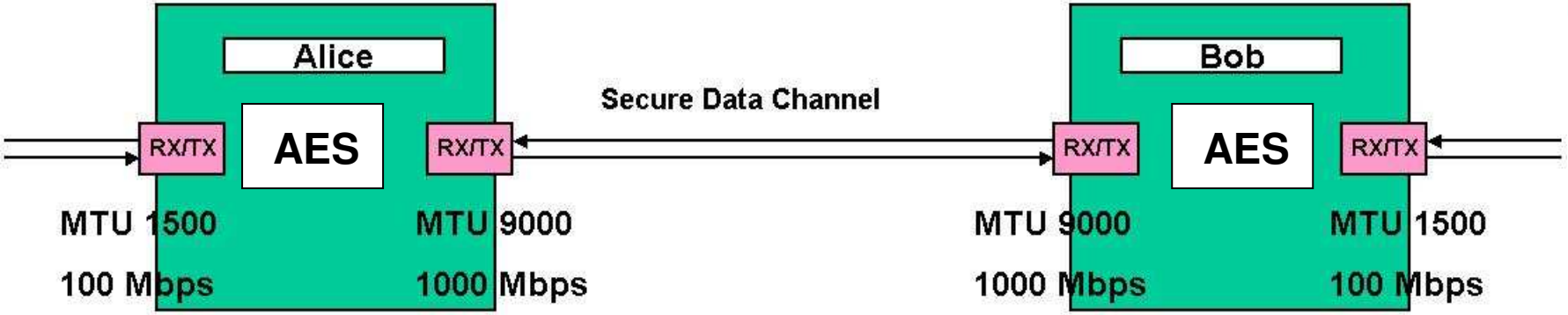
For BB84, see:

Photon-Number-Splitting versus Cloning Attacks in Practical Implementations of the Bennett-Brassard 1984 protocol for Quantum Cryptography, A. Niederberger, V. Scarani, N. Gisin

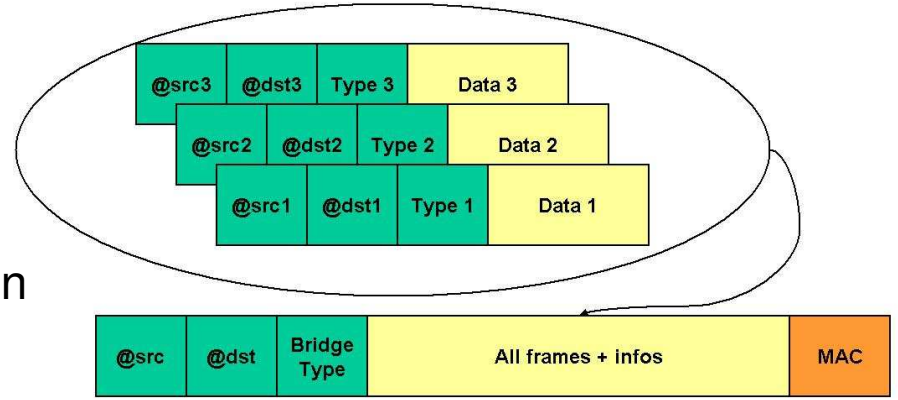
System Integration



Encryption Bridge Principle



Frame Encapsulation



Encrypt payload and headers, without impact on throughput

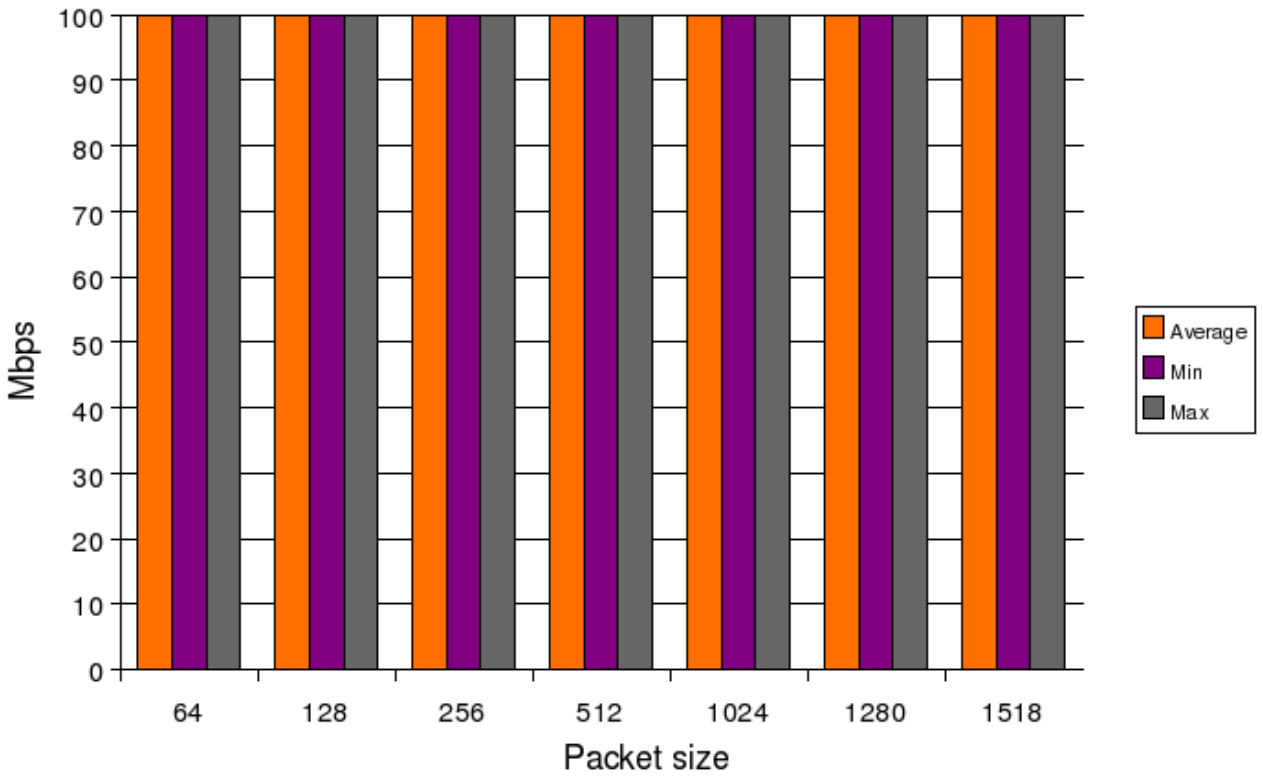
Testing of the encryption bridge

RFC 2544 benchmark tests:

w/ standard frame sizes of 64, 128, 256, 512, 1024, 1280 and 1518 byte

FTB-8510G Packet Blazer
EXFO

Bridge throughput



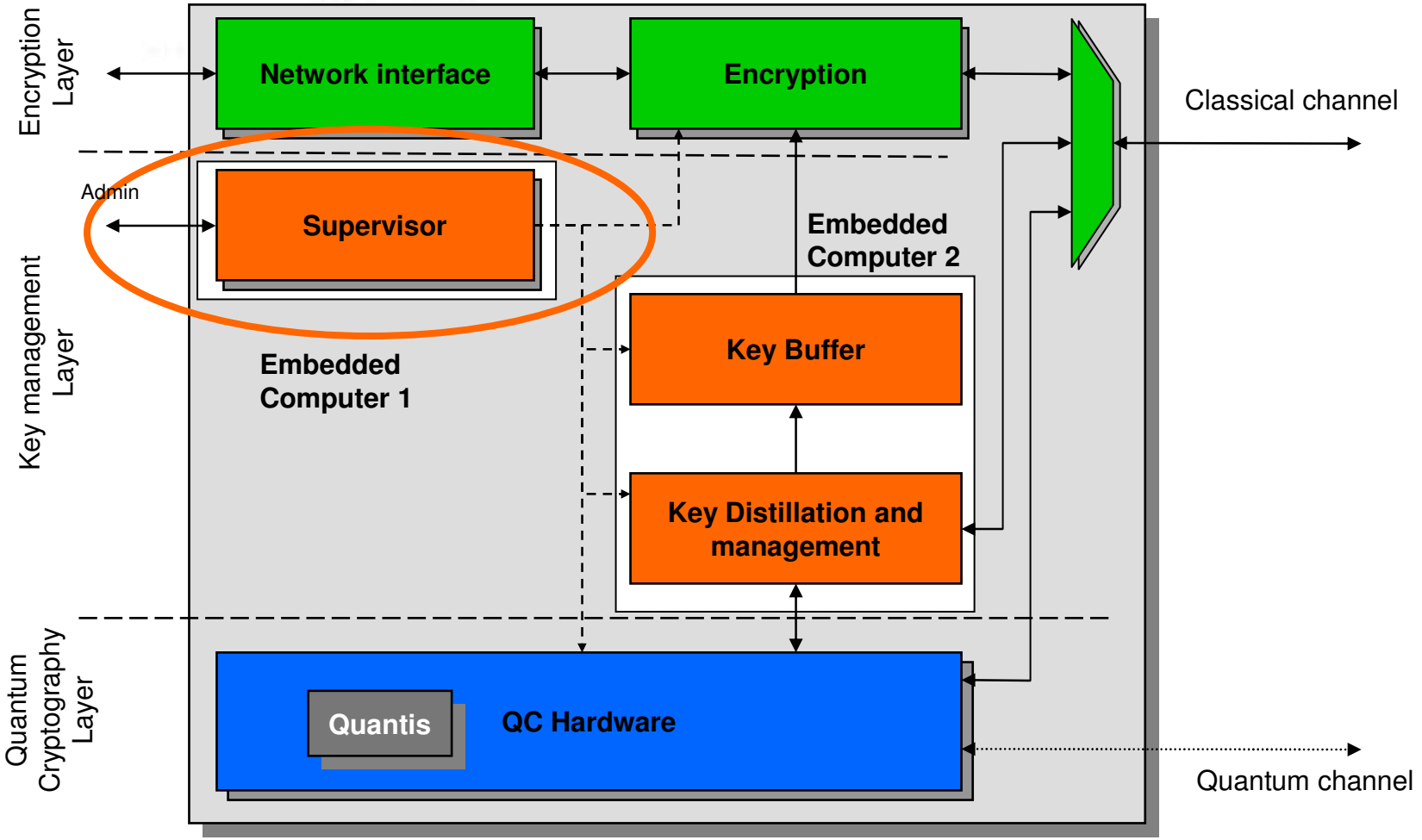
Layer 2 vs. Layer 3

Layer 2	Layer 3
100% bandwidth available	40% bandwidth available (encryption tax)
Negligable latency (< 5 us)	Latency with potential negative effects (≈ 40 us)
No frame loss at all frame sizes	Significant frame losses

Comparison performed on a SONET OC-48 link (Safenet Encryptor vs. Cisco VPN Blade) Rochester Institute of Technology

- Layer 2 Encryption in high-speed networks provides significant benefits

System Integration

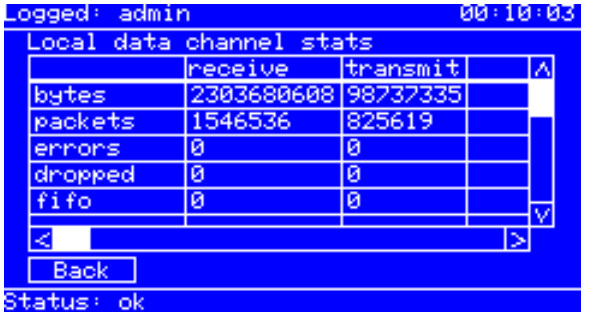


System Administration – User interface

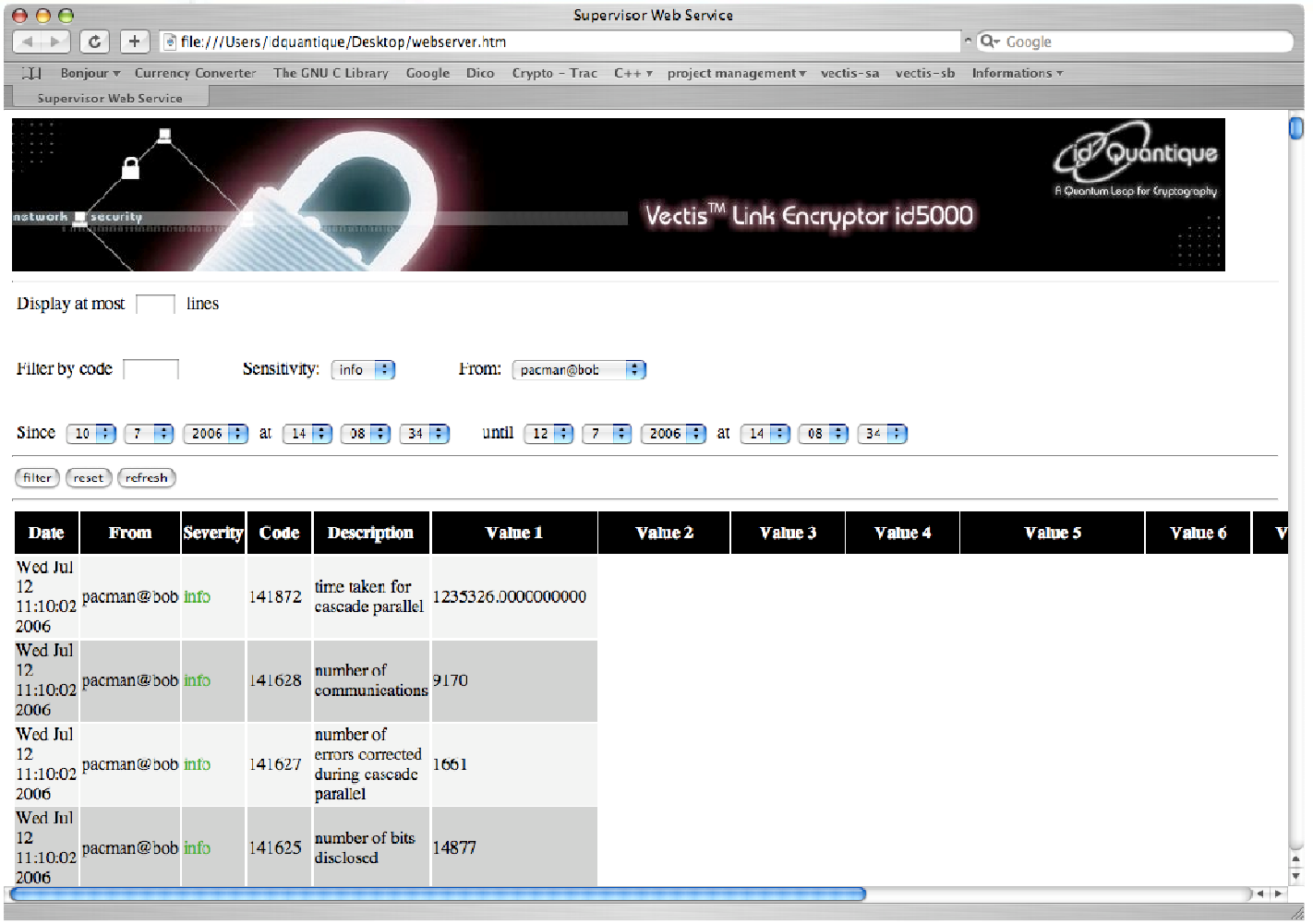
Identity-based authentication

Three authorized roles:

1. **User role**
2. **Crypto officer role**
3. **Maintenance role**



System Administration – Log information



Date	From	Severity	Code	Description	Value 1	Value 2	Value 3	Value 4	Value 5	Value 6	V
Wed Jul 12 11:10:02 2006	pacman@bob	info	141872	time taken for cascade parallel	1235326.0000000000						
Wed Jul 12 11:10:02 2006	pacman@bob	info	141628	number of communications	9170						
Wed Jul 12 11:10:02 2006	pacman@bob	info	141627	number of errors corrected during cascade parallel	1661						
Wed Jul 12 11:10:02 2006	pacman@bob	info	141625	number of bits disclosed	14877						

System Administration – SNMP

SNMPv3 (simple network management protocol)

MIB::System

sysDescr	sysObjectID	sysUpTime	sysContact
sysName	sysLocation	sysServices	

MIB::SNMP

snmpInPkts	snmpOutPkts	snmpInBadVersions	snmpInASNParseErrs
snmpInTooBigs	snmpInNoSuchName	snmpInBadValues	snmpInReadOnlys
snmpInGenErrs	snmpInTotalReqVars	snmpInTotalSetVars	snmpInGetRequests
snmpInGetNexts	snmpInSetRequests	snmpInGetResponses	snmpInTraps
snmpOutTooBigs	snmpOutNoSuchNames	snmpOutBadValues	snmpOutGenErrs
snmpOutGetRequests	snmpOutGetNexts	snmpOutSetRequests	snmpOutGetResponses
snmpOutTraps	snmpEnableAuthenTraps	snmpSilentDrops	snmpProxyDrops

IF-MIB

ifDescr	ifType	ifMtu	ifSpeed
ifPhysAddress	ifAdminStatus	ifAdminStatus	ifOperStatus
ifInOctets	ifInUcastPkts	ifInDiscards	ifInErrors
ifOutOctets	ifOutUcastPkts	ifOutDiscards	ifOutErrors
ifOutQLen			

IDQ-MIB

CryptDiscardedFrames	CryptFramesCongestionDropped	ClearDiscardedFrames	ClearFramesCongestionDropped
AuthErrors	Loss		

Traps

coldStart (0)	warmStart (1)	linkDown (2)	linkUp (3)
authenticationFailure (SNMP) (4)	egpNeigborLoss (5) (will not be used)	entrepriseSpecific (6)	

Vectis traps

System down	System up

System Administration – Procedures

« How do I exchange the initial secret required for authentication ? »

A&B need to share initial short secret; QC is a quantum secret growing protocol.

« What happens if the QBER exceeds the security threshold? »

Use the keys in the buffer until none are left, then

Mode 1: continue using the last key until the problem is fixed

Mode 2: disable the classical channel

Trade-off between security and link availability !

Paranoid

« What happens if power goes down and back up? »

« What happens if the chassis has been opened (e.g. during power outage)? »

Field Testing

Field testing with a Swiss internet provider

Data saved on a farm of 30 servers of the Deckpoint Housing Center are replicated on servers located at the Cern Internet Exchange Point.

Distance: 10 km.

System worked for several weeks without interruption.

Ongoing: test bed at the Center for Information Technology in Geneva.

Distance: 22.8 km, 5.8dB attenuation.

Outline

- Introduction
- Historical perspective on optical platforms and QKD experiments
- Vectis Link Encryptor – state-of-the-art encryption appliance
- Challenges facing the deployment in networks
- Future directions

Challenges facing the deployment in networks

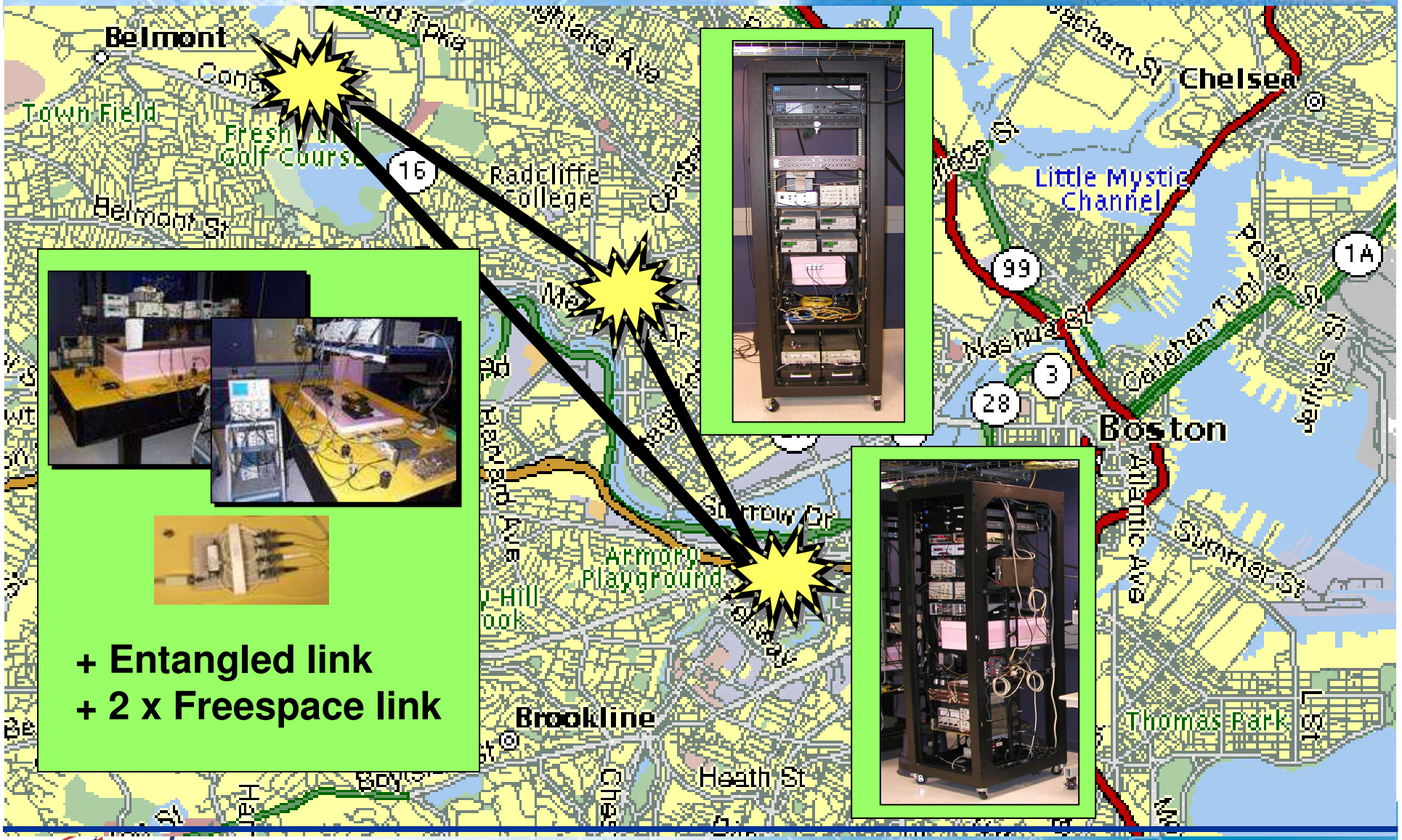
Problematic #1: need dedicated dark fibers

Challenges facing the deployment in networks

Problematic #2: point-to-point link encryption

The DARPA Quantum Network

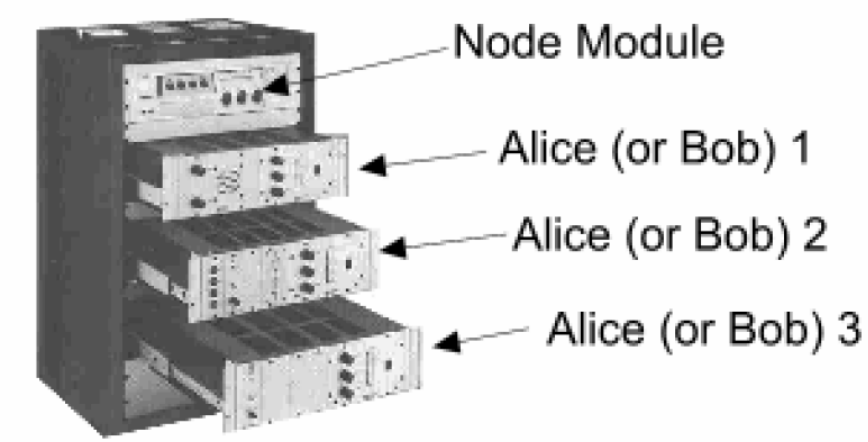
Operating Continuously Across Cambridge Since 6/2004



+ Entangled link
+ 2 x Freespace link

- SECOQC =
  - SEcure COmmunication based on Quantum Cryptography
- European project
- Goal: design and implement a complete QKD network
- From April 2004 to April 2008
- Actors : 41 participants from 12 countries
  - Including 8 private companies (incl. idQ)
- Financing: 11.4 millions euros

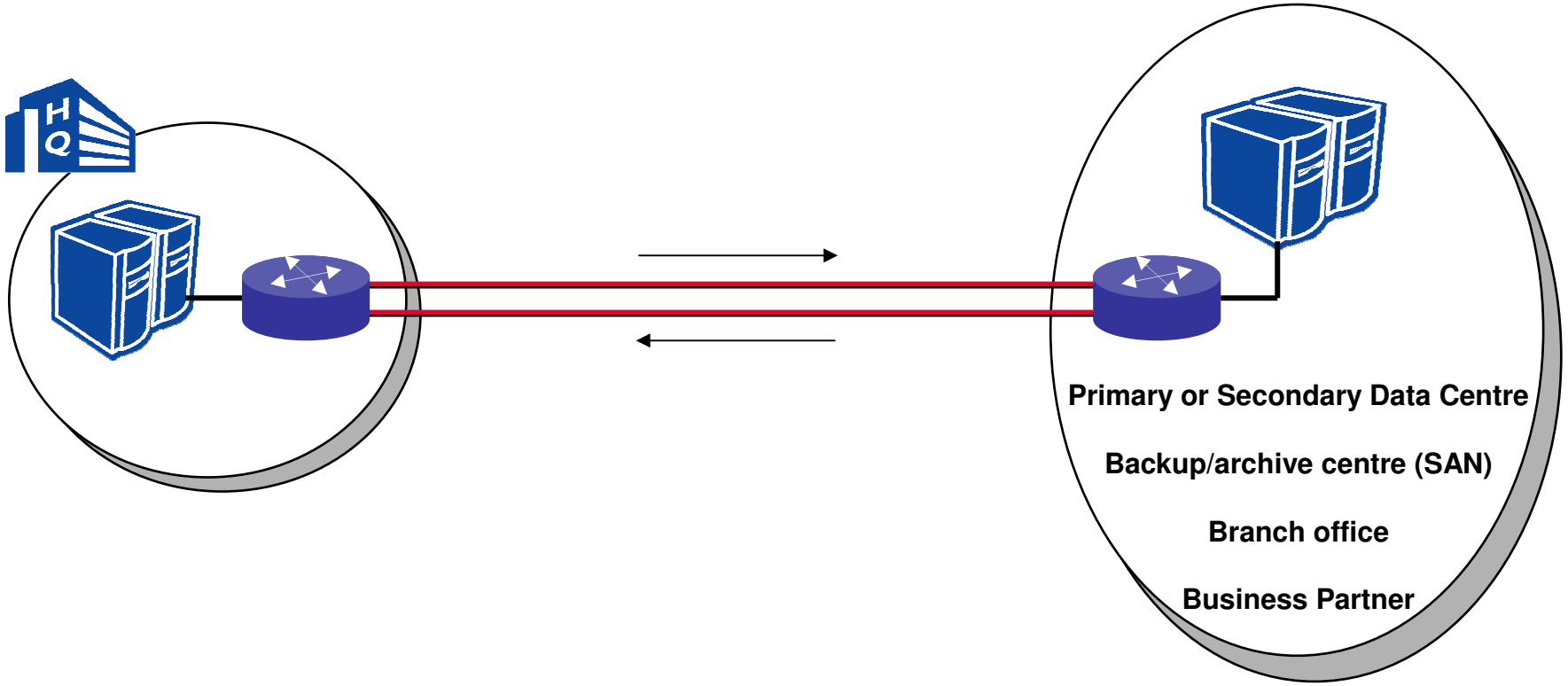
- Node + QKD links



- Network in Vienna

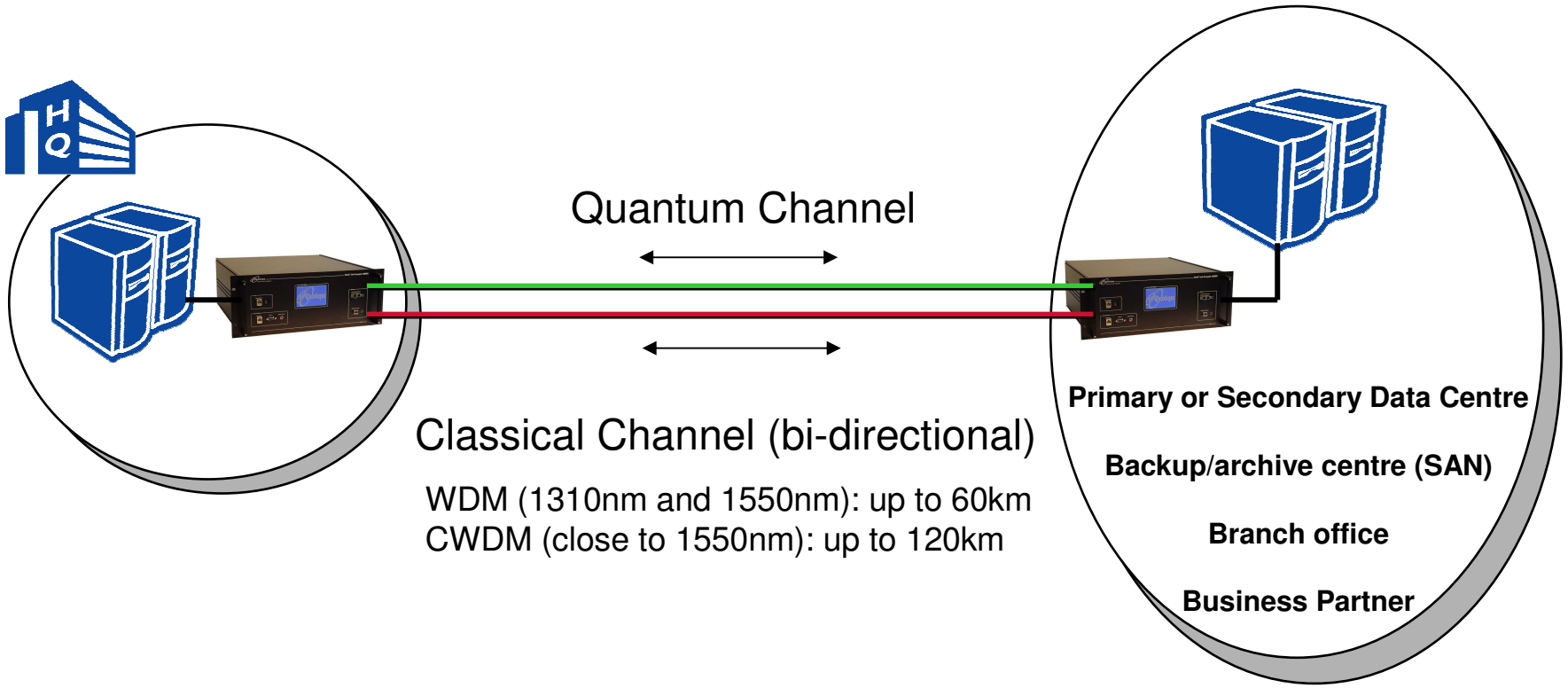
Challenges facing the deployment in networks

Problematic #3: customer has only 2 strands of fiber



Challenges facing the deployment in networks

Solution : **1 strand for quantum channel**
1 strand for classical channel (bidi)

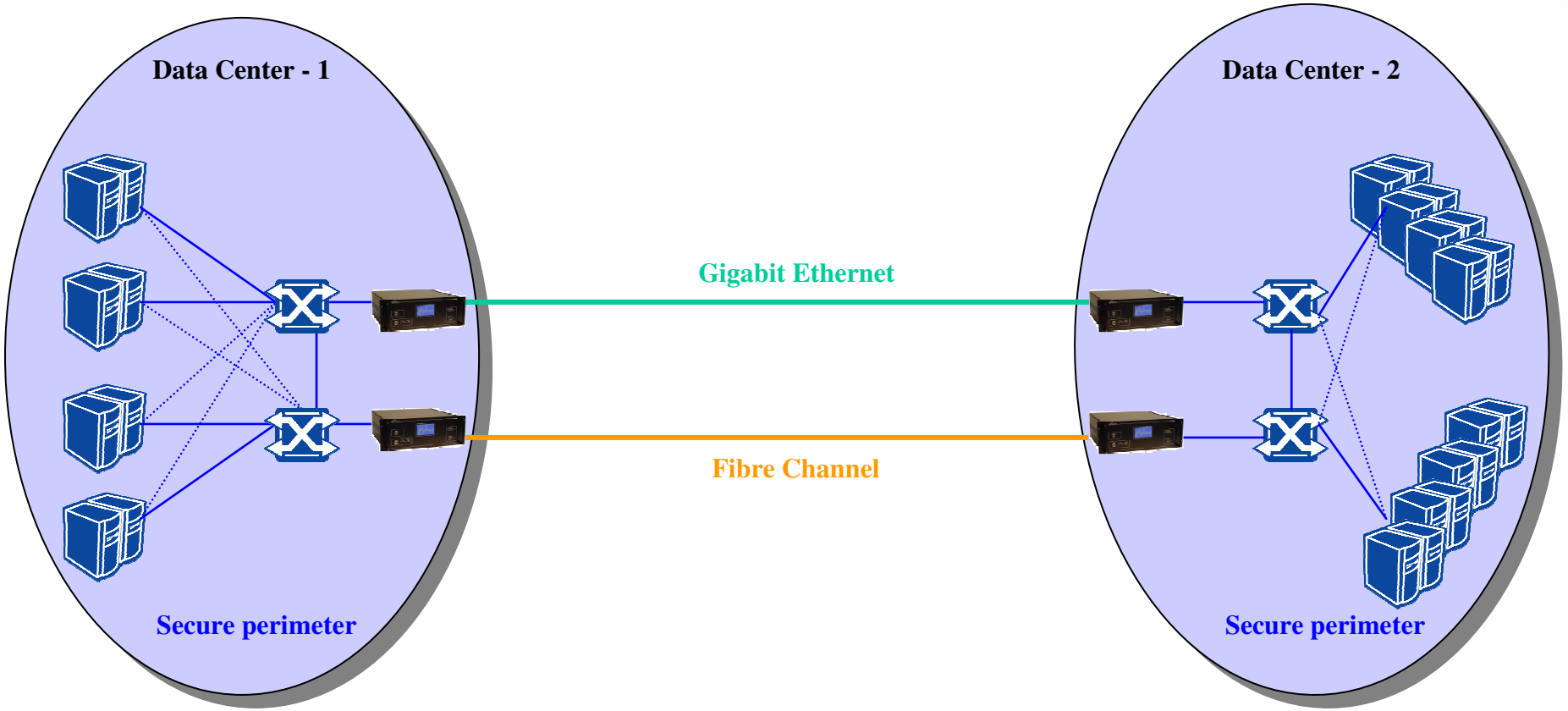


Challenges facing the deployment in networks

Solution : **1 strand for quantum channel**
1 strand for classical channel (bidi)

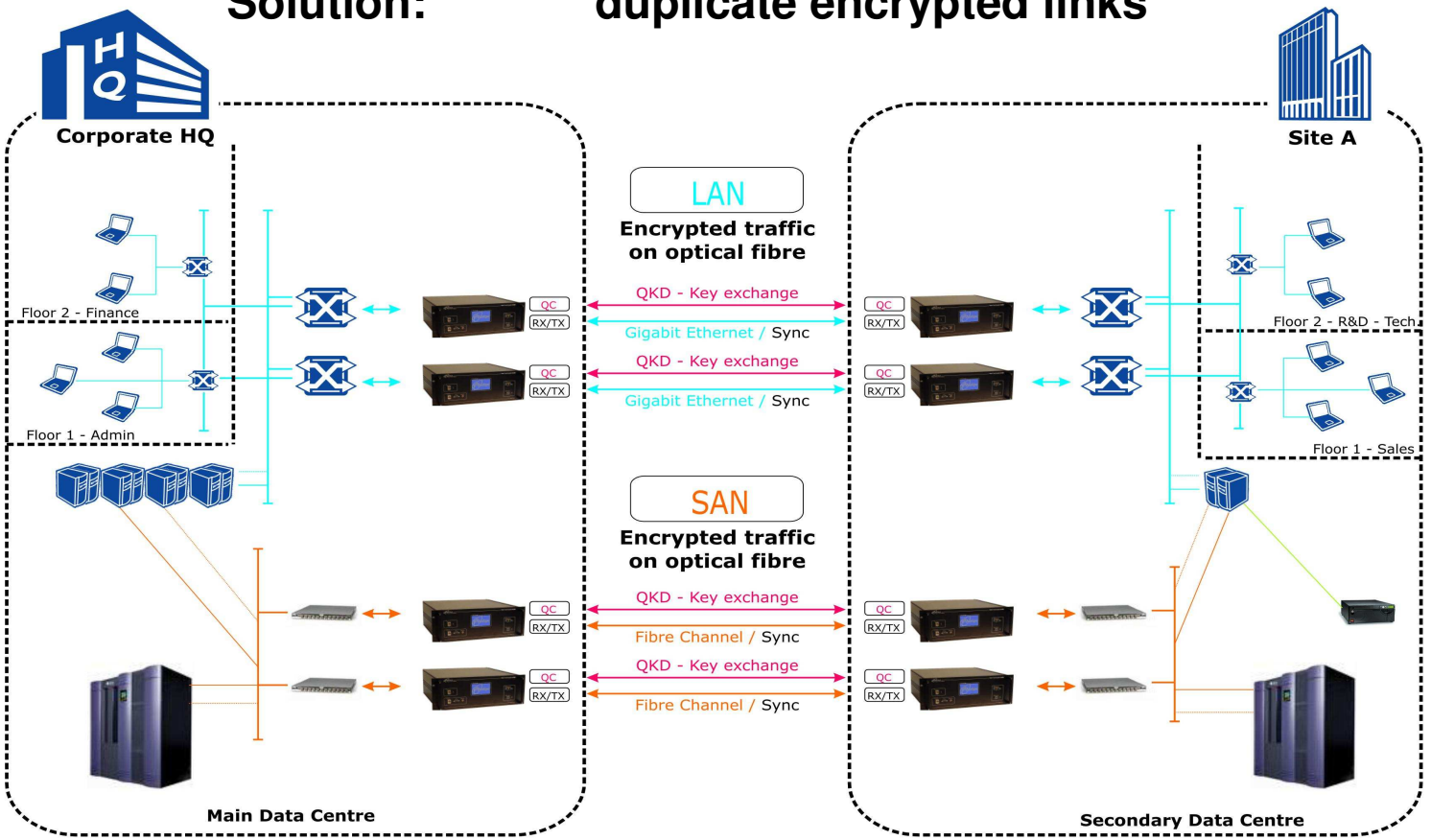
Challenges facing the deployment in networks

Problematic #4: customers use different protocols
Solution: offer encryptors with main protocols



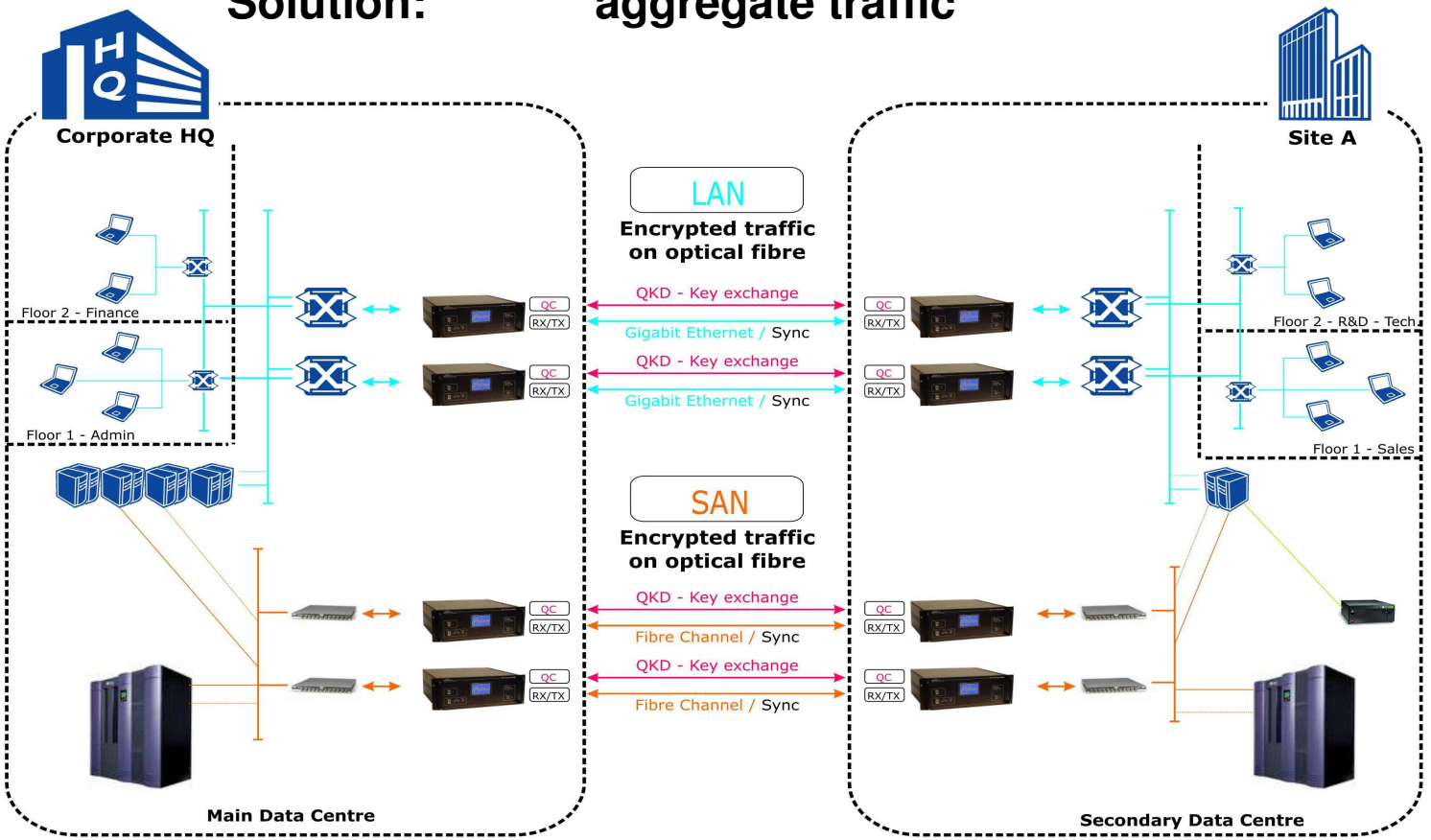
Challenges facing the deployment in networks

Problematic #5: customers need redundancy
Solution: duplicate encrypted links



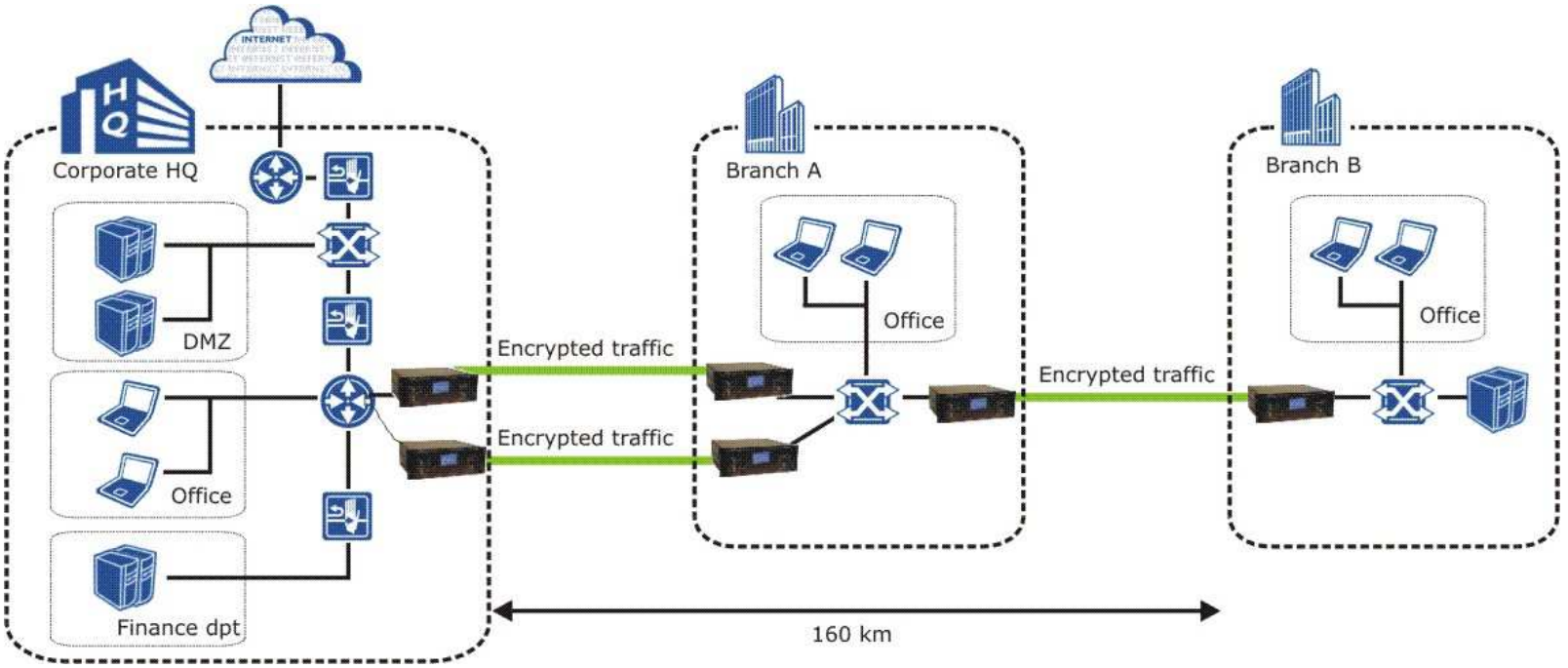
Challenges facing the deployment in networks

Problematic #6: customers need higher throughput
Solution: aggregate traffic

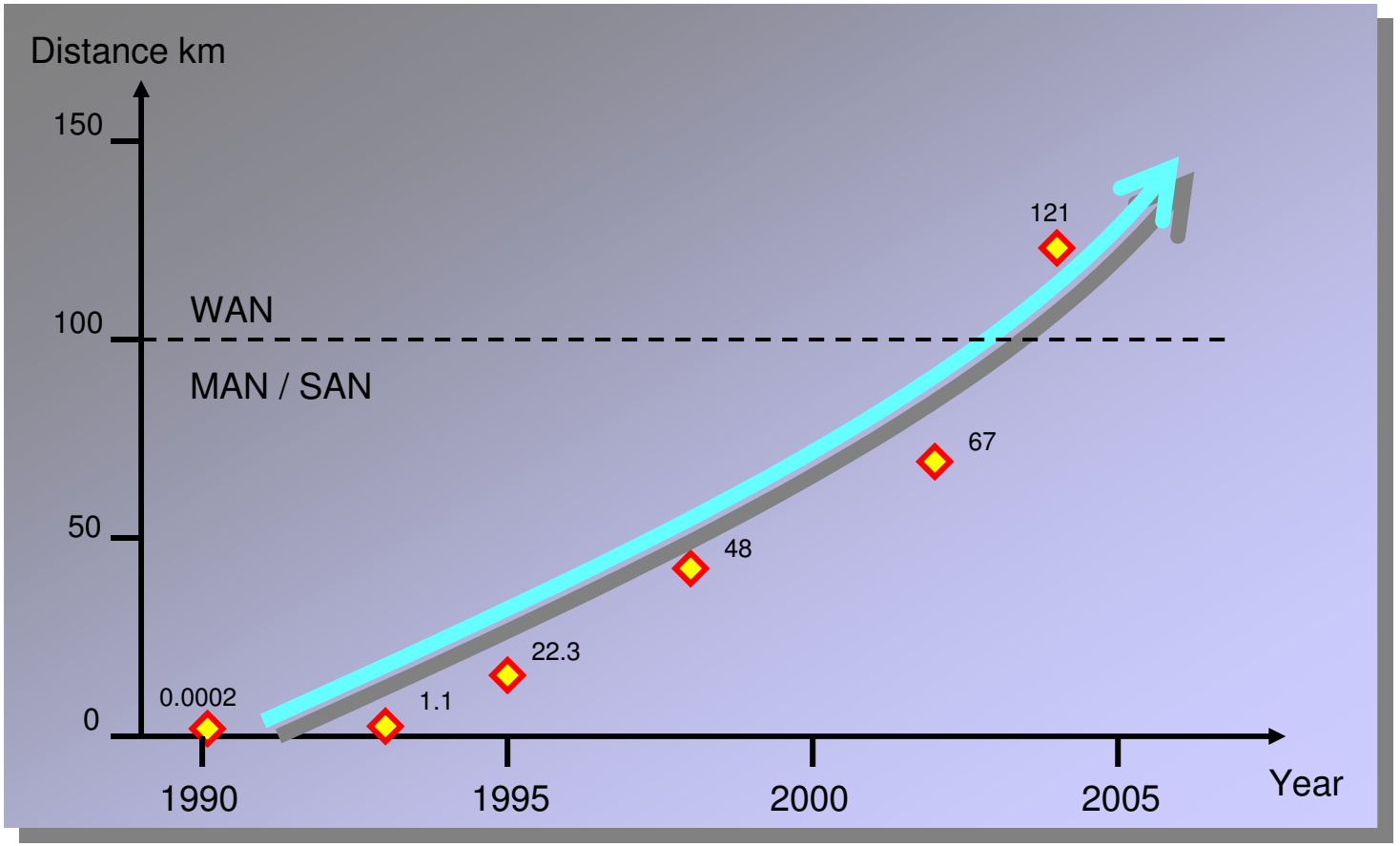


Challenges facing the deployment in networks

Problematic #7: distance larger than 80km
Solution: daisy-chain systems (short-term)



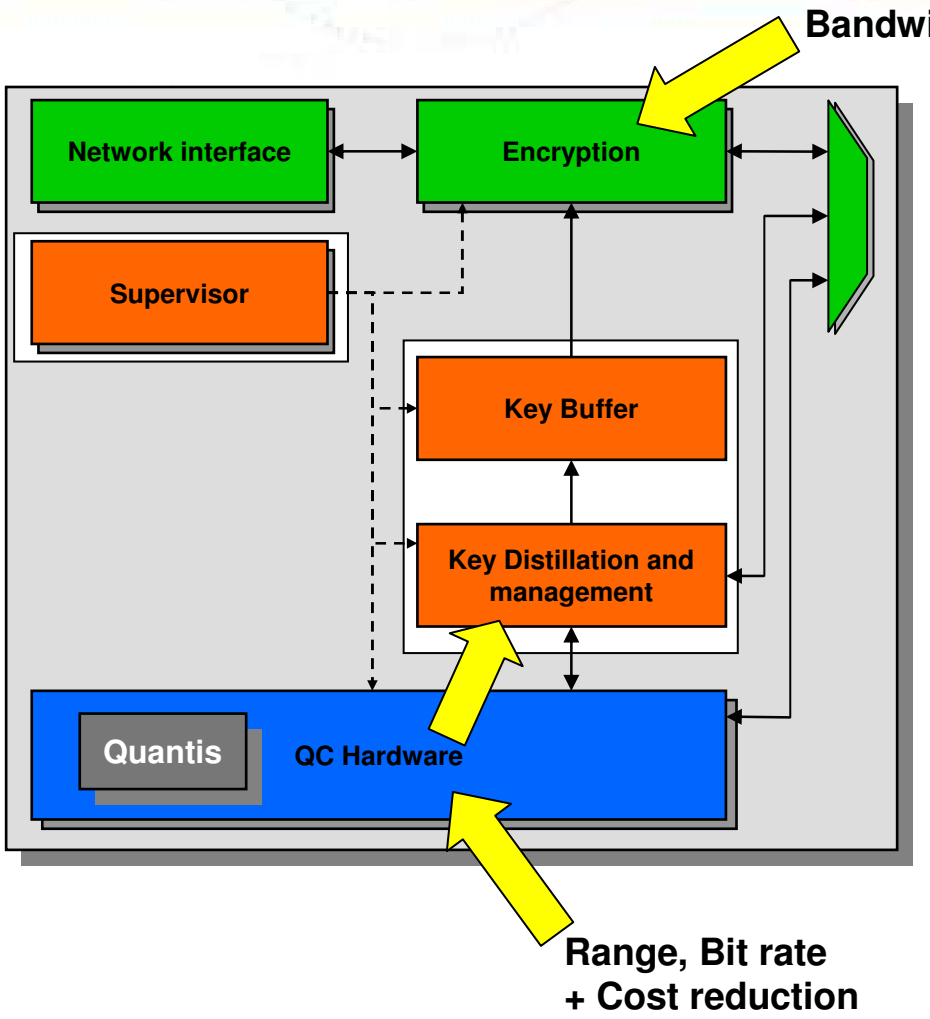
Quantum Cryptography Range



Outline

- Introduction
- Historical perspective on optical platforms and QKD experiments
- Vectis Link Encryptor – state-of-the-art encryption appliance
- Challenges facing the deployment in networks
- Future directions

Future Directions



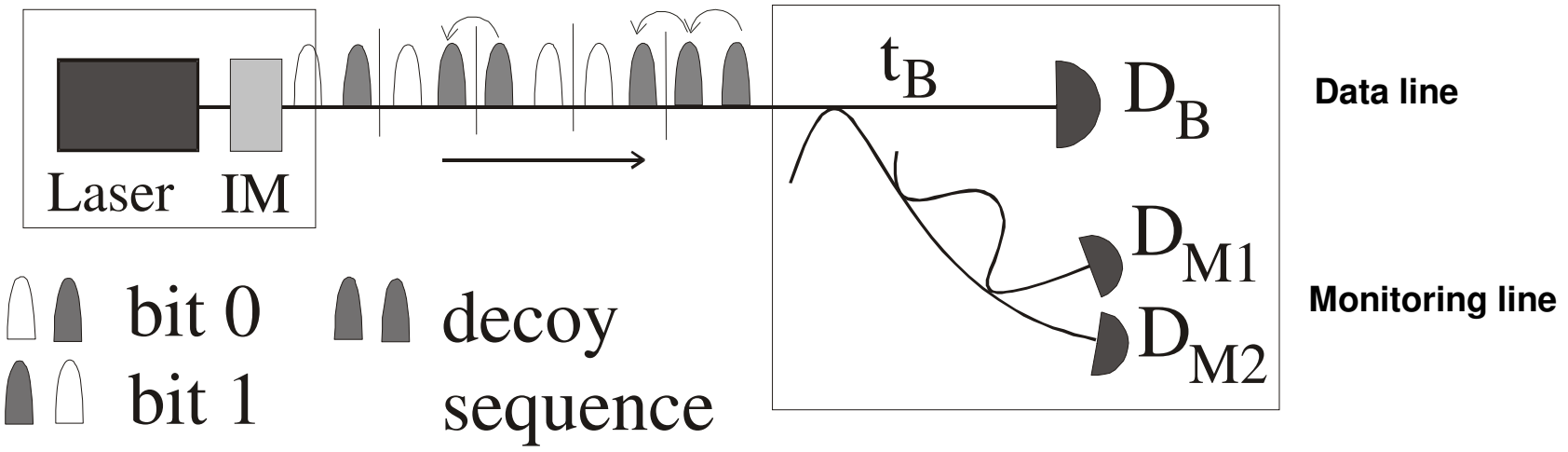
Standardization

Inter-operability

Possibility to compare and evaluate QKD systems

Coherent one-way QKD (COW) (patent pending)

Alice produces a train of equally-spaced coherent pulses.

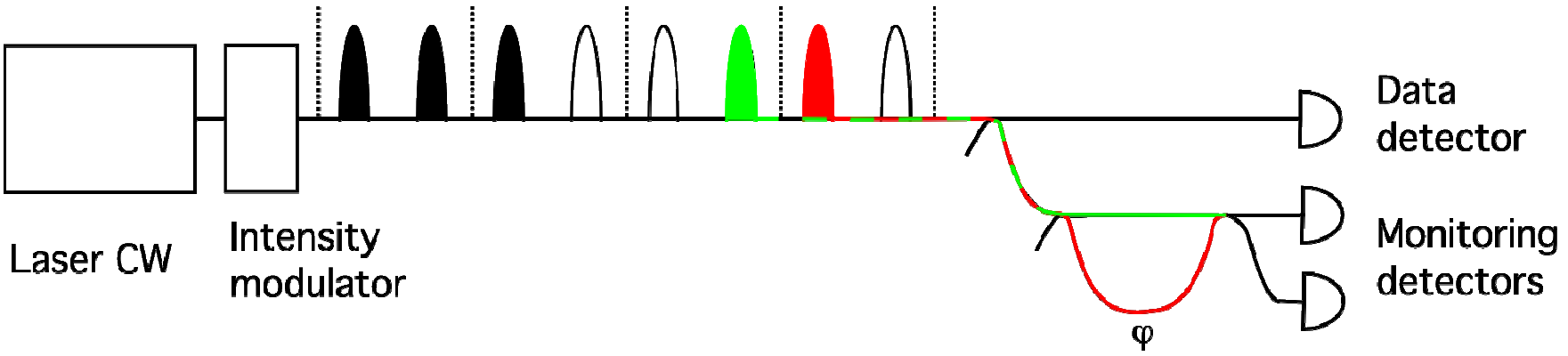


quant-ph/0411022, APL 87, 194105, 2005

- simplicity: measure time of arrival of pulse
  ð insensitive to optical errors
- rapidity: low loss at Bob's side
- security: check occasionally quantum coherence within and across the bit separation
- reliability by using standard telecom components
- no need for single-photon source since resistant to PNS attacks

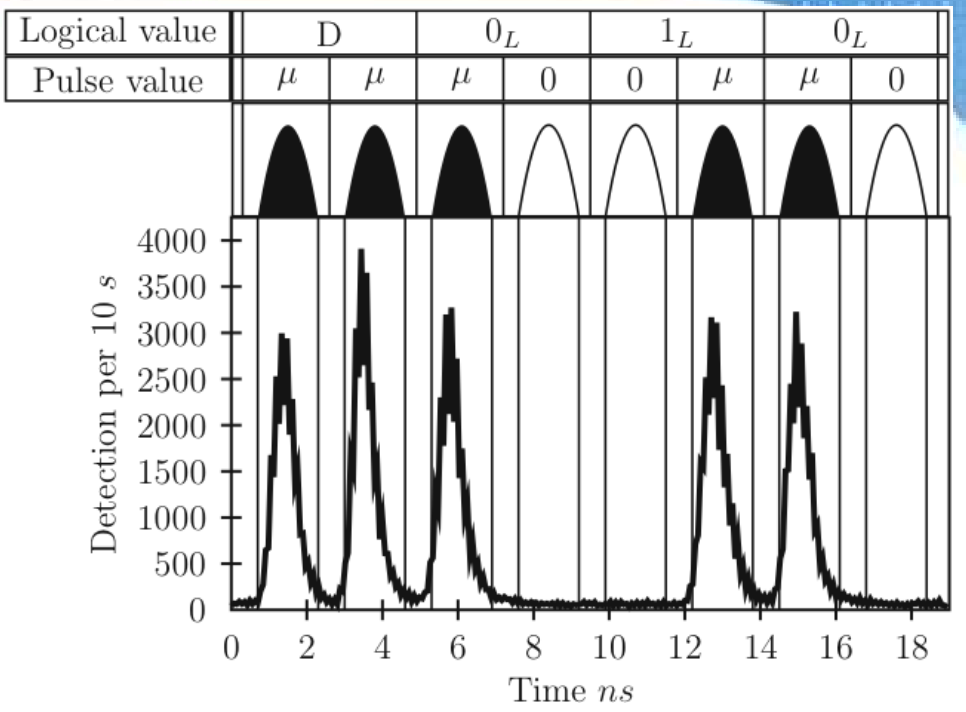
Security of the system

- Security by checking the coherence of successive pulses
  - additional interferometer



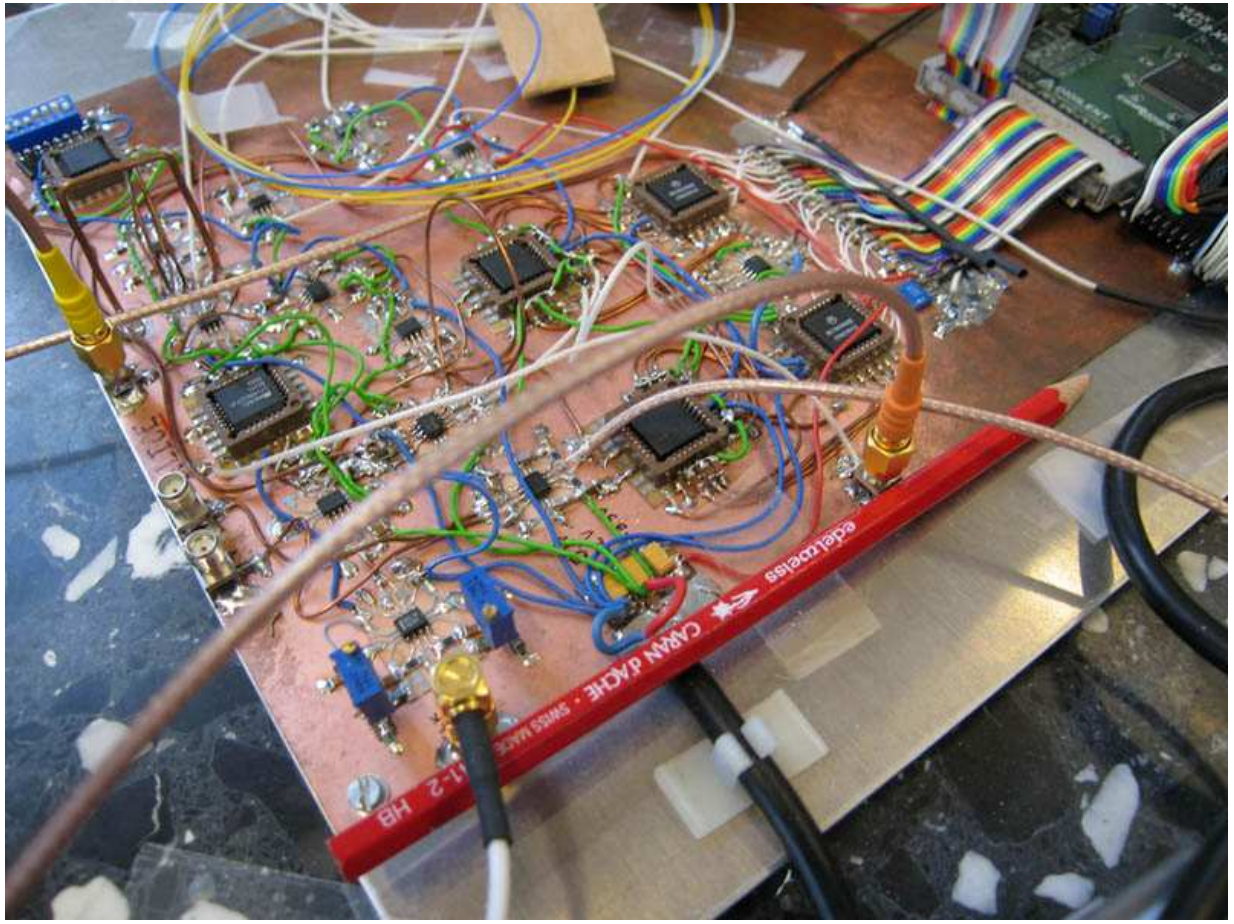
Results – Gisin's group

- Pulse rate 434MHz
- Repetition rate 600kHz
- Raw bit rate 17kHz
- 5dB link losses (25km)
- $QBER_{tot}$=5.2%
- Raw visibility of 92%
- Net visibility of 98%

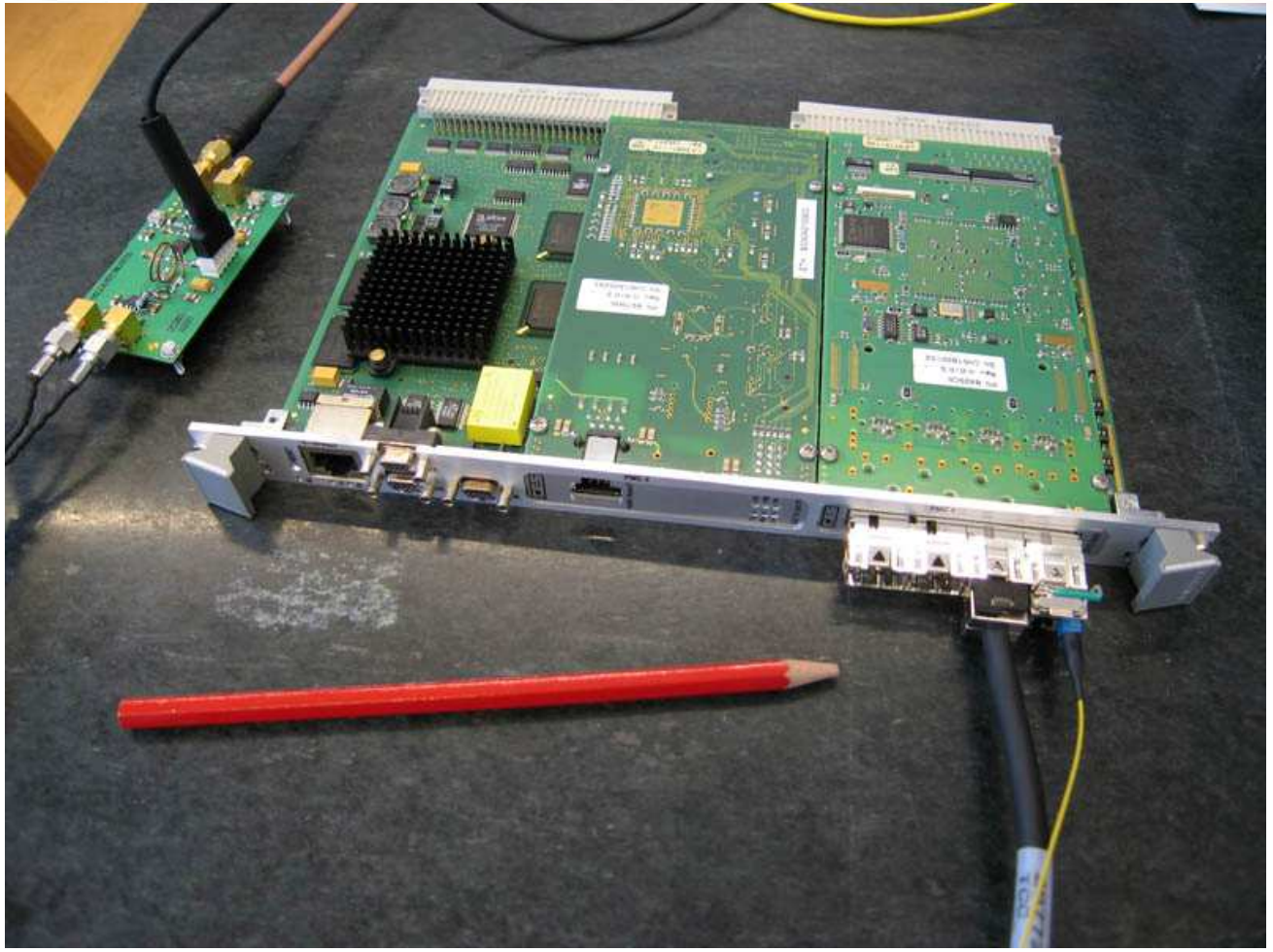


quant-ph/0411022
APL 87, 194105, 2005

Coherent one-way QKD



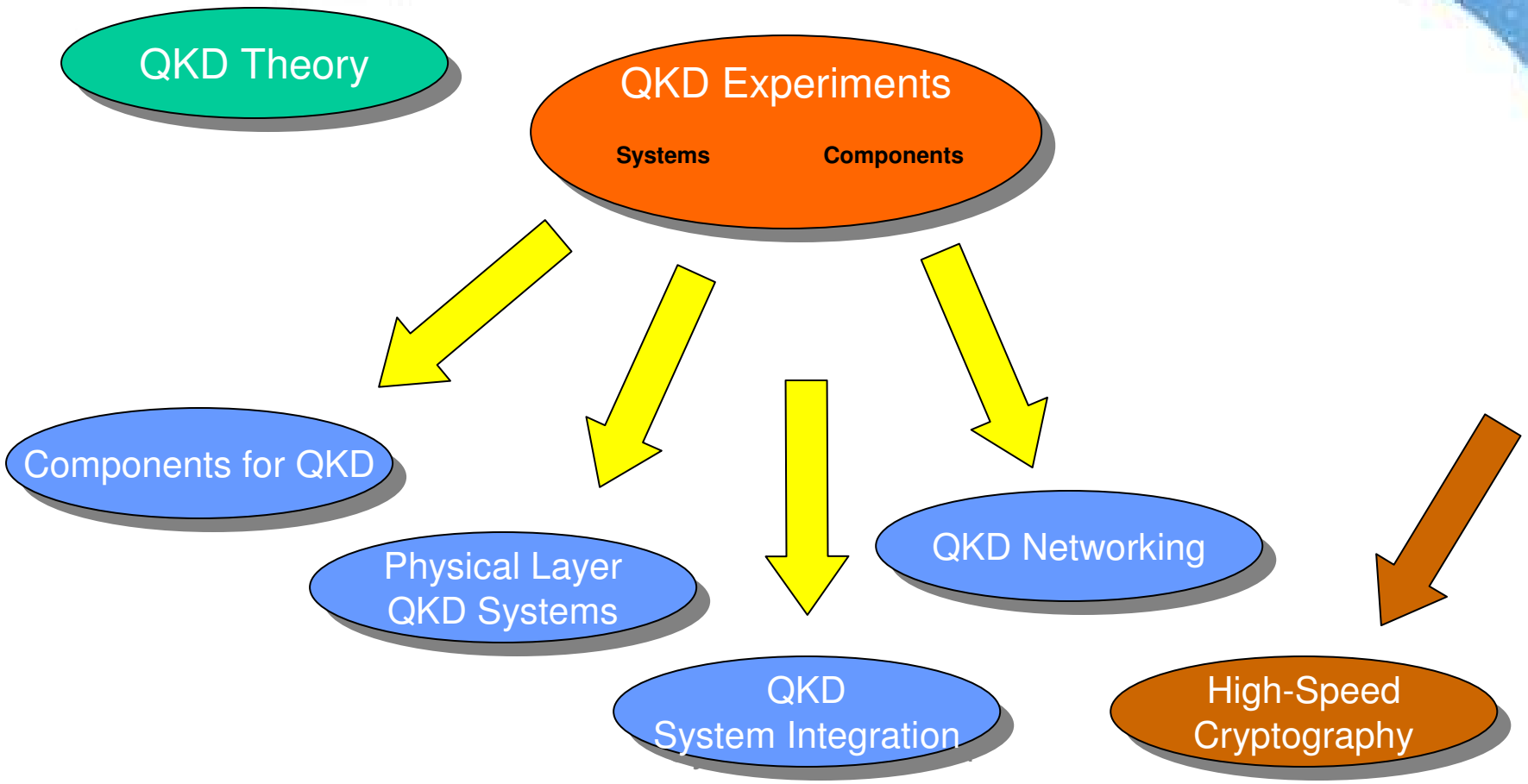
Coherent one-way QKD (part of Secoqc project)



Quantum Cryptography is ready for the market

- Ø Resurgence of layer 2 encryption
  - Strong market growth for high-speed encryption
    - ATM, Sonet/SDH, Ethernet, Fibre Channel
  - Market drivers
    - « Encryption tax » and latency of Layer 3 devices
    - Availability of more bandwidth at a lower cost and in more applications
    - Regulatory intervention forcing security standards
    - More secure posture taken by governments due to war on terrorism
    - Business realizing that security is a business enabler
- Ø Quantum Cryptography can enhance security in high-bit rate applications over MANs and SANs
  - Span of 100km possible
  - High bandwidth means key management is more important
  - Better understanding of security risks associated with public key cryptography by customers

The QKD world is expanding…

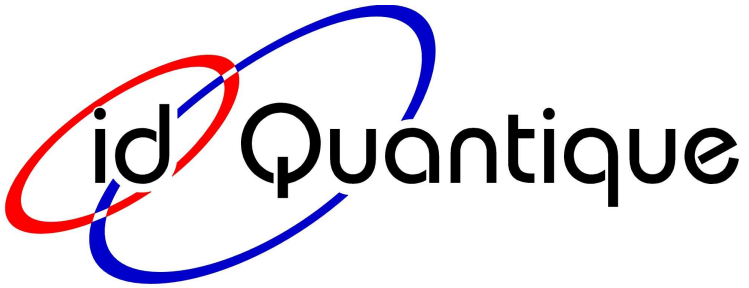


Thank you for your attention

Chemin de la Marbrerie 3
CH-1227 Carouge – Geneva
Switzerland

Info@idquantique.com

www.idquantique.com



A Quantum Leap for Cryptography