Quantum Key Distribution

Norbert Lütkenhaus

The Starting Point …

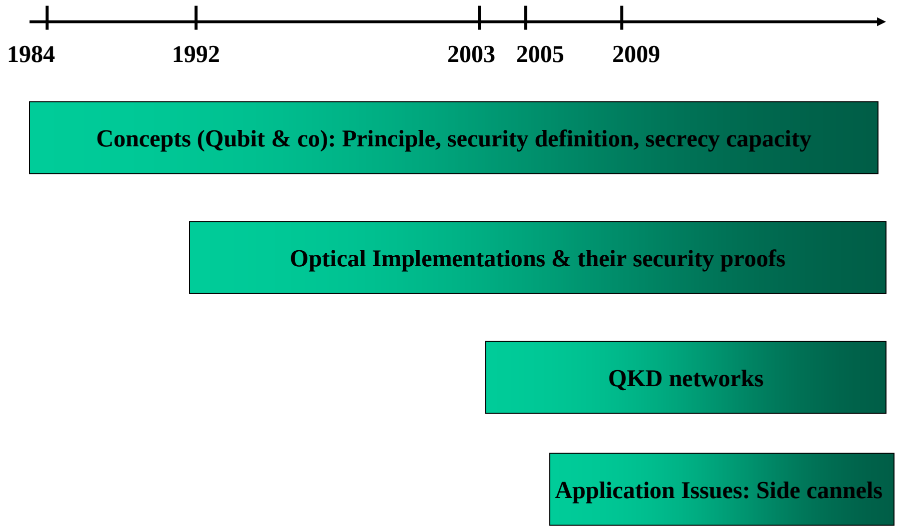
Quantum Mechanics allows
Quantum Key Distribution,
which can create an unlimited amount of secret key using

-a quantum channel
-an authenticated classical channel

without imposing limitations
on an adversary's resources!

Note: no secret key can be generated by
-the use by an authenticated classical channel alone
nor if one additionally provides
-some finite amount of secret seed key
(the latter being one method to generated an authenticated classical channel)

QKD Work lines



Work line I: Concepts

what exactly do we mean by 'secure key'?

Universal composable security definition **[Renner, PhD thesis 2005]**

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

Under which conditions can we generate secret key

1) given many copies of ρ_{AB} ?
   Horodecki[3], Oppenheim (2005): Private states (secret key from bound entangled states)
2) given measurement results from many copies of ρ_{AB}?
   Unknown! (Necessary condition: correlations must show entanglement signature!)

Tools for security proofs:

Quantum DeFinetti Theorem **[Renner, PhD thesis 2005]**

Collective attack = coherent attack

Exploration of new security scenarios:

bounded storage model **[Damgard, Fehr, Salvail, Schaffner, 2005]**

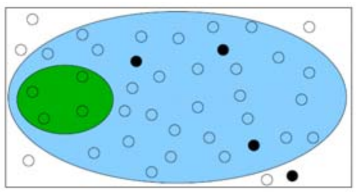
Assume limited quantum storage of adversary

➔ allows also other cryptographic primities such as bit commitment

➔ can be run on BB84 hardware

Quantum DeFinetti Theorem

[Størmer 1969; … Caves, Fuchs, Schack 2002]
[Renner, PhD thesis 2005]
[Renner, Nature, 2007]



general state of N systems

↓ permutation

symmetric state of N systems

↓ subset of n systems

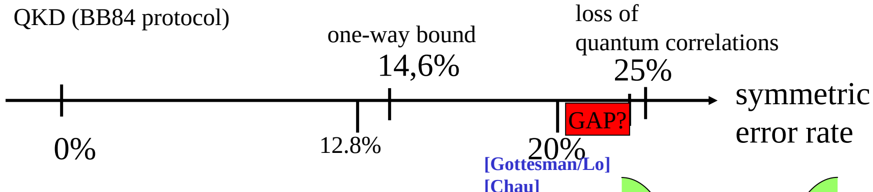
$\rho^{(n)} \rightarrow \sum_i p(i) \; \Pi(\otimes \rho_i + \text{Rest})\Pi$

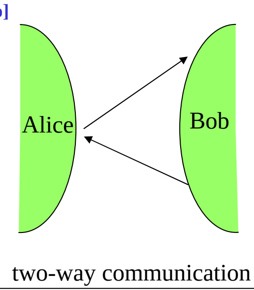
Quantum DeFinetti theorem is at the heart of QM experiments:
how and why can we assign density matrices to sources?

Application also in entanglement verification (e.g. entanglement witnesses)
[van Enk, NL, Kimble, Phys. Rev. A 75, 052318 (2007)]

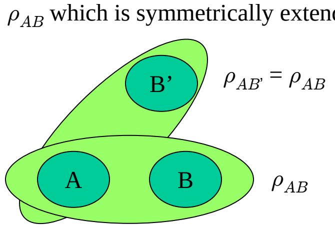
Gap or no gap: are all quantum correlations useful?

QKD (BB84 protocol)





limit for one-way communication:
data should not be explainable
ρ_{AB} which is symmetrically extendible



Existence of
symmetric extension
➔marginal problem
existence of $\rho_{ABB'}$

1) no known first-round communication breaks symmetric extension in gap area
[Myhr, Renes, Doherty, NL, PRA 79, 042329 (2009)]
2) Conjecture of simple criteria for two-qubit case
[Myhr, NL, arXiv:0812.3667]

Workline II: Optical Schemes

Experimental implementations:

weak laser pulses
Photon-pair sources

Security proofs:

finding the qubit in optical modes space!
➔ no single-photon sources required for unconditional security

Improved optical schemes:

decoy state QKD:
Photon-pair schemes with untrusted source
Strong-reference pulse schemes

continuous variable QKD
differential-phase-shift QKD

key rate G scales as
G $\sim \eta$
with transmittivity η
➔ *same as with ideal single photon source*

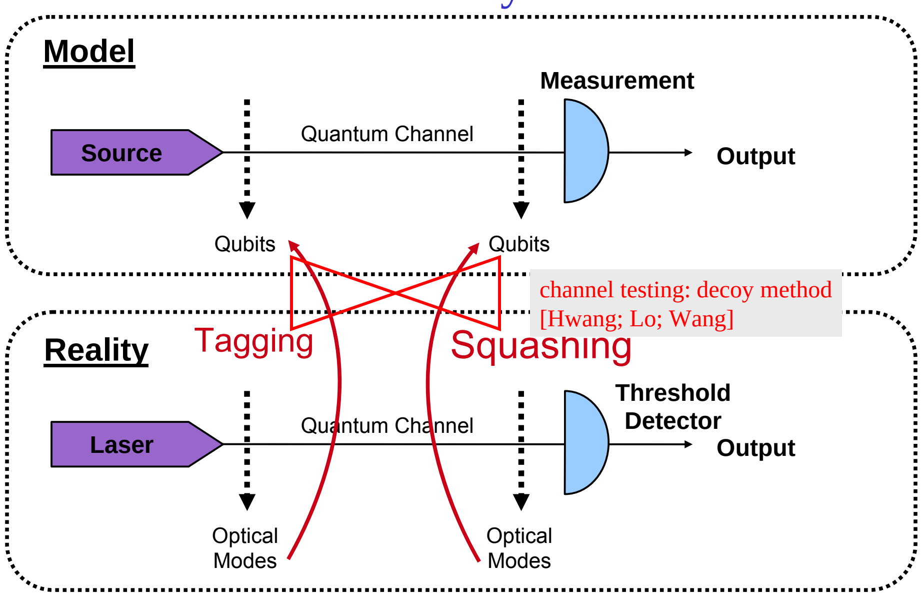
Improved detectors:

detector noise limits distance
detector saturation limits key rate

- up-conversion detectors (Stanford)
- superconducting detectors (NIST)
- self-referencing detectors

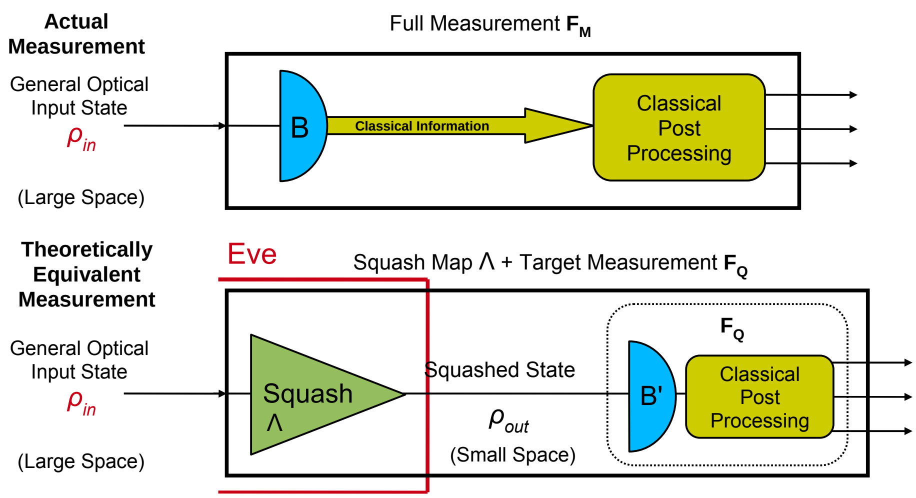
➔ GHZ clock rates, distances more than 100 km

Summary Reduction



Squashing Model

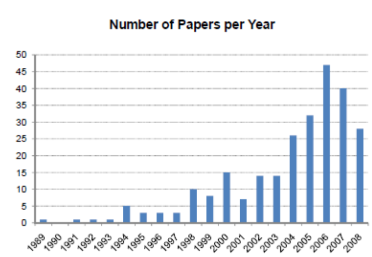
[Beaudry, Moroder, NL, PRL 101, 093601 (2008)]

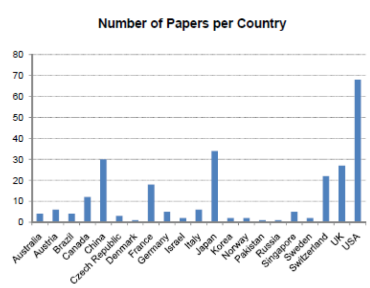


Squashing map exists for BB84 measurements with threshold detectors and random double click assignment!
Squashing has already been anticipated in Gottesman, Lo, NL, Preskill 2004.

See also [Tsurumaru, Tamaki, Phys. Rev. A 78, 032302 (2008)]

Experiments

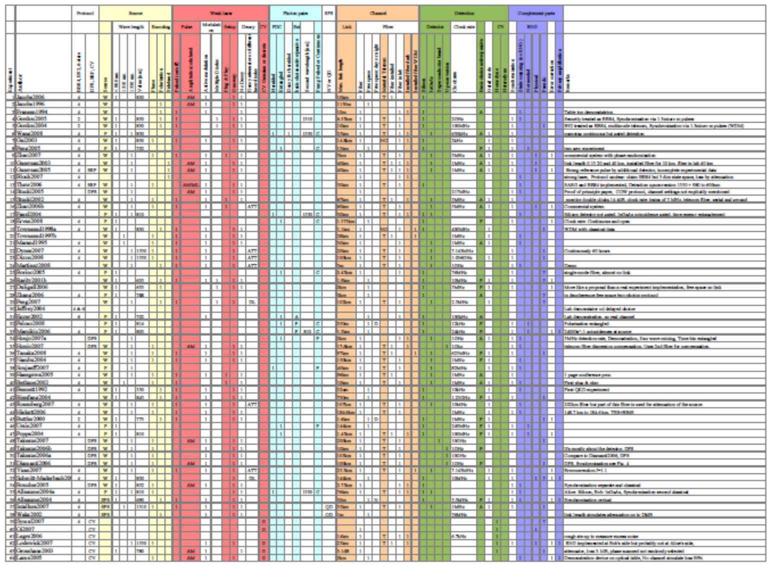




260 full experimental papers on record!

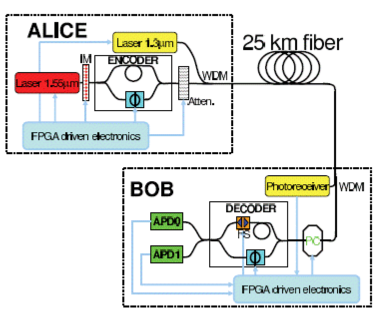
➔list with key words soon available on my webpage

Paper list



Toshiba/NIST/Los Alamos/…

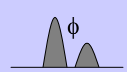
One way weak pulse QKD (phase encoding)



These systems drive detector development!
➔GHz clockrate (NIST)

Security well established:
- weak pulse
- decoy state
- squashing model for detector

1) Keep an eye on amplitudes in phase encoding!

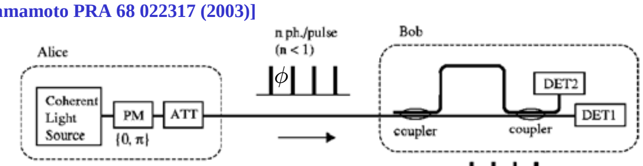


loss in the two arms might be different!

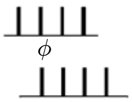
2) fast mode-lock lasers or amplitude modulated continuous signals don't work with the standard security proofs!

Differential Phase Shift QKD

[Inoue, Waks, Yamamoto PRA 68 022317 (2003)]



Elegant set-up adapted to optical networks …



no full security proof so far!

long pulse train looks like ONE high-dimensional signal!

Need to develop new tricks to break the problem down …

Work line III: Application Aspects

Side channel: Optical protocols are unconditional secure

BUT

That does not mean that the optical implementation is secure …
(Same as in classical crypto: side channels, trojan horses …)

Specific attacks:

extra degrees of freedom in signal (residual from signal preparation) (Weinfurter)
Detector Flashback (Kurtsiefer, Weinfurter)
Mismatch of detection windows:
faked state attack (Makarov)
time shift attack (Lo et al)

Countermeasures:

-Theory: estimate damage, include in privacy amplification (GLLP)
-Experiment: better engineering (optical isolators, precise timing)
-Theory: use fundamentals of Quantum Mechanics: Device Independent Security Proofs

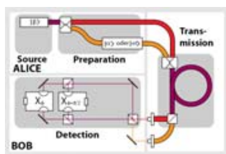
Finite size effects: 100 received signals cannot be turned into secret key
so how many are needed? Guess is 10^6, but it might be 10^{10} … depends on proof technique!

Security and Modelling

Actual Experiment
e.g. reality based

actual devices

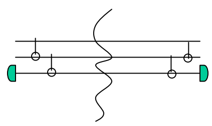
translation into how
we think devices work



Quantum Optical Model
e.g. mode based

e.g. threshold detector model

reduction to essentials
tagging, squashing



Security Model
e.g. qubit based

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

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

Security Proof

Approaches to side channels

security proof
via idealized
model for devices

device independent
security proof

[Acín et al. PRL. 98, 230501 (2007)]

Security of
real QKD
implementation

improve model
to approach implementation
(e.g. efficiency mismatch,
reflections in devices)

include verifiable
assumptions about
devices

security proof
-gives good rate
BUT
- does not really apply

security proof
-applies
BUT
-does not tolerate
sufficient loss

Work line IV: networks

1) Trusted repeater networks
(made up from point-to-point connections)
2) Full quantum networks (➔ Talk Jeff Kimble)

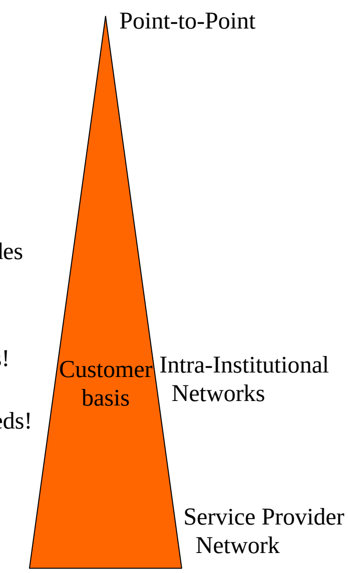
Trusted repeater network:
larger customer base

Interdisciplinary effect:
combination of quantum effects (point-to-point)
and classical crypto protocols (secret sharing)
➔ network stability, stability against some corrupted nodes

Topology of trusted repeater network:
optimum cell size about 20 km (cost optimization)
➔ new optimization direction for point-to-point links!
(not only maximum distance)

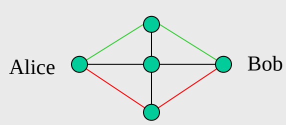
Make precise the leverage QKD has in addressing real needs!
Solve key management problems, initialization etc…

Note:
authentication key (Carter/Wegman) needs to be secure
only for short time!



Network types

Trusted repeater networks: (technologically easy) **[Application: User=Operator]**
Connect trusted repeater stations by point-to-point QKD devices



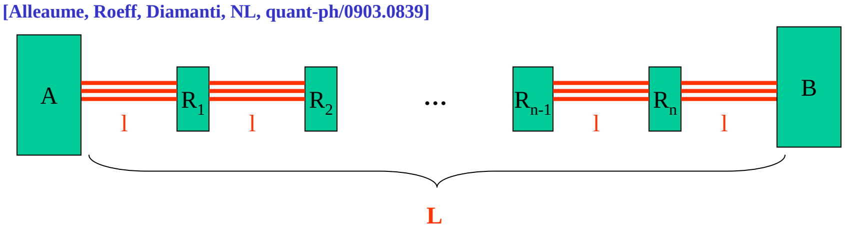
Realisations:
DARPA Network 2002-2005
SECOQC Network 2004-2008

Combine Classical with Quantum Cryptography:
independent pathes allow secure key as long as at least one path is not compromised

Quantum repeater network: (technologically challenging) **[Application: Service Provider]**
Overcomes loss problem
allows routing

Example: Linear Chain

[Alleaume, Roeff, Diamanti, NL, quant-ph/0903.0839]



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

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

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

➔ α = 0.25 dB/km $\rightarrow$ l_{opt}=17.5 km

Summary

QKD is neither purely engineering, nor is it just a theory toy …

by definition, security is a theoretical statement
by definition, only implementation realizes QKD

Ongoing interaction between:

cryptographers
who provide the goal, security definition, tools
quantum theorists
for security proofs and system analysis
system experimentalists
who devise practical schemes
device experimentalists
who build and optimize devices such as detectors

QKD drives and is driven by broader Quantum Information Theory

Quantum Definetti Theorem, Symmetric Extendibility of Quantum States, Channel Capacities …