Quantum Key Distribution: Linking Theory and Experiment

Norbert Lütkenhaus

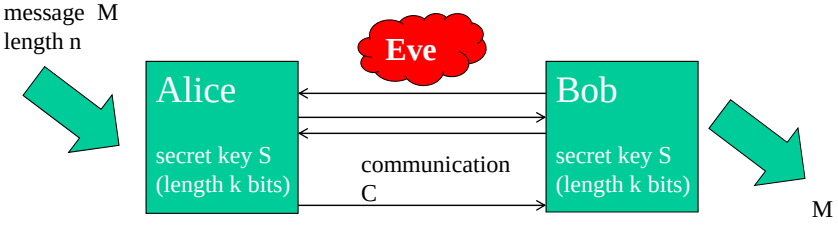
Institute for Quantum Computing
& Department of Physics and Astronomy
University of Waterloo, Canada

Review:
V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev,
A Framework for Practical Quantum Cryptography,
Rev. Mod. Phys. Vol 81, p. 1301 (2009)
quant-ph/0802.4155

Communications Security Establishment

1. Background

Secret Communication



Requirements:

1) **error free decoding** by Bob:
   Bob can recover message M using secret key S and communication C
2) **secrecy:**
   Eve learns nothing about M listening to the communication C

Shannon:
classical communication means that Bob's view and Eve's view of C is identical
➔ key needs to be at least as long as message: $k \geq n$

Quantum Communication: Bob's and Eve's view on communication will differ
➔ initial key can be shorter than message ➔ QKD is possible

Secret key for secret communication

One time pad (Vernam cipher)
Alice and Bob share secret key

Alice: 0 1 0 0 1 0 1 message
XOR 1 1 0 1 0 1 0 key
1 0 0 1 1 1 1 cryptogram (public)
XOR 1 1 0 1 0 1 0 key
Bob: 0 1 0 0 1 0 1 message

Key: - chosen at random
- same length as message
- can be used only once
➔provable secure
➔Key Distribution problem
-Courier (Trust)
-Diffie-Hellman (comp. assumpt.)
-Quantum Key Distribution (QM)

Security idea:

Eavesdropper sees 1 0 0 1 1 1 1 …
could that be the message "Deal finished, see you tomorrow"?
yes! … if the key was "10110101010101000001011101 …"
could that be the message "Deal called off, I am off to Hawaii"
yes! … if the key was "01101011010011010101011 …"

all keys equally likely
➔no hint about message content from cryptogram

Waterloo IQC Institute for Quantum Computing

How to establish a secret key: Diffie-Hellman

Use a mathematical problem that's easy to compute but hard to undo:

- Exponentiation to basis *g* modulo *p* (prime number)

- g, p: publicly known

- Pick a random number x
- Compute g^x

- Pick a random number y
- Compute g^y

g^x →

Compute $(g^x)^y = g^{xy}$

Compute $(g^y)^x = g^{xy}$

← g^y

Both parties know g^{xy}

This is secure if it's hard to compute g^{xy} knowing only g^x and g^y.

Waterloo IQC Institute for Quantum Computing

Secret key for secret communication

Security of
- Public key cryptography,
- Symmetric encryption (AES)

is based on **computational assumptions**,
e.g. 'inverting exponentiation modulo p is hard'
'factoring large numbers is hard'

➔Concerns:

How fast do computational resources grow?
- Precedence: PC clusters connected by internet

Are there other ways to break codes?
- New algorithms for classical computers
- Emergence of quantum computers

=> can factor large numbers efficiently (in principle)

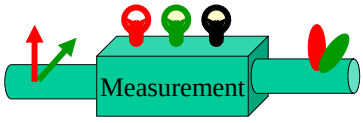
Desirable: Provable security!

Waterloo IQC Institute for Quantum Computing

2. QKD: Basic Ideas and Basic Protocol

Waterloo IQC Institute for Quantum Computing

Quantum mechanics protects information



Non-trivial measurement on non-orthogonal signal states

➔states disturbed ➔errors

No errors for non-orthogonal states ➔Only trivial operation by Eve ➔ no leakage of information

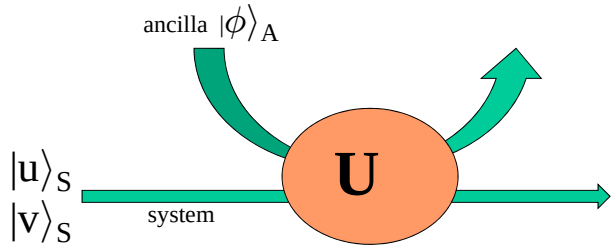
Other formulations:

•No-cloning theorem for non-orthogonal states

•Heisenberg Uncertainty Principle

Unlike classical data, quantum data show a signature of attempts to copy or to measure them.

Eve's interaction



Any channel that transmits two non-orthogonal states perfectly does not leak any information about the signals to a third party!

$$|u\rangle_S |\phi\rangle_A \xrightarrow{U} |\Psi^{(u)}\rangle_{SA} \overset{!}{=} |u\rangle_S |\phi^{(u)}\rangle_A$$

$$|v\rangle_S |\phi\rangle_A \xrightarrow{U} |\Psi^{(v)}\rangle_{SA} \overset{!}{=} |v\rangle_S |\phi^{(v)}\rangle_A$$

(ideal transmission)

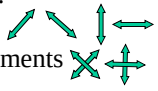
overlap: (unitary!)

$$\langle u|v\rangle \langle \phi|\phi\rangle \overset{!}{=} \langle u|v\rangle \langle \phi^{(u)}|\phi^{(v)}\rangle$$

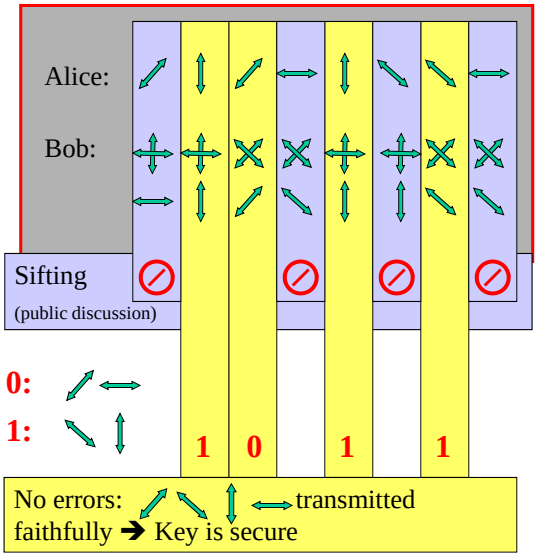
$$\rightarrow \langle \phi^{(u)}|\phi^{(v)}\rangle \overset{!}{=} 1$$

Bennett Brassard Protocol (1984)

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



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



BB84 Protocol: Rough idea

I. Quantum Phase:

(no assumption on quantum channel)

1. Alice: Random sequence of signal states
2. Bob: measurement in sequence of random basis choices

➔ Alice and Bob now both have (correlated) classical data!

II. Classical Phase:

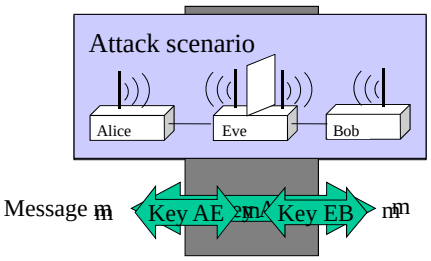
(Eve can listen to message, but cannot change them)

3. Alice and Bob each announce the *bases* of their preparation/measurement
4. Alice and Bob open up some of their signals as statistical test for eavesdropping
5. Alice and Bob exchange confirmation about the absence of eavesdroppers

3. Tools for practical QKD

Public Channel

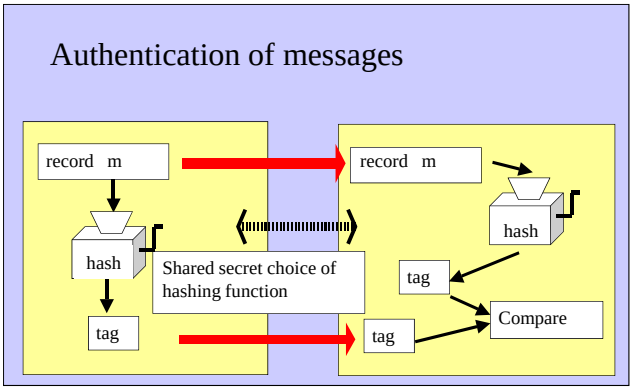
Public channel should be faithful:
•Eve can listen to signal
•Eve cannot change signals

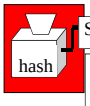


Public channel cannot be protected by physical implementation!
➔need initial secret key for information theoretical secure authentication (Carter/Wegman message authentication)

Change of mission: Grow more secret key from initial seed!

Authentication





Set of universal hash functions

Example: parity bits of random sub-strings

Man in the middle: $(m,t) \rightarrow (m',t')$
Security statement $\Pr(f(m')=t') < 2^{1-s}$
if $\log_2|F| \approx 4s \log_2 \underbrace{\log_2|M|}_{\text{length of record}}$

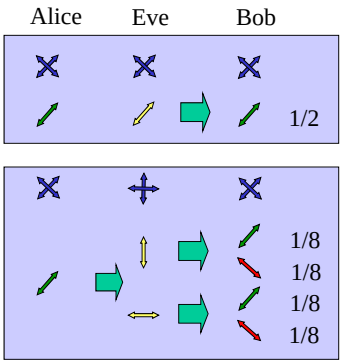
Amount of secret binary key: Need $\log_2|F|$ bits

➔**Quantum Key Growing**

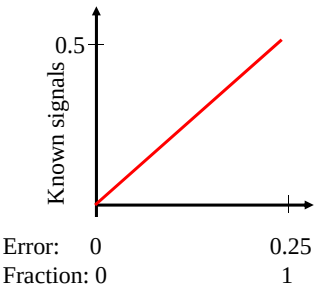
About errors …

1) There are always errors in real implementations, so
Alice and Bob need to perform error correction!

2) Eve should have negligible information on the key:



Sifted key: Right: 3/4
Wrong: 1/4



We need to cut Eve's correlation with the key: **privacy amplification!**
➔ **established classical procedure!**

Principle of Privacy Amplification

Principle:
Assume Eve guesses each bit correctly with probability $p = \frac{1}{2}(1+\varepsilon)$

➔She guesses a parity bit of n bits correctly only with probability

$$p^{(n)} = \tfrac{1}{2}\left(1+\varepsilon^n\right)$$

$$\underbrace{0\ 1\ 1}_{0}\ \underbrace{0\ 1\ 0}_{1}\ \underbrace{0\ 1\ 0}_{1} \qquad p = \tfrac{1}{2}(1+\varepsilon)$$
$$p^{(n)} = \tfrac{1}{2}\left(1+\varepsilon^n\right)$$

Thanks, Steve!

Waterloo IQC Institute for Quantum Computing

Entropy & Privacy Amplification (Scanned Page 1)

Waterloo IQC Institute for Quantum Computing

Error Correction (Scanned Page 2)

Eve's knowledge on the key:
Quantum Generalization
(Scanned Page 3)

Holevo Quantity
(Scanned Page 4)

General Key Formula

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

1) valid for protocol basing key on Alice's measurement results (direct reconciliation)
2) assumes (so far) knowledge of Eve's conditional states

[Renner, PhD Thesis 2005]

Security Definition

Definition 6.1.2. Let KD be a key distillation protocol and let $\rho_{ABE} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$. We say that KD is *$\varepsilon$-secure on ρ_{ABE}* if $\rho_{S_A S_B E'} := \mathcal{E}^{\mathsf{KD}}_{S_A S_B E' \leftarrow ABE}(\rho_{ABE})$ satisfies

Norm: success probability

$$\frac{1}{2} \left\| \rho_{S_A S_B E'} - \rho_{UU} \otimes \rho_{E'} \right\|_1 \leq \varepsilon \ ,$$

where $\rho_{UU} := \sum_{s \in \mathcal{S}} \frac{1}{|\mathcal{S}|} |s\rangle\langle s| \otimes |s\rangle\langle s|$, for some family $\{|s\rangle\}_{s \in \mathcal{S}}$ of orthonormal vectors representing the values of the key space $\mathcal{S}$.

Moreover, we say that KD is *ε-fully secure* if it is ε-secure on all density operators $\rho_{ABE} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$.

Key requirements:
- correct (shared by Alice and Bob)
- uniformly distributed
- secret

Security statement:
the probability that
- key protocol does not abort

AND
- the key is not ideal (requirements!)

is smaller than ϵ

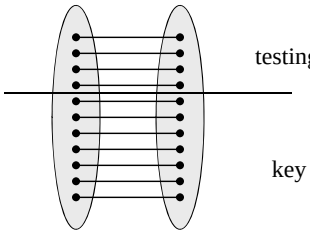
1) ϵ cannot be zero for QKD!
2) Definition does not condition on non-abortion of protocol
   ➔ always aborting protocols are secure by this definition (but useless)!
3) Clear interpretation of imperfection (insurance mathematics!)

General Key Formula

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

Minimization over all ways Eve can be correlated with Alice's signal:

1. Observation p(a,b)
   ➔ constraint: $\rho_{AB} \in \Gamma_{AB}$
   purification of ρ_{AB} ➔ $|\Psi\rangle_{ABE} \in \Gamma_{ABE}$
2. Calculate G for given $|\Psi\rangle_{ABE}$, then minimize G over Γ_{ABE}



testing ➔ determine set Γ_{AB}

key generation (e.g. measurement in Z-basis)

Gain formula

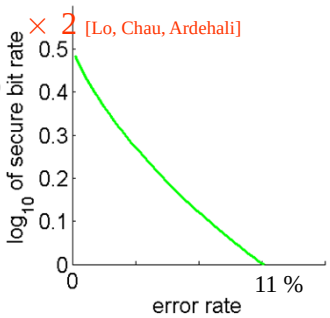
[Mayers; Shor, Preskill;Renner]

The gain formula gives the number of secure bits after error correction and privacy amplification per signal sent by Alice:

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

privacy amplification or one-time pad encryption (Eve's additional information gained during **error correction**)

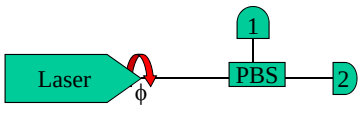
privacy amplification (Eve's information gain due to eavesdropping)



Implementation

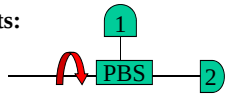
Polarization, Measurement, and Photons

Optical Signals:

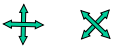


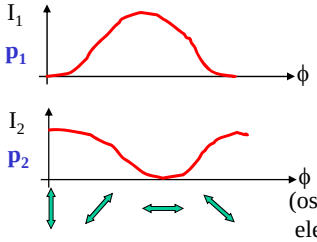
Polarizing beam splitter

Measurements:



Orientation of crystal (PBS):





(oscillating electric field)

Strong light pulse: intensity I

weak pulse: probability p of 'click'
➔ photon as indivisible light quantum!

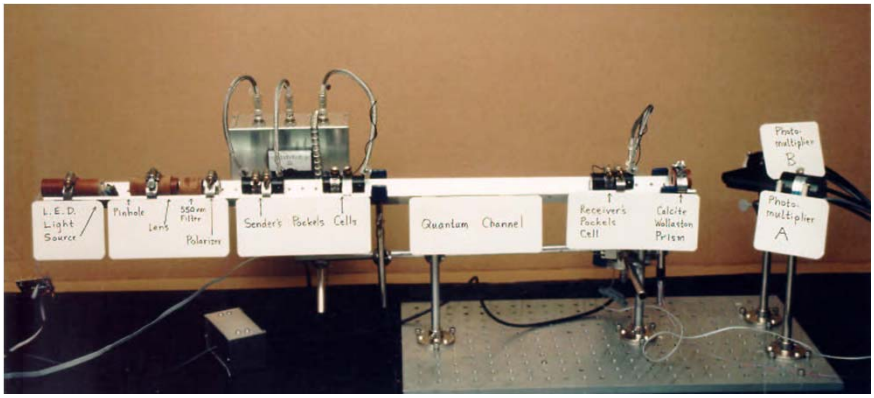
Each photon will leave the PBS in one of the two arms:

measurements: { ↕ ↔ ↗ ↖ } ➔ possible results: { ↕ or ↔ ; ↗ or ↖ }

signal	*measurement*	*result*
Deterministic: ↔	↕	↔
Probabilistic ↗	↕	1/2 ↕ ; 1/2 ↔

Waterloo IQC Institute for Quantum Computing

The first experiment …



IBM Group, 1984/1992

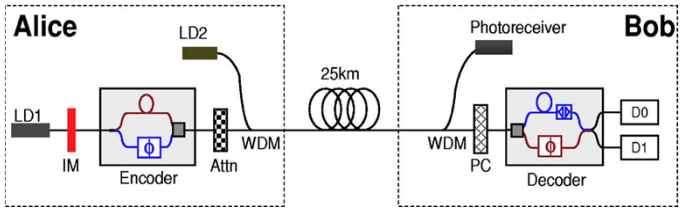
Waterloo IQC Institute for Quantum Computing

Optical Implementations

Sources:
Single Photons not necessary!
- weak laser pulses
- down-conversion sources
- …

Channels:
use
- fiber optics
- free space

Detection devices
use
- single photon counters
- homodyne detection



© Yuan, Sharpe, Shields Appl. Phys. Lett **90**, 011118 (2007)

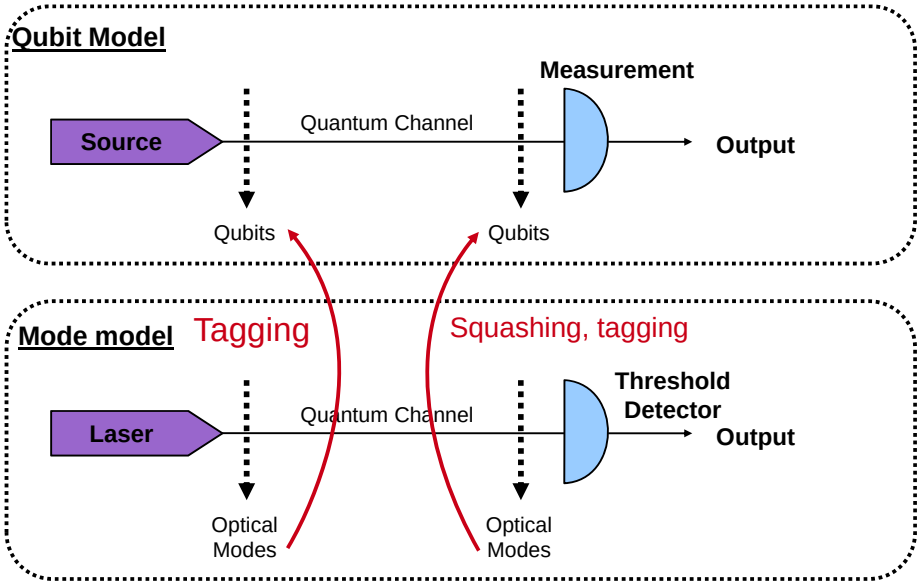
Performance limitations:
loss ➔ key rate scales at most ~ t (transmittivity)
detector saturation ➔ limits key rate per time

detection dark counts ➔ limits maximum distance

Note:
cut-off distance pure technology based
➔ can expect substantial progress

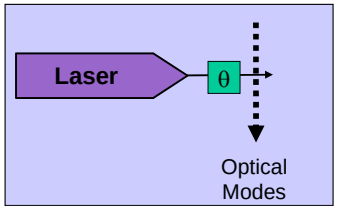
Security: can get performance as with single-photon source!

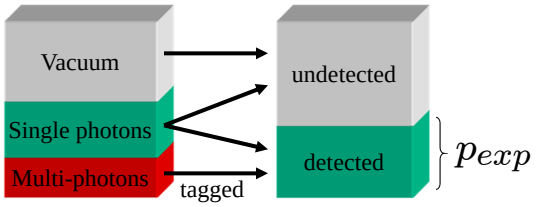
Connecting Qubits & Modes



Output of Lasers
(Scanned page 5)

Photon number splitting attack





In the BB84 protocol, multi-photon signals give their complete information to Eve!
➔ treat these signals as 'tagged', no need for quantum description

Key rate:

$$G \sim p_{exp} - p_{tag}$$

Tagging and Security

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

tagged

final key

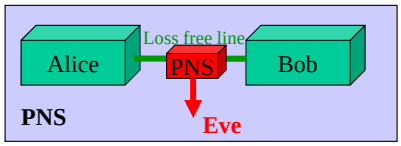
privacy amplification matrix

corrected key

secret

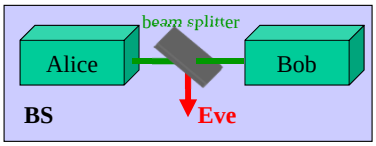
known

Testing Channels: decoy method



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

$\mu_{opt} \approx \eta \quad G \approx \eta^2$



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

$\mu_{opt} \approx 1 \quad G \approx \eta$

Decoy state idea:[Hwang; Lo; Wang]

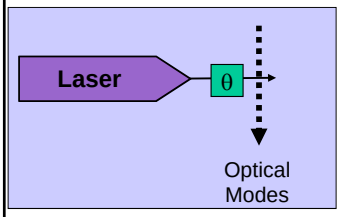
several input intensities μ_i

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

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

Source reduction: tagging



phase randomized laser pulse:
$\sum_n p(n) |n\rangle \langle n|$
+ signal encoding (polarization or phase encoding)

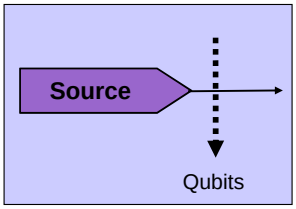
Tagging: consider all multi-photon signals known to Eve
[Inamori, NL, Mayers, quant-ph/0107017
EurPhysJD **41**, 599 (2007)]
[Gottesman, Lo, NL, Preskill, QIC 2004]

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

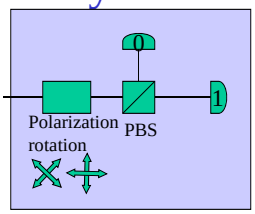
$R_{PNS} = \frac{p_{exp} - p_{multi}}{p_{exp}}$ Minimal fraction of contributing single photon signals

Secure key rate follows from qubit formula by simple rescaling!

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

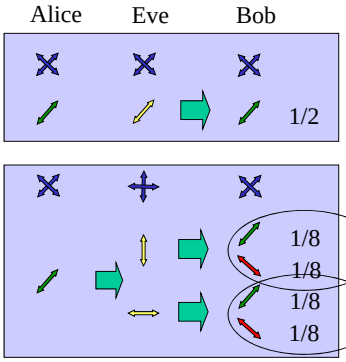


Why worry about detectors?



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

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



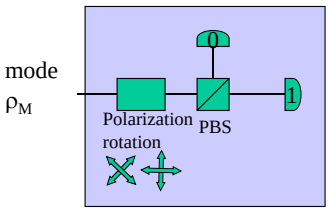
Discarding double clicks:
➔ Error rate: 0%
➔ Eve's information: 100%

double clicks!
(when resending many photons)

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

Discarding all double clicks can compromise QKD!

Finding Qubits in Optical Modes

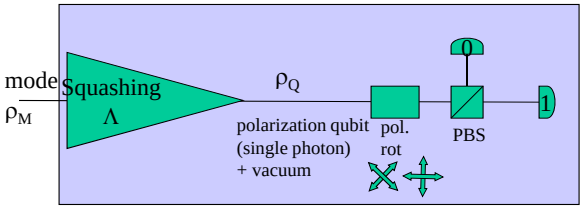


Post-Processing

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

50/50 assignment

POVM elements F_M^i
$p^i = Tr[\rho_M F_M^i]$



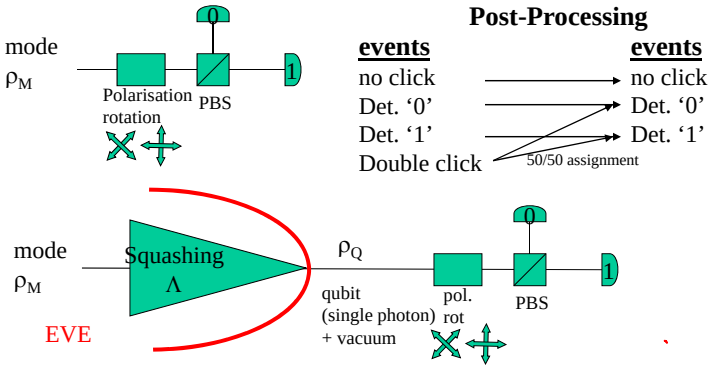
events
no click
Det. '0'
Det. '1'

POVM elements F_Q^i
$p^i = Tr[\rho_Q F_Q^i]$

Squashing map Λ:
-trace preserving
-completely positive
$\Lambda(\rho_M) = \sum_k A_k \rho_M A_k^\dagger$

Requirement on Squashing Map:
$Tr[\rho_M F_M^i] = Tr[\rho_Q F_Q^i]$

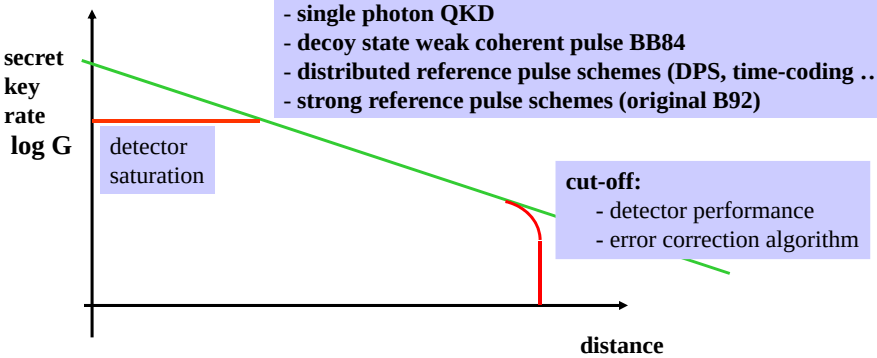
Finding Qubits in optical Modes



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

Limitations of Point-to-Point Links

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



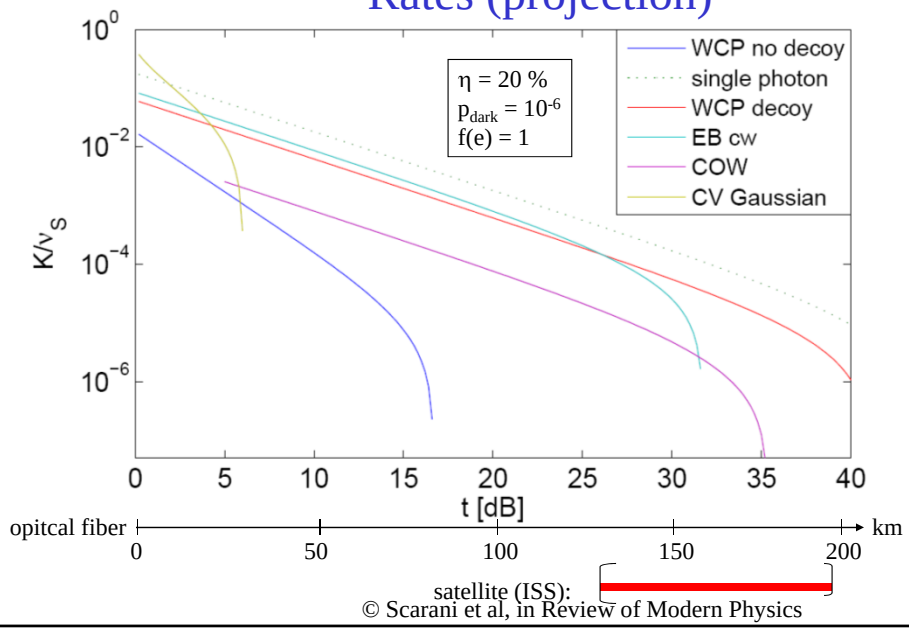
'Classical' Problems for higher clock rates:

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

➔synchronisation

Outlook

Rates (projection)



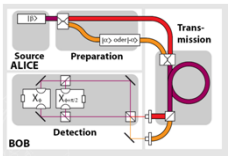
© Scarani et al, in Review of Modern Physics

Waterloo IQC Institute for Quantum Computing

Security and Modelling

Actual Device
e.g. reality based

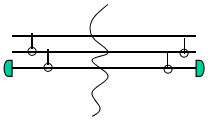
modelling



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)

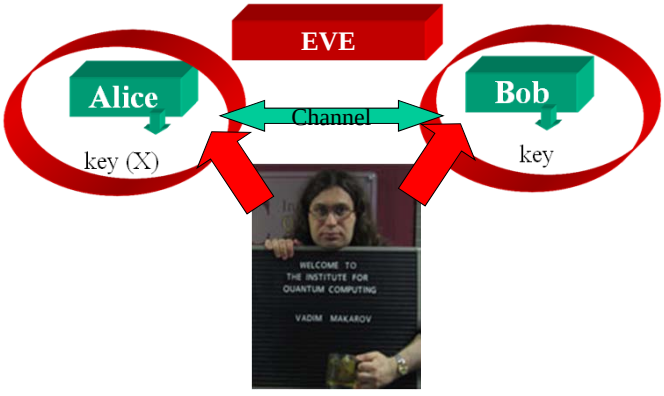
$||\rho_{ABE} - \rho_{AB} \otimes \rho_C||_1 \leq \epsilon$

Security Proof

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

Waterloo IQC Institute for Quantum Computing

Not so friendly …



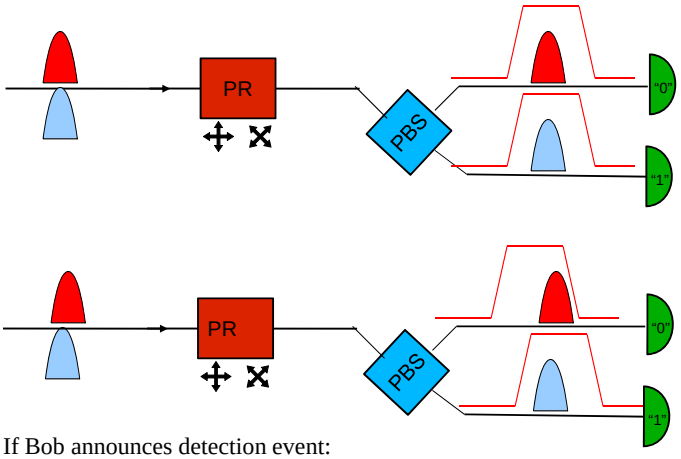
What Vadim Markarov (Trondheim) does:
- find deviations of devices from model assumptions
- actively intrude devices via optical fibers!
- manipulate devices (blind, burn detectors)

Vadim's complices: Hoi-Kwong Lo, Antia Lamas-Linares, Christian Kurtsiefer

Time Shift Attack

[Hoi-Kwong Lo's group]

Input from Eve



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

What is a Security Proof?

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

Calibration (initial and ongoing)

Alignment

Initialization

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

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

-Exact Protocol
-sequence of protocol steps
-Error Correction method
-Privacy Amplification function
-security parameters

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

Waterloo IQC Institute for Quantum Computing

Wh… …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…

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)

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

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

…Privacy Amplification function
-security parameters

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

Security proof defined by scientific standard

Waterloo IQC Institute for Quantum Computing

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

Device Independent QKD

Goal: Reduce assumptions about devices

(will always need to keep SOME assumptions)

Device Independence I: [Masanes, Acin, Gisin]

Do not even assume Quantum Mechanics holds

➔ only constraint on three-party correlations:

non-signaling correlations

Device Independence II: [Mayers, Yao; Mosca]

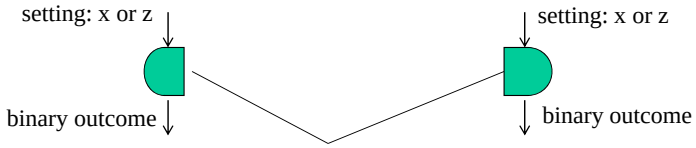
Assume Quantum Mechanic Rules apply

➔ Self-testing of devices

Self-testing similar to Bell test ...

Bell tests

Bell-inequality



Application:

- test of quantum mechanics
- Device Independent Quantum Key Distribution (devices x and z not characterized)

Obstacle:

Loss in distribution channel and in actual detection

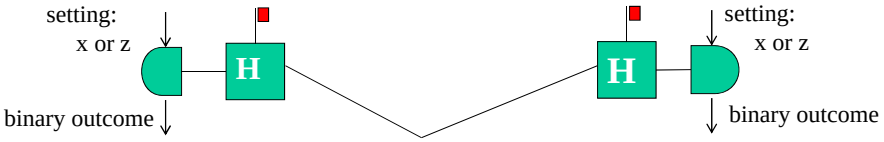
➔ no fair sampling assumption available!

Patch: random assignment for lost signals ➔ increased error rate ➔ loss of violation

[Note: other, non-random assignments might be better in some situations!]

Heralding

Heralding (H) can fight transmission loss



We can condition on flags being raised on both sides, as long as flag is independent of
- setting x or z
- the actual outcome of the measurement

Possible arrangement: first waiting for heralding, then choose setting x and z

➔ counteracts transmission loss (leaves problem of detection efficiency)

Other application: e.g. heralding for quantum repeaters

Tutorial