Quantum cryptography and quantum cryptanalysis

candidate: Vadim Makarov
Quantum cryptography timeline

ca. 1970  Concept ("money physically impossible to counterfeit")

1984  Key distribution protocol (BB84)

1989  Proof-of-the-principle experiment

1993  Key transmission over fiber optic link

2004  First commercial offers

Market?
Secret key cryptography requires secure channel for key distribution.

Quantum cryptography distributes the key by transmitting quantum states in open channel.
Quantum key distribution

Alice's bit sequence: 1 0 1 1 0 0 1 1 0 0 1 1 1 0

Bob's detection basis: + × + + × × + + × × + +

Bob's measurement: 1 0 0 1 0 0 1 1 0 0 0 1 0 0

Retained bit sequence: 1 – – 1 0 0 – 1 0 0 – 1 – 0

Interferometric QKD channel

Alice

Light source

Transmission line

Bob

Detector bases:

\( \phi_A = -45^\circ \) or \(+45^\circ\) : 0

\( \phi_A = +135^\circ \) or \(-135^\circ\) : 1

\( \phi_B = -45^\circ \) : X

\( \phi_B = +45^\circ \) : Z
Quantum cryptography at NTNU

Fiber optic QKD setup

1. Optimal tracking of phase drift
2. Single photon detector with afterpulse blocking

Security against practical attacks

3. Large pulse attack: experiment
4. Faked states attack
5. Detector efficiency mismatch
QKD setup

**Alice**
- Laser: 1310 nm, Pulse rate = 10 MHz
- PM fiber
- Standard SM fiber

**Bob**
- APD
- Polarization combiner
- Phase modulator 1
- Phase modulator 2
- PM coupler 50/50
- Polarizing splitter
- Polarization controller

**Public communication (TCP/IP)**
Photo 1. Alice (uncovered, no thermoisolation installed)
Photo 2. Bob (uncovered, no thermoisolation installed)
Tracking phase drift

To get phase accuracy $\Delta \phi$ within $\pm 10^\circ$ (QBER_{opt}^{\Delta \phi} < 1\%)$, no more than $N_a = \sim 200$ detector counts per adjustment are required.

Optimally counted at $\pm 90^\circ$ points from the extreme of the interference curves. Exact required number of counts

$$N_a = \frac{2k^2}{\Delta \phi^2} \left( \frac{1}{1 - 2(QBER)} \right)^2,$$

where $k$ is the number of standard deviations of not exceeding $\Delta \phi$.

Tracking phase drift

To get phase accuracy $\Delta\varphi$ within $\pm10^\circ$ ($\text{QBER}_{\text{opt}} \Delta\varphi < 1\%$), no more than $N_a = \sim 200$ detector counts per adjustment are required.

Experiment: adjustment every 3 s, $N_a = 230$:

Test of QKD in laboratory conditions

Test run No. 1
best QBER
~ 4%

Test run No. 2
QBER = 5.7% average
Single photon detector: avalanche photodiode in Geiger mode

$t_{\text{gate}}$ down to 1ns
Gate pulse rate = 20 MHz

APD: Ge FD312L
$T=77K$, QE=16%, DC=$5 \cdot 10^{-5}$
In QKD systems, probability of detecting a photon per pulse is always much lower than 1 (e.g., \(~1/1000\)). This makes afterpulse blocking efficient, allowing without much loss in detection probability:

- In our QKD system: 20 MHz gate pulse rate
- In principle: a few orders of magnitude faster gate pulse rate
Hardware implementation of afterpulse blocking
Test of afterpulse blocking

APD: Ge FD312L
Gate pulse rate = 12 MHz
QE = 7%
T = 77K

Counts at 0.005 photon per pulse
Dark counts

Count probability, %

N
Quantum key distribution: components of security

1. Conventional security; trusted equipment manufacturer
2. Security against quantum attacks
   – security proofs for idealized model of equipment
3. Loopholes in optical scheme
   – imperfections not yet accounted in the proof
Large pulse attack

Alice

– interrogating Alice’s phase modulator with powerful external pulses (can give Eve bit values directly)
Large pulse attack: experiment

Alice

Laser

4% reflection

Phase modulator

\[ V_{\text{mod}} \]

Eve

OTDR

Out

In

Variable attenuator

\[ L_1 \]

\[ L_2 \]

Received OTDR pulse

Fine length adjustment to get \( L_1 = L_2 \)

Photo 3. Artem Vakhitov tunes up Eve’s setup
Faked states attack

Conventional intercept-resend:

\[ \text{A} \rightarrow \text{B} \rightarrow \text{A} \rightarrow \text{B} \]

\[ \text{EVE} \]

Faked states attack:

\[ \text{A} \rightarrow \text{B} \rightarrow \text{FS} \rightarrow \text{B} \]

\[ \text{EVE} \]

\[ \text{ALARM!!!} \]

\[ \text{(no alarm)} \]

Exploiting common imperfection: detector gate misalignment

Detector gate misalignment

Detector gate misalignment

BOB

Detector gate misalignment

Detector gate misalignment

Example: Eve measured with basis Z (90°), obtained bit 1

(Eve resends the opposite bit 0 in the opposite basis X, shifted in time)
Eve resends the opposite bit 0 in the opposite basis X, shifted in time.

Example: Eve measured with basis Z (90°), obtained bit 1.

Detector gate misalignment.

- Eve's attack is not detected.
- Eve obtains 100% information of the key.
Partial efficiency mismatch

Detector efficiency

$\eta_0(t_0)$, $\eta_1(t_0)$, $\eta_1(t_1)$, $\eta_0(t_1)$
Partial efficiency mismatch

A. Practical faked states attack:

\[
QBER = \frac{P(\text{error})}{P(\text{arrive})} = \frac{2\eta_0(t_1) + 2\eta_1(t_0)}{\eta_0(t_0) + 3\eta_0(t_1) + 3\eta_1(t_0) + \eta_1(t_1)}
\]

⇒ In the symmetric case (when \(\eta_1(t_0)/\eta_0(t_0) = \eta_0(t_1)/\eta_1(t_1)\)),

Eve causes less than 11% QBER if mismatch is larger than 1:15

B. General security bound (incomplete):

\[
QBER = \frac{\eta\delta}{1 + \eta\delta - \delta} \approx \eta\delta,
\]

where

\[
\eta = \min \left\{ \min_t \frac{\eta_1(t)}{\eta_0(t)}, \min_t \frac{\eta_0(t)}{\eta_1(t)} \right\}
\]
Detector model 1.
Sensitivity curves

Normalized detector sensitivity, arb. u.

$t, \text{ns}$
Detector model 2.

Sensitivity curves at low photon number $\mu=0.5$

![Graph showing detector quantum efficiency vs time](image)

- $t_0 = 5.15$ ns
- $\frac{\eta_1}{\eta_0} \approx 1/9$
- $t_1 = 7.40$ ns
- $\frac{\eta_0}{\eta_1} \approx 1/30$
Detector efficiency mismatch

- Detector efficiency mismatch is a problem for many protocols and encodings: BB84 (considered above), SARG04, phase-time, DPSK and Ekert protocols. [quant-ph/0702262]

- Control parameter $t$ that changes detector efficiencies shall not be necessarily timing; it can be, e.g., wavelength or polarization.

- The worst-case mismatch, no matter how small, must be characterized and accounted for during privacy amplification.
Conclusion

- A phase tracking technique and detector with afterpulse blocking were successfully developed. (QKD was demonstrated with a very limited success.)

- Our group has built unique expertise in quantum cryptanalysis of attacks via optical loopholes. Several attacks have been proposed, studied in detail, and protection measures suggested.
Possible future research

• Continuing security studies beyond those presented in the thesis; we have experimented with passively-quenched Si APD; we are trying to incorporate detector efficiency mismatch into general proof... With sufficient financing, a study of high-power damage can be attempted.

• Improving the QKD experiment, demonstrating it over at least ~20 km distance. Performance of detector and phase tracking can be more accurately characterized.

• The QKD field is abound with novel ideas that can be tried...
Optional slides
Handling errors in raw key

\[ R = 1 - 2 h(\text{QBER}) \]
Commercial offers (as of late 2006)

- **MagiQ Tecnologies**
  - USA

- **id Quantique**
  - Switzerland

Standard VPN router + QKD equipment for frequent key changes

Several other companies also have the QKD technology, but are not selling yet.
Photo 4. Bob (left) and Alice (right), thermoisolation partially installed.
Typical values of reflection coefficients for different fiber-optic components
(courtesy Opto-Electronics, Inc.)
(Eve’s basis = Bob’s basis) is sufficient for eavesdropping

Incompatible basis – discarded by Alice and Bob during sifting
Security state of QKD system

- Insecure
- Not proven (assumed insecure)
- Secure with reduced key rate

\[ QBER \]

\[ \eta \]

(reduced rate at QBER=0 line, too)