Implementation of an attack scheme on a practical QKD system

Christian Kurtsiefer





ICQIT @ NII Tokyo, Dec 2-5, 2009





- Our BB92 QKD implementation
- Photodetector vulnerability
- Practical attack on BBM92 for a fiber channel
- 'Faking' the violation of a Bell test

QKD with photon pairs: BBM92

Quantum correlations & measurements on both sides



public discussion (sifting, key gen / state estimation)

error correction, privacy amplification

- like BB84, but no trusted random numbers for key
- direct use of quantum randomness for measurement basis





free space link, works even in daylight



 polarization encoding, cw pair source, wavelength 810±3nm timestamping photoevents

Very gory details





Typical performance





M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, C.K., NJP 11, 045007 (2009)



Detector saturation and QBER



 main limit is detector saturation, not QBER due to accidental coincidences

 similar for high bit rate systems

Basic photodetector operation

Avalanche photodiodes (APD) are common "single photon" detectors



APD detector vulnerability I





...and forced to give a signal by bright light pulses:



Avalanche diode operates in PIN / normal amplification regime

Hijacking one detector...



Combined to attack scheme by sending 'fake states' of classical light:



• Detector is quiet

blinding level $P_1 > P_B$ (few pW)

 Detector can be forced to a click at well-defined time

 $P_2 > P_T$ (few mW)

Fake state attack : Vadim Makarov, NJP 11, 065003 (2009)

• This works with detector pairs as well:



Choose unpolarized / circularly polarized *P*₁ and different linear polarizations to fake a 'click'

Light: "H" detector: "V" detector:



Why stop at two....



Control of a passive base choice QKD detector:



• Eve now has complete control over this detection scheme....

Four detector attack

"faked state"





our polarization detector



 Choose pule amplitudes above +45 threshold, but below H/V threshold -- ideally 1- √2/2 margin for P₂ Eve's intercept-resend kit





Coincidence timing histograms of a working system



No resolvable influence on detector signal timing (<100 ps jitter)

Insertion delay ~10 nsec

Full intercept/resent scheme



(wireless LAN)

Layout of the plot



"Realistic" fiber link across the Science faculty @ NUS



Results for Alice & Bob



 reasonable photo detection rates on both sides (includes transmission loss)

- reasonable pair rate and raw key rate around 1.1 kcps
- no spurious pulses
- reasonable error ratio for this source allows to extract 500 bits/sec key after PA / EC

Attack Results I



A real-time display of events between **Eve** and **Bob**:



- About 97%-99% of Eve clicks are transferred to Bob
- Eve can identify successful detections by Bob from timing information (classical channel intercept)
- Eve knows correctly identified pairs due to losses (classical channel intercept)
- Eve knows all detector outcomes of Bob



Correlation between Eve and Bob's result (the hijacked receiver) is 100%

630,106	0	0	0
0	841,072	0	0
0	0	1,116,070	0
0	0	0	1,026,603

- Eve has Bob's complete raw key
- By eavesdropping the classical communication in error correction/privacy amplification, Eve can reconstruct the secret key

Does active base choice help?



- Correlation between Eve's command and Bob results is 100%
- Bob's probability of getting Eve's base choice correct is 50%

Presence of Eve looks like 50% loss (no big help)

Do other protocols help?



Device-independent / Ekert-91 protocol idea



For proper settings 1, 2, 1', 2' and state $|\Psi^-\rangle$: $S=\pm 2\sqrt{2}$

 Estimate quantitatively the knowledge of Eve of raw key between A and B from S:

$$I_{E}(S) = h \left(1 + \frac{\sqrt{S^{2}/4 - 1}}{2} \right)$$

No fingerprint problems of photons due to side channels
A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, PRL 98, 230501 (2007)

Implementation attempt

use almost same kit:





A. Ling, M. Peloso, I. Marcikic, A. Lamas-Linares, V. Scarani, C.K., Phys. Rev. A 78, 020301(2008)



core part of device-independent QKD protocol



- Alice & Bob will see "programmed" correlations in 25% of the cases (base match on both sides), rest nothing
- Alice and Bob cannot distinguish from lossy line....
- We programmed (and found) CHSH results from S = -4 4 with active choice

What is going on??

How can device-independent break down?

- Losses in CHSH are removed by post-selecting pair observations using a fair sampling assumption
- Current pair sources (η = 70%) and detectors (η = 50% for non-cryogenic ones)
- Eve hides behind losses of transmission line. Best guess: optical fiber and ideal (η = 100%) detectors. At 0.2dB/km@1550nm, T = 25% for dist = 30 km
- Only very short distances possible with current detectors

Can this be fixed ?

Yes, of course.

Monitor total intensity with a separate, non-saturable photodetector (PIN diode)

Blinding power and bright pulses are much brighter than usual photon signal

 Monitor the state of APD's by looking at their voltage, asserting 'detector readiness'

... of a "Bad Implementation" ??

- Are there detectors / detector concepts which are not susceptible to such or similar attacks?
- Do we have other practical attacks?
- Will all practical implementations always be potentially bad implementations of a theoretically secure protocol?
- Let's leave Hilbert space and have independent challenge/assessments of security claims
- What do we offer in comparison to classical key exchange devices like tamper-safe devices? Is QKD just an elegant version of such a device?

Valerio Scarani, C.K., arxiv:0906.4547

Thank You!

Team members NTNU Trondheim Vadim Makarov Qin Liu

Team members CQT Singapore

Ilja Gerhardt Matt Peloso Caleb Ho Antia Lamas-Linares C.K.

Group: http://qoptics.quantumlah.org/lah/

CQT Graduate program: http://cqtphd.quantumlah.org

Clock synchronization I

No dedicated hardware, use correlations in SPDC

Clock synchronization II

 Step 1: Find "coarse" time difference in short interval via peak in cross-correlation function

sample detection events over two short periodes 1 and 2

find timing difference ΔT in both intervals with coarse timing resolution δT

typical values:

ΔT_A = 250 ms δ*T* = 2...20 μs

```
need \delta T = 2 ns
```

Clock synchronization III

• Step 2: Follow short timing differences in large intervals δt

• Step 3: Extract fine time offset part ΔT and relative frequency difference Δu from residual difference distribution

Works for $\delta T/\Delta T = 10^{-9}$, $\Delta u = 10^{-4}$, up to Sig/BG = 1/100

C. Ho, A. Lamas-Linares, C. Kurtsiefer, NJP **11**, 045011 (2009)