Experimental realization of measurement-device-independent quantum key distribution

Xiongfeng Ma[1], Yang Liu[2], Teng-Yun Chen[2], Liu-Jun Wang[2], Hao Liang[2], Guo-Liang Shentu[2], Jian Wang[2], Ke Cui[2], Hua-Lei Yin[2], Nai-Le Liu[2], Li Li[2], Jason S. Pelc[3], M. M. Fejer[3], Cheng-Zhi Peng[2], Qiang Zhang[2], and Jian-Wei Pan[2]

[1]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China
[2]Shanghai Branch, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, China
[3]E. L. Ginzton Laboratory, Stanford University, 348 Via Pueblo Mall, Stanford CA 94305, USA

Abstract: Quantum key distribution (QKD) is proven to offer unconditional security in communication between two remote users with ideal source and detection. Unfortunately, ideal devices never exist in practice and device imperfections have become the targets of various attacks. By developing up-conversion single-photon detectors with high efficiency and low noise, we faithfully demonstrate the measurement-device-independent (MDI) QKD protocol, which is immune to all hacking strategies on detection. Meanwhile, we employ the decoy-state method to defend attacks on non-ideal source. By assuming a trusted source scenario, our practical system, which generates more than 25 kbits secure key over a 50 km fiber link, serves as a step stone in the quest for unconditionally secure communications with realistic devices. More details can be found at arXiv:1209.6178.

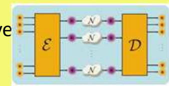
Secure in principle

- QKD protocols
  - Prepare-and-measure: BB84, Bennett92, six-state
  - Entanglement based: Ekert91, BBM92
- Security proofs
  - Mayers, Lo-Chau, Shor-Preskill, Devetak-Winter-Renner
- With imperfect devices
  - Mayers, Lütkenhaus, ILM
  - Koashi-Preskill: basis-independent source
  - Gottesman-Lo-Lütkenhaus-Preskill (GLLP)

Loopholes in practice

- Source **OK**
  - Plug & Play system
  - Coherent state: decoy state
  - Relatively a simple component

- Channel **Great!**
  - Assumed to be controlled by Eve
  - Security guaranteed in security proofs in most cases

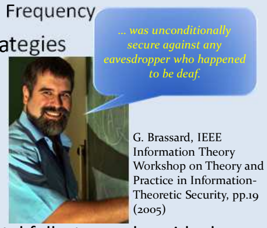


- Detection **Problematic!**
  - Efficiency loophole
  - Detector imperfections: dead time, after pulse.
  - Most attacks launch here

Is a practical QKD system really secure?

Quantum hacking

- Side information
  - Basis (or bit) information may be contained in other degrees of freedom
  - Timing of the pulse, Frequency
- Practical hacking strategies
  - Time-shift attack
  - Fake-state attack
  - Strong pulse attack
  - …

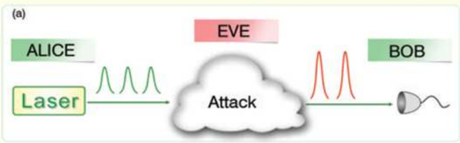


G. Brassard, IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, pp.19 (2005)

- Solutions
  - Push the experimental folks to produce ideal devices: need 20+ years?
  - Self-testing (device-independent) QKD: not practical with current technology

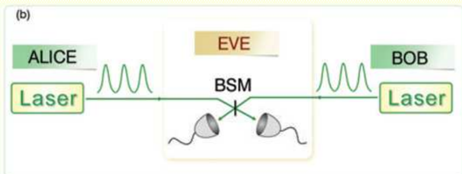
Can we have a secure QKD system in practice?

Conventional QKD setup



- Prepare-and-measure QKD: Alice sends qubits to Bob through an insecure quantum channel, controlled by Eve.
- Key problem: the signal received by Bob may be manipulated by Eve so that Bob's detection system does not function as expected. See, for example time-shift attack.

MDI-QKD setup

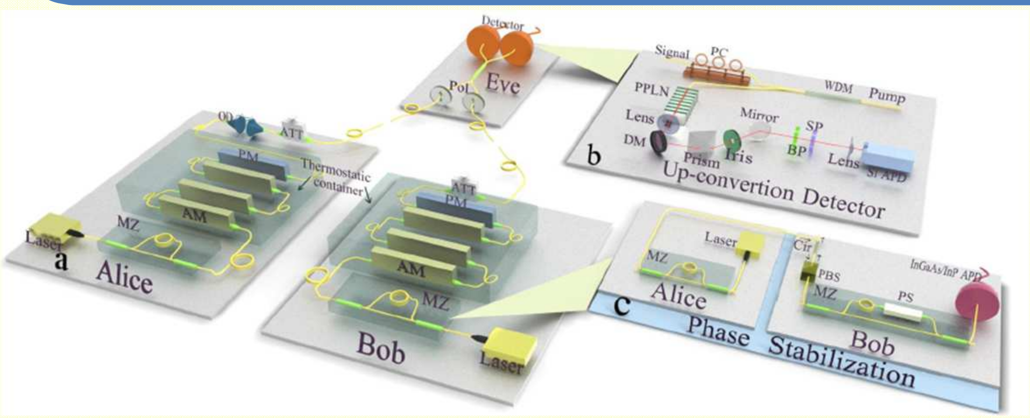


- MDI-QKD: Alice and Bob each sends quantum signals to Eve for measurement.
- To solve the problem: leave the detection system to Eve's hand
- Alice and Bob do not receive any quantum signals from the *unsafe* channel

Selling points

- Completely untrusted detection device scenario
- Decoy-state method is applied to replace single-photon source with practical weak coherent state source
- Can be directly applied to network case: users only need to possess cheap part --- laser source, while the expensive part --- detection can be shared in the untrusted relay

MDI-QKD is able to defend all existing quantum hacking strategies!



Experiment results

- Gains for signal/decoy states in the X/Z basis

	μ/ν	0	0.1	0.2	0.5
Z basis	0	0	4.19×10^{-9}	1.38×10^{-8}	6.22×10^{-8}
	0.1	4.49×10^{-9}	1.98×10^{-6}	4.01×10^{-6}	9.87×10^{-6}
	0.2	8.67×10^{-9}	4.02×10^{-6}	7.97×10^{-6}	1.99×10^{-5}
	0.5	2.51×10^{-8}	1.01×10^{-5}	2.02×10^{-5}	5.06×10^{-5}
X basis	0	3×10^{-10}	1.00×10^{-6}	4.16×10^{-6}	2.68×10^{-5}
	0.1	1.12×10^{-6}	4.20×10^{-6}	9.30×10^{-6}	3.81×10^{-5}
	0.2	4.38×10^{-6}	9.51×10^{-6}	1.67×10^{-5}	5.20×10^{-5}
	0.5	2.73×10^{-5}	3.85×10^{-5}	5.18×10^{-5}	1.06×10^{-4}

- Quantum bit error rates (QBERs)

TABLE V. List of quantum bit error rates (50 km)

	Z basis				X basis			
μ/ν	0	0.1	0.2	0.5	0	0.1	0.2	0.5
0	–	35.71%	50.00%	53.37%	0.00%	50.36%	49.74%	49.85%
0.1	40.00%	0.33%	0.24%	0.38%	50.63%	27.08%	30.41%	37.93%
0.2	41.38%	0.21%	0.19%	0.22%	51.07%	31.02%	27.67%	31.90%
0.5	50.00%	0.22%	0.17%	0.14%	50.13%	37.84%	32.13%	27.70%

- Final key generation: 25 kbit final secure key
- Reference

– Lo, Curty, and Qi, PRL, 108, 130503 (2012)
– Ma and Razavi, PRA, 86, 062319 (2012)
– Ma, Fung, and Razavi, PRA, 86, 052305 (2012)
– Rubenok et al., arXiv:1204.0738 (2012)
– da Silva et al., arXiv:1207.6345 (2012)
– **Liu et al., arXiv:1209.6178 (2012) to appear in PRL**

Experimental Challenges

- Independent laser interference: indistinguishability
  - Frequency, time, polarization, etc.
- Coincident click
  - Detector efficiency: quadratic dependence
- Quantum information stabilization
  - Two channels
- Statistical fluctuation analysis
  - Lots of efforts from theoretical side

Implementation details

- Up-conversion single-photon detectors are employed
  - High efficiency: >15%
  - Low dark count: < 10^{-5} per pulse
- Polarization control
  - Using PBS before interference
- Timing feedback control
- Frequency match
- Post processing
  - Finite-key analysis
- Repetition rate: 1 MHz, duration: 59.5 hours

PhD students and post-doc applicants are very welcome!