Practical measurement-device-independent quantum key distribution

Feihu Xu[1*], Marcos Curty[2], Bing Qi[1], Wei Cui[1], Charles Ci Wen Lim[3], Kiyoshi Tamaki[4] and Hoi−Kwong Lo[1]

[1]Center for Quantum Information and Quantum Control, Dept. of ECE and Dept. of Physics, University of Toronto, Toronto, Canada

[2]Escuela de Ingeniería de Telecomunicación, Dept. of Signal Theory and Communications, University of Vigo, Vigo, Spain

[3]Group of Applied Physics, University of Geneva, Geneva, Switzerland

[4]Research Laboratories, NTT Corporation, 3-1,Morinosato Wakamiya Atsugi-Shi, Kanagawa, Japan

* feihu.xu@utoronto.ca Ref: F. Xu, M. Curty, B. Qi, H.-K. Lo, arXiv:1305.6965 (2013); M. Curty, F. Xu, *et al.*, arxiv:1307.1081 (2013).

Quantum key distribution (QKD) under attack!

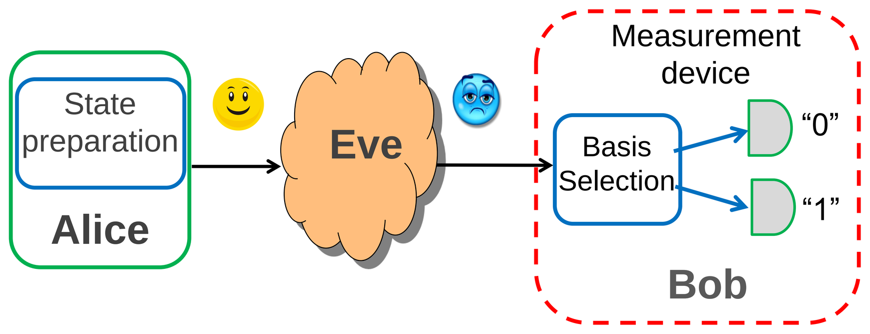
- **The gap between theory and practice.**

- In theory, QKD offers perfect security based on the laws of quantum mechanics.
- In practice, however, physical devices inevitably have overlooked imperfections.

➡ QKD under side-channel attacks!

- **The weakest link in a QKD system is the measurement device.**

Fig.1. Schematic diagram of conventional QKD.

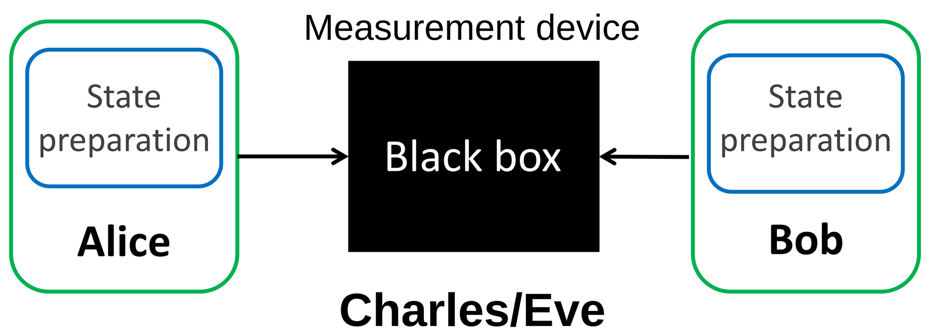


Tab I. Summary of quantum-hacking activities.

Attack	Target component	Tested system
Time-shift	Detector	ID Quantique
Y. Zhao et al., Phys. Rev. A 78, 042333 (2008)		
Phase-remapping	Phase modulator	ID Quantique
F. Xu, B. Qi, H.-K. Lo, New J. Phys. 12, 113026 (2010)		
Detector-control	Detector	ID Quantique, MagiQ Tech.
L. Lydersen et al., Nat. Photonics 4, 686 (2010)		
Channel calibration	Detector	ID Quantique
N. Jain et al., Phys. Rev. Lett. 107, 110501 (2011)		
Detector-control	Detector	research syst.
I. Gerhardt et al., Nat. Commun. 2, 349 (2011)		
Detector deadtime	Detector	research syst.
H. Weier et al., New J. Phys. 13, 073024 (2011)		
…	…	

Measurement-Device-Independent QKD

Fig.2. Schematic diagram of MDI-QKD [1].



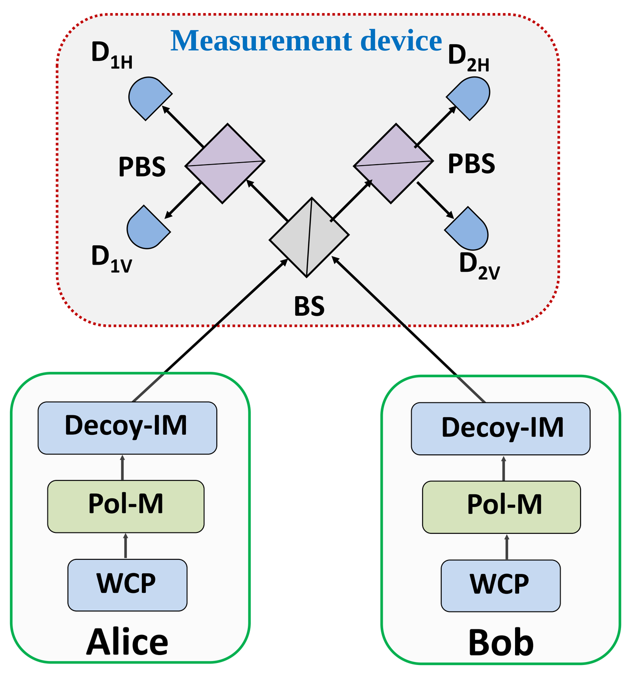


Fig.3. MDI-QKD with decoy states [1]. WCP, weak coherent pulse; Pol-M, polarization modulator; IM, intensity modulator; BS, beam splitter; PBS, polarization beam splitter; D, detector.

- A practical way to do QKD with "untrusted detectors".
- Automatically immune to all side-channel attacks in the detection system.
- Possibility of out-sourcing the manufacturing of detection systems to any untrusted manufacturers.
- Assumption: Alice and Bob trust their state preparation devices.

Secure key rate: $R \geq P_Z^{1,1} Y_{Z,L}^{1,1}\left[1 - H_2\left(e_{X,U}^{1,1}\right)\right] - Q_Z f_e(E_Z) H_2(E_Z)$

- **Experimental measurements**: Q_Z and E_Z are the gain and quantum bit error rate (QBER) in the Z basis.
- **Estimations using the decoy-state protocol**: $Y_{Z,L}^{1,1}$ and $e_{X,U}^{1,1}$ are the lower bound of the yield and the upper bound of the QBER when Alice and Bob send out single-photon pulses.

Two decoy-state protocol

- A practical method to estimate the single-photon contributions (*i.e.* $Y_{Z,L}^{1,1}$ and $e_{X,U}^{1,1}$) using one signal state μ and two decoy states υ and ω.

- Experimental measurements:

$Q_{Z/X}^{q_a,q_b}$ -- Gains in the Z and X basis with intensity setting q_a (Alice) and q_b (Bob), $q \in \{\mu, \nu, \omega\}$.

$E_X^{q_a,q_b}$ -- QBERs in the X basis with intensity setting q_a and q_b.

$E_Z^{\mu_a,\mu_b}$ -- QBER in the Z basis with intensity setting μ_a and μ_b.

- **Our results [3, 5]:**
  - Two Analytical bounds that can be directly used by experimentalists to demonstrate MDI-QKD and are easy for parameter optimizations.
  - A practical approach with two general decoy states satisfying $\mu > \nu > \omega \geq 0$.
  - We simulate the key rates numerically and optimize this decoy-state method.

Finite-key analysis

- **Problem:** a real QKD experiment is completed in finite time, which means that the length of output keys is finite. Thus, the estimation of relevant parameters suffers from statistical fluctuations. This is called the finite-key effect.

- **Our solutions [5]:**
  - A novel parameter-estimation method in high-loss regime and against the most general attacks.
  - A rigorous finite-key analysis using smooth min-entropy method and satisfying the composable security definition of QKD.

- **Secret key length:**

$$l_k \leq n_0 + n_1\left(1 - h_2(e_1)\right) - \text{leak}_{\text{EC}} - log_2\frac{8}{\epsilon_{cor}} - 2log_2\frac{2}{\hat{\epsilon}\epsilon'} - 2log_2\frac{2}{2\epsilon_{PA}}$$

Numerical simulation

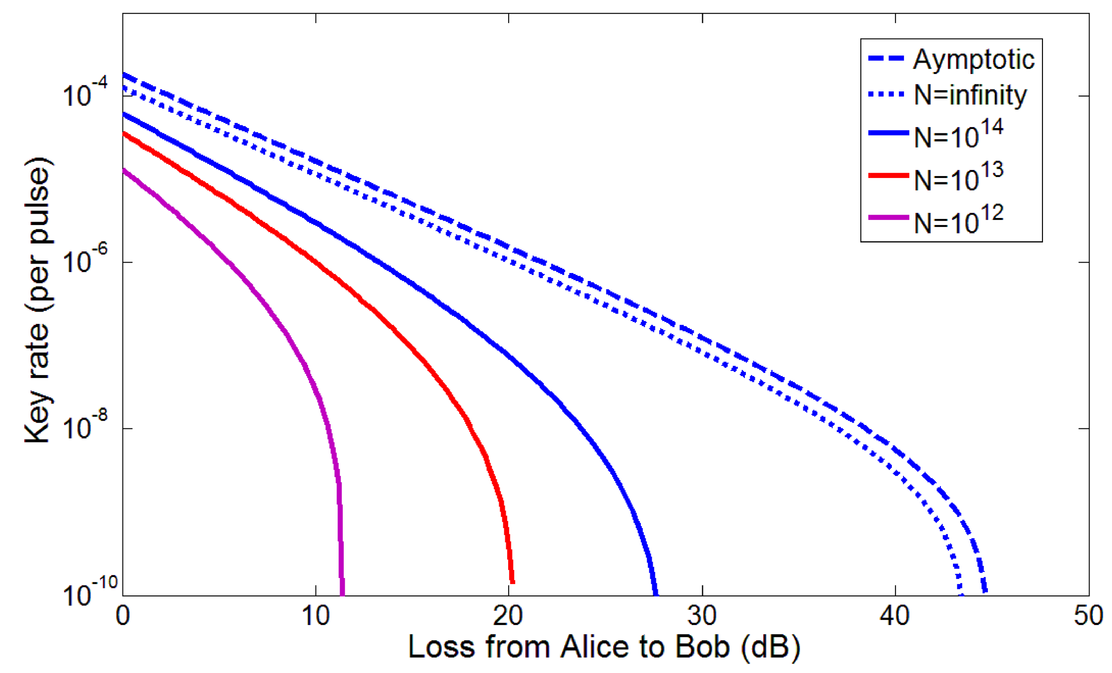


Fig.5. Finite-key rate using the practical parameters from [2]: the detector efficiency is 14.5%; the dark count rate is 6×10^{-6}; the system misalignment error is 1.5%; the security bound is $\epsilon = 10^{-10}$. Channel model: three unitary operators are used to model the polarization misalignments.

- **For a 1 GHz system, Alice and Bob can easily distribute a 1 Mb secret key over a 75 km standard fiber link within 3 hours.**

Conclusion

We have presented an analysis for real-life MDI-QKD. To evaluate its performance, we study various practical errors by developing a general system model [3]. For the finite decoy-state protocol, we have discussed a simple analytical method [3], which can be directly used by experimentalists to demonstrate MDI-QKD [4]. Most importantly, we provide, for the first time, a rigorous security proof of MDI-QKD in the finite-key regime that is valid against general attacks, and satisfies the composable security definition of QKD [5].

Acknowledgement: The authors acknowledge S. Gao, X. Ma, L. Qian for enlightening discussions. Support from funding agencies NSERC, the CRC program, European Regional Development Fund, and the Galician Regional Government is gratefully acknowledged.

References

[1] H.-K. Lo, M. Curty, and B. Qi, *Physical Review Letters*,108, 130503 (2012).
[2] R. Ursin, *et al.*, *Nature Physics*, 3, 481 (2007).
[3] F. Xu, M. Curty, B. Qi, and H.-K. Lo, *arXiv:1305.6965* (2013).
[4] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization-encoding measurement-device-independent quantum key distribution" *arxiv:1306.6134* (2013).
[5] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution" *arxiv:1307.1081* (2013).