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] *Centre for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[2] *Escuela de Ingeniería de Telecomunicación, Dept. of Signal Theory and Communications, University of Vigo, Vigo, Pontevedra, 36310, Spain*
[3] *Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland*
[4] *NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato Wakamiya Atsugi-Shi, Kanagawa, 243-0198, Japan*
(Dated: July 19, 2013)

We present an analysis for practical implementations of measurement-device-independent quantum key distribution (MDI-QKD): a general system model, a finite-decoy protocol and a finite-key analysis. This is of particular interest both to researchers hoping to demonstrate MDI-QKD and to others performing non-QKD experiments involving quantum interference.

Introduction

Quantum key distribution (QKD) enables an unconditionally secure means of expanding secret keys between two remote parties. However, real-life implementations of QKD may contain overlooked imperfections that deviate from the theoretical model. In particular, by exploiting practical imperfections, especially those in the detectors, researchers have proposed and successfully demonstrated various quantum attacks, called quantum hacking, against practical QKD systems [1]. Therefore, quantum hacking has become a major problem for the real-life security of QKD.

Lo, Curty, and Qi proposed a groundbreaking scheme – measurement device independent QKD (MDI-QKD) [2] – to solve the quantum hacking problem. More precisely, MDI-QKD removes all attacks in the detection system, the most important loophole of QKD implementations. In a general MDI-QKD [2] (Fig. 1(a)), each of Alice and Bob locally prepares phase randomized decoy states in the BB84 protocol and sends them via a quantum channel to an *untrusted* quantum relay, Charles, who is supposed to perform a Bell state measurement and broadcasts his measurement results. Since the measurement setting is only used to post-select entanglement between Alice and Bob, it can be treated as a true black box. Hence, MDI-QKD is inherently immune to all attacks on detectors including side channel attacks.

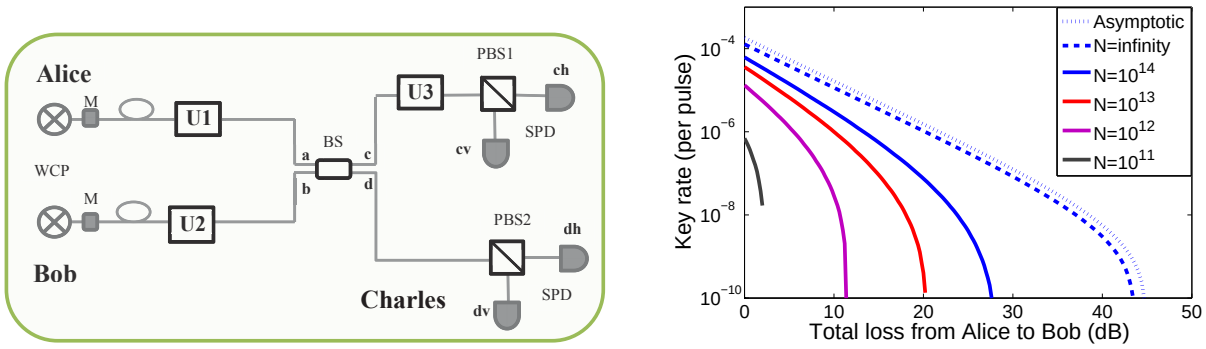
MDI-QKD is highly practical and can be implemented with standard optical components. Very recently, MDI-QKD has been demonstrated by a number of research groups [3, 4], but before it is applicable in real life, it is important to resolve a number of practical issues. Firstly, a practical implementation of MDI-QKD may involve various practical errors such as the mode mismatch for a non-perfect quantum interference. Thus, the question is: how will the practical errors affect the performance of MDI-QKD? Secondly, the source typically emits weak coherent pulses and the single photon contributions are estimated by the decoy-state protocol. Hence, how many types of decoy states are needed for MDI-QKD in practice? Thirdly, a real experiment is implemented in finite time, which means that the output data-size introduces statistical fluctuations and any estimation techniques necessarily carry finite size corrections. How can one analyze this finite-data effect? Finally, before the implementation, one has to know the optimal intensities for signal and decoy states. What is the optimal choice of these intensities?

Summary of results

We answer the above questions in this work. Our main contributions are summarized below, and we refer the details to Refs. [5, 6].

1. We study the physical origins of the quantum bit error rate (QBER) in real-life MDI-QKD by proposing general models for various practical errors [5], in which we particularly investigate two important sources of errors – polarization misalignment (see Fig. 1(a)) and mode mismatch. We find that in a polarization-encoding MDI-QKD [2, 4], the polarization misalignment is the major source of QBER, while mode mismatch in other domains does not appear to be a major problem. Moreover, we provide an analytical method to model the system. Although this model is proposed to study MDI-QKD, it can also be applied to other non-QKD experiments involving quantum interference.

2. Despite numerous progress on the decoy-state protocol of MDI-QKD [7], a rigorous analysis of the finite-key effect remains missing. Here, we fill this gap by presenting a rigorous method to study both the finite-decoy



(a) (b)

FIG. 1: **(a)** MDI-QKD system model. We consider a polarization-encoding system [2, 4], where three Unitary rotations (U_1-U_3) are used to model the polarization misalignment (or rotation). The PBS2 (polarization beam splitter) is chosen to define the polarization basis. U_1 (U_2) represents the misalignment of Alice's (Bob's) channel transmission, while U_3 models the misalignment of the other measurement setting, PBS1. WCP: weak coherent pulse; M: modulator; BS, beam splitter; SPD, single-photon detector. **(b)** (color online) Secure key rates. The practical parameters are mostly from an entanglement based QKD experiment [8]. Asymptotic (dotted curve) denotes the case of infinite decoy states and infinite data-size. In finite-decoy case (dashed and solid curves), N denotes the total number of signals sent by Alice/Bob; we consider an *analytical* approach with two general decoy states to estimate the single-photon contributions [5]. Our results show that MDI-QKD is feasible for a reasonable number of signals (order of 10^{11} to 10^{14}).

protocol [5] and the finite-key analysis [6]. For the finite-decoy protocol, we primarily present how one can use two general decoy states to analytically estimate the single-photon contributions, *i.e.*, their gain and QBER. In the finite-key analysis, we use the Chernoff bound to estimate the statistical fluctuations and consider the smooth min-entropy formalism to analyze the finite-key effect. We emphasize that our result is valid against the most general attacks, while the previous analysis [7] is only valid against collective attacks. With the practical parameters from an entanglement based QKD experiment [8], the key rates for different cases are shown in Fig. 1(b).

3. We finally offer a general framework to evaluate the optimal choice of intensities of signal and decoy states [5]. This is particularly useful for experimentalists who wish to implement MDI-QKD. Note that this framework has already been adopted in our experimental demonstration [4].

Acknowledgments

We thank S. Gao, Z. Liao, L. Qian for enlightening discussions. Support from funding agencies NSERC and the CRC program is gratefully acknowledged.

* Electronic address: feihu.xu@utoronto.ca

[1] Y. Zhao, et al, *Phys. Rev. A* **78**, 042333 (2008); F. Xu, B. Qi, H.-K. Lo, *New J. Phys.* **12**, 113026, (2010); L. Lydersen, et al., *Nat. Photon.*, **4**, 686, (2010); I. Gerhardt, et al, *Nat. Commun.* **2**, 349, (2011); N. Jain et al., *Phys. Rev. Lett.*, **107**, 110501 (2011); H. Weier et al., *N. J. Phys.* **13**, 073024, (2011).
[2] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.*, **108**, 130503 (2012).
[3] A. Rubenok et al., *arXiv*:1204.0738 (2012); T. F. da Silva, et al., *arXiv*:1207.6345 (2012); Y. Liu et al., *arXiv*:1209.6178 (2012).
[4] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.-K. Lo, *arXiv*:1306.6134 (2013).
[5] F. Xu, M. Curty, B. Qi, H.-K. Lo, *arXiv*:1305.6965 (2013).
[6] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, H.-K. Lo, *arXiv*:1307.1081 (2013).
[7] X. Ma, C.-H. F. Fung, and M. Razavi, *Phys. Rev. A*, **86**, 052305 (2012); X.-B. Wang, *Phys. Rev. A*, **87**, 012320 (2013); S. Sun et al., *Phys. Rev. A*, **87**, 052329 (2013).
[8] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, *Nat. Phys.* **3**, 481 (2007).