Recent battle between quantum cryptographer and hacker

Xiongfeng Ma,[1,*] Yang Liu,[2] Yan-Lin Tang,[3] Teng-Yun Chen,[3] Hua-Lei Yin,[2] Chi-Hang Fred Fung,[4] Hai-Lin Yong,[2] Liu-Jun Wang,[2] Hao Liang,[2] Guo-Liang Shentu,[2] Jian Wang,[2] Ke Cui,[2] Li Li,[2] Nai-Le Liu,[2] Cheng-Zhi Peng,[2] Zeng-Bing Chen,[3] Qiang Zhang,[2] and Jian-Wei Pan[2,3]

[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, Anhui, China*
[3] *Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui, China*
[4] *Department of Physics and Center of Theoretical and Computational Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

Throughout history, every advance in encryption has been defeated by advances in hacking with severe consequences. In theory, quantum cryptography [1, 2] holds the promise to end this battle by offering unconditional security [3–5] when ideal single-photon sources and detectors are employed. In practice, unfortunately, the battle revives due to the gap between ideal devices and realistic setups, which has been the root of various security loopholes [6–8] and has become the targets of many quantum attacks [9–16]. Tremendous efforts have been made towards loophole-free quantum key distribution (QKD) with practical devices [17, 18]. However, the question of whether security loopholes will ever be exhausted and closed still remains.

The measurement-device-independent (MDI) QKD [19] protocol closes all loopholes on detection at once. In fact, the detectors in a MDI-QKD setup can even be assumed to be in Eve's possession. The legitimate users of QKD, Alice and Bob, encode the key information onto their own quantum states independently and then send them to the detection station for a Bell-state measurement (BSM). The quantum signals from two arms interfere in a beam splitter and are then detected by two detectors. Certain post-selected coincidence events are used as the raw key. As discussed in Ref. [19], even if Eve controls the measurement site, she cannot gain any information on the final key without being noticed. The security of MDI-QKD is based on the time-reversed version of entanglement-based QKD protocols [20, 21], which is naturally immune to any attack on detection and hence is able to shield against all aforementioned practical attacks [9–16].

In this work, we will present recent experimental realizations of MDI-QKD [22], see also [23, 24]. By developing up-conversion single-photon detectors with high efficiency and low noise, the MDI-QKD protocol is faithfully demonstrated. Meanwhile, the decoy-state method is employed to defend attacks on non-ideal source, such as photon-number-splitting attacks [25]. In the end, the system generates more than 25 kbits secure key over a 50 km fiber link. The experimental setup is shown in Fig. 1.

The main security assumption for the MDI-QKD protocol is the usage of trusted sources: phase randomized coherent state sources with intensity modulations. In the security proof of the decoy-state method, phase randomization is assumed for the sources [26]. A security analysis for decoy-state QKD without phase randomization is not yet available [27]. This fact can easily be overlooked and QKD system designers often neglect the implementation of phase randomization without realizing the danger of opening up a security loophole. Indeed, the experimental demonstration of our hacking strategy shows that this is a major security loophole. A practical attack on the source part of a decoy-state QKD system with WCS is proposed for the case where phase randomization is not implemented. By using a combination of an unambiguous-state-discrimination (USD) measurement and a photon-number-splitting (PNS) attack [25], one can show that the final key generated by the non-phase-randomized system can be compromised. The experimental setup is shown in Fig. 2.

By exploiting the phase information of the signal and decoy states, our experimental attack succeeds in stealing the final secret key when the transmission loss is over a certain threshold. We prove that phase randomization cannot be neglected in decoy-state QKD using WCS, unless a new security proof is available. Our result also answers a long-standing question. Before our work, it was unclear whether performing phase randomization improves the key rate performance of decoy-state BB84 using a WCS. Our result implies that performing phase randomization is strictly better. We remark that our attack is not limited to the phase-encoding system with strong phase-stabilization pulses [29–31] on which our experiment is based. As long as the phase of each state, be it a signal or decoy state, is known by Eve, she does not need the strong phase reference from Alice. Eve can simply prepare an auxiliary pulse with the corresponding phase. Therefore, this attack can be launched to hack regular decoy-state QKD (including MDI-QKD) systems without phase randomization.

A key feature of our experiment is the implementation of USD with linear optics. Even with only linear optics, this attack system can efficiently compromise the security

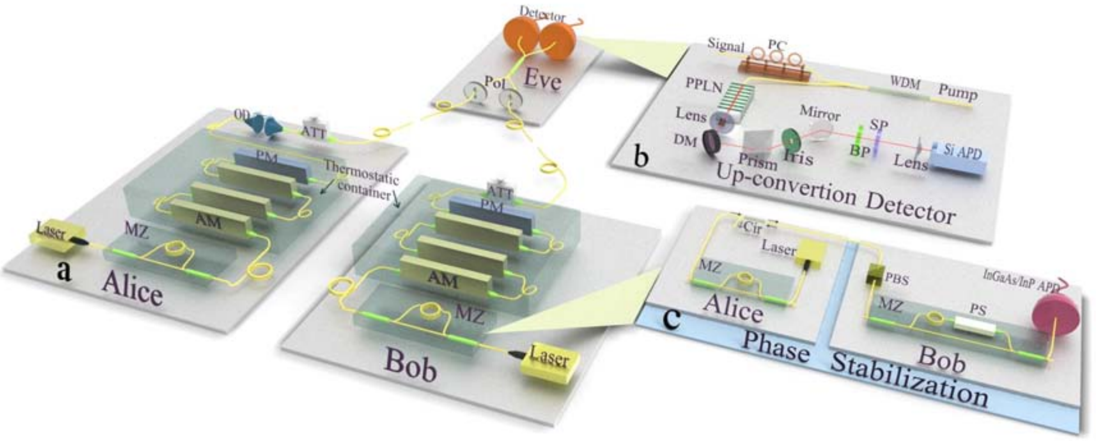

FIG. 1. (a) Diagram of our MDI-QKD setup. Alice passes her laser pulses through an unbalanced Mach-Zehnder (MZ) interferometer, with an arm difference of 6 meters, to generate two time-bin pulses. A phase modulator (PM) and three amplitude modulators (AM) are used to encode the qubit and generate decoy states. All the modulations are controlled by quantum random number generators. In order to reduce the temperature fluctuation, we put all the modulators into thermostatic containers. Bob's encoding system is the same as Alice's. The pulses are then attenuated by an attenuator (ATT) and sent out via fiber links from Alice and Bob to the measurement site. After traveling through 25 km fiber spools of each arm and polarizers (Pol.), signal pulses from two sides interfere at a 50:50 fiber beam-splitter (BS) for a partial BSM. The output photon is detected by up-conversion detectors and recorded with a time interval analyzer. (b) Diagram of an up-conversion single-photon detector. PC: polarization controller, DM: dichroic mirror, BP: band pass filter, SP: short pass filter. (c) Phase stabilization setup. Cir: circulator, PS: phase shifter, PBS: polarizing beam splitter.

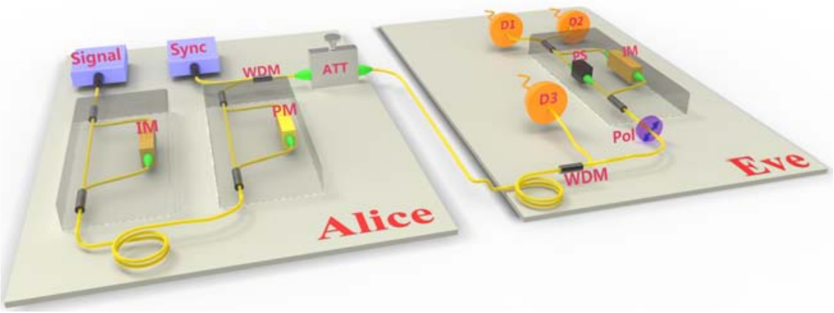

FIG. 2. Schematic diagram of our experiment setup for USD measurement demonstration [28]. Alice's first AMZI splits the signal pulse into two pulses, the strong one for phase stabilization, and the weak one for the quantum signal modulated by the intensity modulator (IM) to be either a decoy state or a signal state. The second AMZI encodes the BB84 states by a phase modulator (PM).Then a synchronization pulse is coupled with the signal pulses into a signal fiber and sent to Bob. At Eve's site, she utilizes a polarization controller and polarizer (Pol) to compensate for the polarization change, and a phase shifter (PS) to compensate for the phase drift. Then she uses the same AMZI setup as Alice's first one to interfere the quantum pulse with the strong phase-stabilization pulse modulated by IM. The interference result either indicates the identity of the quantum pulse (signal or decoy) or is inconclusive.

of the key. To our best knowledge, our work is the first application of USD with linear optics in quantum information, which opens a new avenue to fully linear-optics-based implementation of general quantum measurements as a powerful technique. Several aspects of our USD experiment renders the USD success probability suboptimal. Firstly, our proof-of-concept USD experiment is not an implementation of the optimal USD measurement. Secondly, losses in Eve's polarization controller, asymmetric Mach-Zehnder interferometers (AMZI) and the detector further reduce the intensity and hence the success probability. For future work, it is an interesting perspective topic to study the case where Eve knows partial information on the phases. A related question will be whether a fully randomized phase is necessary for Alice and Bob to guarantee the security.

* xma@tsinghua.edu.cn

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett., **67**, 661 (1991).

[3] D. Mayers, Journal of the ACM (JACM), **48**, 351 (2001).

[4] H.-K. Lo and H. F. Chau, Science, **283**, 2050 (1999).

[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. , **85**, 441 (2000).

[6] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput., **4**, 325 (2004).

[7] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett., **101**, 093601 (2008).

[8] T. Tsurumaru and K. Tamaki, Phys. Rev. A, **78**, 032302 (2008).

[9] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A, **74**, 022313 (2006).

[10] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput., **7**, 073 (2007).

[11] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A, **75**, 032314 (2007).

[12] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A, **78**, 042333 (2008).

[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature photonics, **4**, 686 (2010).

[14] F. Xu, B. Qi, and H.-K. Lo, New Journal of Physics, **12**, 113026 (2010).

[15] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New Journal of Physics, **13**, 073024 (2011).

[16] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett., **107**, 110501 (2011).

[17] D. Mayers and A. Yao, in *FOCS, 39th Annual Symposium on Foundations of Computer Science* (IEEE, Computer Society Press, Los Alamitos, 1998) p. 503.

[18] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett., **97**, 120405 (2006).

[19] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett., **108**, 130503 (2012).

[20] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A, **54**, 2651 (1996).

[21] H. Inamori, Algorithmica, **34**, 340 (2002).

[22] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, Q. Zhang, and J.-W. Pan, Arxiv preprint arXiv:1209.6178 (2012).

[23] A. Rubenok, J. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Arxiv preprint arXiv:1204.0738 (2012).

[24] T. da Silva, D. Vitoreti, G. Xavier, G. Temporão, and J. von der Weid, Arxiv preprint arXiv:1207.6345 (2012).

[25] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. , **85**, 1330 (2000).

[26] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. , **94**, 230504 (2005).

[27] H.-K. Lo and J. Preskill, Quantum Inf. Comput., **7**, 0431 (2007).

[28] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, arXiv preprint arXiv:1304.2541 (2013).

[29] Z. Yuan and A. Shields, Optics Express, **13**, 660 (2005).

[30] T. Chen, H. Liang, Y. Liu, W. Cai, L. Ju, W. Liu, J. Wang, H. Yin, K. Chen, Z. Chen, *et al.*, Optics Express, **17**, 6540 (2009).

[31] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, New Journal of Physics, **11**, 075001 (2009).