This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTQE.2014.2361796, IEEE Journal of Selected Topics in Quantum Electronics

Field Test of Measurement-Device-Independent Quantum Key Distribution

Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, Jian-Wei Pan

***Abstract*—A main type of obstacles of practical applications of quantum key distribution (QKD) network is various attacks on detection. Measurement-device-independent QKD (MDIQKD) protocol is immune to all these attacks and thus a strong candidate for network security. Recently, several proof-of-principle demonstrations of MDIQKD have been performed. Although novel, those experiments are implemented in the laboratory with secure key rates less than 0.1 bps. Besides, they need manual calibration frequently to maintain the system performance. These aspects render these demonstrations far from practicability. Thus, justification is extremely crucial for practical deployment into the field environment. Here, by developing an automatic feedback MDIQKD system operated at a high clock rate, we perform a field test via deployed fiber network of 30 km total length, achieving a 16.9 bps secure key rate. The result lays the foundation for a global quantum network which can shield from all the detection-side attacks.**

***Index Terms*—Field test, Measurement-Device-Independent Quantum Key Distribution, Automatic Feedback Systems.**

I. Introduction

QUANTUM key distribution (QKD) can in principle provide information-theoretical security based on quantum mechanics. It is the most practical application of the fast developing field of quantum information technology. After some early experimental demonstrations carried out in 1990s to verify the feasibility of QKD, in 2000s the QKD systems are successfully transformed from controlled laboratory environments to real-life implementations [1], [2], [3], to realize the practical value of QKD. Up till now, quite a few commercial QKD systems are available in the market [4] and are under rapid development.

Despite the progress considering either the experiment development or commercialization, practical QKD systems are suffering from various attacks that render the QKD systems insecure [5], [6], [7], [8], [9], [10], [11]. These attacks take advantage of the imperfections, especially the detection-side ones, rooted in the gap between the theoretical model and the practical QKD systems. Some of them are experimentally demonstrated [8], [9] based on these practical QKD systems. Although certain countermeasures are provided to close some specific side channels [12], [8], [13], there might still be some side channels which are hard to estimate and will cause potential threats. A practical QKD system that can close all the detection-side loopholes is still missing.

Recently, the newly proposed measurement-device-independent QKD (MDIQKD) [14] protocol, whose security does not rely on any assumption on the detection system, can defeat all the detection-side attacks. Many efforts have been made extensively on the experimental demonstrations of the MDIQKD protocol [15], [16], [17], [18]. These results they have achieved demonstrate the feasibility of MDIQKD, while they are far away from practicability. Generally, there are three basic criteria for a practical QKD system: stabilization under real-world environment, a moderate secure key rate, and an automatic operation.

Firstly, all previous demonstrations are taken in the laboratory without perturbation of the field environment. A field test [15] of the MDIQKD scheme has been attempted over an 18.6 km deployed fiber (9 dB transmission loss), but random modulated decoy state is not added in that experiment and thus secure key could not be generated. Secondly, the secure key rates in all previous experiments [15], [16], [17], [18] are limited, of which the highest is $0.12\ bps$ at 50 km transmission distance (10 dB transmission loss) [16]. Last but not least, all previous experiments need manual calibration frequently to maintain the system performance per 10 minutes. This is fatal for a practical application. A sufficiently good performance will involve many aspects, such as time, spectrum and polarization modes. This poses another challenge on implementing an automatic calibration system. It is wondered whether the MDIQKD system is suitable for a practical deployment or not.

II. Experimental Setup

In this work, we take the field test in three adjacent sites located in Hefei City, China. We adopt the running fiber network of Hefei Cable Television Broadband Network Corp Ltd due to the low dispersion, low attenuation of the optical fiber at the telecom wavelengths. As shown in Fig. 1, Alice

Y.-L. Tang, H.-L. Yin, Y. Liu, X. Jiang, J. Wang, J.-Y. Guan, D.-X. Yang, H. Liang, N. Zhou, T.-Y. Chen, Q. Zhang and J.-W. Pan are with Department of Modern Physics and National Laboratory for Physical Sciences at Microscale, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China, and also with CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China (e-mail: tychen@ustc.edu.cn; qiangzh@ustc.edu.cn).

S.-J. Chen, W.-J. Zhang, L. Zhang, L.-X. You and Z. Wang are with State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China.

Z. Zhang and X. Ma are with Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, 100084, China, and also with CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China.

Y.-L. Tang, H.-L. Yin and S-J. Chen contribute equally to this work.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTQE.2014.2361796, IEEE Journal of Selected Topics in Quantum Electronics

is placed in the site of Animation Industry Park in Hefei (AIP) $(N31°50'6'', E117°7'52'')$, Bob in the site of an office building(OB) $(N31°50'57'', E117°16'50'')$ and Charlie in the campus of University of Science and Technology of China (USTC) $(N31°50'8'', E117°15'47'')$. The total deployed fiber length is 30 km, with AIP-USTC link of 25 km (7.9 dB) and OB-USTC link of 5 km (1.3 dB). The signal laser pulses are transmitted through the two links. The auxiliary synchronization laser and the phase-stabilization laser in the feedback systems are multiplexed by the wavelength division multiplexer (WDM), and are transmitted through two additional fiber links.

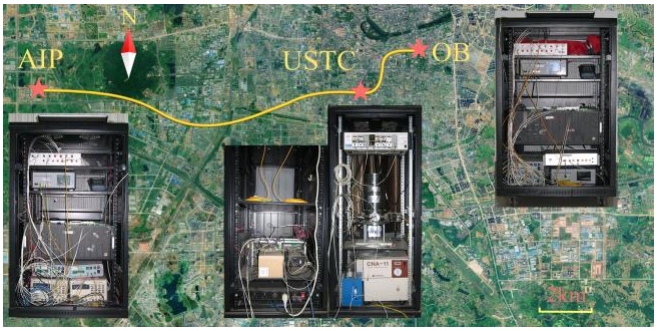

Fig. 1. Bird's-eye view of the field-environment MDIQKD. Alice is placed in Animation Industry Park in Hefei (AIP), Bob in an office building (OB), and Charlie in the University of Science and Technology of China (USTC). Alice (Bob) is on the west (east) side of Charlie. AIP-USTC link is 25 km (7.9 dB), and OB-USTC link is 5 km (1.3 dB).

In this field-environment test, we develop a decoy-state MDIQKD system, operated at a clock rate of 75 MHz and with a superconducting nanowire single photon detector (SNSPD) system of more than 40% detection efficiency [19]. Our experimental setup is illustrated in Fig. 2. To rule out the unambiguous-state-discrimination attack [20], we have utilized the internally modulated signal laser source which is intrinsically phase randomized. Besides, we employ the vacuum+weak decoy-state scheme [21], [22], [23] to defeat the PNS attack [24]. According to the decoy-state method, Alice (Bob) randomly sets the laser pulse intensity to be among three different values, $0, \nu = 0.07, \mu = 0.40$, as the intensities of vacuum state, weak decoy state and signal state. Their probabilities are set as 22%, 45% and 33%, respectively. We employ the time-bin phase-encoding scheme [14], [25], and utilize an asymmetrical Mach-Zehnder interferometer (AMZI), three AMs and one PM to encode qubits. AMZI splits the laser pulse into two time bins with a 6.5 ns time delay. If Z basis is used, the key bit is encoded in only one time bin by two AMs. If X basis is used, the key bit is encoded into two time bins' relative phase, 0 or π, by PM. The random basis and bit choices are of uniform probabilities. Another AM in the three AMs serves to normalize the average photon numbers in the two bases. The electrical variable optical attenuator (EVOA) is to attenuate the laser's output intensity to single photon level. We remark that two AMs are employed to not only increase the fidelity of time bin 0 or 1, but also improve the extinction ratio of the vacuum state intensity for the decoy-state method.

The laser pulses of Alice (Bob) go through the Alice-Charlie (Bob-Charlie) fiber link, to interfere with the ones sent by Bob (Alice). Charlie in the measurement station then takes a partial Bell-state measurement (BSM) implemented with an interference beam splitter (BS) and two SNSPDs at the two output arms of the BS. Then Charlie announces the BSM results to Alice and Bob for them to distill the secure key. Bell state $|\psi^-\rangle$ is post-selected when the two SNSPDs have a coincidence detection at two alternative time bins, i.e., SNSPD1 has a detection at time bin 0 (1) and simultaneously SNSPD2 has a detection at time bin 1 (0). The information of Alice and Bob are thus anti-correlated. Alice just needs to flip all the key bits to get correlated key stream with Bob's.

III. Automatical Feedback Systems

In order to achieve both a highly efficient coincidence count rate and a desirable error rate, we require a perfect and stable BSM, namely, the two independent laser pulses should keep indistinguishable after traveling through two separated fiber links, especially in the scenario of an unstable field environment. Thus, three aspects, time, spectrum and polarization, should be taken into account. To maintain the system performance and continuous operation, we develop several automatical feedback systems, serving for calibrating the time, spectrum and polarization modes of two independent laser pulses.

For the time synchronization of the whole system shown in Fig. 2(b), two synchronization laser (SynL) pulse trains are directly modulated by 500 KHz electric signals from a crystal oscillator circuit, and are sent from Charlie to Alice and Bob, respectively. Alice (Bob) utilizes a photoelectric detector (PD) to detect the SynL pulses. The output signals of the PD are used to regenerate a 75 MHz system clock as the time reference for the signal lasers and all amplitude and phase modulators. Thus the whole system becomes synchronized.

Then we precisely overlap the two signal pulses through a feedback control. Alice and Bob alternatively send her (his) signal laser pulses to Charlie. She (He) increases the intensity of the output signal laser pulses by adjusting the EVOA, so that Charlie can get enough detection events of SNSPD to calculate the average arriving time of Alice's (Bob's) signal laser pulses within several seconds. Based on the arriving time difference, Charlie adjusts the time delay between the two SynL pulses with a programmable delay chip.

There are several aspects that can influence the system's timing jitter: 1) the programmable delay chip that adjusts the time delay of the SynL's triggering signal. As in our experiment, the timing jitter increases with the time delay value. 2) the received power of the SynL pulses and the distinguishing voltage level of the electronics circuit with PD on it. They both should be optimized correspondingly at a certain transmission distance. 3) the SNSPD used in the BSM module. Besides the merits of high detection efficiency and low dark counts, the SNSPD has another advantage of low timing jitter within 100 ps that largely improves the overall timing jitter performance [26], [27]. 4) the time interval analyzer, which in our experiment is a high-performance time-to-digital converter (TDC). It records the time between the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTQE.2014.2361796, IEEE Journal of Selected Topics in Quantum Electronics

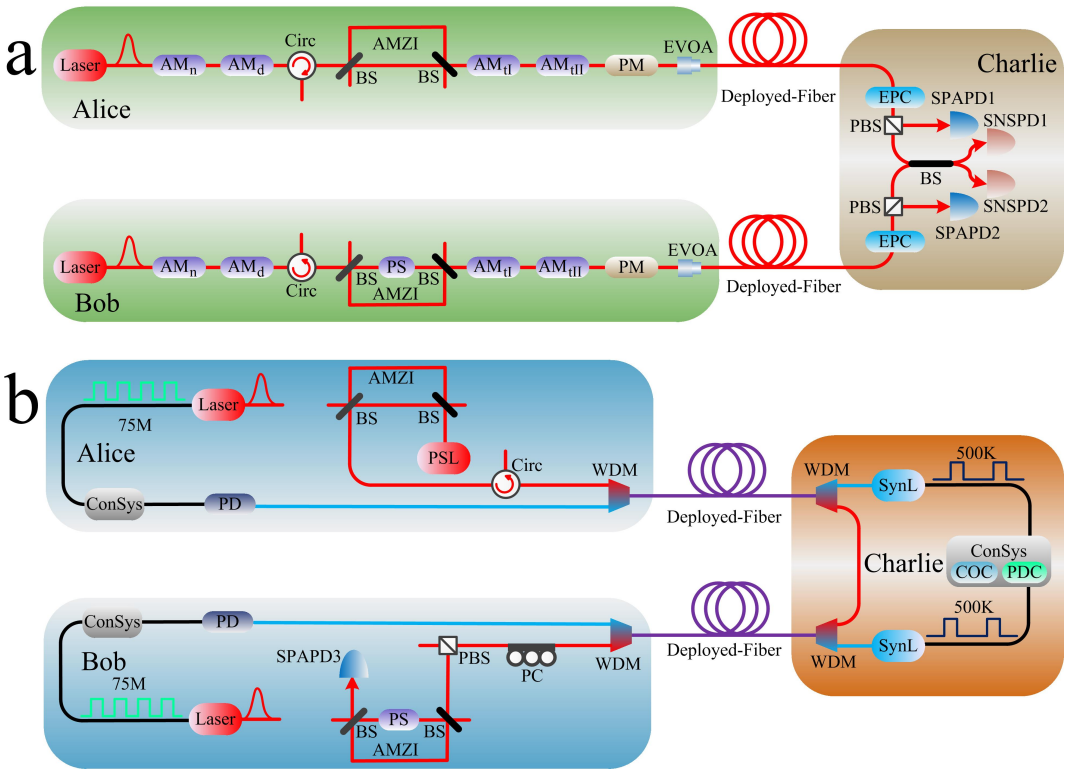

Fig. 2. (a) Diagram of our experimental setup. The signal laser source is phase randomized by internal modulation. AM_d is adopted to modulated Alice's (Bob's) signal laser pulses (1550 nm) into three decoy-state intensities. AMZI, AM_{tI}, AM_{tII}, AM_n and one PM are used to encode qubits. A circulator (Circ) is inserted before AMZI to separate the forward signal laser pulses from the backward PSL pulses. In the measurement station, Charlie receives the pulses sent through the deployed fiber links, stabilizes the input polarization by the polarization stabilization system (comprised of an EPC, a PBS and a SPAPD), and then takes a partial BSM (implemented with an interference BS and two SNSPDs). (b) Time calibration system and phase stabilization system. The time calibration system adopts two synchronization lasers (SynLs, 1570 nm), with the 500 kHz shared time reference generated from a crystal oscillator circuit (COC) and with the time delayed by a programmable delay chip (PDC) within the control system (ConSys). The SynLs are transmitted to Alice and Bob through two additional fiber links, respectively. The phase stabilization system utilizes a PSL with the same wavelength as the signal laser's. With the help of WDM, the Alice-Charlie fiber link and the Bob-Charlie fiber link are combined to be the channel transmitting the PSL pulses. PC: polarization controller, PS: phase shifter.

input detection event and its start signal. The start signal here is of the same clock rate with the SynL pulse. Since the timing jitter of TDC gets better with a smaller measurement range of recorded time, we set the SynL clock rate to be 500 kHz in our setup. Thus, considering all the aspects $1) \sim 5)$, as well as that of the time calibration system, we can confirm a good pulse overlap of the time mode.

For the spectrum mode, we firstly select two nearly identical laser diodes as Alice's and Bob's laser sources, considering the aspects of both the same full width at half maximum (FWHM) wavelength and the same central wavelength. Then, we develop a temperature controlled circuit in the laser to automatically stabilize the wavelength. At last, to calibrate the wavelength precisely, we utilize an optical spectrum analyzer (OSA) (YOKOGAWA AQ6370B) to measure the central wavelengths of Alice's and Bob's lasers alternatively. The precision for central wavelength measurement is less than 1 pm, which is decided by the sampling interval and repeatability of the OSA [28] if one cares relative wavelength difference of two lasers more than the absolute wavelength value. The temperatures are readjusted through temperature controlled circuits based on the wavelength difference. The temperature controlling precision is 0.005 degree centigrade, and the wavelength controlling precision is about 0.5 pm. Then the difference between Alice's and Bob's spectrum modes can be controlled to be smaller than the spectrum span of the laser pulses, in our case, 4 pm (FWHM) measured by the Fabry-Perot (FP) interference method.

For the polarization mode, we insert an electric polarization controller (EPC) and a polarization beam splitter (PBS) before the interference BS, and connect the transmission port of PBS with the BS. The reflection port of the PBS is monitored by an InGaAs/InP single-photon avalanche photodiode (SPAPD), whose count rate is used as the feedback signal to control the EPC, to guarantee that the maximum amount of laser power is transmitted through the PBS. Using this polarization stabilization system, we can control and eliminate the polarization change to an acceptable low level.

For the phase-encoding scheme of MDIQKD, an important task is to make sure Alice and Bob use the same phase reference frame to avoid the X-basis misalignment. The phase reference frame, namely the relative phase between AMZI's two arms, may fluctuate with temperature and stress. Thus, we firstly put the AMZIs in a thermal container to isolate it from the temperature and stress perturbation. Besides, we adopt a phase stabilization system [16], [29] to maintain the phase

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTQE.2014.2361796, IEEE Journal of Selected Topics in Quantum Electronics

reference frames of Alice's and Bob's AMZIs, as shown in Fig. 2(b). We employ a phase-stabilization laser (PSL) with the same wavelength as the signal laser's. The PSL pulses are sent through Alice's and Bob's AMZIs connected by an auxiliary fiber link, and are monitored by another InGaAs/InP SPAPD at an output of Bob's AMZI. The phase difference is then calibrated by a phase shifter inside Bob's AMZI. Note that the auxiliary fiber link between Alice and Bob is comprised of the auxiliary Alice-Charlie link and Bob-Charlie link, and the PSL pulses are multiplexed with SynL pulses by WDM.

All the aforementioned feedback systems contribute to a good interference and a minimal basis misalignment, and the automatic calibration procedure can largely improve the time utilization efficiency. While the polarization and phase stabilization systems are operated in real time, the time and spectrum calibration systems need to operate in a calibration procedure alternative with the QKD process. We switch the QKD process to calibration procedure every half an hour.

TABLE I
LIST OF THE TOTAL COINCIDENCE EVENT COUNTS OF BELL STATE $|\psi^-\rangle$ IN THE 30 KM FIELD TEST FOR 18.2 HOURS.

	μ_a/μ_b	0	ν	μ
$M_z^{\mu_a\mu_b}$	0	0.00×10^0	1.93×10^2	2.64×10^3
	ν	3.60×10^1	8.12×10^5	3.36×10^6
	μ	1.46×10^2	3.49×10^6	1.35×10^7
$M_x^{\mu_a\mu_b}$	0	0.00×10^0	8.58×10^5	2.03×10^7
	ν	4.30×10^4	2.72×10^6	4.42×10^7
	μ	9.94×10^5	6.55×10^6	4.48×10^7

TABLE II
LIST OF THE QBERS IN THE 30 KM FIELD TEST FOR 18.2 HOURS.

	μ_a/μ_b	0	ν	μ
$E_z^{\mu_a\mu_b}$	0	0.00%	52.33%	49.26%
	ν	52.78%	0.04%	0.10%
	μ	47.26%	0.01%	0.02%
$E_x^{\mu_a\mu_b}$	0	0.00%	51.49%	49.90%
	ν	52.10%	38.12%	46.85%
	μ	49.92%	27.72%	36.82%

IV. EXPERIMENTAL RESULTS AND SECURE KEY CALCULATION

Using this MDIQKD system integrated with the feedback systems, we has accumulated the raw data for 18.2 hours. During this period, the feedback systems work effectively. Compared with all the previous laboratory experiments, the field test faces much more severe environment turbulence. Especially, the polarization mode dispersion of the deployed fiber may cause the polarization overlap of the two independent lasers fluctuating. With the help of the aforementioned polarization stabilization system, we have compensated for the polarization change and achieved a fluctuation less than 3%. Besides, the field environment will also change the arriving time of the signals. The time calibration system works to monitor the time shift and then compensate it effectively. The achieved timing calibration precision is below 20 ps, which is much smaller than the 2.5 ns pulse width of the signal laser.

Furthermore, monitored by the optical spectrum analyzer, the wavelength difference between Alice's and Bob's signal laser sources can be maintained within 1 pm for a few hours. It indicates that the temperature controlled circuit built in the signal laser source can control the wavelength of the laser precisely and stabilize it effectively. Thanks to the feedback procedure with these aforementioned feedback systems, as well as the temperature controlled circuit, this MDIQKD system can run continuously for a long time without manual efforts.

We adopt in the BSM a time window of 1.5 ns, 60% of the pulse width of 2.5 ns. The details for the experimental results, including the coincidence event counts M and quantum bit error rates (QBERs) E, can be found in Table I and II. Here, $M^{\mu_a\mu_b}$ ($E^{\mu_a\mu_b}$) is the overall coincidence event count (error rate) given that Alice sends out her state with an intensity of μ_a and Bob sends out his state with an intensity of μ_b. In the Z basis, the results show both a high-efficient coincidence count rate and a desirable low error rate (the QBERs are less than 0.1% when the intensities are neither vacuum). In the X basis, note that $M_x^{\mu\mu} \approx M_x^{\nu\mu} > M_x^{\mu\nu}$, because when Alice's and Bob's pulses interfere in Charlie's site with quite different intensities, the coincidence event count is mainly determined by the larger intensity. Since the transmission loss of Alice-Charlie link is about 6 dB higher than that of the Bob-Charlie link, Alice's laser pulses contributes to the coincidence event count much less than Bob's. Besides, among all the QBERs in the X basis (when the intensities are neither vacuum), the minimal error rate is $E_x^{\mu\nu}$, not $E_x^{\mu\mu}$, since the QBER in the X basis gets better when the two received pulses interfere with each other with less different intensities.

The final key is assumed to be extracted from the case where both Alice and Bob encode the states in the Z basis using signal states in the decoy-state method. The final secure key length is given by [14]:

$$\begin{aligned} K^{\mu\mu} &\geq M_{11}^{\mu\mu}[1-H(e_{11}^{p\mu\mu})] - K_{ec}^{\mu\mu}, \\ K_{ec}^{\mu\mu} &= M^{\mu\mu} f H(E^{\mu\mu}), \end{aligned} \tag{1}$$

Here, $M_{11}^{\mu\mu}$ and $e_{11}^{p\mu\mu}$, the coincidence event counts and phase error rate when both sources generate single-photon states within signal states, can be estimated through the decoy-state method. $K_{ec}^{\mu\mu}$ denotes the number of the secure bits cost in error correction, f is the inefficiency of error correction, and $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

The decoy state method [21], [22], [23], which has been widely used in conventional QKD protocols such as BB84, can also be applied in the MDIQKD scheme. In this protocol, the pulse Alice (Bob) prepared can be considered as Fock state. Therefore, the decoy state method can be used to estimate the gain and the QBER of the single-photon components and get the final key generation rate. In more details, the analytical key rate method [30] and finite-key analysis method [31], [32] can also be applied in security analysis and parameter estimation. In our experiment, we follow the same postprocessing detailed in [29]. We use the decoy-state method [30] and make the finite-key analysis with the Chernoff bound [32] to estimate $M_{11}^{\mu\mu}$ and $e_{11}^{p\mu\mu}$. The main results of the postprocessing, as

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSTQE.2014.2361796, IEEE Journal of Selected Topics in Quantum Electronics

shown in Fig. 3, are calculated as follows:

1) From the experimental data, we can directly obtain $K_{ec}^{\mu\mu} = 4.7485 \times 10^4$. This ratio of error correction consumption in the raw key is thus 0.35%.
2) We can get the lower bound of $M_{11}^{\mu\mu} = 6.0671 \times 10^6$ through the decoy-state method and finite-key analysis. The ratio of multi-photon component ($M^{\mu\mu} - M_{11}^{\mu\mu} = 7.4528 \times 10^6$) is thus 55.12%.
3) Using the random sampling model [33], we can get the upper bound of $e_{11}^{p\mu\mu} = 24.93\%$. Within it, the base line error is 21.68% which is mainly caused by the imperfection of the modulating signals of the control system. The remaining error, 3.25%, is caused by the finite-key effect. Thus the ratio of the phase error correction part ($M_{11}^{\mu\mu} H(e_{11}^{p\mu\mu}) = 4.9153 \times 10^6$) is 36.36%.
4) To sum up, the final key length is 1.1046×10^6, which is 8.17% of $M^{\mu\mu}$.

Dividing the final key length by the total time in second, we get the secure key rate of 16.9 bps.

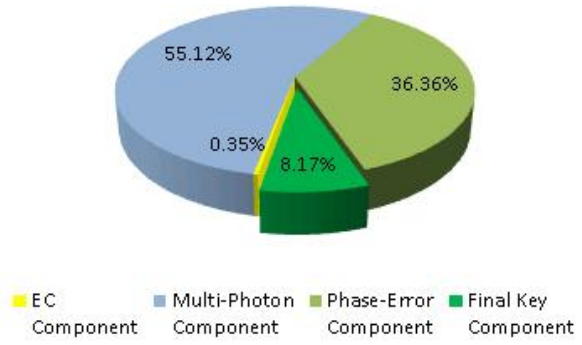

Fig. 3. The main results of postprocessing through decoy-state method and the finite-key analysis. Each part denotes its corresponding ratio in the raw key. The final key ratio is 8.17%, and the secure key rate is 16.9 bps.

V. Conclusion

The field test demonstrates the feasibility and robustness of the MDIQKD protocol in an unstable environment. In this test, we have generated a final key rate of 16.9 bps, which is at least two orders of magnitude higher than the previous results of MDIQKD demonstrations.

Besides, the goal of regular QKD protocols and the MDIQKD protocol is not restricted to point-to-point communication, but is to realize a global quantum network [34]. The MDIQKD protocol has an intrinsic property which is desirable for constructing quantum network with the star-type structure, since the detection system placed in Charlie's site in the middle node can be shared by all the transmitters. Furthermore, when more transmitters are added in the network, only laser sources and modulators are needed which are much cheaper and smaller than the detection system. While the existing quantum networks are suffering from various attacks, especially the detection-side ones, the MDIQKD protocol will perfectly shield the QKD network from these existing and potential detection-side attacks. We can expect that the MDIQKD network may be built within reach of current technology in the near future.

We remark that there is still much room for us to make MDIQKD system more practicable. Firstly, we can increase the system clock rate by further minimizing the overall timing jitter. Secondly, with the development of the SNSPD technology, the detection efficiency can be further improved [35]. Besides, the dark count rate may be effectively reduced to sub-Hertz [19]. Last but not least, with the decoy-state parameters and the basis choice optimized [36], we can expect a faster key rate generation to enable some practical applications. We note that this field test utilizes the system based on which we have implemented a long-distance MDIQKD over 200 km [29].

Acknowledgment

The authors would like to thank Xiaoming Xie and Mianheng Jiang for enlightening discussions. This work has been supported by the National Fundamental Research Program (under Grant No. 2011CB921300, 2013CB336800 and 2011CBA00300), the National Natural Science Foundation of China, the Chinese Academy of Science, the Quantum Communication Technology Co., Ltd., Anhui, and the Shandong Institute of Quantum Science & Technology Co., Ltd.

References

[1] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Opt. Express*, vol. 17, no. 8, pp. 6540–6549, 2009.

[2] 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, "The secoqc quantum key distribution network in vienna," *New J. Phys.*, vol. 11, no. 7, p. 075001, 2009.

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, L. M, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and Z. A, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[4] "For example www.quantum-info.com, www.magiqtech.com, www.idquantique.com, www.quintessencelabs.com, and www.sequrenet.com, all visited 1th august 2014."

[5] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022313, Aug 2006.

[6] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 75, p. 032314, Mar 2007.

[7] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *Quantum Inf. Comput.*, vol. 7, no. 1, pp. 073–082, 2007.

[8] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, p. 042333, Oct 2008.

[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. Photon.*, vol. 4, no. 10, pp. 686–689, 2010.

[10] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New J. Phys.*, vol. 13, no. 7, p. 073024, 2011.

[11] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, "Laser Damage Helps the Eavesdropper in Quantum Cryptography," *Phys. Rev. Lett.*, vol. 112, no. 7, FEB 18 2014.

[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[13] Z. Yuan, J. Dynes, and A. Shields, "Avoiding the blinding attack in qkd," *Nat. Photon.*, vol. 4, no. 12, pp. 800–801, 2010.

[14] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012.

[15] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, p. 130501, Sep 2013.

[16] 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, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, p. 130502, Sep 2013.

[17] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A*, vol. 88, p. 052303, Nov 2013.

[18] 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," *Phys. Rev. Lett.*, vol. 112, p. 190503, May 2014.

[19] X. Yang, H. Li, W. Zhang, L. You, L. Zhang, X. Liu, and Z. Wang, "Superconducting nanowire single photon detector with on-chip bandpass filter," *Opt. Express*, vol. 22, no. 13, pp. 210–214, 2014.

[20] 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, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, p. 022308, Aug 2013.

[21] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, Aug 2003.

[22] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, Jun 2005.

[23] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, p. 230503, Jun 2005.

[24] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, Aug 2000.

[25] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 062319, Dec 2012.

[26] S. Chen, D. Liu, W. Zhang, L. You, Y. He, W. Zhang, X. Yang, G. Wu, M. Ren, H. Zeng, Z. Wang, X. Xie, and M. Jiang, "Time-of-flight laser ranging and imaging at 1550 nm using low-jitter superconducting nanowire single-photon detection system," *Applied Optics*, vol. 52, no. 14, p. 3241, 2013.

[27] L. X. You, X. Y. Yang, Y. H. He, W. X. Zhang, D. K. Liu, W. J. Zhang, L. Zhang, L. Zhang, X. Y. Liu, S. J. Chen, Z. Wang, and X. M. Xie, "Jitter analysis of a superconducting nanowire single photon detector," *AIP Advances*, vol. 3, no. 7, p. 072135, 2013.

[28] http://support.us.yokogawa.com/downloads/TMI/COMM/AQ6370B/IM735302-01E_010.pdf.

[29] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yong, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over 200 km," *arXiv:1407.8012*.

[30] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Practical aspects of measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 15, no. 11, p. 113007, 2013.

[31] X. Ma, C.-H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 052305, Nov 2012.

[32] 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," *Nat. Commun.*, vol. 5, 2014.

[33] C.-H. F. Fung, X. Ma, and H. Chau, "Practical issues in quantum-key-distribution postprocessing," *Phys. Rev. A*, vol. 81, no. 1, p. 012318, 2010.

[34] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, pp. 441–442, 2014.

[35] F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin *et al.*, "Detecting single infrared photons with 93% system efficiency," *Nat. Photon.*, vol. 7, no. 3, pp. 210–214, 2013.

[36] F. Xu, H. Xu, and H.-K. Lo, "Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution," *Physical Review A*, vol. 89, no. 5, p. 052333, May 2014.

Yan-Lin Tang received her B.S. degree in Physics from University of Science and Technology of China (USTC), Hefei, China, in 2009. She is currently a Ph.D student majoring in Physics of Quantum Information, National Laboratory for Physical Sciences at Microscale (NLPSM), USTC.

Hua-Lei Yin received his B.S. degree in Physics from USTC, Hefei, China, in 2011. He is currently a Ph.D student majoring in Physics of Quantum Information, NLPSM, USTC.

Si-Jing Chen received his B.S. degree in Huazhong University of Science & Technology, Wuhan, China, in 2008. Then he received his doctors degree in Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Beijing, China, in 2013. He is currently a staff in Shanghai Center for Superconductivity, Shanghai Institute of Microsystem and information technology.

Yang Liu received his B.S. and M.S. degrees in Physics from USTC, Hefei, China, in 2007 and 2012, respectively. He is currently a Postdoctoral Researcher in NLPSM, USTC.

Wei-Jun Zhang received his Ph.D. degree in Condensed Matter Physics from the Institute of Physics, Chinese Academy of Sciences (CAS), Beijing, China, in 2012. He is currently an Associate Researcher with the SNSPD Group, State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology (SIMIT), CAS, Shanghai. His current research interests include electrical and magnetic properties of nanostructures, superconducting devices and physics, and single-photon detectors.

Xiao Jiang received his B.S. and M.S. degrees in Physics from USTC, Hefei, China, in 2004 and 2009, respectively. He is currently an Associate Researcher in NLPSM, USTC.

Lu Zhang received her B.S. degree from Yangtze University in July 2008, and M.S. degree in Condensed Matter Physics from Soochow University, in 2011. Her current research interest lies in the deposition and characterization of thin films.

Jian Wang received his B.S. and Ph.D degrees in Physical Electronics from USTC, Hefei, China, in 1998 and 2003, respectively. From 2003 to 2005, he was a Postdoctoral Researcher with Department of Modern Physics in USTC. Since 2005, he has been an associate professor with Department of Modern Physics in USTC. His research interests include physical electronics, software system design, information processing and quantum cryptography.

Li-Xing You received his B.S., M.S., and Ph.D. degrees in Physics from Nanjing University, Nanjing, China, in 1997, 2001, and 2003, respectively. From 2003 to 2005, he worked as a Postdoctoral Researcher in the Department of Microtechnology and Nanoscience (MC2), Chalmers University of Technology, Göteborg, Sweden. Later on, from 2005 to 2006, he worked as a Postdoctoral Researcher with the Condensed Matter Physics and Devices Group, University of Twente, Twente, Netherlands. Since 2006, he has been a Guest Researcher with the Electromagnetics Division, National Institute of Standards and Technology, Boulder, CO. Since 2007, he has been a Research Professor with Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Beijing, China. His research focuses on superconductive electronics, including micro/nano superconductive devices and high-frequency applications.

Jian-Yu Guan received his B.S. degree in Physics from USTC, Hefei, China, in 2011. He is currently a Ph.D student majoring in Physics of Quantum Information, NLPSM, USTC.

Dong-Xu Yang received his B.S. degree in Physics from USTC, Hefei, China, in 2012. He is currently a Ph.D student majoring in Physical Electronics, Department of Modern Physics, USTC.

Zhen Wang received his Ph.D. degree in Electrical Engineering from Nagaoka University of Technology, Nagaoka, Japan, in 1991. From 1991 to 2013, he worked at the National Institute of Information and Communications Technology (NICT), Japan. He is currently a Research Professor at the Shanghai Institute of Microsystem and Information Technology (SIMIT), Chinese Academy of Science, China. He is Fellow of NICT. His research interests focus on superconducting electronics, including superconducting devices and physics, superconducting SIS terahertz mixers, and photon detectors.

Hao Liang received his B.S. and Ph.D degrees in Physical Electronics from USTC, Hefei, China, in 1992 and 1997, respectively. From 1992 to 2004, he was a lecturer with the Department of Modern Physics in USTC. Since 2004, he has been an Associate Professor with Department of Modern Physics in USTC. His research focuses on nuclear electronics, including data acquisition, pulse amplitude, time measurement and digital pulse process.

Zhen Zhang received his B.S. degree in Computer Science from Tsinghua University, Beijing, China, in 2012. He is currently a Ph.D student in the Institute for Interdisciplinary Information Sciences, Tsinghua University.

Nan Zhou received the B.S. degree in Applied Physics in Anhui University, Hefei, China, in 2011. He is currently studying for the Ph.D. degree in USTC, Hefei, China.

Xiongfeng Ma received his B.S. degree in Physics from Tsinghua University, Beijing, China, in 2003, and received his Ph.D degree in Physics from University of Toronto, Canada, in 2008. From 2008 to 2010, he was a Postdoctoral Researcher with University of Toronto in Canada, and also a Visiting Scholar with University of Leeds in England. Since 2012, he has been an Tenure-Track Associate Professor in the Institute for Interdisciplinary Information Sciences, Tsinghua University. His research interests include the quantum cryptography, the quantum random number generator, as well as the quantum repeater.

Teng-Yun Chen received his B.S. degree in Physical Electronics from USTC, Hefei, China, in 2001, and received his Ph.D degree in Applied Physics from USTC, Hefei, China, in 2006. Now, he is an Associate Professor in NLPSM, USTC, China. His research focuses on quantum cryptography, quantum key distribution systems and the corresponding techniques.

Qiang Zhang received his B.S. and M.S. degrees in Physics from USTC, Hefei, China, in 2001 and 2006, respectively. From 2006 to 2008, he was a Postdoctoral Researcher in the Department of Applied Physics in the University of Stanford, America. From 2008 to 2011, he worked as a researcher in the National Institute of Information and Communications Technology (NICT), Japan. Since 2011, he has been a professor with NLPSM, USTC, Shanghai Branch, China. His research focuses on quantum physics and quantum information, including the quantum cryptography, the up-conversion single-photon detection devices and their various applications.

Jian-Wei Pan received his B.S. and M.S. degrees in Physics from USTC, Hefei, China, in 1992 and 1995, respectively. He received his Ph.D degree from University of Vienna, Austria, in 1999.

From 1999 to 2000, he was a Postdoctoral Researcher in University of Vienna, Austria. Since 2001, he has been a professor in USTC. From 2003 to 2008, he was a guest professor in University of Heidelberg. Since 2009, he has been awarded as the honorary professor. Now, Prof. Pan is also the director of Division of Quantum Computation and Quantum Information at NLPSM. His research interests include the theory and experiment on quantum communication and quantum computation, etc.