# Experimental Decoy State Quantum Key Distribution Over 15km

Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, Li Qian

Center for Quantum Information and Quantum Control
Department of Physics and Department of Electrical & Computer Engineering
University of Toronto, Toronto, Ontario, Canada

March 25, 2005

**Abstract**

Decoy state protocols have recently been proposed as an innovative approach to improve dramatically the performance of quantum key distribution systems. Here, we present the first experimental demonstration of decoy state quantum key distribution, over 15km of Telecom fibers.

## 1 Introduction

After the proposal of BB84 protocol[1], quantum key distribution (QKD) has aroused great interest among both scientists and engineers. Quantum key distribution provides unconditional security guaranteed by the fundamental laws of quantum physics. Experimental quantum key distribution was demonstrated successfully for the first time in 1989[2] at a distance of 32cm. More than fifteen years have now passed and people have extended this distance to 150km of Telecom fibers[3, 4]. Commercial quantum key distributions are currently on the market [5, 6].

The most important question in quantum key distribution is its security. This fact has finally been proven in a number of important papers [7, 8]. See also [9]. Unfortunately, for real-life experimental set-ups, which are mainly based on faint laser pulses, the occasional production of multi-photons and channel loss make it possible for sophisticated eavesdroppers to launch various subtle eavesdropping attacks including the PNS (photon number splitting) attack. Although those attacks may appear to be beyond current technology, the first rule in cryptography is: never under-estimate the determination and ingenuity of your opponents in breaking your codes. This is particularly so because institutions (such as IBM, Los Alamos, NEC, NTT, Toshiba and NSA) have spent hundreds of millions of dollars on the subject and yet much experimental work on quantum eavesdropping attacks has so far been classified. The security of practical QKD systems has been proven in [10], following [11]. Unfortunately, with the method in GLLP [10], QKD is only proven to be secure at very limited key generation rates and distances. Most of the previous experiments do not appear to satisfy the strict security analysis demanded in [10]. This is because many of them take an ad hoc value of 0.1 for the average photon number of the signal and few consider the most general eavesdropping attack allowed by quantum mechanics.

A key question is: How can one increase the key generation rates and distances of unconditionally secure QKD? A brute force solution to the problem is to develop single photon sources, which is a subject of much recent interest [12]. However, such a brute force approach clearly takes a lot of experimental research efforts. It came as a big surprise that a simple solution—the decoy state method—to the problem actually exists. Such a simple solution is based on better theory, rather than better experiments. The decoy state method allows us to kill two birds with a single stone—a) to achieve unconditional security based on quantum mechanics and b) to improve dramatically the performance of QKD systems. As clearly demonstrated in the present paper, in contrast to single photon sources, decoy state QKD can be implemented with only current technology.

The decoy method is firstly proposed by Hwang[13], and made rigorous by us[14, 15] and also Wang[16]. Decoy state QKD has attracted much recent interest. See also [17]. Let us recapitulate the basic ideas of decoy state QKD. We assume that Alice can prepare phase-randomized coherent states and can change the intensity of each signal independently and randomly. The weak coherent state emitted by Alice can be denoted by $|\sqrt{\mu}e^{i\theta}>$. If the phase $\theta$ is totally randomized, the signal state becomes a mixture of photon number eigenstates and the number of photons per signal follows a Poisson distribution. That is, the probability of emitting $n$ photons is $p_n = e^{-\mu}\mu^n/n!$. In addition to the signal state with average photon number $\mu$, in the decoy state idea, one introduces some "decoy" states with some other average photon numbers $\nu_i$ and mixes up signal states with decoy states randomly. Since one assumes all characteristics (except photon number distribution) of the signal state and the decoy state are the same, Eve's eavesdropping attack can depend on the actual photon number in each state, but nothing else. Computing the number of detection events and error rates of each state, one can effectively detect eavesdropping attacks and therefore achieve a rather high unconditionally secure key generation rate.

In [14], combining the idea of security proofs using the entanglement distillation approach in GLLP[10] with decoy method, we gave a formula for the key generation rate

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\} \tag{1}$$

where $q$ depends on the protocol, the subscript $\mu$ is the average photon number per signal in signal states, $Q_\mu$ is the gain of signal states, $E_\mu$ is the quantum bit error rate (QBER) of signal states, $Q_1$ is the gain of the single photon states in signal states, $e_1$ is the error rate of single photon states. $f(x)$ is the bi-directional error correction rate (see, for example, [18]), and $H_2(x)$ is binary Shannon information function:

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$$

Our implementation is based on BB84[1] protocol. Among total $N$ pulses sent in experiment, $N_S$ pulses are used as signal states. Therefore the factor $q$ is given by $q = \frac{1}{2}N_S/N$.

$Q_\mu$ and $E_\mu$ can be measured directly from experiments. In [15], we have proposed a practical protocol with only one decoy state with average photon number $\nu$. Such a protocol is relatively simple to implement. The gain of weak decoy state $Q_\nu$ and its error rate $E_\nu$ could also be acquired directly from experiments. Considering statistical fluctuations, the lower bounds of $Y_1$[1] and $Q_1$,

[1] $Y_1$ is the yield of a single photon state. That is to say, the conditional probability that Bob will see a detection event, given that a single photon is emitted by Alice.

and the upper bound of $e_1$ are given by [15]

$$\begin{aligned} Y_1^L &= \frac{\mu}{\mu\nu-\nu^2}(Q_\nu^L e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2-\nu^2}{e_0\mu^2}) \\ Q_1^L &= \frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}(Q_\nu^L e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2-\nu^2}{e_0\mu^2}) \\ e_1^U &= \frac{E_\mu Q_\mu e^\mu}{\mu Y_1^L}, \end{aligned} \tag{2}$$

in which

$$Q_\nu^L = Q_\nu(1 - \frac{u_\alpha}{\sqrt{N_W Q_\nu}}), \tag{3}$$

and therefore the lower bound of key generation rate is

$$R^L = q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L[1 - H_2(e_1^U)]\} \tag{4}$$

In the later calculations, we give a very conservative estimate with 10 standard deviations (i.e., $u_\alpha = 10$), which promises a confidence interval for statistical fluctuations of $1 - 1.5 \times 10^{-23}$.

## 2 Our Experiment

In this paper, we present the first experimental implementation of decoy state QKD. Before we describe our experiment, we would like to point out that the decoy protocol is much easier to implement with a uni-directional QKD system as [4], [19], and [20], because one can modulate the intensity of each laser pulse inside the laser directly. However, we emphasize that the same modulation strategy fails miserably for a bi-directional ("Plug and Play") QKD system where a strong pulse is sent from Bob to Alice, who attenuates it to single photon level and modulates it before sending it back to Bob. This is because, if one were to modulate the intensity inside Bob's laser in a bi-directional system, the eavesdropper can detect the intensities of *strong* laser pulses from Bob to Alice using standard powermeters, thus breaking security.

Unfortunately, existing commercial QKD systems are bi-directional. To show conceptually how simple it is to apply the decoy state idea to a commercial QKD system, we chose ID-500 commercial Quantum Key Distribution system manufactured by id Quantique[6]. The intrinsic parameters of this "Plug & Play" QKD system is listed in Table 1.

We remark that, strictly speaking, existing security proofs [10] for imperfect devices apply only to a polarization-based QKD system. In what follows, we will take the assumption that those existing security proofs will carry over directly to a bi-directional QKD system. This assumption is commonly made in the community and appears to be necessary at the moment, if we are to discuss the security of commercial bi-directional QKD system. Further investigations will explore the validity of this assumption.

Another assumption that we will make is that the phase of the laser is indeed random. Therefore, it is valid to consider the signal or decoy state as classical mixtures of photon number eigenstates, rather than their superpositions. As noted in a recent paper [21], this assumption is crucial in some parameter regions.

| $\lambda$ | $e_{detector}$ | $Y_0$ | f |
|---|---|---|---|
| 1551.7nm | $\leq 1\%$ | $\leq 5 \times 10^{-5}$ | 5MHz |

Table 1: Intrinsic parameters of ID-500 commercial QKD system as given in its specifications data sheet.

Modulo the above two assumptions, our experiment satisfies the requirement of unconditional security [15] against the most general attack allowed by quantum mechanics. It also gives a rather high key generation rate.

The prototype of this QKD system is described in section 2 of [22]. Here we describe it briefly: a frame of $N_P$ pulses (in our experiment, $N_P = 624$) is generated from Bob and sent to Alice. Within a frame, the time interval between signals is 200ns. The next frame will not be generated until the whole frame has returned to Bob. The long delay line inside Jr. Alice promises that the incoming signal and returning signal will not overlap in the channel between Bob and Jr. Alice so as to avoid Rayleigh Scattering. It will take roughly 0.4ms to complete a frame for 15km fiber. Considering time spent to load data from computer, the efficiency of our QKD system is about 2.3s per megabit.

To implement the one decoy state protocol[15], we have to attenuate each signal to the intensity of either signal state or decoy state randomly. In our implementation, the attenuation is done by placing a VOA (variable optical attenuator) in Alice's side. Specifically, our QKD system requires the polarizations of the two pulses from the same signal to be orthogonal. Therefore the VOA must be polarization independent so as to attenuate the two pulses equally. The VOA utilized in our experiment to attenuate signals dynamically is Brimrose AMM-100-20-25-1550-2FP Acousto-Optic Modulator (AOM), whose maximum attenuation is -50dB and maximum working frequency is 20MHz. It is driven by Brimrose FFA-100-B1/B2(20)-F0.8 fixed frequency RF Driver whose output frequency is 100MHz. We call this AOM the "Decoy AOM".

The transmittance of the AOM is determined by the modulation voltage (0V$\sim$1V) applied on its driver, which is controlled by Agilent 88250A Function/Arbitary Waveform Generator at 5MHz. The output of generator is triggered by the synchronization signal from the classical detector in Alice's side. We call this functional generator the "Decoy Generator".

The Decoy AOM, although polarization-independent, introduces a frequency shift of the laser due to Doppler effect from its intrinsic 100MHz acoustic frequency. This frequency shift causes a significant phase shift in unbalanced Mach-Zehnder interferometer in Bob's side when the signal is going back, increasing the QBER to around 90%. To compensate this frequency shift, we place a Brimrose AMM-55-8-70-1550-2FP AOM in front of the Decoy AOM. This AOM is called "Compensating AOM".

The Compensating AOM is driven by another Agilent 88250A Function/Arbitary Waveform Generator instead of its own 55MHz FFA-55-B2-F0.24 fixed frequency RF driver. Since the frequency shift introduced by AOM is only dependent on the acoustic frequency, we can change the phase shift in Bob's Mach-Zehnder interferometer to $2n\pi$ by precisely adjusting the driven frequency of this AOM. Minimum QBER is achieved when the frequency of the functional generator is set to 56.60MHz, at which the phase shift in Bob's Mach-Zehnder interferometer is $20\pi$. This

| $e_{detector}$ | $Y_0$ | $\eta$ |
|---|---|---|
| $8.269 \times 10^{-3}$ | $3.40 \times 10^{-5}$ | $1.75 \times 10^{-2}$ |

| Parameter | Optimal Value | Our Value |
|---|---|---|
| $\mu$ | 0.80 | 0.80 |
| $\nu$ | 0.12 | 0.12 |

Table 2: Comparison of optimal values and the values we used in our experiment for pre-set parameters. The optimal values are given by numerical simulation using MatLab according to the intrinsic parameters of our QKD system.

functional generator is called "Compensating Generator".

Here we would like to emphasize that if we had a variable frequency driver for Decoy AOM (which is also available in Brimrose Corp.), the Compensating AOM and Compensating Generator would not be necessary any more, and our set-up would be even simpler.

Prior to the experiment, we have measured $Y_0$, $e_{detector}$ and the total transmittance $\eta$. According to these data and the fact that the data size in our experiment is 100M bits, through numerical simulation we could find out the optimal parameters. We set the parameters in our experiment to their optimal values, as shown in Table 2.

According to the percentages of signal states and decoy states, the exact distribution of the states is given by id Quantique Quantis-PCI-1 Quantum Random Number Generator (QRNG), which promised the choice of signal states and decoy states within each frame is truly random: we generated a sequence of 624 integers $\{1 \leq n_i \leq 100\}$, if $n_i \leq 88$, the $i$ th position will be assigned as signal state, otherwise decoy state. Among total 624 positions, 67 positions are assigned as decoy states, while the rest are assigned as signal states. We call this particular choice of a sequence of 624 pulses within each frame the "Decoy Profile". This Decoy Profile is generated before the experiment and loaded from computer to the Decoy Generator as an "Arbitary Waveform". In principle, for perfect security, a new Decoy Profile should be chosen for each frame. This will require fast electronics for data input. For ease of demonstration, here we apply the same decoy profile for every frame. Note, however, that each signal within a frame is still attenuated individually. Therefore, in our opinion, our experiment addresses most essential technical challenges in the modification of the optical layer of a commercial QKD system for a decoy state implementation. A section of the Decoy Profile is visualized in Figure 1.

Figure 2 illustrates the schematic of the optical and electric layouts in our system. The commercial QKD system by id Quantique consists of Bob and "Jr. Alice". In our decoy state experiment, the actual (sender's) system is called "Alice". It consists of "Jr. Alice" and four new optical and electronics components added by us. A vivid photo of the who system except the controlling computer is shown in Figure 3.

More concretely, for our decoy state protocol, we place the Decoy AOM (denoted by DA in Fig. 2) right in front of Jr. Alice. Its "idle state" is set to maximum transmittance. When the frame comes from Bob, the Decoy AOM is in the idle state. After the first pulse reaches coupler $C_2$, it will be detected by the classical detector and a synchronization signal will be output to trigger the

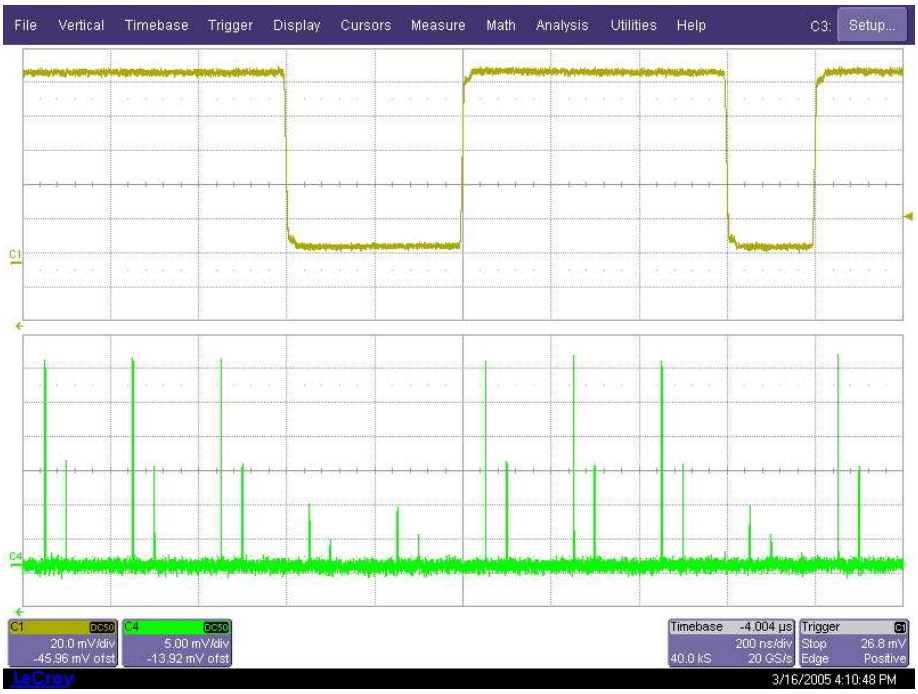


Figure 1: Visualization of the Decoy Profile. Upper chart: output from the Decoy Generator (For ease of visualization, we have shifted the signal by a constant time to offset the constant time delay between the signals in the Decoy Generator and those in laser pulses shown in the Lower Chart.); Lower Chart: corresponding attenuated laser pulses detected by ThorLabs SIR-5 5GHz Photodetector; bottom letters: corresponding section from the Decoy Profile, S=signal state, D=decoy state. For ease of visualization, we use strong laser pulses to obtain this figure. Here, we can also see the two pulses from the same signal. However, in the actual experiment, we set things up such that the intensity of the output from the AMO is at single photon level. The data in the chart were acquired by a LeCroy Wavepro7200 2GHz Oscilloscope.

Decoy Generator. The Decoy Generator (DG in Fig.2), being triggered, will hold a delay time $t_d$ before outputting $N_P$ modulation voltages driving the Decoy AOM to attenuate the intensity of each the $N_P$ signals to be either that of signal state or decoy state dynamically, according to the Decoy Profile. [As mentioned earlier, the compensating AOM (CA) is used only for the purpose of shifting the frequency of the signal and, thus maintaining the alignment between Alice's and Bob's interferometers. A compensating generator (CG) is used to drive the compensating AOM (CG).]

Within a frame, the time interval between signals is 200ns, while the time interval between the two pulses of the same signal is 50ns. To keep high visibility, these two pulses of the same signal must be applied the same attenuation, which is probably different from the attenuation applied on the next signal. Considering the rising time and the "jitter time", $t_d$ must be very precisely calibrated to make sure both pulses of the same signal are in the "platform" of the attenuation corresponds to this signal. In our experiment, $t_d = 123.51$ $\mu$s with an accuracy of 10ns.

After the transmission of the total $N$ pulses, Alice and Bob could share the Decoy Profile, according to which Bob could extract $Q_\mu$, $Q_\nu$ and $E_\mu$.

As we have mentioned, the data size we used in the experiment is 100M bits. The total

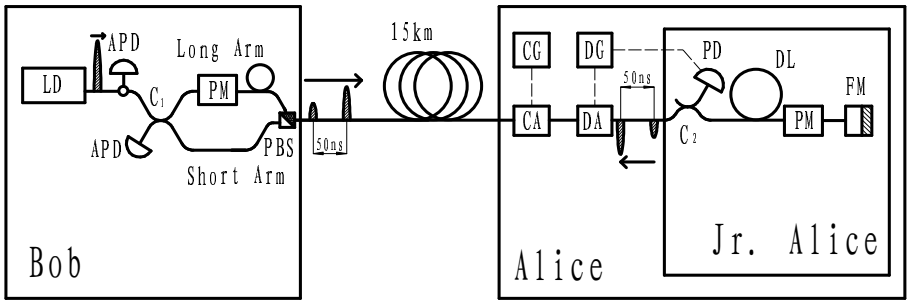


Figure 2: Schematic of the experimental set-up in our system. Inside Bob/Jr. Alice: components in Bob/Alice's package of ID-500 QKD system. Our modifications: CA: Compensating AOM; CG: Compensating Generator; DA: Decoy AOM; DG: Decoy Generator. Components of original ID-500 QKD system: LD: laser diode; APD: avalanche photon diode; $C_i$: fiber coupler; PM: phase modulator; PBS: polarization beam splitter; PD: classical photo detector; FM: faraday mirror. Solid line: SMF28 single mode optical fiber; dashed line: electric signal.

transmission time of these 100M bits was less than 4 minutes. However, we had to calibrate the attenuation of the AOM, the distance between Alice and Bob, and the delay time $t_d$ from time to time. We also had to measure the intrinsic characteristics like $\eta$ prior to the experiment to achieve the optimal pre-set parameters. The whole experiment took us roughly 3 hours.

## 3 Results and Discussion

The experimental results are shown in Table 3.

| Parameters | $Q_\mu$ | $Q_\nu$ | $E_\mu$ | $E_\nu$ | $q$ | $f(E_\mu)$[18] |
|---|---|---|---|---|---|---|
| Value | $1.393 \times 10^{-2}$ | $2.100 \times 10^{-3}$ | $9.479 \times 10^{-3}$ | $2.689 \times 10^{-2}$ | 0.4463 | 1.22 |

Table 3: Direct results from our experiment.

With the data in Table 3, we could calculate the bounds of $Y_1$, $Q_1$, $e_1$ and $R$ through Eqs. (2), (3), and (4), as shown in Table 4. We could see that we have achieved a pretty high key generation rate $5 \times 10^{-4}$ at 15km. The finite size of data (100M) gives a final secure key 50k bits and introduces statistical fluctuations and therefore reduces the key generation rate (per pulse) below the fundamental limit of $R_{perfect}$, which corresponds to infinite data size and infinite decoy state protocol. We remark that, as discussed in [15], here we consider only the fluctuations of the parameters, $Q_i$'s and $e_1$'s because we believe they, being rather small numbers, are the main source of statistical fluctuations. We do not consider, for example, the fluctuations in the number of different type of pulses (vacuum, single-photon, etc) as such fluctuations are negligible, in comparison. Notice that, even with our very conservative estimation for a confidence of $1 - 1.5 \times 10^{-23}$, the lower bound of $R$ is still roughly 1/4 of $R_{perfect}$. This fact hints that it is not necessary, or rather, not "economical", to use either very large data size or a lot of different decoy states. The transmission time was less than 4 minutes, thus demonstrating that the method of decoy state in quantum key distribution is indeed practical. Given a faster laser diode, the Decoy AOM can work at a frequency as high as

| Parameter | Value |
|---|---|
| $Y_1^L$ | $9.230 \times 10^{-3}$ |
| $Q_1^L$ | $3.318 \times 10^{-3}$ |
| $e_1^U$ | $3.980 \times 10^{-2}$ |
| $R^L$ | $5.369 \times 10^{-4}$ |
| $R_{perfect}$ | $2.271 \times 10^{-3}$ |

Table 4: The lower bounds of $Y_1$, $Q_1$, $R$ and the upper bound of $e_1$. The values are calculated from Eqs. (2), (3), and (4), taking statistical fluctuation into account. As a comparison, $R_{perfect}$, which is directly calculated from Eq. (1) in which the statistical fluctuation is not taken into account, is also shown. $R_{perfect}$ represents the situation of infinite long data size and infinite decoy states.

20MHz and performance of our system can be substantially improved.

Just to emphasize the importance of the decoy method, let us see what will happen if we do not use decoy states. In the absence of decoy states, the key generation rate is given by[10]

$$R \geq \max\left(0, Q_\mu\{-H_2(E_\mu) + (1-\Delta)[1 - H_2(\frac{E_\mu}{1-\Delta})]\}\right)$$

where[10]

$$\Delta = \frac{1-(1+\mu)e^{-\mu}}{Q_\mu}.$$

Now, from the model in [15] we could estimate by

$$Q_\mu = Y_0 + e^{-\eta\mu}$$

$$E_\mu = e_{detector} + \frac{1}{2}\frac{Y_0}{Q_\mu}$$

with data in Table 2. We performed numerical simulation ranging $\mu$ from 0 to 1, while no positive lower bound on $R$ can be found. This fact indicates that for our set-up, at a distance of 15km, without decoy states, we would have been unable to prove the security of our protocol in an analogous manner. [We remark that using the idea of advantage distillation, it is known [23] that BB84 can achieve unconditional security even at QBER as high as 18.9 percent.]

We conclude with a discussion of some problems and future work on the subject. We have measured the fluctuation of the output from the Decoy AOM. As expected, the fractional fluctuation for the decoy state ($\sim \pm 0.1$dB) is (naturally) higher than that of the signal state ($\sim \pm 0.01$dB). In fact, the visibility of decoy states is lower than that of signal states. Put it another way, there are imperfections ("Trojan Ponies") in both the signal and the decoy states. In principle, Eve might exploit such imperfections to gain more information about the final key than what is otherwise allowed. In future, it will be interesting to study both theoretically and experimentally this type of imperfections in QKD. This is, however, beyond the scope of the present paper.

## 4 Conclusion

A big recent surprise in quantum key distribution (QKD) is the idea of decoy state protocols, which allows both perfect security and unsurpassed performance with only current technology. In this

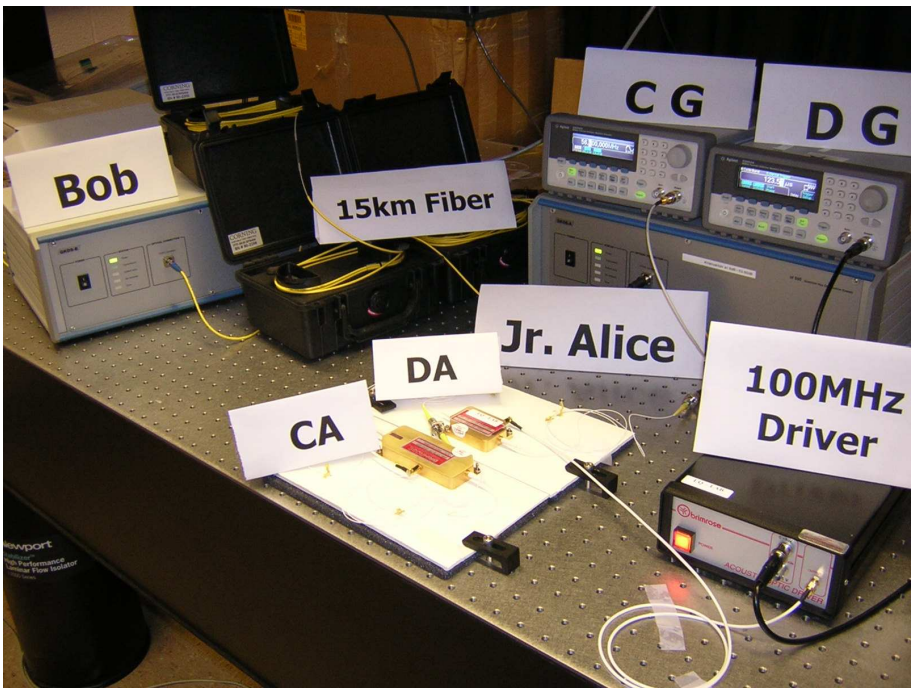


Figure 3: A photograph of the whole QKD system except the controlling computers. The new components that we have added are placed around Jr. Alice. All the labels correspond to the labels in Figure 2.

paper, we provide the first experimental demonstration of decoy state QKD over 15km of Telecom fibers. Our result shows that, with rather simple modifications (by adding commercial variable optical attenuators) to a commercial QKD system, decoy state QKD allows us to achieve much better performance (in terms of substantially higher key generation rate and longer distance) than what is otherwise possible. Modulo two technical assumptions discussed earlier, our experiment gives unconditional security against the most general attack allowed by quantum mechanics. Moreover, it gives a rather high key generation rate. We expect that decoy state QKD will play a major role in future QKD systems in both fibers and open air. A new chapter in the real-life arms race between quantum code-makers and quantum code-breakers has just begun.

We thank enlightening discussions with colleagues including Charles Bennett, Gilles Brassard, Frédéric Dupuis, Jim Harrington, Norbert Lütkenhaus, Kiyoshi Tamaki, John Preskill, and Zhiliang Yuan. Financial supports from Canadian NSERC, Canada Research Chairs Program, Connaught Fund, Canadian Foundation for Innovation, Ontario Innovation Trust, Premier's Research Excellence Award, Canadian Institute for Photonics Innovations, and University of Toronto start-up grant are gratefully acknowledged. H.-K. Lo also thanks travel support from the Institute for Quantum Information at the California Institute of Technology through the National Science Foundation under grant EIA-0086038.

## References

[1] Bennett, C. H. & Brassard, G., *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE, 1984, pp. 175-179.

[2] Bennett, Ch.H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography", J. Cryptology, **5** 3-28.

[3] Kimura, T. *et al.*, On-line available at http://arxiv.org/abs/quant-ph/0403104

[4] C. Gobby, Z. L. Yuan, and A. J. Shields, *"Quantum key distribution over 122 km of standard telecom fiber"*, Applied Physics Letters, Volume 84, Issue 19, pp. 3762-3764, (2004).

[5] MagiQ Technologies, Inc. website: http://www.magiqtech.com/

[6] id Quantique website: http://www.idquantique.com

[7] Mayers, D. *J. of ACM* **48**, 351 (2001). A preliminary version in Mayers, D. *Advances in Cryptology–Proc. Crypto '96*, vol. 1109 of *Lecture Notes in Computer Science*, Koblitz, N. Ed. (Springer-Verlag, New York, 1996), pp. 343-357; Lo, H.-K. & Chau, H. F., *Science*, **283**, 2050 (1999); Biham, E., Boyer, M., Boykin, P. O., Mor, T. & Roychowdhury, V., *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC'00)* (ACM Press, New York, 2000), pp. 715-724; Ben-Or, M. Presentation at MSRI, available on-line at http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/+

[8] P. W. Shor and J. Preskill, *"Simple proof of security of the BB84 quantum key distribution protocol"*, Phys. Rev. Lett., vol. 85, p. 441, 2000. Also, [*Online] Available: http://xxx.lanl.gov/abs/quant-ph/0003004.

[9] A. K. Ekert, and B. Huttner, *J. of Modern Optics* **41**, 2455 (1994); D. Deutsch *et al.*, *Phys. Rev. Lett.* **77**, 2818 (1996); Erratum: *Phys. Rev. Lett.* **80**, 2022 (1998).

[10] D. Gottesman, H.-K. Lo, Norbert Lutkenhaus, and John Preskill, "Security of quantum key distribution with imperfect devices", Quantum Information and Computation. Vol. 4, No.5 (2004) 325-360, http://arxiv.org/abs/quant-ph/0212066

[11] Inamori, H., Lütkenhaus, N. & Mayers, D. Los Alamos e-Print archive (available at http://arxiv.org/abs/quant-ph/0107017).

[12] M. Keller *et al.*, "Continuous generation of single photons with controlled waveform in an ion-trap cavity system," Nature 431, 1075 - 1078 (2004); B. Lounis and W. E. Moerner, "Single photons on demand from a single molecule at room temperature," Nature 407, 491 - 493 (2000); P. Michler *et al.*, "Quantum correlation among photons from a single quantum dot at room temperature," Nature 406, 968 - 970 (2000); J. Kim, O. Benson, H. Kan and Y. Yamamoto, "A single-photon turnstile device," Nature 397, 500 - 503 (1999); P. Michler *et al.*, "A Quantum Dot Single-Photon Turnstile Device," Science 290: 2282-2285 (2000); Z. Yuan *et al.*, "Electrically Driven Single-Photon Source," Science 295: 102-105 (2002); J. McKeever *et al.*, Science 303: 1992-1994 (2004).

[13] W.-Y. Hwang, *"Quantum Key Distribution with High Loss: Toward Global Secure Communication"*, Phys. Rev. Lett. 91, 057901 (2003)

[14] H.-K. Lo, X. Ma and K. Chen "Decoy State Quantum Key Distribution", http://lanl.arxiv.org/abs/quant-ph/0411004 (2004) Preliminary results were presented in Proceedings of IEEE ISIT 2004, July 2004 and various scientic conferences such as Fields Institute Conference on Quantum Information and Quantum Control, http://www.elds.utoronto.ca/programs/scientic/04-05/quantumIC/abstracts/lo.ppt ; See also X. Ma, "Security of Quantum Key Distribution with Realistic Devices," http://arxiv.org/abs/quant-ph/0503057 (2005).

[15] X. Ma, B. Qi, Y. Zhao and H.-K. Lo, "Practical Decoy State for Quantum Key Distribution", http://www.arxiv.org/abs/quant-ph/0503005 (2005)

[16] Xiang-Bin Wang, *"Beating the PNS attack in practical quantum cryptography"*, http://arxiv.org/absquant-ph/0410075 ; Xiang-Bin Wang, *"A decoy-state protocol for quantum cryptography with 4 intensities of coherent states"*, http://arxiv.org/abs/quant-ph/0411047

[17] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, *"Enhancing practical security of quantum key distribution with a few decoy states"*, available at http://arxiv.org/abs/quant-ph/0503002

[18] G. Brassard and L. Salvail, in Advances in Cryptology EUROCRYPT '93, Vol. 765 of Lecture Notes in Computer Science, edited by T. Helleseth (Springer, Berlin, 1994), pp. 410-423.

[19] Z. L. Yuan, A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre", Optics Express 13, 660-665(2005)

[20] Xiao-fan Mo, Bing Zhu, Zheng-Fu Han, You-zhen Gui, Guang-can Guo, "Intrinsic-Stabilization Uni-Directional Quantum Key Distribution Between Beijing and Tianjin", http://www.arxiv.org/abs/quant-ph/0412023

[21] H.-K. Lo and J. Preskill, "Phase Randomization Provably Improves Security of Quantum Key Distribution," paper under preparation.

[22] D. Stuck, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system", New Journal of Physics. 4 (2002) 41.1-41.8

[23] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Trans. Inf. Theory* **49**, 457 (2003).