Practical gigahertz quantum key distribution based on avalanche photodiodes

Z L Yuan\textsuperscript{1,3}, A R Dixon\textsuperscript{1,2}, J F Dynes\textsuperscript{1}, A W Sharpe\textsuperscript{1} and A J Shields\textsuperscript{1}

\textsuperscript{1}Toshiba Research Europe Ltd, Cambridge Research Laboratory, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK
\textsuperscript{2}Cavendish Laboratory, University of Cambridge, J J Thompson Avenue, Cambridge CB3 0HH, UK
E-mail: zhiliang.yuan@crl.toshiba.co.uk

New Journal of Physics 11 (2009) 045019 (11pp)
Received 17 December 2008
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045019

Abstract. We report in this paper a gigahertz clocked quantum key distribution (QKD) system using only practical components. Compact semiconductor avalanche photodiodes are used for high-speed single photon detection, whereas an attenuated laser is used as a light source in combination with the decoy protocol for guarding against photon-number-splitting attacks. The system is characterized by secure key rates of 1.02 Mbit s\(^{-1}\) for a fibre distance of 20 km and 10.1 kbit s\(^{-1}\) for 100 km. The suitability of standard single mode fibres as the quantum channel is also demonstrated.

Contents

1. Introduction 2
2. Practical high-speed single photon detection in the near infrared 2
3. Experimental QKD setup 5
4. GHz QKD using decoy pulses 6
5. Standard single mode fibre as the quantum channel 9
6. Conclusion 10
Acknowledgment 10
References 10

\textsuperscript{3}Author to whom any correspondence should be addressed.
1. Introduction

Communication with single photons allows the distribution of digital keys over fibre networks, the security of which can be guaranteed by the laws of quantum mechanics [1]. Since its first proof-of-principle demonstration over a free space distance of 32 cm [2], experimental quantum key distribution (QKD) has advanced significantly across fibre optic links [3]–[13]. Nowadays, QKD is run at clock rates of 1 GHz or higher [7]–[12] and/or a distribution distance of over 100 km [6], [9]–[11]. The secure key rate has already reached 1 Mbit s⁻¹ over 10–20 km fibres [11, 12], thus allowing the use of QKD in a wider range of applications, such as secure video links [14]. Point-to-point QKD links have emerged out of the laboratory as building blocks towards a wide area QKD network [15].

In the original BB84 protocol, a truly single photon source is required to guarantee unconditional security [1]. Such a requirement would lead to an impractical system because a truly single photon source at present still needs cryogenic cooling and/or a sophisticated optical setup [16, 17]. Instead, attenuated lasers have always been used for practical systems [3]–[14]. An attenuated laser sometimes emits more than one photon per pulse, which can compromise the security of QKD [18, 19]. Recently, the conflict between security and practicality has been subdued thanks to the decoy protocol, developed by Lo et al [20] and Wang [21] based on the original idea of Hwang [22]. By replacing a subset of the signal pulses with less intense ‘decoy’ pulses, the transmitter (Alice) and receiver (Bob) can detect any attempted photon-number-splitting (PNS) attack [18, 19] through monitoring the quantum channel transmittances. As a simple modification to the original BB84 protocol, the decoy protocol provides a practical route to maintain security in an attenuated laser-based fibre system [23]–[28].

High-speed single photon detectors are crucial for achieving a high key rate. For practicality, such a detector should be compact and cryogenic-free. Semiconductor InGaAs avalanche photodiodes (APDs) are highly practical, and recent advances in InGaAs APD technologies have made them suitable for operation with gigahertz (GHz) clock rates [29, 30]. Their use in a GHz system has already been demonstrated [10, 11] with multi-megabit sifted key rates. Here, we describe the development of high-speed InGaAs APDs and their integration into a practical GHz decoy QKD system. The system is characterized by a secure key rate of 1.02 Mbit s⁻¹ over a fibre distance of 20 km and 10.1 kbit s⁻¹ for 100 km. The suitability of standard single mode fibres as the quantum channel is also demonstrated.

2. Practical high-speed single photon detection in the near infrared

Fibre-optic GHz QKD requires high-speed single photon detection at telecom wavelengths (1.31/1.55 µm). Previously, InGaAs/InP APDs have been widely used for QKD with megahertz (MHz) clocked rates for over a decade due to their compactness and non-cryogenic operation [5, 6]. Their progress into GHz-clocked QKD systems was thought impossible due to the poor quality of InGaAs materials. Alternatively, other detectors, such as those based on up-conversion [7] or superconducting nanowires [9], were developed for GHz systems to increase the key rates. However, the key rate increase comes at the cost of inconvenience. Up-conversion detectors require a high-power optical pump and precise optical alignment for noise rejection, while a superconducting nanowire detector requires cryogenic cooling. Moreover, both types of detectors have a typical usable efficiency of merely 1%.
Afterpulsing is the main factor limiting the use of InGaAs APDs for GHz operation. An APD senses single photons through avalanche multiplication to convert a single photo-excited carrier into a macroscopic current flow. Avalanche carriers that are trapped by defects can trigger a secondary avalanche by spontaneous release, contributing to erroneous detector noise. InGaAs APDs are particularly vulnerable to this noise. Afterpulsing can be suppressed through gating with nanosecond voltage pulses to reduce the number of charge carriers produced in an avalanche. However, the number must be sufficiently high to surpass the capacitive response produced by a pulsed gate, giving rise to an avalanche gain of the order of $10^7$. With such a gain, the afterpulse noise is significant, even for MHz operation, and a dead time of a few microseconds is typically required after each photon detection.

The avalanche gain needs to be reduced for high-speed operation. A shorter gate helps reduce the gain. However, this will also increase the amplitude of the capacitive response to the applied gate, which makes the detection of weak avalanches more problematic. To overcome this, a self-differencing (SD) circuit can be used [29]. As shown in figure 1(a), an SD circuit contains a 50/50 signal splitter and a signal differencer connected by two pieces of electrical cables with length difference corresponding to an integer number of the gating

**Figure 1.** (a) Schematic diagram of an APD in the SD mode. (b) Distribution of an APD’s peak output signal generated by the SD circuit running at 1 GHz. In QKD experiments, a signal discrimination level is set such that a detector offers the highest ratio of photon detection efficiency to dark count probability.
Figure 2. Photon detection rate and photocurrent as a function of photon flux with the APD illuminated by a directly modulated telecom laser diode at 0.98 GHz [29]. The arrows indicate the detector dark rate and dark current, which were subtracted from the measured results.

clock period. Due to the periodic gating, the capacitive signal can be near-perfectly removed by the subtraction of the self-differencer. As shown in figure 1(b), amplitude distribution of avalanches is clearly distinguished from the background electronics noise after cancellation of the capacitive response. Moreover, the signal amplitude is proportional to the number of photons that stimulate an avalanche, making the SD-APD a practical photon-number resolving detector [31].

The avalanche gain can be extracted from the photocurrent dependence on photon count rate in the linear regime. As shown in figure 2, the count rate increases linearly with the incident photon flux over the > 30 dB dynamical range. The increase in count rate becomes sub-linear for count rates greater than 20 MHz, and finally saturates at 100 MHz. The photocurrent also displays linear dependence on the incident photon flux, but over a larger dynamical range. The photocurrent continues to increase, even when the photon count rate is saturated, suggesting that the 100 MHz saturation count rate is limited by the photon counting electronics. The measured count rate is less than 50% of the theoretical value, which is 1/4 of its driving clock frequency, e.g. 250 MHz for a gating frequency of 1 GHz, under the present illumination condition. In the linear regime, we can obtain an average avalanche charge of 0.2 pC, corresponding to a gain of $1.25 \times 10^6$. This gain is an order of magnitude lower than in conventional gated mode operation, and is essential for high-speed operation.

SD-APDs also offer excellent timing performance. Figure 3(a) is a time-resolved histogram of photon arrivals under the illumination of a 1.036 GHz attenuated pulsed laser, recorded by a correlation setup that has a time resolution of 4 ps and an instrumental jitter of 60 ps (10 dB width). Each photon arrival peak has a sharp distribution with a clear separation between neighbouring peaks thanks to the gated mode operation. As an advantage inherited from the differential nature, all dc signals are removed after the SD. As a result, the photon arrival time

New Journal of Physics 11 (2009) 045019 (http://www.njp.org/)
Figure 3. (a) Histogram of photon detections under the illumination of a 1 GHz laser pulse train. (b) Full-widths at 1/10 (10 dB) and 1/1000 (30 dB) intensity of the maximum as a function of photon count rate.

Figure 4. Schematic diagram of the QKD system. PBS/PBC: polarization beam-splitter/combiner; APD: InGaAs avalanche photodiode. All the modulating optics are driven by stand-alone GHz pattern generators with pre-loaded pseudorandom patterns.

is not significantly affected by an increase in the photon count rate. As shown in figure 3(b), the full-widths at 1/10 (10 dB) and 1/1000 (30 dB) intensity vary by less than 20% for the photon count rate change from 20 kHz to 10 MHz. At a count rate of 10 MHz, the 30-dB width is only 240 ps, thus guaranteeing unambiguous bit assignments in a GHz QKD system.

3. Experimental QKD setup

Figure 4 shows a schematic diagram of the decoy QKD setup. Photons are generated by a 1.55 μm pulsed laser operating at 1.036 GHz. The three intensity levels required for signal, decoy and near vacuum pulses are created using a fibre-optic intensity modulator. The quantum information is transmitted by the phase of the photons, using phase encoding/decoding optics based on an asymmetric fibre Mach–Zender interferometer (AMZI). Off-the-shelf
optical components were used to construct the AMZIs. The AMZI pairs have matching time differences, of 440 ps in this case, to ensure that single photon interference takes place at the exit of the second AMZI. Fine phase control is achieved through a fibre stretcher placed in one of Bob’s AMZI arms [6, 32]. The AMZIs are carefully insulated from the environment to achieve sufficient stability to allow QKD to take place. The optical pulses are strongly attenuated to the desired levels before leaving the sender’s apparatus, with the intensity level of the pulses monitored using a beam-splitter and optical power meter (not shown). A dispersion shifted fibre (DSF) is used as the quantum channel, with an attenuation loss of 0.20 dB km\(^{-1}\). A polarization controller at Bob’s side recovers the polarization alignment before his AMZI. Each photon detection event is recorded with a unique time stamp by time-tagging electronics, and these events are used by Alice and Bob to generate a secure key.

The InGaAs APDs (JDS Uniphase EPM239AA) used in this study were thermal–electrically cooled to \(-30\,^{\circ}\mathrm{C}\) to suppress the detector dark count rate. They were gated with a 1.036 GHz square wave with an excess voltage to achieve an optimal secure key rate. Under such conditions, the detector dark count probability was measured as \(6.8 \times 10^{-6}\) per gate at a photon detection efficiency of 10%.

4. GHz QKD using decoy pulses

QKD systems that use an attenuated laser to approximate a single photon source have a finite probability of generating a multi-photon state. This opens up the possibility of PNS attacks [18, 19]. This attack can be defeated by the use of decoy protocols, in which Alice replaces some of her signal pulses (average intensity \(\mu\) photons per pulse) with decoy pulses of different intensities (average intensities \(\nu\) photons per pulse). These intensities relate only to the statistical probability that each type of pulse contains 0, 1 or more photons; any single signal or decoy pulse appears indistinguishable to Eve. As such, any attempted PNS attack, in which single photon pulses are blocked and multi-photon pulses are preferentially transmitted by Eve, will affect the transmission and error rates of signal and decoy pulses differently. By monitoring these rates, the amount of information gained by Eve can be upper bounded; this information can then be removed in the privacy amplification process using the GLLP [33]. The final secure key rate is determined using

\[
R_S = \frac{1}{2} N_\mu \left( -Q_L f_{EC} H_2(\epsilon_\mu) + Q_U^1 \left[ 1 - H_2(\epsilon_U^1) \right] \right) / t,
\]

where \(N_\mu\) is the total number of signal pulses sent by Alice and \(t\) is the QKD session time. \(\epsilon_\mu\) is the quantum bit error rate (QBER) for the signal pulses (\(\mu\)). \(Q_U^1\) and \(\epsilon_U^1\) are the lower bound for transmittance and the upper bound for the QBER of the single photon pulses, respectively, and are inferred from the measured characteristics of the signal and decoy pulses. \(f_{EC}\) is the error correction efficiency and \(H_2(x) = -x \log_2(x) + (1 - x) \log_2(1 - x)\) is the binary Shannon entropy. We use \(f_{EC} = 1.10\) in this study based on the previous results of our error correction module [24].

The weak plus vacuum decoy protocol [34] was selected for use in the QKD experiment. This protocol utilizes three intensity levels, a signal (\(\mu\)) used for key generation and two weaker decoy intensities, \(\nu_1\) and \(\nu_2\), with the condition that \(\mu > \nu_1 > \nu_2\). The different intensities were produced by a high-speed intensity modulator, with a maximum extinction ratio of 29 dB. This means that the intensity of \(\nu_2\) can be at most 29 dB lower than the signal \(\mu\). Theory predicts that the protocol is most efficient when \(\nu_2 = 0\), but the effect of using the very weak but non-vacuum pulses is found to be insignificant. Numerical simulations were performed to determine
Figure 5. Numerical simulation of the secure key rate as a function of signal ($\mu$) and weak decoy ($\nu_1$) intensities for a fibre distance of 20 km. In this simulation, the probabilities for signal, weak decoy and near vacuum decoy pulses are fixed at 0.80, 0.16 and 0.04, and the QKD session time is 2 s. The contour line labelled ‘1M’ shows the range of $\mu$ and $\nu_1$ within which a secure key rate of $\geq 1$ Mbit s$^{-1}$ can be achieved.

The experimental parameters for an optimized key rate, as shown in figure 5, where the secure key rate is plotted as a function of the signal ($\mu$) and weak decoy ($\nu_1$) pulse intensities for a fibre distance of 20 km and a key formation time of 2 s. It is found that a secure key rate exceeding 1 Mbit s$^{-1}$ can be obtained over a wide range of $\mu$ and $\nu_1$ values, illustrating the relatively weak dependence on $\mu$ and $\nu_1$. Based on this simulation, we choose $\mu = 0.55$ and $\nu_1 = 0.10$, which give close to optimal secure bit rates for a fibre distance of 20 km, for all the distances studied below.

QKD was initially performed over a 20 km fibre link. The average photon intensities (duty cycles) for this experiment were $\mu = 0.55$ (0.8), $\nu_1 = 0.10$ (0.16) and $\nu_2 = 0.00076$ (0.04). Key generation sessions were fast due to the high clock rate employed, ensuring tight statistical bounds on the parameters measured. A key session time of 2.3 s yielded 7.91 Mbit of sifted signal bits with a QBER of 2.53%. In determining the single photon pulse characteristics for use in equation (1), each experimentally measured parameter, such as transmittances of signal and decoy pulses, is replaced conservatively with its 10-standard deviation upper or lower bound [21, 34]. This gives a lower bound for the final secure key rate. For the 2.3 s QKD session, we obtain a lower bound for the final secure bit rate of 1.02 Mbit s$^{-1}$ over a fibre distance of 20 km. This rate is more than a factor of 100 higher than the previous unconditionally secure QKD record of 10 kbit s$^{-1}$ [27].

A longer key formation time helps to improve the secure key rate, but only to a limited extent for the current 20 km experiment. As shown by the calculation in figure 6, the 2.3 s key formation time is sufficient to achieve 90% of the saturation value that may be obtained with an infinite QKD session. This is a direct result of our high system clock rate, which allows the
accumulation of sufficient photon counts for bounding statistical fluctuation even over a short duration. The threshold for a positive key rate at 20 km is as short as 0.01 s.

Increasing the fibre length induces a higher loss over the quantum channel, leading to a decreasing photon count rate. As shown in figure 6, the key formation time threshold has increased to 0.045 and 3.3 s for 50 and 100 km of fibres, respectively. Thus, to obtain a satisfactory key rate, QKD must be performed over a sufficiently long time, especially for 100 km. In our 100.8 km experiment, a key formation time of 16.5 s has allowed a final secure bit rate of 10.1 kbit s\(^{-1}\). Although this rate is nearly three orders of magnitude greater than the previous record of 10 bit s\(^{-1}\) [25] at a similar distance and an equivalent level of security, it can be further increased twofold by distributing quantum keys over a longer duration in future once an active stabilization system has been implemented [32].

We now compare our results with two recent high-speed QKD experiments using alternative detectors. Firstly, Tanaka et al [13] performed a QKD experiment using cryogenic temperature superconducting nanowire detectors. Based on standard decoy-protocol analysis, the secure key rate was asymptotically estimated to be 0.78–0.82 kbit s\(^{-1}\) for a 97 km fibre link. Secondly, Zhang et al [12] used an up-conversion hybrid detector in their differential phase shift QKD system. The obtained key rate reaches 1 Mbit s\(^{-1}\) for a 10 km fibre link, but falls below 1 Mbit s\(^{-1}\) for 20 km fibre. These two systems have a lower bit rate than the present InGaAs APD-based system. Both superconducting and up-conversion detectors have a significantly lower detection efficiency than InGaAs APDs. Moreover, the up-conversion detector suffers from high background noise, which limits the key distribution distance to less than 40 km. Besides giving the highest key rates, InGaAs APDs are the most compact high-speed detector and do not require cryogenic cooling. We believe that the present work will stimulate greater research interest in the use of InGaAs APDs for high-speed single photon detection. The performance of InGaAs APDs will be significantly improved with further progress either in device design [35] or a better photon detection circuit [29, 30]. InGaAs APDs are likely to be a key component of future GHz QKD implementations, as they are in the current MHz systems.

**Figure 6.** Experimental (solid circles) and theoretical (lines) secure key rates as a function of key formation time for a fibre distances of 20, 50 and 100 km.
Figure 7. (a) Optical pulses measured by an oscilloscope under various conditions: 0 and 100 km SMF without/with FBGs. (b) QBERs measured as a function of fibre distance for a quantum channel made of SMF-28 fibre with or without FBGs to pre-compensate chromatic dispersions. In this experiment, the standard BB84 protocol was used with an average pulse intensity of 0.2 photons pulse$^{-1}$ and a clock rate of 1.036 GHz.

5. Standard single mode fibre as the quantum channel

Standard single mode fibres, such as SMF-28, are widely used in telecom networks and are also a popular choice for quantum channels. These fibres, like the DSFs used in the above experiment, have low attenuation at 1550 nm, which is of great importance for transmitting signals at the single photon level. However, the nonzero chromatic dispersion at 1550 nm, 17 ps km$^{-1}$ nm$^{-1}$, results in pulse broadening. Although this broadening would not be noticeable for several hundreds of kilometres for the QKD system transmitting at MHz clocked rate, it deteriorates the QKD performance after even 50 km for a GHz system. This is caused by photons spreading outside detector gates, which reduces count rates, and even into neighbouring gates, which directly increases the QBER. To avoid the chromatic dispersion, DSF is frequently chosen as a quantum channel in GHz clocked QKD experiments.

The fibre dispersion problem can be overcome by pre-compensating [10]. For example, this can be done by inserting a fibre Bragg grating (FBG) in Alice’s apparatus before the signal is launched into the quantum channel. This introduces dispersion opposite to that caused by the specified length of fibre, resulting in zero net dispersion at the receiver’s side. Figure 7(a) shows the shape of an optical pulse generated by a 1550 nm pulsed laser. The pulse is measured after 100 km of fibre both with and without a FBG, providing corresponding dispersion compensation. The grating corrects for the dispersion, reducing the pulse width to the same level as that observed at the laser output (0 km of fibre). The effect of dispersion on the QBER is shown in figure 7(b). Use of FBGs significantly reduces the measured QBER. After
compensating for the dispersion, the obtained QBER is similar to those obtained with DSFs (not shown), suggesting that standard single mode fibres can also serve as the quantum channel for GHz QKD systems.

6. Conclusion

In conclusion, we have demonstrated that QKD is now capable of 1 Mbit s\(^{-1}\) secure key rate operation over a fibre distance of 20 km. At 100 km, the secure key rate still reaches 10 kbit s\(^{-1}\). We stress that the present achievement is based on only practical components. Vulnerabilities of attenuated lasers are avoided through the use of the decoy protocol, while high-speed single photon detection is realized using compact and cryogenic-free semiconductor APDs. The result is applicable to either DSF or a standard single mode fibre as the quantum channel. With the present advances, we believe that QKD is now practically useful for realizing high-band-width information-theoretically secure communication.

Acknowledgment

We thank the EU for funding this work under the FP6 Integrated Project SECOQC.

References

[1] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India) pp 175–9
[2] Bennett C H et al 1992 J. Cryptol. 5 3
[3] Townsend P, Rarity J G and Tapster P R 1993 Electron. Lett. 29 634
[4] Hughes R J, Morgan G L and Peterson C G 2000 J. Mod. Opt. 47 533
[5] Stucki D et al 2002 New J. Phys. 4 41
[6] Gobby C, Yuan Z L and Shields A J 2004 Appl. Phys. Lett. 84 3762
[7] Takesue H et al 2005 New J. Phys. 7 232
[8] Gordon K J et al 2005 Opt. Express 13 3015
[9] Takesue H et al 2007 Nat. Photonics 1 343
[10] Yuan Z L et al 2008 Appl. Phys. Lett. 92 201104
[11] Dixon A R et al 2008 Opt. Express 16 18790
[12] Zhang Q et al 2008 arXiv:0809.4018
[13] Tanaka A et al 2008 Opt. Express 16 11354
[14] Mink A et al 2006 Proc. SPIE 6244 62440M
[15] The European Integrated Project SECOQC http://www.secoqc.net
[16] Ward M B et al 2005 Appl. Phys. Lett. 86 201111
[17] Intallura P M et al 2007 Appl. Phys. Lett. 91 161103
[18] Dušek M, Haderka O and Hendrych M 1999 Opt. Commun. 169 103
[19] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 Phys. Rev. Lett. 85 1330
[20] Lo H K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[21] Wang X B 2005 Phys. Rev. Lett. 94 230503
[22] Hwang W Y 2003 Phys. Rev. Lett. 91 057901
[23] Zhao Y et al 2006 Phys. Rev. Lett. 96 070502
[24] Yuan Z L, Sharpe A W and Shields A J 2007 Appl. Phys. Lett. 90 011118
[25] Rosenberg D et al 2007 Phys. Rev. Lett. 98 010503

New Journal of Physics 11 (2009) 045019 (http://www.njp.org/)
[26] Peng C Z et al 2007 Phys. Rev. Lett. 98 010505
[27] Dynes J F, Yuan Z L, Sharpe A W and Shields A J 2007 Opt. Express 15 8465
[28] Yin Z Q et al 2008 Chin. Phys. Lett. 25 3547
[29] Yuan Z L, Kardynal B E, Sharpe A W and Shields A J 2007 Appl. Phys. Lett. 91 041114
[30] Namekata N, Adachi S and Inoue S 2009 Opt. Express 17 6275
[31] Kardynal B E, Yuan Z L and Shields A J 2008 Nat. Photonics 2 425
[32] Yuan Z L and Shields A J 2005 Opt. Express 13 660
[33] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 Quantum Inf. Comput. 4 325
[34] Ma X, Qi B, Zhao Y and Lo H K 2005 Phys. Rev. A 72 012326
[35] Itzler M A et al 2007 J. Mod. Opt. 54 283