PRACTICAL SOLUTION FOR SECURE NETWORK IN A QUANTUM COMPUTING ERA

Anindita Banerjee and MT Karunakaran

info@qnulabs.com

sales@qnulabs.com

QuNu Labs Pvt Ltd., MG Road, Bangalore, India

Abstract: Data security in a network is a major concern in quantum era. One of the major challenges faced by quantum technology is to integrate itself seamlessly into present cryptographic infrastructure. The encryption algorithms prevalent today should be revisited from the perspective of threat from a quantum computer. In this paper, we demonstrate a practical demonstration and integration of a Differential Phase Shift Quantum Key Distribution (DPS QKD) protocol with commercial router cum encryptor. This QKD protocol is based on a family of Distributed Phase Reference protocol which is best suited for fiber transmission. We have achieved with 1 GHz pulse repetition rate in conjunction with gated single photon detectors, a sifted key rate of 600 Kb/s and secure key rate of 271 Kb/s at 40 km. The quantum bit error rate in our QKD system is less than 4% for the present implementation. We have validated the randomness of the final secure keys generated from QKD in NIST test suite and it has passed all the 15 tests. The QKD system was integrated with a commercial router cum encryptor and we have successfully performed data transmission from a source router to a destination router.

1. Introduction

Cryptography is an art of secret writing. The primary objective of cryptography is to protect the authenticity, integrity, and confidentiality of the information being sent. The message (plaintext) is encrypted by an encryption algorithm using an encryption key and delivered to the recipient through a conventional channel in the form of a cryptogram. The encryption algorithm is again applied in an inverse manner to retrieve the message from the cryptogram. The cryptographic key is the most vital part of any cryptographic process, it needs to remain private to ensure any secure communication. All the public key infrastructures use asymmetric keys comprising of public key and private key. The certification authority gives the private key to the key-requester

while the public key can be shared over public channel. These keys are used for various cryptographic purposes like encryption-decryption, creation-verification of digital signatures, key transport etc. All the cryptographic algorithms that utilizes these keys for encryption-decryption or any other cryptographic tasks are based on mathematical algorithms ensuring computational security to our data. This computation security is based on the capability of classical computers. In quantum information theory, the information is processed by the laws of quantum mechanics which provides huge computational power and there are quantum algorithms which can break prevalent classical cryptographic algorithms like Diffie–Hellman (DH), Rivest Shamir Adleman (RSA) and Elliptic-curve cryptography (ECC) on a large-scale quantum computer. The threat lies if the encrypted data-in-transit is copied today then, it can be later decrypted by anyone who will have an access to the quantum computer. Therefore, the efforts by global standardization bodies are towards making present cryptographic backbone quantum-safe. A prospective candidate for quantum-safe encryption is Quantum Key Distribution (QKD) which is one the most mature fields of Quantum Information Theory. The theoretical security of the QKD protocols are based on the fundamental principles of quantum physics. The composability [1] of QKD allows the keys to be used for other cryptographic primitives for enabling forward security. Differential Phase Shift (DPS) QKD is one of the most prominent QKD protocols in Differential Phase Reference (DPR) QKD protocol family. It can be implemented using standard telecommunication fiber and off-the-shelf components. With respect to QKD performance, DPS has a major advantage over other QKD protocols [2,3] using weak coherent state. The reason being, it is insensitive to multi-photon states. Considering the photon-number-splitting (PNS) attack, the secure key rate of DPS QKD is close to BB84 when performed with an ideal source, in other words it outperforms BB84 protocol with coherent source. In this work, we have authenticated the QKD nodes (Alice and Bob) from 2-universal hash family with prior shared keys required for the same. We have implemented a QKD protocol in fiber medium and performed sifting, error correction using cascade, privacy amplification [4] and finally key reconciliation. In section 2, we have mathematically explained the QKD protocol, in section 3 we have briefly discussed the eavesdropping techniques on quantum channel, in section 4 we have explained our experimental setup, in section 5 we have discussed the quantum-safe network and integration in the commercial router system and in section 6 we have concluded our work.

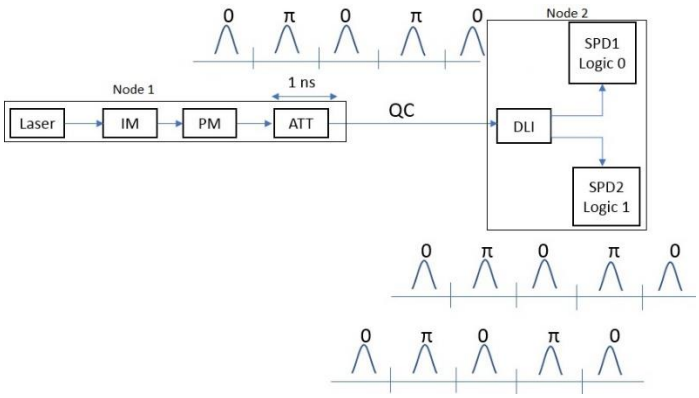


Fig.1. Schematic of DPS QKD. The intensity modulator (IM) generates the pulses, phase modulator (PM) modulates the optical signal, thereafter it is attenuated by an attenuator (ATT) and passed through a quantum channel (QC). Bob has DLI is Delay line interferometer (DLI) and he detects the photons using InGaAs based Single Photon Detector (DPD).

2. QKD protocol

In QKD, the carriers of binary information are a quanta of light. Ideally, it is a single photon Fock state. Single photon sources are difficult to realize experimentally, this is the reason that QKD is mostly implemented by faint laser pulse/weak coherent source. This kind of source obeys Poisson statistics. We have demonstrated the DPS QKD protocol using weak coherent source between sender Node 1 (Alice) and receiver Node 2 (Bob). The schematic is presented in Fig.1. Each pulse is randomly phase modulated by phase 0 or π by a phase modulator according to the random numbers which are generated by a random number generator. These random numbers form Alice's raw key. She applies a π phase when the raw key is 1 and 0 phase when raw key is 0. She attenuates the Weak Coherent Pulses (WCP) to a mean photon number of $\mu = 0.1$. Alice sends them to Bob through a quantum channel (QC). Bob receives the travel photons, demodulates them through Delay Line Interferometer (DLI) and detects them randomly. Precisely, the WCPs that reaches the Bob's side enters the one-bit DLI which comprises of two beam splitters and an optical delay of 1-bit in one of it's paths. After interference at the second beam splitter the photon is detected by either (ideally) of the two single photon detectors obeying the laws of interference. Bob announces the time-slot where he has received the detection. Alice computes her sifted key from Bob's announcement. Bob randomly select a small fraction of keys to give an estimate of the error rate. If the error rate does not exceed the threshold error rate then Bob initiates the post processing algorithms like error correction, privacy amplification and

key reconciliation to finally generate secure keys which can be used for cryptographic purposes. Mathematically, this train of weak coherent states is represented by

$$\begin{aligned} |\psi\rangle &= \bigotimes_{i=1}^{n_p} e^{i(\phi_r+\phi_i)}|\alpha\rangle_{s_i} \\ &= \bigotimes_{i=1}^{n_p} (-1)^{s_i} e^{i\phi_r}|\alpha\rangle_{s_i} \end{aligned} \quad (1)$$

where, ϕ_r is the reference phase, ϕ_i is the phase induced on the weak coherent state $|\alpha\rangle$ by the phase modulator and n_p is the number of pulses in the coherence time. Bob can detect an event at different time-slots say j^{th} time-slot due to superposition of n_j and n_{j+1} coherent pulses. Valid time-slot is when detection occurs at $1 < j < n_p - 1$. When valid detection occurs then Alice calculates the sifted key as $s_j \otimes s_{j+1}$ and Bob's sifted key is generated from the detector which has clicked, if detector which clicks on Logic 0 (1) has detected an event then sifted key is 0 (1). Thereafter, Alice and Bob perform error correction and privacy amplification to arrive at final secure key. We can define a bosonic operator as $\hat{\psi}^\dagger = \frac{1}{\sqrt{n_p}} \sum_{n_p=0}^{n_p-1} e^{i\phi_i} \hat{a}_{n_p}^\dagger$ where, $\hat{a}_{n_p}^\dagger$ is the creation operator for a photon in time-slot n_p. We assume that the time-slots do not overlap and hence these operators can commute with each other. A weak coherent state can be written as $|\alpha\rangle_{s_i} = e^{-\frac{|\alpha|^2}{2}} \sum \frac{\alpha^n}{\sqrt{n!}} |n\rangle$, therefore, we can write the state in equation (1) as

$$\begin{aligned} |\psi\rangle &= \sqrt{P(j)} e^{ij\phi_r} \left(\frac{\hat{\psi}^\dagger}{\sqrt{j!}} |0\rangle \right) \\ &= \sqrt{P(j)} e^{ij\phi_r} |\psi_j\rangle \end{aligned}$$

where, $P(j)$ is the Poisson distribution with an average photon number $\mu_{eff} = n_p \mu$. If we consider coherence time to be infinite then we can represent the state as

$$|\psi\rangle = \left(\frac{1}{\sqrt{n_p}} \sum_{k=1}^{n_{ts}} e^{i\phi_k} |k\rangle_1 \right) \otimes \left(\frac{1}{\sqrt{n_p}} \sum_{k=1}^{n_{ts}} e^{i\phi_k} |k\rangle_2 \right) \otimes .. \otimes \left(\frac{1}{\sqrt{n_p}} \sum_{k=1}^{n_{ts}} e^{i\phi_k} |k\rangle_{ph} \right)$$

where n_{ts} is the number of pulses in the coherence time of the laser, ϕ_k is the phase of the time-slot and k is the time-slot. Let us consider that there are just 3 pulses in the coherence time, thus equation becomes $|\psi\rangle = \frac{1}{\sqrt{3}} \left(e^{i\phi_1} |1\rangle_1 + e^{i\phi_2} |2\rangle_2 + e^{i\phi_3} |3\rangle_3 \right) \otimes \ldots \otimes \frac{1}{\sqrt{3}} \sum_{k=1}^{3} e^{i\phi_k} |k\rangle_{ph}$. Basic assumption is that Eve does not possess the phase reference thus, the state appears as that to

be averaged out over the different values of phase resulting in a mixed state $\rho = \sum_{j=0}^{\infty} P(j) \left|\psi_j\right\rangle\left\langle\psi_j\right|$.

3. Eavesdropping on DPS

The average number of photons per pulse is $\mu \leq 0.1$. Thus, the number of photons is much smaller than the number of phase difference i.e. $ph < n_{ts} - 1$. We can safely interpret that the total wave-function cannot be recreated with ph measurements. Thus, security of DPS is based on the non-orthogonality of a wave-function spanned by many time-slots. This forms the basis of security of DPS QKD. We will review the security of the protocol from the perspective of realistic attacks on the protocol and security loopholes due to non-ideal implementation.

Intercept and resend attack: Intercept and resend **(IR)** attack is a type of Individual attack. Eve will have a setup similar to that of Bob. She will intersect and measure all pulses. If she detects any photon in a particular time say at t then, she will resend a pair of WCP or a photon in superposition of two pulses with similar phase difference between them. If Bob measures them at that particular time then, he cannot detect Eve but if he detects them at times $t \pm 1$ then it induces 25% error at Bob's detection setup. If Eve attacks only $4e$ of the photons, then Eve can learn $2e$ of the fraction and will not have any information from a fraction $1 - 2e$.

Beam splitter attack: In beam splitter attack (BS) [5], Eve will place a beam splitter in the quantum channel (as the name goes). Eve has to apply a strategy which can have a lossless channel or substitute the quantum channel from beam splitter to Bob by a lossless channel. She will obtain the fraction of photons equal to channel loss without disturbing the communication rate. The probability that Eve will know the value of bit at a particular time given Bob detected a photon at that time is $\mu(1 - T) \approx \mu$ without quantum memory and $2\mu(1 - T) \approx \mu$ with quantum memory, where T is the transmission efficiency of channel.

Photon-number-splitting attack: In Photon-number-splitting (PNS) attack [6], Eve measures the photon number using state preserving operation. She can store $\mu_{eff}T$ in her quantum memory and send $\mu_{eff}(1 - T)$ to Bob. She will measure it after Bob reveals the time of detections. How much information is gone to Eve from each photon she stores? If Eve has k photons then she has k copies of the state $\hat{\psi}^{\dagger}|0\rangle$ which she can measure later. Eve entangles her probe with the sent photons and measures this probe after Bob's announcement. This is a

general positive-operator valued measurement (POVM) attack on single photons. Since, Eve does not know the phase reference hence it will be sent as

$$\rho = \sum_{\phi_1 \phi_2 \ldots \phi_k} p(j\phi_1\phi_2 \ldots \phi_k) \left|\psi_j\right\rangle\left\langle\psi_j\right|$$

Comparison with BB84

1. In DPS QKD Eve's information from PNS attack is independent on channel loss. It is a function of μ. Final key rate decreases linearly with channel loss. Hence its robustness against PNS attack is evident.
2. In BB84, Eve's information from PNS attack is dependent of channel loss. Thus, if losses are higher then Eve can send multi-photon fractions and stop single photon states. In other words as loss increases Eve can have information over large fraction of key. Hence, final key rate is a quadratic function of channel loss. In Fig. 2 we have shown the key rates with distance for an ideal source, weak coherent source and decoy for BB84 and compared it with DPS QKD (considering restricted attack) using standard experimental parameters.

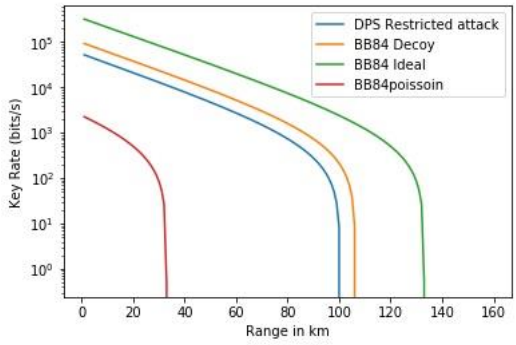


Fig. 2. Key rates with distance for BB84 and DPS QKD

Sequential attack: Sequential attack (SA) [7] is a type of IR attack. Eve places measurement device very close to Alice. She waits for k consecutive clicks and then constructs $k+1$ time-slot state. The error induced by it is $e_{seq} = \frac{1}{2(k+1)}$. This happens because of probability of measuring side time bins is $\frac{1}{(k+1)}$ hence error is $\frac{1}{2(k+1)}$. The probability of k consecutive clicks is $p_k = \mu^k$. Therefore, probability of observing k consecutive clicks decreases with k consecutive

clicks. Eve needs to conserve overall detection rate thus, $p_k \geq \mu T$. This gives an upper bound for k. Eve knows anything if it clicks for $2 < k < k+1$ with probability $\frac{1}{k+1}$. (since k and $k+2$ will give random result). The average collision probability is $P_c = P_{c_0}^n = \left(\frac{1}{2}\right)^{n(1-2ke)}$. Compression factor is $\tau = \frac{\log_2 P_c}{n} = 1 - 2ke = 1 - 2e\left(\log_\mu T + 1\right)$. According to a study [3,7] it is advantageous to do individual attack (IA) than SA and that security against IA implies security against SA. Eve can employ different strategies to reduce the error rate. She can modulate the envelope of the pulse block so that the amplitudes of the end pulses are smaller than that of the central pulses. A lot of research has been done on sequential attacks on DPS QKD. Several studies have been reported on sequential attacks. However, the strategy [8] that utilizes Unambiguous State Discrimination (USD) for phase differences and optimized pulse envelope, is considered threatening for long-distance DPS QKD. However, to combat this attack, solutions like decoy strategy and strategic phase modulation at Alice Node can be exploited to combat the sequential attacks based on intensity modulation.

Unconditional security: Coherent attacks are the most challenging attack on any QKD systems and the security against it is difficult to prove. Several studies have been reported on different strategies of coherent attack on DPS QKD where they attack: pairs of adjacent pulses, noiseless DPS QKD and block randomization. In [3] it is analyzed that COW and DPS are similar in QKD performance however, DPS is somewhat better than COW [9]. The scientific proof of any QKD protocol is dependent upon construction of the QKD scheme and in it's realistic implementation. In every security proof some assumptions will be considered and it is very important to see that these assumptions do not open any security loophole from product perspective. It is to be noted that unconditional security by coherent state based DPS QKD is proven in [10] using complementarity approach.

Quantum Hacking: There are certain demonstrations of quantum hacking on DPS QKD based on inefficient detectors. These hacking [11,12] can fall into IR attack. It exploits the drawback like detector efficiency mismatch, functioning of detector, thermal effects etc. These are basically the side channel attacks. These can be prevented by effective monitoring of the transmission and error detection. Security patches i.e. by strategic detection setup, adding optical components at Bob's side, monitoring the power, are effective in preventing such hacking. Eve

also needs to plan execution of such attacks for which she makes some assumptions of the QKD system. We can conclude that these side channel attacks can be detected by proper countermeasures and effective monitoring.

4. Experimental setup

In Fig. 3, we have shown the experimental setup, we have used a 1550 nm continuous wave laser. It is passed through Lithium Niobate $(\mathrm{LiNbO_3})$ Intensity Modulator (IM) to generate 1 GHz train of pulses with 400 ps width. Chromatic dispersion of DLI is 1 ps/nm and SMF fiber is 18 ps/(nm.km). We find that the chromatic dispersion has negligible effect. The train of pulses are phase modulated by $(\mathrm{LiNbO_3})$ based phase modulator at random and thereafter, strongly attenuated using variable optical attenuators (VOA). The weak coherent source is then passed through the quantum channel which is a standard telecommunication fiber to reach Bob. The random numbers for phase modulation are generated from a random number generator (PRNG). The train of WCP travel to Bob system via QC. At Bob's side we have a Mach-Zehnder interferometer with 1 ns delay which is fine tuned to match the path difference between consecutive WCPs to cause interference.

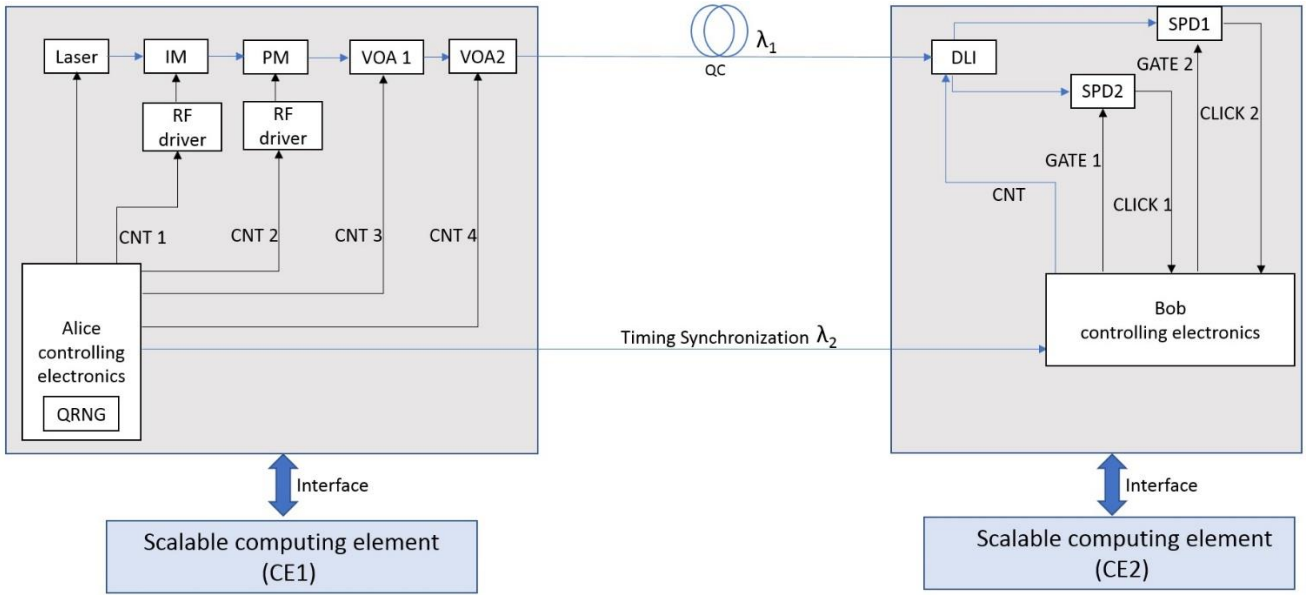


Fig. 3. Experimental setup

The WCP are randomly detected by single photon detectors. Probability of detector getting clicks is $p_{click} = p_{sig} + p_{dark} - p_{sig}p_{dark}$. However, the probability of simultaneous click due to

signal and dark count i.e. $p_{sig}\, p_{dark}$ is very small. Therefore, $p_{click} \approx p_{sig} + p_{dark}$. The probability of signal p_{sig} is μT, where the channel transmission is given by $T = \eta 10^{-\frac{(\alpha L + L_{DLI})}{10}}$, α is the fiber attenuation, L is the distance and L_{DLI} is the total loss from Bob's optics. The Quantum Bit Error Rate (QBER) is an important parameter in QKD protocol and it depends on the electronics, optical error and detector parameters. We have considered following errors

$$QBER_{Total} = QBER_{opt} + QBER_{\text{phasejitter}} + QBER_{\text{darkcount}} + QBER_{\text{Jitter}}$$

The total $QBER_{Total}$ is estimated to be 3.9%. The secure key rates for DPS QKD is given by $R_{sec} = R_{sif}\big(\tau + f(e)h(e)\big)$ where sifted key is obtained by $R_{sif} = \mu T \nu$. Secure key rate considering realistic attack (IR attack and BS attack with quantum memory) is given by $R_{sec} = R_{sif}\big(1 - 2\mu(1-T) - 2e + f(e)h(e)\big)$. Secure key rate considering general individual attack (PNS attack) is given by $R_{sec} = R_{sif}\left(-\big[1 - [2\mu(1-T)]\big]\log_2\left[1 - e^2 - \frac{(1-6e)^2}{2}\right] + f(e)h(e)\right)$. Secure key rate for sequential attack is given by $R_{sec} = R_{sif}\left(1 - 2e\big(\log_\mu T + 1\big) - f(e)h(e)\right)$. We have calculated the sifted and secure key rates based on the experimental parameters shown in Table 1a. In Fig. 4, we have presented a test case where we have shown the SPD counts when Alice sent Logic 0 continuously (00000 i.e. a fixed pattern). We find that port 1 is always giving constructive interference while port 2 is always giving destructive interference. When we change to 01010 pattern from Alice side, we find that port 1 always shows destructive interference and port 2 shows constructive interference, this is shown in Fig. 5. After generating secure keys, we have ensured the randomness of the key through NIST test suite [13] because the keys will be used for cryptographic purposes. In Fig. 6, we have shown the NIST test results on the keys after key reconciliation process. The computing elements CE1 (Alice side) and CE2 (Bob side), address the sifting, authenticity, error correction, privacy amplification and reconciliation activities. This subsystem also implements quantum enabled Internet Protocol Security (IPsec) and VPN protocols for communicating between Alice and Bob over a standard internet network. In Fig.7, we have shown the sifted and secure key rates for different distances. We have also specified the key rates in Table 1b.

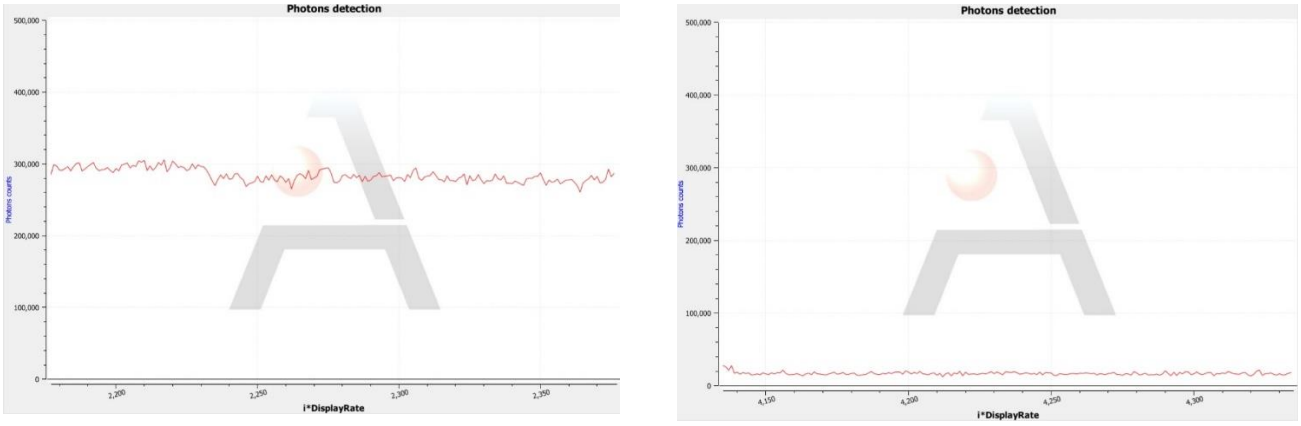
Parameters	values
Mean photon number	0.1
Pulse width of WCS	400 ps
Optical loss at Bob	4 dB
Dark count	10000 Hz
Pulse repetition rate (ν)	1 GHz
Detector efficiency	10 %
Dead time	$1\mu s$
After pulse probability	0.1 %
Fiber attenuation	0.2 dB/km

(a)

Distance (km)	Sifted key (kbit/s)	Secure key rate	
		Restricted (kbit/s)	Individual (kbit/s)
20	1585	694	326
40	631	271	122
60	251	104	41
80	100	37	9
100	40	11	-

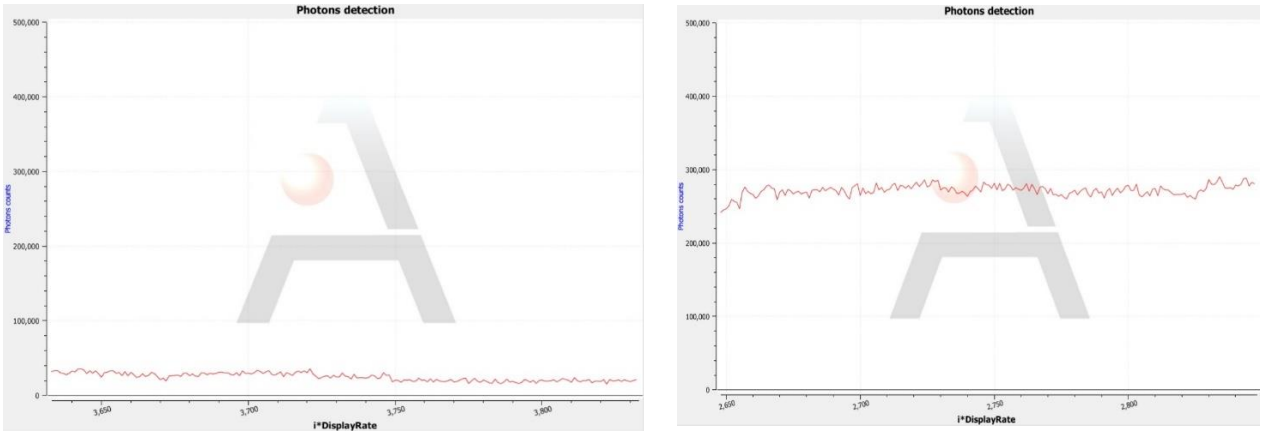
(b)

Table 1. (a) Parameters of critical components in the QKD experiment and (b) Summary of QKD experiment



(a) (b)

Fig. 4. Counts at (a) port1 and (b) port2 of the DLI when Alice raw keys has generated only logic 00000 (fixed pattern is given).



(a) (b)

Fig. 5. Counts at (a) port1 and (b) port2 of the DLI when Alice raw keys has generated only logic 010101 (fixed pattern is given).

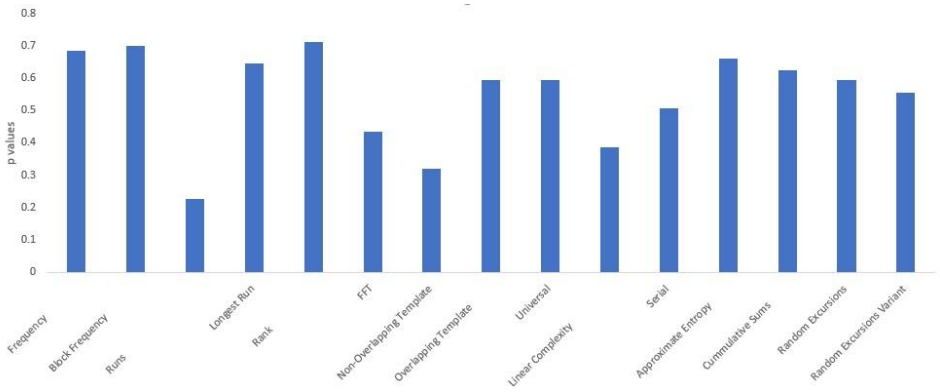


Fig. 6. Results of the NIST tests applied to the final secure keys.

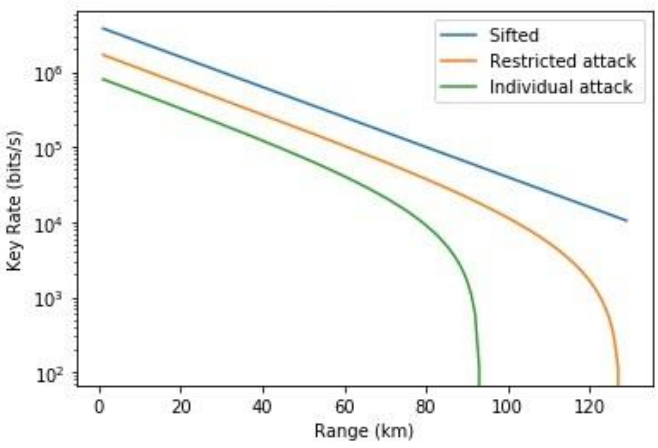


Fig. 7. Key rate vs distance for DPS QKD

5. Quantum safe network

Transforming present network security into quantum-safe is one of the biggest challenges faced by International standardization bodies like ETSI, NIST, CSA etc. The QKD has been successfully demonstrated, deployed, and applications in industry and government are growing. We present below application and scenarios from technical perspective. We have presented the integration of our product with commercial router thereby demonstrating point to point QKD within 40 km.

Application1: Key generation in a QKD network

QKD network comprises of multiple nodes that are connected to form a quantum network. With our present system we can generate secure keys at a modest rate till 80 km. The nodes may contain multiple ‘Alice’ and ‘Bob’ combinations depending on the network topology. These nodes contain QKD stack that communicates with the adjacent nodes and learns about the routes required for reaching other nodes. The information transfer needs to happen between entities R1 and R3, which has to be encrypted. R1 requests key from QN1 for encrypting the data. QN1 passes key K1 to R1. R3 will request QN4 for corresponding key. QN1 finds the route to QN4 through the network (QN1-QN2-QN3-QN4). Using quantum hopping technique, key gets transferred to QN4. QN4 further transfers key K1 to R3. R3 after receiving the key K1 from QN4, decrypts the information.

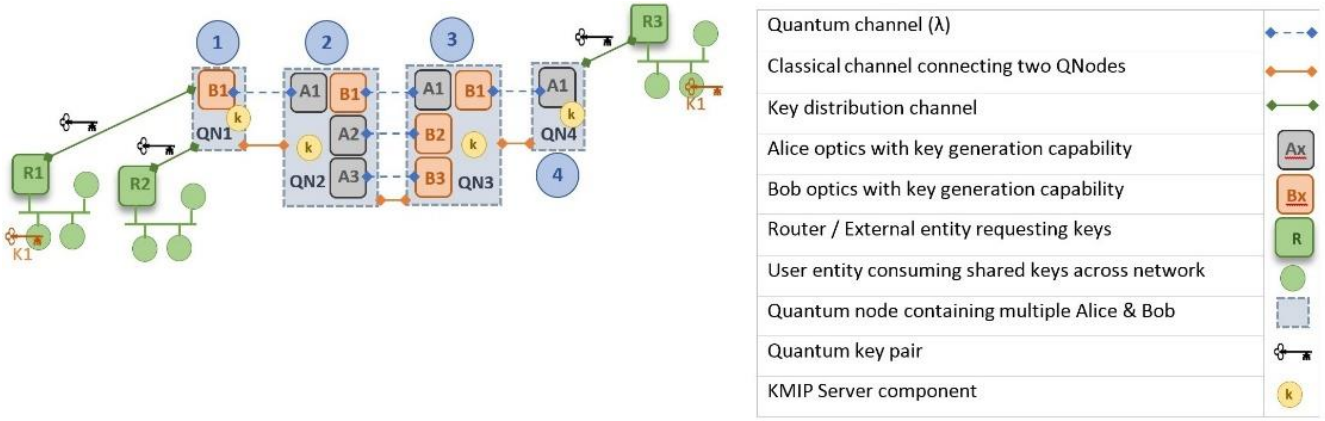


Fig. 8. QKD network with trusted nodes

We have configured our system for implementation of the trusted node concept [14] as presented in Fig. 8 to increase the distance. The scalability of the computing element and flexible

architecture in our product allowed us to evaluate point-to-multipoint QKD networking and multi-hopping scheme integration of classic cryptography with quantum cryptography to ensure quantum-safe key management across all different layers of information and communication technology.

Application 2: Quantum key transportation between end applications

To understand the key transfer from one quantum node to the other, where two end applications are asking for the quantum keys between them, consider the scenario depicted in figure. In this scenario, user ‘A’ wants to communicate with a user ‘B’ securely. The Quantum key (QKey) from quantum node (QN1) is produced and transported to the end quantum node (QN3). Application ‘A’ ask for a QKey to QN1 via KMIP interface. The QN1 finds the route to reach ‘B’ and selects best route via QNs QN1→QN2→QN3. QN1 generates QKey ‘K1’ with QN2. QKey ‘K1’ is passed to R1. QN2 and QN3 creates VPN using Qkeys with strengthened hash function. After which using OTP1 send key ‘K1’ to QN3. QN3 transfers QKey to R3.

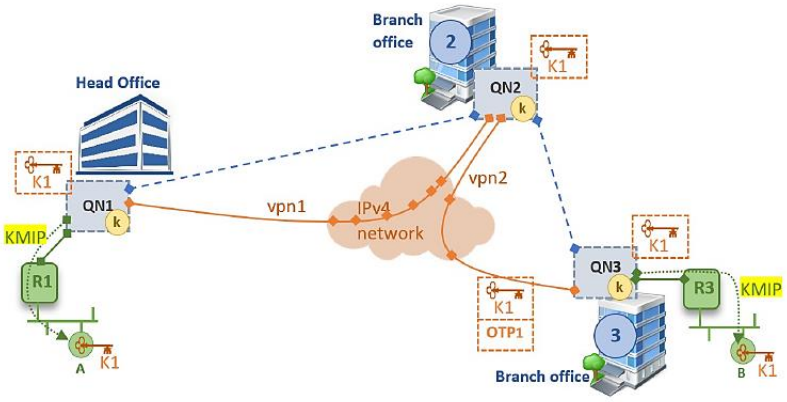


Fig. 9 Quantum key transportation between end applications

Application 3:

We have implemented a few solutions based on ETSI recommendations [15].

Layer 2

1. As a key exchange protocol for PPP.
2. In IEEE 802.1MACsec

3. QKD link-encryptor for encrypting traffic on an Ethernet of fiber channel link
4. QKD link-encryptor as VPN tunnel

Layer 3 IPsec defines the architecture for security services for IP network traffic. It includes 3 main protocols: Internet Key Exchange protocol (IKE), Authentication Header protocol (AH) and Encapsulating Security Payload protocol (ESP). IKE is used to manage the cryptographic keys and also initiate the security associations required for the secure data transfer. AH and ESP will provide the necessary integrity and confidentiality required for the data being transferred. QKD solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of quantum physics. So, to combine the advantages of QKD with the structure of the IPsec, the key exchange in IKE (Phase 1 and 2) should be replaced by the QKD system to provide the secure key on both end points. These keys can be used to create a session (Handshake) between the two nodes with the Security associations discussed and also the authentication and encryption supported by these keys. The DH, RSA are the currently used public key exchange algorithms that depend on the computational complexity of factorization of the multiplication of two huge prime numbers, which increases exponentially with the size of the prime number. This complexity can be brought down exponentially using Shor's algorithm after the onset of quantum computers, thus making the key exchange unreliable. Also, the current standard method of hashing (SHA2) is an extended version (increased tag length from 160 to 256) of the already failed SHA1 algorithm which had a weak collision avoidance probability. This should be replaced by an Information theoretically secure universal hashing algorithm which provides for the mapping of every key bit used for the authentication with every bit of the message thus providing maximum randomness for the input key length. Modified IKE to provide shared session keys for security association in IPsec protocol.

Application 5: Practical demonstration for point to point QKD

Layer 4 (session keys): We have successfully integrated our QKD with a commercially available router and this is shown in Fig. 9. The keys are requested by the source router as and when needed. The quantum node at the source end provides the key to the source router along with the key ID. The source router communicates the key ID to the destination router. The destination router conveys the key ID to the QKD unit at the destination site. The destination QKD passes

the corresponding key. In this technique, both the source router and destination router will refer to the same key in a secure way while encrypting data-in-transit.

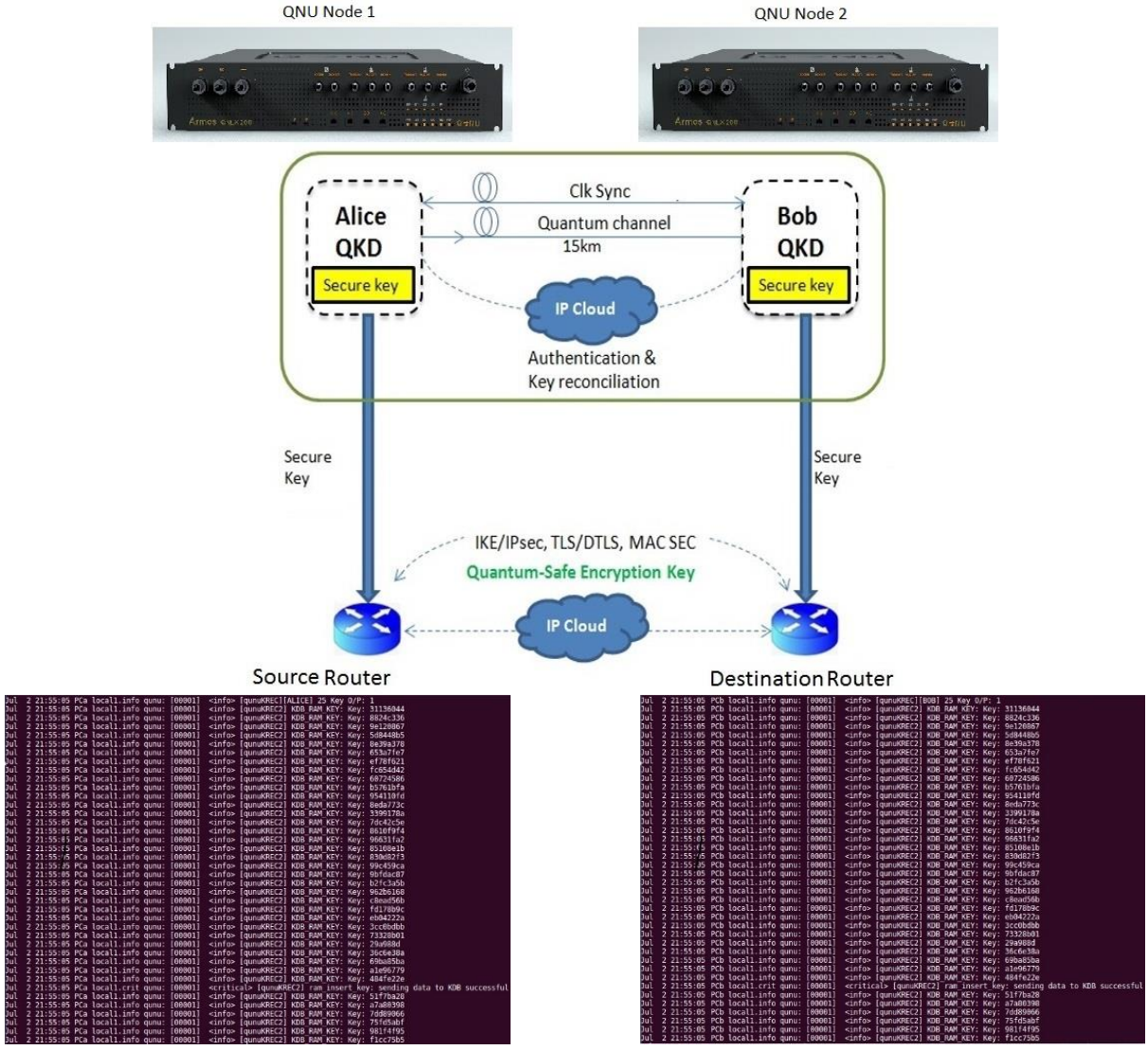


Fig. 10. Integration of QNu QKD with commercial routers cum encryptor

Application 4: Highly secure

In Fig. 11, we have presented an application for secure defense communication. The entire network can be quantum secured in the prescribed manner which is connected from Army Office 1 to Army Office 2. The quantum channel and classical channel are depicted differently as they serve different purposes. The keys generated by QKD are symmetric and information theoretic

secure with composable security framework. This will be shared securely to encryptor/decryptor, which can then be shared with different applications that will want to access the keys.

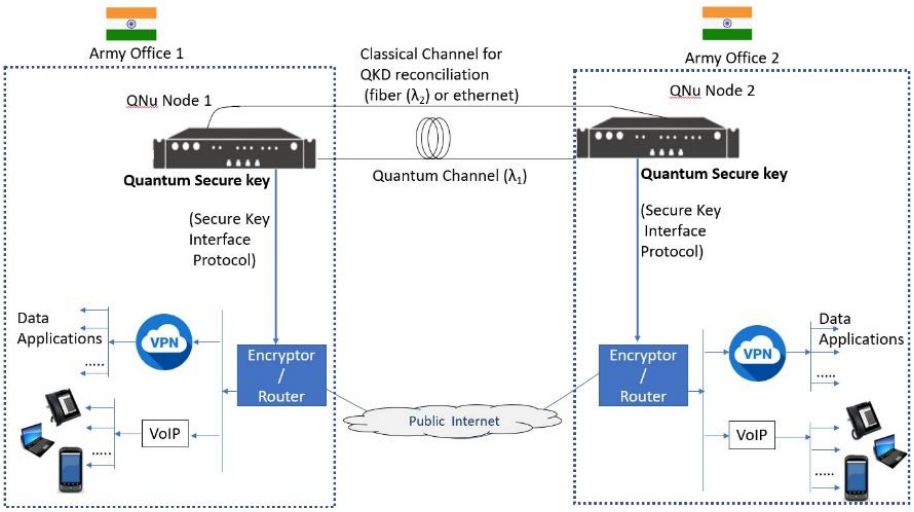


Fig. 11. QKD point to point communication between two Office

5. Conclusions

We have performed a 1 GHz pulse rate DPS-QKD experiment utilizing InGaAs detectors. We have successfully generated random quantum keys which can be used for any cryptographic purposes. We have also discussed the present security status of DPS QKD including theoretical and implementation security. This protocol is recognized by ETSI and is in the process of becoming as one of the standards for QKD protocol. We have also brought forth the requirement for transition from current cryptosystem into quantum safe encryption as per the ETSI recommendations. We particularly emphasize on transition of classical network security to quantum-safe network security and moving forward in that direction we have reported the integration of our system with commercial router and successfully performed data transmission from a source router to a destination router.

References

1. Renner R.,König R.: Universally composable privacy amplification against quantum adversaries. Proceedings of the Second international conference on Theory of Cryptography TCC'05, 407--425 (2005)

2. Bennett C. H., Brassard G.: Quantum cryptography: public key distribution and coin tossing. Proceeding of the IEEE International Conference on Computers, Systems and Signal Processing, 175-179 (1984)
3. Inouye K.: Differential Phase-Shift Quantum Key Distribution Systems. IEEE Journal of Selected Topics in Quantum Electronics (2015)
4. Bennett C. H., Brassard G., Crepeau C., Maurer U. M., Generalized privacy amplification. IEEE Trans. Inf. Theory **41** (6), 1915--1923 (1995)
5. Inoue K., Waks E., Yamamoto Y.: Security of differential-phase shift quantum key distribution against individual attacks. Phys. Rev. A **73** (7), 012344-1--012344-9 (2006)
6. Inoue K., Honjo T.: Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. Phys. Rev. A **71** (4), 042305-1--042305-4 (2005)
7. Curty M., Zhang L. L., Lo H. -H., L¨utkenhaus N.: Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states. Quant. Inf. Comput. **7** (7), 665—688 (2007)
8. Gomez-Sousa H., Curty M.: Upper bounds on the performance of differential-phase-shift quantum key distribution. Quantum Inf. Comput. **9** (1/2), 62--80 (2009)
9. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H.: Fast and simple one-way quantum key distribution. Appl. Phys. Lett. **87** (19), 194108-1--194108-4 (2005)
10. Mizutani A., Sasaki T., Kato G., Takeuchi Y., Tamaki K.: Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity. Quantum Science and Technology **3** (1), 2017
11. Lyderson L., Skaar J., Makarov V.: Tailored bright illumination attack on distributed-phase-reference protocol. J. Mod. Opt. **58** (8), 680—685 (2011)
12. Curty M., Tamaki K., T.: Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks. Phys. Rev. A **71** (77), 052321-1--052321-20 (2008)
13. Juan S.: Statistical Testing of Random Number Generators. NIST company (2012)
14. Elliott C.: Building the quantum network. New J. Phys. **4**, 46.1--46.12 (2002)
15. Quantum Safe Cryptography; Case Studies and Deployment Scenarios, ETSI GR QSC 003 V1.1.1 (2017-02)