WHITE PAPER

EMINENCE OF QUANTUM KEY DISTRIBUTION

Document Version: 1.1

Author: Anindita Banerjee

Reviewers:
Mr. Mark Mathias
Prof. Anil Prabhakar
Mr. Ravie Menon
Miss Prithvi Kini

Contents

1 Executive summary

Development in the different facets of quantum information and quantum computing is changing the perception of information. The information which is coded in 0 and 1 in a classical computer is coded in 0, 1 and both 0 and 1 simultaneously in a quantum computer. The ability to exist in multiple distinct states simultaneously is the prime advantageous resource in quantum computation. There are certain quantum algorithms that can substantially outperform their classical counterparts, for eg. Grover's algorithm provides quadratic speedup in database searches and Shor's algorithm solves factorization problem. This causes a major concern because today's state-of-art cryptosystem is based on cryptographic algorithms such as RSA, Diffie-Hellman, ECC for distribution of symmetric keys. The strength of these cryptographic algorithms is based on mathematical complexity. This is referred to as computational security and it implies that a given secret is safe within the limits of existing technology for a limited period of time. The present-day cryptosystem was not developed from the perspective of a futuristic technology, that could provide huge computational resources. The primary concern for the consumer is that a hacker could copy unlimited encrypted data in motion and wait for a superior computational machine, which could very well be a quantum computer. Recent accomplishments in quantum experiments and global efforts towards quantum supremacy have posed a substantial threat to the existence of today's state-of-art cryptosystem. Global industries and governments are investing in labs to build a large-scale quantum computer that can perform tasks in a superior manner compared to its classical counterpart. Once a large-scale quantum computer capable to decode the conventional cryptosystem, is built, it would lead to the collapse of the entire public cryptosystem like a house of cards. Government security agencies of US and UK, standardization bodies such as European Telecommunications Standards Institute (ETSI), National Institute for Standards and Technology (NIST), International Organization for Standardization (ISO) and Cloud Security Alliance (CSA) believe that transition to "quantum-safe encryption" is inevitable. Quantum-safe implies being resistant to attacks by the quantum computer. There are cryptographic algorithms called Post-Quantum Cryptography (PQC) or Quantum Resistant Algorithm (QRA) that are quantum resilient. Quantum Key Distribution (QKD) is an essential approach of quantum-safe. It delivers a secure key by eliminating the possibility of an eavesdropper in the key distribution channel (quantum transmission). The key is encoded in the quantum properties of light thereby making it impossible to copy the state without disturbing it. The importance of laying the foundation of a cryptosystem on quantum key distribution is applicable not only in the post-quantum era but also in the pre-quantum era. In the pre-quantum era, although cracking an encryption algorithm is intractable, they can become redundant if the key is compromised. Thus, ensuring the safety of the key becomes paramount and it can be guaranteed by QKD. Additionally, it will help in frequently refreshing the key, thereby establishing a robust key management system. According to the experts and international standardization bodies, the arrival of a quantum computer is estimated to be within 5 to 10 years, therefore, the transition time is now. Establishing a cryptographic system incurs a physical cost and time. If the sum of the time of transition to quantum-safe architecture and shelf life of confidential document is more than the arrival of a large-scale quantum computer then there will be an apocalypse [1]. We believe that rather than playing the gamble of arrival we should work towards quantum-safe transition. QuNu's white paper aims individuals from various background, about the imminent quantum technology and its impact on state-of-art cryptosystems. Today, we are on the cusp of this transition, with global digi-

tization and the increasing need for data security in sectors such as Government, Intelligence Agencies, Defence, Finance and Healthcare, the move to "Quantum-safe cryptosystem" is imperative.

2 Cryptography

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 architecture of a cryptosystem is presented in Figure 1. It comprises of two or more parties sharing an encrypted message. The message (plain text) 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.

2.1 Symmetric key cryptography

Symmetric key cryptography is a cryptographic algorithm that uses the same keys for encryption and decryption. The most commonly used algorithms are One-Time Pad (OTP), Data Encryption Standard (DES), 3-DES, Advanced Encryption Standard (AES) etc. The OTP is the only symmetric key cryptographic algorithm that provides information theoretic security. In this case a key equal to the length of a message is XORed with the message. However, this requires long key length and greater time to process. The other symmetric algorithms require a relatively lesser key. Symmetric key cryptography is primarily used for bulk encryption of data from point-to-point and can be easily implemented in a hardware. One major drawback is that the key management of symmetric algorithm is tedious and prone to breaches by malicious actions. This is where QKD when implemented adds an additional layer of security.

2.2 Public key cryptography

A major problem is faced when you need to setup secure keys to encrypt data transmission with an unknown party, this is where Public Key Cryptography (PKC) comes in. In PKC the message is encrypted using a public key and decrypted using a private key. This cryptographic algorithm relies on mathematical complexity i.e. functions which are easy to compute but requires an infeasible amount of computational resources to invert e.g. factorization (RSA), discrete logarithms (Diffie-Hellman, DSS) and elliptic curves (ECC). PKC guarantees the authenticity of the message. It is used in digital signatures, email encryption software (PGP, MIME), SSL protocol, SHL protocol etc. The PKC has some limitations in terms of slow speed and capability to encrypt only smaller size of data. However, its advantage lies in the fact that the key distribution can be done in public. Practical deployment of PKC is through the Public Key Infrastructure (PKI) that requires a trusted third party for certification. Finally, PKI can be used to share secret keys which can then be used for encryption through AES or OTP. The PKC has paved the way for a pragmatic approach to key distribution.

2.3 Key distribution

In any encryption algorithm, the security lies in the secrecy of the key. The distribution of the keys is very critical as they need to be shared by the legitimate parties, without divulging the keys to an adversary. A simple way to do this is to meet in person and share the key. This system is currently prevalent in high-level security applications. Conventional cryptosystem mostly rely on PKC which is vulnerable to the human ingenuity, increased computational power, and quantum code breaking. These three weakness imply that the PKC cannot provide higher shelf life to highly confidential government documents and trade secrets. An adversary can store the encrypted messages in 2018 and decode later say 2033 when it will

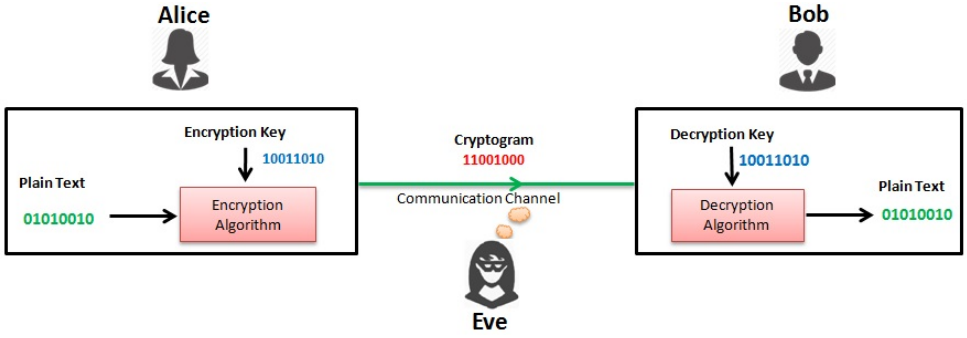

Figure 1: Schematic of cryptosystem

be able to factorize large numbers on a quantum computer.

3 Quantum computing

The quantum information refers to the information encoded in a quantum state called qubits. Qubits can exist in logic 0, logic 1 and in a superposition of both. To visualize the potential of superposition we can extend the idea to an n-qubit system which will enable us to store information in 2^n states. In quantum mechanics the principle of superposition enables parallel computation which enables a quantum computer to outperform certain tasks than a classical computer. Quantum computation refers to the processing of quantum algorithm on a quantum hardware which is a quantum machine governed by the laws of quantum physics. According to Feynman [2] quantum mechanical system cannot be efficiently simulated in a classical system. Thus, we need a quantum machine (quantum computer) to run a quantum algorithm.

3.1 Impact of a quantum computer on cryptosystem

In 1994, P. W. Shor [3] introduced a quantum algorithm for finding the prime factors of an integer. This would mean that if we have a multipurpose quantum computer that can implement Shor's algorithm, it will immediately render present cryptographic systems which are based on mathematical complexities ineffective. Another quantum algorithm is Grover's algorithm [4] which is used for unsorted database search. It can perform exhaustive key searches. This will have a crucial effect on the length of the key being used in public key cryptography. Statistically, to crack a key by brute force method involving a key which takes N different combinations is given by N/2. Applying Grover's algorithm, this gets speeded up in a quadratic fashion and require only $\sqrt{N}$ iterations. We know that the strength of the security of a cryptographic algorithm is primarily dependent on two factors, nature of algorithm and key size. In Table 1 we have presented a comparison for maximum security strength provided by prevalent cryptographic algorithms in a classical computer and a quantum computer, respectively. The symmetric key systems like AES can still be used with a greater length of key to provide a near equivalent layer of security as of today. We can improve the security level multi-fold by changing the key as frequently as possible. With QKD systems in place, keys can be changed every few minutes in need be, therefore, a combination of QKD with symmetric key systems is a viable post-quantum solution.

4 Quantum-safe cryptography

Quantum-safe cryptography [1] refers to a cryptosystem which is resilient to attacks by any quantum algorithm. Post-Quantum Cryptography (PQC) refers to the classical algorithms which will be resilient to quantum com-

Cryptographic algorithm	Strength on a classical computer (bits)	Strength on a quantum computer (bits)
RSA-1024	80	0
RSA-2048	112	0
RSA-3072	128	0
ECC-256	128	0
ECC-384	192	0
AES-128	128	64
AES-256	256	128

Table 1: Impact of quantum computer on state-of-art cryptosystem [1, 5].

puters. Some post-quantum primitives such as lattice, hash-based cryptosystem are only believed to be quantum-safe unless proven otherwise. Irrespective of the level of security of the algorithm, if an adversary can obtain the keys by any means, it will get compromised. It is therefore imperative to safeguard the key or ensure unconditional security of the key. This is provided by QKD. Quantum key distribution considers the adversary to be arbitrarily powerful. The hybrid approach encompasses both classical and quantum-safe techniques for delivering security of the highest level and timeless duration. It is a prerequisite for any infrastructure/company which, relies on PKC and long-term security, to switch to quantum-safe infrastructure. As per ETSI [1], "Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure". Hence, it is essential to take steps towards building a future-proof cryptosystem. It is mentioned in the NIST SP 800-57 [5], in the Recommendation for the Key Management, "If quantum attacks become practical, the asymmetric techniques may no longer be secure". In this scenario, PQC and QKD will be the only solutions that can provide long shelf life to encrypted data.

5 Quantum key distribution

Quantum key distribution is a state-of-art key exchange mechanism that ensures elimination of every possible threat of eavesdropping or

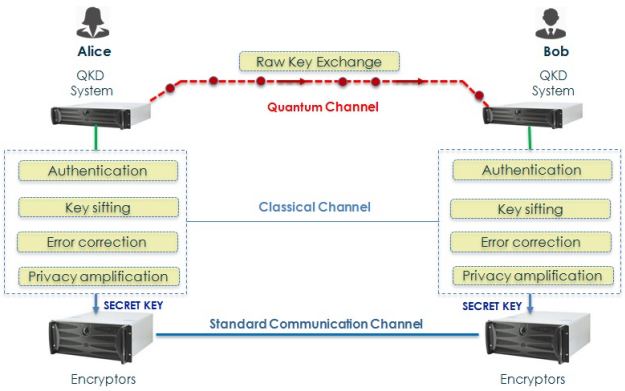

Figure 2: Quantum key distribution configuration

leakage by treason, to make the key secure. It establishes a secure link between two points with a specified distance. The key exchange is done by encoding binary key on the properties of quantum particles and sending them across through a quantum channel. This is done right under the presence of an eavesdropper and any attempt to eavesdrop gets detected by virtue of the properties of quantum mechanics. It states that any act of measurement ends up in changing the system which reflects as errors in the key sifting process. After the raw key exchange both the parties agree on an elaborate method of key distillation which is described later. Since the 1980s, starting from a theoretical concept to moving in research labs and presently, the QKD has entered the commercial domain. Today, several quantum network demonstrations have been successfully realized in many parts of the world.

5.1 QKD is quantum-safe

Quantum key distribution is quantum-safe. The adversary is bounded not by the technology but by the laws of physics itself. QKD does not rely on the mathematical assumptions. Considering the huge potential of the adversary i.e. ideal and advanced (futuristic), QKD ensures that the key obtained through QKD is safe to be used for long-term confidential applications. The fundamental laws of quantum mechanics like Heisenberg's uncertainty principle and No-cloning theorem enable effective monitoring of the key distribution channel against eavesdropping. According to Heisenberg's uncertainty principle, measuring the key data causes perturbation in the system. The No-cloning theorem prohibits duplicating the quantum state. The security of QKD is governed by the laws of quantum physics. The QKD is a perfect solution for the key distribution problem. Therefore, all information protected by quantum key distribution will be secure forever. The QKD technology is a potential candidate for quantum-safe cryptography.

5.2 QKD configuration

The QKD system is presented in Figure 2. The sender is referred to as Alice, the receiver is referred to as Bob and Eve is the adversary. Eve has access to unlimited resources facilitated by quantum physics.

1. Alice and Bob share a pre-authenticated classical channel (IP/Ethernet network).
2. Alice encodes the binary numbers generated by an efficient random number generator on the quantum properties of the light such as polarization, phase etc.
3. Alice sends the quantum objects called qubits over a quantum channel.
4. Quantum channel is a medium through which light propagates with some losses. It can propagate through standard optical telecommunication fiber or it can propagate through free-space.
5. Bob performs quantum measurement in a manner stated by the key distribution protocol on the received qubits.
6. The raw key then undergoes the sifting process in which photons with same bases (criteria will differ for different QKD schemes) are selected and rest of them are discarded resulting in a sifted key.
7. Alice and Bob check whether the quantum channel is being eavesdropped by measuring the quantum bit-error rate. If there is no eavesdropping then the process continues, else, it is terminated. The sifted key will have errors which are generated either by an eavesdropper or occurs due to imperfections in the QKD device and transmission line. Error correction is a process where Alice and Bob with given sifted key arrive to a common sequence. There are different methods for error correction such as Low Density Parity Codes (LDPC), cascade, winnow etc. During error correction classical information is exchanged which leads to leakage of information.
8. Further security is provided by privacy amplification. The sifted key is further processed to final key by compressing the key to an appropriate factor. This process decreases the mutual information between Alice and eavesdropper and enhances the security of the key.

6 QKD protocols

There are several QKD protocols [6]-[10] proposed till date (see references in [11]). Regardless of the progress in theoretical and experimental domain, practical QKD implementation is faced with following challenges:

1. communication rate
2. distance

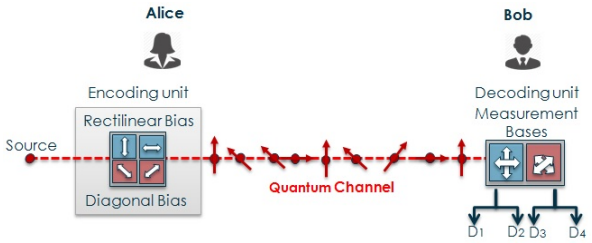

Figure 3: Schematic of BB84

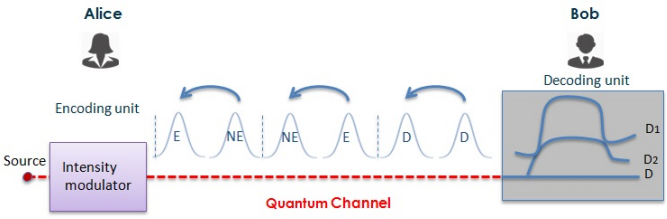

Figure 4: Schematic of COW-QKD

3. low-cost and

4. robustness.

The key rate is heavily dependent on the detection procedure. In order to achieve high key rate the single-photon detection techniques will require high efficiency and short dead-time of the detectors. The range of the QKD system is dependent on the type of detection system particularly its parameters like noise, operation temperature etc. The cost and robustness can be addressed on the basis of integration of the QKD system. It is to be noted that the security of a protocol is determined by the nature of attacks considered in the corresponding security proof. In this section, some of the quantum key distribution protocols are summarized.

6.1 BB84

In 1984, Bennett and Brassard [6] proposed the first QKD scheme which was based on polarization encoding and came to be known as BB84. A schematic for BB84 is presented in Figure 3. Alice and Bob are two legitimate users with a prior shared quantum channel and authenticated classical channel. Alice sends a sequence of randomly polarized photons in different polarization states (from two conjugate bases) to Bob over a quantum channel. Bob randomly selects a basis and measures the state. He keeps a note of the resultant state and the basis selected for measurement. Bob broadcasts his measurement bases. Alice and Bob thereafter discard the results for which mismatched bases were used and thereby generate a sifted key. They compare the error rate with threshold and verify the presence of an eavesdropper. If there is no eavesdropping, they perform classical post-processing steps which include error correction and privacy amplification. Finally they share a secure key.

6.2 Coherent one-way QKD

D. Stucki *et al.* [8] proposed Coherent One-Way QKD (COW-QKD) based on time encoding. The experimental setup is presented in Figure 4. COW-QKD is simple in configuration and tolerant to reduced interference visibility. It is robust to PNS attacks. It generates a higher secret bit rate. Alice sends coherent pulses that are either empty (E) or a non-empty (NE) having a mean photon number $\mu < 1$. Logic 0 is encoded when two sequential pulses are NE-E and logic 1 is encoded by E-NE. Alice can send decoy sequences NE-NE to step up the security of the protocol. Bob retrieves the key by measuring the time-of-arrival of the photon on a detector. He measures the coherence between consecutive non-empty pulses with the interferometer to check eavesdropping.

6.3 Differential phase shift QKD

Differential Phase Shift QKD (DPS-QKD) was proposed by K. Inoue *et al.* [9]. The schematic of DPS-QKD is presented in Figure 5. Alice randomly phase-modulates a pulse train of weak coherent states by $\{0, \pi\}$ and transmits it to Bob. Bob measures the phase difference between two consecutive pulses using

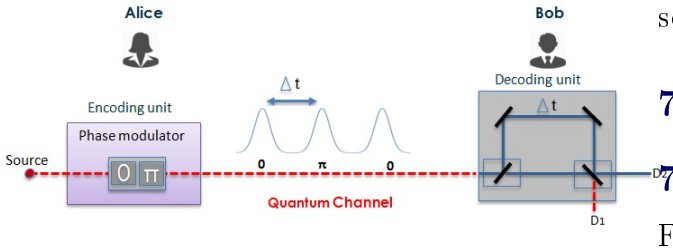

Figure 5: Schematic of DPS-QKD

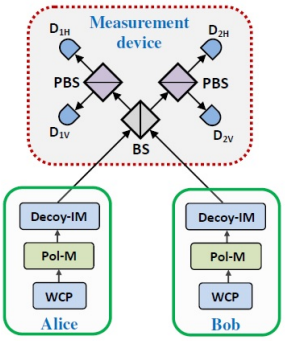

Figure 6: Schematic of MDI-QKD [10]

an interferometer and single photon detectors. Bob broadcasts the time-stamps to Alice. In the end, Alice and Bob obtain an identical bit string. The DPS-QKD scheme is easy to implement in optical fiber due to its simple configuration and it is robust against Photon Number Splitting attack (PNS) attack.

6.4 Measurement-device-independent QKD

Measurement-Device-Independent QKD (MDI-QKD) [10] is performed with untrusted measurement devices, which can be developed by an adversary. The schematic of MDI-QKD is presented in Figure 6. Alice and Bob carefully monitor the prepared quantum state in their respective laboratories. They send them to an untrusted party (Charlie) who performs a Bell-state measurement on the states received. The honesty of Charlie can be validated by comparing a part of the transmitted data. The security relies on the violation of Bell inequality. MDI-QKD is a suitable candidate for QKD network with untrusted nodes, which is favorable from security perspective.

7 Implementations of QKD

7.1 Free-space QKD

Free-space QKD implies that the quantum transmission can be established between: 1) ground-to-ground, 2) ground-to-satellite and 3) satellite-to-satellite. In 1992, the first free-space QKD [12] was demonstrated over a distance of 32 cm. About more than two decades later free-space QKD [13] was established across two Canary Islands (La Palma and Tenerife) 144 km apart. QKD was performed between a ground station and a hot-air balloon [14]. This experiment can be considered as the first ground to Lower Earth Orbit (LEO) QKD. The atmospheric attenuation is about 0.07 dB/km at 2400 m above sea level. This attenuation increases at lower altitudes and decreases at higher altitudes. It is observed that free-space QKD cannot yield better key rate at more than 100 km due to the atmospheric attenuation. Satellite QKD may seem technologically challenging at present but, it has been demonstrated effectively and could prove to be the optimal candidate for a global QKD network.

7.2 Fiber-optic QKD

Fiber-optic QKD is independent of line-of-sight connection between sender and receiver. Practical implementation is appropriate for shorter distances approx. 150 km. Longer distances (150-200 km) [15] makes the quantum transmission very weak due to the absorption by impurities in the fiber. Commercial telecom communication exhibits optimal transmission at three particular bands

1. 890 nm with very high attenuation,
2. 1310 nm with less noisy and higher attenuation and
3. 1550 nm with noisy and lowest attenuation of 0.2 dB/km (and 0.16 dB/km in ultra

low-loss fibers).

Significant achievements are 250 km [16] and 307 km [17] in ultra low-loss fiber. The fiber-optic-based QKD protocols have been successfully demonstrated in the past. They are robust to hostile environmental conditions thereby offering higher key rate. In particular, DV MDI-QKD was demonstrated over 200 km telecom fiber [18] and 404 km of ultra low-loss fiber [19] in lab conditions, and over 30 km of deployed fiber [20].

8 Global QKD network

QKD provides point-to-point security for a communication link. Establishing a network is a challenge because of limited ranges due to point-to-point links and high cost deploying QKD systems. In this section, we briefly discuss the different techniques for establishing a QKD in a Metropolitan Area Network (MAN) and at a global scale.

1. Trusted node has been implemented in existing QKD networks [21, 22, 23]. It can be used to transmit the keys from one node to another thereby establishing secure communication over an arbitrarily long distance. In 2008, European FP6 project Secure Communication based on Quantum Cryptography (SECOQC) [21] was launched in Vienna which integrated 6 different QKD systems together through trusted repeaters. Interestingly, from this project, the European Telecommunications Standards Institute (ETSI) launched a forum for QKD standards. In 2010, the US Defense Advanced Research Projects Agency (DARPA) [22] together with BBN Technologies, Boston University and Harvard University designed DARPA quantum network across a metropolitan area. In 2010, Tokyo QKD network [23] successfully demonstrated high-speed QKD network where video conference was presented using one-time-pad (OTP) encryption system.

2. Quantum repeaters will eventually replace trusted nodes. At present quantum repeaters is a subject of intense research. Recent progress in building quantum repeaters is based on heralded entanglement generation and purification [24] and quantum error correction techniques [25].

3. Global distribution network can be achieved through satellites. They are used as trusted nodes. Several nations like China, the EU, and Canada are all exploring the ground-to-satellite QKD involving LEO satellites [26, 27].

9 Post-quantum cryptography

Post-quantum cryptography refers to the classical cryptographic algorithms robust to attacks from quantum algorithms and increased computational power. Precisely, arrival of quantum computer is not the end of the cryptography. There are other cryptographic algorithms apart from RSA, DH etc. which can resist attacks by a classical and quantum computer. PQC is based on the family of lattice, codes, hash and multivariate polynomials. NIST has emphasized on the development of such algorithms which will replace PKC and facilitate inter-operation with current communication protocols and networks. PQC is advantageous in a manner that it can cover wider secure communications tasks ranging from key operations, signatures, e-voting etc. However, at present there is no proof to prove that it will remain resistant to quantum attacks i.e. quantum-safe forever.

10 Random number generator

Conventionally a sequence of random numbers are either produced by a Pseudo Random Number Generator (PRNG) or a True Random Number Generator (TRNG). PRNG is an algorithm (software solution) for generating random numbers. A TRNG is a hardware random number generator (RNG) that

do not rely on algorithmic processes. It digitizes the analog physical noise source to retrieve random numbers that are uniform and independent. There is a fundamental proof of complexity theory, according to which one cannot prove that a particular sequence of numbers is genuinely unpredictable. Proper analysis, testing of device and verification determines the quality of TRNG. There are certain commercial test methods, precisely 15 individual test methods, for testing the correlation of random numbers prescribed by the National Institute of Standards and Technology (NIST) [28]. Further, the Diehard-Test [29] is another RNG testing suite. The random numbers produced from a TRNG on successfully passing these tests can be considered reliable to be used directly for cryptographic applications or as a seed for PRNG.

10.1 Why do we need quantum random number generator

A classical TRNG can never, in principle guarantee, that, an adversary will not be able to obtain information either by passive monitoring, malicious modification or signal injection. The chaotic source of classical randomness is very sensitive to initial conditions and the deterministic nature hides behind the complexity. The PRNG will produce the same random numbers when the same seed is fed to the algorithm. This gravely compromises the security of QKD. Quantum physics is the only theory that is intrinsically random and it guarantees that at any given identical initial conditions it will in principle give random output. In other words, the quantum system will never reproduce an output with given same conditions. Thus, true random numbers based on the principles of quantum physics, called QRNG are preferred in QKD systems. Consider a quantum particle i.e. a photon with a definite energy falling on a half-silvered mirror or a 50:50 Beam Splitter (BS). If the photon emerges at both arms of BS, it would mean that it will have half the energy at both the outputs corresponding to longer wavelengths. However, this is contrary to observation. Quantum physics tells us that there is 50 percent probability that photon takes transmitted path and 50 percent probability that it takes reflected path. For any given photon there is no technology that can predict the path of the photon after the beam splitter. Thus, the unpredictability inherent in a quantum evolution makes it a worthy candidate for implementation in TRNG.

11 About QuNu Labs

QuNu Labs is a Bangalore based technology start-up incubated out of IITM. Established in Sep 2016, it is the first and only Indian Company in the quantum cryptography space. QuNu is currently offering a DPS based QKD with built-in QRNG as an immediate solution to urgent need for securing the key. Once this is done, the customer can be rest assured that even with the advent of quantum computers his communication link will be safe. At a later stage, QuNu plans to offer new age cryptographic primitives which will be quantum resistant and is planning to develop proprietary lattice based codes and algorithm that will be quantum-safe. In future, QuNu plans to foray into free space, Li-Fi and satellite-based QKD systems.

References

[1] ETSI White Paper Quantum Safe Cryptography V1.0.0 (2014-10): Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges; ISBN 979-10-92620-03-0.

[2] R. P. Feynman, Simulating physics with computers, Int. J. Theo. Phys., **21** (1982) 467.

[3] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM,

IEEE Computer Society Press, (1994) 124.

[4] L. K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev. Lett, **79** (1997) 325.

[5] NIST Special Publication (SP) 800-57 Recommendation for Key Management Part 1 Rev 4, National Institute of Standards and Technology, USA.

[6] C. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984) 175.

[7] C. H. Bennett, Quantum cryptography using any two non-orthogonal states, Phys. Rev. Lett., **68** (1992) 3121.

[8] D. Stucki *et al.*, Fast and simple one-way quantum key distribution, Appl. Phys. Lett., **87** (2005) 194108.

[9] K. Inoue, E. Waks and Y. Yamanoto, Differential-phase-shift quantum key distribution using coherent light, Phys. Rev. A, **68** (2003) 022317.

[10] H. -K. Lo, M. Curty and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett., **108** (2012) 130503.

[11] E. Diamanti *et al.*, Practical challenges in quantum key distribution, npj Quantum Information, **2** (2016) 16025.

[12] C. H. Bennett *et al.*, Experimental quantum cryptography, J. Cryptol., **5** (1992) 3.

[13] R. Ursin *et al.*, Entanglement-based quantum communication over 144 km, Nature Phys, **3** (2007) 481.

[14] J. -Y. Wang *et al.*, Direct and full-scale experimental verifications towards ground-satellite quantum key distribution, Nat. Photon, **7** (2013) 387.

[15] H. -K. Lo, M. Curty and K. Tamaki, Secure quantum key distribution, Nat. Photon, **8** (2014) 595.

[16] D. Stucki *et al.*, High Rate, Long-distance quantum key distribution over 250 km of ultra low loss fibers, New J. Phys., **11** (2009) 075003.

[17] B. Korzh *et al.*, Provably secure and practical quantum key distribution over 307 km of optical fiber, Nat. Photon, **9** (2015) 163.

[18] Y. -L. Tang *et al.*, Measurement-device-independent quantum key distribution over 200 km, Phys. Rev. Lett., **113** (2014) 190501.

[19] H. -L. Yin *et al.*, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett., **117** (2016) 190501.

[20] Y. -L. Tang *et al.*, Field test of measurement-device-independent quantum key distribution, IEEE J. Sel. Top. Quantum Electron, **21** (2015) 6600407.

[21] M. Peeveta *et al.*, The SECOQC quantum key distribution network in Vienna, New J. Phys., **11** (2009) 075001.

[22] C. Elliott, Current status of the DARPA quantum network, in Quantum Information and Computation III, Proc. SPIE, **5815** (2005) 138.

[23] M. Sasaki *et al.*, Field test of quantum key distribution in the Tokyo QKD Network, Opt. Express, **19** (2011) 10387.

[24] N. Sangouard *et al.*, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys., **83** (2011) 33.

[25] A. G. Fowler *et al.*, Surface code quantum communication, Phy. Rev. Lett., **104** (2010) 180503.

[26] J. -W. Pan, Quantum Science Satellite, Chin. J. Sp. Sci., **34** (2014) 547.

[27] L. Sheng-Kai *et al.*, Satellite-to-ground quantum key distribution, Nature, **549** (2017) 43.

[28] M. S. Turan *et al.*, Recommendation for the entropy sources used for random bit generation, NIST Special Publication 800-90B, Second draft (2016).

[29] G. Marsaglia, Diehard battery of tests of randomness, The Marsaglia random number CDROM, Department of Statistics, Florida State University (1995).