International Journal of Sociology and Humanities

ISSN Print: 2664-8679
ISSN Online: 2664-8687
Impact Factor: RJIF 8
IJSH 2024; 6(1): 37-39
www.sociologyjournal.net
Received: 09-12-2023
Accepted: 16-01-2024

Meet Sharma
MCA 3rd Semester, CMR University, Bangalore, Karnataka, India

Dr. VN Sudheer
Associate Professor, School of Liberal Studies, CMR University, Bangalore, Karnataka, India

Corresponding Author:
Meet Sharma
MCA 3rd Semester, CMR University, Bangalore, Karnataka, India

Convergence of irrevocable reliability of quantum variability: A comprehensive study on quantum cryptography

Meet Sharma and Dr. VN Sudheer

DOI: https://doi.org/10.33545/26648679.2024.v6.i1a.74

Abstract
This manuscript delves into the realm of quantum cryptography, examining its integral contribution to a defense-in-depth strategy for achieving completely secure key distribution. The paper encompasses an exploration of the vulnerabilities inherent in contemporary digital crypto systems, an elucidation of the foundational principles of quantum cryptography, a scrutiny of real-world implementations alongside their limitations, and a contemplation of the prospective trajectory that quantum cryptography is poised to undertake. The discussion spans various facets, encompassing the computational model of quantum computers, the pivotal quantum algorithms impacting cryptography, the looming risks associated with the potential construction of "Cryptographically Relevant Quantum Computers" (CRQCs), and the ensuing ramifications for the security of both symmetric and public-key cryptography in the presence of CRQCs. Furthermore, the paper investigates the ongoing standardization efforts by NIST for "Post-Quantum Cryptography" (PQC), the evolving landscape toward quantum-resistant public-key cryptography, and the pertinence of "Quantum Key Distribution" (QKD) as a complementary element to conventional cryptography. Lastly, it explores the significance of "Quantum Random Number Generators" (QRNGs) as an augmentation to current hardware Random Number Generators.

Keywords: Conventional cryptography, computational models, future directions, secure key distribution, quantum algorithms, etc.

Introduction
Quantum cryptography provides many benefits over traditional cryptography because it does not rely on potentially solvable math equations to secure encrypted data. It also prevents eavesdropping since quantum data cannot be read without also being changed, and quantum cryptography can also integrate well with other types of encryption protocols. This type of cryptography enables users to digitally share a private encryption key that cannot be copied during transit. Once this key is shared, it can be used to encrypt and decrypt further messages in a way that has almost no risk of being compromised. Quantum cryptography also requires specific infrastructure. Fiber optic lines are necessary for transferring protons and have a limited range of typically about 248 to 310 miles, which computer science researchers are working to extend. Additionally, quantum cryptography systems are limited by the number of destinations where they can send data. This type of cryptography enables users to digitally share a private encryption key that cannot be copied during transit. Once this key is shared, it can be used to encrypt and decrypt further messages in a way that has almost no risk of being compromised.

Limitations
Public key cryptography involves intricate calculations that are relatively slow, primarily employed for key exchange rather than the encryption of extensive data sets. Well-established solutions, exemplified by RSA and the Diffie-Hellman key negotiation schemes, play a pivotal role in distributing symmetric keys among remote entities. Nevertheless, the inherent sluggishness of asymmetric encryption prompts the adoption of a hybrid methodology, capitalizing on the speed of a shared key system and the security attributes of a public key system during the initial symmetric key exchange.

This strategic approach harnesses the efficiency of a symmetric key system while capitalizing on the scalability inherent in a public key infrastructure.

However, public key crypto systems, including RSA and Diffie-Hellman, lack concrete mathematical proofs. Instead, their security is derived from years of public scrutiny regarding the presumed "intractability" of factoring large integers into primes. Essentially, the encryption algorithm's strength lies in the absence of a known mathematical operation for swiftly factoring large numbers given the current state of computer processing power. While contemporary public key crypto systems may currently provide a satisfactory level of confidentiality, they are not immune to risks. One notable risk is the potential vulnerability to technological advancements, particularly quantum computing, which could render systems like RSA obsolete. Similarly, historical cases, such as the DES algorithm, with its 56-bit key, once considered secure, were later deemed vulnerable due to technological progress. The development of the Advanced Encryption Standard (AES) was prompted by the realization that powerful computers could swiftly crack DES, highlighting the susceptibility of public key cryptography to evolving technology. Moreover, there is uncertainty regarding the potential development or existence of a theorem capable of factoring large numbers into primes in a timely manner. The absence of a definitive proof stating the impossibility of such a factoring theorem introduces vulnerability to public key systems. This uncertainty poses a potential risk to areas of national security and intellectual property that demand a higher level of security assurance.

In summary, modern cryptography faces susceptibility to both technological advancements in computing power and potential mathematical breakthroughs that could rapidly reverse one-way functions, such as factoring large integers. The hypothetical disclosure of a factoring theorem or the emergence of sufficiently powerful computing could necessitate substantial resources for research and the rapid deployment of new and costly cryptography systems by businesses, governments, military, and other affected institutions.

Key Confidentiality in Quantum Key Distribution-A Paradigm Shift in Secure Communication

The paramount focus on Quantum Key Distribution (QKD) emanates from the pivotal concern for confidentiality. In contrast to public key systems facing perpetual uncertainty surrounding the mathematical intractability of decryption, key agreement primitives employed in contemporary Internet security frameworks, such as Diffie-Hellman, may potentially succumb to breaches in the future. Such a compromise not only jeopardizes the ability to communicate seamlessly in the future but also poses the risk of exposing past traffic patterns.

Traditional secret key systems have grappled with distinct challenges, including vulnerabilities to insider threats and the logistical complexities of distributing keying material. In contrast, the integration of QKD techniques into a comprehensive secure system, if executed judiciously, promises an automatic and efficient distribution of keys. This approach holds the potential to furnish a level of security surpassing that offered by its counterparts. As a result, Quantum Key Distribution emerges as a paradigm shift, providing enhanced key confidentiality while mitigating the vulnerabilities associated with traditional cryptographic systems.

Imperfections in Quantum Key Distribution-Addressing Deviations for Enhanced Security Assurance

In the realm of Quantum Key Distribution (QKD), the imperfections in encoding play a crucial role that parallels the significance of selecting optimal prime numbers in the RSA algorithm. Just as a weak choice of prime numbers can compromise the overall security in RSA, the QKD protocol necessitates specifying the preparation of quantum states for transmission over an insecure public channel.

The prepared quantum states, however, are susceptible to deviations from the protocol specifications due to imperfections in the physical equipment. While it may seem intuitive that such deviations would minimally impact security, applying standard security proofs reveals a vulnerability to the typical losses inherent in a communication channel. This vulnerability results in a more significant reduction in the key rate than anticipated.

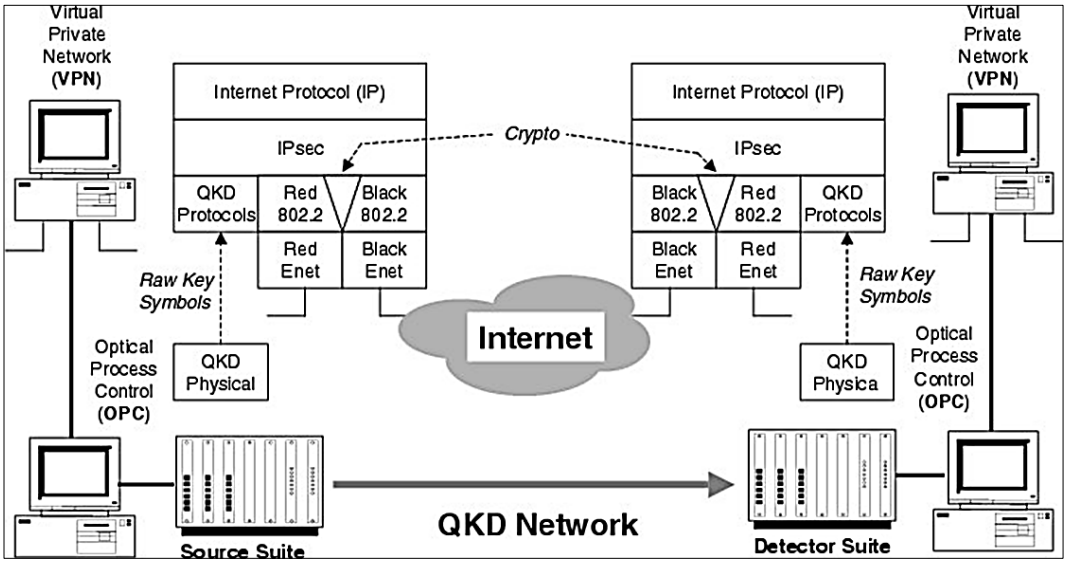

Fig 1: QKD Network Protocols

Implementation of (QKD) Protocols- A Comprehensive Overview of Unconventional Aspects in Communications Security

The field of quantum cryptography encompasses a remarkably intricate collection of specialized protocols collectively referred to as "QKD protocols." These protocols exhibit distinctive features both in their motivation and implementation, offering intriguing insights for specialists in communications protocols.

This section delves into the operational details of the QKD protocol implementation in our C language framework. Engineered by DARPA, this platform is designed for seamless integration of new protocols, with a commitment to dedicating substantial efforts to the invention and practical testing of novel QKD protocols in the years ahead. These protocols can be best conceptualized as sub-layers within the broader QKD protocol suite. It is noteworthy, however, that these layers do not align directly with the conventional layers in a typical communications stack, such as the OSI layers. Instead, their structure resembles more closely the stages of a pipeline, introducing a distinctive and unconventional aspect to the QKD protocol suite.

Ensuring Prompt Key Delivery in KDS- Addressing Throughput Challenges in Quantum Key Distribution

Efficient key distribution systems are imperative to ensure a sufficiently rapid delivery of keys, preventing encryption devices from depleting their supply of key bits. This challenge constitutes a dynamic race between the deployment rate of keying material and its consumption in encryption or decryption processes. Present-day Quantum Key Distribution (QKD) systems exhibit a throughput of approximately 1,000 bits per second for keying material in realistic scenarios, often operating at even lower rates. This throughput is deemed unacceptable when employing these keys in certain applications, such as one-time pads for high-speed traffic flows. However, the same throughput may be deemed acceptable when the keying material serves as input for less secure, yet sufficiently robust, algorithms like the Advanced Encryption Standard (AES). Despite the current limitations, there exists both a desirability and feasibility to significantly enhance the throughput rates offered by contemporary QKD technology. This pursuit aims to meet the evolving demands for faster and more secure key delivery systems in the realm of quantum communication.

Prospects and Challenges in the Advancement of Quantum Key Distribution Networks-A Comprehensive Examination

The Defense Advanced Research Projects Agency (DARPA) is embarking on the construction of an intricate Quantum Key Distribution (QKD) network. This network seamlessly interconnects QKD endpoints through a mesh of QKD relays or routers, showcasing resilience against potential point-to-point QKD link failures, such as fiber cuts or intrusive eavesdropping. Coined as a "key transport network," the DARPA Quantum Network is designed to remain robust even in the face of active eavesdropping attempts or denial-of-service attacks.

Looking towards the future, the key limitation of untrusted QKD networks, namely limited geographic reach, may find a resolution through the integration of quantum repeaters. Research efforts are underway to develop practical quantum repeater devices that can be seamlessly incorporated into the overarching architecture of untrusted QKD networks. This integration holds the promise of extending the reach of QKD operations over significantly greater distances than currently achievable. One proposed solution to overcome distance constraints involves "chaining" quantum cryptography links with secure intermediary stations. Another alternative explores the transmission of quantum keys through free space or low-orbiting satellites, with the satellite acting as the intermediary station and less photon attenuation in the atmosphere. Ongoing research, both in the United States and Europe, is actively exploring the feasibility of securely transmitting quantum keys from satellites to designated destinations.

Conclusion

Despite notable strides in quantum cryptography over the past decade, several challenges persist before it can evolve into a widely adopted key distribution system. These challenges encompass the need for advanced hardware to enhance the quality and extend the transmission distances of quantum key exchange. However, the continuous threat of obsolescence for traditional cryptography systems and the ever-advancing capabilities of computer processing will propel ongoing research and development in quantum cryptography. Anticipated investments of nearly $50 million from both public and private funds over the next three years underscore the commitment to advancing quantum cryptography technology. While still in its nascent stages, quantum cryptography holds immense promise. If it fulfills even a fraction of its anticipated potential, it stands to revolutionize realms such as e-commerce, business security, personal security, and intergovernmental security, significantly impacting diverse aspects of our lives.

References

1. Bernstein DJ. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete. SHARCS. 2009;9:105.
2. Broadbent A, Schaffner C. Quantum Cryptography Beyond Quantum Key Distribution; c2015. arXiv preprint arXiv:1510.06120.
3. Schenker JL. A quantum leap in codes for secure transmissions. The IHT Online; c2004 Jan 28.
4. Johnson RC. MagiQ employs quantum technology for secure encryption. EE Times; c2002 Nov 6.
5. Elliott C. Building the quantum network. New J Phys. 2002 Jul;4:46.
6. https://www.ibm.com/topics/cryptography