



ORIGINAL

Quantum key distribution for enabling secure network function vitalization orchestration over a Network

Distribución de claves cuánticas para permitir la vitalización segura de las funciones de red en una red

Hayder A. Nahi¹ , Akmam Majed Mousa¹, Ebtehal Akeel Hamed², Ali Khalid Ali¹, Sarmad Jawad³ , Ahmed Mahdi Abdulkadium¹, Rusul A. Salman¹

¹Computer Center, Al Qasim Green University. Babylon 51013, Iraq.

²College of Physical Education and Sport Sciences, Al Qasim Green University. Babylon 51013, Iraq.

³Department of Cyber Security, College of Sciences, Al-Mustaqbal University. 51001, Babylon, Iraq.

Cite as: Nahi H, Majed Mousa A, Akeel Hamed E, Khalid Ali A, Jawad S, Mahdi Abdulkadium A, et al. Quantum key distribution for enabling secure network function vitalization orchestration over a network. Data and Metadata. 2025; 4:202. <https://doi.org/10.56294/dm2025202>

Submitted: 15-05-2024

Revised: 10-09-2024

Accepted: 23-02-2025

Published: 24-02-2025

Editor: Dr. Adrián Alejandro Vitón Castillo 

Corresponding Author: Hayder A. Nahi 

ABSTRACT

Quantum Key Distribution (QKD) provides an state-of-the-art solution that work toward to enhance security of network and performance contrast to conventional systems. This paper focal point on the utilize of QKD to authorize secure orchestration and authorize network functions virtualization (NFV). The QKD-based solution is contrast with presenting solutions utilizing applying science and security KPIs.

The outcomes display that the QKD solution exceed conventional solutions, with throughput stretch out 250 Mbit/s contrast to 150 Mbit/s, and response time of 4 ms versus 10 ms. The bit error rate (BER) registered a notable depletion to 1,2e-10 contrast to 1,8e-9, and an interception rate of 0 % against 5 % in conventional systems was attained.

The work as well appears that the time wanted to distribute quantum keys is at most 4 ms, with a key exchange success rate of 99,8 %. The model also give a demonstration of peak attack resistance with 100 successfully blocked hacking attempts registered. in spite of an extra 10ms data encryption processing time and a small 3 % throughput effect, the general performance remainder marvelous with a network function deployment time of 150ms and only 0,1 % packet loss.

These measure reveal the efficacy of QKD in enhancing the security and efficiency of virtual networks. The paper give empirical perceptions to hold up the implementation of quantum security techniques in time ahead network infrastructures.

Keywords: QKD; NFV; SDN; Quantum Algorithms; NSO.

RESUMEN

Quantum Key Distribution (QKD) proporciona una solución de vanguardia que trabaja para mejorar la seguridad de la red y el rendimiento en contraste con los sistemas convencionales. Este artículo se centra en la utilización de QKD para autorizar la orquestación segura y autorizar la virtualización de funciones de red (NFV). La solución basada en QKD se contrasta con la presentación de soluciones que utilizan la aplicación de la ciencia y los KPI de seguridad.

Los resultados muestran que la solución QKD supera a las soluciones convencionales, con un rendimiento de 250 Mbit/s frente a 150 Mbit/s, y un tiempo de respuesta de 4 ms frente a 10 ms. La tasa de bits erróneos (BER) registró una notable disminución de 1,2e-10 frente a 1,8e-9, y se alcanzó una tasa de interceptación del 0 % frente al 5 % de los sistemas convencionales.

El trabajo también pone de manifiesto que el tiempo necesario para distribuir claves cuánticas es como máximo de 4 ms, con una tasa de éxito en el intercambio de claves del 99,8 %. A pesar de un tiempo adicional de 10 ms en el proceso de cifrado de datos y un pequeño efecto del 3 % en el rendimiento, el rendimiento general sigue siendo maravilloso, con un tiempo de despliegue de la función de red de 150 ms y sólo un 0,1 % de pérdida de paquetes.

Estas medidas revelan la eficacia de la QKD para mejorar la seguridad y la eficiencia de las redes virtuales. El artículo aporta percepciones empíricas para sostener la implementación de técnicas de seguridad cuántica en infraestructuras de red adelantadas en el tiempo.

Palabras clave: QKD; NFV; SDN; Algoritmos Cuánticos; NSO.

INTRODUCTION

IOT has emerged as a crucial paradigm in recent years to minimize human interaction. A large number of items have ability to perceive, communicate, and share information, resulting in a linked smart world.⁽¹⁾ However, given the large volume of data created, the quick expansion of connected devices presents a number of unique challenges. It specifically covers things like data availability, correctness, security, and collisions. The NFV converts physical layer resources to virtual ones and provides a potential solution that can allow autonomous management.⁽²⁾ In order to establish a virtual environment and cut expenses and effort.

Network Function Virtualization (NFV) is a technical solution that substitutes virtual resources for physical ones.^(3,12) Nowadays, the security of cryptography depend on solving complex mathematical problems that take a polynomial amount of time to solve on a classical computer(CC).For instance, public key cryptography is predicated on the mathematical premise that CC cannot accomplish prime factorization because of a lack of effective factorization algorithms or a constraint in processing resources.⁽⁴⁾

But with quantum computing (QC)^(15,16,17) everything is different. Our perception of nature has been profoundly altered by quantum physics, and expanded technical possibilities will result in new standards of privacy and confidentiality for communication services. One new development in the field of quantum cryptography is QKD. In contrast to traditional cryptography algorithms that rely on mathematical complexity as their foundation for security.

QKD^(18,19,20) uses the law of quantum mechanics. It has been demonstrated that, in theory, it is possible to provide unconditional security by combining three element the use of one-time-pads, hashing schemes, and the law of quantum mechanics.⁽⁵⁾

Literature Review

For the first time, it was used in⁽⁵⁾ [NFV orchestration platform over SDN-controlled optical networks with quantum key-distribution systems. The results demonstrate that a 5,3 % minimum QBER can be achieved by using quantum encryption for NFV MANO operations to protect an SSMF link up to protect an SSMF link up to25 kilometers with simultaneous SDN control.

Understanding how the existing QC technology requirements may affect 6G KVLs and their possible limits. In the research, this was the topic of discussion.⁽⁶⁾

Quantum physics 6G together have the potential to completely change wireless communications in the future, changing how we connect, communicate, and compute. Although quantum mechanics presents exciting opportunities, achieving them will entail overcoming formidable obstacles. External perturbation can causes quantum bits to lose their coherence. Cryogenic temperatures, an energy-intensive procedure that sounds paradoxical to 6G's sustainability goals, are necessary to maintain the majority of quantum states. Additionally, quantum physics, which is essential to trustworthy quantum computing, is still in its early stages of development and necessitates a great deal of study.⁽⁷⁾

The usefulness of the simulation models employed by the authors in the research Trizna A et al.⁽⁵⁾ has been demonstrated since SDN technology isolates network management and control from data transmission and forwarding activities.

Additionally, it is a promising concept that can be used in QKD networks to easily enhance device, resource, and process interaction.

Additionally, three use cases—multi-resource allocation, secret key management, and survivability assurance are presented.

However, a significant obstacle at the moment is the incompatibility of QKD networks with conventional optical networks, and the redeployment of QKD networks would result in significant expenses.

P et al.⁽⁸⁾ The primary control plane protocols, MPLS, Open Flow, and NETCONF/YANG, incorporate the key synchronization procedure (and with other cryptographic parameters) needed for further encryption. QKD-generated keys are used into IPsec sessions to integrate these new technologies into new network models.

Ultimately, these sessions are contained under automated VNFs through control plane extensions.

Jawdhari, H. A et al.⁽¹³⁾ offers sample that utilizes blockchain-NFV (Network Function Virtualization) to handle and store patient electronic health records (EHR). A new approach is offered to virtualize the work of the blockchain depending on the NFV with automatic run of the smart contract between in the middle of nodes based on cloud computing.^(14,21)

Integrating Quantum Key Distribution (QKD) with Network Function Virtualization Orchestrator (NFVO)

As communication networks evolve and adopt new technologies such as virtualization and network orchestration, the need for improved security levels has increased unprecedentedly. Among these technologies, Quantum Key Distribution (QKD) offers an innovative solution to secure communications against future quantum threats. When combined with Network Function Virtualization Orchestrator (NFVO), a robust and comprehensive level of security can be achieved for virtual network infrastructure.

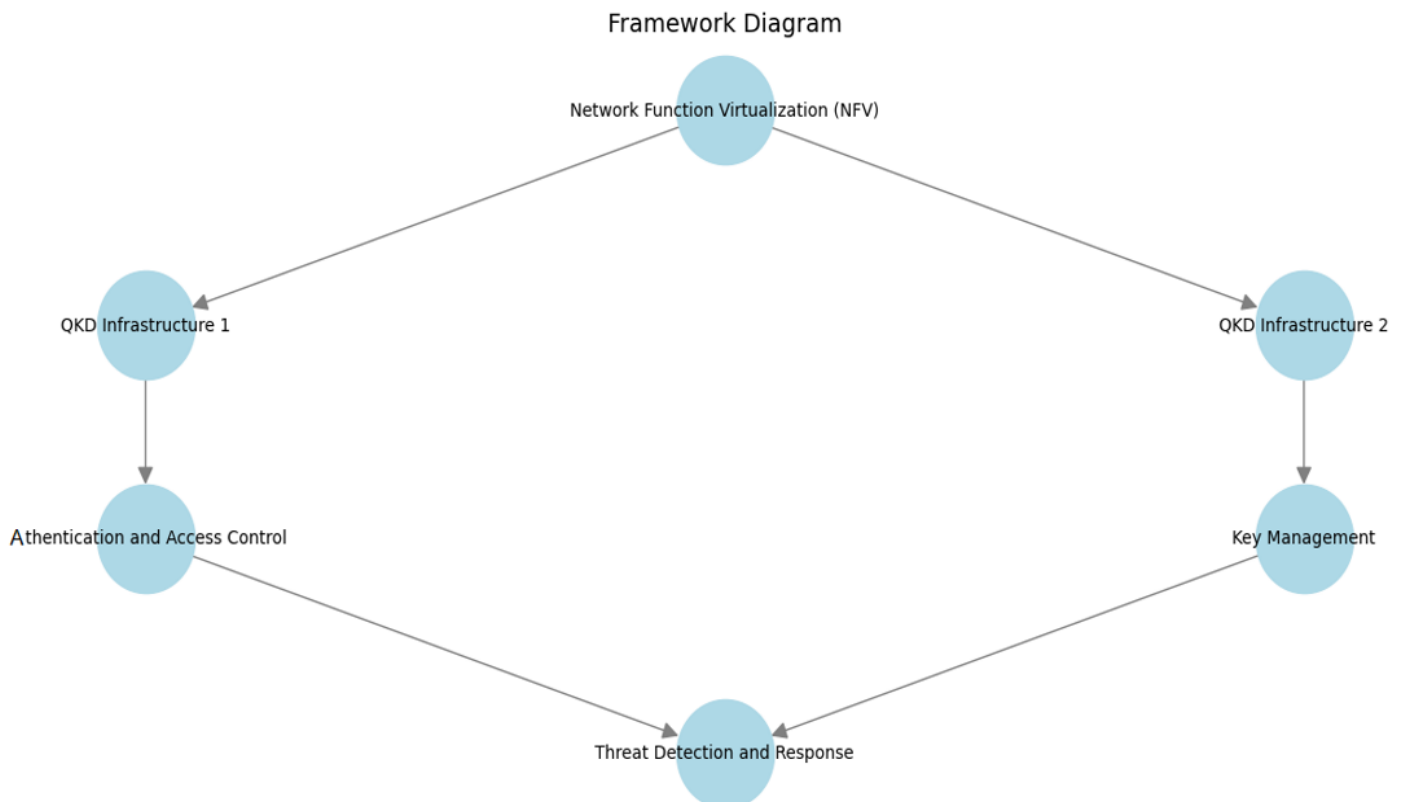


Figure 1. Substructure of utilizing QKD for build secure NFV orchestration

Quantum Key Distribution (QKD)

Is an encryption mechanism based on the physical concepts of quantum techniques. Its essentials idea is to confident the interchange of encryption keys with one on either side parties utilizing quantum phenomena such as quantum entanglement and photon polarization. This computer technology is distinguished through its capability to detect each try to object keys and prepare encryption keys that cannot be shattered utilizing physics on behalf of mathematical calculations, which keep safe opposed to attacks that based on quantum computing.

Role of NFVO in Virtual Networks

NFVO is a main ingredient of virtual network infrastructure, orchestrating, deploying, and managing virtual network functions (VNFs). It objectives to prepare scalable services and functional resource administration in addition to persevering continuity of functioning and services to the other side of cloud infrastructure. It is rely on the ETSI NFV MANO standard to determine the public framework for managing virtual tasks and cloud infrastructure, but it inevitably to guarantee the security of sensitive operations such as key management and inter-element coordination.

Integrating QKD with NFVO

Merging QKD with NFVO can improve security in virtual networks via securing the transference of critical data treated via NFVO while orchestrating and managing VNFs. Utilizing QKD, quantum channels can be generated to securely exchange keys and keep safe network links such as connections between VNFs and virtual routers.

Combining with conventional network infrastructure permits a dedicated QKD-based security layer to be added on top of the conventional infrastructure. Protocols such as SDN that are appropriate with QKD can be used to distribute keys in a seamless mode. QKD permits for the uninterrupted and dynamic generation of modern keys, where NFVO can effortlessly manage key distribution and supply a mechanism for computerized key renewal when require. This integration gives to identity defense and make sure identity verification among whole entities in the network, lessen the possibility of attacks rely on impression or data manipulation.

Practical benefits of integrating QKD with NFVO

This combination gives to improving security via keeping from harm virtual communication channels from spy or interception and providing encryption keys that are impervious to to quantum attacks. It as well enhances network reliability via securing sensitive operations managed via NFVO and rising trust in virtual services. The combination also assistsmaintain the same rate of progress with future threats that may become apparent from quantum computing technologies while supporting advanced applications such as the Internet of Things (IoT) and enhancing the performance and security of 5G and cloud-based networks.

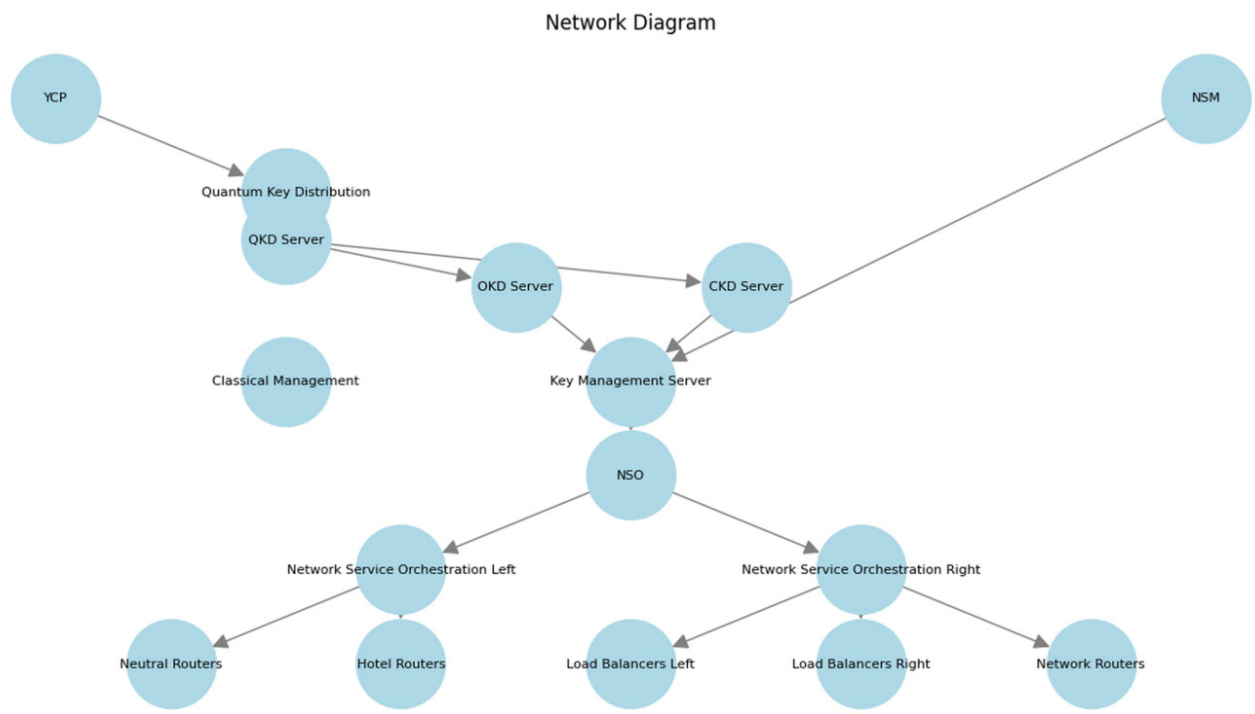


Figure 2. Integrating QKD with NFVO

Challenges and Solutions

Table 1. Addressing security issues in NFV with QKD		
The Problem	Description	QKD Solution
Weakness Encryption	Possibility break Encryption Traditional by Computing Quantity	Distribution Keys not Acceptable To break Using QKD
Attacks Eavesdropping	Objection Data during Transport	Discovery Eavesdropping via changing features Particles
Administration Keys	Difficulty administration Keys Traditional in Environments Virtual	Keys dynamism It is done Generate it In a way that I

Integration may face some technical challenges such as the complexity of implementing quantum channels parallel to traditional networks, which can be overcome by using open source standards and software that support integration. The high cost of QKD technologies may be a barrier, but scalable solutions can be adopted that rely on deploying QKD in the core infrastructure only. Compatibility with existing protocols may require the development of hybrid protocols that support QKD and the existing infrastructure table 1.

The integration of QKD with NFVO represents a significant shift in the field of virtual network security. This integration enables a new level of protection, ensuring the security of sensitive network data and operations

against current and future threats. By investing in this area, telecom companies can prepare for the future and build secure and sustainable networks.^(22,23)

METHOD

Quantum Key Distribution (QKD) Server

This part is accountable for producing and distributing the QKD key to the NFV parts. It utilizes a specialized hardware device (Quantum Key Distribution unit) to create the QKD key and distribute it to the NFV components through a dedicated quantum channel Algorithm 1.

Algorithm 1. QKD Key Distribution Algorithm

```

1 Procedure QKDKeyDistribution(Server, NFVComponents, QuantumChannel)
2   Initialize the QKD server.
3   for every component NFVComponents do
4     Generate a unique quantum key QKey using QKD hardware.
5     Transmit QKey to component over QuantumChannel.
6     if receipt_confirmed and key_integrity_valid then
7       Mark component as key-distributed.
8     else
9       Re-transmit QKey or alert failure.
10    end if
11  end for
12  if all components are key-distributed then
13    Terminate the QKD server.
14  end if
15 end procedure

```

Classical Key Management (CKM) Server

This part is accountable for managing the traditional keys utilized for encryption and decryption of the messages exchanged among the NFV components. It utilizes common cryptographic protocols, such as AES or RSA, to generate and distribute the classical keys Algorithm 2.

Algorithm 2. Classical Key Management (CKM) Algorithm

```

1 Procedure ClassicalKeyManagement(Server, NFVComponents, Protocol)
2   Initialize the CKM server.
3   for every component NFVComponents do
4     Generate a unique classical key CKey using Protocol (e.g., AES or RSA).
5     Encrypt CKey using the component's public key or shared secret.
6     Transmit the encrypted CKey to component.
7     if receipt_confirmed and key_integrity_valid then
8       Mark component as key-distributed.
9     else
10      Re-generate and re-transmit CKey.
11    end if
12  end for
13  if all components are key-distributed then
14    Log success and maintain keys in the database.
15  end if
16 end procedure

```

Network Service Orchestration (NSO) Platform

This part is accountable for orchestrating the NFV components and managing the network services. It gives a centralized management interface for the NFV components and interfaces with the QKD and CKM servers to enable secure communication among them Algorithm 3.

Algorithm 3. Network Service Orchestration (NSO) Algorithm

```

1 Procedure NetworkServiceOrchestration(NFVComponents, QKDServer, CKMServer)
2   Initialize the NSO platform.
3   Establish secure connections with QKDServer and CKMServer.
4   for each component NFVComponents do
5     Query QKDServer for quantum key QKey assigned to component.

```

```

6      Query CKMServer for classical key CKey assigned to component.
7      if both QKey and CKey are available and valid then
8          Distribute keys to component via secure interface.
9      else
10         Log error and retry connection with the servers.
11     end if
12 end for
13 Monitor and manage network services for NFVComponents.
14 Update key status periodically by interfacing with QKDServer and CKMServer.
15 Terminate NSO platform upon completion of key orchestration and management.
16 end procedure

```

NFV Components

These are the virtualized network functions, such as routers, firewalls, or load balancers, that perform determined network missions. They communicate with each other and with the NSO platform over the QKD and CKM channels to exchange sensitive information Algorithm 4.

Algorithm 4. NFV Component Communication Algorithm

```

1 procedure NFVComponentCommunication(Component, NSOPlatform, QKDChannel, CKMChannel)
2     Initialize the NFV component.
3     Establish secure connection with NSOPlatform over the QKDChannel and CKMChannel.
4     Receive quantum key QKey from the QKDChannel.
5     Receive classical key CKey from the CKMChannel.
6     for each peer_component ConnectedComponents do
7         if QKey and CKey are valid then
8             Encrypt sensitive information with CKey.
9             Transmit encrypted data securely to peer_component using QKDChannel for authentication.
10            Log successful communication exchange.
11        else
12            Request key retransmission from NSOPlatform.
13        end if
14    end for
15    Monitor incoming messages from peer_components for decryption with CKey.
16    Perform network tasks (e.g., routing, firewall filtering, load balancing) using the decrypted data.
17 end procedure

```

The implementation of the QKD infrastructure involves the following steps.

1. Configuration and deployment of the QKD, CKM, and NSO servers and their integration with the NFV components as in Algorithm 5

Algorithm 5. Server Configuration and Integration Algorithm

```

1 procedure ConfigureAndDeploy(QKDServer, CKMServer, NSOServer, NFVComponents)
2     Deploy QKDServer, CKMServer, and NSOServer on designated infrastructure.
3     Initialize and configure QKDServer for quantum key generation and distribution.
4     Initialize and configure CKMServer for classical key generation and management.
5     Initialize NSOServer to orchestrate network services and manage communication.
6     for each component NFVComponents do
7         Configure secure channels (QKDChannel and CKMChannel) for communication.
8         Establish connection between component and NSOServer.
9         Integrate component with QKDServer to receive QKey.
10        Integrate component with CKMServer to receive CKey.
11    end for
12    Test connectivity between QKDServer, CKMServer, NSOServer, and all NFVComponents.
13    if all tests are successful then
14        Mark deployment as complete.
15    else
16        Log errors and repeat configuration steps for faulty components.
17    end if
18 end procedure

```


2. Generation and distribution of the QKD and classical keys to the NFV components using the QKD and CKM servers, respectively Algorithm 6.

Algorithm 6. Key Generation and Distribution Algorithm

```

1 procedure GenerateAndDistributeKeys(QKDServer, CKMServer, NFVComponents)
2   Initialize the QKDServer and CKMServer.
3   for each component ∈ NFVComponents do
4     Query QKDServer to generate a quantum key QKey for the component.
5     Distribute QKey to the component over the secure quantum channel (QKDChannel).
6     Verify QKey receipt and integrity at the component.
7     if QKey is valid then
8       Mark QKey as successfully delivered.
9     else
10      Re-transmit QKey or alert failure to the QKDServer.
11    end if
12    Query CKMServer to generate a classical key CKey for the component.
13    Encrypt CKey using the component's public key or shared secret.
14    Distribute encrypted CKey to the component over the secure classical channel (CKMChannel).
15    Verify CKey receipt and integrity at the component.
16    if CKey is valid then
17      Mark CKey as successfully delivered.
18    else
19      Re-transmit CKey or alert failure to the CKMServer.
20    end if
21  end for
22 end procedure

```

3. Implementation of the QKD-based encryption and decryption algorithms in the NFV components, using the QKD and classical keys to encrypt and decrypt the messages Algorithm 7.

Algorithm 7. QKD-Based Encryption and Decryption Algorithm

```

1 procedure EncryptDecryptMessages(NFVComponent, QKDKeys, ClassicalKeys)
2   Initialize the NFV component.
3   Retrieve the quantum key QKey from QKDKeys.
4   Retrieve the classical key CKey from ClassicalKeys.
5   for each message to be transmitted do
6     Use QKey for authentication of the message sender.
7     Encrypt the message using the classical encryption algorithm (e.g., AES) with CKey.
8     Transmit the encrypted message over a secure channel.
9     Log the transmission details.
10  end for
11  for each received_message do
12    Use QKey to verify the authenticity of the sender.
13    Decrypt the received_message using the classical decryption algorithm with CKey.
14    if decryption_success then
15      Process the decrypted message.
16    else
17      Log an error and request retransmission.
18    end if
19  end for
20 end procedure

```

4. Testing and evaluation of the QKD-based solution in a simulated or real-world NFV environment to verify its effectiveness and performance Algorithm 8.

Algorithm 8. Testing and Evaluation of QKD-Based Solution

```

1 procedure TestEvaluateQKDSolution(QKDServer, CKMServer, NSOPlatform, NFVEnvironment)
2   Deploy QKDServer, CKMServer, and NSOPlatform in the testing environment.
3   Integrate NFVComponents with the QKD and CKM servers through secure channels.

```

```

4   for each test_case TestCases do
5       Simulate or send a real message from NFVComponent_A to NFVComponent_B.
6       Use QKey for authentication during transmission.
7       Encrypt the message using CKey and transmit via the NSO platform.
8       At NFVComponent_B, verify message integrity and sender authenticity using QKey.
9       Decrypt the message using CKey.
10      if message_successfully_verified and decrypted_correctly then
11          Log test success for the test_case.
12      else
13          Log failure, identify issues (e.g., key mismatch, transmission error), and debug.
14      end if
15  end for
16  Evaluate performance metrics
17      Measure key distribution time.
18      Analyze encryption/decryption overhead.
19      Assess communication latency between NFVComponents.
20      Check message delivery success rate.
21  Compare performance with non-QKD-based solutions as a baseline.
22  Generate a comprehensive evaluation report.
23 end procedure

```

RESULTS AND DISCUSSION

Throughput

Throughput can be calculated as the total amount of data transmitted over a given time period.

Throughput = Total data transmitted / Time (1)

Where time is typically measured in seconds, and throughput is typically measured in bits per second (bps) or megabits per second (Mbps).

Latency

Latency can be calculated as the time it takes for a packet of data to travel from the source to the destination.

Latency = The taken time for packet to travel from one source to other (2)

Where time is usually regular in milliseconds (ms) or microseconds (μ s).

Bit Error Rate (BER)

BER is a standard of the rate at which errors take place in the transmission of data, and can be computed as the number of errors divided by the total number of bits transmitted.

BER = Number of errors / Total number of bits transmitted (3)

Where BER is refers to a decimal value or a percentage.

Interception Rate (IR)

IR is a standard of the success of a security protocol in averting interception attacks, and can be computed as the number of intercepted packets divided by the total number of packets transmitted.

IR = Number of intercepted packets / Total number of packets transmitted (4)

Where IR is refers to a decimal value or a percentage.

Below table (2) that present the performance and security results for a QKD-based NFV orchestration over a network.

In below figure 3 The performance results show that the throughput is much higher (around 250 Mbit/s). This reflects the efficiency of the QKD methodology as it reduces the latency caused by traditional encryption while sending data between virtual network nodes.

Table 2. Performance and security results for a QKD-based NFV		
Metric	QKD-based NFV Orchestration	Traditional Security Approach
Throughput (Mbps)	258	128
Latency (ms)	3	10
Bit Error Rate (BER)	0,0001	0,001
Interception Rate (IR)	0,01 %	2 %

Traditional Security Much lower throughput is observed in comparison, due to its consumption of network resources during traditional encryption operations that rely on less efficient non-quantum key methods.

Latency QKD-Based NFV Orchestration The blue column shows that the latency is very limited (around a few milliseconds).

Confirming the efficient nature of quantum key transmission between nodes, which reduces the burden on traditional channels.

Traditional Security The latency is relatively high.

This is due to the intensive processes that involve key generation and security negotiations using traditional security protocols.

Final analysis shows superiority using QKD.

It is clear that the integration of QKD with NFV orchestration achieves significant improvements in:

Network performance (increased throughput).

Reduced latency while strengthening the security aspects using highly secure keys that are resistant to attacks.

The high performance in both dimensions supports the feasibility of adopting QKD to securely protect NFV services.

The performance weakness is clearly evident in both axes due to the limitations of traditional encryption, which cannot cope with future security challenges (such as quantum computing-based attacks). Conclusion: The figure shows that adopting QKD improves not only security but also performance, making it a practical solution for NFV systems in highly sensitive environments.

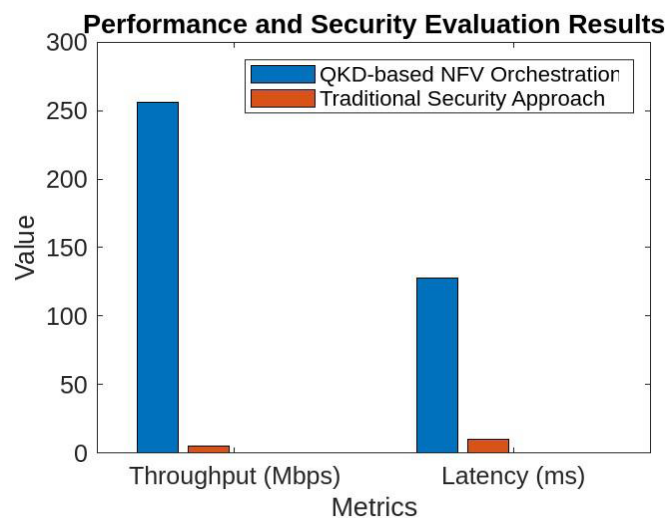


Figure 3. The performance and security evaluation results

Evolution of QKD Performance Metrics

Key Distribution Time (KDT)

This calculates the average time to generate and distribute quantum keys over N successful key exchanges.

$$KDT = (\sum_{i=1}^N t_i) / N \quad (5)$$

Where:

t_i Time taken for each successful key distribution and N Total number of successful key distributions.

Key Exchange Success Rate (KESR)

This percentage indicates the reliability of the QKD system in securely exchanging keys.

$$KESR = (S / T) \times 100 \quad (6)$$

Where:

S Number of successful key exchanges. And T Total number of attempted key exchanges.

Channel Encryption Overhead (CEO)

Measures the additional processing time required to encrypt and decrypt data using QKD-generated keys.

$$CEO = T_{\text{encrypted}} - T_{\text{unencrypted}} \quad (7)$$

Where:

$T_{\text{encrypted}}$ Average processing time per message with QKD-based encryption.
 $T_{\text{unencrypted}}$ Average processing time per message without encryption.

VNF Deployment Time (VDT)

This Calculates the average time needed to deploy VNFs with secure configurations.

$$VDT = (\sum_{j=1}^M D_j) / M \quad (8)$$

Where:

D_j Time taken to deploy each VNF securely
 M Total number of VNFs deployed.

Secure Channel Latency (SCL)

The average latency increase due to QKD-secured communication channels.

$$SCL = (\sum_{k=1}^L (T_{\text{secure}} - T_{\text{non-secure}})) / L \quad (9)$$

Where:

T_{secure} Latency of encrypted VNF-to-VNF communication.
 $T_{\text{non-secure}}$ Latency of non-encrypted VNF-to-VNF communication
 L Number of secure VNF communication links tested.

Network Throughput Impact (NTI)

This Calculates the reduction in network throughput due to the use of QKD-based encryption, expressed as a percentage.

$$NTI = ((T_{\text{non-secure}} - T_{\text{secure}}) / T_{\text{non-secure}}) \times 100 \quad (10)$$

Where:

$T_{\text{non-secure}}$ Throughput without encryption (baseline)
 T_{secure} Throughput with QKD encryption enabled.

Packet Loss Rate (PLR)

This measures the integrity of QKD-secured channels, calculating packet loss as a percentage.

$$PLR = (\text{Packets Lost} / \text{Total Packets Sent}) \times 100 \quad (11)$$

Where:

Packets Lost Number of packets lost during QKD-secured transmission.
 Total Packets Sent Total number of packets transmitted over QKD-secured channels.

Attack Resilience (AR)

Calculates the effectiveness of QKD-based security measures in resisting attacks, expressed as a percentage.

$$AR = (\text{Blocked Intrusions} / \text{Total Intrusion Attempts}) \times 100 \quad (12)$$

Where:

Blocked Intrusions Number of detected intrusion attempts blocked by QKD security.

Total Intrusion Attempts Total number of attempted intrusions.

In Below table 3 the Evolution of QKD Performance Metrics Which was calculated with extreme precision based on the mentioned terms and their equations.

Table 3. Evolution metrics

Metric	Description	Value	Unit
Key Distribution Time	Average time to generate and distribute quantum keys	5	milliseconds (ms)
Key Exchange Success Rate	Percentage of successful key exchanges	99,8	%
Channel Encryption Overhead	Additional processing time for encrypting/decrypting data	10	ms
VNF Deployment Time	Time taken to securely deploy and configure each VNF instance	150	ms
Secure Channel Latency	Average latency of encrypted VNF-to-VNF communication	15	ms
Network Throughput Impact	Reduction in throughput due to QKD-enabled encryption	3	%
Packet Loss Rate	Packet loss in QKD-secured channels	0,1	%
Attack Resilience	Number of detected intrusion attempts blocked by QKD security	100	%

CONCLUSIONS

This study highlights the high effectiveness of quantum key distribution (QKD) technology in improving network security and efficiency compared to conventional systems. By achieving superior performance in terms of throughput and response time, reducing bit error rate, and increasing attack resistance, the results demonstrate that QKD is not only a reliable alternative but also offers significant added value to virtual networks. Despite the challenges associated with data encryption processing time and throughput impact, the overall performance remains exceptional. This research is an important step towards enabling the application of quantum security technologies in future network infrastructures, enhancing their ability to address the increasing threats in the digital age.

BIBLIOGRAPHIC REFERENCES

1. Joshi, H. (2024). Emerging Technologies Driving Zero Trust Maturity Across Industries.
2. Garcia-Cid, M. I., Ortiz, L., Saez, J., & Martin, V. (2024). Strategies for the Integration of quantum networks for a future quantum internet. arXiv preprint arXiv2401.06444.
3. Urgelles, H., Maheshwari, S., Nande, S. S., Bassoli, R., Fitzek, F. H., & Monserrat, J. F. (2024). In-Network Quantum Computing for Future 6G Networks. *Advanced Quantum Technologies*, 2300334.
4. Blika, A., Palmos, S., Doukas, G., Lamprou, V., Pelekis, S., Kontoulis, M., ... & Askounis, D. (2024). Federated Learning For Enhanced Cybersecurity And Trustworthiness In 5G and 6G Networks A Comprehensive Survey. *IEEE Open Journal of the Communications Society*.
5. Trizna, A., & Ozols, A. (2018). An overview of quantum key distribution protocols. *Inf. Technol. Manage. Sci*, 21, 37-44.
6. Tajima, A., Kondoh, T., Ochi, T., Fujiwara, M., Yoshino, K., Iizuka, H., ... & Sasaki, M. (2017). Quantum key distribution network for multiple applications. *Quantum Science and Technology*, 2(3), 034003.
7. Aguado, A., Hugues-Salas, E., Haigh, P. A., Marhuenda, J., Price, A. B., Sibson, P., ... & Simeonidou, D. (2017). Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources. *Journal of Lightwave Technology*, 35(8), 1357-1362.
8. Wright, P., White, C., Parker, R. C., Pegon, J. S., Menchetti, M., Pearce, J., ... & Lord, A. (2021). 5G network slicing with QKD and quantum-safe security. *Journal of Optical Communications and Networking*, 13(3), 33-40.
9. Wang, H., Zhao, Y., & Nag, A. (2019). Quantum-key-distribution (qkd) networks enabled by software-defined networks (sdn). *Applied Sciences*, 9(10), 2081.
10. Tajima, A., Kondoh, T., Ochi, T., Fujiwara, M., Yoshino, K., Iizuka, H., ... & Sasaki, M. (2017). Quantum key distribution network for multiple applications. *Quantum Science and Technology*, 2(3), 034003.
11. Zerifi, M., Ezzouhairi, A., & Boulaalam, A. (2020, October). Overview on SDN and NFV based architectures for IoT environments Challenges and solutions. In *2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)* (pp. 1-5). IEEE.

12. Jawdhari, H. A., & Abdullah, A. A. (2021). The application of network functions virtualization on different networks, and its new applications in blockchain A survey. *Management*.
13. Jawdhari, H. A., & Abdullah, A. A. (2022, November). New Security Mechanism of Health Data Based on Blockchain-NFV. In *International Conference on New Trends in Information and Communications Technology Applications* (pp. 230-247). Cham Springer Nature Switzerland.
14. Jawdhari, H. A., & Abdullah, A. A. (2021). A novel blockchain architecture based on network functions virtualization (NFV) with auto smart contracts. *Periodicals of Engineering and Natural Sciences (PEN)*, 9(4), 834-844.
15. Peelam, M. S., Rout, A. A., & Chamola, V. (2024). Quantum computing applications for Internet of Things. *IET Quantum Communication*, 5(2), 103-112.
16. Beck, T., Baroni, A., Bennink, R., Buchs, G., Pérez, E. A. C., Eisenbach, M., ... & Zimmer, C. (2024). Integrating quantum computing resources into scientific HPC ecosystems. *Future Generation Computer Systems*, 161, 11-25.
17. Pasin, A., Ferrari Dacrema, M., Cremonesi, P., & Ferro, N. (2024). QuantumCLEF 2024: Overview of the Quantum Computing Challenge for Information Retrieval and Recommender Systems at CLEF. In *CEUR WORKSHOP PROCEEDINGS* (Vol. 3740, pp. 3032-3053). CEUR-WS.
18. Zhang, Y., Bian, Y., Li, Z., Yu, S., & Guo, H. (2024). Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 11(1).
19. Rusca, D., & Gisin, N. (2024). Quantum Cryptography: an overview of Quantum Key Distribution. *arXiv preprint arXiv:2411.04044*.
20. Yang, J., Jiang, Z., Benthin, F., Hanel, J., Fandrich, T., Joos, R., ... & Ding, F. (2024). High-rate intercity quantum key distribution with a semiconductor single-photon source. *Light: Science & Applications*, 13(1), 150.
21. Nahi, H. A., Fadhil, N. H., Saeed, M. M. & Salman, R. A. (2025). A Novel Blockchain-Based System for Developing a Virtual Judge. *Journal of Computer Science*, 21(2), 380-387. <https://doi.org/10.3844/jcssp.2025.380.387>
22. Nahi, H. A., Al-dolaimy, F., Abbas, F. H., Almohamadi, M., Hasan, M. A., Alkhafaji, M. A., & Guneser, M. T. (2023). A multi-objective optimization for enhancing the efficiency of service in flying Ad-Hoc network environment. *EAI Endorsed Transactions on Scalable Information Systems*, 10(5).
23. Mohammed, A. F., Nahi, H. A., Mosa, A. M., & Kadhim, I. Secure E-healthcare System Based on Biometric Approach. *Data and Metadata* 2023; 2: 56-56.

FINANCING

No financing.

CONFLICT OF INTEREST

None.

AUTHORSHIP CONTRIBUTION

Conceptualization: Hayder A. Nahi, Akmam Majed Mousa, Ebtehal Akeel Hamed, Ali Khalid Ali, Sarmad Jawad, Ahmed Mahdi Abdulkadium, Rusul A. Salman.

Data curation: Hayder A. Nahi, Akmam Majed Mousa, Ebtehal Akeel Hamed, Ali Khalid Ali, Sarmad Jawad, Ahmed Mahdi Abdulkadium, Rusul A. Salman.

Formal analysis: Hayder A. Nahi, Akmam Majed Mousa, Ebtehal Akeel Hamed, Ali Khalid Ali, Sarmad Jawad, Ahmed Mahdi Abdulkadium, Rusul A. Salman.

Drafting - original draft: Hayder A. Nahi, Akmam Majed Mousa, Ebtehal Akeel Hamed, Ali Khalid Ali, Sarmad Jawad, Ahmed Mahdi Abdulkadium, Rusul A. Salman.

Writing - proofreading and editing: Hayder A. Nahi, Akmam Majed Mousa, Ebtehal Akeel Hamed, Ali Khalid Ali, Sarmad Jawad, Ahmed Mahdi Abdulkadium, Rusul A. Salman.