O-RAN next Generation Research Group (nGRG)

Research Report

Research Report on Quantum Security

Report ID: RR-2023-04

Contributors:

HCLSoftware

CICT

Dell

Nokia

Rakuten Mobile

Reliance Jio

Qualcomm

Release date: 2023.09

Authors

Swaminathan Arunachalam	HCLSoftware (Editor-in-Chief)
Alex Reznik	Dell
Aritra Banerjee	Nokia
Clifton Fernandes	Nokia
Prabhu K	Rakuten Mobile
Raghavendran Ramiya	Rakuten Mobile
Ravi Sinha	Reliance Jio
Sanket Gaikwad	Reliance Jio
ShiHan Bao	CICT
Soo Bum Lee	Qualcomm
Uday Joshi	Reliance Jio

Disclaimer

Copyright

Executive summary

Quantum computing poses threats to the security of mobile systems. Both public-key and symmetric-key cryptographic algorithms that are widely used in mobile systems as of today would become vulnerable to quantum attacks. The mobile industry needs to transition to quantum-resistant cryptography to ensure the security and integrity of communications in mobile systems. PQC and QKD are fields of research that aims to develop new cryptographic algorithms that are secure against quantum attacks. There are few challenges such as performance, interoperability that need to be addressed in order to adopt those new algorithms for secure communication in future mobile systems.

Table of Contents

Authors 2
Disclaimer 2
Executive summary 3
List of abbreviations 5
List of figures 7
List of tables 7
1 Background 8
2 Objectives and scope 8
3 Introduction 9
4 Quantum's 6G Security threats 10
4.1 Quantum threats to cryptographic algorithms 11
4.2 Quantum threats to cellular systems 12
4.2.1 Symmetric key algorithms 12
4.2.2 Public key algorithms 13
5 Quantum's opportunities in 6G security 16
1.1 Quantum Secure Communication 17
1.2 Quantum key generation and distribution 17
1.4 Quantum secure direct communication (QSDC) 18
6 Quantum readiness in 6G 19
6.1 Cryptographic techniques to mitigate quantum threats 19
6.1.1 Computational Post-quantum cryptography (PQC) 19
6.1.1.1 Challenges in adopting Post-quantum cryptography (PQC) 20
6.2 Other techniques 21
6.3 Building Secure Communication Systems 23
6.4 Standardization efforts 26
References 27
Copyright 31

List of abbreviations

3GPP - 3rd Generation Partnership Project

5G-AKA - 5G Authentication and Key Agreement

6G - Sixth Generation (of wireless communication)

ACME - Automatic Certificate Management Environment

AES - Advanced Encryption Standard

AKA - Authentication and Key Agreement

AS - Access Stratum

BB84, E91, BBM92, B92, MSZ96, SRG04, COW, KMB08, T12, HDQKD - Different protocols or algorithms for Quantum Key Distribution (QKD)

BRSKI - Bootstrapping Remote Secure Key Infrastructure

CA - Certificate Authority

CAGR - Compound Annual Growth Rate

CCSA - China Communications Standards Association

CMPv2 - Certificate Management Protocol version 2

CRQC - Cryptographically Relevant Quantum Computer

CRYSTALS-Dilithium - A post-quantum cryptographic candidate algorithm for digital signature

CRYSTALS-Kyber - A post-quantum cryptographic candidate algorithm for public-key encryption

EAP-AKA - Extensible Authentication Protocol for AKA

EAP-TLS - Extensible Authentication Protocol with Transport Layer Security

ECC - Elliptic Curve Cryptography

FALCON - A post-quantum cryptographic candidate algorithm for digital signature

FrodoKEM - A post-quantum cryptography candidate algorithm

IEEE - Institute of Electrical and Electronics Engineers

IKE - Internet Key Exchange

IPsec - Internet Protocol Security

ISO/IEC JTC 1/SC 27 WG3 - International Organization for Standardization / International Electrotechnical Commission Joint Technical Committee 1 / Subcommittee 27 Working Group 3

ITU-T - International Telecommunication Union - Telecommunication Standardization Sector

JWE - JSON Web Encryption

JWS - JSON Web Signature

JWT - JSON Web Token

KEM - Key Encapsulation Mechanisms

LMS - Leighton-Micali Signature Scheme

mTLS - Mutual Transport Layer Security

NAS - Non-Access Stratum

NDS - Network Domain Security

NIST - National Institute of Standards and Technology

NSA - National Security Agency

PKI - Public Key Infrastructure

PQC - Post-Quantum Cryptography

QKD - Quantum Key Distribution

QRAND - Quantum Random Number Generation

QRNG - Quantum Random Number Generator

QSDC - Quantum Secure Direct Communication

Qubits - Quantum Bits

RFC - Request for Comments

RNIB - Radio Network Information Base

RSA - Rivest–Shamir–Adleman (a widely-used public-key encryption algorithm)

SaaS - Software as a Service

SASE - Secure Access Service Edge

SBOM - Software Bill of Material

SIKE - Supersingular Isogeny Key Encapsulation

SPHINCS+ - A post-quantum cryptographic candidate algorithm for digital signature

ST7 - State Technical Committee 7

SUCI - Subscriber Concealed Identifier

SUPI - Subscriber Permanent Identifier

SZTP - Secure Zero-Touch Protocol

TLS - Transport Layer Security

TS - Technical Specification

VPN - Virtual Private Network

XMSS - Extended Merkle Signature Scheme

802.1x - IEEE 802.1X

List of figures

Figure 1: NIST PQC Competition Milestones as in [8] 10
Figure 2: QRAND with a QKD secured satellite link 18
Figure 3: The Mosca model for evaluating PQC migration timeframe as in [8] 25

List of tables

Table 1: Example of PQC algorithm selection for applications 20

1 Background

Quantum computing is set to change the dynamics of computing within the next decade. What was hitherto impossible to decrypt the current encrypted information, would be possible to break the current encrypted data within a matter of days, if not hours using the quantum computing capabilities [1]**Error! Reference source not found.**.

Quantum safe cryptography is intended to protect the information exchange between individual users or data sources using algorithms that are resistant to attacks by both classical and quantum computers and keep this information secure even with the development of a mature quantum computing capability.

NIST has initiated the process of the Post Quantum Cryptography (PQC) standardization in 2017. As part of this initiative, NIST has announced the standard candidates of four post-quantum cryptographic algorithms for public-key encryption (CRYSTALS-Kyber), and for digital signature (CRYSTALS-Dilithium, FALCON and SPHINCS+) on 5th Jul 2022. These algorithms are developed to resist against attacks leveraging quantum computing.

These PQC techniques that would have implications for enterprises, defense, governments, factory automation, education, power and transport infrastructure, and telecom infrastructure services, are expected to be standardized in 2 years. Global Quantum cryptography market is projected to reach USD 2587.7 Million by 2028, growing at a CAGR of 38.10% [2].

While much work is on-going across these topics, it is proposed as part of this Research Item to explore a holistic 6G security threat landscape related to quantum computing and application of PQC algorithms to mitigate potential threats, especially in those areas which differ in significant aspects from 5G.

2 Objectives and scope

This Research Item aims to provide a perspective on the Post-Quantum Cryptographic algorithms selected by NIST with regard to the 6G threat landscape. The result is expected to be largely based on existing industry and academia work. The resulting output should provide a rough classification of the various threats based on risk/impact profile and potential mitigation techniques using PQC, thus serving as a reference to guide further research. Detailed analysis of potential solutions (if any) is out of scope for this Research Item.

3 Introduction

Classical cryptography is divided into two types: symmetric and public-key (asymmetric) cryptography. These methods rely on mathematical problems that are challenging for traditional computers to solve. However, the rise of quantum computers and advanced algorithms like Shor's Algorithm has made public-key cryptography vulnerable. As a result, quantum-resistant algorithms are needed to mitigate this risk. Furthermore, Grover's Algorithm for symmetric cryptography can expedite the key search process, potentially making symmetric encryption vulnerable as well. This has led to a need for quantum-resistant symmetric cryptography algorithms.

Post-quantum cryptography (PQC) refers to a family of asymmetric cryptographic algorithms, which are conjectured to be quantum resistant as explained in [3]. In other words, they are based on mathematical problems that appear to be intractable even for a largescale quantum computer. These algorithms will eventually replace the algorithms that underpin today’s public-key infrastructure, such as the earlier-mentioned RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) algorithms, as well as the accompanying public-key encryption, key-exchange, and digital signature schemes. RSA-based protocols rely on the hardness of finding the prime factors of large integers, while elliptic curve-based methods and Diffie-Hellman key exchanges rely on the hardness of the discrete log problem.

A CRQC (Cryptographically Relevant Quantum Computer) is a quantum computer, capable of breaking today’s real world cryptographic algorithms currently used for public-key encryption, key exchange, and digital signature. Specifically, CRQCs [4] will be built with sufficient size, much larger, more robust, and fault-tolerant than normal Quantum computers.

The National Institute of Standards and Technology (NIST) is actively working to standardize PQC algorithms. Figure 1 illustrates the competition-like process that NIST initiated in 2016 to select new algorithms for standardization. After three evaluation rounds, NIST selected for standardization four cryptographic primitives for Key Encapsulation Mechanisms (KEM) and Digital Signatures, presented in Table 1. Note that the table does not include the Extended Merkle Signature Scheme (XMSS) and the Leighton-Micali Signature Scheme (LMS), which are stateful, hash-based, quantumsafe signature schemes and have already been standardized by NIST [5]. The reason is that NIST did not consider stateful algorithms for this competition. Shortly after this announcement on July 5th, 2022, researchers broke the Supersingular Isogeny Key Encapsulation (SIKE) algorithm [6], one of the candidates for the 4th round. A first draft of the NIST standard is expected in 2023 and the final standard is anticipated by 2024. Apparently, each of these algorithms presents certain tradeoffs, and NIST is currently evaluating the different options to compare the many aspects including security, performance, resistance to side-channel attacks, simplicity, and flexibility [7]. The latter notion of flexibility pertains to a very important concept of cryptographic agility, which is extremely relevant to the

migration process towards post-quantum cryptography. Cryptographic agility refers to the capacity of a system to accommodate, exclude or update new and obsolete algorithms, without severe impact to the existing infrastructure.

Figure 1: NIST PQC Competition Milestones as in [8]

Both public-key and symmetric cryptography are widely used in mobile networks for security protocols such as IPsec/IKE and TLS. As quantum computing continues to advance, it is essential for the industry to transition to quantum-resistant cryptography to ensure the security and integrity of communications.

4 Quantum's 6G Security threats

The security threats posed by Quantum technology to next generation network are a concern. In the current 5G era, Public Key Cryptography is used in various security domains, including Network domain security, and Service-Based Architecture (SBA) domain security.

Symmetric cryptography is used for the protection of the Non-Access Stratum (NAS) and Access Stratum (AS) using 128-bit symmetric key algorithms.

The 3GPP Authentication and Key Agreement (AKA) protocol is used for authentication, and 5G networks define three authentication methods: 5G-AKA, EAP-AKA', and EAP-TLS.

Quantum cloning and quantum collision attacks are potential threats that may lead to a loss of confidentiality, integrity, and availability of data transmitted in 5G or next-generation networks. It has been shown that a quantum state may be precisely copied

via a number of efficient cloning methods [9]. Quantum cloning attacks are a possible kind of quantum hacking in a secure quantum channel, even with high dimensional QKD techniques. Furthermore, when two different inputs to a hash function provide the same output in a quantum setting, quantum collision attacks can also take place.

Satellite communications used in 5G, or next-generation networks are also vulnerable to quantum attacks, and it is crucial to support promising PQC algorithms such as lattice-based cryptography and code-based cryptography to enhance security. Algorithm negotiation, key sizes, signature sizes, ciphertext size, and performance are important factors that should be carefully evaluated during the design phase to ensure a secure and robust network.

While quantum computers are not yet powerful enough to threaten classical cryptography, we need to also acknowledge the risks of the “harvest-now-decrypt later” threat. While quantum computers are not yet powerful enough to threaten classical cryptography, we need to also acknowledge the risks of the “harvest-now-decrypt later” threat. Most of the encrypted data we transfer today for managing and controlling the network might be prone to this threat [8]. Crypto-agility for migration is one of the many strategies to mitigate the risk of the "Harvest Now, Decrypt Later" problem.

4.1 Quantum threats to cryptographic algorithms

Technical advances of Quantum computing would threaten cellular system security since the cryptographic algorithms widely used in today's cellular system can be broken or at least weakened by Quantum algorithms such as Shor’s Algorithm [10] or Grover’s Algorithm [11].

Shor’s algorithm, leveraging the Quantum Fast Fourier Transform, can break the public key cryptographic algorithms such as RSA and ECC in polylogarithmic time.

Grover’s algorithm provides quadratic speedup in solving the unstructured search problem, which can be used to reduce the security level of symmetric key algorithms (e.g., AES) by half. Hence there is an assumption that Grover’s algorithm theoretically requires us to double the key sizes of the algorithms we deploy today to achieve quantum resistance.

For example, with Grover’s algorithm a 128-bit symmetric cryptography will need 2^64 quantum operations (instead of 2^128 classical operations), which might sound computationally feasible however, the following considerations illustrate that this is not the case:

- Whereas 2^64 operations performed in parallel are feasible for modern classical computers, 2^64 quantum operations performed serially in a quantum computer are not feasible.
- Grover’s algorithm is highly non-parallelizable. Even if we deploy 2^c computational units in parallel to brute-force a key using Grover’s algorithm, it

will complete in time proportional to 2^(128-c)/2, or put simply, running even hundreds of quantum computers in parallel would offer negligible advantage gains to attack the key [12], [13].

How can we then be sure that an improved algorithm won't outperform Grover's algorithm in the near future? Firstly, Christof Zalka has shown that Grover's algorithm, and in particular its non-parallel nature, achieves the best possible complexity for an unstructured search [14]. Secondly, in their evaluation criteria for PQC, NIST is considering a security level equivalent to that of AES-128. In other words, NIST has confidence in standardizing parameters for PQC that offer similar levels of security as AES-128 does [12].

Ongoing research to reduce the time complexity and the Quantum resource requirements for Shor's algorithm and Grover's algorithm and the corresponding Quantum resource estimate [15][16] [17] [18] indicate that the latest Quantum computers (e.g., IBM Osprey [19], Google Sycamore [20]) have made significant progress in term of number of Qubits, yet they are still far from practical to become a real threat to the widely used cryptographic algorithms as of writing of this report. However, considering the longevity of the cellular systems (e.g., 20 or more years) and the time to adopt new cryptographic algorithms, introduction of Quantum-safe technology for 6G is deemed necessary. It may even be necessary during 5G timeframe, NSA has recently published the CNSA 2.0 [21] which recommends to NSS operators to transition to PQC by 2025.

On a final note, we witness some interesting attacking advancements leveraging concepts from Quantum Signal Processing and we encourage the research and industry communities to stay alert for developments in this area [22].

4.2 Quantum threats to cellular systems

4.2.1 Symmetric key algorithms

In 3GPP systems, symmetric key based cryptographic algorithms are widely used for authentication and secure communication between UE and network as well as between network functions and they are mostly based on 128-bit algorithms. The primary authentication algorithms such as 5G AKA (Authentication and Key Agreement) and EAP-AKA' are specified in TS 33.501 [23] and they use the MILENAGE Algorithm Set specified in TS 35.909 [24] or TUAK Algorithm Set specified in TS 35.231 [25]. While TUAK supports both 128-bit and 256-bit algorithms, the MILENAGE only supports 128-bit algorithms. These algorithms are not only used for 5G but also used for prior generations of 3GPP system, e.g., 3G and 4G.

Meanwhile, security algorithms for NAS (Non-Access Stratum) security between UE and AMF and AS (Access Stratum) security between UE and base station (i.e., gNB) use 128-bit algorithms for both ciphering and integrity protection as listed below (see TS 33.501[23]).

- Encryption algorithms: 128-NEA1, 128-NEA2, 128-NEA3
    - 128-NEA1 is based on SNOW 3G specified in TS 35.215 [26]
    - 128-NEA2 is based on 128-bit AES [27] in CTR mode [28]
    - 128-NEA3 is based on 128-bit ZUC specified in TS 35.221 [29]
- Integrity protection algorithms: 128-NIA1, 128-NIA2, 128-NIA3
    - 128-NIA1 is based on SNOW 3G specified in TS 35.215 [26]
    - 128-NIA2 is based on 128-bit AES [26] in CMAC mode [30]
    - 128-NIA3 is based on 128-bit ZUC specified in TS 35.221 [26]

For IPsec and TLS used to protect the traffic between network functions, support of 128-bit algorithms is mandatory and support of 256-bit algorithms is optional (recommended). The IPsec and TLS cipher suites that need to be supported by the network products profiled in TS 33.210 [31].

To be resilient against Quantum attacks, 256-bit algorithms need to be used and 3GPP is currently discussing adoption of 256-bit algorithms in coordination with ETSI SAGE (Security Algorithms Group of Experts). Considering the lifetime of each generation of the 3GPP systems (e.g., 20 years or more), the 256-bit algorithms are expected to be adopted for 5G in 3GPP (i.e., 5G Advanced).

4.2.2 Public key algorithms

The public key based cryptographic algorithms are widely used for authentication and key agreement (or encapsulation) between network functions in the 3GPP system as well as the O-RAN system. More specifically, certificate-based authentication in IKEv2 in IPsec and TLS handshake relies on public-key based cryptographic algorithms such as RSA or ECC. Also, the public key algorithms for certificate management protocol in the 3GPP systems (i.e., CMPv2) are profiled in TS 33.310 [32].

In addition, 5G introduced the SUPI (Subscriber Permanent Identifier) privacy protection mechanism to defeat IMSI catcher [33]**Error! Reference source not found.**, which uses public key encryption of SUPI (which is called SUCI – Subscriber Concealed Identifier).

4.2.2.1 Usage in the 3GPP system

The Network domain security specified in TS 33.210 [31] defines the security architecture for network domain IP based control planes and serves as a repository for 3GPP profiles of protocols above the IP layer. The profiles for IKEv2, TLS, JSON Web Encryption (JWE) [34], and JSON Web Signature (JWS) [35] include the public key algorithms. Also, authentication framework specified in TS 33.310 [32] defines the

PKI architecture and profiles for various NDS/IP and TLS deployment scenarios, and certificate enrolment for base stations.

Such protocols and profiles are used to protect various interfaces defined in 3GPP system including those between network elements, between network element and security gateway (SEG), between security gateways and TLS entities within or between operator networks. Example interfaces and the corresponding security protocols are listed below.

- N2: interface between gNB and AMF, IPsec/DTLS
- N3: interface between gNB and UPF, IPsec
- N9: interface between UPFs, IPsec
- Xn: interface between gNBs, IPsec
- N32-c: inter PLMN interface between SEPPs (Security Edge Protection Proxy), TLS
- N32-f: inter PLMN interface between SEPPs (via IPX), TLS (PRINS over TLS/IPsec or TLS)
- PRINS: Protocol for N32 Interconnect Security, JWE/JWS
- F1: interface between gNB-CU and the gNB-DU, IPsec/DTLS, IKEv2
- E1: interface between gNB-CU-CP and the gNB-CU-UP, IPsec/DTLS, IKEv2

The Service-Based Architecture (SBA) in the 5G core network (5GC) requires all network functions to support mutually authenticated TLS and HTTPS and to support both server-side and client-side certificates. The SBA certificate profiles for TLS client and server certificates are specified in TS 33.310 [32]. In addition to TLS, NDS/IP can still be used between network functions in 5GC. For validation of service authorization, OAuth 2.0 authorization framework specified in RFC 6749 [36] is used in 5GC and JSON Web Token (JWT) [37] secured with JSON Web Signature (JWS) [35] is used as an access token.

Additionally, certificate-based authentication and JWT with JWS are used for Edge applications in 3GPP (see TS 33.558) [38].

4.2.2.2 Usage in the O-RAN system

Public key algorithms are more widely used in O-RAN. In addition to IPsec and TLS, O-RAN defines Port-based network access (i.e., IEEE 802.1x) for the access to the Open Fronthaul interface, which is based on either a manufacture certificate (for on-boarding) or an operator certificate. Similar to the 3GPP system, authorization is based on the JWT with JWS, while O-RAN only allows digital signature for JWS.

The O-RAN defined interfaces (in addition to 3GPP defined interfaces) require certificate-based authentication and key agreement include:

- C/U/S and M-Plane: interface between O-DU and O-RU, 802.1X certificate-based authentication, mTLS
- A1: interface between SMO (including Non-Realtime RIC) and Near-Realtime RAN Intelligent Controller (RIC), mTLS
- O1: interface between SMO and O-RAN elements, mTLS
- O2: interface between SMO and O-Cloud, mTLS
- R1: interface between Non-Realtime RIC and rApp, mTLS
- E2: interface between Near-Realtime RIC and O-CU-CP/UP between Near-Realtime RIC and O-DU, IPsec

In addition to certificate enrolment based on CMPv2 as in 3GPP system, O-RAN considers further automation using ACME (Automatic Certificate Management Environment) [39], SZTP (Secure Zero-Touch Protocol) [40] and BRSKI (Bootstrapping Remote Secure Key Infrastructure) [41], each of which is based on the architecture utilizing public key algorithms.

For software security and lifecycle management, O-RAN requires software bill of material (SBOM) [42], App signing and App enrolment procedures that all rely on public key algorithms as listed below.

- Software signing/verification requires public key algorithms (digital signature) and PKI
- Software Bill of Material (SBOM) requires signing/verification using public key algorithms and PKI
- xApp/rApp signing/verification/onboarding (or registration) requires public key algorithms and PKI

Near-Realtime RIC and Non-Realtime RIC can employ PKI algorithms to secure sensitive data (e.g., RNIB, network policy data, performance data, configuration data, operational data) at rest.

Finally, public key algorithms are used to ensure O-Cloud platform security (e.g., secure boot) and secure storage (e.g., for key storage).

5 Quantum’s opportunities in 6G security

The utilization of quantum technologies in communication systems has the potential to offer substantial advantages. As next generation networks continue to be developed, the importance of implementing quantum technologies in communication systems is increasing. In the realm of quantum-based secure communication protocols, there are several opportunities for quantum technologies, particularly in the areas of quantum key distribution (QKD), quantum secure direct communication (QSDC), and quantum secret sharing (QSS).

QKD is a technique that utilizes the principles of quantum mechanics to establish a secret key between two parties, as opposed to traditional encryption methods that rely on complex mathematical problems. In light of the growing threat posed by quantum computers, QKD will become an essential tool for secure communication in next generation networks. Specifically, QKD can be used to establish a secure key for post-quantum cryptography (PQC), which will be a vital component of secure communication in the next generation of networks.

QSDC is a technique that enables two parties to communicate with each other in a secure manner without the need for a shared key [43]. This is achieved through the use of quantum mechanics principles, ensuring the communication remains completely secure, and cannot be intercepted and read by an eavesdropper. QSDC will prove to be an essential tool for secure communication in next generation networks, particularly in cases where direct communication between two parties is necessary.

Other quantum-based secure communication protocols, such as Quantum Digital Signature (QDS) and Quantum Secret Sharing (QSS), offer secure authentication and sharing of secret information, respectively [44] [45]. QSS uses quantum mechanics principles to ensure complete security during communication. As opposed to traditional secret sharing methods that rely on mathematical algorithms, QSS is entirely secure, making it an important tool for secure communication in next generation networks, especially in situations where a group of parties need to share a secret key.

Quantum technology is advancing rapidly, and research is continuously underway to develop solutions for managing quantum threats in various applications. One such approach involves post-quantum cryptography (PQC), which requires the development of new cryptographic algorithms capable of resisting quantum attacks. Additionally, quantum key distribution (QKD) can be used to securely distribute cryptographic keys using the principles of quantum mechanics.

1.1 Quantum Secure Communication

Existing Telco networks, advance Applications and IT networks highly rely on PKI based security fabric which would become the major targets for the quantum attacks as compromise of a Certificate Authority (CA) certificate would compromise the security of the entire system whose security relies on the integrity of the CA.

Quantum Key Distribution (QKD) aims to protect the information transferred between individual users or data sources within one network. QKD enables a key sharing between a sender and a recipient using the quantum mechanical properties of photons. QKD provides anti-interception property since any attempts of key identification by measuring the photon would inevitably change the photon's state.

Drivers for the Quantum secure communication include

- Ever increasing datacenter workloads and widely used PKI based SASE.
- Increasing complexity of classical binary computing systems
- Growing preference for (SaaS) business models

Potential uses of the Quantum secure communication include

- Next Generation 6G SASE.
- Defense and Enterprise Infra Security
- Quantum Internet

1.2 Quantum key generation and distribution

1.3 QRAND - Quantum Random Number Generation

Quantum Random Number Generation mechanism is gaining momentum in two frameworks, one where the QRAND (Quantum Random number) is generated locally whereas the more scalable model where the QRAND is generated remotely and delivered via Quantum secured linked from Satellites.

1. Generating Quantum Random number locally with QRNG (Generator) powered by local Quantum source with the highest level of Entropy. QRNs are delivered to the key vaults by the Optical ground receivers and distributed to Network elements and end points with a Quantum secured Quantum Cloud NW.
2. Satellite based Quantum Encryption generates Entropy at the satellite and injects it to Quantum safe cloud, so that the end nodes and end elements generates trust less keys. Here data is quantum encrypted and transactions are signed with quantum key distribution of these QRAND with a QKD secured satellite link to the ground receivers and distributed by a fully secured Optical fiber Quantum Cloud network to all connected Distributed Telco network elements as well as end points.

Note: Ground receivers may send the QRNs to the Vaults on IPSEC or extended Quantum cloud with Quantum secured generic or proprietary solutions.

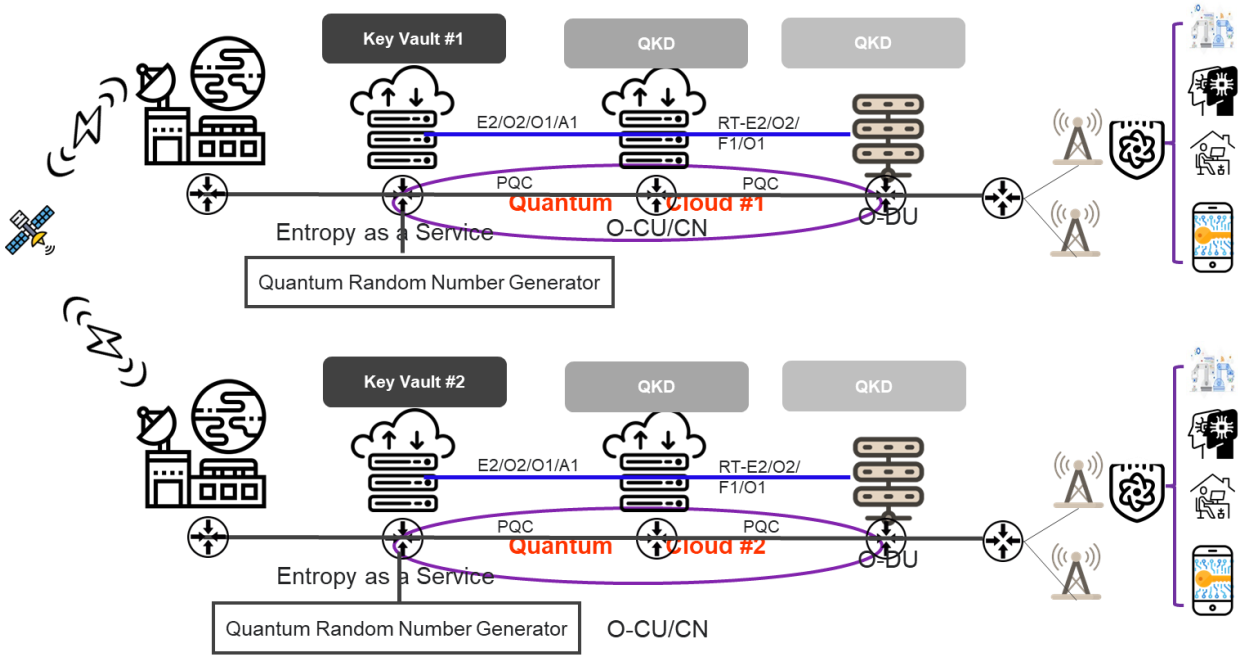

Figure 2: QRAND with a QKD secured satellite link

1.3.1.1 QKD

Quantum Key Distribution (QKD) is an integral part of Quantum encryption. It's a unique set of protocols, which promotes the growth of initial secret key among a two-party communication to the scaled one by providing a mechanism to securely generate symmetric keys. QKD systems are developed for use in large-scale networks, and an open architecture for QKD-based silicon packaged with devices can improve security, interoperability, innovation, and transparency. In this way no classic or Quantum attack will be able to break the security ecosystem protected by QKD.

Within a QKD Protocol stack framework, Quantum Signals are transmitted on a quantum channel, where the signal encapsulates Qubits being transmitted between the two parties and it provides the capabilities to the two ends to detect the legitimacy and the information is not changed, with the secured and authentic delivery. Equivalent pair used within QKD protocol framework may or may not use Quantum entanglement.

QKD is limited by the attenuation in the propagation medium within the quantum channel, which limits the propagation distance. Photons are the carriers of QKD.

BB84, E91, BBM92, B92, MSZ96, SRG04, COW, KMB08, T12, HDQKD are some of the examples of QKD protocols being used in Quantum Key distribution.

1.4 Quantum secure direct communication (QSDC)

QSDC is a method of securely transmitting information without the need of cryptographic keys that has the potential to provide a very secure and efficient way of

communication. When the parties exchange random keys rather than private information, QSDC can work as a deterministic QKD.

In contrast to QKD, which focuses on building safe cryptographic keys, particularly for symmetric key cryptography, QSDC is a protocol that permits direct secure transmission of quantum information between parties without the need of pre-established keys.

The implementation of QSDC protocols varies, but the unifying purpose is to securely transfer quantum states from one party (say, Alice) to another (say, Bob). To accomplish secure communication, these methods often employ quantum entanglement or quantum teleportation concepts. Alice can transmit quantum information to Bob in such a way that any effort to intercept the information is detectable by using the features of entangled particles or quantum entanglement swapping methods.

QSDC maintains the secrecy and integrity of transmitted quantum states by utilizing entanglement, quantum teleportation, and other quantum phenomena, enabling for secure quantum communication applications such as quantum cryptography and quantum computing protocols. [46]

QSDC aims to provide secure and direct communication channels that are resistant to eavesdropping. It eliminates the need for a prior shared key exchange, which is a requirement in protocols like Quantum Key Distribution (QKD).

6 Quantum readiness in 6G

6.1 Cryptographic techniques to mitigate quantum threats

6.1.1 Computational Post-quantum cryptography (PQC)

The transition to post-quantum security in next generation networks is expected to be smoother for symmetric protocols since Grover's method poses less of a quantum threat to them. This means that the same cryptographic techniques can still be used, but with a better degree of security, such as larger key sizes for AES.

For Public-key (asymmetric) cryptography method, a couple of post-quantum cryptography (PQC) algorithms, including lattice-based, code-based, hash-based, and multivariate-based ones, are being developed and tested. These PQC algorithms are designed to resist quantum computer attacks and can be applied to encryption (NIST PQC candidate algorithms called CRYSTALS-KYBER [21] and FrodoKEM), key exchange (NIST PQC candidate algorithm called CRYSTALS-KYBER [21]), digital signatures (NIST PQC candidate algorithms CRYSTALS-DILITHIUM, SPHINCS+ and FALCON [21]), and hash functions (NIST PQC candidate algorithm called SPHINCS+). PQC algorithms are expected to address potential threats posed by quantum computing and ensure the security of sensitive data and communications.

6.1.1.1 Challenges in adopting Post-quantum cryptography (PQC)

There are a set of challenges in adopting PQC for O-RAN and 3GPP systems.

Performance

PQC algorithms and their operations may require more computational resources than existing cryptographic algorithms, resulting in higher energy consumption [47] due to increased CPU and memory resources utilization for cryptographic operations of O-RAN and 3GPP systems. Even though Standard bodies would specify a variety of PQC schemes and associated parametric variations along with different levels of Energy consumption based on different security levels, it would be a very complex problem for the Mobile Network Operators (MNOs) to adopt the appropriate PQC algorithms for various use cases without compromising their efficiency and security protection. This may lead to a non-optimal and sub-optimal choice of PQC algorithms resulting in higher consumption of resources and energy in O-RAN and 3GPP systems. To address these challenges, need an optimal and efficient method to identify the appropriate PQC algorithms for Network Functions and Applications and its interfaces is required. Following approaches could be considered while adopting PQC algorithms in O-RAN and 3GPP systems.

Contextual usage of PQC algorithms can be based on combination of specific security requirements, energy efficiency and network requirements. Below table provides an example for selecting appropriate PQC algorithm for potential 6G applications.

Table 1: Example of PQC algorithm selection for applications

Potential 6G Applications	Security Level	Energy Efficiency	Network Criticality
Connected Autonomous Vehicle (CAV)*	High	Low	High
Unmanned Aerial Vehicle (UAV)*	High	High	High
Extended Reality (AR/VR)*	Medium	Medium	Low

*This system has a complex supply chain with different service providers and consumers. Each application or service demands to create Network Slices to improve service performance and the quality based on specific use case and their requirements. Securing a large volume of data and enabling secure communication between different interfaces and services using appropriate PQC algorithms for potential 6G applications are crucial. Also, it is recommended to identify appropriate PQC algorithm for UEs using EAP-TLS protocol (Example. Private 5G networks) as mentioned in Section 4.

Offload PQC computation to Hardware accelerators for faster and energy efficient operation.

Adopt Lightweight Cryptography for energy constraint use cases such as IOT devices. NIST has already initiated a process to evaluate and standardize lightweight cryptographic algorithms [48].

Interoperability and Migration to PQC

As migration from existing cryptographic algorithms to PQC may not happen at once in O-RAN and 3GPP systems, it is important to ensure the interoperability between Network Functions, Applications, and interfaces where one side of component uses existing cryptographic algorithm, and another side uses PQC based algorithms for establishing secure communication and enabling secure storage. One of the potential options for MNOs to support Hybrid X.509 certificates in the Operator's PKI infrastructure. These Hybrid certificates contains both classical and quantum-resistant keys and signatures. Once the migration completes for all components in the system, then usage of hybrid certificates can be made obsolete and use only quantum-safe certificates.

Key Management

Larger key sizes are required for most of the PQC algorithms compared to traditional cryptographic algorithms. Security design for such system must efficiently handle larger key sizes. Also, ensure key generation, key distribution, key revocation performs securely.

6.2 Other techniques

Computational post-quantum cryptography (PQC), as described in paragraph 6.1.1, and quantum key distribution (QKD), as described in paragraph 1.3.1.1, are cryptographic techniques for addressing the threat quantum computing presents to modern security systems. Nevertheless, both have limitations and concerns. The study of computational PQC is relatively new, with no systems having yet undergone the kind of rigorous "trial by fire" that is provided by decades of wide-spread use. As such, these may come with an inherent risk of vulnerabilities that are not yet understood. Moreover, like all other computational cryptographic algorithms they come with a cost of potentially significant computational complexity. QKD is costly to deploy, requiring specialized equipment. Other limitations include distance constraints, susceptibility to physical attacks and lack of authentication. Moreover, it is currently impractical over the air and expected to remain so as 6G systems mature. Thus, while QKD may be practical for securing the backbone networks of communication systems, it is not clear that it can be used to secure access, especially wireless access.

Several other approaches may be used to help mitigate the limitations of computations PQC and QKD. All of these have their own limitations, and thus are not necessarily replacements to either of PQC and QKD. However, such techniques might be considered in compliment with PQC and QKD in designing and deploying effective

and efficient quantum-secure wireless communication systems. Many such techniques focus on deriving and/or distributing information-theoretically key material using physical sources/processes that inherently produce shared/shareable randomness.

In the context of 6G, one particularly relevant example of such an approach is taking advantage of the properties of wireless channels to derive and/or distribute information-theoretically secure key material. Specifically, the assumption we rely on is that two receivers located a sufficient distance away from a single transmitter observe channels with characteristics that are probabilistically independent. This statement comes with a number of additional caveats, the most important being:

- The two receivers are more than ½ wavelength away from each other in physical distance.
- The environment is sufficiently complex so that the channel is not dominated by line-of-sight (LOS) components.

The first of these assumptions dictates certain aspects of system design and how and when these techniques should be used, while the second assumption is easily testable by examining the measured channel itself (LOS-dominant channels are “easy to detect”). We refer the interested reader to the references on these and other topics, see for example, [49], [50], [51] and many other references.

The use of wireless channels for information-theoretically secure communication can further be divided into two distinct approaches. The first, sometimes referred to as “RF fingerprinting,” treats the channel as a source of secrecy. Moreover, when the channel is reciprocal – i.e. in TDD systems – it becomes a source of shared secrecy: the legitimate parties observe channels that are highly statistically similar while any potential enemy, subject to the two assumptions above, observes a channel from each of the legitimate parties that is statistically nearly independent from their common observation. The practicality of such an approach has been demonstrated, using, e.g. Wi-Fi systems. The latter approach is reliant on essentially the same beamforming as well-known beamforming approach in use for MIMO systems, with the beams formed so that the attackers’ channels is effectively un-recoverable (and some appropriate channel coding).

A comparative analysis of the two approaches is beyond the scope of this report – our main purpose here is to note that both are well-studied and understood. Moreover, both rely on channel estimation and forward-error-correction (FEC) techniques. Both are signal processing components that are typically present in modern communication systems. Thus, these techniques come with relatively small incremental cost to overall system complexity. As with all other cryptographic techniques, the challenge is how to use these in building communication systems that leverage the unique advantages

that these techniques offer while neutralizing the weaknesses of each through appropriate system design.

6.3 Building Secure Communication Systems

As should be clear from the discussion in paragraph 6.1, there are a number of techniques that can be brought to bear in securing against the threat of quantum computing. Each of these has its own advantages and limitations and it is quite likely that these techniques may need to be used in conjunction with each other. Most importantly, none of these – not even QKD – is capable of generating key material at rates that allow its straightforward use in a one-time pad cipher.

This begs the question of what to do with all these new cryptography techniques and how to mesh them together. Interestingly, modern communication systems are already designed to do so. The principle is simple: separate the three aspects of key management and cryptography into architectural entities each with well-defined scope responsibility. By the three aspects we mean the following:

1. Generation of “source key material” – i.e., generation and maintenance of “anchor” keys (e.g., K_{AUSF} in 5G) as defined in many communication systems today, see e.g., 3GPP TS 33.501 [52], but provably secure against Quantum Computing.
2. Creation of “derivative” key material from the “source key material” – specifically the generation of the key hierarchy containing the various session key, temporary keys, etc. as defined in the various communication standards today. This component is also responsible for key refresh to ensure security criteria such as forward secrecy.
3. The use of “derivative” key material in the various security protocols.

We note that steps 2 and 3 in this approach are not dependent on *where* the source material comes from. Their security against Quantum computing should derive from proper design (e.g. use of PQC algorithms for key hierarchy derivation and encryption, authentication, etc.) and the assumption that the source key material delivered by step 1 is secure. This means that as we transition from modern, computational cryptography to a future mixed cryptography, we do not need to drastically change how Steps 2 and 3 operate (of course, that does not prevent us from improving them!). To make this clear, let’s consider 5G as an example. In that case, what we mean here is that once K_{AUSF} is derived, the rest of the process does not have to change drastically from what is specified in 33.501 [52], provided that the algorithms used for keys derivative from K_{AUSF} are quantum-secure themselves.

Consequently, in developing a quantum-secure communication system we simply need to focus on how to generate quantum secure “source key material”. An obvious answer may indeed be sufficient. Simply generate key bits by any means available and put them into a “key bit bucket”. If necessary, associate a “quality” with these bits

(e.g., QKD bits may have higher “quality” then PQC bits). Whenever the sub-system in step 2 needs to generate a new key hierarchy or refresh an existing one, it simply reaches into the key bit bucket, extracts the required number of key bits (or required quality, if applicable) and proceeds. As noted, at this point the source of the keys is irrelevant. A specific example and details of how to enhance a Wi-Fi system using this approach and channel-generated keys is provided in [53]. In the context of 5G systems, this does mean that derivation of K_{AUSF} needs to be adapted to take advantage of quantum-secure key material generated by any of the means available (i.e., from our “bit bucket”).

There are several technical reasons that make it necessary to evaluate postquantum cryptography options already today. On the implementation side, it is anticipated that, for many applications, PQC will be offered as a software-based solution. Current implementations indicate that PQC is well supported by the existing network infrastructure and hardware, however, further testing and benchmarking is required to fully understand their behavior in different computational environments [54]. Industrial control systems represent a case with unique challenges. These systems adhere to very high standards of resiliency and safety, which means that they need to be upgraded without impacting the underlying industrial processes. Furthermore, as the recent cases of the NIST signature scheme candidates RAINBOW and SIKE have emphatically showcased [55], PQC algorithms are no exception to cryptanalysis and so it is always possible that new vulnerabilities are discovered. As a result, mechanisms need to be in place to allow for a failover to safer PQC options. Finally, although the incorporation of PQC algorithms in protocols such as Transport Layer Security (TLS), IPsec or Virtual Private Network (VPN) might not be technically very complicated, there is still a lot of work to be done and implementers should consider the specific needs of their applications in order to choose an appropriate PQC scheme safely. In the upcoming years, more and more standards, libraries, and protocols will add support for PQC. Until then, we can leverage the existing libraries and start experimenting with post-quantum as well as hybrid versions of protocols such as TLS to better understand the characteristics and performance of these new algorithms [56].

Apart from the technical difficulties outlined in the previous paragraph, there are several other reasons we need to stay vigilant and start evaluating PQC technologies already today. Security in the quantum era – Evaluating post-quantum solutions First, we acknowledge the problem of “harvest-now-decrypt-later”, which means that malicious actors with adequate resources may be storing sensitive encrypted data today with the aim to decrypt the data once a quantum computer is available. This implies that every day we lose today by not implementing quantum-safe strategies can correspond to data being exposed in the future. Moreover, cryptography is the type of technology that historically matures slowly. NIST acknowledges that it has taken almost 20 years to deploy a public-key infrastructure that we can trust. With regards

to post-quantum cryptography, NIST expects a timeframe of 5-15 years after the release of the standards [57] while other analysts and academics give a more conservative estimate of 10-20 years [58]. These challenges are illustrated nicely by the so called Mosca model in Figure 2 [59]. In the figure, x denotes the time that our systems and data need to remain secure, y the number of years to migrate to a PQC infrastructure and z the time until a practical quantum computer that can break current cryptography is available. The model assumes that encrypted data can be intercepted and stored before the migration is completed in y years. This data remains vulnerable for the complete x years of their lifetime, thus the sum x + y gives us an estimate of the full timeframe that data remain insecure [57]. The model essentially asks the question of how we are preparing our IT systems during those y years, or on the other hand, how can we minimize those y years, so as to minimize the duration of the transition phase to a PQC infrastructure and hence minimize the risks of data being exposed in the future. Additionally, we should not underestimate other factors that could accelerate the introduction of a large-enough quantum computer, such as faster-than-expected advances in quantum computing and more efficient versions of Shor's algorithm requiring less qubits. For example, IBM, one of the leading actors in the development of a large-scale quantum computer, has recently published a roadmap committing to new quantum processors that will support more than 1000 qubits by 2025 and networked systems with 10k-100k qubits beyond 2026 [59]. Innovation often comes in waves, so it is to the industry's benefit to remain vigilant and prepare as early as possible. Finally, there are other threat landscapes that do not pertain to quantum computing per se but can be utilized to attack legacy and post-quantum crypto, namely Artificial Intelligence (AI) and Machine Learning (ML). Although it is still very early to judge their merits, some recent attacks employing the concept of "transformers" (used extensively in ML and AI models like GPT) clearly highlight that we cannot wait until the next breakthrough to take actions for our post-quantum migration journey [60].

Figure 3: The Mosca model for evaluating PQC migration timeframe as in [8]

Even though quantum computers are still in an experimental status, their security implications need to be addressed already today. We need to get prepared for the post-quantum era with proactive strategies. Our role is to enable technology and knowledge transfer as well as foster collaboration to identify key areas that should be addressed during the initial steps for the introduction of quantum-safe solutions. Moreover, Industry needs to partner with leading universities to extend their in-house

research and enable smooth integration and evaluation of PQC solutions in its 5G ecosystem.

6.4 Standardization efforts

In August 2022, NIST selected seven PQC algorithms for the third round of the standardization process, and issued PQC migration guidance in collaboration with Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security (DHS). Additionally members of the research consortiums are heavily involved in deploying a 5G system testbed in the NIST 5G Cybersecurity Lab at the National Cybersecurity Center of Excellence (NCCoE) to experiment with open-source implementations of PQC algorithms and protocols [61].

The IETF's Crypto Forum Research Group (CFRG) has been investigating the impact of PQC on security protocols like TLS and IPsec/IKE, while the ETSI Cyber group has drafted a specification for Quantum-safe Hybrid Key Exchanges (QSC) and Security Algorithms Group of Experts (SAGE) has evaluated 256-bit algorithms for use in 3GPP.

3GPP SA3 is studying the support of 256-bit algorithms and is expected to revisit PQC after NIST standardization. Two active groups in the IEEE are focusing on definitions and metrics/performance related to quantum, while the PQTN is investigating the impact of PQC on telecommunications networks and has published a white paper prior to MWC 2023.

ITU-T has focused on the QKD standardization since 2018. Their dedicated SG11, SG13 and SG17 are actively working on over 30 projects, notably enhancing the network and security aspects of QKD. In addition, ITU-T established the Focus Group on Quantum Information Technology for Networks (FG-QIT4N)[62]. This group manages pre-standardization areas of quantum information technology, with a mission to simplify terminology, analyze usage cases for this technology, and accelerate QKD integration within the broader ICT sphere.

ISO/IEC JTC 1/SC 27 WG3 is engaged in an in-depth study of equipment safety evaluation technology standards. ISO/IEC 23837-1 and 23837-2 focus on the security requirements, test and evaluation methods for quantum key distribution [63] [64].

CCSA has been working on over 35 pre-standardization about QKD. ST7 has been developing a national specification that defines application scenarios and requirements for quantum secure communication [65].

References

[1] Office, U. S. G. A. (n.d.). Science & Tech spotlight: Securing Data for a Post-Quantum World. Science & Tech Spotlight: Securing Data for a Post-Quantum World | U.S. GAO. https://www.gao.gov/products/gao-23-106559

[2] Semiconductors and Electronics. Data Bridge Market Research. (n.d.). https://www.databridgemarketresearch.com/reports/global-quantum-cryptography-market

[3] W. Beullens, “Breaking Rainbow Takes a Weekend on a Laptop,” Cryptology ePrint Archive, vol. 214, 2022.

[4] https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

[5] David Cooper (NIST), Daniel Apon (NIST), Quynh Dang (NIST), Michael Davidson (NIST), Morris Dworkin (NIST), Carl Miller (NIST), “Recommendation for Stateful Hash-Based Signature Schemes,” NIST, 2020.

[6] W. Castryck and T. Decru, “An Efficient Key Recovery Attack on SIDH,” [Online]. Available: https://eprint.iacr.org/2022/975.pdf. [Accessed 24 08 2022].

[7] Q. E. D. Consortium, “A Guide to a Quantum-safe organization,” QED-C, 2021

[8] Nokia: Security in the quantum era: Evaluating post-quantum solutions https://onestore.nokia.com/asset/213086

[9] Porambage, P., Gur, G., Osorio, D. P., Liyanage, M., Gurtov, A., & Ylianttila, M. (2021). The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society, 2, 1094–1122. https://doi.org/10.1109/ojcoms.2021.3078081

[10] Peter W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134

[11] Lov K. Grover, "A fast quantum mechanical algorithm for database search". Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery: 212–219

[12] “Post-Quantum Cryptography,” NIST, [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantumcryptography-standardization/evaluation-criteria/security-(evaluation-criteria).

[13] Bas Westerbaan, “NIST’s pleasant post-quantum surprise,” Cloudfare, 7 July 2022. [Online]. Available: https://blog.cloudflare.com /nist-post-quantum-surprise/. [Accessed 7 11 2022]

[14] C. Zalka, “Grover’s quantum searching algorithm is optimal,” Physical Review A, vol. 60, pp. 2746-2751, 1999.

[15] M. Suchara, J. Kubiatowicz, A. Faruque, F. T. Chong, C. -Y. Lai and G. Paz, "QuRE: The Quantum Resource Estimator toolbox," 2013 IEEE 31st

International Conference on Computer Design (ICCD), Asheville, NC, USA, 2013, pp. 419-426.

[16] Rötteler, Martin, Michael Naehrig, Krysta Marie Svore and Kristin E. Lauter. “Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms.” International Conference on the Theory and Application of Cryptology and Information Security (2017).

[17] “GRI Quantum Risk Assessment Report - Part 5: A Resource Estimation Framework for Quantum Attacks against Cryptographic Functions - Recent Developments.” Global Risk Institute, https://www.globalriskinstitute.org/publication/gri-quantum-risk-assessment-report-part-5-a-resource-estimation-framework-for-quantum-attacks-against-cryptographic-functions-recent-developments/

[18] Grassl, M., Langenberg, B., Rötteler, M., & Steinwandt, R. (2015). Applying Grover's Algorithm to AES: Quantum Resource Estimates. Post-Quantum Cryptography.

[19] https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

[20] https://quantumai.google/hardware

[21] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

[22] J. G. a. B. W. Y. Zheng, “New Quantum Search Model on Symmetric Ciphers and Its Applications.,” https://eprint.iacr.org/2023/327, Online, 2023.

[23] 3GPP TS 33.501: Security architecture and procedures for 5G system

[24] 3GPP TS 35.909: Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation

[25] 3GPP TS 35.231: Specification of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification

[26] 3GPP TS 35.215: Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications

[27] NIST: Advanced Encryption Standard (AES) (FIPS PUB 197)

[28] NIST Special Publication 800-38A (2001): Recommendation for Block Cipher Modes of Operation

[29] 3GPP TS 35.221: Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications

[30] NIST Special Publication 800-38B (2001): Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.

[31] 3GPP TS 33.210: Network Domain Security (NDS); IP network layer security

[32] 3GPP TS 33.310: Network Domain Security (NDS); Authentication Framework (AF)

[33] “Defeating IMSI Catchers”, Fabian van den Broek and Roel Verdult and Joeri de Ruiter, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015
[34] https://datatracker.ietf.org/doc/html/rfc7516
[35] https://datatracker.ietf.org/doc/html/rfc7515
[36] https://www.rfc-editor.org/rfc/rfc6749
[37] https://datatracker.ietf.org/doc/html/rfc7519
[38] 3GPP TS 33.558: Security aspects of enhancement of support for enabling edge applications
[39] https://www.rfc-editor.org/rfc/rfc8555
[40] https://www.rfc-editor.org/rfc/rfc8572/
[41] https://www.rfc-editor.org/rfc/rfc8995/
[42] O-RAN Security Requirements Specifications
[43] Long GL (2017) Quantum secure direct communication: principles, current status, perspectives. In 2017 IEEE 85th Vehicular Technology Conference (VTC Spring) 1-5.
[44] Hussein Abulkasim, Safwat Hamad, Amal Khalifa, and Khalid El Bahnasy. Quantum secret sharing with identity authentication based on Bell states. International Journal of Quantum Information, 15(04):1750023, 2017
[45] Hua-Lei Yin and others, Experimental quantum secure network with digital signatures and encryption, *National Science Review*, Volume 10, Issue 4, April 2023, nwac228, https://doi.org/10.1093/nsr/nwac228
[46] G. -L. Long, "Quantum Secure Direct Communication: Principles, Current Status, Perspectives," 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, Australia, 2017, pp. 1-5, doi: 10.1109/VTCSpring.2017.8108697.
[47] https://cacr.uwaterloo.ca/techreports/2018/cacr2018-06.pdf
[48] https://csrc.nist.gov/projects/lightweight-cryptography
[49] R. Liu and W. Trappe, Ed., Securing Wireless Communications at the Physical Layer, Springer, 2010
[50] Y. Chen, et. al, Securing Emerging Wireless Systems, Springer 2009.
[51] Y.-S. Shiu, et. al, “Physical Layer Security in Wireless Networks: a Tutorial,” in IEEE Wireless Communications., April 2011.
[52] 3GPP; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 18), v. 18.0.0, 01/20023.
[53] S. Mathur et al., "Exploiting the physical layer for enhanced security,” in IEEE Wireless Communications, October 2010.
[54] W. Barker, W. Polk, and M. Souppaya, “Getting Ready for Post Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms,” 28 April 2021. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf. cfm?pub_id=932330. [Accessed 9 May 2022].

[55] C. Ye, et. al, "Information-theoretically Secret Key Generation for Fading Wireless Channels," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pg. 240-254, June 2010.

[56] D. Stebila, “Post-quantum key exchange for the Internet and the Open Quantum Safe project,” Selected Areas in Cryptography (SAC), vol. 10532, pp. 1-24, 2017.

[57] M. P. M. Mosca, “Quantum Threat Timeline Report 2020,” Global Risk Institute, 2020. [Online]. Available: Quantum Threat Timeline Report 2020 - Global Risk Institute

[58] M. Mosca, “(2015) Cybersecurity in a quantum world: will we be ready? Invited talk at NIST workshop on Cyber Security in a Post-Quantum World (Gaithersburg, MD, 2015), National Institute of Standards and Technology (NIST),” 2015. [Online]. Available: https://csrc.nist.gov/src/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

[59] IBM, “Our new 2022 Development Roadmap,” IBM, [Online]. Available: https://www.ibm.com/quantum/roadmap [Accessed 24 08 2022].

[60] C. L. e. al., “SALSA PICANTE: a machine learning attack on LWE with binary secrets.,” SALSA PICANTE: a machine learning attack on LWE with binary secrets (iacr.org) , Online, 2023

[61] “5G Cybersecurity,” National Cybersecurity Center of Excellence, [Online]. Available: 5G Cybersecurity | NCCoE (nist.gov) [20]

[62] https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx

[63] ISO/IEC 23837-1: Information security — Security requirements, test, and evaluation methods for quantum key distribution — Part 1: Requirements, Available: https://www.iso.org/standard/77097.html

[64] ISO/IEC 23837-2Information security — Security requirements, test, and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods, Available: https://www.iso.org/standard/77309.html

[65] CCSA ST7 https://www.china-cic.cn/upload/202012/05/73453ac5127a48aeb2a01f218460b9e5.pdf

Copyright