TUTORIAL: Post-Quantum Cryptography and 5G Security*

T. Charles Clancy
Virginia Tech
Arlington, VA, United States
tcc@vt.edu

Robert W. McGwier
Virginia Tech
Blacksburg, VA, United States
rwmcgwi@vt.edu

Lidong Chen
National Institute of Standards and Technology
Gaithersburg, MD, United States
lily.chen@nist.gov

ABSTRACT

The Fifth Generation (5G) mobile broadband standards make a fundamental shift in cryptography. Prior generations based their security and privacy principally on symmetric key cryptography. The Subscriber Identity Module (SIM) and its successors contain a shared key used to authenticate the User Equipment (UE) to the network, and vice versa.

However 5G is shifting its core network over to a microservices, cloud-first architecture and is heavily leveraging protocols like TLS and OAuth2.0 to authenticate and authorize transactions. As a result, it is shifting to a PKI-based trust model. This shift is happening just as quantum computing threatens to unravel the security of traditional ciphers such as RSA and ECC.

In this paper we highlight the need to advance the 3GPP 5G standards and NIST post-quantum cryptography standards in tandem, with the goal of launching a "quantum ready" 5G core network.

CCS CONCEPTS

• **Networks** → Mobile networks; • **Security and privacy** → Public key (asymmetric) techniques.

KEYWORDS

5G, cellular networks, post-quantum cryptography

ACM Reference Format:
T. Charles Clancy, Robert W. McGwier, and Lidong Chen. 2019. TUTORIAL: Post-Quantum Cryptography and 5G Security. In *WiSec '19: ACM Conference on Security and Privacy in Wireless and Mobile Networks, May 15–17, 2019, Miami, FL.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3317549.3324882

1 INTRODUCTION

The Fifth Generation (5G) mobile broadband standards represent a fundamental shift in telecommunications. The radio access network (RAN) standards, known as New Radio (NR), offer increased spectral efficiency and new millimeter-wave (mmw) spectrum. Meanwhile the 5G Core (5GC) fully embraces a cloud service-oriented mentality fueled by virtualized networks, compute, and storage. Rather than the physically isolated interfaces between core network functions that were fundamental to earlier standards, the 5GC is designed to support microservices implemented on an elastic cloud backplane. Consequently, 5GC envisions each microservice having its own public-key certificate that can be used to authenticate, authorize, and secure transactions.

Additionally, 5G reenvisions user and device authentication and can support public key cryptography-based authentication in addition to subscriber identity modules (SIMs) for user equipment (UE) authentication. Low-power Internet of Things (IoT) devices can be equipped with digital certificates to avoid the power and space constraints of a physical SIM. Similarly, the rise of enterprise cellular service–think college campuses or hospitals–means that third-party credentials such as usernames and passwords can be supported for network authentication.

As a consequence, 5G takes advantage of public-key infrastructure (PKI). It affects both UE authentication to the network, in addition to how control and management plane services securely interact with each other. This embrace of PKI is happening just as advances in quantum computing begin to make cryptographers nervous about the longevity of workhorse ciphers like Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC).

To date, the density of qubits in quantum computers has more or less matched a Moore's Law curve of doubling every 18 months. If these trends continue, ciphers like RSA will be broken and unusable before 2030. Continually increasing the key size is also not practical as doubling the key size would only provide an additional 18 months of key lifetime. While these developments are by no means guaranteed, as there are a whole host of different physics and engineering challenges to overcome in scaling general-purpose quantum computers, they are certainly cause for concern.

Fortunately, over the past few years NIST has been working on post-quantum cryptography (PQC). These ciphers do not rely on the same underlying mathematics as RSA and ECC, and as a result are more immune to advances in quantum computing. While many of these ciphers have been around in academic literature for upwards of 20 years, concern over quantum computing advances has motivated a deeper inspection of their properties that is expected to lead to standardized ciphersuites by 2022.

2 5G SECURITY

3GPP, the governing standards body for 5G cellular protocols, has recently published Release 15 of the standards which has included "5G Phase 1". This defines the radio access network and control plane functions. 3GPP Release 16 will be termed "5G Phase 2" and incorporate more advanced core network features like network slicing. Release 16 is expected in the second half of 2020.

*This paper is an extended abstract associated with a tutorial presented by the lead author at ACM WiSec 2019.

WiSec '19, May 15–17, 2019, Miami, FL

ACM ISBN 978-1-4503-6726-4/19/05.
https://doi.org/10.1145/3317549.3324882

However 5G Phase 1 paints a vivid picture of how authentication, authorization, trust, and identity management are fundamentally changing in 5G.

2.1 Subscriber and Access Network Security

5G is migrating to support both the legacy Authenticated Key Agreement (AKA) protocol, with some updates to address concerns over weak hash functions, in addition to full support for the Extensible Authentication Protocol (EAP). EAP is the mechanism used by the WPA2 Enterprise mode for WiFi, and supports public key authentication and username/password authentication, in addition to SIM-based shared key authentication. These new modes imply a wide range of new trust relationships where third party authentication servers can be used in a roaming-style mechanism to authenticate to carrier-operated 5G networks.

2.2 Control Plane Security

5G anticipates a *cloud native* approach to core network services. In 4G and earlier, the core network consisting of a collection of static functions that were grouped together and implemented as a piece of rack-mount hardware, interacting through defined protocol interfaces with other pieces of hardware. In 5G, the core network is reenvisioned as a collection of microservices, each existing as an *app* in the cloud, and communicating using web service APIs with other components over a HTTPS. These Virtualized Network Functions (VNFs) can be elastically provisioned within a cloud environment and wired together and into the core network using Software Defined Networking (SDN) technologies.

The consequence of this change is that each of the VNFs needs a public/private key pair and digital certificate that can be used to authenticate and authorize each control plane transaction. Built on top of HTTPS, Transport Layer Security (TLS) provides authentication and the OAuth2.0 protocol is used to authorize interactions among core services.

Additionally, when the core network from one carrier network is communicating with the network of another carrier, for example in a roaming scenario, there are additional required layers of security, including IPsec. When interacting via an intermediary roaming broker, there are also provisions whereby intermediaries make auditable changes to messages each independently digitally signed.

The consequence is that an extremely complex, PKI-secured ecosystem is emerging within the 5G core network.

3 POST-QUANTUM CRYPTOGRAPHY

In this section we explore the emerging ecosystem of Post Quantum Cryptography (PQC), or ciphers that are designed in such a way to be immune to advances in quantum computing.

3.1 Quantum Impact on Cryptography

Shor's algorithm was introduced in 1994 and shows how to factor large products of prime numbers efficiently on a quantum computer, which undermines the security of RSA [8]. Extensions show how it can be used to defeat the discrete logarithm problem and thus undermine ECC ciphers. Grover's algorithm was introduced in 1996 and shows how symmetric key ciphers like AES can be more rapidly exploited through quantum database structures [4]. Table 1 summarizes common ciphers, their equivalent symmetric key strength using classical algorithms, and their equivalent security with a sufficiently-capable quantum computer [6].

Table 1: Comparison of Classical and Quantum Security Levels for Ciphers

Cipher	Key Size	Effective Strength	
		Classical	Quantum
RSA	1024	80	0
RSA	2048	112	0
ECC	256	128	0
ECC	384	256	0
AES	128	128	64
AES	256	256	128

3.2 Post-Quantum Ciphers

PQC does not have the same building blocks as traditional public-key cryptography. For example, there is no Diffie-Hellman type algorithm for key agreement in PQC. Thus concepts do not necessarily map 1:1 from traditional ciphers to the PQC domain. In this section we discuss the different types of PQC approaches.

3.2.1 Lattice-Based Cryptography. Mathematically, a lattice is the set of all integer linear combinations of a set of basis vectors. A central mathematical problem to lattices is the shortest vector problem which seeks to find the shortest non-zero vector in the vector space spanned by the basis vectors. Solving this problem is NP-hard.

The most well known lattice-based cryptographic scheme is NTRU, which has both an encryption and signature formulation. NTRU is actually based on operations within a truncated polynomial ring, however instead of its security being based on the complexity of solving the discrete log problem cracking it has been shown related to solving the shortest vector problem for a lattice. So while not strictly implemented mathematically using a lattice, its proof of security is equivalent to solving the shortest vector problem.

NTRU was originally published in 1998 [5] and undergone considerable study. A variety of vulnerabilities have been identified and patched along the way.

Other approaches include the Goldreich-Goldwasser-Halevi (GGH) scheme built on the closest vector problem [3] and more recent Bimodal Lattice Signature Scheme (BLISS) [2].

Of these approaches, an updated version of NTRU has been approved as IEEE Standard 1363.1 and ANSI standard X9.98.

3.2.2 Hash-Based Cryptography. The recent risk of blockchain technology has renewed focus around hash-based cryptography. Based on the Merkle has trees, this approach can be used as an alternative to traditional digital signatures. The eXtended Merkle Signature Scheme (XMSS) has been published as an informational document by the IETF as RFC 8391.

3.2.3 Code-Based Cryptography. Code-based cryptography is based on the difficulty of decoding a general linear code. The McEliece scheme was introduced in 1978 and is based on computing random

linear transformations of an error correcting code's generator matrix, and only the private key holder knowing the factors of that matrix [7]. The cipher has been recommended for consideration in a PQC environment, but requires extremely long key lengths [1]. There are a few other code-based schemes, notably Niederreiter's approach that also supports digital signatures.

3.2.4 Supersingular Elliptic Curve Isogeny Cryptography. While the ciphers discussed so far offer equivalents to encryption and signature schemes, a key agreement protocol with forward secrecy is notably lacking. In 2012, researchers showed that supersingular elliptic curves and supersingular isogeny graphs can be used to create a post-quantum Diffie-Hellman-type cipher, but these approaches remain relatively nascent and unstudied in academic literature.

3.3 NIST Standards Efforts

Developing PQC standards has been seriously challenged in many different aspects. First and foremost, in the past thirty years, public-key cryptography has been deployed in almost all the computation and communication applications. The new cryptographic standards must be able to adapt to the existing applications without creating disruption. Furthermore, new applications such as those in 5G certainly propose distinct requirements to the cryptographic tools. Second, compared to the theoretical and practical research on the classical security of public-key cryptography, understanding quantum security for the cryptosystems proposed in the literature has a long way to go as it takes time to understand quantum computers and algorithms. Last but not least, as we discussed before, with the progress made in developing large scale quantum computers, it is urgent to identify counterparts for RSA and ECC, because it takes years to deploy new cryptographic mechanisms in the existing and new applications.

After a five-year study and research, NIST announced an initial plan in February 2016 to develop PQC standards. Historically, NIST has selected standards on major cryptographic primitives such as block cipher (i.e. AES) and hash function (i.e. SHA3) through worldwide competitions. The standardized algorithms were selected among the submissions. To develop post-quantum standards, NIST announced call for proposals in December 2016. It called for proposals on public key encryption, key establishment, and digital signature. In November 2017, NIST received 82 submissions from 6 continents and 25 countries. Among them, 69 submissions were announced as the first round candidates. After about one year analysis and evaluation, 26 candidates were advanced to the second round, which was announced in January 2019.

The PQC candidates are designed in the major categories as published in the research literature, including lattice-based, coding-based, multivariate, stateless hash-based signatures, and supersingular elliptic curve isogeny based. NIST will standardize stateful hash based signatures based on standards developed in IETF without including them in the scope of call for proposals. NIST plans to spend about 12-18 months to analyze and evaluate the second round candidates and start to release draft standards for public comments in 2022 to 2023 timeframe.

Adapting NIST PQC standards to 5G is critical for mobile security in quantum era. Even though it has been on the top of the wish list to design PQC algorithms as "drop-in replacement" for RSA and ECC, many features in the candidates may propose challenges to the applications such as public-key size, signature size, alternative auxiliary functions, etc. When developing 5G standards, the special features of the PQC algorithms shall be considered for cryptographic agility. NIST has reached out to different application communities to solicit feedback on special requirements and restrictions to be considered in selecting algorithms for standards and welcome input from 5G development community.

4 PATH FORWARD

Looking forward, there is a critical need to ensure that 5G standards, as developed, envision future adoption of PQC for public key ciphers. As was discussed, the goal is to have a drop-in replacement that could simply be added as a new ciphersuite definition for TLS, but associated Certification Authority (CA) infrastructure is needed that can issue, manage, and revoke PQC keys.

The cellular industry has a considerable up-hill climb in front of itself simply to adopt public-key based approaches to trust and authentication. If PQC is part of the initial thinking, then the migration to new keys and ciphers can happen more smoothly.

REFERENCES

[1] Augot, D., Batina, L., Bernstein, D. J., Bos, J., Buchmann, J., Castryck, W., Dunkelman, O., Guneysu, T., Gueron, S., Hulsing, A., Lange, T., Mohamed, M. S. E., Rechberger, C., Schwabe, P., Sendrier, N., Vercauteren, F., and Yang, B.-Y. Initial recommendations for long-term secure post-quantum systems. PQCRYPTO: Post-Quantum Cryptography for Long-Term Security, 2015.

[2] Ducas, L., Durmus, A., Lepoint, T., and Lyubashevsky, V. Lattice signatures and bimodal gaussians. In *Proceedings of the 33th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'13)* (2013).

[3] Goldreich, O., Goldwasser, S., and Halevi, S. Public-key cryptosystems from lattice reduction problems. In *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'97)* (1997), pp. 112–131.

[4] Grover, L. A fast quantum mechanical algorithm for database search. Bell Labs, New Jersey, Technical Report, 1996.

[5] Hoffstein, J., Pipher, J., and Silverman, J. Ntru: A ring based public key cryptosystem. In *Algorithmic Number Theory (ANTS III)* (1998), pp. 267–288.

[6] Mavroeidis, V., Vishi, K., Zych, M. D., and Josang, A. The impact of quantum computing on present cryptography department of informatics. *International Journal of Advanced Computer Science and Applications 9* (2018).

[7] McEliece, R. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report 44* (1978), 114–116.

[8] Shor, P. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 124–134.