Requirements and Security Models for Post-Quantum Cryptography Analysis

Kateryna Isirova[1] and Oleksandr Potii[2]

[1] School of Computer Science
V. N. Karazin Kharkiv National University,
4, Svobody Sqr, Kharkiv, 61022, Ukraine, KaterinaIsirova@gmail.com

[2] School of Computer Science
V. N. Karazin Kharkiv National University,
4, Svobody Sqr, Kharkiv, 61022, Ukraine, potav@fm.ua

Abstract. In the paper problems and risks for classical systems in the field of cryptographic protection of information in connection with the development of quantum computing are formulated. Problems the need to finding new solutions are grounded. The paper includes analysis of requirements of two major organizations NIST and ETSI. There are security models for cryptographic primitives offered in terms of post quantum cryptography.

Keywords: Post quantum cryptography, Requirements for crypto algorithms in post quantum period, NIST requirements, ETSI requirements, Security models for post quantum cryptography.

1 Introduction

The progress in the field of quantum computing is an important challenge for modern cryptography. The rapid evolution of quantum computers, and as a result the growth of computational speed leads to the new risks for existing cryptographic systems. In particular, Shor's algorithm and Grover search algorithm pose a real threat to the asymmetric systems, based on RSA, Diffie-Hellman, Elliptic Curves [1, 3]. These cryptosystems are used to implement digital signatures and key establishment and play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks.

In the near future the trust to the information systems that handle critical information without any means of quantum-resistance cryptography will be impossible.

On the way of building the new solutions it is important step to development and formation characteristics and requirements that should be presented to new candidates and possible conditions for their use.

The paper includes analysis of requirements of two major organizations: NIST and ETSI. There are models for security and cryptographic primitives offered in terms of post quantum cryptography.

2 A Brief Analysis of NIST Requirements

NIST understands the need to find new primitives that will be relevant in the post quantum period. Appropriate work carried out in the framework of an open competition Post-Quantum crypto Project [1, 2].
The analysis showed that all requirements can be divided into the following groups:

1. The requirements of security, the main of which is the use of public key cryptography, "semantically secure encryption" scheme, compliance with IND-CCA2 and EUF-CMA security models; «Perfect forward secrecy», resistance to side-channel attacks;
   (a) parameter sets should meet or exceed each of five target security strengths:
      (i) 128 bits classical security / 64 bits quantum security
      (ii) 128 bits classical security / 80 bits quantum security
      (iii) 192 bits classical security / 96 bits quantum security
      (iv) 192 bits classical security / 128 bits quantum security
      (v) 256 bits classical security / 128 bits quantum security
2. Technical and economic requirements, such as: focus on Internet protocols packets size, hash key information, ensuring efficiency as the hardware and software implementation, matching the size of the selected key system;
3. Technical and operational requirements: cross-platform, the possibility of parallelization, understandability construction.

3 A Brief Analysis of ETSI Requirements

The European Union has also started the preparation of a new post quantum standards. European Organization for Standardization ETSI in cluster "Security" formed a new direction «Quantum-Safe Cryptography» [3].
The major safety requirements defined by them include:

- confidence in the associated security proof;
- relevance of the security model;
- the high difficulty of possible attacks;
- potential to provide or enable multiple security features (e.g. associated key establishment and authentication schemes);
  Ease of quantifying the claimed classical and quantum security levels;
- certainty of the recommended key sizes for a given level of security (e.g. 80-bits, 112-bits, 128-bits or 256-bits);
- practicality of key and signature sizes for transmission or storage across a range of platforms, including resource-limited devices;
- ease of integration into existing protocols or systems (e.g. is this drop-in replacement?);
- re-use of code base (e.g. to provide authentication as well as key establishment) ;
- compatibility (e. g. flexibility in hash functions in schemes Merkle tree).

4 Justification of Security Models for Post Quantum Cryptography

Justification of resistance of cryptographic primitives should be based on complex computational problems for quantum computers. Today the basic directions of development of new quantum-safe or quantum-resistance algorithms are Hash-based cryptography (HB-cryptography), Code-based cryptography (CB-cryptography), Lattice-based cryptography (LB-cryptography), Multivariate-quadratic-equations cryptography (MQ-cryptography) [4, 5].

Requirements of cryptographic strong should be formulated in accordance with the following security models:

- for encryption - in accordance with IND-CCA2 security model (Indistinguishability under Adaptive Chosen Ciphertext Attack);
- for digital signatures - in accordance with EUF-CMA model (Existentially unforgeable under adaptive chosen message attacks).

4.1 IND-CCA2 Security Model

For probabilistic algorithm asymmetric encryption indistinguishability under non-adaptive chosen ciphertext / adaptive chosen ciphertext attack (IND-CCA1 / IND-CCA2) is defined by the following game between the challenger (legitimate user) and the adversary (cryptanalyst) [4, 5].

It is important to establish a definition: $E(PK, M)$ is encrypting message M under the key PK.

Additional condition is: the adversary is modeled by a probabilistic polynomial time Turing machine, meaning that it must complete the game and output a guess within a polynomial number of time steps.

The adversary has access to the public key (encryption oracle, in the symmetric case), as well as the adversary is given access to a decryption oracle which decrypts arbitrary ciphertexts at the adversary's request, returning the plaintext.

The Game consists of the following steps:

1. The challenger generates a key pair PK, SK based on some security parameter k (e.g., a key size in bits), and publishes PK to the adversary. The challenger retains SK.
2. The adversary may perform any number of encryptions, calls to the decryption oracle based on arbitrary ciphertexts, or other operations.
3. Eventually, the adversary submits two distinct chosen plaintexts to the challenger.
4. The challenger selects a bit $b \in \{0, 1\}$ uniformly at random, and sends the "challenge" ciphertext $C = E(SK, M)$ back to the adversary.
5. The adversary is free to perform any number of additional computations or encryptions.
   (a) In the non-adaptive case (IND-CCA1), the adversary may not make further calls to the decryption oracle.

(b) In the adaptive case (IND-CCA2), the adversary may make further calls to the decryption oracle, but may not submit the challenge ciphertext C.

6. Finally, the adversary outputs a guess for the value of *b*.

A scheme is IND-CCA1/IND-CCA2 secure if no adversary has a non-negligible advantage in winning the above game.

4.2 EUF-CMA Security Model

A security notion (or level) is entirely defined by pairing an adversarial goal with an adversarial model. Depending on the context in which a given signature scheme (or cryptosystem) is used, one may formally define a security notion for the system [6, 7].

- By telling what goal an adversary would attempt to reach (the adversarial goal), and
- What means or information are made available to the attacker (the adversarial or attack model).

Some of the adversarial goals as well as adversarial models related to digital signatures are briefly described [6].

Adversarial Goals.

Unbreakability: The attacker recovers the secret key sk from the public key pk (or an equivalent key if any). This goal is denoted UB. It is implicitly appeared with public-key signature scheme (or cryptography).

Universal Unforgeability: The attacker, without necessarily having recovered sk, can produce a valid signature s of any message m in the message space. It is noted UUF.

Existential Unforgeability: The attacker creates a message m and a valid signature s of it (likely no control over the message). This is denoted EUF.

Adversarial Models.

Key-Only Attacks: The adversary only has access to the public key pk. This is denoted KOA. This is an unavoidable scenario in public-key signature scheme (or cryptography).

Known Message Attacks: An adversary has access to signatures for a set of known messages. It is noted KMA.

Chosen Message Attacks: Here the adversary is allowed to use the signer as an oracle (full access), and may request the signature of any message of his choice (multiple requests of the same message are allowed). It is denoted CMA.

Putting the adversarial goal on the y-axis and adversarial model on the x-axis, the security notions are obtained. The intersecting points represent security notions. For example, UB-KOA, UB-KMA, EUF-CMA etc are security notions. If there are u adversarial goals and v adversarial models, there will be u * v security notions (Figure 1).

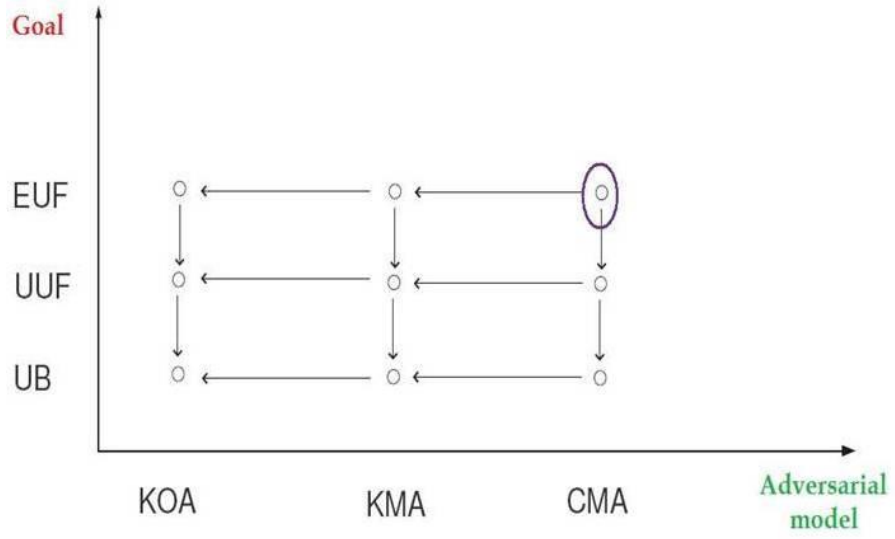

Figure 1 - The notions of security for signature scheme [6]

Let $S = (K, S, V)$ be a signature scheme, and let A^{euf} be a probabilistic polynomial time algorithm. Consider the following attack scenario:

- compute a key pair (sk, pk) $\leftarrow K(1^k)$, and hand *pk* as input to A^{euf};
- the adversary A^{euf} is given unrestricted access to a signing oracle O_S to run $S_{sk}(\cdot)$;
- eventually, A^{euf} outputs a message *M* and a signature σ.

Let QueriedEarlier be the event that A^{euf} outputs a message M that has already been queried to the signing oracle OS. The success probability $SucceA^{euf} = SuccA^{euf}(k)$ *of* A^{euf} is defined as

$$Succ_{Aeuf} = Pr\left[v_{pk}(M, \sigma) = true \ and \ \neg QueriedEarlier\right] \quad (1)$$

Signature scheme S secure in the sense of EUF-CMA if SuccAeuf is negligible for all probabilistic polynomial time adversaries A^{euf} [7].

5 Conclusions

The latest advances in technology of quantum computing form the new challenges for modern cryptography and determine the need to find the new ways of ensuring information security and its main properties - confidentiality, integrity, authentication and repudiation.

At present, there are several post-quantum cryptosystems that have been proposed, including lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems, hash-based signatures, and others. However, for most of these proposals, further research is needed in order to gain more confidence in their security (particularly against adversaries with quantum computers) and to improve their performance.

Should be understood the fact that a transition to post-quantum cryptography will not be simple as there is unlikely to be a simple “drop-in” replacement for our current public-key cryptographic algorithms. A significant effort will be required in order to develop, standardize, and deploy new post-quantum cryptosystems. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive when that compromise occurs.

An important task for the deployment of research and development quantum-safe algorithms is to determine the requirements for them. As a result of the analysis, we can see that such requirements are derived in several groups, such as: the requirements of security, technical and economic requirements .

Requirements of cryptographic strong should be formulated in accordance with the security models. According to the research we can conclude that such models allowing the highest degree of adversary awareness

References

1. NISTIR 8105 (DRAFT) Report on Post-Quantum Cryptography
2. NISTIR (DRAFT) Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process
3. ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.
4. Lindell, Y.: A Simpler Construction of CCA2-Secure Public-Key Encryption Under General Assumptions. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 241–254. Springer, Heidelberg (2003)
5. Nojima, R., Imai, H., Kobara, K., Morozov, K.: Semantic security for the mceliece cryptosystem without random oracles. Des. Codes Cryptography 49(1-3), 289–305 (2008)
6. Faust, S., Kiltz, E., Pietrzak, K., Rothblum G. Leakage-Resilient Signatures [Electronic resource] / S. Faust, E. Kiltz, K.Pietrzak, G. Rothblum. Cryptology ePrint Archive, 2009 Available at http://eprint.iacr.org/2009/282.
7. Muñiz M., Steinwandt R. Security of signature schemes in the presence of key-dependent messages. Tatra Mountains Mathematical Publications, 2010, vol. 47, No. 3. Available at: https://www.sav.sk/journals/uploads/0317154702go-st.pdf