National Institute of Standards and Technology
U.S. Department of Commerce

Crypto-Transition and Agility

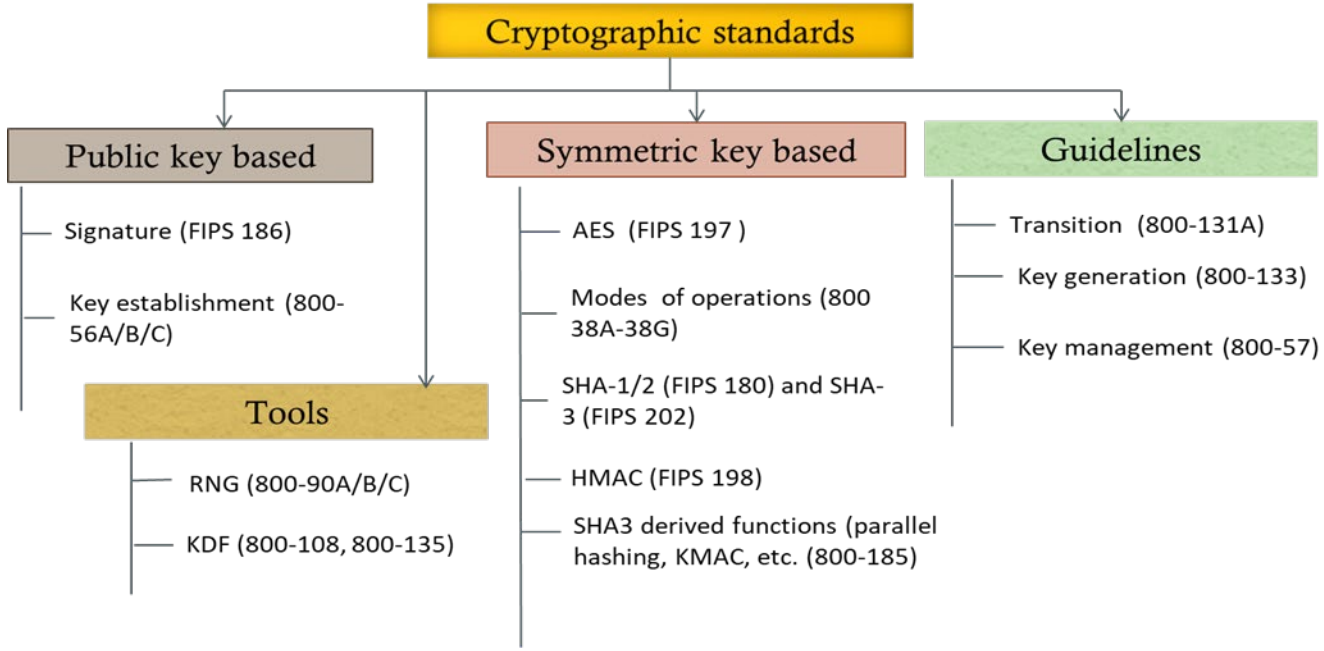
Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

Cryptographic Transition

- Cryptographic standards have been in a constant transition for
  - Increased computing power by Moore's law and emerging quantum computer
  - More sophisticated cryptanalysis techniques
- NIST provided guidance for transitions in the past
  - DES → Triple DES →AES
  - SHA1 →SHA2/3
  - 80-bits (RSA/DL 1024) →112-bits (RSA/DL 2048 and ECC 224)
- Next revision of SP 800-131A will lay out a plan of transition to 128-bit classic security with the corresponding quantum security
  - The exact year will be determined based on considerations of migration to and adoption of PQC.

New Perspectives in Cryptographic Transition

- In the past, the transition decisions were made if
  - An algorithm is broken, or
  - Security strength is lower than needed
- The advancements of cryptography have introduced new perspectives for transition
  - To consider new security features, requirements, definitions, etc.
  - Two examples
    - Mode of operations
    - Key encapsulation mechanisms



56A – (EC) DH, (EC) MQV;
56B – RSA based key establishment;
56C- Key derivation
FIPS 186-5 – RSA signature, ECDSA, EdDSA

New Perspectives for Modes of Operations

- Draft NIST IR 8459 summarizes a review of existing modes of operations (SP 800-38 series)
- SP 800-38A specifies encryption only modes – the oldest modes and implemented in most of the applications (e.g. CBC)
  - It has been a trend to use authenticated encryption modes (AEAD) (e.g. TLS 1.3)
- SP 800-38D (GCM) is an authenticated encryption and adopted in IETF and IEEE 802.1AE
  - GCM has limitations, e.g. very restrictive rules for the nonce and low max plaintext length
- Desired properties for new modes
  - Misusing resistance
  - Multi-key security
  - Key commitment
  - …

- NIST plans to develop a new mode of the AES that is a tweakable, variable-input-length-strong pseudorandom permutation (VIL-SPRP) with a reduction proof to the security of the underlying block cipher
  - Workshop: June 20-21. 2024 in NCCoE to discuss requirements, properties, parameters, and features
- The transition to new modes is not because the old modes are broken but new modes are more robust – we need new strategies for new transitions

Modes of operations
38A – Encryption only mode
38B – CMAC;
38C- CCM (authenticated encryption)
38D-GCM (authenticated encryption)
38E- XTS-AES (based on IEEE 1619)
38F- Key wrapping
38G- format preserving

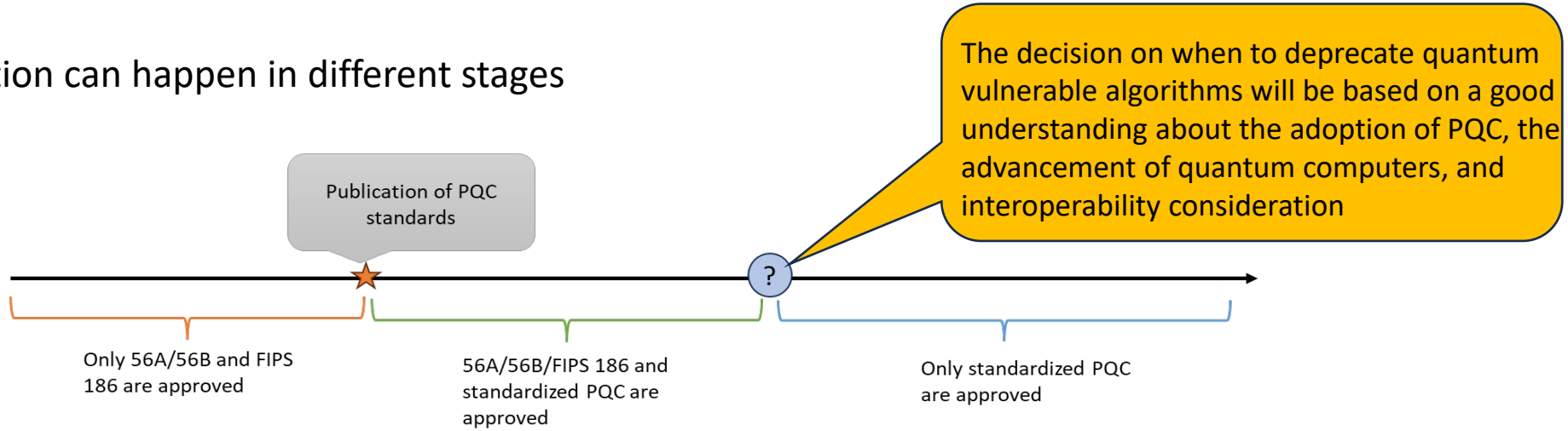
New Perspectives for Key Encapsulation Mechanism

- The schemes specified in SP 800-56A (DH, MQV) and SP 800-56B(RSA) were based on X9.42, X9.63, and X9.44 developed in 1990s
  - They are not key encapsulation mechanisms but “key exchange” or “key transport”. They can not be proved to be IND-CCA2 secure (or at the time CCA2 concept was not proposed.)
- NIST PQC call for IND-CCA2 secure KEM
  - ML-KEM (Kyber), specified in draft FIPS 203, can be proved IND-CCA2 secure
- The transition is beyond quantum vulnerable to quantum resistance
  - The transition is to schemes with a more advanced security concept
  - SP 800-227 is under development to provide guidance on using KEM in key establishment protocols

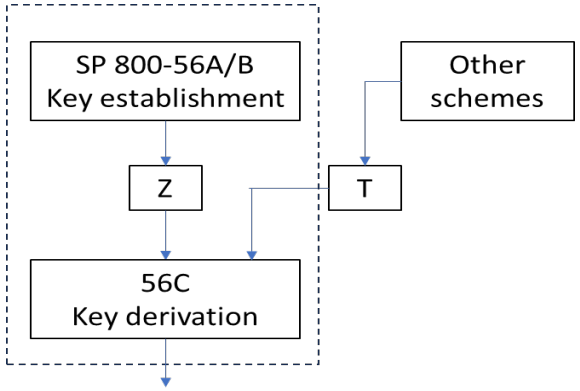
Informally, IND-CCA2 security requires the ciphertext is random to an attacker no matter how an attacker inquires a decryption oracle with adaptively chosen ciphertext to obtain the plaintext. That is after the attacker gets many pairs of ciphertext, plaintext, for two messages M_1 and M_2 generated by the attacker, a returned ciphertext C is an encryption of one of M_1 and M_2, selected randomly. The probability of correct guess which of M_1 and M_2 is not significantly larger than ½.

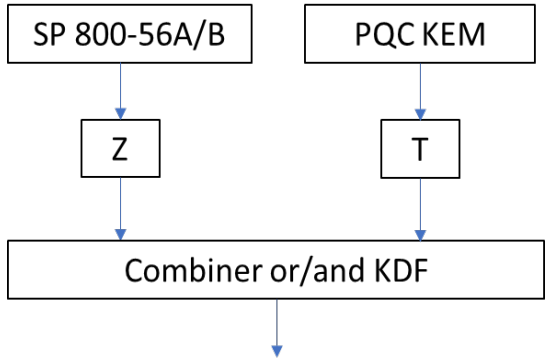
PQC Transition and Hybrid Mode

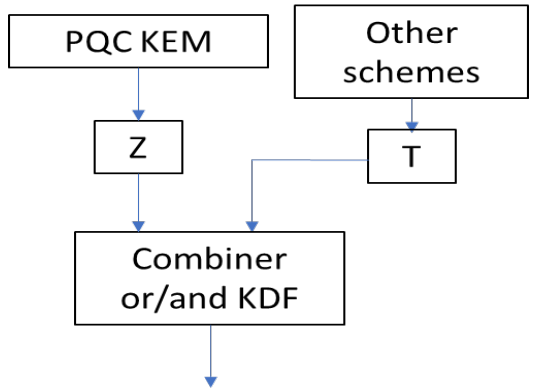
- The transition can happen in different stages



- In each stage, hybrid mode and dual signatures will be validated differently
  - Currently, NIST approves implementation with 56A and 56B with hybrid key derivation in 56C – allow input of another shared secret from a PQC algorithm or a QKD







Transition Challenges and Crypto-Agility

- Each transition, whether the transition is to adopt a different key/parameter size or to adopt a different algorithm, will impact hardware, software, API, protocols, and more
- It must consider interoperability and backward compatibility – also prevent from downgrade attacks
- Crypto-agility has been considered as a key for smooth transitions

Crypto Agility is

1) the ability for machines to select their security algorithms in real time and based on their combined security functions;
2) the ability to add new cryptographic features or algorithms to existing hardware or software, resulting in new, stronger security features; and
3) the ability to gracefully retire cryptographic systems that have become either vulnerable or obsolete

Crypto-agility: Notations, Requirements, Motivations

the **feasibility** of replacing and adapting cryptographic schemes in software, hardware and infrastructures, and should enable such procedures without interrupting the flow of a running system

the **ability** to adopt and integrate new cryptographic algorithms with no significant changes to the infrastructure, and without disruptions to running systems

the **capability** to apply repeated cryptographic changes (migrations) over time within a stable (non-changing) IT-architecture

the **stability** towards other systems, even after adapting its cryptographic measures

the **flexibility** to implement, update, and replace cryptographic components within IT-systems, without affecting its functionality

Existing Approaches and Solutions

Protocol agility

Design agility

Hardware agility

API agility

Crypto-agility: Protocol and Algorithm

- Support of multiple cryptographic algorithms can be interpreted as an implementation of crypto-agility
  - TLS, IKE, etc. allow negotiation among multiple options
  - Hybrid mode to use multiple algorithms for key establishment
  - PKI: composite and non-composite certificate
- RFC 7696 “Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms” (2015) – provides guidelines to ensure that protocols can migrate from one mandatory-to-implement algorithm suite to another over time
- Cellular network (5G, 3GPP 133.501) supports negotiations of the algorithms for access authentication and protections of connections

Crypto-agility: Design

- Expand existing infrastructure to be able to exchange cryptographic algorithms, e.g.
  - allow multiple algorithm options in design, e.g. some V2V secure communication protocol takes adaptation of key length and cryptographic algorithms during PKI operation into account [1)]
  - consider algorithm agility on TPM 2.0 ECC Functionalities [2)]
- Algorithm independent design, e.g. in blockchain [3)]

1) "Public Key Infrastructure and Crypto Agility Concept for Intelligent Transportation Systems" https://personales.upv.es/thinkmind/dl/conferences/vehicular/vehicular_2015/vehicular_2015_1_30_30028.pdf
2) "Algorithm Agility – Discussion on TPM 2.0 ECC Functionalities" https://link.springer.com/chapter/10.1007/978-3-319-49100-4_6
3) "PQFabric: A Permissioned Blockchain Secure from Both Classical and Quantum Attacks" https://arxiv.org/abs/2010.06571

Crypto-agility: Hardware

- FPGA based cryptographic accelerator, designed with algorithm-agility in mind [1)]
- Repurpose hardware designed for RSA together with lattice-based algorithms (integer multiplier) [2)]
- Unified instruction-set architecture leverages the synergies between similar PQC schemes [3)]

1) "Algorithm-agile cryptographic coprocessor based on FPGAs"
2) "Post-Quantum Cryptography with Contemporary Co-Processors" https://eprint.iacr.org/2020/1303.pdf
3) "A Unified Cryptoprocessor for Lattice-Based Signature and Key-Exchange" https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9920009

Crypto-agility: API

- plug-in structure in the Cryptography API: Next Generation from Microsoft to exchange cryptographic algorithms without any change to the code of the program [1)]
- extended library that provides many PQC algorithms and makes it easy to select and interchange them in different security strength levels, e.g. LibOQS [2)]

1) "Security Issues on the CNG Cryptography Library (Cryptography API: Next Generation)" https://ieeexplore.ieee.org/document/6603762
2) https://openquantumsafe.org/

Crypto-agility: Challenges, tradeoffs and limitations

- Security and complexity trade-offs - having many cryptographic options opens an unknown space for attack surfaces, such as downgrade attacks
- Resource limitations for crypto-agility
  - Hardware size may limit how many and which algorithms can be implemented – new algorithms require additional hardware resources to be efficiently integrated into the established protocols
  - Bandwidth may limit deploying new algorithms with large pk or sig or cipher or hybrid mode in some protocols
- Some cryptographic schemes are primitive dependent, e.g.
  - Password-based key derivation* Argon+ relies on the compress function of a hash function Blake, one of the finalists in SHA3 competition
  - Identity-based encryption (IBE), attribute-based encryption (ABE), threshold cryptography/multi-party computation, rely on algebraic properties of the underlying cryptographic primitives

*NIST SP 800-131 specifies PBKDF2 computing-hard for brute-force attack. New trend is use memory-hard password KDFs e.g. Argon+

How to evaluate Crypto-Agility?

- A proposal on a maturity model for crypto-agility assessment [1)]
  - a maturity model for determining the state of crypto-agility
  - it consists of five levels, for each level a set of requirements have been formulated based on literature review
- The model provides certain guidance and can be considered as a framework
  - Is it possible to use a general framework for different “systems”?

    - Level 0 - Initial/Not Possible: hardware or software limitations that do not allow subsequent changes to the original design
    - Level 1 – Possible: can be adapted so that their cryptography can respond dynamically to future cryptographic challenges
    - Level 2 – Prepared: already implement certain measures for crypto- agility, but are not yet fully ready to actively realize it
    - Level 3 – Practiced: migration between different cryptographic methods is demonstrably, effectively, and securely feasible
    - Level 4 – Sophisticated: compatibility is not limited to a specific system but can be scaled across a broader infrastructure; allows for a fast and automated migration between different cryptography schemes

1) “Towards a maturity model for crypto-agility assessment” https://arxiv.org/abs/2202.07645

Crypto-Agility: Research areas

- Security analysis on protocols and countermeasures for downgrade attack
- Security and complexity study for systems (platforms and protocols)
- Agility for resource limited communication environments
- Limitations and potentials for re-purpose cryptographic co-processors

Crypto-agility: What NIST can do to move forward?

- Constantly review and update published standards and include crypto-agility as a consideration
- Timely provide guidelines for each stage of transition and enable algorithm validation
- Work with industry communities and standards organizations to understand challenges and explore specific agility strategies and techniques for different systems
- Accommodate best practice – NCCoE partnership, workshops and reports to enable crypto-agility – maturity assessment
- Encourage research of hardware optimizations for crypto-agility
- Promote protocol level crypto-agility through contributions to IETF initiatives

THANKS!