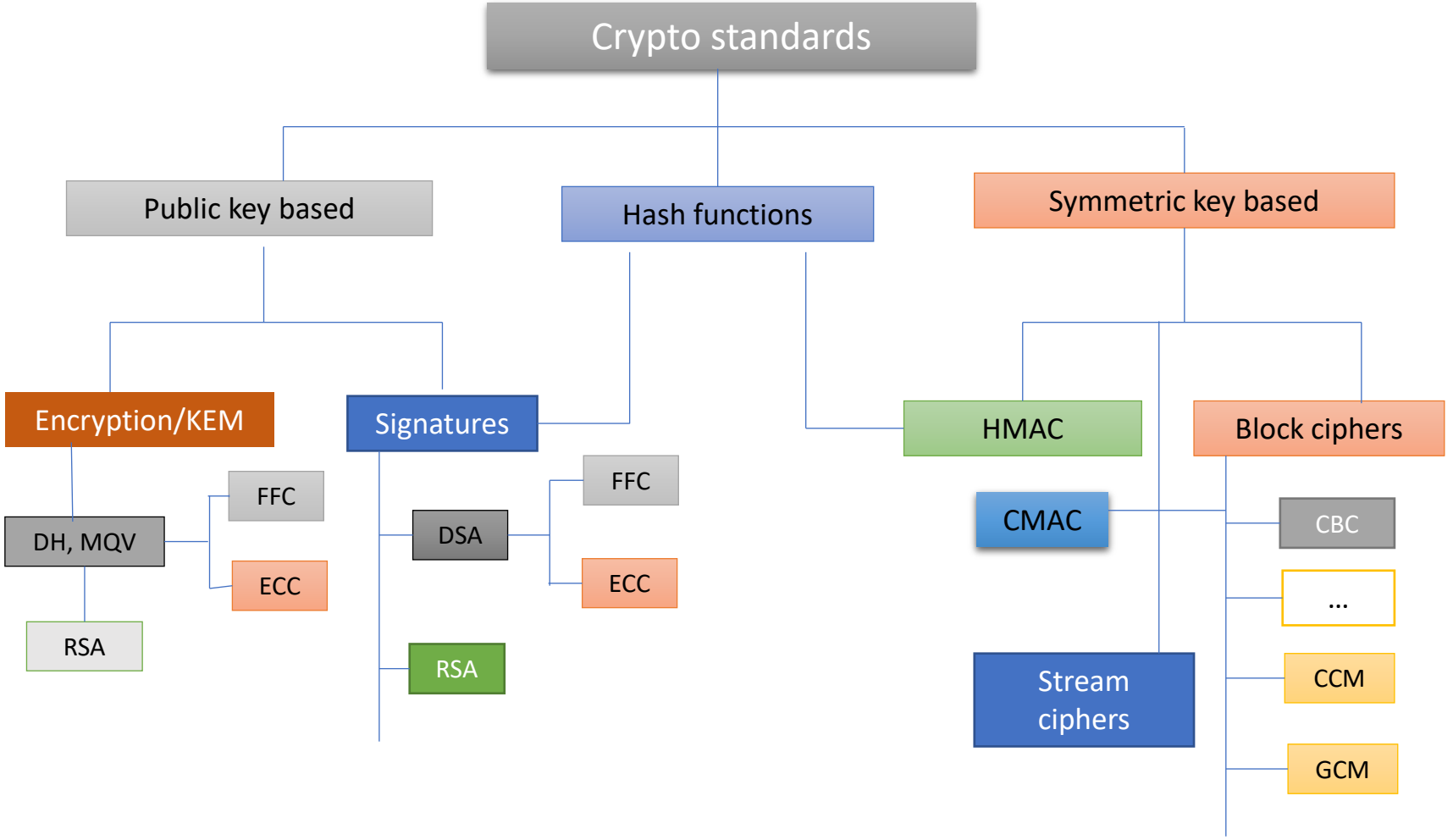
National Institute of Standards and Technology
U.S. Department of Commerce

Next Generation Cryptography Standards

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

ICISC 2020

Cryptography standards – Algorithms and Categories



Cryptography standards - Organizations

Cryptography standards – Early Stage

- NIST developed the first encryption standards in 1970s, Data Encryption Standards (DES), and published as Federal Information Processing Standard (FIPS) 47 in 1977
  - The main application was ATM machine for banks and credit card companies
- Cellular standards, 2G and earlier, use proprietary cryptographic algorithms and security flaws were identified when they were published. e.g.
  - A5/1 and A5/2 in GSM standards
- Public-Key cryptography was invented in 1976 -1977, while the standardization activities did not start until 1994 -1995
  - IEEE-SA – P1363
  - X9 for Financial Service
- Internet Protocols (SSL, TLS, IPSec) were early adopters for public-key cryptography
  - PKI support enabled many-to-many authenticated key establishment

Cryptography standards – Evolution

- Only publicly scrutinized cryptographic algorithms and mechanisms are considered for standardization
  - Completely abandoned proprietary algorithms
- Diversified cryptographic algorithm designs provide more options for standardization
  - Hash function, from Merkel-Damgaard structure to permutation-based sponge function
  - Bock cipher, from Feistel design to substitution-permutation network (SPN), tweakable block cipher, etc.
- Formal security definitions have been introduced and provably security considered for candidate algorithms in standardization, e.g.
  - Indistinguishability under chosen ciphertext attack/adaptive chosen ciphertext attack (IND-CCA1 , IND-CCA2) for encryption
  - Existential unforgeability under chosen message attack (EUF-CMA) for digital signatures

Cryptography standards – New Trends in Applications

- Perfect forward secrecy is highly desired for authenticated key establishment
  - Use ephemeral public keys for key establishment
- Use authenticated encryption with additional data instead of ad hoc combinations of encryption and authentication
  - e.g. GCM, CCM, etc.
- Privacy-enhancing cryptography is demanded to protect user in the cloud
  - Fully Homomorphic Encryption, Zero-Knowledge Proof, Secure Multi-party Computation
- Target on extended security objectives to resist
  - Side-channel attack
  - Multiple key attack
  - Leakage attack

Challenges in Next Generation of Crypto Standards

- Deal with extremes
  - Extremely powerful attack technologies, e.g. using quantum computers
  - Extremely constrained implementation environment, e.g. sensors
- Transition and backward compatibility
  - Increased key sizes, stronger hash functions
  - Post-quantum cryptography migration
- Future technologies and applications demand a more diversified cryptography portfolio, e.g. 5G, AI, Blockchain, etc.
  - Cryptography implementation challenges hardware resource
- Hardware attacks can be catastrophic
  - Applying countermeasures can increase the cost of implementations
- And more …

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

Post-Quantum Cryptography

NIST Process Update: Milestones and Timeline

2016

Determined criteria and requirements

Announced call for proposals

2017

Received 82 submissions

Announced 69 1st round candidates

2018

1st round analysis

Held the 1st NIST PQC standardization Conference

2019

Announced 26 2nd round candidates

Held the 2nd NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidates

2021

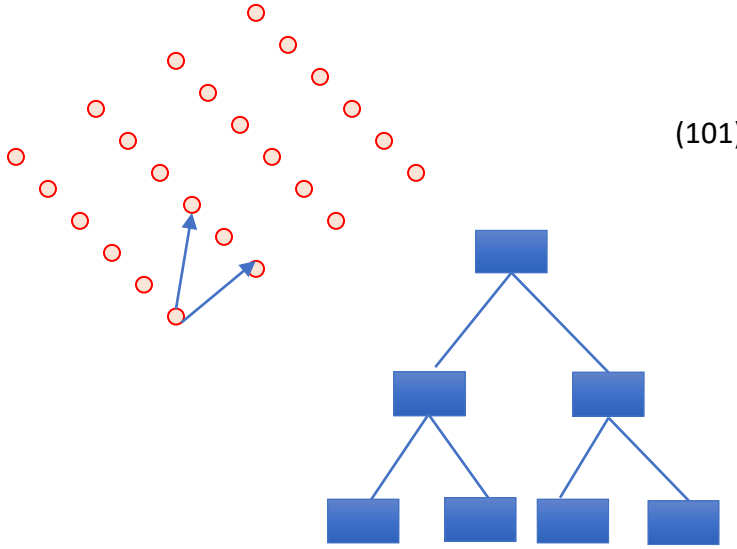
Hold the 3rd NIST PQC Standardization Conference

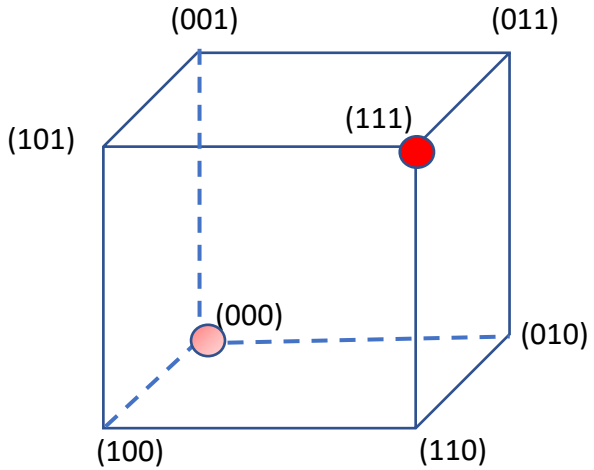
2022-2023

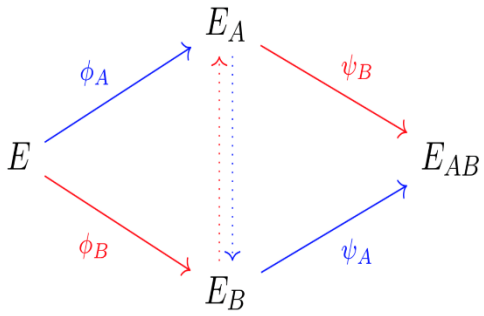
Release draft standards and call for public comments

Post-Quantum Cryptography

- Some actively researched PQC categories
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key -based signatures
  - Isogeny-based schemes







$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

Scope, Security Definitions, Strength Levels

- The scope of submissions
  - Public key encryption /Key establishment
  - Digital signature
- Definitions (proofs recommended, but not required) used to judge whether an attack is relevant
  - IND-CPA/IND-CCA2 for encryptions and KEMs
  - EUF-CMA for signatures
- Security strength is defined at 5 levels

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

Challenges and Considerations in Selecting Algorithms

Security

- Security levels offered
- (confidence in) security proof
- Any attacks
- Classical/quantum complexity

Performance

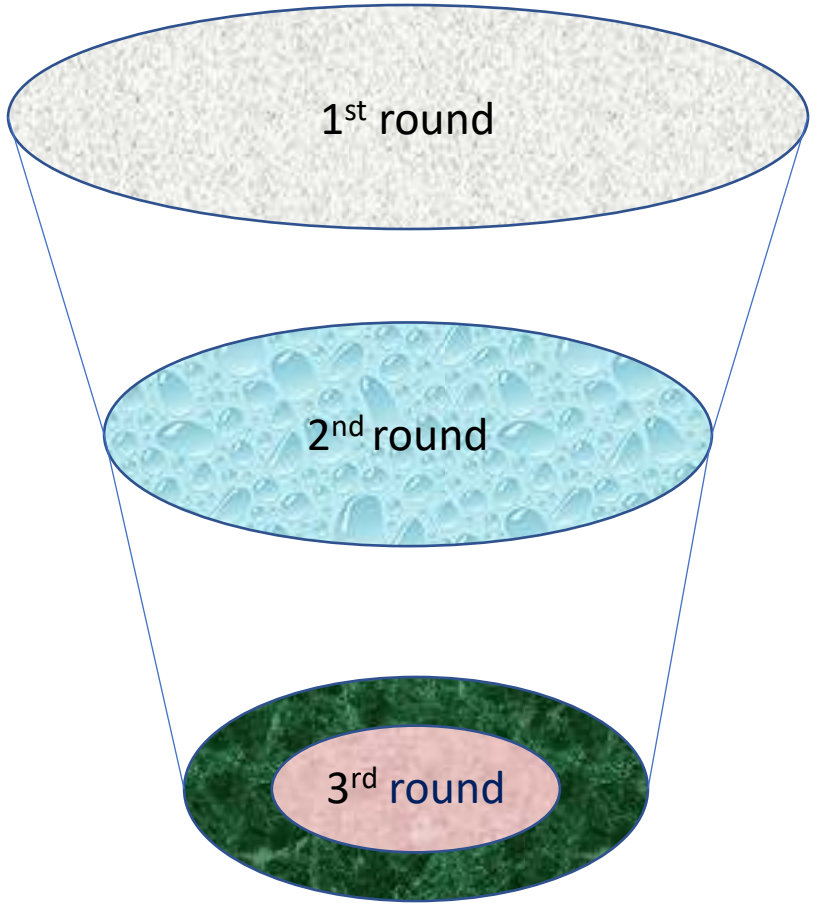
- Size of parameters
- Speed of KeyGen, Enc/Dec, Sign/Verify
- Decryption failures

Algorithm and implementation characteristics

- IP issues
- Side channel resistance
- Simplicity and clarity of documentation
- Flexible

Other

- Official comments/pqc-forum discussion
- Papers published/presented



First, Second, and Third Round Candidates

1st round	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate			
Stateless Hash/Symme			
Other			
Total			

2nd round	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-			
Statele based			
Isoger			
Total			

3rd round	Signatures		KEM/Encryption		Overall	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	3	4	5	7	8

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

Lightweight Cryptography

Background, Scope, Challenges

- Respond to the need for cryptography standards for applications in constrained environment that are not well-served by existing NIST standards
- NIST started to explore approaches in 2015 – Held workshops and published NISTIRs
  - Feedback shaped the submission requirements and identified the scope
- Scope: Symmetric Key Based Authenticated Encryption with Additional Data (AEAD) with optional hashing functionality
- The task is not light – more challenging in the design to satisfy all security requirements and performance for different platforms
  - Tailoring to target devices and applications could lead to many standards
  - The attackers are not constrained and can use powerful computing tools

Milestones, Timeline and Candidates

- Timeline and milestones
  - In April 2019, announced 56 Round 1 candidates (out of 57 submissions)
  - In August 2019, announced 32 Round 2 candidates
    - Selection based on cryptographic maturity of the designs
- Expected to announce finalists in December 2020 and final winners in December 2021
- The candidates include (tweakable) block ciphers, stream ciphers, permutation, …
  - The designs reflected the technology advance in the past 20 years
  - Most designs are based on the primitives used in the standardized algorithms such as AES, Keccak, PHOTON, SKINNY, SPONGENT
  - Maturity of analysis by the submitters and third parties
  - Many candidates claimed additional security features: Nonce misuse security, releasing unverified plaintext (RUP) security, post-quantum security, side channel resistance, etc.
- Benchmarks are provided by NIST team and teams research community on different software and hardware platforms

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

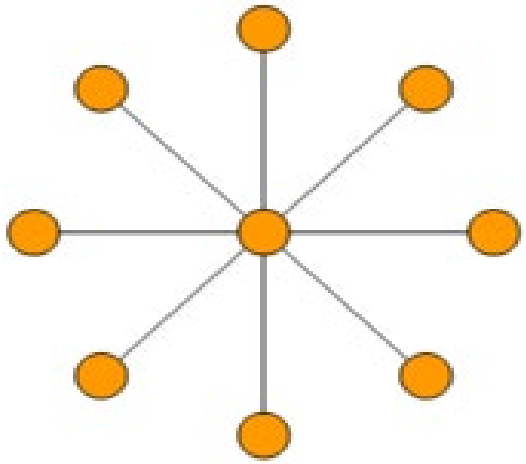
Threshold Cryptography

Security through multi-party computation

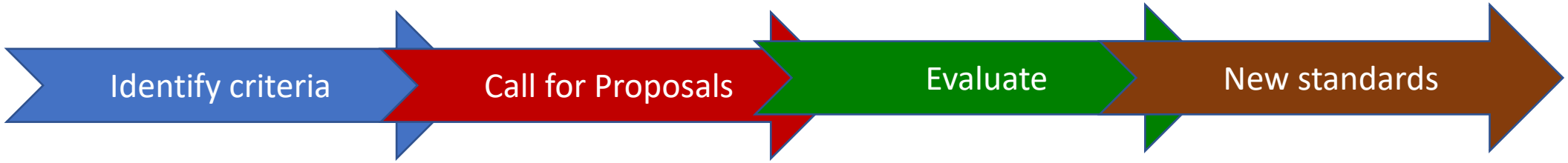
- Security can be affected by implementation vulnerabilities
  - Operators of cryptographic implementations can go rogue
  - Attacks can exploit differences between ideal vs. real implementations
- The threshold approach use redundancy & diversity to mitigate the compromise of up to a threshold number (f-out-of-n) of components
- Threshold cryptography is to avoid single point of failure through multiparty computation – not put all the eggs in one basket
- Multiparty computation has been an active area
  - Many approaches are on the table
- Introducing threshold cryptography to the standards must consider interoperability

Approaches and Next Steps

- NISTIR 8214A "NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives" outlines the potential candidate space into specification levels of domains, primitives, and threshold modes
- Potential standards
  - Key-generation (e.g., RSA, ECC, AES)
  - Signing (e.g., RSA, ECDSA, EdDSA)
  - Enciphering (e.g., AES, lightweight ciphers)
  - Decryption (e.g., RSA)
  - Random number generation
  - Post-Quantum Crypto (emerging standards)



- Next steps



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

Privacy- Enhancing Cryptography

Privacy in a Data-Based World

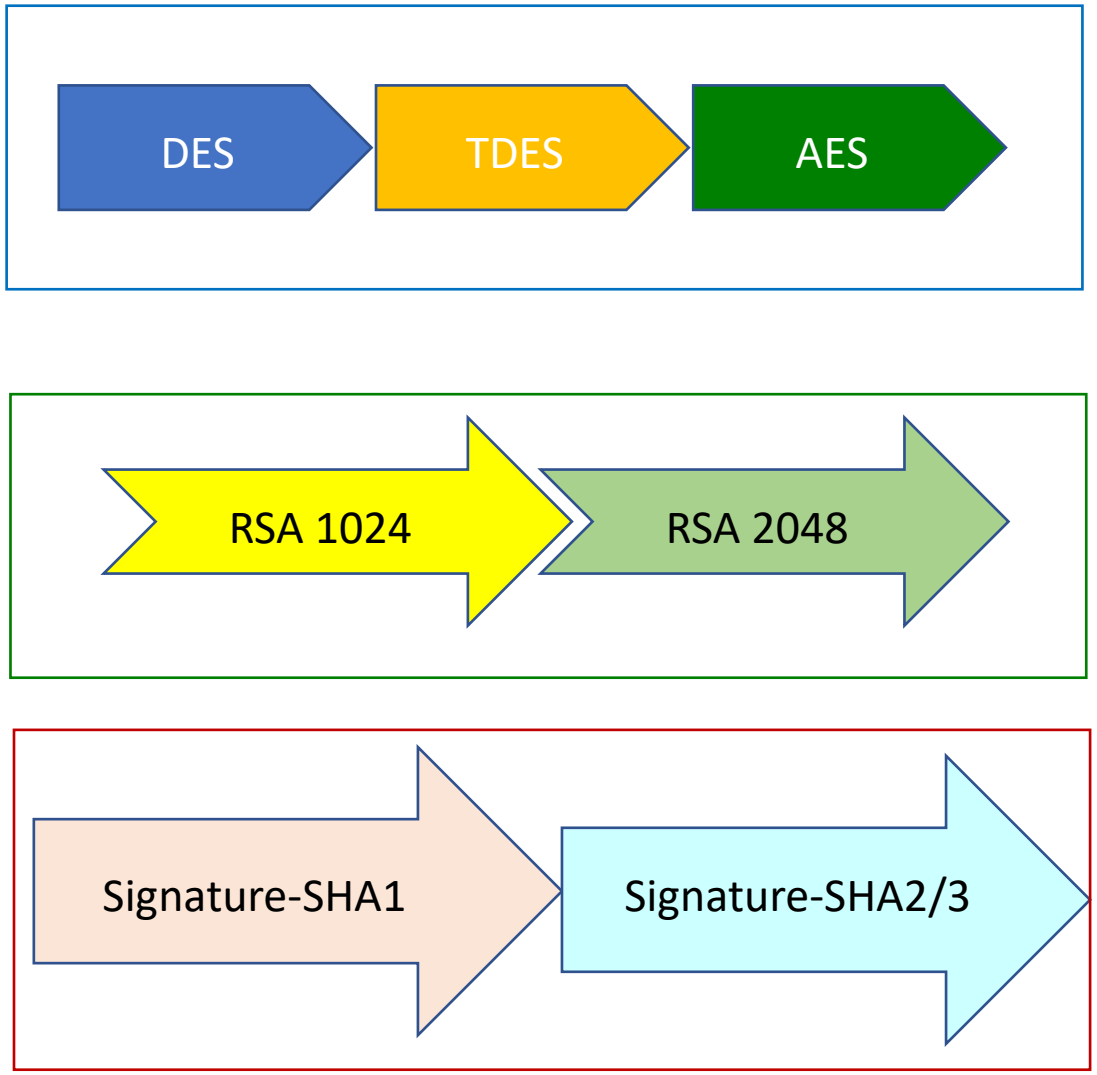
- Large amount of user data have been processed in the cloud and privacy protection becomes more important than ever.
  - User data are collected for many different purposes., e.g. Covid-19 contact tracing
- Cryptography standards are needed for privacy
- Issue: many cryptographic techniques for privacy have been invented and no consensus on what are the most essential primitives and how those will be adopted
- Approaches: Outreach through participation and contribution to academic/industry initiatives to understand the need and potential adoption
  - ZKProof (https://zkproof.org) – Zero-Knowledge Proofs allow one party (the prover) to prove to another party (the verifier) that a given statement is true and/or that some mathematical solution is known to the prover without revealing the knowledge
  - FHE (http://homomorphicencryption.org/introduction/) - Fully homomorphic encryption (FHE) allows performing computation on encrypted data without having to perform decryption

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

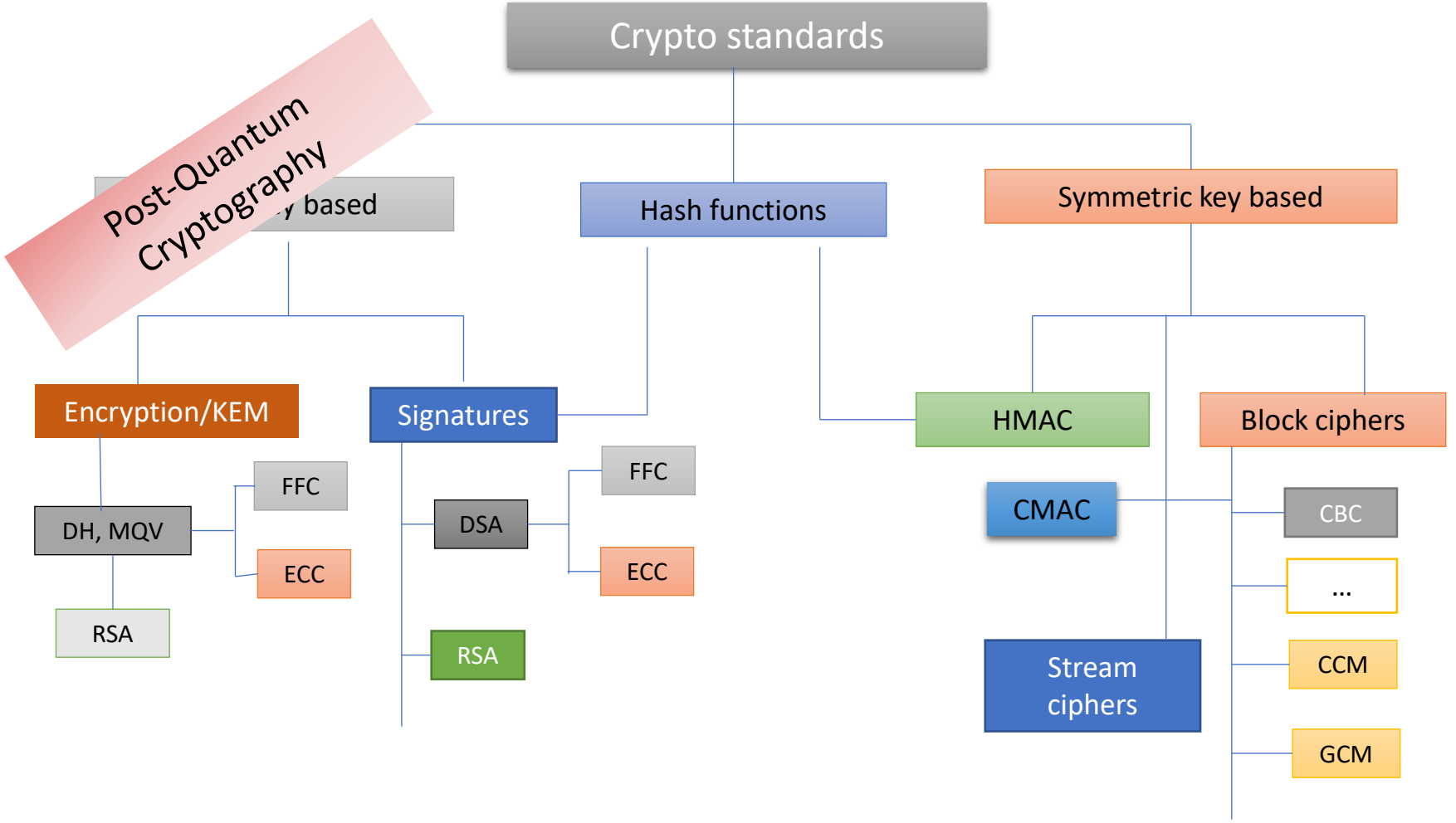
Transition and Migration

Cryptography Standards – Constant Transition

- Technology advancements and more sophisticated cryptanalysis empower attackers and increase threat levels
  - Algorithms become deprecated and need removal
  - New primitives and algorithms are introduced
  - Larger key/signature/ciphertext sizes are needed
  - Alternative parameter sets are introduced
- Transition is often costly and may be an obstacle for compatibility

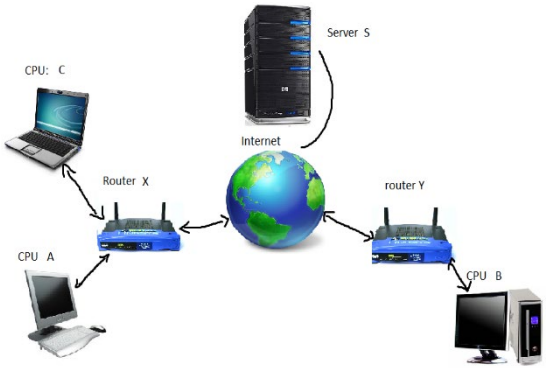


Transition to Post-Quantum Cryptography



Challenges and Strategies in Transition to PQC

- Public key Cryptography has been used everywhere and two most important usages are for
  - Communication security (IPsec, TLS, etc)
  - Trusted platforms (Code signing)
- Transition is going to be a long journey and full of exciting adventures
  - New features, characters, implementation challenges
  - Not quite drop-in replacements
  - Risk of disruptions in operation and security
- Enable crypto agility is the key for smooth migration
  - A capability allowing to remove some algorithms and to introduce new algorithms



Initiatives in Transition to PQC

- Prototype PQC candidates in TLS and other protocols
- Stateful Hash Based Signatures for Early Adoption
  - Internet Engineering Task Force (IETF) has released two RFCs on hash-based signatures
    - RFC 8391 "XMSS: eXtended Merkle Signature Scheme" (By Internet Research Task Force (IRTF))
    - RFC 8554 "Leighton-Micali Hash-Based Signatures" (By Internet Research Task Force (IRTF))
  - NIST SP 800-208 "Recommendation for Stateful Hash-Based Signature Schemes" published in October 2020
  - ISO/IEC JTC 1 SC27 WG2 Project: Stateful hash-based signatures will be specified in ISO/IEC 14888 Part 4
- Hybrid mode as an approach for migration to PQC
  - Use an existing public key standard, e.g. Diffie-Hellman Key Agreement and a PQC mechanism
  - Each of them establishes a "shared secret value"
  - Derive session keys from both secret values

Summary

- It is full of challenges and opportunities in developing next generation cryptography standards
- Future technologies will shape the trends of cryptography applications
- Next generation cryptography standards will deal with
  - Quantum threats with Post-quantum Cryptography
  - Protection demand for constrained environment with Lightweight Cryptography
  - Hardware attacks and implementation failures with Threshold Cryptography
  - Privacy concerns in all digital service with privacy-enhancing cryptography
- Transition will be constantly required
  - Cryptography agility is the key
- The next generation will target on extended security objectives to resist advance attacks