NIST Crypto Standard Approaches

- Past, Present, and Future

Lily Chen
Manager of Cryptographic Technology Group
Computer Security Division, ITL, NIST

March 11, 2019

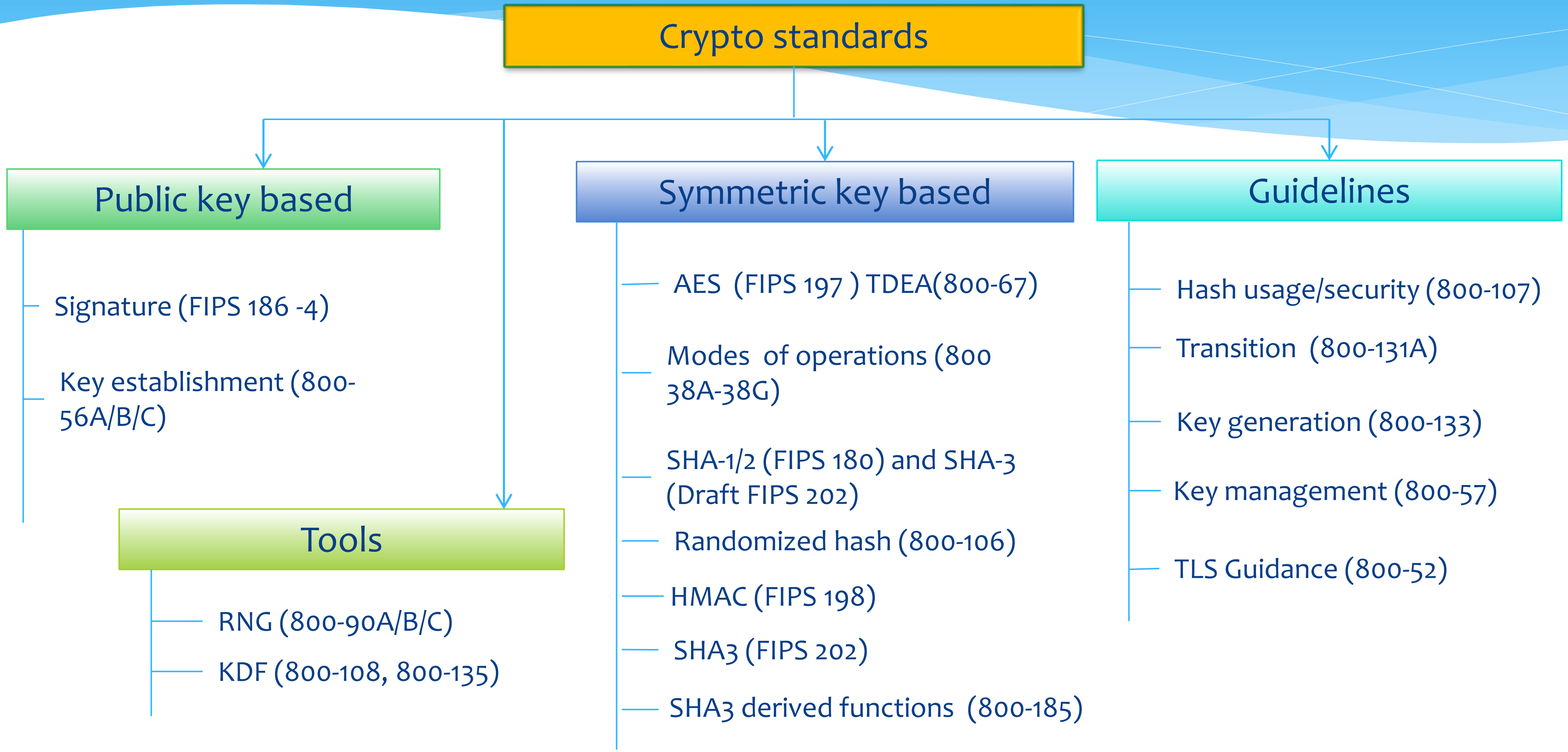
A Short History of NIST Crypto Standards
- Major Milestones

- FIPS 46 ”Data Encryption Standard (DES)” - 1977
- Public–key Cryptography (FIPS 186, SP 800-56A/56B) – 1990s
- FIPS 197 “Advanced Encryption Standard (AES)” – 2001
- FIPS 202 “SHA-3” (Secure Hash Function 3) – 2015
- Ongoing projects
  - Post-Quantum Cryptography (PQC)
  - Lightweight Cryptography (LWC)
  - Threshold Cryptography
- What is next?

NIST Crypto Standards Approaches

- Cryptographic algorithm competitions
  - Advanced Encryption Standard (AES)
  - Secure Hash Algorithm – 3 (SHA-3)
- Adoption of standards developed in other standards organizations
- Develop new standards
  - In-house development based on well accepted research results (e.g. SP 800-56C)
  - Selected among submissions (e.g. modes of operations in SP 800-38 series)
- Not quite a competition but based on call for submissions (PQC, LWC)
- What other approaches?

NIST Crypto Standards – Overview[1]



Crypto standards

- Public key based
  - Signature (FIPS 186 -4)
  - Key establishment (800-56A/B/C)
- Tools
  - RNG (800-90A/B/C)
  - KDF (800-108, 800-135)
- Symmetric key based
  - AES (FIPS 197) TDEA(800-67)
  - Modes of operations (800 38A-38G)
  - SHA-1/2 (FIPS 180) and SHA-3 (Draft FIPS 202)
  - Randomized hash (800-106)
  - HMAC (FIPS 198)
  - SHA3 (FIPS 202)
  - SHA3 derived functions (800-185)
- Guidelines
  - Hash usage/security (800-107)
  - Transition (800-131A)
  - Key generation (800-133)
  - Key management (800-57)
  - TLS Guidance (800-52)

[1] This is not a complete list

Cryptographic Competitions

- AES competition
  - 1997 -2001
  - 15 → 5 → 1
  - Cryptographers from 12 countries were involved in the candidates design
- SHA-3 competition
  - 2007-2012
  - 51 → 14 → 5→ 1
  - Cryptographers from more than 24 countries were involved in SHA-3 candidates design

Cryptographic “Non-Competitions”

- Post-quantum cryptography (encryption, Key exchange, and signature)
  - Call for proposals - 2016
  - 69 → 26 →
  - Submissions received from 6 continents and 26 countries
  - Plan to release draft standards in 2022-2023
- Lightweight cryptography (Authenticated encryption and optional hash function)
  - Call for proposals - 2019
  - 57 submissions (first round candidates will be announced after March 29, 2019)
  - Plan to release draft standards in 2021

NIST

Adoptions from Other Standards

- X9F1
  - FIPS 186 (ECDSA X9.62 (now X9.142) and RSA X9.31
  - SP 800-56A: based on X9.42 and X9.63
  - SP 800- 56B: based on X9.44
  - SP 800-90A: based on X9.82 part 3
- IEEE 802.11 (wireless)
  - 800-38C CCM mode
- IEEE Std 1619-2007
  - 800- 38F XTS-AES

Selection and In House Development

- Call for submissions on block cipher modes of operations, e.g.
  - SP 800-38D GCM mode
- Guideline standards
  - SP 800-131A (crypto transition)
  - SP 800-57 (key management)
  - SP 800-52 (TLS guidelines)

Review and Revision

- Standards are reviewed every 5 years[1] or when needed and may be revised to
  - Correct errors
  - Clarify raised issues
  - Cover new development (e.g. 800-52 Rev. 1 TLS), attacks (e.g. revise FIPS 180 after SHA-1 attack), implementation need (e.g. add SHA512/224 and SHA512/256), etc.
- All the draft revisions are released for public comments before the finalization

[1] started to establish the 5 year review routine

Make Decisions Through Study and Public Input

- Before moving forward with PQC and LWC standardization, we conducted internal studies, published NIST Internal Reports (NISTIRs), and held workshops
- The decision may not always be to move forward, for example
  - Pairing-based cryptography has been used to provide special featured cryptosystems such as Identity Based Cryptography (IBE)
  - NIST conducted a study, held a workshop, and published a technical report in 2015
  - Decision was made not to move forward
- The decision can be on how to move forward, e.g. Threshold cryptography

Challenges to Crypto Standardization

- Deal with extremely powerful attack technologies (e.g. quantum computers) and constrained implementation environments (e.g. RFID and sensors in IoT)
- Deprecate weak cryptographic algorithms and methods and assure backward compatibility (e.g. sunset triple DES and PKCS#1 v1.5 padding)
- Handle variations created in practice (e.g. KDFs 800-56C, 800-108, 800-135, …)
  - It has never been easy to find a common ground for standardization
- Emerging technologies constantly demand for new crypto tools
- Resource limits
  - Standards development and maintenance are always costly
  - It takes months or even years to develop or revise a standard

Practical Security Guidance

- Introduce countermeasures to physical attacks (e.g. side-channel attacks)
- Mitigate impact of compromising parties (e.g. threshold cryptography)
- Apply domain size limit on format preserving encryption
- Set restrictions on the usage of lightweight cryptography algorithms
- Guide the application community to avoid pitfalls (e.g. DUHK (Don't Use Hard-coded Keys))

New Crypto Tools on Demand

- For privacy enhancement, e.g.
  - Zero-knowledge proof
  - Fully homomorphic encryption
- For BlockChain, e.g.
  - Ring signatures
- For access control, e.g.
  - Attribute-based encryption (ABE)
- And more …

Interoperability Considerations

- Cryptography standards shall support interoperability
  - Not to limit the creativity in each application area
- NIST crypto standards have focused on primitives rather than protocols
  - Allow applications to use them as basic blocks
- Significant effort is needed to identify a right scope, for example,
  - Basic mathematics operations
  - The range of parameters and keys
  - Auxiliary functions
  - Error condition handling, and
  - More

Evaluation and Testing

- Cryptographic implementations have been evaluated through NIST Cryptographic Module Evaluation Program (CMVP) based on FIPS 140 for US government usage
- Algorithm implementations are tested through Cryptographic Algorithm Evaluation Program (CAVP)
- When new techniques are standardized, evaluation and testing must be considered to make sure to allow the new NIST standards being served for its primary purpose, i.e. government usage

Work with Other Standards Organizations

- Worked with other standards organizations on crypto standards and crypto applications such as IETF, IEEE-SA, TCG, ISO/IEC JTC1 SC27, X9, etc. to
  - Understand the application needs, the trend , and the best practice
  - Promote US in the global marketplace
  - Support usage of NIST crypto standards to enable government using "off the shelf" products
  - Identify issues and problems for improvement opportunities for NIST standards

Future Approaches

- Rule of Thumb – Make our decisions in an open and transparent manner
- No cookie cutter approaches for all the crypto areas and situations
- Work with application community to understand the need, trend, and best practice
- Continue to grow internal expertise and engage with academic research community
- Always open for suggestions, comments, questions, …
- Follow us at http://csrc.nist.gov

NIST