Cryptography Standards

Lily Chen
Computer Security Division
NIST
Outline

- Scope and status of NIST cryptography standards
- Major development methods
- Challenges and research opportunities
- Cryptographic standard applications
- Cryptographic standard process review
- Move forward
Crypto Standards - Overview

Crypto standards

Public key based
- Signature (FIPS 184)
- Key establishment (SP800-56A/B)

Symmetric key based
- AES (FIPS 197)
- Modes of operations (SP800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- Randomized hash (SP800-106)
- HMAC (FIPS 196)

Guidelines
- Hash usage (SP800-107)
- Transition (SP800-131A)
- Key generation (SP800-133)
- Key management (SP800-57)

Tools
- RNG (SP800-90A/B/C)
- KDF (SP800-108, 800-135, 56C)
Symmetric Key Based Cryptography

- **Block Ciphers**
  - FIPS 197 Advance Encryption Standard (AES)
  - Modes of operations
    - NIST SP 800-38A-38G
- **Hash Functions**
  - FIPS 180-4 SHA-1 and SHA-2
  - Draft FIPS 202 SHA-3
- **Message authentication codes**
  - FIPS 196 HMAC (hash function based)
  - NIST SP 800-38B CMAC (block cipher based)
Public Key Cryptography

- **Digital Signature**
  - FIPS 186-4
    - DSA (Discrete Logarithm Based); and
    - RSA (Factorization Based)

- **Key Establishment**
  - NIST SP 800-56A Discrete Logarithm Based
    - DH, MQV
  - NIST SP 800-56B Factorization Based
    - RSA based key transport and key agreement
Major development methods

- Cryptographic algorithm competitions, e.g.
  - Advanced Encryption Standard (AES)
  - Secure Hash Algorithm – 3 (SHA-3)
- Adoption of standards developed in other standard organization
- Develop new standards
  - In house development
  - Selected among submissions
Cryptographic Competition

- **AES competition**
  - 1997-2000
  - 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
Adoptions

- X9F1
  - 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
Selection and In House Development

- Call for submissions on block cipher modes of operations
  - SP 800-38D GCM mode
- Guideline standards
  - SP 800-131A
  - SP 800-133
Cryptographic Applications

- NIST crypto standards have been used in many protocols and implemented in different devices, e.g.
  - Key establishments and signatures
    - Internet Key Exchange (IKE)
    - Transport Layer Security (TLS)
  - Encryption (AES) and integrity protection (HMAC and CMAC)
    - IP layer (IPsec)
    - Transport layer (TLS between server and client)
    - Link layer (e.g. WiFi, Bluetooth, etc.)
  - Devices: servers, routers, laptops, smartphones, etc.
Guidelines on Crypto Applications

- SP 800-147 - BIOS Protection Guidelines (April 2011)
- Draft SP 800-157- Guidelines for Derived Personal Identity Verification (PIV) Credentials (work in progress)
Work with Standards Bodies

- Internet Engineering Task Force (IETF)
  - Internet security standards

- IEEE 802 wireless
  - Wireless security

- The Accredited Standards Committee X9
  - X9F-Data & Information Security
    - X9F1 Cryptographic Tools for financial service

- ISO/IEC JTC 1/SC 27 IT Security techniques
  - SC27 WG2 International crypto standards
    - Cryptography and security mechanisms
Challenges

- NIST published the first cryptography standard—FIPS 47 Data Encryption Standard (DES) in 1976, almost 40 years ago
- During the past 40 years
  - Cryptography research has significantly advanced
  - The cryptanalysis techniques is much more sophisticated
  - Many new algorithms/ideas have been proposed
  - Increased computing capacity super-powered both designers and attackers
  - Crypto applications are pervasive
  - The industry adopts crypto algorithms and schemes in a faster speed and broader scope
Research Opportunities

- Newly emerged cryptographic algorithms and schemes
  - Post-Quantum Cryptography
    - Resistant to quantum computing, e.g. Lattice-based
  - Light-weight crypto
    - For constrained environment
  - Privacy enhanced crypto
    - To protect user privacy
  - etc.

- The main questions to answer
  - Whether the technology is mature enough to be standardized; and
  - Whether it is truly demanded and what are the use cases
Cryptographic Standard Process Review

- Since September of 2013, news reports about leaked classified documents have caused concerns about NIST Crypto Standards
  - In particular, a Deterministic Random Bit Generator Dual_EC_DRBG in NIST SP 800-90A (X9.82) has been in question
    - Contributed by NSA
    - Parameters (P, Q) can embed a backdoor, unless selected randomly and independently
- In responding to the concern, NIST initiated review of crypto standard development process
- NIST released Interagency draft Report 7977 (NIST IR 7977) to request for public comments in February 2014
VCAT/COV Reviews

- Commissioned independent review by VCAT/COV
  - VCAT – Visiting Committee on Advanced Technology
  - COV – Committee of Visitors
- The NIST team provided materials and gave presentations about NIST cryptographic standards development process
- VCAT released a report with assessments and recommendations
- Recommendation summary
  - Openness and Transparency
  - Independent Strength and Capability
  - Clarification of NIST-NSA Relationship
  - Recommendation on specific technical issues
Future views

- Rely on crypto research community for security analysis and performance comparison
  - How much to weigh security proof is always a question
- Communicate with industry players to understand the applicability and interoperability.
  - Promote communications through actively involved in major industry standards
Summary

Cryptography Research

Cryptography Standards

Cryptography Applications