About ISO/IEC JTC 1 SC 27

- ISO/IEC JTC 1/SC 27 focus on IT Security techniques
  - A standardization subcommittee of the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- It consists of five working groups
  - Working Group 2: Cryptography and Security Mechanisms
- WG 2 usually has more than 20 active working projects (new standards, standards under revision, 5-year confirmation on published standards, study periods for new projects, etc.)
  - Lightweight cryptography is one of the projects (with multiple sub-projects)
  - The standards developed under this project is ISO/IEC 29192 series
Outline of ISO/IEC 29192

- ISO/IEC 29192 consists of six parts
  - Part 2 – Block Ciphers (2012)
  - Part 3 – Stream Ciphers (2012)
  - Part 4 – Mechanisms Using Asymmetric Techniques (2013) and Amendment 1 (2016)
  - Part 5 – Hash functions (2016)
  - Part 6 – Message Authentication Codes (MACs) (work in progress)
ISO/IEC 29192-1 General

  - Security: 80 bit security is considered as the minimum security strength for lightweight cryptography
  - Classification: Lightweight cryptography is classified by a combination of the constraints on chip area, energy consumption, program code size and RAM size, communication bandwidth, execution time
    - Hardware considers chip area and energy consumption (cycles, bits per cycle, power, energy, energy per bit, etc.)
    - Software considers program code size and ram size as well as the speed it can achieve
    - Other performance properties: short input performance and latency
ISO/IEC 29192-1 General (Cont’d)

- In Part 1 2012 version,
  - block ciphers and stream ciphers are listed as symmetric key based lightweight mechanisms, and
  - for mechanisms using asymmetric techniques, it introduces three kinds of schemes: authentication and key exchange, identity-based signature, and challenge-response authentication

- The security mechanisms in 29192 series overlap with other ISO/IEC standards, e.g.
  - ISO/IEC 18033 series specify encryption (block ciphers, stream ciphers, etc.)
  - ISO/IEC 9798 series specify entity authentication (symmetric key algorithms, digital signatures, etc.)
  - ISO/IEC 10118 series specify hash functions
ISO/IEC 29192-2 Block Ciphers

• ISO/IEC 29192 Part 2 (2012) specifies two block ciphers
  • PRESENT: block size 64 bits and key size 80 or 128 bits (CHES 2007)
  • CLEFIA: block size 128 bits and key size 128, 192, and 256 bits (FSE 2007)
• Amendment was proposed in the fall of 2014 to include two block ciphers
  • SIMON: with many block and key size combinations Block sizes from 32 to 128 and key sizes from 64 to 256
  • SPECK: with many block and key size combinations Block sizes from 32 to 128 and key sizes from 64 to 256
• After two six-month study periods, the first working draft (WD1st) of the amendment 1 with SIMON and SPECK was initiated in the fall of 2015
  • The minimum block and key size included in the working draft are 48 and 96 bits respectively
ISO/IEC 29192-3 Stream Ciphers

  - Enocoro: key size of 80 or 128 bits
  - Trivium: key size of 80 bits (selected by eSTREAM)
- Both of them are hardware oriented
ISO/IEC 29192-4 Mechanisms Using Asymmetric Techniques

  - A unilateral authentication mechanisms based on discrete logarithms on elliptic curves
    - Use zero-knowledge proof
    - Multiple variants are specified in ISO/IEC 9798-5
    - The version in ISO/IEC 29192-4 is a lightweight version and was proposed for RFID
  - An authenticated lightweight key exchange (ALIKE) mechanism for unilateral authentication and establishment of a session key
    - Designed for contactless transaction
    - A variant of RSA
  - An identity-based signature mechanism for wireless sensor network
    - Elliptic curve Schnorr signature with a trusted server involved for private key generation
ISO/IEC 29192-4 Amendment 1 Mechanisms Using Asymmetric Techniques

- ISO/IEC 29192 Part 4 Amendment 1 (2016) includes an Elliptic Curve based authentication scheme - ELLI
  - ELLI is designed for RFID reader to authenticate RFID tag
    - It is actually a static-ephemeral Diffie-Hellman key exchange
    - The reader uses an ephemeral public value as a challenge
    - The tag authenticate by demonstrating the shared secret value
  - It is executed over binary curves
ISO/IEC 29192-5 Hash Functions

- ISO/IEC 29192 Part 5 (2016) specifies three hash functions
  - PHOTON with permutation sizes of 100, 144, 196, 256 and 288 bits and hash output lengths 80, 128, 160, 224, and 256 respectively (Crypto 2011)
  - SPONGENT with permutation sizes of 88, 136, 176, 240 and 272 bits and hash output lengths 88, 128, 160, 224, and 256 respectively (CHES 2011)
  - Lesamnta–LW with permutation size 384 bits and hash output length 256 bits (ICISC 2010)
- Some of the variants cannot provide the minimum security strength (80 bits)
  - Those were warned not to be used as a general purpose hash function
ISO/IEC 29192-6 Message Authentication Codes (MACs)

- ISO/IEC 29192 Part 6 is still under development
  - Chaskey was submitted in Fall of 2014 - a permutation-based MAC algorithm that uses the Addition-Rotation-XOR (ARX) design methodology (SAC 2014)
  - A working draft was initiated in the fall of 2015
Summary

• Lightweight cryptography standards developed in ISO/IEC JTC SC27 cover the essential symmetric key based primitives (Block cipher, stream cipher, hash function, and MAC)
• The standards cover a relatively large range w.r.t. key size, block size, hash value, etc.
• Public key based algorithms are mainly for authentication purpose designed for specific applications (RFID, contactless transaction, and sensor networks)
• By Revisions/Amendments, additional algorithms/mechanisms may be included and the ones already specified may be deleted through
  • National experts proposal and
  • Study period