The overview of SC 27/WG 2 and lightweight cryptography

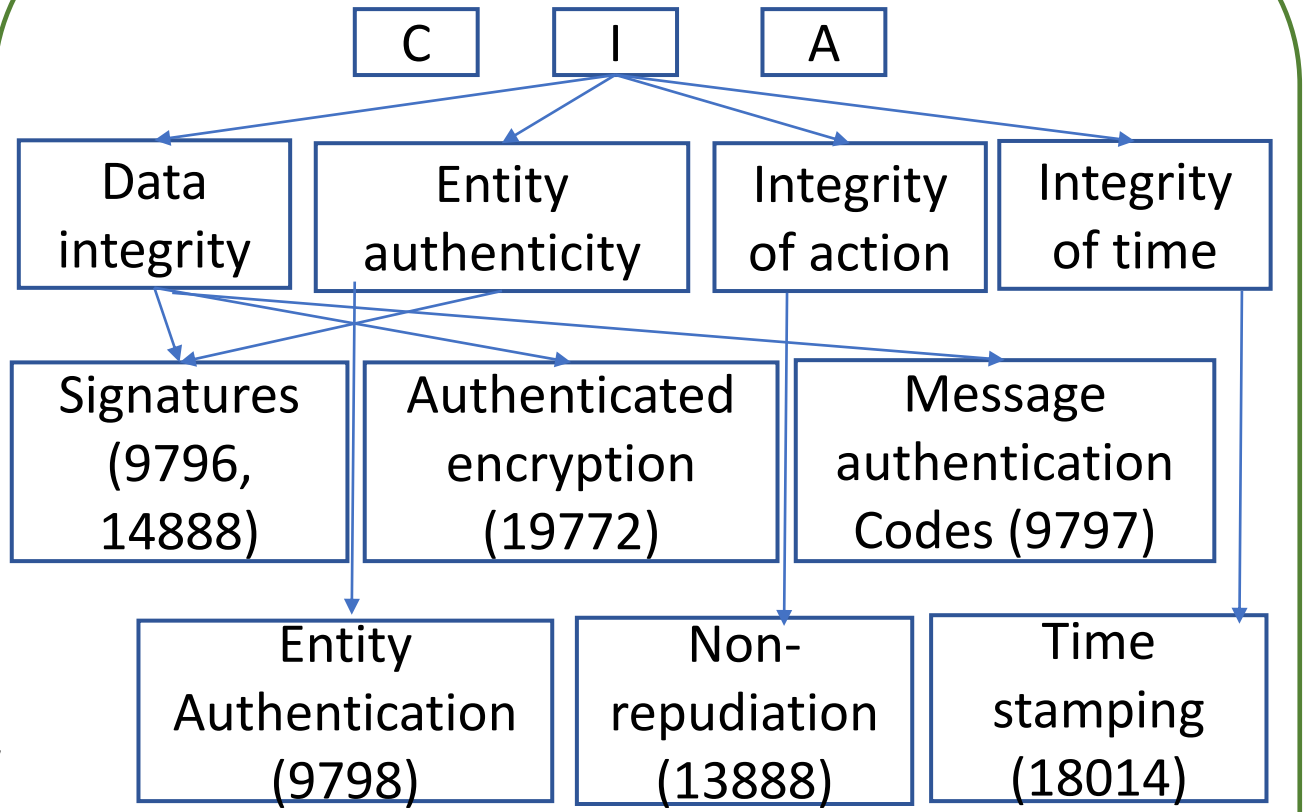
Hirotaka Yoshida
WG 2 Convenor Support Officer
AIST
Joint work with
Takeshi Chikazawa
SC 27/WG 2 Convenor
IPA

17th September 2020

Table of contents

Introduction to SC27 WG2

- SC27 WG2 Mission:
  Cryptography and Security Mechanisms
  - Information security systems provide a fundamental framework and methodology.
  - Cryptography provides technical means to meet C (confidentiality), I(integrity), and A (availability).
- The Terms of Reference:
  - *Identify the need and requirements for these techniques and mechanisms in IT systems and applications; and*
  - *Develop terminology, general models and standards for these techniques and mechanisms for use in security services.*



SC27/WG2 standards maybe classified this way[1]
(There is no single way to classify the project).

[1] Takeshi Chikazawa, Toshio Tatsuta, and Kenji Naemura, Cryptographic Standards: Recent Results and Future Perspectives of SC 27/WG 2, SC 27 Platinum Book.

Management and Collaboration w.r.t SC27 WG2

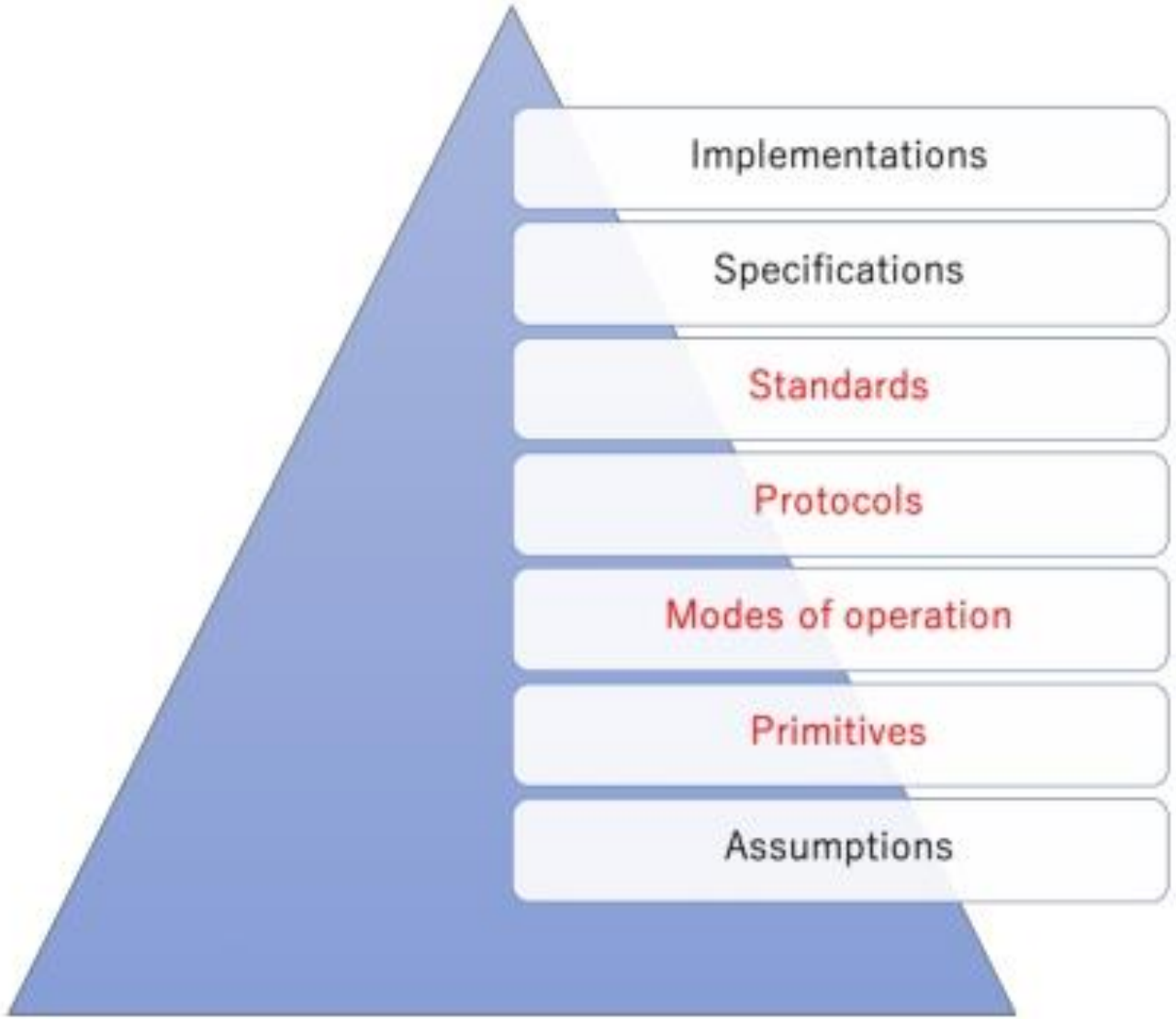
- Convenorship
  1st: Luis Guillou
  2nd: Marijke de Soete
  3rd: Kenji Naemura
  4th: Takeshi Chikazawa (Convenor) and Toshio Tatsuta (Vice-convenor)
  5th: Takeshi Chikazawa (Convenor) and Hirotaka Yoshida (Convenor support)
- Collaboration with Partners
  1) Liaison reports/statements within ISO/IEC JTC 1
    - SC 31/WG 4
    - TC 68/SC 2
    - TC 307

  2) Others
    - ITU-T SG17, Mastercard, ETSI TC Cyber, GlobalPlatform, CSA, IIC, STRATUS, IEEE CS, …
    - EU H2020 projects (WITDOM, PQCRYPTO, SAFEcrypto, CREDENTIAL, PRISMACLOUD), …

Consideration and discussion points in WG 2

- Mathematics
  - Reduce the problem rather than solve the one
- Recent results from cryptographic community (IACR)
  - Security analysis
  - Performance analysis
- Guidance for users
  - Numerical examples

Crypto Stack



Numerical Examples

- Why?
  - Implantation of crypto is difficult.
  - Test if the implemented cipher is the intended one.
- Where?
  - Annex
- What?
  - Input and output are specified.

I/O	Values
Input	6BC1BEE22E409F96E93D7E117393172A
Output	FEC2D0E565C4EE8CE18279DC1F5394E8

WG 2 published standards

9798: Entity authentication
11770: Key management
13888: Non-repudiation

11770-5
Group key management

11770-3 (3rd ed. (+Amd 1))
Mechanisms using asymmetric techniques

11770-2 (2nd ed.)
Mechanisms using symmetric techniques

11770-4 (2nd ed.)
Mechanisms based on weak secrets

9798-2 (3rd ed.)
Mechanisms using symmetric encipherment algorithms

11770-1 (2nd ed.)Framework

9798-1 (3rd ed.)General

9798-6 (2nd ed.) Mechanisms using manual data transfer

11770-6
Key derivation

9798-4 (2nd ed.)
Mechanisms using cryptographic check function

9798-5 (3rd ed.)
Mechanisms using zero knowledge techniques

9798-3 (2nd ed. (+Amd1))
Mechanisms using digital signature techniques

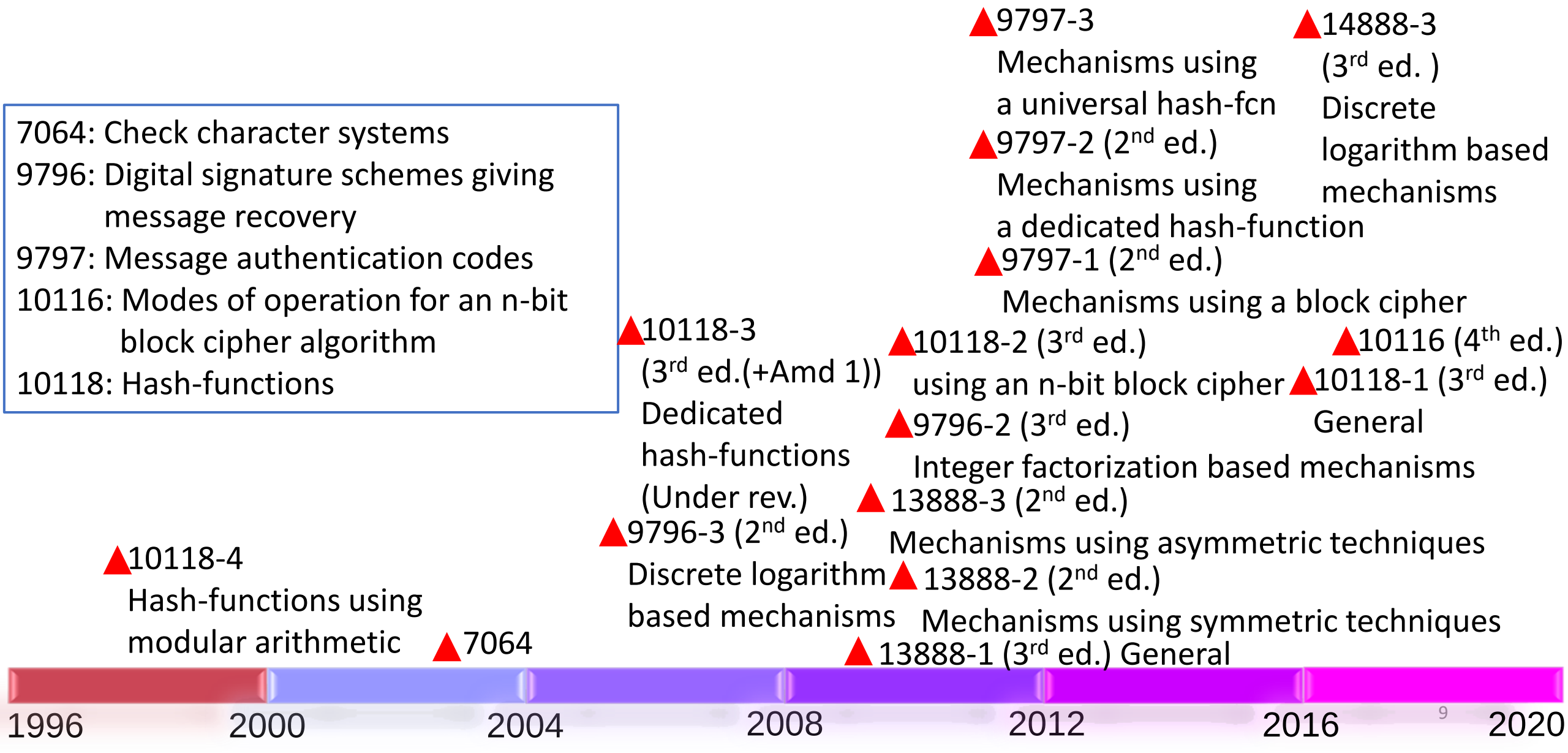
13888-3 (2nd ed.)
Mechanisms using asymmetric techniques

13888-2 (2nd ed.)
Mechanisms using symmetric techniques

13888-1 (3rd ed.) General

WG 2 published standards

7064: Check character systems
9796: Digital signature schemes giving message recovery
9797: Message authentication codes
10116: Modes of operation for an n-bit block cipher algorithm
10118: Hash-functions



WG 2 published standards

14888: Digital signatures with appendix
15946: Cryptographic techniques based on elliptic curves
18014: Time-stamping services
18031: Random bit generation
18032: Prime number generation
18033: Encryption algorithms
19592: Secret sharing
19772: Authenticated encryption
29150: Signcryption

18032

14888-1 (2nd ed.)
General

14888-2 (2nd ed.)
Integer factorization based mechanisms

19772

29150

18031 (2nd ed.)

18014-3 (2nd ed.)
Mechanisms producing linked tokens

18014-2 (2nd ed.)
Mechanisms producing independent tokens

18014-1 (2nd ed.)
Framework

19592-2
Fundamental mechanisms

19592-1
General

15946-1 (3rd ed.)
General

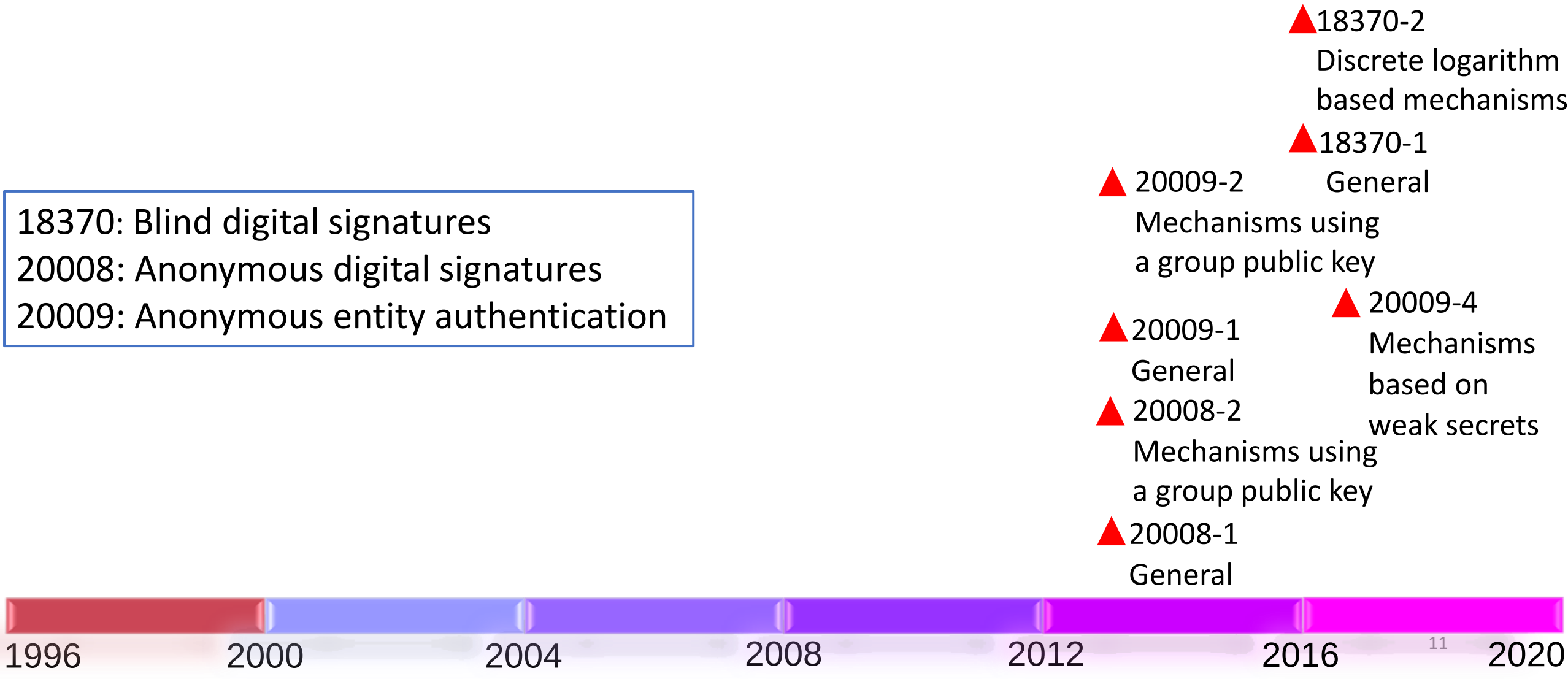
15946-5 (2nd ed.)
Elliptic curve generation

18014-4
Traceability of time sources

1996 2000 2004 2008 2012 2016 2020

WG 2 published standards

18370: Blind digital signatures
20008: Anonymous digital signatures
20009: Anonymous entity authentication



Global change affecting the scope of WG2

- Internet
  - Made available to commercial apps, causing an explosion of the World-Wide-Web services.
- ICT devices
  - Financial and other applications of smart cards, mobile phones were expanding.
- Progress in cryptanalysis
  - Academic research of cryptanalysis

- Advanced Encryption Standard (AES)
  - Open procedure, replace the Data Encryption Standards (DES)
- Guidelines for Cryptography Policy in 1997
  - Organization for Economic Co-operation and Development (OECD)
  - Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.

Global change affecting the scope of WG2

- Encryption algorithm was out of scope in 1990
  - Cryptography was considered to belong to military area
- ISO/IEC 9979 (procedures for the registration of cryptographic algorithm)
  - The Register contained 24 algorithms in 2001.
- In 2001, the project 18033 (Encryption algorithms) was approved by JTC 1.

ISO/IEC 18033 Encryption algorithms	Status
Part 1: General	2005 Under revision
Part 2: Asymmetric ciphers	2006 (+Amd 1)
Part 3: Block ciphers	2nd ed. 2010
Part 4: Stream ciphers	2nd ed. 2011
Part 5: Identity-based ciphers	2015
Part 6: Homomorphic encryption	2019
Part 7: Tweakable block ciphers	Under development

ISO/IEC 18033-1: encryption algorithms

SC27/WG2 developed annexes in the 2nd edition of ISO/IEC 18033-1:

- Criteria for submission of ciphers for possible inclusion in this international standard
- Criteria for the deletion of ciphers from this international standard
- Attacks on encryption algorithms

These annexes improves the quality of encryption algorithms specified in the standards.

On-going WG 2 projects

Overview of WG 2 on-going projects

Time (Stage)

WD	CD CDAM	DIS, FDIS DAM, FDAM
11770-8	10118-1 Amd1	9797-2
14888-4	11770-3 Amd2	10116 Amd1
18031	15946-5	11770-4 Amd2, 11770-5, 11770-7
18033-7	18014-2	18032
29192-8	18033-1	13888-1, 13888-3
	20009-3	18033-3 Amd1, 18033-5 Amd1
	23264-2	19772
		20008-2 Amd1
		23264-1

Explained
In the next slides

Amd: Amendment

Modes of operations for an n-bit block cipher (10116)

- 10116/DAM 1
- 4th edition

#	Abbreviation	Mechanism
a	ECB	Electronic Codebook
b	CBC	Cipher Block Chaining
c	CFB	Cipher Feedback
d	OFB	Output Feedback
e	CTR	Counter
f	CTR-ACPKM	Counter Advanced Cryptographic Prolongation of Key Material

Counter Advanced Cryptographic Prolongation of Key Material (CTR-ACPKM) mode of operation

- Property
  - Prevents the same plaintext corresponding to the same ciphertext
    - the use of different SV values
  - Use the encryption operation of the cipher for decryption
  - does not depend on the plaintext to generate the keystream

- Reference

AKHMETZYANOVA L. R., ALEKSEEV E. K., SMYSHLYAEV S. V. "Security bound for CTR-ACPKM internally re-keyed encryption mode." Cryptology ePrint Archive Report 2018/950, 2018, <https://eprint.iacr.org/2018/950.pdf>

Message authentication codes (MACs) (9797)

- Part 2: Mechanisms using a dedicated hash-function
- DIS 9797-2
- Four MAC algorithms (the tag length in bit is at least 32.)
  HMAC, KMAC

#	Dedicated Hash	#	Dedicated Hash
1	RIPEMD-160	10	SHA-512/256
2	RIPEMD-128	11	STREEBOG 512
3	SHA-1	12	STREEBOG 256
4	SHA-256	13	SHA3-224
5	SHA-512	14	SHA3-256
6	SHA-384	15	SHA3-384
7	Whirlpool	16	SHA3-512
8	SHA-224	17	SM3
9	SHA-512/224		

MAC Algorithm 4
Keccak Message Authentication Code (KMAC) algorithm

- Properties

- The SHA-3 family (Hash 13,14,15,16) shall be used.

- Two variants, KMAC128 and KMAC256.
  Both can support any security strength up to 256 bits of security

- Reference
  J. Kelsey, J. Chang, R. Perlner, R. "SHA-3 derived functions: cSHAKE, KMAC, TupleHash And ParallelHash" NIST Special Publication 800-185. December 2016. http://csrc.nist.gov

An informative annex in 9797-2
A Security Analysis of the MAC Algorithms

- An annex discusses the security level.
- Its goal is to assist the user.

#	Attack strategies
1	forgery attack
2	key recovery attack
3	guessing the MAC
4	brute force key recovery
5	birthday forgery
6	shortcut key recovery

B. Preneel, P.C. van Oorschot, "MDx-MAC and building fast MACs from hash functions," Advances in Cryptology, Proceedings Crypto'95, LNCS 963, D. Coppersmith, Ed., Springer-Verlag, 1995, pp. 1–14.

Key management (11770)

- Amendment 2 to Part 3 (Mechanisms using asymmetric techniques)
- 11770-3/DAM2
- Key agreement mechanism 15
  - Establishes a shared secret key in two passes between two entities
- Describes example of bilinear pairing based key establishment mechanisms
- Bibliography

- GM/T 0044.4-2016, *SM9 Identity-Based Cryptographic Algorithms using Bilinear Pairings - Part 3: Key Exchange Protocol*.

- CHENG Z. *Security analysis of SM9 key agreement and encryption*. In: Information Security and Cryptology - Inscrypt 2018. Springer, Vol. 11449, 2019, pp. 3-25.

- GALBRAITH S. D., PATERSON K. G., SMART N. *Pairings for cryptographers*. Journal of Discrete Applied Mathematics. Vol. 156. Issue. 16, pp. 3113-3121, 2008.

Key management (11770)

- Amendment 2 to Part 4 (Mechanisms based on weak secrets)
- 11770-4/DAM2
- Key establishment mechanisms based on weak secrets
  - secrets will be chosen from a small set of possibilities.
  - establish secret keys based on a weak secret derived from a memorized password
- Prevents offline brute-force attacks associated with the weak secret
- Annex discusses the selection of parameters

Category	Mechanism	Abbreviation	Bib.
Password-authenticated key agreement	Balanced Key Agreement Mechanism 1	BKAM1	[6] [8] [17]
	Balanced Key Agreement Mechanism 2	BKAM2	[1] [5]
	Augmented Key Agreement Mechanism 1	AKAM1	[8] [27]
	Augmented Key Agreement Mechanism 2	AKAM2	[19] [20]
	Augmented Key Agreement Mechanism 3	AKAM3	[23][24]
Password-authenticated key retrieval	Key Retrieval Mechanism 1	KRM1	[4] [8]

Bibliography for 11770-4/DAM2

[1] M. Abdalla, F. Benhamouda, P. MacKenzie. Security of the J-PAKE password-authenticated key exchange protocol. IEEE Symposium on Security and Privacy 2015, pp. 571-587, IEEE Computer Society, 2015

[4] W. Ford and B. Kaliski. Server-assisted generation of a strong secret from a password. In *Proceedings of the* IEEE 9th *International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 176-180, IEEE, June 2000

[5] F. Hao, P. Ryan. Password authenticated key exchange by juggling. Proceedings of the 16th Workshop on Security Protocols (SPW), Cambridge, UK, Springer LNCS 6615, pp. 159-171, 2008.

[6] F. Hao, S.F. Shahandashti. The SPEKE protocol revisited. Proceedings of the 1st International Conference on Research in Security Standardisation (SSR), 2014. Cryptology ePrint Archive.

[8] IEEE P1363.2/D21:2005-07-17, *Standard specifications for password-based public key cryptographic techniques*

[17] D. Jablon. Strong password-only authenticated key exchange. Computer Communication Review, ACM SIGCOMM, 26(5): 5-26, October 1996

[19] T. Kwon. Ultimate solution to authentication via memorable password. Submission to the IEEE P1363 study group for future PKC standards, May 2000

[20] T. Kwon. Addendum to summary of AMP. Submission to the IEEE P1363 study group for future PKC standards, Nov. 2003

[23] S. Shin and K. Kobara. Efficient augmented password-only authentication and key exchange for IKEv2. RFC 6628, ISSN 2070-1721, IETF, June 2012

[24] S. Shin, K. Kobara and H. Imai. Security proof of AugPAKE. Cryptology ePrint Archive: Report 2010/334.

[27] T. Wu. SRP-6: improvements and refinements to the secure remote password protocol. Submission to IEEE P1363 Working Group, October 29, 2002

Key management (11770)

- Part 5: Group key management
- DIS 11770-5
- Enables a secret key to be shared by all members of a defined group with the assistance of a trusted third party (Key Distribution Centre).
- Key chains consider group forward secrecy and group backward secrecy

  - the number of keys shall be carefully chosen

Symmetric key-based key establishment mechanisms

Mechanism	Goal
Mechanism 1	Key establishment with individual rekeying
Mechanism 2	Key establishment with batch rekeying

Normative references and Bibliography for DIS 11770-5

Normative references

[A] ISO/IEC 19772, *Information technology — Security techniques — Authenticated encryption*

[B] ISO/IEC 11770-6, *Information technology — Security techniques — Key management — Part 6: Key derivation*

Bibliography

[1] ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

[2] ISO/IEC 9797-2, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

[3] ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

[4] ISO/IEC 11770-1, *Information technology — Security techniques — Key management — Part 1: Framework*

[5] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[6] ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

[7] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

Key management (11770)

- Part 7: Cross-domain password-based authenticated key exchange
- DIS 11770-7
- Enables two communicating entities establish a shared session key using just the login PWs that they share with their respective servers.
- The servers, part of a standard PKI, act as ephemeral CAs certifying key materials that the users can use to agree on as a session key.

Cross-domain password-based authenticated key exchange

Mechanism	Overview (sub-protocols on which mechanisms are built)
Mechanism 1	two-party password-based authenticated key exchange (2PAKE) protocol and a *signature-based* two-party asymmetric-key authenticated key exchange (2AAKE) protocol
Mechanism 2	a two-party password-based authenticated key exchange (2PAKE) protocol and a two-party asymmetric-key authenticated key exchange (2AAKE) protocol
Mechanism 3	a two-party non-interactive key exchange protocol (2NIKE), a two-party password-based authenticated key exchange (2PAKE) protocol and a two-party symmetric-key authenticated key exchange (2SAKE) protocol

Normative references and Bibliography for DIS 11770-7

Normative references

[A] ISO/IEC 11770-2:2018, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[B] ISO/IEC 11770-3:2015, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[C] ISO/IEC 11770-4:2017, *Information technology — Security techniques — Key management — Part 4: Mechanisms based on weak secrets*

Bibliography

[1] ISO/IEC 8825-1:2015, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules* (*BER*), *Canonical Encoding Rules* (*CER*) *and Distinguished Encoding Rules* (*DER*)

[2] ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

[3] ISO/IEC 9797-2:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

[4] ISO/IEC 10118-3:2018, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

[5] ISO/IEC 10181-1, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview — Part 1*

[6] ISO/IEC 11770-1:2010, *Information technology — Security techniques — Key management — Part 1: Framework*

[7] ISO/IEC 11770-6:2016, *Information technology — Security techniques — Key management — Part 6: Key derivation*

[8] ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

[9] ISO/IEC 18033-3:2010, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

[10] ISO/IEC 18033-4:2011, *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*

[11] M. Abdalla, P. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In *Proceedings of the PKC Conference*, pp. 65-84, 2005

[12] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Proceedings of EUROCRYPT*, pp. 139-155, 2000

[13] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *Proceedings of EUROCRYPT*, pp. 453-474, 2001

[14] L. Chen, H.W. Lim, and G. Yang. Cross-domain password-based authenticated key exchange revisited. ACM Trans. Inf. Syst. Secur. 16(4): 15:1-15:32, 2014

[15] D.P. Jablon. Strong password-only authenticated key exchange. *ACM SIGCOMM Comput. Commun. Rev.* 26(5):5-26, 1996

Prime number generation (18032)

- FDIS 18032
- Methods to generate and test prime numbers
  - Enables to test whether a given number is prime
  - Enables to generate prime numbers.
    Both probabilistic and deterministic methods are presented.

Prime number generation

Goal	Method
Primality test	Probabilistic Miller-Rabin primality test on randomly chosen candidates
	Deterministic Elliptic curve primality proving algorithm
	Deterministic Primality certificate based on Shawe-Taylor's algorithm
Prime number generation	Probabilistic Miller-Rabin primality test on randomly chosen candidates
	Deterministic Shawe-Taylor method which yield integers known to be prime

Normative references and Bibliography for FDIS 18032

Normative references

[A] ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

Bibliography

[1] ANSI X9.80-2010, *Prime number generation, primality testing, and primality certificates.*
[2] A.O.L. Atkin, F. Morain. *Elliptic curves and primality proving.* Mathematics of Computation 61, 1993, pp. 29-68
[3] Robert Baillie, Samuel S. Wagstaff, Jr. *Lucas Psuedoprimes.* Mathematics of Computation 35, 1980, pp 1391-1417.
[4] Ian F. Blake, Gadiel Seroussie, Nigel P. Smart. *Elliptic curves in cryptography*, third printing, Cambridge University Press, 2000
[5] Jørgen Brandt, Ivan Damgård. *On generation of probable primes by incremental search.* Proceedings CRYPTO 92, LNCS 740, Springer, 1993, pp. 358-370
[6] John Brillhart, D. H. Lehmer, J. L. Selfridge. *New Primality Criteria and Factorizations of* $2^m \pm 1$. Mathematics of Computation 29(130) 1975, pp. 620-647
[7] Don Coppersmith. *Finding a Small Root of a Bivariate Integer Equation; Factoring with high bits known*. Advances in Cryptography – EUROCRYPT 1996, pp 178-189.
[8] ISO/IEC 15496-1, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General
[9] Ivan Damgård, Peter Landrock, Carl Pomerance. *Average case error estimates for the strong probable prime test.* Mathematics of Computations 61(203), 1993, pp. 177-194
[10] NIST, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-4, July 2013.
[11] N.D. Elkies. *Elliptic and modular curves over finite fields and related computational issues.* Computational Perspectives on Number Theory, volume 7 of AMS/IP Stud. [] Adv. Math. Amer. Soc., Providence, RI, 1998.
[12] H. W. Lenstra. Divisors in Residue Classes. *Mathematics of Computation 42 (165)*, 1984, pp. 331-340.
[13] Daniel Marcus. *Number Fields*, third printing, Springer-Verlag, 1995.
[14] Matus Nemec, Marek Sys, Petr Svenda, Dusan Klinec, Vashek Matyas. *The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*. P15roceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp 1631-1648.
[15] Carl Pomerance. *Are there Counter-examples to the Baillie – PSW Primality test?* 1984
[16] Rene Schoof. *Counting points on elliptic curves over finite fields.* J. Theory. Nombres Bourdeaux, 7:219-254, 1995.
[17] Douglas R. Stinson. *Cryptography, Theory and Practice*, 2nd edition, Chapman & Hall/CRC, 2002
[18] J. Shawe-Taylor. *Generating strong primes.* Electronics Letters (22) 16, 1986, pp. 875-877
[19] L. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, 2003, 2nd ed. 2008.

Topics for consideration

Topics for consideration at the September 2020 meeting in SC27/WG2

#	Topics	#	Topics
1	ISO/IEC 20008-3: Mechanisms using multiple public keys	5	Security of MQ_DRBG in ISO/IEC 18031
2	Inclusion of format preserving encryption in ISO/IEC standards	6	Possible reduction of the number of rounds for two versions of Skinny in ISO/IEC 18033-7
3	Revision of ISO/IEC 9797-1	7	Suitability of standardization of fully homomorphic encryption schemes in ISO/IEC standards
4	Modes of operation for tweakable block ciphers	8	Inclusion of Pointcheval-Sanders Anonymous Signature Schemes in ISO/IEC 20008-2

Future Perspective

- Future focus of WG2 activities will depend on market needs and technological seeds.
- Review of existing standards
- To avoid the mechanisms become vulnerable to new attacks.

Conclusion 1 (for overview of SC 27/WG 2)

SC 27/WG 2 has developed standards through generations.

- 1st generation in 1990s
  - Entity authentication, digital signatures, and …, under a restriction of standardization of encryption algorithms
- 2nd generation
  - Characterised by the ISO/IEC 18033 development and others in advanced cryptography
  - Used in including JTC 1/SC 17, ISO/TC 68/SC 2, ITU-T and IETF
- 3rd generation
  - produce cryptographic standards of mechanisms and algorithms to meet diversified business needs for cyber security

SC 27/WG 2 continues to work together with other SDOs that enable more specific, application oriented techniques.

Lightweight Cryptography

Cyber-physical systems (CPS)

- Cyber-physical systems (CPS) connect information with physical objects: auto-motives, factory automation, medical devises
- The security in these systems could be safety-critical, which could impose an interesting challenge for cryptographers one engineers.
- In CPS security, problem is bridging the gap between the publicly-available scientific results and the real-world deployment
- One of the key solutions is standardisation bodies's activities.

Figure: Cyber Physical

PKES Hacking

- Tillich, S. and W´ojcik, M.: Security Analysis of an Open Car Immobilizer Protocol Stack, Presented at the industry track of the 10th International Conference on Applied Cryptography and Network Security (ACNS'12), (2012)..

Figure: A Car and Key Fob

TPMS Hacking

- Rouf, I., Miller, R. D., Mustafa, H. A., Taylor, T., Oh, S.,Xu, W., Gruteser, M., Trappe, W. and Seskar, I.: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study,19th USENIX Security Symposium, 2010, Proceedings, USENIX Association, pp. 323–338 (2010).

Figure: A Car and TPMS sensor

- Security should be needed on 8-bit micro controllers for TPMS sensors.

Lightweight cryptography

- Growing demand for applications using smart devices: low-end micro-controllers and RFID tags
- Security problems such as confidentiality, data authentication and privacy
- Challenge: design cryptographic primitives or protocols that meet the system requirements
- To meet these requirements, lightweight cryptographic algorithms can be implemented under restricted resources, such as low-cost, low-energy, or low-power environments

ISO/IEC 29192 series: Lightweight cryptography

Title	Status
Part 1: General	2012
Part 2: Block ciphers	2012
Part 3: Stream ciphers	2012
Part 4: Mechanisms using asymmetric techniques	2013
Part 5: Hash-functions	2016
Part 6: Message authentication codes (MACs)	2019
Part 7: Broadcast authentication protocols	2019
Part 8: Authenticated Encryption	Under Development

Explained
In the next slides

ISO/IEC 29192-5: 2016 mechanisms

- Lesamnta-LW
  - 256-bit hash function using a block cipher employing AES components
  - low RAM-used (50 Byte) implementation on 8-bit microcontrollers is possible
  - presented in ICISC 2010 conference and IEICE journal
- Spongent
  - Sponge function-based hash function
  - hash length supports 80, 128, 160, 224, 256
  - Presented in CHES 2011 conference
  - Low-gate count (738GE) hardware implementation is possible
- Photon
  - Sponge function-based hash function
  - hash length supports 80, 128, 160, 224, 256
  - Presented in conference(CRYPTO 2011)
  - Low-gate count (865GE) hardware implementation is possible

Importance of hash functions

- Used in a wide variety of cryptographic applications:
  - Digital Signature Schemes
  - Key Derivation Function
  - Deterministic Random Bit Generators
  - Message Authentication
- Achieve security in these cryptographic applications
- Standardized in ISO/IEC JTC 1 and NIST
- Needed in any cryptographic software library:
  - Randomness extraction
  - Public key encryption

Hash function crisis and NIST SHA-3 Competition (2007-2012)

- The crisis
  - 2005: cryptanalysis of hash functions: MD5 and SHA-1.
  - 2006, Federal agencies should stop using SHA-1 for certain applications must use the SHA-2 family for them after 2010.
  - NIST recommends the transition from SHA-1 to SHA-2
  - SHA-2 may be vulnerable to similar techniques
  - Similarities in the design principles between SHA-2 and SHA-1
  - 2007: NIST started the SHA-3 competition
- The Breakthrough: Wang et al.'s Differential collision search
  - Attack complexity optimization together with differential cryptanalysis
  - Biham and Shamir, Differential Cryptanalysis of the Data Encryption Standard, 1993.
- The competition
  - 51 candidates to advance to the first round in December 2008
  - 14 to advance to the second round in July 2009
  - 5 finalists - BLAKE, Grøstl, JH, Keccak, and Skein
  - NIST selected Keccak as the winning algorithm on October 3, 2012

What is a hash function?

- Maps input strings to short output strings of fixed length
- n-bit hash function returns an n-bit hash value
- The description of hash function must be publicly known
- Does not require any secret information for its operation.

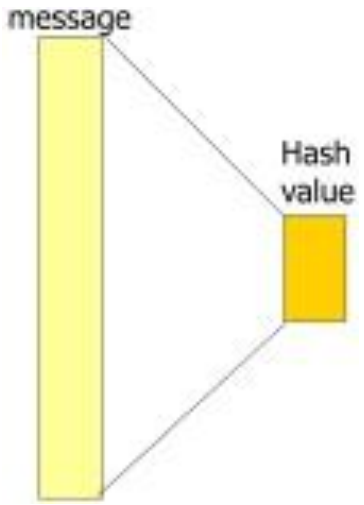


Figure: Hash function

Hash Functions' properties

Hash functions' properties expected in cryptographic applications

- Security property:
  - Preimage resistance
  - Second preimage resistance
  - Collision resistance
  - Indifferentiability from a random oracle
- Performance:
  - Efficiency
  - Hardware/Software implementation flexibility

The motivation and design goals of Lesamnta-LW

- Compact and fast, optimized for lightweight applications in a wider variety of environments

- Our primary target CPUs are 8-bit

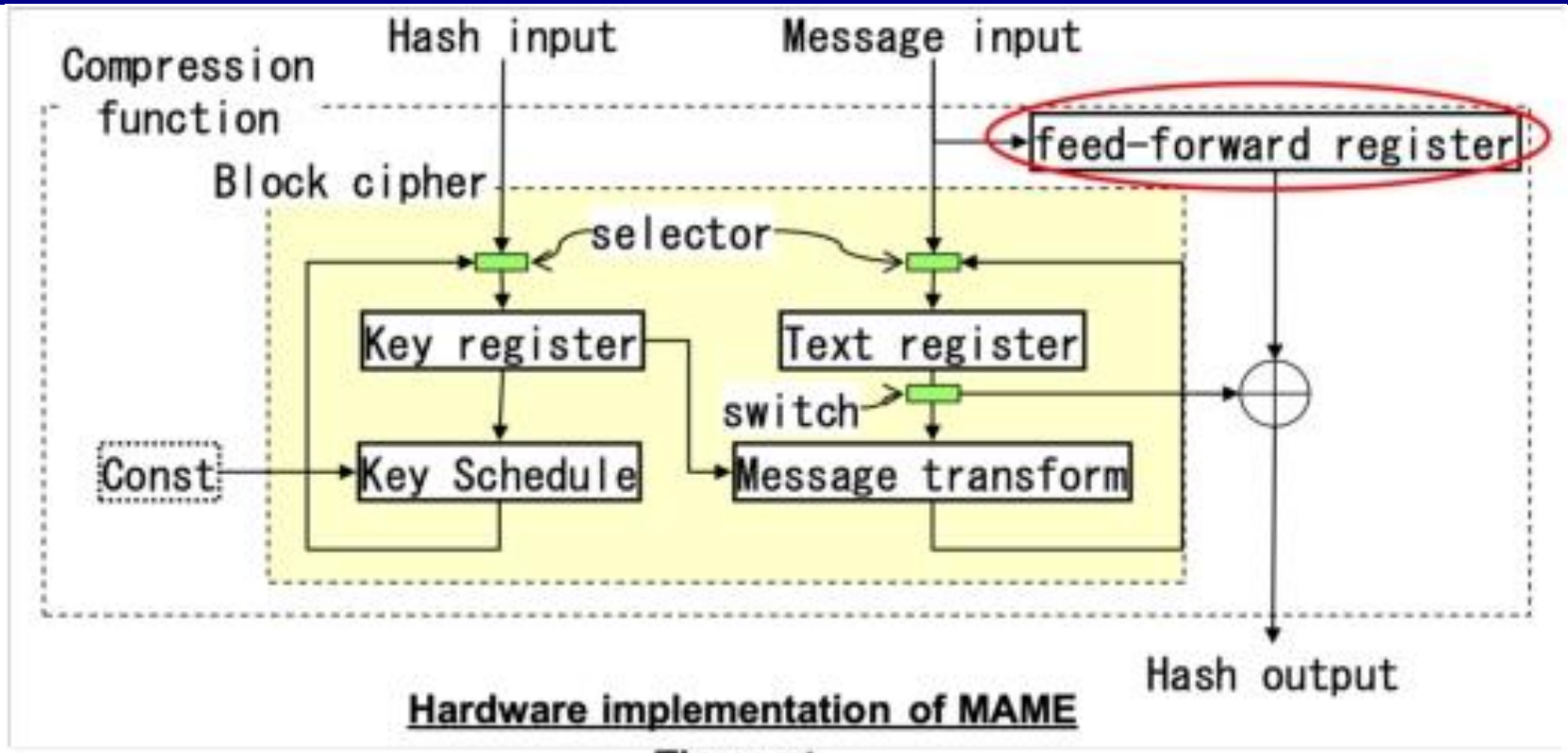
Low-cost 8-bit CPUs are popular

- Over 4 billion 8-bit controllers were sold in 2006

RAM (byte)	Microchip Technology	Freescale	National Semiconductors	NXP	Atmel	Renesas
- 255	PIC10 PIC12	RS08 HC08	COP8	80C51		
256 - 511	PIC16 PIC18	HC08 HCS08	COP8	80C51		
512 -	PIC16 PIC18	HC08 HCS08	COP8	80C51	megaAVR	H8

- 2^{120} security level achieved with a high security margin:
- Provide proofs reducing the security of Lesamnta-LW to that of the underlying block cipher performance

The Problem with a conventional lightweight hash



Hardware implementation of MAME

The cost

Circuit		GE
transform	Non-linear Layer	640
	Linear Layer	576
Total		**8200**

MAME (bean in Japanese):

- 256-bit hash function proposed by Yoshida *at al*. in CHES 2007
- Block cipher based hardware-oriented lightweight design

The overview of Lesamnta-LW

- LW1 mode can be proved to be collision resistant if the underlying cipher behaves as PRF
- LW1 mode does not have the feedforward of inputs, which contributes to a small memory

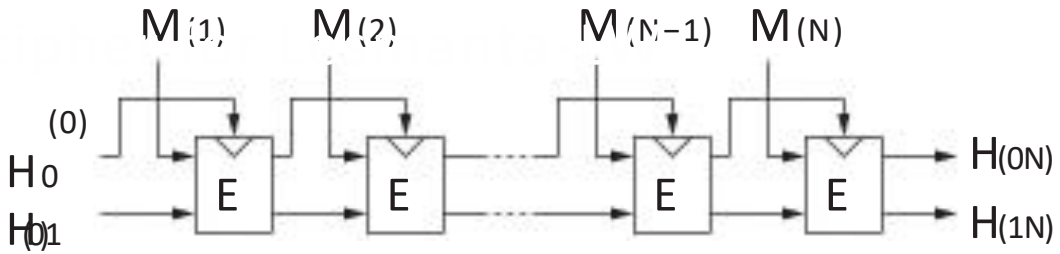
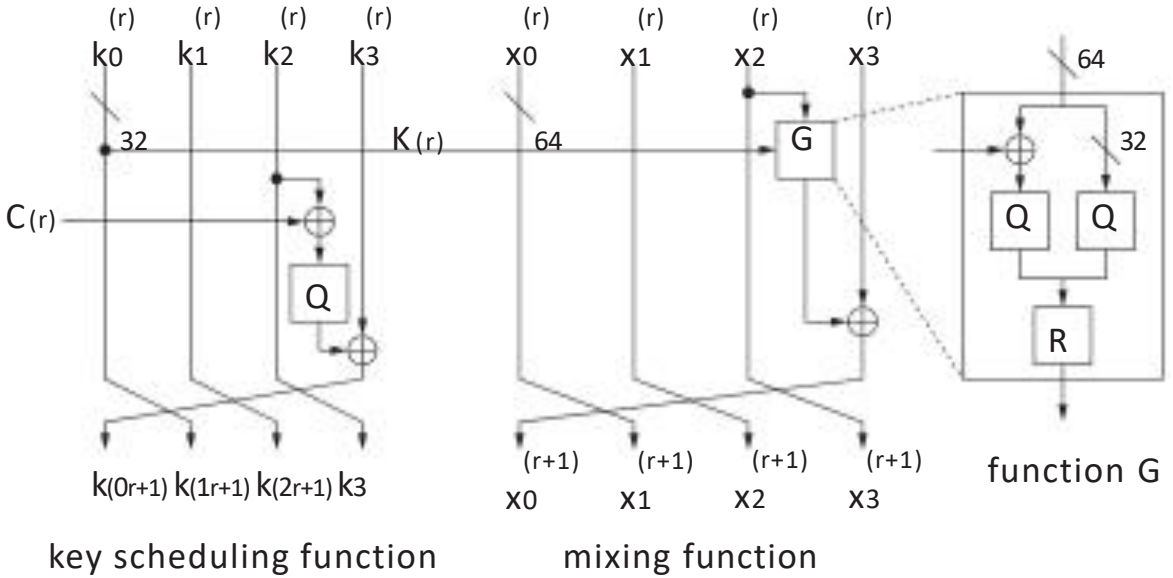


Figure: The structure of Lesamnta-LW

- The underlying block cipher for Lesmanta-LW is designed to be compact in software/hardware, and to offer a reasonable speed on high-end/low-end CPUs



Security analysis

- The best way to verify this pseudo-randomness, is to apply block cipher analysis techniques to the block cipher E, and to check whether this reveals any weakness or non-random behavior
- We evaluate the security of Lesamnta-LW and the underlying block cipher against all relevant attacks
  - Differential Attacks
  - Linear Attacks
  - Higher Order Differential
  - Interpolation Attack
  - Impossible Differential Attack
  - Related-key Attacks
  - Collision Attacks Using Message Modification
  - Attacks on the Lesamnta Compression Function Using Self-Duality

Our software implementation estimates on an 8-bit CPU Renesas H8

- We have estimated speed and ROM/RAM size of Lesamnta-LW and SHA-256 on an 8-bit CPU Renesas H8

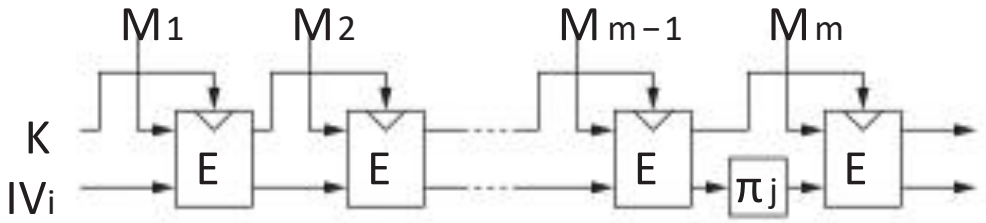
  https://www.overleaf.com/project/5bd94b7fb82dc105473ae00f

Algorithm	Bulk Speed (cycles/ byte)	Short Message (cycles/ message)	ROM (CONST. +CODE) (byte)	RAM (byte)
SHA-256	1033.3 1046.9 1281.1	66434 67308 82296	32 + 37034 288 + 5046 288 + 948	330 330 330
Lesamnta-LW	1650.9 1736.5 2055.0	52828 55568 65760	512 + 20006 768 + 1346 768 + 370	50 50 54

- Requires only 50 byte of RAM while achieving 3478 cycles/byte for short (128-bit) messages on an 8-bit CPU:
  - 84% smaller than SHA-256 while running 21% faster

Lesamnta-LW to TPMS security

- Convert Lesamnta-LW to multiple independent (PRFs) in TPMS.



- Generate five PRFs this way and then use one PRF for MAC-generation and four for key derivation.
- Y. Watanabe, H. Yamamoto, H. Yoshida ”A Study on the Applicability of the Lesamnta-LW Lightweight Hash Function to TPMS” [Escar Asia 2018]

Cyber physical systems

- Real time requirement
- AES-CTR can be problematic for programmable logic controller (PLC)

Crypto eats too much resources on PLC

Figure: A Factory

Target IoT System: Automotives

V2X (Vehicle-to-X) system

- Over-the-air programming (OTA) gets a lot of attention.
- ITU-T SG17 is developing a protocol for remote software update.
- Hash, MAC and PRF play core roles in this protocol.

In-vehicle system

- Short-message performance important:
  - Packets are as short as 8 bytes (CAN) to 64 bytes (CAN-FD).
  - Realtime req. is severe: 1–100ms periodic tasks are processed.
- 50–100 ECUs are employed in a car:
  - Limited cost can be paid for each ECU.
  - Cost comes from circuit size in HW and RAM/ROM size in SW.

ISO/IEC 29192-6: 2019 lightweight MAC standard

- 3 mechanisms: Chaskey-12, LightMAC mode, Tsudik mode
- Tsudik mode for Lesamnta-LW, faster than HMAC-SHA-256
- Chaskey-12, Implementation results

  Achieve the speed of 7.0 cycles/byte on ARM Cortex-M4

  - Comparing to AES-128-CMAC, Chaskey achieves 12time higher speed, program size is 1/20

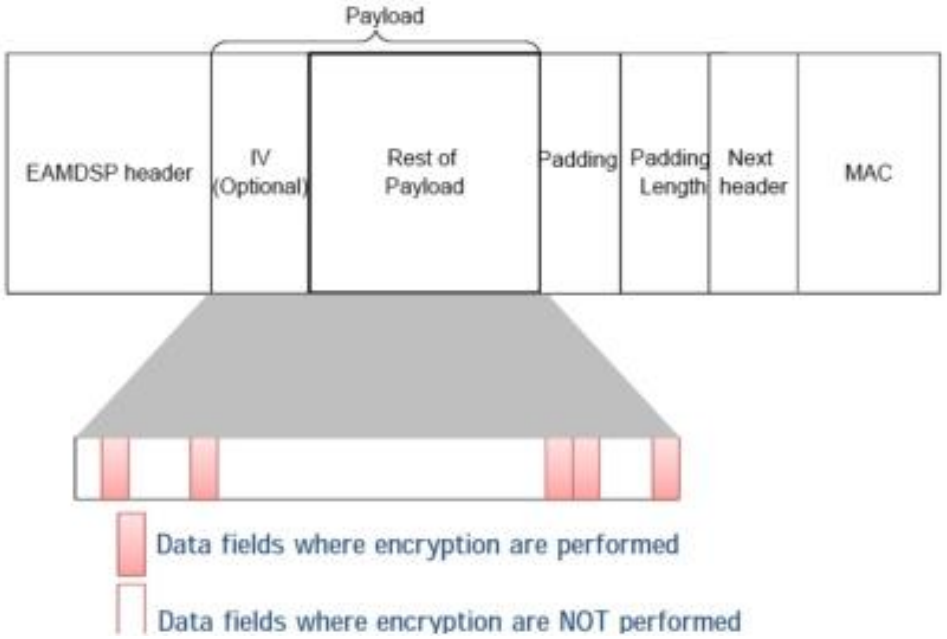
CPU	Algorithm	Data size (Byte)	Program size (Byte)	Speed (cycles/byte)
Cortex-M4	AES-128-CMAC	128	8,740	89.4
Cortex-M4	Chaskey-8	128	402	7.0

Overview of X.1362

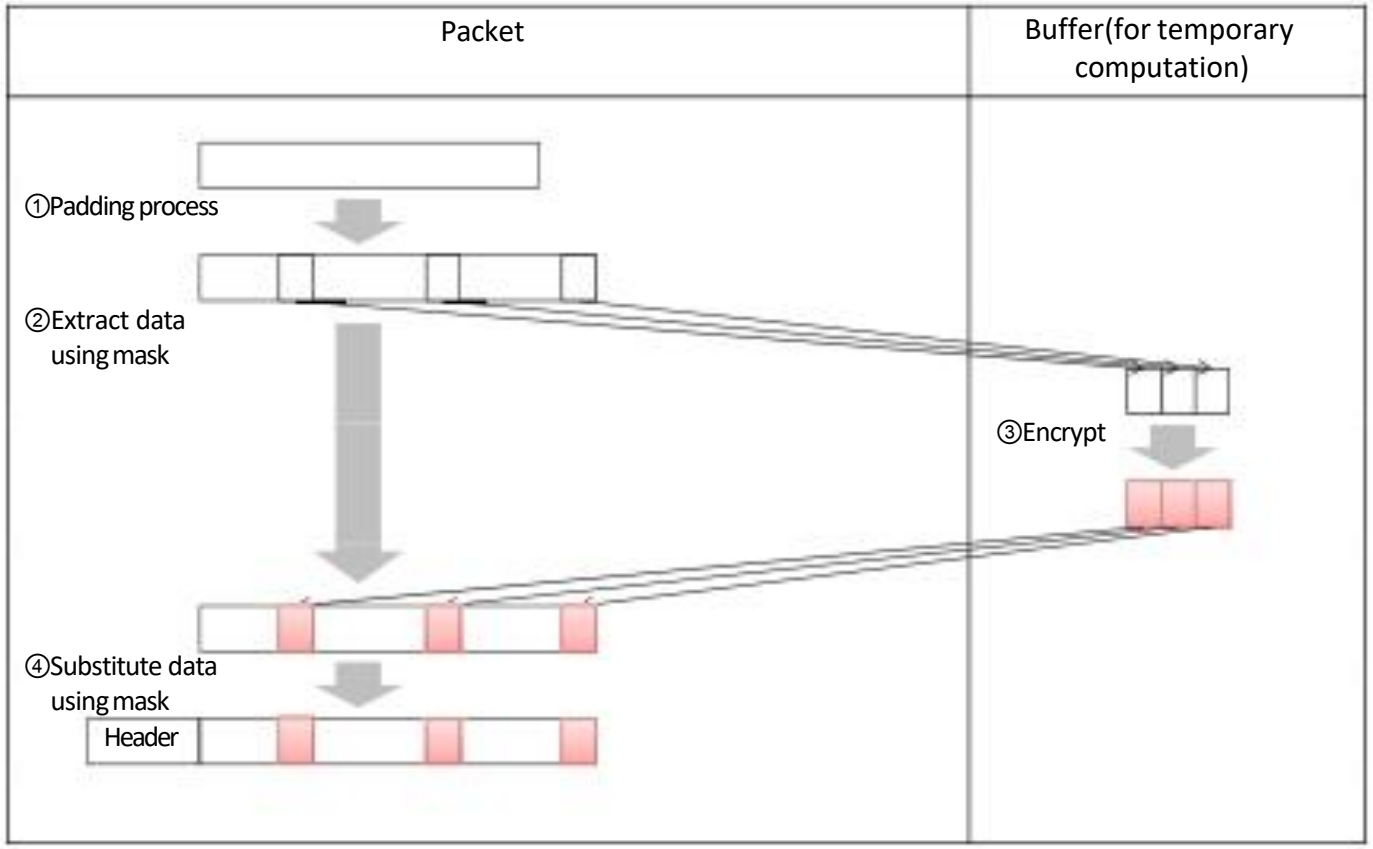
- Published in 19 June 2017 as 1st ITU-T IoT security std.
- ITU-T SG17: Standardization organization regarding telecommunication security
- Scope
  Reduce the overhead by encrypting the only data that are sensitive
- Main contents
  - Specification of how to communicate cryptographic application mechanism EAMD (encryption with associated mask data) communication flow, packet format
  - Specification of the abstract of EAMD (basic data flow, parameter set)
  - Specification of how to communicate using cryptographic primitives such as AES-GCM etc. and packet authentication is possible.
  - Guideline on how to use cryptographic parameter

The EAMD protocol

Reduce the overhead by encrypting the only data that are sensitive



Generate packet using the mask indicating sensitive data location



Packet sending flow in EAMD-used communication

NIST LWC workshop, Nov. 2019

1. Timeline
   - 1 year evaluation for 2nd round 32 candidates
   - 8 finalists to advance Round 3
   - Select winner(s) in 2021
2 Selection for 2nd round
   - Security and maturity are considered but performance was not considered.
   - Main issues with 1st round candidates include domain separation (message and tags).
   - NIST IR 8268: status report of 1st round: https://doi.org/10.6028/NIST.IR.8268
3 Discussion on the number of the winners
   - The winners could be multiple.
   - Categories could be considered in NIST.

   Categories may be based on performance.

Conclusion 2 (for Lightweight Cryptography)

- The problem is bridging the gap between the publicly-available results and the real-world deployment.
- Standardisation bodies, ISO/IEC SC27 WG2, NIST, ITU-T are active to solve this.
- The requirements-oriented view and the use of the lightweight Cryptography (LWC) could be the key solutions to them.

- LWC for size requirement
  - Lesamnta-LW requiring small RAM in ISO/IEC 29192-5:2016
  - Its applications to Automotive TPMS presented in Escar Asia 2018
- LWC real-time requirement
  - ITU-T X.1362 (2017) EAMD protocol
  - lightweight MAC project: ISO/IEC 29192-6:
  - Chaskey-12, software oriented, fast on ARM in ISO/IEC 29192-6:2019

Thank you very much for your attention.