Report on FY2001 Evaluation of Symmetric-Key Cryptographic Techniques

April 16, 2002

Toshinobu Kaneko

Chair, Symmetric-Key Cryptography Subcommittee

(Science University of Tokyo)

Symmetric-Key Cryptography Subcommittee

K.Araki (TIT)
T.Kaneko (SUT)
S.Kawamura (Toshiba)
M.Kanda (NTT)
T.Kohda (Kyushu U.)
K.Kobara (U. of Tokyo)
K.Sakurai (Kyusyu U.)
T.Shimoyama (Fujitsu)
K.Takaragi (Hitachi)
M.Tatebayashi (Matsushita)
Y.Tsunoo (NEC)
T.Tokita (Mitsubishi)
M.Morii (Tokushima U.)

13 members

Cryptographic Technologies

- Symmetric ciphers
  - 64-bit block cipher (key length ≧ 128 bits)
  - 128-bit block cipher (key length ≧128 bits)
  - stream cipher (IV ≧128 bits, State ≧128 bits)
- Hash Function

  160-bit or longer hash value
- PRNG

Activities

(1) General Evaluation

- submitted techniques and added ones by CRYPTREC

(a) Screening Evaluation

- examine trivial weakness

(b) Full Evaluation

- Inspect weaknesses in detail and performance

(c) Continual Evaluation

  - fully evaluated in 2000 & deserve further evaluation
- Additional Security/Performance evaluation

(2) Specific Evaluation

- request by another organization and the techniques added by CRYPTREC for more detailed evaluation in a specific use

(1-a.) General Evaluation (Newly Submitted Tech.)

- Stream Cipher
  - C4-1 (Focus)
  - FSAngo (Fuji Soft)
  - MUGI (Hitachi) → Full Eval. In FY2002
- PRNG
  - RNG by Clutter Box (HMI)
  - FSRansu (Fuji Soft)
  - RNE (SIL)
  - TAO TIME (JCN)

General Evaluation (Newly Submitted Tech.) (cont.)

- Screening evaluation (Oct.2001~Mar.2002)
  - Submission completeness examination
- Security evaluation (examine trivial weakness)

  (based on the self evaluation report by experts)
  - Stream Cipher
    - statistical properties, length of period & linear complexity
    - resistance against well known attack and heuristic attack
  - PRNG
    - statistical properties with randomness tests etc.
    - resistance against attacks, unpredictability

Screening evaluation (Oct.01'~Mar.02') (cont)

- Implementation aspects
  (Stream Cipher & PRNG)
  - implementability by third parties
    - sufficient information in the specification
    - disclosure to public for evaluation.
    - not require extremely special HW
- Superior or equal feature (for security or performance) to the existing techniques in CRYPTREC 2000 project.
- Call for public comments

(1-b) Full evaluation

- Schedule
  - April.2002~ (selected techniques in 2001)
    - Oct.2000~March.2001 (techniques in 2000)
- Security Evaluation
  - Inspect weakness in detail
    - http://www.ipa.go.jp/security/enc/CRYPTREC/fy13/guidance.pdf
    - http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy13/call20010801e.pdf
  - includes external experts evaluation in Japan and abroad

Full evaluation (cont.)

- Security Evaluation
  - Block cipher
    - well-known attacks (DC & LC)
    - other attacks (HOD, SA,etc)
    - Avalanche property
    - heuristic attack
  - Stream Cipher
    - statistical properties (period, Linear complexity, etc)
    - well-known attacks (correlation, divide & conquer,..)
    - heuristic attack

Full evaluation (cont.2)

- Hash Function
  - one way and collision free in practical time
  - well-known attack (DC, algebraic attack)
  - statistical properties
  - heuristic attack
- PRNG
  - statistical properties with randomness (FIPS140-1)
  - unpredictability, heuristic attack

Full evaluation (cont.3)

- Implementation
  - Block & stream cipher
    - Software: encryption, key scheduling (speed, memory usage)
    - Hardware: process, speed, resource used
  - Hash function
    - Software/Hardware
  - PRNG
    - Software

(1-c) General Evaluation Continual Evaluation

- fully evaluated in 2000 & deserve further evaluation
- status of availability clarified by the applicant
- 64-bit Block Cipher
  - CIPHERUNICORN-E * (NEC)
  - Hierocrypt-L1 (Toshiba)
  - MISTY1 (Mitsubishi)
  - T-DES

  * further detailed evaluation in FY2001

Continual evaluation (cont.)

- 128-bit Block Cipher
  - Camellia (NTT&Mitsubishi)
  - CIPHERUNICORN-A * (NEC)
  - Hierocrypt-3 (Toshiba)
  - RC6 Block Cipher (RSA)
  - SC2000 (Fujitsu)
  - AES *

Continual evaluation (cont.2)

- Stream Cipher
  - MULTI-S01 * (Hitachi)
- Hash function
  - RIPEMD-160
  - SHA-1
  - Draft SHA-256/384/512 *
- PRNG
  - PRNG based on SHA-1

(2-1) Specific Evaluation

- Request from CRYPTREC Advisory committee
- Cryptographic techniques
  - (64-bit)　MISTY1, Hirocrypt-L1
  - (128-bit) Camellia, Hierocrypt-3, SC2000
- CRYPTREC2000 Report + additional evaluation

(2.-2) Specific Evaluation

- Request from WG discussing requirements for cryptographic techniques and guidelines concerning to the Japanese e-Govermment
  - cryptographic technique used in SSL environment (RC2,RC4(Arcfour), T-DES ,DES)

(2.-3) Specific Evaluation

- Request from CRYPTREC Advisory committee
  - 128 bit block cipher SEED proposed by KISA

(3) 64 bit block cipher Overall Eval.

- CIPHERUNICORN-E (16R Feistel)
  - No security problem has so far been found.
  - Slow processing speed (compared to DES)
- Hierocrypt-L1 (6R SPN)
  - No security problem has so far been found
  - Fast processing speed
- MISTY1 (8R Feistel)
  - No security problem has so far been found
  - Fast processing speed

Overall Eval.(cont.)

- T-DES (48R Feistel)
  - There should not be any security problem so long as guarantee is provided by FIPS (or an equivalent)

SW implementation eval.

- Pentium III (650MHz)

  Enc/Dec [Mbps]

  UNI-E 29/29

  Hiero-L1 209/204

  MISTY1 195/200

  T-DES 49/49

  – {UNI-E,T-DES} slow
  – {Hiero-L1,MISTY} fast
- Enc/Dec with key schedule → See Report

- Ultra SPARC IIi (400MHz)

  Enc/Dec[Mbps]

  UNI-E 18/18

  Hiero-L1 68/51
- Alpha21264 (463MHz)

  Enc/Dec[Mbps]

  UNI-E 19/19

  Hiero-L1 141/141

  MISTY1 139/144

HW implementation eval.

- Hiero-L1 and MISTY1: evaluated
- T-DES: values from Ref. paper
- Approx. value relative to T-DES (T-DES=1)
  - Non Loop architecture

	size	speed
Hiero-L1	2.5	2.25

  - Loop architecture

MISTY1	10~7.6	2.5~1.9

Security Margin & Speed

	S.Margin	Algorithm	Speed
UNI-E	16/-*		0.60
Hiero-L1	6/3.5	H.O.D	4.25
MISTY1	8/5	H.O.D	4.07
T-DES	48/48	meet in the middle	1

S.Margin=rounds / best known rounds that can be attacked

Speed(Data randomization part):T-DES=1

*For UNI-E attack algorithm which is faster than brute force search is not yet known

(4) 128 bit block cipher Overall Eval.

- AES (10R~14R SPN)
  - No security problem has so far been found
  - Fast processing speed
- Camellia (18R~24R Feistel)
  - No security problem has so far been found
  - Fast processing speed
- CIPHERUNICORN-A (16R Feistel)
  - No security problem for practical use. Though, not yet well proved the security against DC & LC
  - Slow processing speed

Overall Eval. (cont.)

- Hierocrypt-3 (6R~8R SPN)
  - No security problem has so far been found
  - Fast processing speed
- RC6 (20R mod.Feistel)
  - No security problem has so far been found
  - Fastest encryption speed on Pentium III
  - Speed depends on the platform greatly
- SC2000 (19R~22R Feistel+SPN)
  - No security problem has so far been found
  - Fast processing speed

Overall Eval. (cont2.)

- SEED (16R Feistel)
  - No security problem has so far been found
  - Rather slow processing speed

SW implementation eval.

- Pentium III (650MHz)

  Enc/Dec[Mbps]

  Came 255/255
  UNI-A 53/53
  Hiero-3 206/195
  RC6 323/318
  SC2K 214/204
  SEED 98/98
  T-DES 49/49

- Ultra SPARC IIi (400MHz)

  Came 144/144
  UNI-A 23/22
  Hiero-3 109/84
  RC6 25/25
  SC2K 186/182

- Alpha21264 (463MHz)

  Came 210/210
  UNI-A 32/34
  Hiero-3 149/154
  SC2K 226/216

Additional SW Evaluation(Specific)

- Software Implementation feature on Z80
  - Compared to the property of Rijndael
  - RAM restriction: around 66 bytes
  - Memory usage (RAM, ROM)
  - Speed for a block encryption
  - 128-bit Block Ciphers

Z80 Software Implementation

	RAM [Bytes]	ROM [Bytes]	Enc/Dec Speed 5MHz Z80 [ms]
Camellia	48	1268	7/8
Hiero-3	73	4746	10/14
SC2000	64	2350	19/19
Rijndael*	63	1221	7/10

* 2nd NESSIE Workshop

HW implementation eval.

- {Hiero-3,RC6,Came} evaluated
- AES: values from Ref. paper
- Approx. value relative to T-DES (T-DES=1)
  - Non Loop architecture

	size	speed
AES	4.1	>4
Hiero-3	4.8	>4
RC6	>10	<1

  - Loop architecture

Came	4~6	2.5~3

Security Margin & Speed

	S.Margin	Algorithm	Speed
AES	14/8	H.O.D	2.15
Came	24/10	H.O.D	5.24
UNI-A	16/-	-	1.02
Hiero-3	8/3.5	H.O.D	4.12
RC6	20/15	X^2 attack	6.57
SC2K	22/13	DC	4.29
SEED	16/7	DC	2.02

S.Margin=rounds for 256-bit key / best known rounds that can be attacked

(5) Stream Cipher

- MULTI-S01
  - Security:
    - No security problem has so far been found
    - SW processing speed is fast
    - Security depends on the security of PANAMA
  - SW implementation aspect
    - 238[Mbps] on Pentium III (650MHz)
  - HW implementation aspect
    - > 1[Gbps] on FPGA(EP20K1000E)
- MUGI → Full Eval. In FY2002

(6) Hash function

- RIPEMD-160
  - No security problem for practical use.
- SHA-1
  - No security problem for practical use.
- Draft SHA-256/384/512
  - Enhanced security version of SHA-1
  - No security problem has so far been found.
  - Recommend the use after reevaluation of the FIPS version
  - Needs to watch the security trends on hash bit length for the long term use

(7) PRNG

- Pseudo-Random Number Generator based on SHA-1（FIPS186-1:DIGITAL SIGNATURE STANDARD APPENDIX C）(NIST,1995)
  - No security problem for practical use

(8) RC2,DES (Specific Eval.)

- cryptographic technique used in SSL environment
- 40 bit key {DES,RC2}
  - Should not be used for security system
  - Easily broken
- 56 bit key DES
  - Recommend not to use expecting high security
  - Practically broken

RC2,DES (Specific Eval.) (cont.)

- T-DES
  - There should not be any security problem so long as guarantee is provided by FIPS (or an equivalent)
- 128 bit key RC2
  - Recommend not to use for e-government security system
  - Scientifically broken
- RC4(Arcfour)
  - Evaluation will be conducted in FY2002