Report on Evaluation of Symmetric-Key Cryptographic Techniques

May 22, 2003

Toshinobu Kaneko

Chair, Symmetric-Key Cryptography Subcommittee

(Science University of Tokyo)

Symmetric-Key Cryptography Subcommittee(2002)

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.) A.Satoh(IBM)

T.Shimoyama (Fujitsu) K.Takaragi (Hitachi)

M.Tatebayashi (Matsushita) Y.Tsunoo (NEC)

T.Tokita (Mitsubishi) M.Morii (Tokushima U.)

14 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

CRYPTREC Recommended List for the use in E-Government in Japan

Symmetric-key cryptographic techniques

64-bit block ciphers:

128-bit block cipher is desirable if longer block length is permitted in a newly constructed e-Government systems

- CIPHERUNICORN-E (submitted by NEC)
  - *practically secure*
- Hierocrypt-L1 (submitted by Toshiba)
  - *practically secure*
- MISTY1 (submitted by Mitsubishi)
  - *practically secure*
- Triple DES (FIPS46-3)
  - *practically secure, limited usage in 3 key Triple DES*
  - *accept for the present use under the following conditions:*
    1) *to be specified in FIPS46-3*
    2) *to keep the status of de facto standard*

128-bit block ciphers

- AES (FIPS-197)
  - *practically secure*
- Camellia (submitted by NTT)
  - *practically secure*
- CIPHERUNICORN-A (submitted by NEC)
  - *practically secure*,
- Hierocrypt-3 (submitted by Toshiba)
  - *practically secure*
- SC2000 (submitted by Fujitsu)
  - *practically secure*

Stream ciphers

- MUGI (submitted by Hitachi)
  - *practically secure,*
- MULTI-S01 (submitted by Hitachi)
  - *practically secure,*
- RC4 (Ref:S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," LNCS 2259, pp.1-24, Springer-Verlag, 2001)
  - *supposed to be used with 128-bit key length in SSL3.0 or TLS1.0*

Hash functions

- RIPEMD-160　(ISO/IEC 10118-3)
  - *practically secure* *
- SHA-1　　(FIPS-180-1)
  - *practically secure* *
- SHA-256/384/512（FIPS Approved)
  - *practically secure*

** Provided that a hash function is not specified in the public-key schemes in this list, more than 256-bit length hashed value is desirable if longer block length is permitted in a newly constructed e-Government systems.*

Pseudo-random number generators

There is no problem in the use of any generator, if it is cryptographically secure, in accordance with no needs for interconnectivity. The followings PRNGs are examples:

- PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1:
  - *practically secure*
- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+change notice 1)Appendix 3.1
  - *practically secure*
- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+change notice 1) revised Appendix 3.1
  - *practically secure*

Evaluation Respects

- Security:
  - Strength of each algorithm against general (well-known) cryptanalytic techniques
  - Strength of a specific algorithm against effective cryptanalytic methods
- Implementability:
  - Software implementation
    - Pentium III, UltraSPARC Iii, Alpha 21264,Smart card: Z80 simulator
      - Enc/Dec speed, Mem. Size of the program
  - Hardware implementation
    - FPGA,ASIC

Security Evaluation

- Block cipher
  - Differential / Linear cryptanalysis
  - Higher order differential attack (SQUARE attack)
  - Avalanche property
  - heuristic attack (Chi-square,Mod n,Meet-in-the-middle impossible differential,.., etc.)
- Stream Cipher
  - statistical properties (period, Linear complexity, etc)
  - well-known attacks (correlation, divide & conquer,..)
  - heuristic attack

Security 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

Security Eval. Results (Block Cipher)

- Differential / Linear cryptanalysis
  - Provable security (= Bounds of Max. diff./linear prob.):
    - MISTY1: 2^{-56} or lower with 3 rounds
    - AES: 2^{-96} or lower with 4 rounds
  - Practical security (= Bounds of Max. diff./linear char. prob.):
    - AES: 2^{-150} in 4 rounds
    - Camellia: 2^{-132} in 12 rounds without FL/FL^{-1} functions
    - CIPHERUNICORN-E: 2^{-64} in 8 rounds for DC. 2^{-70} in 12 rounds for LC
    - CIPHERUNICORN-A: 2^{-128} in 13 rounds
    - Hierocrypt-3: 2^{-150} in 2 rounds
    - Hierocrypt-L1: 2^{-90} in 2 rounds
    - SEED: 2^{-192} in 13 rounds for DC. 2^{-128} in 6 rounds for LC
    - SC2000: 2^{-134} in 15 rounds for DC. 2^{-142} for LC
  - Heuristic security (= Max. diff./linear char. Prob.):
    - RC6: 2^{-140} in 14 rounds for DC. 2^{-128} in 6 rounds for LC
    - Triple DES: $2^{-54.1}$ in 16 rounds for DC. $2^{-44.9}$ in 16 rounds for LC

Security Evaluation Results (cont.)

- Higher order differential attack (SQUARE attack)
  - More efficient attack than differential/linear cryptanalysis:
    - MISTY1 can be attacked up to 5 rounds.
    - AES can be attacked up to 7 rounds for 128-bit key or 8 rounds for 192-/256-bit key.
  - Successful attack:
    - Camellia can be attacked up to 8 rounds for 128-bit key or 11 rounds for 192-/256-bit key
- Effective cryptanalytic methods
  - Chi-square attack:
    - RC6 can be attacked up to 12 rounds for 128-bit key, 14 rounds for 192-bit key, or 15 rounds for 256-bit key.
  - Meet-in-the-middle attack:
    - Triple DES can be theoretically broken.

SW implementation eval. (64-bit block)

- 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

Security Margin & Speed (64-bit block)

	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

SW implementation eval.(128-bit block)

- 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 eval.(128-bit block)

- 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

Security Margin & Speed (128-bit block)

	S.Margin	Algorithm	Speed
AES	14/8	H.O.D	2.15
Came	24/11	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

Security & Impl. eval. (Stream Cipher)

- Secuirity
  - No security problem has so far been found for MUGI, MULTI-S01
  - Weak Initial Value for RC4
  - No Security problem has been reported for 128-bit key RC4 in SSL3.0 or TLS 1.0
  - Recommend not to use 40-bit key algorithm for e-government security system
- Implementation
  - SW processing speeds are fast for MUGI, MULTI-S01 and RC4
    - on Pentium III (650MHz)
      - MULTI-S01 350[Mbps] Enc. Speed