Report on Present State of CIPHERUNICORN-E Cipher Evaluation (full evaluation)

January 28, 2002

Toshio Tokita, Member

Symmetric-Key Cryptography Subcommittee

CIPHERUNICORN-E

- CIPHERUNICORN-E was presented by NEC Corporation in 1998.
- Symmetric-key block cipher
  (block length: 64 bits; key length: 128 bits)
- Registered in ISO9979 (1998)
- Continual evaluation cipher from CRYPTREC2000
- Features
  - Feistel structure (16 rounds) + auxiliary functions (inserted every 2 rounds)
  - Round function with dual structure consisting of a *main stream* and a *temporary key generation mechanism*.
  - Round function designed by cipher evaluation support system (NEC proprietary development).

CRYPTREC2000 evaluation results

- **So far, no security-related problems have been discovered.**
  - In general terms, given that the specification has 16 rounds, it would seem impossible to cryptanalyze the cipher using current theoretical cryptanalysis techniques.
- **In terms of processing speed, CIPHERUNICORN-E is classified as a slow group among 64-bit block ciphers**
  - Among the 64-bit block ciphers which are in CRYPTREC2000 continual evaluation, this cipher belongs to the slow group. (Speed is approximately 3/5 that of Triple DES in a PC environment.)

– – – – – – – – – – – – – –

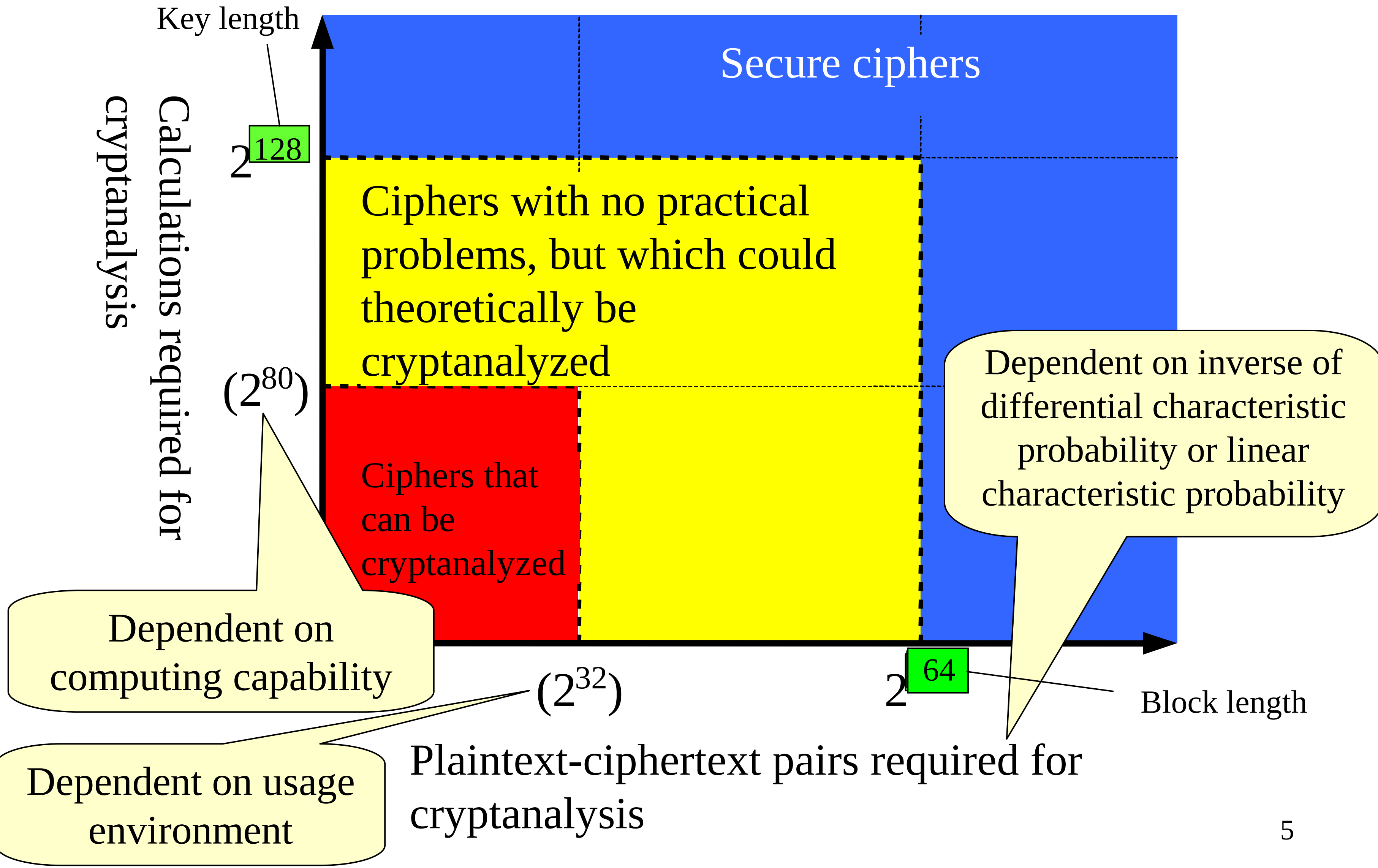
- **Because this cipher is a complex round function, accurate evaluation is difficult, so continual evaluation is considered necessary.**
  - It is difficult to accurately evaluate and analyze security against theoretical cryptanalysis techniques such as differential cryptanalysis and linear cryptanalysis.
  - It is necessary to conduct a more-detailed evaluation, replacing the (simplified) mF function with the actual round function.

Evaluation procedure

- Continual evaluation this fiscal year:
  - We requested four specialists (teams) in cipher research in Japan and abroad to conduct a security evaluation based on the following perspectives:
    - Security against *differential cryptanalysis*, from the perspective of differential characteristic probability
    - Security against *linear cryptanalysis*, from the perspective of linear characteristic probability
    - Appropriateness of conducting evaluation using mF function
    - Other noted security-related issues

Overview of security evaluation

Block length: 64 bits
Key length: 128 bits



Key length

2^{128}

(2^{80})

Calculations required for cryptanalysis

Secure ciphers

Ciphers with no practical problems, but which could theoretically be cryptanalyzed

Ciphers that can be cryptanalyzed

Dependent on inverse of differential characteristic probability or linear characteristic probability

Dependent on computing capability

(2^{32})

2^{64}

Block length

Dependent on usage environment

Plaintext-ciphertext pairs required for cryptanalysis

Comments of Evaluator 1

- It is difficult to imagine that CIPHERUNICORN-E, with 16 rounds, could be attacked by differential cryptanalysis or linear cryptanalysis.

  – Security against differential cryptanalysis
    - Upper bound of maximum characteristic probability for round function: $\leq 2^{-21}$

      (Upper bound of maximum characteristic probability for 13 rounds: $\leq 2^{-126}$)
    - Conclusion: CIPHERUNICORN-E with 16-round specifications cannot be cryptanalyzed by differential cryptanalysis.

  – Security against linear cryptanalysis
    - The cipher seems more secure against linear cryptanalysis than against differential cryptanalysis.
    - Upper bound of characteristic probability for round function: $\leq 2^{-24.64}$

      (Upper bound of maximum characteristic probability for 13 rounds: $\leq 2^{-147.84}$)
    - Conclusion: CIPHERUNICORN-E with 16-round specifications cannot be cryptanalyzed by linear cryptanalysis.

Comments of Evaluator 2

- I found no grounds for suspecting any problems related to security against differential cryptanalysis and linear cryptanalysis.

  - Security against differential cryptanalysis
    - My calculated results differed from the evaluation results in the self-evaluation

      (upper bound of characteristic probability with mF function: $\leq 2^{-72.0}$)
    - However, at present it seems impossible to attack the cipher with differential cryptanalysis.
  - Security against linear cryptanalysis
    - My calculated results differed from the evaluation results in the self-evaluation

      (upper bound of characteristic probability with mF function : $\leq 2^{-62.0}$)
    - However, at present it seems impossible to attack the cipher with linear cryptanalysis.

Comments of Evaluator 3

- Differential cryptanalysis: My evaluation results differed from the results in the self-evaluation, but I see no problem in terms of security.
  - I calculated an upper bound value different from the value in the self-evaluation for the differential characteristic probability.
  - Upper bound for maximum characteristic probability with mF function: $\leq 2^{-14}$
  - Upper bound for characteristic probability with 15 rounds: $\leq 2^{-98}$
  - Given that CIPHERUNICORN-E has 16 rounds, it seems secure against differential cryptanalysis.

- Linear cryptanalysis: My evaluation results differed from the results in the self-evaluation, but I see no problem in terms of security.
  - I calculated an upper bound value different from the value in the self-evaluation for the linear characteristic probability.
  - Upper bound for maximum characteristic probability with mF function: $\leq 2^{-27.309}$
  - Upper bound for maximum characteristic probability with 15 rounds: $\leq 2^{-191.163}$
  - Given that CIPHERUNICORN-E has 16 rounds, it seems secure against linear cryptanalysis.

Comments of Evaluator 4

- I evaluated whether the 16-round CIPHERUNICORN-E can be attacked by differential cryptanalysis or linear cryptanalysis.
  - Differential cryptanalysis: I believe 16 rounds cannot be attacked.
    - Upper bound for characteristic probability of round function: $\leq 2^{-16}$
    - This does not contradict the results in the self-evaluation, in terms of evaluation based on an upper bound value.
    - I believe that there are no effective differential characteristics for 10 rounds or more.
  - Linear cryptanalysis: I believe 16 rounds cannot be attacked.
    - Upper bound for characteristic probability of round function: $\leq 2^{-16}$
    - I believe the upper bound value ($2^{-63.90}$) for the round function in the self-evaluation is not appropriate. However, this does not change the conclusion that 16 rounds cannot be attacked.
    - I believe that there are no effective linear characteristics for 10 rounds or more.

Conclusion

- Based on this fiscal year’s follow-up evaluation results, so far no security-related problems have been discovered in CIPHERUNICORN-E with 16 rounds, which is the number of rounds in the specifications.
  - The evaluators obtained evaluation results (upper bound values in all cases) that differed from the evaluation results in the self-evaluation, with respect to the evaluation of the round function’s differential/linear characteristic probability, etc. However, in no case was there an indication that the number of rounds in the specifications (16 rounds) could be attacked.