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

January 28, 2002

Masayuki Kanda, Member

Symmetric-Key Cryptography Subcommittee

CIPHERUNICORN-A

- CIPHERUNICORN-A was presented by NEC Corporation in 2000.
- Symmetric-key block cipher
- Block length: 128 bits; key length: 128/192/256 bits
- Follow-up evaluation cipher from CRYPTREC2000
- Features
  - Feistel structure (16 rounds) + whitening
  - Round function with dual structure consisting of a *main stream* and a *temporary key generation mechanism*.
  - Round function designed by cipher-robustness 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 defines the number of rounds as 16, it would seem impossible to cryptanalyze the cipher using current theoretical cryptanalysis techniques.
- **Because this cipher has a complex round function, accurate evaluation is difficult, so follow-up 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.
- **In terms of processing speed, CIPHERUNICORN-A is among the slower.**
  - Among the 128-bit block ciphers which are in CRYPTREC2000 continual evaluation, this cipher belongs to the slowest group. (Speed is on par with Triple DES.)

Evaluation procedure

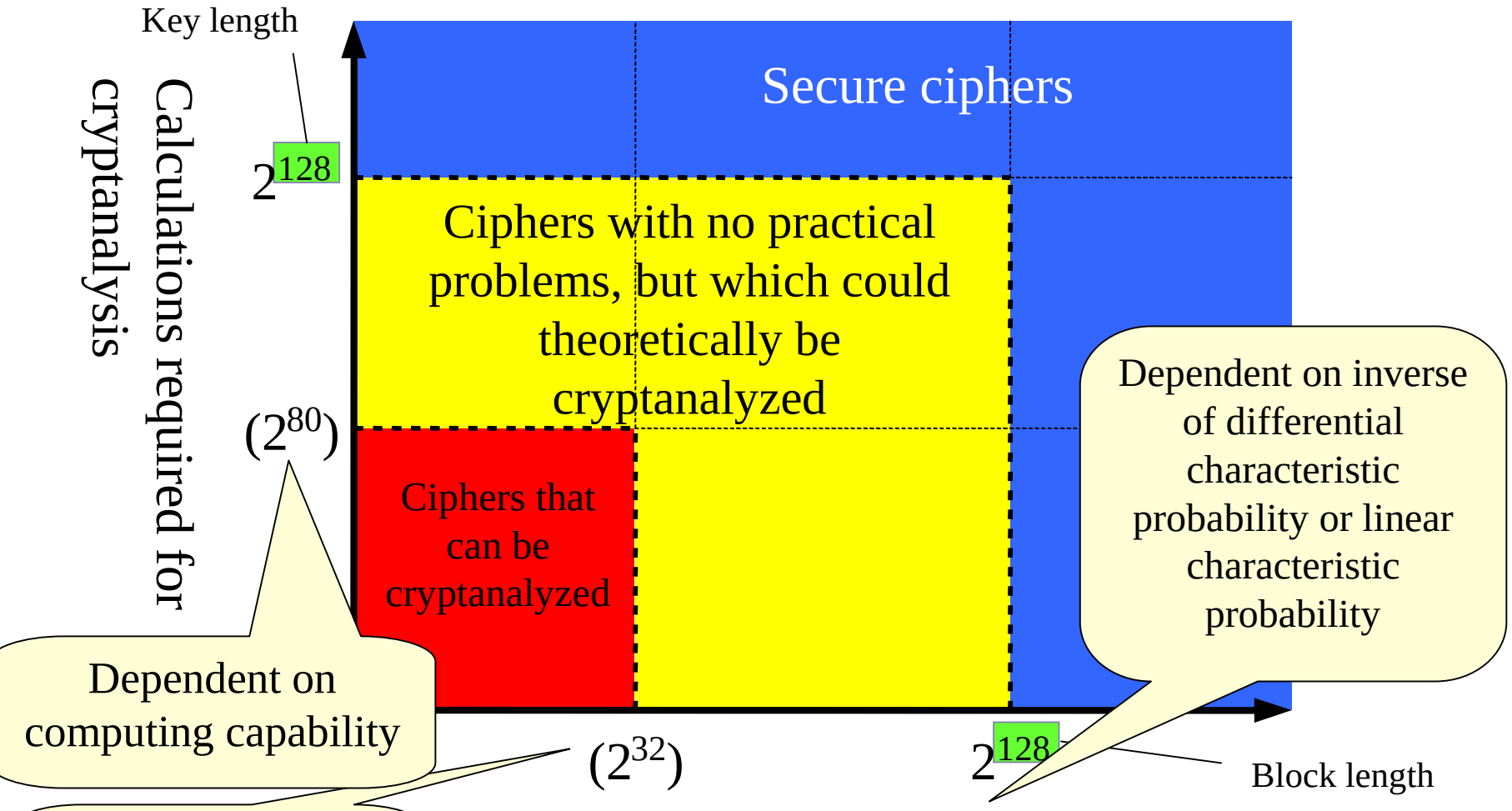
- Full evaluation:

  We requested four specialists (teams) in cipher research in Japan and abroad to conduct an evaluation based on the following perspectives:

  - Appropriateness of conducting evaluation using mF function
  - Security against differential cryptanalysis, from the perspective of differential characteristic probability
  - Security against linear cryptanalysis, from the perspective of linear characteristic probability
  - Other noted security-related issues

Overview of security evaluation

Block length and key length are both 128 bits



Comments of Evaluator 1

- **Supporting evidence is provided indicating the cipher is secure against differential cryptanalysis and linear cryptanalysis**
  - **Security against differential cryptanalysis**
    - Upper bound of characteristic probability with round function: $\leq 2^{-21}$
    - Upper bound of characteristic probability with 13 rounds: $\leq 2^{-126}$
  - **Security against linear cryptanalysis**
    - The cipher seems more secure against linear cryptanalysis than against differential cryptanalysis
    - Assuming the security in the self-evaluation is correct, the following upper bound values are calculated.
      - Upper bound of characteristic probability with round function $\leq 2^{-13.9}$
      - Upper bound of characteristic probability with 13 rounds: $\leq 2^{-83.4}$
    - The obtained results contradict the security in the self-evaluation.
      - The possibility of a higher upper bound of linear characteristic probability with the round function exists.
    - There is almost no consideration for the effects of the A3 function, constant multiplication unit, and temporary key generating mechanism.

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**
    - Upper bound of characteristic probability of the round function without A3 function and multiplication: $\leq 2^{-14.4}$
    - There cannot be any cases where the characteristic probability with the round function greatly exceeds $2^{-12.}$ In addition, the A3 function and constant multiplication can be expected to contribute to improved security.
  - **Security against linear cryptanalysis**
    - The characteristic probability upper bound in the security self-evaluation is incorrect.
    - Upper bound of characteristic probability with mF function: $\leq 2^{-21.68}$
    - The A3 function and constant multiplication can be expected to contribute to improved security.
- **Existence of weak keys**
  - **All 32-bit subkeys are identical to the first 32 bits in the secret key**

    { 0x61db99c8, 0x9f3d618, 0x9f3d618, 0x9f3d618, … }

    This becomes the exact subkey value

Comments of Evaluator 3

- **The evidence is not so strong as to provide clear proof of security against differential cryptanalysis**
  - Discovered differential characteristics more efficient than those in the security self-evaluation.
  - Upper bound of characteristic probability with mF function: $\leq 2^{-7}$
  - Upper bound of characteristic probability with 15 rounds: $\leq 2^{-70}$
    (Upper bound of characteristic probability with 13 rounds: $\leq 2^{-56}$)
  - The above results are from a byte-level search. Therefore, the characteristic probability (upper bound) may fluctuate if the effects of constant multiplication and the A3 function are studied in detail.
- **The cipher seems secure against linear cryptanalysis**
  - The characteristic probability upper bound in the security self-evaluation is incorrect.
  - Upper bound of characteristic probability with mF function: $\leq 2^{-21.37}$
  - Upper bound of characteristic probability with 15 rounds: $\leq 2^{-149.58}$
    (Upper bound of characteristic probability with 13 rounds: $\leq 2^{-128.22}$)

Comments of Evaluator 4

- **Supporting evidence is provided indicating the cipher is secure against differential cryptanalysis**
  - Evaluation using round function (main stream section only) excluding the effects of the temporary key generation mechanism
    - Upper bound of characteristic probability: $\leq 2^{-7}$
    - Upper bound of characteristic probability with 6-round iterative expression: $\leq 2^{-56}$
    - Upper bound of characteristic probability with 13 rounds: $\leq 2^{-119}$
  - Effects of temporary key generation mechanism
    - The temporary key generation mechanism has characteristics opposite those of the A3 function, so it can be expected to contribute to improved security.

Summary of evaluations

Attack method		Evaluator 1	Evaluator 2	Evaluator 3	Evaluator 4
Differential cryptanalysis	Model	Full	mF function	mF function	Main stream section, 6-round iterative
	Characteristic probability upper bound with round function	$\leq 2^{-21}$	$\leq 2^{-14.4}$	$\leq 2^{-7}$	$\leq 2^{-7}$
	Characteristic probability upper bound with 13 rounds	$\leq 2^{-126}$	$\leq 2^{-115}$	$\leq 2^{-56}$	$\leq 2^{-119}$
Linear cryptanalysis	Model	mF function	mF function	mF function	---
	Characteristic probability upper bound with round function	$\leq 2^{-13.9}$ (see note)	$\leq 2^{-21.6}$	$\leq 2^{-21.3}$	---
	Characteristic probability upper bound with 13 rounds	$\leq 2^{-83.5}$ (see note)	$\leq 2^{-130}$	$\leq 2^{-128}$	---

Note: These results assume the designer's evaluation is correct.

Conclusion

- **The cipher's security level is not high enough to completely eliminate all security concerns**
  - In terms of security against differential cryptanalysis and linear cryptanalysis, the possibility of problems occurring, at least in practical use, is extremely low.
    - *Supporting evidence has been obtained suggesting that* attacks based on these cryptanalysis methods *would probably not succeed*.
    - *The evidence is not so strong as to prove clearly that the cipher is theoretically secure* against these cryptanalysis methods.
  - The existence of weak keys that seem non-trivial was discovered
    - There is at least one secret key in which only the first 32 bits are used for all subkeys
    - The level of impact of this on security is not known at the present time.