Report on Present State of MUGI Cipher Evaluation (screening evaluation)

January 28, 2002

Kouichi Sakurai

Member,

Symmetric-Key Cryptography Subcommittee

A. Summary of screening evaluation results

(1) Based on the verification results, (some) test vectors are not correct.

(2) The characteristics compared to a FY2000 full evaluation cipher are not superior in the self-evaluation.

B. Items requiring review and study for full evaluation

(1) Why were the test vectors not correct?

Check whether the reason is technical or editorial.

(2) Study of MUGI's characteristics compared to FY2000 full evaluation ciphers (MULTI-S01 and TOYOCRYPT-HS1) as a stream cipher. Especially, MUGI is to be compared against MULTI-S01 to determine which is better and to identify differences from MULTI-S01, which uses the PANAMA as a random number generator algorithm.

C. General comments of individual evaluators

(unedited excerpts)

Evaluator 1:
General evaluation comments

According to my review, a full evaluation should be conducted and security should be evaluated.

(1) Characteristics compared to FY2000 full evaluation cipher

- "MULTI-S01", which was provided by the same submitter (company), is a stream cipher which uses the PANAMA algorithm just as this submission does. Therefore, these two ciphers need to be compared (identify their differences).
- In addition, the cipher uses a function corresponding to a block cipher round function, so its performance (speed) should also be compared against block ciphers.
- Although the submitted document says it is on par with AES, there is no numerical comparison.

(2) Useful applications

None are stated, but presumably it could be used in nearly all applications relating to confidentiality.

Evaluator 1: Comments on cryptographic technique specifications

These specifications included detailed information for third party implementation. Following are my comments.

(1) Design criteria

There was no description of quantitative base values pertaining to design, other than a statement that the secret key is 128 bits.

(2) Support for multiple key lengths

The only inputs during encryption are plaintext, secret key (128 bits), and initial vector (128-bit public parameter). Therefore, this method is a 128-bit fixed length method.

(3) Characteristics compared to FY2000 full evaluation cipher

This proposal is presented as a stream cipher, but the text does not include characteristics compared to FY2000 full evaluation (MULTI-S01 and TOYOCRYPT-HS1).
In addition, because its cipher method is categorized as a Vernam cipher, it is similar to TOYOCRYPT-HS1. However, it uses PANAMA internally, so the submitted document should include a comparison against MULTI-S01, and identify differences between it and MULTI-S01.

Evaluator 1:
Comments on self-evaluation (1)

(1) Security evaluation

The security of the proposed method depends on the capabilities of the pseudo-random number generator, but symmetric-key cryptography is actively used as a component.

Therefore, in the full evaluation, it is also necessary to evaluate from the perspective of symmetric-key cryptography analysis. At the same time, in evaluating the (statistical) randomness of the pseudo-random number generator, it is also necessary to consider more-detailed evaluations (NIST evaluation method “Random Number Generation and Testing” (http://csrc.ncsl.nist.gov/rng/).

(2) Third party evaluation and usage history

The self evaluation did not contain any third party evaluation or usage history relating to the proposed method.

(3) Characteristics compared to FY2000 full evaluation cipher

Not included. As mentioned above in the general evaluation comments regarding the specifications, it is necessary to compare the characteristics of the cipher against MULTI-S01, which includes a similar system.

Evaluator 1:
Commends on self-evaluation (2)

Issues where parts in the document was unclear

(1) Proof on page 16

The following text is at the end of Case 2 (2-round iterative expression): a_2=f^{-1}(a_2 + C_a, 0) + C_b.

This seems to be a variation of the formula a_2=F^{-1}(β, 0) +C_1 + F(a_1, 0), which is located five lines above it. If that is the case, then the variation is inappropriate. Simplifying the formula gives β =a_2+C_a (where C_a is a constant dependent on a1). However, this is contradictory in that β is a nonlinear transform with two inputs—“a_2” and a “constant dependent on a1”.

In contrast, the original claim of Case 2 (“On average, there exists a single a2 satisfying the above conditions.”) seems correct.

(2) Claim in Section 3.5.3

This section only shows an example of simple linear sum relationships between buffers. Perhaps the authors meant to claim that these relationships also disappear after the initial mixing is completed, but there is no statement to that effect.

Evaluator 2:
General evaluation comments

The specifications are written at a level that enables implementation.
In addition, aspects such as the design policy are also described clearly.
Security evaluations were conducted from a variety of perspectives, ranging from general attack methods to structure-specific attacks. In addition, statistical evaluations were performed with customized FIPS140-1.

Performance evaluations were conducted satisfactorily for both software and hardware, and the values obtained for processing speed, resources, hardware scale, and the like seem satisfactory.

However, the specifications have a number of text omissions and errors that seem to be typographical errors.

In addition, when I ran the reference code in our computing environment, one of the test vectors in the specifications did not match the output values.

There is no clear description of characteristics compared to a FY2000 full evaluation cipher in the submitted documents.

MULTI-S01, which is a FY2000 full evaluation cipher, also uses the PANAMA structure. However, the present technology seems characterized in that it uses the AES function internally.

Evaluator 2: Comments on cryptographic technique specifications

Design policy and base theory are clearly described. In the specification, there were text omissions and errors that seemed to be typographical errors (e.g., the last line on page 4, around the 11th line on page 11).

However, the specification itself can be identified, and implementation seems possible.

I compiled and ran the reference code in our computing environment (UltraSPARCII-Solaris8 and Pentium III-Windows NT4.0). Two test vectors described in the specification as well as 15 reference code test vectors were outputted. The output values matched for the first vector in the specification and the 15 reference code test vectors .

However, the output for the second test vector was different from the specification. The output vector is included in Attachment 1.

Evaluator 2:
Comments on self-evaluation (1)

Overall, the self-evaluation covers various attacks in detail with respect to security, and provides a satisfactory level of detail regarding performance as well.
For security evaluations, the FIPS140-1 test was customized to handle long plaintext for statistical evaluation, and frequency tests and run tests (areas where “0” or “1” is consecutive) were conducted.

This FIPS140-1 type statistical evaluations seem to be a satisfactory test item.

Other types of attacks were also evaluated in detail, and the test items and attack details seem satisfactory. Because they are outside my specialty, however, I cannot provide a conclusive assessment of them.

However, the basis for discussion in some instances was not clearly described. One example is the estimate that the period is greater than or equal to OFB. It will probably continue to be necessary to perform security evaluations going forward.

Evaluator 2: Comments on self-evaluation (2)

For performance evaluations, estimates can be calculated based on a conversion from AES, since MUGI contains an AES (Rijndael) function.

With respect to software, the code whose performance is described in the self-evaluation seems different from the reference code. However, the processing speed in the self-evaluation seems satisfactory when converted from the Rijndael processing speed. With respect to resources, only the work area and code are described. The work area component of these seems satisfactory. However, the amount of memory used by the code cannot be derived from the lines of code alone, so it is not possible to determine whether it is satisfactory.

With respect to hardware, the speed priority implementation seems satisfactory in terms of both resources and processing speed when converted from AES.

In addition, the small gates implementation seems satisfactory in terms of both resources and processing speed when converted from the speed priority implementation.

There is no clear description of characteristics compared to FY2000 full evaluation cipher in the submitted documents.

MULTI-S01, which is a FY2000 full evaluation cipher, also uses the PANAMA structure. However, the proposed technique seems characterized in that it uses the AES function internally.

Evaluator 3:
General evaluation comments

- The submitted technique is proposed as a cipher enabling high speed or deployment with minimal system requirements, on any software and hardware platform.
- While this cipher is a stream cipher, it enables both long periodicity and high speed because it handles processing in blocks with a length of 64 bits.
- If it simply handled processing in block increments, there would be doubts about its long periodicity. However, this does not appear to be a problem since it has a data mixer.
- However, it needs to be designed very carefully.

Evaluator 3: Comments on cryptographic technique specifications

The proposed method seems to provide sufficient security and high speed as a candidate stream cipher for use in the e-Government.

Evaluator 3:
Comments on self-evaluation (1)

In the self-evaluation of the submitted method, two requirements for pseudo-random number generator security are listed:

(1) The output series must be sufficiently random.

(2) If a different initial value is provided, the output series should change significantly.

Evaluator 3: Comments on self-evaluation (2)

As an evaluation of Requirement (1), first a frequency test and run test are performed.

In the frequency test, 512 random number sequences with series lengths of 222, 226, and 230 were generated, and 1-bit, 2-bit, 4-bit, and 8-bit tests were performed. In addition, run test was also performed on the 222 series length.

Series periods, linear complexity, and divide-and-conquer attacks are discussed as other traditional and theoretical random number series evaluation methods. With respect to these issues, there should be a focus on F-function design, i.e., S-box and matrix M design. The authors also investigate issues such as differential and linear characteristics of F-function, and the application of linear cryptanalysis.

Evaluator 3: Comments on self-evaluation (3)

For Requirement (2), the authors study fluctuations in output relative to initial vector changes while keeping the secret key fixed, with respect to ρ function differential and linear paths and re-synchronization attacks. In addition, as an investigation of fluctuations in output when the key is changed while the initial vector is kept fixed, the authors study issues such as buffer mixing performance, square attacks, and buffer correlations.

S-box in the F-function and matrix M are the same as those used by AES. However, I believe S-box and matrix M design methods would need to be studied in order to use the submitted technique in this self-evaluation.

Evaluator 4:
General evaluation comments

- The PANAMA modification is acceptable, but a full evaluation is needed with respect to the discussion regarding security and the like.

- There is also not enough PANAMA comparison data relating to software and hardware implementation. This issue needs to be studied in a full evaluation.

Evaluator 4: Comments on cryptographic technique specifications

There is no problem with the specification. However, because design policy and design criteria are closely related to security, a full evaluation of the correctness and reliability of these areas is needed.

Evaluator 4:
Comments on self-evaluation

- A full evaluation is needed with respect to the discussion regarding security and the like.
- The theory has not been established even in academia, so the potential attack cannot be fully discussed.

★Unclear issues and insufficiently discussed issues in self-evaluation

The self-evaluation uses phrases such as ‘it would be difficult’ etc. without providing sufficient grounds for these conclusions.
See Attachment 2.

- The verity of the above excerpts needs to be studied in a full evaluation.
- There is also not enough comparison data (PANAMA, AES, etc.) relating to software and hardware deployment. This issue needs to be studied in a full evaluation.

Divide-and-conquer attacks

Attacks categorized as divide-and-conquer attacks are attacks that guess part of the internal state. They may be used in cases where the internal state (partial) in any round can be described based on a guess in a given round.

However, with PKSG, internal states are generally large, and it is not possible to divide the state transition function so as to describe just part of the internal state. For reasons such as these, I believe it would be difficult to apply divide-and-conquer attacks to MUGI.

Other attack methods

Other block cipher attacks such as differential cryptanalysis [BS93], higher order differential attacks [Ku94], and interpolation attacks [JK97] are all chosen plaintext attacks. It seems difficult to apply these attacks (as randomness evaluation techniques) to PKSG. The reason for this is that the attacker is unable to obtain arbitrary output sequences, unlike in the case of block ciphers. Therefore, known plaintext attacks may be considered the only attacks on the random number sequences.

In addition, with any chosen plaintext attack, it is difficult, in terms of computational complexity, to obtain the chosen plaintext required for the attack from the output sequence. For example, in a case where some distinguisher is constructed from a 16-round output sequence, the original number of spaces constructed by the output sequence is 264×16. Thus in order to obtain the desired single set of chosen plain text, it is necessary to have known plaintext equal to approximately 264×8.

An example of differential cryptanalysis will now be considered. When a differential path is searched for with differential cryptanalysis as in 3.3.2, the attacker must be capable of freely observing internal state differentials in a given round. This is not possible in cases where sufficient initialization has been performed. Therefore, it would seem difficult to apply differential cryptanalysis.

(Im)possibility of Linear Buffers

Nonlinear mixing, done in conjunction with IV for these extremely limited keys, is performed over the entire buffer. As a result, during key setup, it is concluded that the buffer will be sufficiently randomly mixed.

Square attack

With stream ciphers, the attacker must set differences in either the key or the initial value. Therefore, it seems that related-key attacks or chosen initial value attacks are the only cases where Square attacks would be applicable to stream ciphers.