Report on Present State of MULTI-S01 Cipher Evaluation (full evaluation)

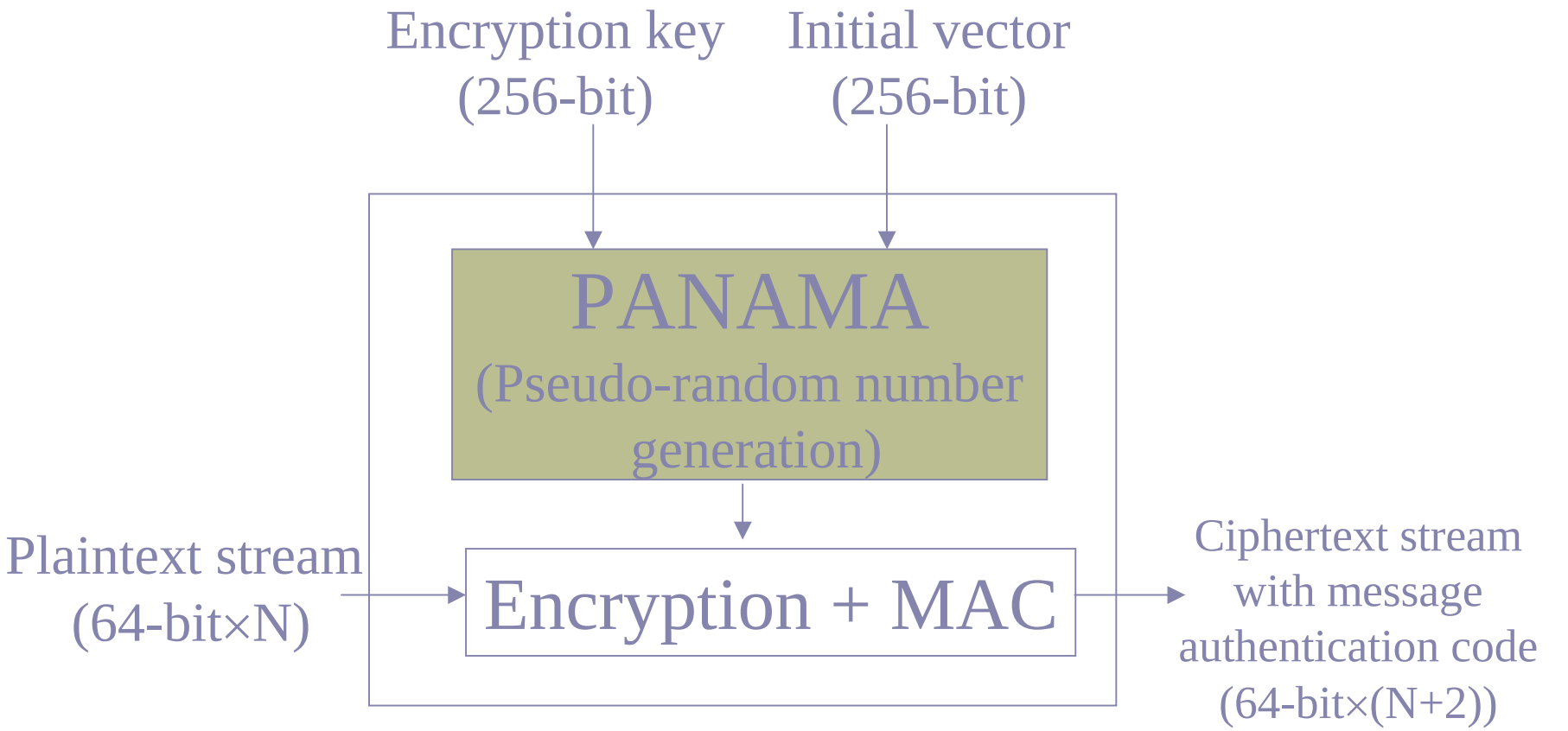
January 28, 2002

Takeshi Shimoyama,Yukiyasu Tsunoo,
Kiyomichi Araki, Members
Symmetric-Key Cryptography Subcommittee

MULTI-S01

- Presented by Hitachi, Ltd. in 2000
- Stream cipher with message authentication code (MAC)
- 256-bit key length, 256-bit initial vector
- Uses PANAMA as pseudo-random number generator in MULTI-S01

Conceptual view of MULTI-S01 (encryption)



Last year’s evaluation

- No problems have been discovered so far in terms of the cipher’s security as a stream cipher.
- The cipher has yet to undergo a rigorous evaluation by an organization such as an academic society. Thus a follow-up evaluation is necessary.
- In terms of processing speed in the SW, MULTI-S01 is among the fastest.

(CRYPTREC Report 2000)

Evaluation procedure

- The pseudo-random number generator unit (PANAMA) was evaluated separate from the encryption unit in which modes of operation are realized.
- Full evaluation details
  1. Evaluation in which MULTI-S01 is regarded as modes of operation [2]
  2. PANAMA's security against theoretical cryptanalysis [2]
  3. Randomness tests of PANAMA using a computer [1]

  (The numbers in brackets are the number of evaluators for each evaluation category.)

1. Evaluation as modes of operation

- This evaluation pertains to the relationship between security and the method of using PANAMA (the cipher component) in the MULTI-S01 device.
- This evaluation does not go so far as to examine PANAMA’s internal structure.

Modes of operation (Evaluator 1)

- The submitter's definition of *security* is insufficient.
- Security was redefined for this evaluation. Based on the evaluation results, it would seem possible to reduce from MULTI-S01's security for encryption and the impossibility of forging messages to PANAMA's properties.

Modes of operation (Evaluator 2)

- The self-evaluation does not provide appropriate descriptions of the definition of the encryption algorithm for multiple data streams, and the definition of security as a stream cipher with authentication.
- The cipher was evaluated using definitions provided by the evaluator. The evaluation results indicated that MULTI-S01's security for encryption and the impossibility of forging messages could be reduced to PANAMA.
- When MULTI-S01 was compared with "Carter-Wegman MAC" (a faster cipher with authentication that can be realized by a slight addition of bits to the ciphertext), no advantages for MULTI-S01 were observed.

2. Theoretical cryptanalysis of PANAMA

- PANAMA has a large factor in the security of MULTI-S01, so the security of PANAMA itself was evaluated from a theoretical perspective.
- PANAMA is a cipher algorithm proposed by Daemen and Clapp in 1998. It contains two components: a hash function and a pseudo-random number generator.
- Only PANAMA’s pseudo-random number generator mechanism is used by MULTI-S01. Therefore, only PANAMA’s pseudo-random number generator mechanism was evaluated.

Theoretical analysis (Evaluator 1)

- Three different simplifications (PANAMA-S1, -S2, -SM; Evaluator 1 considers PANAMA-SM to be closest to the real PANAMA) were performed, and the complexity of attack was calculated.
- PANAMA-SM can be cryptanalyzed with an amount of data proportional to 100 and a number of calculations proportional to 2^{65}. (The internal state of the cipher device can be constructed.)
- However, it would be difficult to apply this attack method to PANAMA itself.

Theoretical analysis (Evaluator 2)

- This analysis focused on PANAMA's initial vector IV (256 bits).
- An analysis of cases where a pseudo-random number sequence is generated using a different IV selected by an attacker indicated the following:
  - The same pseudo-random number sequence does not occur.
  - There are no trivial weaknesses in relation to differential attacks and related-key attacks.
- No weaknesses were discovered in PANAMA, although the short time period available for the evaluation may have been a factor.

3. PANAMA randomness tests

- PANAMA’s statistical properties were verified using NIST’s SP800-22.

What is SP800-22?

- SP800-22 is a pseudo-random number statistical testing tool and document published by NIST.
- The test output consists of 189 different “pass rates” and “distributions”.
- These tools are used for tests for AES selection.

Randomness tests (experimental results)

- There do not seem to be any particular deficiencies in PANAMA's pseudo-randomness.

* Reference information

- It was learned that the heuristic parameters may differ from those of genuine random numbers in at least two locations in the test program included with NIST's randomness test document SP800-22 (evaluations of "distribution" for test items DFT and Lempel-Ziv).

Conclusion

- MULTI-S01’s security can be reduced to the security of PANAMA.
- Fatal problems in PANAMA’s security have yet to be discovered.
- A randomness tests of PANAMA showed no particular deficiencies.