S01 latest news

Soichi Furuya
Systems Development Laboratory
Hitachi, Ltd.

Copyright 2002 Hitachi Ltd. All rights reserved.

MULTI-S01

- Stream cipher submission
- Technically, Panama + Mode of operation
- 256-bit key length
- Efficient SW/HW implementations

Copyright 2002 Hitachi Ltd. All rights reserved.

S01 publications

- A number of talks at domestic workshops from early days of its design
    1. Furuya, Sato, Takahashi, Miyazaki and Takaragi, “[illegible]” in the Proceedings of SCIS2000, Symposium on Cryptography and Information Security, SCIS2000-A17, 2000.
    2. Furuya, Takahashi, Watanabe and Takaragi, “A New Encryption Scheme with Message Authentication Employing Pseudorandom Number Generator,” Technical report of IEICE, ISEC2000-8, 2000.
    3. Furuya, Watanabe and Takaragi, “[illegible],”Technical report of IEICE, ISEC2000-68, 2000.
- Submission to CRYPTREC 2000.
- Continual evaluation algorithm at CRYPTREC 2001 (no modifications in S01’s specification)
- Specification and Evaluation reports are available via WWW.

Copyright 2002 Hitachi Ltd. All rights reserved.

S01 latest information

- Specification document update(Jan 27, 2002)
  - the definition of the ceiling function (Japanese and English docs)
  - example way of inverse function (English)
  - Panama initializing schedule (English)
  - Clearly specify the use of “Q” variable (Japanese and English docs)
  - Q is consistently called as “initial vector.” (Japanese and English docs)
  - “ai+” was corrected to be “ai+4” (Japanese)
  - “two objectives” was corrected to be “three objectives (Japanese)
  - change the electronic codes for these characters “+” and “–” (Japanese and English)
  - Change some symbols ‘ to keep consistency (Japanese)
  - Change the name of variables for decryption for easy comprehension (Japanese and English docs)
  - Referred the original paper of Panama (Japanese and English docs)
- a relevant talk at SCIS2002

Copyright 2002 Hitachi Ltd. All rights reserved.