# MUGI latest news

Soichi Furuya

Systems Development Laboratory

Hitachi, Ltd.

# MUGI

- Stream cipher submission
- Technically PRNG proposal
- 128-bit key length
- Efficient SW/ HW implementations
- Design based on Panama PRNG

# MUGI publications

- A number of talks at domestic workshops from early days of its design
  - Watanabe, Furuya, Takaragi, “The design of key stream generator using F-function of a block cipher,” in the Proceedings of SCIS2000, Symposium on Cryptography and Information Security, SCIS2001 6A-4, 2001.
  - Watanabe, Furuya, Takaragi and Seto “A Keystream Generator Suitable for Software Implementation,” Technical report of IEICE, ISEC2001-8, 2001.
  - Watanabe, Furuya, Takaragi and Seto “The correlation of the output sequence generated by the Panama-like keystream generator,” Technical report of IEICE, ISEC2001-57, 2001.
- Submission to CRYPTREC 2001.
- Specification and Evaluation reports are available via WWW.

# MUGI latest information

- Specification document update(Dec 14, 2001)
  - Revisited the definition of a data structure (Japanese)
  - The second test vector is corrected (Japanese and English docs)
- Specification of t.v. generator (Dec 14, 2001)
  - The example data is chosen so that they correspond to the key and iv shown at 3.1.
  - The index of the array **`rand_out`** was corrected.
- Specification document update(Dec 14, 2001)
  - Corrected the example of addition over GF2.
  - The definition of the symbol “∧” is corrected (the same change for the evaluation report)
- A MUGI talk at FSE2002

# test vector correction

```
key[16] =
{
0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
0x08 0x09 0x0a 0x0b 0x0c 0x0d 0x0e 0x0f
} iv[16] =
{
0xf0 0xe0 0xd0 0xc0 0xb0 0xa0 0x90 0x80
0x70 0x60 0x50 0x40 0x30 0x20 0x10 0x00
} output =
2d86a1d3 83f40baa a917564c 319d05ed
40753118 01de8aba 6d02a054 f6078bdd
4998c7cb ebc30757 76933701 bc95d2e9
ab9f8102 357ed636 c38d075a 66ddef6c
...
```

```
key[16] =
{
0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07
0x08 0x09 0x0a 0x0b 0x0c 0x0d 0x0e 0x0f
} iv[16] =
{
0xf0 0xe0 0xd0 0xc0 0xb0 0xa0 0x90 0x80
0x70 0x60 0x50 0x40 0x30 0x20 0x10 0x00
} output =
0xbc62430614b79b71, 0x71a66681c35542de,
0x7aba5b4fb80e82d7, 0x0b96982890b6e143,
0x4930b5d033157f46, 0xb96ed8499a282645,
0xdbeb1ef16d329b15, 0x34a9192c4ddcf34e,
...
```