MUGI最新情報

㈱日立製作所
システム開発研究所
古屋　聡一

MUGI

- ストリーム暗号として提案
- 技術的実態は鍵ストリーム生成器
- 鍵長128ビット
- ソフトウェア、ハードウェアで効率的
- Panama疑似乱数生成器に基づいた設計

MUGI出版物

- 設計段階から国内講演を重ねる：
  - 渡辺大，古屋聡一，宝木和夫，「F関数を利用した鍵ストリーム生成器の設計法」、暗号と情報セキュリティシンポジウムSCIS2001講演予稿集, 6A-4, 2001．
  - 渡辺大，古屋聡一，宝木和夫，瀬戸洋一，「ソフトウェアに適した擬似乱数生成器の提案」，電子情報通信学会技術研究報告, ISEC2001-8, 2001．
  - 渡辺大，古屋聡一，宝木和夫，瀬戸洋一，「PANAMA型疑似乱数生成器の乱数性，電子情報通信学会技術研究報告, ISEC2001-57, 2001．
- CRYPTREC応募者説明会
- WEBで仕様書、自己評価書などを公開

MUGI最新情報

- 仕様書の改訂（12月14日）
  - データ構造の表現の改訂（和）
  - 仕様書中のテストベクトル2例目を訂正（和英）
- テストベクトル生成プログラム仕様書（12月14日、和英）
    - 例示するデータを3.1で示した鍵、初期値の例に合わせた
    - rand_out配列の配列番号を訂正した
- 仕様書の改訂（12月14日）
  - GF2上の加算の例を正しいものに書き換えた（和英）
  - 演算子「^」の説明を訂正した（英、自己評価書も）
- FSE2002にて講演予定

テストベクトルの訂正

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,
...