

## 「日本語版MULTI-S01自己評価書」に関する

### 平成12年度からの更新情報

#### 更新情報

[1] 訂正とおわびで紹介されたエラーなどを反映しました。

| 修正箇所         | 誤                                             | 正                                             |
|--------------|-----------------------------------------------|-----------------------------------------------|
| 8 ページ 4 行目   | $B_1=(C_1\oplus F_1)\otimes A^{-1}\oplus P_1$ | $B_1=(C_1\oplus F_0)\otimes A^{-1}\oplus P_1$ |
| 8 ページ 23 行目  | $(A, B)$ の数は $2^b-1$ ...                      | $(A, B)$ の数は $2^{64}-1$ ...                   |
| 15 ページ 2 行目  | 鍵、攪拌用パラメータは、...                               | 鍵、乱数列番号は、...                                  |
| 15 ページ 4 行目  | テスト結果を表、表、表に...                               | テスト結果を表 3.2、表 3.3、表 3.4 に...                  |
| 16 ページ 23 行目 | その差分を...                                      | その差分 $a'$ を...                                |
| 18 ページ 1 行目  | 線形相関攻撃に対する...                                 | 線形攻撃に対する...                                   |
| 19 ページ 19 行目 | このことから、PANAMA の...                            | このことから、TOY2 の...                              |

[2] 3 ページ：自己評価書概要

最新情報を掲載する WEB の URL を記載しました。

[3] 13 ページ：擬似乱数生成器 PANAMA の安全性

最近の解析結果である「Panama のハッシュモードで、ハッシュ値の衝突を起こすメッセージの生成方法」に関する講演について触れ、参考文献を示しました。

[4] 21 ページ：ソフトウェア実装

MULTI-S01 のソフトウェア実装に関して、新たに Pentium(R) III プロセッサ、MAP1000 プロセッサでの実装結果について記載しました。

[5] 31 ページ：参考文献

更新情報[3]に関連して、該当情報に関連する文献を新たに参照しました。

Rijmen, V., B. Rompay, B. V., Preneel, B., Vandewalle, J., "Producing Collisions for PANAMA," Preproceedings of FSE2001, 8th Fast Software Encryption Worksop, Yokohama Japan, 2001.

[6] 文書全体

登録商標表示などを付加しました。

- Pentium は、米国およびその他の国における Intel Corp.(or Intel Corporation)またはその子会社の商標または登録商標です。
- その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。