Camellia: 様々な環境に適した 128 ビットブロック暗号

— 更新情報 —

青木和麻呂 † 市川哲也 ‡ 神田雅透 †
松井充 ‡ 盛合志帆 † 中嶋純子 ‡ 時田俊雄 ‡

† 日本電信電話株式会社
〒 239-0847 神奈川県横須賀市光の丘 1-1
{maro,kanda,shiho}@isl.ntt.co.jp

‡ 三菱電機株式会社
〒 247-8501 神奈川県鎌倉市大船 5-1-1
{ichikawa,matsui,june15,tokita}@iss.isl.melco.co.jp

2001 年 9 月 26 日

以下の内容が平成 12 年度提出の自己評価書から更新されました。

- 要旨 性能数値例を最新の情報に更新。
- 1 章 「将来の標準化活動」の段落を現状にあわせて改め、タイトルも「標準化活動」と変更。
- 3 章 実装評価を最新の情報に更新。
- 4 章 4.2.7 章 式 (3) 中の SP_1, SP_2, SP_3, SP_4 のみを用いて実装する場合の計算式の誤植を訂正。
- 5 章 ハードウェア実装評価に最新の情報を追加。
- 6 章 表 10 「Camellia の差分特性確率の上界」の FL/FL^{-1} 関数無の場合の 4 段 Camellia の評価結果の誤植を修正
- 6.2 章 (丸め差分攻撃) に最新解析結果を追加。

- 6.4 章 (不能差分利用攻撃) に最新解析結果をもとに更新。
- 6.6 章 (高階差分攻撃) 最新解析結果をもとに更新。
- 6.7 章 (スクエア攻撃) を追加。
- 6.12 章 (統計量情報による評価) に情報を追加。