Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms

– Difference from the previous version –

Kazumaro Aoki† Tetsuya Ichikawa‡ Masayuki Kanda†
Mitsuru Matsui‡ Shiho Moriai† Junko Nakajima‡ Toshio Tokita‡

†Nippon Telegraph and Telephone Corporation
1-1 Hikarinooka, Yokosuka, Kanagawa, 239-0847 Japan
{maro,kanda,shiho}@isl.ntt.co.jp

‡Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, Kanagawa, 247-8501 Japan
{ichikawa,matsui,june15,tokita}@iss.isl.melco.co.jp

September 26, 2001

The following are updated on the self-evaluation document for CRYPTREC2000 (Ver 1.0).

- Abstract was renewed with the latest performance figures.
- Section 1, the paragraph of "Future developments" was renewed based on the current status. The title was also changed into "Standardization activities".
- Section 3 was renewed with the latest performance figures.
- In Section 4.2.7, the equation to calculate Eq.(3) using only four tables, SP_1, SP_2, SP_3, SP_4, was corrected.
- Section 5 was renewed by adding the latest information on hardware evaluations.
- In Section 6.1 (Differential and Linear Cryptanalysis), an erratum in Table 10 "Upper bounds of differential characteristic probability of Camellia" (in the row of "without FL/FL^{-1}-functions") was fixed.
- Section 6.2 (Truncated Differential Cryptanalysis) was renewed by adding the recent result.
- Section 6.4 (Cryptanalysis with Impossible Differential) was renewed by adding the recent result. An erratum was also fixed: "more than 6 rounds" → "more than 5 rounds"
- Section 6.6 (Higher Order Differential Attack) was renewed based on the recent result.

- Section 6.7 (SQUARE Attack) was added.
- Section 6.12 (Statistical Tests) was renewed by adding more information.