

Cover sheet for Camellia

1 Name of submitted algorithm

Camellia

2 Type of submitted algorithm, proposed security level, and proposed environment

Type of submitted algorithm Block cipher

Proposed security level Normal (Supported key lengths are 128-, 192-, and 256-bits. Block length is 128 bits.)

Proposed environment Camellia is designed to have suitability for both software and hardware implementations and to cover all possible encryption applications that range from low-cost smart cards to high-speed network systems. A distinguished feature of Camellia is small hardware design. Also Camellia establishes high software performance in modern PC processors in the same level as that of the AES finalists.

3 Principal submitter's information

Shiho Moriai
Nippon Telegraph and Telephone Corporation
1-1 Hikarinooka, Yokosuka, Kanagawa, 239-0847 Japan
Phone: +81-468-59-2007
Fax: +81-468-59-3858
Email: shiho@isl.ntt.co.jp

4 Name of auxiliary submitter

Mitsuru Matsui (Mitsubishi Electric)

5 Names of algorithm inventors/developers

Kazumaro Aoki (NTT)
Tetsuya Ichikawa (Mitsubishi Electric)
Masayuki Kanda (NTT)
Mitsuru Matsui (Mitsubishi Electric)
Shiho Moriai (NTT)
Junko Nakajima (Mitsubishi Electric)
Toshio Tokita (Mitsubishi Electric)

6 Names of owners of the algorithm

Nippon Telegraph and Telephone Corporation
and
Mitsubishi Electric Corporation

7 Signature of submitter

Shiho Moriai

8 Backup point of contact

Nippon Telegraph and Telephone Corporation
Information Sharing Platform Laboratories
Information Security Project
1-1 Hikarinooka, Yokosuka, Kanagawa,
239-0847 Japan
Phone: +81-468-59-2007
Fax: +81-468-59-3858
Email: camellia@isl.ntt.co.jp

Mitsubishi Electric Corporation
Information Technology R&D Center
5-1-1 Ofuna, Kamakura, Kanagawa,
247-8501 Japan
Phone: +81-467-41-2180
Fax: +81-467-41-2185
Email: MISTY@isl.melco.co.jp