(Press release note)

128-bit Block Cipher "Camellia" Standardized in ISO

The 128-bit block cipher "Camellia," jointly developed in 2000 by Nippon Telegraph and Telephone Corporation (NTT) and Mitsubishi Electric Corporation (Mitsubishi), has now been selected as an international standard by ISO/IEC[*1] (ISO). It was chosen because of its recognition as a particularly secure and practical method of encryption.

Background

ISO has been focusing on standardizing its information security signature algorithm and authentication mechanisms. As of 2000, however, they had not focused on standardizing encryption algorithms; ISO had only been involved in managing registration of encryption algorithms (ISO/IEC 9979). In 2000, ISO started working on the standardization of encryption algorithms, when about fifteen nations initially proposed various algorithms. After careful investigation and evaluation of these proposals by ISO, Camellia from Japan (ISO/IEC 18033) was among six other block-cipher algorithms from four nations to be adopted as a cipher algorithm standard. Besides Camellia, ISO adopted only two other algorithms in the standardization of 128-bit block ciphers[*2]; AES[*3], a U.S. standard and SEED, a Korean standard. For Camellia, this selection by ISO is a large step forward in the development of products and services that support the next-generation of block ciphers.

Features of Camellia

Camellia is a 128-bit block size cipher (allowing key sizes of 128, 192 and 256-bits). It was developed by NTT and Mitsubishi using the following:
i)   NTT's cipher design technologies for use in high-speed software
ii)   Mitsubishi's cipher design technologies for use in compact, high-speed hardware
iii)   State-of-the-art security evaluation technology from both companies.

Camellia has a higher security margin than AES. It can also be efficiently implemented in software including 8-bit processors used in low-end smart cards, 32-bit processors widely used in PCs, and 64-bit processors used in some servers. Camellia encryption hardware offers the smallest area and best efficiency in the world among existing 128-bit block ciphers.

Camellia is now internationally recognized as the de facto Japanese standard for 128-bit block ciphers, and can compete at equivalent security and performance levels as AES. Camellia has been already been adopted by cryptographic evaluation projects such as NESSIE[*4] and CRYPTREC[*5], as well as the ongoing standardization activities at IETF[*6], authorizing Camellia encryption algorithms for use on the internet.

Camellia home page: http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
Camellia press release: http://www.ntt.co.jp/news/news00e/0003/000310.html
                         http://global.mitsubishielectric.com/news/news_releases/2000/mel0497_b.html

Future development
NTT and Mitsubishi jointly developed the next-generation block cipher "Camellia" and proposed the Camellia algorithms in both national and international standardization activities. With the adoption of Camellia by ISO, it will have been standardized in all three major encryption standardization projects: Japan (Secure E-Government), Europe (NESSIE) and global (ISO). This means Camellia will now become further widely used on a global scale.

NTT and Mitsubishi grant non-exclusively royalty-free licenses of the essential patents for Camellia under reciprocal principles in order to establish a leadership role toward achieving a low-cost secure advanced telecommunication society through the proliferation and promotion of encryption technologies that contribute to the construction of an environment in which various security products and services can be used widely. Especially, for manufacturers and applicants that develop products that support Camellia encryption algorithms whose specification is open to the public, the agreement for the royalty-free licensing of the essential patents has been prepared since 2001.

Camellia royalty-free licenses: http://www.ntt.co.jp/news/news01e/0104/010417.html

NTT and Mitsubishi shall actively promote the future development of products and services that support Camellia encryption algorithms, so that Camellia's world-highest levels of technologies become widely used.

History of Camellia
May 2005   Camellia adopted by ISO (this release)
Feb. 2003   Camellia adopted as a DRM encryption by TV-Anytime Forum
Feb. 2003   Camellia adopted by NESSIE
Feb. 2003   Camellia adopted by CRYPTREC
April 2001   Camellia royalty-free licenses prepared
March 2000   The encryption algorithm "Camellia" released by NTT and Mitsubishi

Glossary
*1 ISO/IEC
International Organization for Standardization / International Electrotechnical Commission

*2 128-bit block ciphers
These are symmetric-key encryption algorithms that process data by 128-bit block size (the size of each data bundle). Symmetric-key encryption is an encryption algorithm that uses the same key for both encryption and decryption. Since its encryption speed is fast, it is widely used to quickly encrypt large quantities of data in messages or files, and authenticate mobile terminals. There are 64-bit block ciphers that were developed before the mid 1990s and 128-bit block ciphers that were developed after late 1990s. The former examples include Triple-DES and MISTY1, while the latter examples include Camellia and AES.

*3 AES (Advanced Encryption Standard)
This is the U.S. standard 128-bit block cipher. It was standardized in the AES project (from 1997 to 2000) based on the Belgian "Rijndael" algorithms, whose security and performance levels were considered to be the highest among the proposed algorithms.

*4 NESSIE (New European Schemes for Signatures, Integrity, and Encryption)
NESSIE is a three-year project for making a portfolio of strong cryptographic primitives starting in 2000 within the Information Societies Technology (IST) Programme of the European Commission. NESSIE selected seventeen algorithms out of 44, including the 39 proposed encryption algorithms. Among the

algorithms proposed by Japan, Camellia, MISTY1 (a 64-bit block cipher developed by Mitsubishi) and PSEC-KEM (a public-key encryption algorithms developed by NTT) were adopted.

*5 CRYPTREC (Cryptography Research and Evaluation Committee)
CREPTREC was organized for investigating and evaluating cryptographic techniques suitable for the Japanese electronic government in terms of security, implementation, and other characteristics from the viewpoints of various objective specialists. 31 algorithms were selected out of 66, including 52 proposed encryption algorithms.

*6 IETF (Internet Engineering Task Force)
IETF is a large, open international community concerned with the evolution of the internet architecture (excluding WWW-related technologies). The protocol specifications standardized by IETF vary from TCP/IP to higher-level application layers. IETF is not an international standardization organization as ISO is, but the specifications standardized by IETF are considered as de facto international standards in the internet.

Contact information
Chizuka, Sano, Ida
The Public Relations Section
The Planning Department
NTT Information Sharing Laboratory Group
Nippon Telegraph and Telephone Corporation
Phone: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp

Travis Woodward
Public Relations Department
Mitsubishi Electric Corporation
Phone: 03-3218-2346
E-mail: Travis.Woodward@hq.melco.co.jp

NTT NEWS RELEASE ▶