Sony's 'CLEFIA' encryption technology adopted as an international standard

January 26 2012

Sony Corporation has been working to standardize ‘CLEFIA,’ the block cipher algorithm it developed and presented as a state-of-the-art cryptography technique in 2007, and announced today that after final ISO/IEC approval, ‘CLEFIA’ was adopted as one of the ISO/IEC 29192 International Standards in lightweight cryptography.

Information security technology to support safe and secure network access for customers has become indispensable in recent years in light of the increase in the wide range of network enabled devices. In particular, there is focus on lightweight cryptography technology suitable for ensuring the security of devices with low-power consumption requirements or those with limited hardware or memory. Under these circumstances ‘CLEFIA’ met the requirements of ISO/IEC 29192, as prescribed by ISO/IEC JTC 1/SC 27 – the organization responsible for determining the International Standards for information security.

‘CLEFIA’ has the same interface as the US government's Advanced Encryption Standard (AES). This block cipher has a block length of 128 bits, while key length can be selected from 128 bits, 192 bits or 256 bits. The most impressive feature of ‘CLEFIA’ is its realization of implementation efficiency while maintaining a high level of security. The development of ‘CLEFIA’ maintains superior security based on the latest block cipher design theory. Furthermore, ‘CLEFIA’ adopts the general Feistel structure, which is suited for implementation in constrained environments. Also, the ‘Diffusion Switching Mechanism’ (DSM) is employed to reduce processing operations whilst ensuring security. In addition, components for data processing and key scheduling part are shared. These improvements have made it possible to achieve efficient implementations in hardware and software, which had been difficult with conventional encryption technologies.

This excellent implementation efficiency enables ‘CLEFIA’ to demonstrate high performance in devices with limited resources or those with low-power consumption requirements. Accordingly, CLEFIA is suited for lightweight cryptographic applications as indicated in ISO/IEC 29192 in smartcards, RFID tags, sensor networks, medical devices and more, in addition to conventional applications.

Having been recognized as an ISO/IEC International Standard on this occasion, Sony will strive to expand the application of ‘CLEFIA’ in a variety of devices and services. Furthermore, Sony will continue its research and development in the field of lightweight cryptography, in which further progress is anticipated.

Provided by Sony Corporation

Citation: Sony's 'CLEFIA' encryption technology adopted as an international standard (2012, January 26) retrieved 3 May 2024 from https://phys.org/news/2012-01-sony-clefia-encryption-technology-international.html