Yokohama Research Laboratory

Enterprise Systems Research Dept.

Hitachi, Ltd., web site【1st Oct 2012 News Release】http://www.hitachi.com/New/cnews/121001c.html

Hitachi's light-weight "Enocoro" stream cipher adopted as an ISO/IEC standard

【Achievement】

"Enocoro" a light weight stream cipher*1 developed by Hitachi in 2007, has received final approval by ISO/IEC and has been adopted as an ISO/IEC29192*2 standard.

Since developing MULTI-2 in 1989, Hitachi has continued research in cryptography and standardization of the technology. In recent years, the stream ciphers MULTI-S01 and MUGI in 2005, and the public key cipher HIME(R) in 2006, have been adopted as international standards. With the adoption of Enocoro this time, four cryptographic algorithms developed by Hitachi have become standards.

*1)Stream cipher: A cryptographic method which encrypts data bit by bit using a random bit stream (key stream) generated by means of a private key.

*2) ISO/IEC 29192 (Light-weight cryptography): An encryption standard for implementation in constrained environments. The standard consists of 4 parts: 1) General, 2) Block ciphers, 3) Stream ciphers, and 4) Mechanism for using public key cryptography. Part 1 and Part 2 were issued on 29th May 2012 and 10th January 2012, respectively.

■ Characteristics

Compared to AES*3 the current de facto standard for data encryption, Enocoro achieves the encryption process with about one-tenth the amount of power consumption. Due to this feature, it is able to provide the basic security functions for compact control equipment and sensors used in important infrastructure, at a low cost.

■ Plan

Through its cipher technology including Enocoro, Hitachi will continue research on technologies for a reliable networked society to improve security as important infrastructure and industrial systems become increasingly connected.

*3)Advanced Encryption Standard: An encryption standard adopted by the US government in 2001, and the de facto world standard for data encryption. AES was ratified after 3 years of open public assessment sponsored by the National Institute of Standards and Technology (NIST).