FOR IMMEDIATE RELEASE

Chaskey Message Authentication Technology Developed for IoT Systems Supporting Key Infrastructure Adopted by ISO/IEC for Lightweight Cryptography

Enables high-speed processing with little memory when compared with standard encryption technologies

Tokyo, September 20, 2019, Hitachi, Ltd. (TSE: 6501; “Hitachi”) and KU Leuven today announced that Chaskey, the jointly developed message authentication technology for small IoT devices such as sensors or controllers, was adopted as international standard for lightweight cryptography ISO/IEC[*1] 29192-6, after obtaining final approval from the International Organization for Standardization (“ISO”). The standardization was made possible with the cooperation of the National Institute of Advanced Industrial Science and Technology (“AIST”, Japan). Chaskey enables high-speed processing with less memory than other cryptographic technologies. The standard enables the introduction of security to small components of critical infrastructure and vehicle systems resulting in an overall more secure infrastructure.

The development of IoT technology has connected a broad range of devices to the Internet, which has enabled convenient and ubiquitous access to information. However, this has also led to an increased need for security management, to prevent the leakage of information and to protect the privacy of users. During the last years, ISO has been working the standard ISO/IEC 29192 that specifies lightweight cryptography for small IoT devices. In order to manage IoT systems safely in real time, there is a need for fast and authenticated transfer of sensor and control information in order to enable correct and in-time control decisions. However, computational and memory resources in small IoT devices are limited. This creates a need for new cryptographic algorithms that are fast and that require limited memory. Together Hitachi and KU Leuven have developed the Chaskey algorithm that can protect authenticity of information in small IoT devices. Chaskey requires five time less memory and is two to seven times faster than current standards. Chaskey can be characterized as follows.

1. Parameter selection technology that realizes high speeds with various CPUs.
Chaskey utilizes the ARX design*2 that uses the basic operations present in every CPU. The ARX design yields a small memory footprint and uses operations that are aligned with the register size of the CPU. The KU Leuven has developed a special tool that allows to fine-tune the parameters of the algorithm to achieve high-speed processing with 8-bit to 32-bit CPUs present in small IoT devices.

2. Construction of message authentication function suited to IoT data processing
With IoT systems, there is a need for low latency data processing of short strings for sensor data and control commands. There is also a need to quickly change cryptographic keys, which is known as key agility. It has been shown that the Even-Mansour technique developed for block ciphers can be used in Chaskey to achieve fast and secure key expansion resulting in a very high key agility.

Starting with Chaskey, Hitachi and KU Leuven will apply cryptographic technology to innovative products, and will continue their research collaboration on critical infrastructure security in order to create a safe and secure digital society.

Note: *1 IEC: International Electrotechnical Commission

*2 ARX (Addition-Rotation-XORing) design: a method that organizes processing only with addition, rotation, and logical operations installed in most CPUs.

About Hitachi, Ltd.

Hitachi, Ltd. (TSE: 6501), headquartered in Tokyo, Japan, is focusing on Social Innovation Business combining its operational technology, information technology and products. The company's consolidated revenues for fiscal 2018 (ended March 31, 2019) totaled 9,480.6 billion yen ($85.4 billion), and the company has approximately 296,000 employees worldwide. Hitachi delivers digital solutions utilizing Lumada in five sectors including Mobility, Smart Life, Industry, Energy and IT, to increase our customer's social, environmental and economic value. For more information on Hitachi, please visit the company's website at https://www.hitachi.com.

About KU Leuven

KU Leuven is Europe's most innovative university. Located in Belgium, it is dedicated to research, education, and service to society. KU Leuven is a founding member of the League of European Research Universities (LERU) and has a strong European and international orientation. Our scientists conduct basic and applied research in a comprehensive range of disciplines. University Hospitals Leuven, our network of research hospitals, provides high-quality healthcare and develops new therapeutic and diagnostic insights with an emphasis on translational research. The university welcomes more than 50,000 students from over 140 countries. The KU Leuven Doctoral Schools train approximately 4,500 PhD students.
https://www.kuleuven.be/english/

For more information regarding this release

Research & Development Group, Hitachi, Ltd.
Inquiries form: https://www8.hitachi.co.jp/inquiry/hqrd/news/en/form.jsp

###

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
