Lightweight Cryptography Applicable to Various IoT Devices

OKAMURA Toshihiko

Abstract

With the IoT systems that make use of data in the real world, the data collection from devices can also be a target of cyberattacks. It is because of this that countermeasures based on encryption are currently gaining in importance. Lightweight cryptography is an encryption method that features a small footprint and/or low computational complexity. It is aimed at expanding the applications of cryptography to constrained devices and its related international standardization and guidelines compilation are currently underway. Authenticated encryption that achieves both confidentiality and integrity has been attracting special attention and a technology competition called CAESAR has been held. NEC has developed TWINE, which is a lightweight block cipher, and OTR, which is an authenticated encryption method that has passed the CAESAR second-round selection.

Keywords

security, encryption, authentication, lightweight cryptography, authenticated encryption

1. Introduction

The IoT has created new values by connecting various devices to the network, but has also led to security threat becoming important issues as seen in the recent reports of illegal surveillance camera manipulation and automobile hacking etc. The Information-technology Promotion Agency of Japan (IPA) has ranked "Exteriorization of vulnerability of IoT devices" as 8th in its report entitled "The 10 Major Security Threats of 2017."

Encryption is an effective countermeasure, and the IoT is now required to apply encryption to sensor devices in environments with various restrictions that have not previously been subject to encryption. Lightweight cryptography is a technology researched and developed to respond to this issue. In this paper the author will describe the security threats of IoT and discuss the countermeasures that are based on encryption. We discuss the requirements of lightweight cryptography, the technology and trends, the block cypher TWINE and authenticated encryption OTR that have been developed by NEC.

2. Security Threats for IoT, Countermeasures Based on Encryption

The biggest security-related threat of IoT systems from the traditional IT systems is that even using devices for data collection from the real world can become a target of cyberattacks. For example, the purpose of applying IoT to a plant is to significantly improve the productivity and maintainability by collecting data from a large number of sensors installed in production equipment, by analyzing it and performing autonomous control in real time. If sensor data should be falsified during this process, incorrect analysis results would be induced and erroneous control would result due to such an occurrence having the potential of leading to major damage. Moreover, since measurement data and control commands are trade secrets associated with the know-how of production and management, preventing leakages is also important from the viewpoint of competitiveness. Even if there is no problem at present, it is necessary to consider the effect of threats that might become evident in the future.

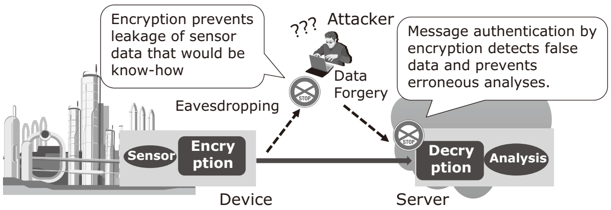
Encryption prevents leakage of sensor data that would be know-how
???
Attacker
Message authentication by encryption detects false data and prevents erroneous analyses.
Data Forgery
Eavesdropping
STOP
Sensor
Encry ption
Decry ption
Analysis
Device
Server

Fig. 1 Encryption-based countermeasure against attack on data collection.

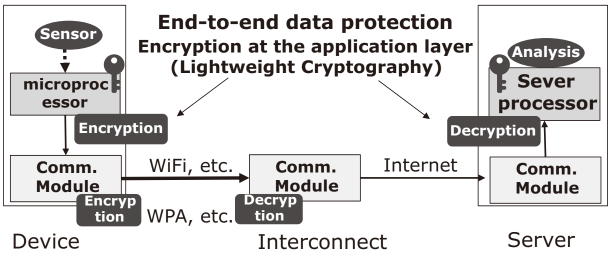

Fig. 2 Example of lightweight cryptography applications.

Applying encryption to sensor devices means the implementation of data protection for confidentiality and integrity, which can be an effective countermeasure against the threats (**Fig. 1**). Lightweight cryptography has the function of enabling the application of secure encryption, even for devices with limited resources.

Encryption is already applied as standard on the data link layer of communication systems such as the cellphone. Even in such a case, encryption in the application layer is effective in providing end-to-end data protection from the device to the server and to ensure security independently from the communication system (**Fig. 2**). Then encryption must be applied at the processor processing the application and on unused resources and hence should desirably be as lightweight as possible.

3. Lightweight Cryptography

3.1 Requirements for Lightweight Cryptography

The following factors on the implementation are required for lightweight cryptography.

- Size (circuit size, ROM/RAM sizes)
- Power
- Power consumption
- Processing speed (throughput, delay)

The first factor determining the possibility of implementation in a device is the size. Power is especially important with the RFID and energy harvesting devices while the power consumption is important with battery-driven devices. A high throughput is necessary for devices with large data transmissions such as a camera or a vibration sensor, while a low delay is important for the real-time control processing of a car-control system, etc.

Since the power is greatly dependent on the hardware such as the circuit size or the processor in use, the size becomes the reference point for the lightness of the encryption method and also for the power. The power consumption is dependent on the processing speed because of the execution time, so the number of computations that determines the processing speed becomes the index of the lightness. The throughput depends greatly on the parallel processing capability.

With regard to security, since encryption is the technological point of origin of the overall system security the lightweight cryptography needs to adopt a method that is evaluated as having a sufficient security level of modern cryptography. Even when the block length and/or secret key length are set shorter than for the standard cryptography by prioritizing the ease of implementation (such as via 64-bit block and 80-bit secret key, for example,) it is still required to correctly apply a proven method.

3.2 Symmetric Key and Public Key Cryptographies

Cryptography can roughly be divided into symmetric key and public key (asymmetric key) cryptographies. The symmetric key cryptography uses the same secret key for encryption and decryption. With the processing that is relatively lightweight, it is used in data encryption and authentication. On the other hand, public key cryptography uses a secret key in decryption and a public key different from the secret key in encryption, and it is quite difficult to guess the secret key from the public key. The computational complexity of the public key cryptography is typically as high as more than 1,000 times that of the symmetric key cryptography, but this technology is used in sharing the secret key used in symmetric key cryptography and the digital signature, thanks to the asymmetrical property.

With a system such as a plant or car- control system, it may be possible to embed the secret keys shared by the devices in advance. In such a case, secure and efficient data protection can be implemented using symmetric key cryptography alone. On the other hand, with a system that performs encrypted communications dynamically with unspecified parties such as an inter-vehicle communication system, the use of public key cryptography is effective.

We focus mainly on the symmetric key cryptography

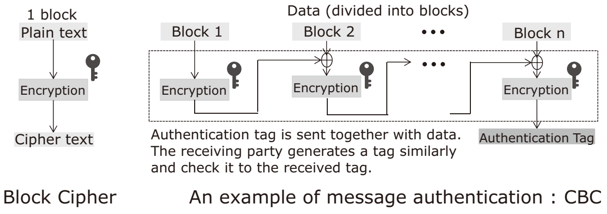
1 block
Plain text
Encryption
Cipher text
Data (divided into blocks)
Block 1
Block 2
•••
Block n
Encryption
Encryption
•••
Encryption
Authentication tag is sent together with data.
The receiving party generates a tag similarly
and check it to the received tag.
Authentication Tag
Block Cipher
An example of message authentication : CBC

Fig. 3 An Example of block cipher mode of operation.

that can be widely applied to devices that are subject to severe resource restrictions. The symmetric key cryptography consists of core functions such as block or stream ciphers (cryptographic primitives) and methods to apply the core function to a packet called the block cipher mode of operation for encryption and/or authentication. **Fig. 3** shows an example of the block cipher mode of operation used for the authentication (called CBC-MAC: cipher block chaining message authentication code). To render a cryptography lightweight, it is required to improve the efficiency of the block cipher mode of operation as well as the cryptographic primitives.

3.3 Trends in Lightweight Cryptography

R&D of lightweight cryptography was begun around 2004 with a project in Europe and it has recently been reactivated via the M2M/IoT process. The international standard ISO/IEC 29192 "Lightweight Cryptography" was established at ISO/IEC JTC 1/SC 27. The U.S. National Institute of Standards and Technology (NIST) that issues guidelines on cryptographic technologies initiated the Lightweight Cryptography Project in 2013 and announced a public call for applications of lightweight cryptographies in 2017.

PRESENT is a block cipher regarded as being the precursor of lightweight cryptography. It was published in 2007 and has been registered in ISO/IEC 29192. It has a small circuit size that enables implementation in the RFID tag, which is not possible using the standard AES encryption. The U.S. National Security Agency (NSA) published lightweight block cipher SIMON/SPECK that features a very small ROM size suitable to a constrained microprocessor (2013) and proposed its addition to ISO/IEC 29192 with the aim of achieving international standardization.

A block cipher mode of operation that can achieve both encryption and message authentication is called "authenticated encryption." Considering the importance of false data detection in IoT, it is expected that encryption will mean authenticated encryption in the future. Even when the same block cipher is used, the efficiency and the security vary considerably depending on how it is implemented as an authenticated encryption. There exist NIST-recommended authenticated encryptions called the AES-CCM/GCM, but considering the importance of authenticated encryption and the progress in research, next-generation authenticated encryptions of lighter weight and higher security are desirable. Under these circumstances, an international authenticated encryption competition called CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) was started with NIST's support in 2014 and there were 60 submissions. Candidates have been narrowed down every year in accordance with the algorithm characteristics and functions, and the final selection will be published by the end of 2017.

In Japan, the CRYPTREC (Cryptography Research and Evaluation Committee) assesses electronic government-recommended ciphers and monitors the trends of cryptographic technologies. Its Lightweight Cryptography WG has been developing its activities since 2013. These include the evaluation of the implementation of representative block ciphers, as well as security surveys and research into the effective use of lightweight cryptographies.

4. Lightweight Cryptographies of NEC

4.1 Block Cipher TWINE

NEC's lightweight block cipher called TWINE[1)] is designed to solve issues with the previous lightweight cryptography PRESENT by its ease of implementation in software. At the same time its implementation will be enabled in small-size circuitry. It employs the same setting as for PRESENT, namely a block length of 64 bits and two kinds of secret key lengths of 80 and 128 bits.

TWINE was selected as one of the ciphers to be evaluated by the Lightweight Cryptography WG of CYRPTREC described in the above, and manifested top-class performances in both hardware and software. Below, we will discuss the implementation of TWINE based on the results of evaluation by the Lightweight Cryptography WG.

The block cipher is composed of algorithms that repeat the same processing procedures known as the round functions. With regard to hardware implementation, the circuit sizeper round of AES is 15K gates but that of TWINE is about 2K gates, which is about 1/7th that of AES (of a similar scale to PRESENT). When the circuit size per throughput is compared, the efficiency of TWINE is more than twice that of AES. For the high-speed communication compatibility, encryption increases the circuit scale due to parallel processing, but the small-scale circuitry of TWINE is also effective in such a case.

On the other hand, AES is superior in terms of software implementation. In the case of the microproecessor (Renesas RL78) implementation, it is faster than the lightweight cryptographies including TWINE when the ROM is 1K bytes or more. However, when the ROM size is 512 bytes, AES cannot be implemented but TWINE can. Compared to PRESENT, the processing speed achieved by TWINE is higher at 250%.

Regarding the security, we evaluated TWINE on the attacks used in modern cryptanalysis like the AES evaluation and showed no problems. Some papers attempting to attack TWINE have been issued, but none of them succeeded in degrading the security level of TWINE up to the present.

4.2 Authenticated Encryption OTR

In general, the amount of computation required for message authentication is equivalent to that for encryption (secrecy), and the computation amount of AES-CCM/GCM, NIST-recommended authenticated encryptions, is twice the amount required for merely encryption. Since the computation amount of authenticated encryption is more than that for encryption alone, the computation amount equivalent to that for encryption alone becomes the theoretical limit for authenticated encryptions.

OCB is an authenticated encryption that can clear the theoretical limit, but it necessitates a block cipher decryption function to perform decryption. On the other hand, as is evident in the fact that AES-CCM configures the decryption processing via the block cipher encryption function, the size can be reduced by reducing the number of its composite elements. OTR[2)] developed by NEC is the world's first authenticated encryption that achieves the theoretical limit of computation amount using only block cipher encryption functions exclusively. OTR was proposed in the CAESAR authenticated encryption competition mentioned above, and it was selected as one of 30 candidates passing the first round (2015) and also as one of 15 ones passing the second round (2016).

Fig. 4 shows the algorithm of OTR. The message authentication (authentication tag generation) of OTR is based on encryption of checksum of data blocks and can be implemented by encryption of a single block regardless of the data length. The encryption employs a structure called the 2R Feistel structure and decryption is possible using the block cipher encryption functions as in encryption.

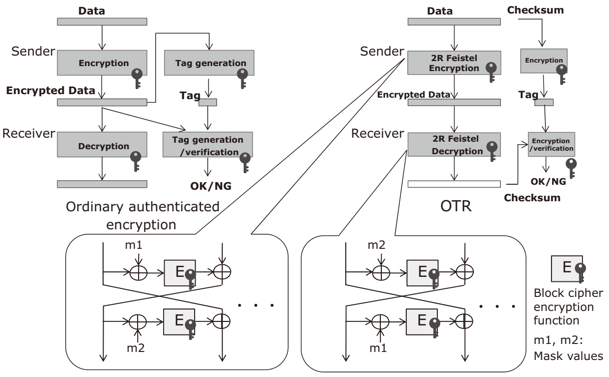

Fig. 4 OTR algorithms.

The security of OTR is proved based on that of the block cipher. OTR can be combined with an arbitrary block cipher. As combination with AES makes it possible to use the rich implementation assets of AES, and "AES-OTR" has been proposed to the CAESAR. Combination with TWINE, "TWINE-OTR" can reduce the size further compared to AES-OTR.

At NEC, we developed authenticated encryption CLOC/SILC jointly with Nagoya University et al. CLOC/SILC features a small surplus of computation amount compared to the small data size. It was also proposed to CAESAR and passed the second-round selection.

5. Conclusion

In the above, we introduced the lightweight cryptographies applicable to the resource-constrained environments of IoT by focusing on the ones developed by NEC. Lightweight cryptography also requires consideration of the key management functions and operations in actual applications. NEC is therefore promoting R&D for the practical realization of a lightweight cryptography library by also covering updating and exchanging of keys. We are also conducting research into lightweight cryptography in key exchange based on public key encryption. In the future, we intend to continue to contribute to secure IoT systems via research into the cryptographic technologies as discussed in this paper.

Reference

1) T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi: TWINE: A lightweight block cipher for multiple platforms, SAC 2012.
2) K. Minematsu: Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions, EUROCRYPT 2014

Authors' Profiles

OKAMURA Toshihiko

Principal Researcher
Security Research Laboratories

The details about this paper can be seen at the following.

Related URL:

NEC develops authenticated encryption technology for IoT sensors and devices
http://www.nec.com/en/press/201507/global_20150721_04.html

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.1 IoT That Supports Digital Businesses

Remarks for Special Issue on IoT That Supports Digital Businesses
NEC's IoT Operations That Support Digital Businesses

Papers for Special Issue

Platforms built to support IoT

An IoT Platform to Support Business Transformation - "NEC the WISE IoT Platform"
Edge Computing Supporting Customer Values in the IoT Era
Edge Computing Technologies to Connect the Missing Link of IoT
Case Studies of Edge Computing Solutions

IoT solutions that offer value to customers

NEC Industrial IoT - For Manufacturing in the Age of IoT
Warehouse Product Inspection System Achieves Work Efficiency and Quality Improvements
Warehouse Staffing Optimization Solution Using Autonomous and Adaptive Control - NEC's latest AI technology
Human-Oriented IoT Solutions Using Hearable Technology from NEC
Video Streaming Technology That Supports Public Safety
IoT and AI Innovations for the Retail Industry
Wireless Networking Technology for Real-time Remote Control of Factory Equipment: Wireless ExpEther
Lightweight Cryptography Applicable to Various IoT Devices
PoC of AI Demand Forecast Deployment in the NEC Group's Manufacturing Facilities from an Ethnographical Perspective

General Paper

"My Number" Collection Service Utilizes Several Key Image Recognition Technologies

\Orchestrating a brighter world NEC
NEC Technical Journal
IoT That Supports Digital Businesses
Vol.12 No.1

Vol.12 No.1
October 2017

Special Issue TOP