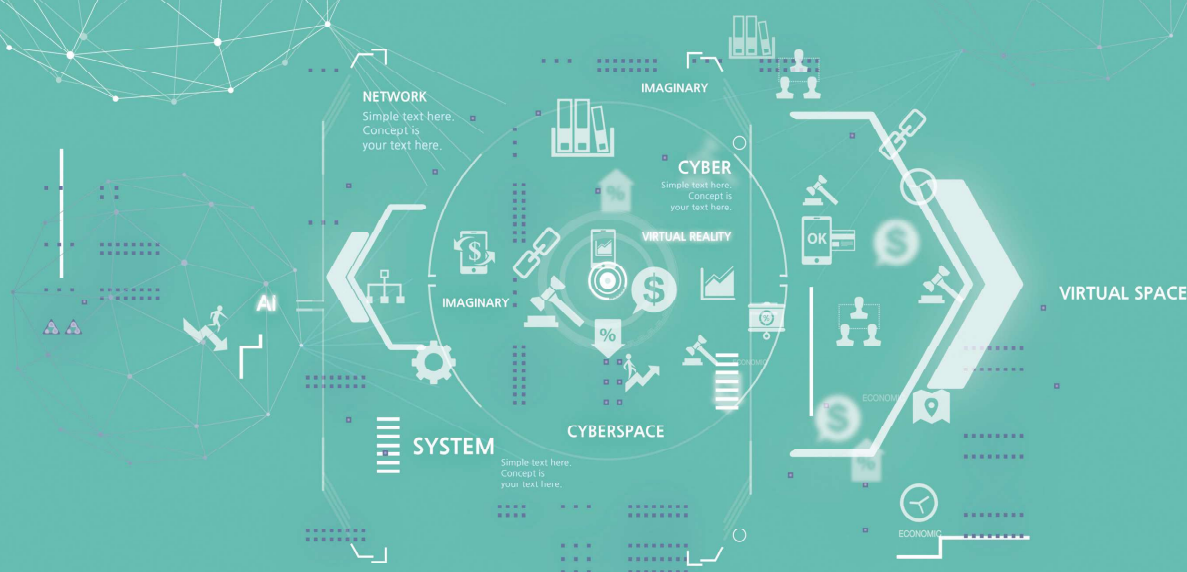




2019 International Conference on Platform Technology and Service

28-30 January, 2019, Jeju, Korea

PlatCon-19

Proceedings

IEEE Catalog Number : CFP19B77-ART (Xplore)
ISBN : 978-1-7281-1288-6 (Xplore)
IEEE Catalog Number : CFP19B77-CDR (CD-ROM)
ISBN : 978-1-7281-1287-9 (CD-ROM)

Multi-Label Bias-Based Predictor	61
<i>Tae-gyu Hwang; Sung-Kwon Kim</i>	
A Study on the Needs for Enhancement of Personal Information Protection in Cloud Computing Security Certification System	66
<i>Min Ju Kang; Hun-Yeong Kwon</i>	
TAPS: Trust-based Access Control and Protect System	71
<i>Yoon-Sik Yoo; Hyungkyu Lee; Boo-Geum Jung; HeaSook Park; Kiwon Kim; Cheong Hee Park</i>	
Security Evaluation Methodology for Software Defined Network Solutions	76
<i>Jean Nikoue; Sergey Butakov; Yasir Malik</i>	
Semantic Analysis of NIH Stroke Scale Using Machine Learning Techniques	82
<i>Jaehak Yu; Da mee Kim; HongKyu Park; Seung-chul Chon; Kang Hee Cho; Se-Jin Park; Sunjin Kim; Sungkyu Yu; Seung Hee Hong</i>	
 <u>Future Security and Privacy</u>	
Simulation System of a Reservation-Based 3D Intersection Crossing Scheme for UAVs	87
<i>Areeya Rubenecia; Myungwhan Choi; Hyo Hyun Choi</i>	
Dynamic Frame Length Adaptation for Anti-Collision Management in Wi-Fi Backscatter System	92
<i>Jung-Hyok Kwon; Sang-Woo Lee; Eui-Jik Kim</i>	
Digital Forensic Artifact Collection Technique Using Application Decompilation	94
<i>Dongkyun Yoo; Yeonghun Shin; SungJin Kim; Hyunjin Kim; Sungmoon Kwon; Taeshik Shon</i>	
Digital Forensic Analysis Using Android Application Cache Data	97
<i>Hyungchan Kim; Donghyun Kim; Wooyeon Jo; Taeshik Shon</i>	
Digital Forensic Readiness for Financial Network	101
<i>Sungmoon Kwon; Jaehan Jeong; Taeshik Shon</i>	
Cyber Attack Scenarios on Smart City and Their Ripple Effects	105
<i>JooChan Lee; JangHoon Kim; Jung Taek Seo</i>	
A Study on IoT Device Authentication Protocol for High Speed and Lightweight	110
<i>Seul-Ki Choi; Ju-Seong Ko; Jin Kwak</i>	

A Study on IoT Device Authentication Protocol for High Speed and Lightweight

Seul-Ki Choi

ISAA Lab. Dept. of Computer Engineering
Ajou University
Suwon, Republic of Korea
skchoi.isaa@gmail.com

Ju-Seong Ko

ISAA Lab. Dept. of Computer Engineering
Ajou University
Suwon, Republic of Korea
jsko.isaa@gmail.com

Jin Kwak

Dept. of Cyber Security
Ajou University
Suwon, Republic of Korea
security@ajou.ac.kr

Abstract— In Authentication to IoT devices is a very important step in providing secure IoT services. Accordingly, studies on an authentication protocol suitable for low-power and low-performance IoT devices are being actively conducted. Therefore, in this paper, we have selected the LEA-128-CTR and Chaskey algorithms to increase the high-speed parallelization effect of SIMD-based IoT device authentication protocol and proposed protocol for light weight and high speed

Keywords—SIMD, authentication protocol, lightweight protocol, mobile security, IoT security, network security

I. INTRODUCTION

Recently, the convenience of life has been increased by providing various IoT services based on IoT devices. IoT services continue to expand, ranging from smart homes and smart medical environments that use dozens of IoT devices to smart factories and smart city services that connect hundreds to thousands of multiple IoT devices. However, these IoT services are continuously threatened by various malicious codes because they are technologies that actively utilize IT technology.

Figure 1 below shows the statistics of malicious code that occurred in McAfee Labs Threats Reports from McAfee Labs in December 2018 until the third quarter of 2018[1].

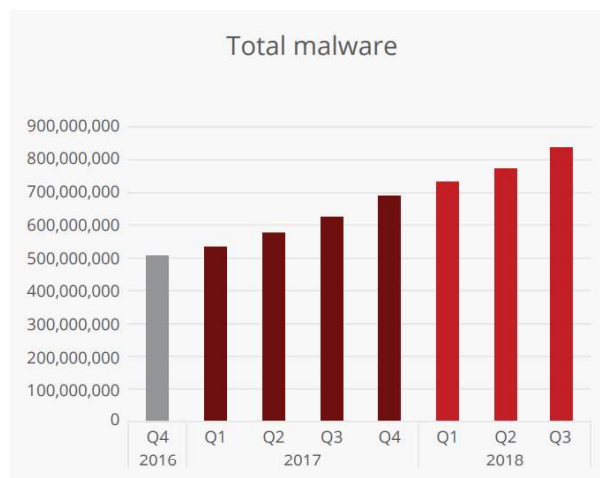


Fig. 1. Total number of malicious codes (until 2018 Q3)

And Figure 2 below shows the number of IoT malicious codes that occurred until the third quarter of 2018[1].

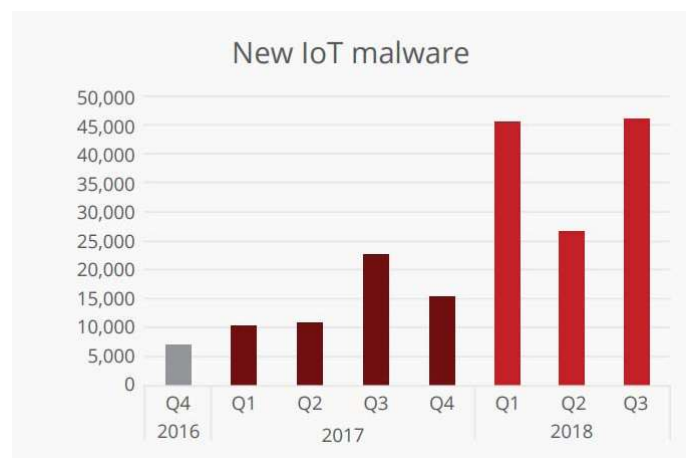


Fig. 2. Number of IoT malicious codes (until 2018 Q3)

The statistical data in Figure 2 shows that the malicious code for the IoT environment increased sharply in 2018. Therefore, research is needed to strengthen the authentication protocol for IoT devices in order to provide a secure IoT environment from rapidly increasing IoT malicious codes. However, since the performance of the IoT device is not good enough to apply the existing authentication protocol, the lightweight of the authentication protocol should be considered. Therefore, this paper proposes a high-speed and lightweight authentication protocol suitable for IoT devices.

II. RELATED WORKS

A. SIMD

SIMD stands for Single Instruction Multiple Data. It refers to a technique for simultaneously processing multiple data with a single instruction.

It is often used in the multimedia field, such as graphics related processing. CPUs that provide SIMD include Intel's MMX, SSE series, and ARM-developed NEON. SIMD has the advantage of improving the processing speed efficiency when processing a larger amount of data than the single instruction

single data (SISD) method, which is generally used in general programs. Figure 3 shows the SISD and SIMD processing structure.

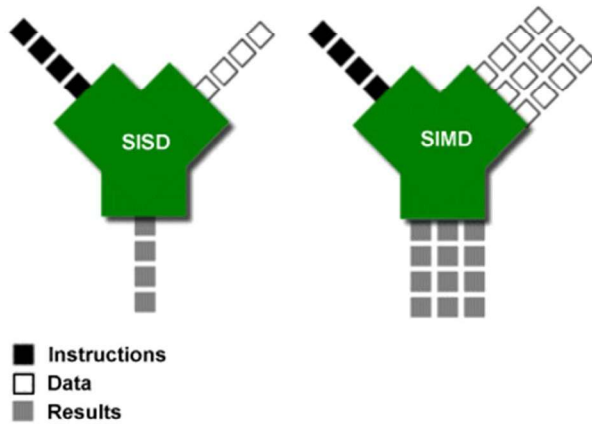


Fig. 3. Processing structure of SISD and SIMD

B. Chaskey

The Chaskey MAC (Message Authentication Code) algorithm is a MAC algorithm that can be used in a 32-bit microcontroller. By eliminating key scheduling, it reduces the number of cycles required for encryption[2]. In addition, it is composed of only ARX(Addition, Rotation, XOR) operation and has a very fast execution speed[2].

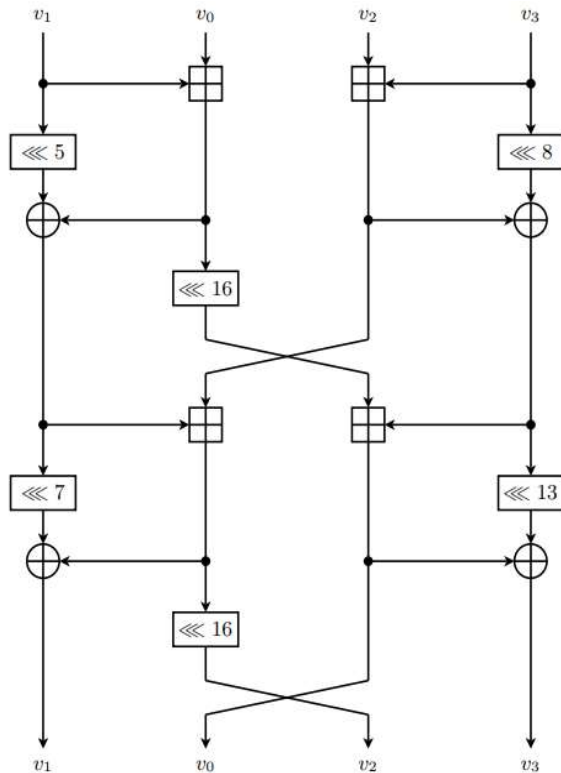


Fig. 4. A round of the Chaskey permutation

Chaskey MAC Algorithm has the following features

- **Dedicated Design:** Chaskey is a dedicated design for 32-bit microcontroller architectures. The addition and XOR operations are performed on 32-bit words, and each of these operations requires only one instruction on these architectures.
- **Cross-Platform Versatility:** Nicky et al took into account that certain microcontrollers do not support variable-length bit rotations and bit shifts. By choosing some rotation constants to be multiples of 8, these bit rotations are efficiently implemented by swapping 8-bit or 16-bit registers.
- **Efficient Implementation:** Benchmarks on an ARM Cortex-M4 show that Chaskey requires only 7.0 cycles/byte for long (≥ 128 byte) messages, and 10.6 cycles/byte for short (16 byte) messages. It has been implemented in only 402 bytes of ROM. Results for the Cortex-M0 are very good as well: 16.9 cycles/byte for long messages, 21.3 cycles/byte for short ones, and 414 bytes of ROM for the implementation.
- **Resistance Against Timing Attack:** On all microcontroller architectures that Nicky et al are aware of, every instruction of Chaskey takes a constant time to execute. The total number of cycles depends only on the message length. Therefore, Chaskey is inherently secure against timing attacks.
- **Key Agility:** Chaskey does not have a key schedule, as keys are simply XORed into the state. Updating the key in Chaskey requires generating a new uniformly random 128-bit key, and only two shifts and two conditional XORs on 128-bit words to generate two subkeys.
- **Tag Truncation:** Chaskey is robust under tag truncation.
- **Nonces are Optional:** Several MAC algorithms require a nonce, and become completely insecure if this nonce is reused. Chaskey does not require a nonce, and therefore avoids these issues altogether.

C. LEA

Hong et al propose a new block cipher LEA, which has 128-bit block size and 128, 192, or 256-bit key size[3].

It provides a high-speed software encryption on general-purpose processors. They show that LEA is faster than AES on Intel, AMD, ARM, and ColdFire platforms[3]. LEA can be also implemented to have tiny code size[3]. Its hardware implementation has a competitive throughput per area. It is secure against all the existing attacks on block ciphers[3]. LEA consists of only ARX(modular Addition, bitwise Rotation, and bitwise XOR) operations for 32-bit words. Those operations are well-supported and fast in many 32-bit and 64-bit platforms[3].

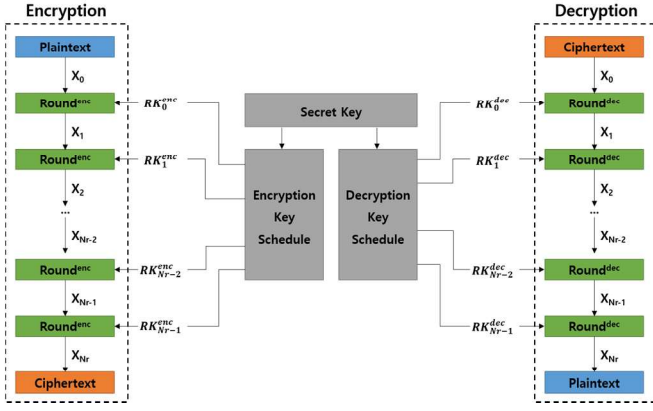


Fig. 5. LEA encryption and decryption process

III. PROPOSED SCHEME

A. Applicable Target Processor in IoT industry

The SIMD-based authentication protocol proposed in this paper is applied to the ARM processor which is widely distributed and distributed in various IoT devices. Among them, IoT devices that collect information from these IoT sensors and perform their own processing or processing themselves, rather than IoT sensors that perform only information gathering functions, are the subjects of this paper. These IoT devices are equipped with Cortex A or higher processors among the ARM processors. Table 1 below shows examples of IoT industry devices that are equipped with Cortex A processor[4].

TABLE I. MAJOR DEVICE AND PROCESSOR TYPE BY IoT INDUSTRY SECTOR

Industry	Table Column Head
Smart home	Home gateway (Cortex A9) Thermostat (Cortex A8)
Medical	Smart watch (Cortex A9)
Tranportation	Automovoice sensor (Cortex A9) Electronic Control Unit (Cortex A9)

Industry	Table Column Head
Energy	Remote Terminal Unit (Cortex A9)

B. SIMD-based Authenticaion Protocol

The proposed protocol utilizes a pre-shared key distribution scheme considering low-power and low-performance IoT devices. The notation used in the protocol is shown in Table 2 below.

TABLE II. A DESCRIPTION OF NOTATION USED IN PROTOCOL

Notation	Description
ID_x	Identifier(ID) of x
EA_Data	Extra-Authentication data (fingerprint, iris etc.)
T	Timestamp
N_x	Nonce value generated by x
PSK	Pre-Shared Key
SK	Session Key
$E_k(...)$	Encryption with k
$D_k(...)$	Decryption with k
$MAC_k(...)$	Generate MAC with k
$Device$	IoT device
$Verifier$	Verifier (gateway or user device)

Figure 6 shows the overall process of an SIMD-based authentication protocol.

In order to speed up the protocol proposed in this paper, a cryptographic algorithm and a MAC algorithm suitable for parallel processing are selected. The selected algorithms can improve performance by actively utilizing Neon, the SIMD technology provided by ARM Cortex A.

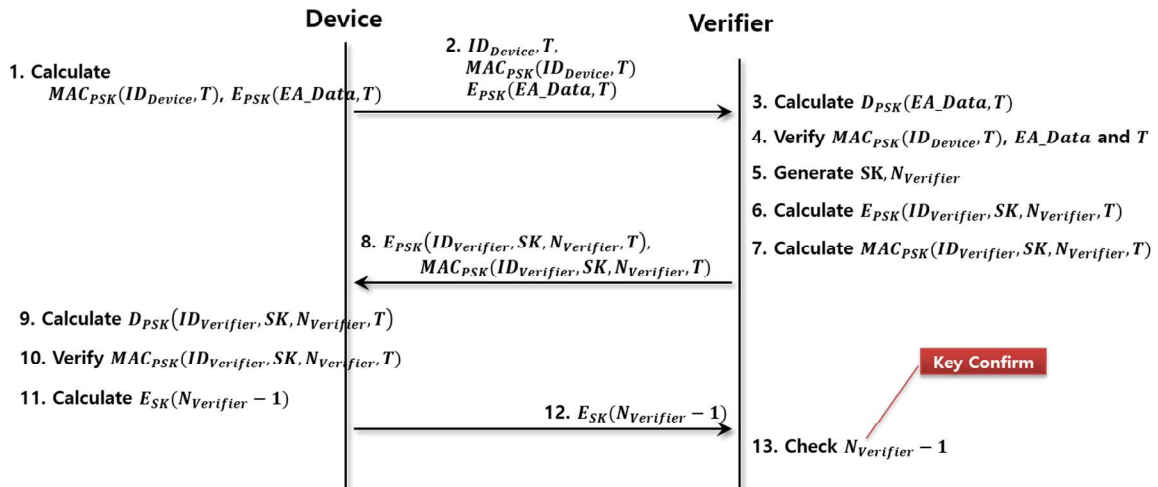


Fig. 6. Overall process of proposed authentication protocol

- Encryption/Decryption algorithm: LEA-128-CTR
- MAC algorithm: Chaskey

The LEA-128-CTR is composed of only ARX operation. In the CTR mode, it is possible to parallelize both encryption and decryption, so it can be speeded up by using SIMD, and code size can be minimized because only encryption code is required.

In addition, the Chaskey algorithm is composed of only ARX operations, and is a high-speed MAC algorithm adapted to a 32-bit microcontroller. In addition, since there is no key scheduling process, the code size can be minimized.

C. Security Analysis

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

The security of the proposed protocol in this paper is based on the security of PSK distributed in advance. Therefore, the following assumptions are essential for the proposed protocol.

- Assumption 1) The process of distributing the PSK in advance is a perfectly secure process.
- Assumption 2) Each Entities(Device, Verifier etc.) are managing the PSK securely.

When the above assumptions are followed, the protocol can be secured against representative attacks on the authentication protocol.

The step number and data transmitted in the proposed protocol are as follows. These messages are also the only information an adversary can acquire.

- ② $ID_{Device}, T, MAC_{PSK}(\dots), E_{PSK}(\dots)$
- ⑧ $E_{PSK}(\dots), MAC_{PSK}(\dots)$
- ⑫ $E_{SK}(\dots)$

- Eavesdropping Attack

Significant information that an adversary can obtain through eavesdropping attack during the authentication process of the proposed protocol is only the ID_{Device} and the T value. However, these information are either public or temporary. Therefore, confidential information (PSK, SK, EA_Data etc.) is not exposed by eavesdropping attack.

- Replay Attack

The following figure shows an example of a Replay attack. The only messages that adversary can use in replay attacks are the messages obtained in steps ②, ⑧ and ⑫. However, each message contains a timestamp and a nonce value that can be used to verify the time validity of the message. Therefore, a replay attack can be prevented by verifying the message as shown in Figure 7.

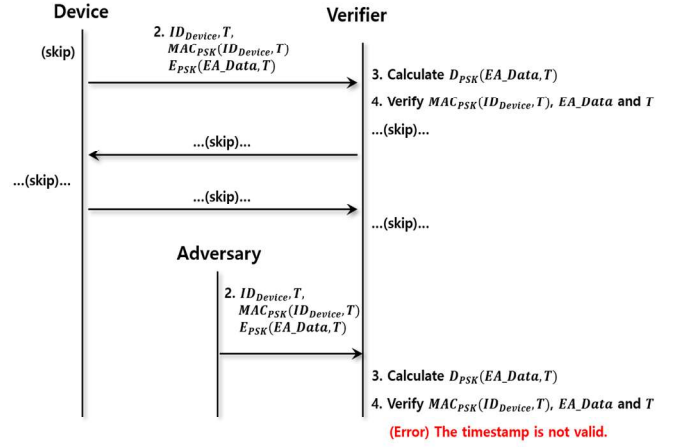


Fig. 7. Example of replay attack

- Message Modification Attack

The adversary can modulate the messages obtained through steps ②, ⑧ and ⑫. However, if the T and MAC values and the encryption data are modulated, it is possible to check whether or not the message is modulated in each message verification process.

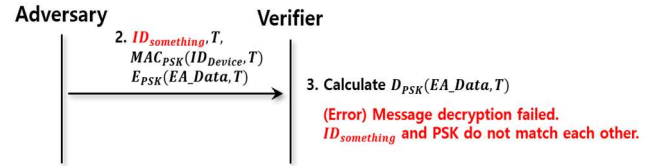


Fig. 8. Example of message modification attack

Even if the ID value is modulated, the PSK that can be matched with the corresponding ID is not the correct decryption key. Therefore, message decryption fails and the protocol is terminated.

D. Processing Speed Analysis

Table 3 below shows data on the processing time of the SIMD method and the non-SIMD method when performing authentication for various IoT devices in terms of the verifier in the proposed protocol.

TABLE III. PROCESSING TIME DATA OF NON-SIMD AND SIMD

Size of Auth_Data	Processing Time (ms)		Speed ratio of SIMD (A/B)
	Non-SIMD (A)	SIMD (B)	
1k	2.364	1.862	1.27
10k	2.403	1.914	1.26
100k	2.753	2.036	1.35
1M	6.379	4.396	1.45
2M	10.364	6.397	1.62
5M	22.391	12.764	1.75
10M	42.354	22.770	1.86

Figure 9 is a graph showing the processing time and the processing speed ratio of SIMD and non-SIMD. Through the above graph, it can be seen that the effect of high-speed parallel processing increases as the size of authentication data increases.

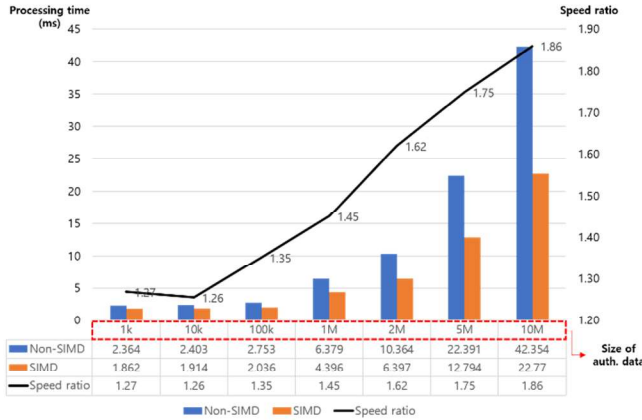


Fig. 9. Processing speed comparison graph

IV. CONCLUSIONS

In this paper, we propose a protocol to perform authentication procedure for IoT devices. We propose a protocol that can actively utilize SIMD technology as a method to make lightweight and high speed authentication process of ARM Cortex A processor which is widely used and applied in various industrial fields.

In the future, we will study the lightweight of the IoT authentication protocol that can be used in various processors besides ARM.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1E1A1A01075110).

REFERENCES

- [1] McAfee Labs, "McAfee Labs Threats Report December 2018," December, 2018
- [2] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel and Ingrid Verbauwhede, "Chaskey: An efficient MAC Algorithm for 32-bit Microcontrollers," SAC 2014, vol.8781, pp.306-323, 2014.
- [3] Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu and Dong-Geon Lee, "LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors," in *Information Security Applications: 14th International Workshop, WISA 2013*, Jeju Island, Korea, August 19-21, 2013.
- [4] Ministry of Science, ICT and Future Planning, Korea Internet Security Agency, "Guide to Using Password Authentication Technology in Internet (IoT) Environment," March, 2017
- [5] Liu Cheng, Lin shenwen, Li Yingbo, Li Na and Wang Xuren, "A Secure and Lightweight Authentication Protocol for RFID," in *2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*. pp.317-320, May 2015.
- [6] Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang and Lei Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," in *Security and Communication Networks*. Volume 2017, Article ID 6562953, 41pages, September 2017.