

IoT용 보안기능 내장 칩과 현황 소개

I. 서론

지난 수년간 많은 IoT기기들이 선을 보였다가 수익모델의 부재로 사라지기를 반복하고 있다. 이를 반영이라도 하듯이 2016년에 가트너에서 발표한 “가트너 하이퍼 사이클 2016”에서 IoT는 기술에서 사라졌다. 사라진 것에 대해 2016년 10대 전략 기술로 IoE(Internet of Everything)을 제시하였으며 2017년에는 지능형사물(Intelligent Things)을 제시하여 연결이라는 키워드를 당연한 것으로 취급한 것으로 생각되나, 가트너에서 확실히 밝힌 적은 없다.

“아루바 휴렛팩커드 엔터프라이즈 컴퍼니”는 한국과 미국, 인도, 일본, 중국, 호주등 세계 20개국 3100명의 IT, 비즈니스 의사결정권자를 대상으로 조사하여 발간한 IoT 트렌드 리포트 “사물인터넷:현재와 미래”를 2017년 4월 3일 공개했다. IoT(Internet of Things)로 얻은 실제 이점은 혁신, IT 효율성, 비즈니스 효율성, IT 효과성, 비즈니스 가시성 순이며, 기대했던 이점 대비 실제 경험한 혜택은 IT 효율성, 비즈니스 효율성, 고객경험, IT 효과성, 혁신측면의 순으로 나타났다. 또한, 한국 기업들은 당초 기대치 대비 실제 얻은 이익이 2.8배로 타 지역보다 월등히 높다고 평가했으며, 산업·제조 부문에서는 62%가 이미 IoT를 도입해 사용하고 있으며 그 중에서 시스템 모니터링과 유지관리를 가장 많이 활용하고 있다고 제시하였다. 그러나, 가장 큰 IoT 장애요소는 ‘보안’으로 전 세계 조직의 84%가 IoT 관련 보안침해를 경험한 것으로 나타났다. 이중 아태지역은 88%, 한국은 86%로 타 지역보다 높게 나타났다^[1].



이재수
지엘큐

IoT 활용이 높은 부문은 스마트공장으로 대변되고 있는 제조업과 스마트홈으로 볼 수 있다. 물론 이 두 분야에 적용되는 것들로 지능형이라는 단어를 빼놓고는 생각할 수 없다. 제조업에서의 진입장벽은 작업

환경에서의 통신방식의 채용과 최적화된 센서의 설치라고 볼 수 있다. 이 중에서 무선통신을 이용한 센서들과의 통신은 무선의 특성상 보안에 대한 부담이 크며, 수익증대를 목적으로 하는 공장의 입장에서 보안을 위해서 모니터링의 속도를 저하시키는 것도 말이 안되는 입장이다. 특히 빠른 공정으로 인해 단위시간 생산량이 많은 공정의 경우에는 보안적용으로 인한 데이터 수집 지연이 전체적인 생산성에도 영향을 끼칠 수 있다. 스마트홈의 경우도 마찬가지로 현재 아이들이나 반려동물을 보호하기 위해 설치한 영상장치들의 보안 미비, 의식부재로 많은 사생활이 담긴 영상들이 인터넷으로 유포되고 있는 상황이다. IP카메라에 아이디와 패스워드 접속이라는 단순한 보안의식이 악용하고자 하는 사례를 유도하고 있다고 본다. 무선공유기에서도 사용하고 있는 mac address로 제한하는 기능만으로도 많은 해킹시도를 막을 수 있듯이 IP카메라 서비스에서도 원격에서 보고자하는 스마트폰이나 PC에 보안코드를 설정하고 그 외에 것들의 접근은 막는 정도만 되어 있어도 쉽게 사생활이 침해되지 않을 것이다. 요즘 전시회에 전시되고 있는 스마트미러, 스마트냉장고, 스타일코디 서비스를 예고한 아마존의 에코 Look 등이 후 IT는 음성과 영상을 이용하여 연결되는 시대로 변화하고 있다. 이 음성과 영상의 데이터는 중요한 개인정보이기에 시장은 점점 더 고속화되고 촘촘한 보안을 요구하게 될 것이다.

본 기고에서는 보안이 적용될 형태별로 적용 가능한 보안기능 내장·지원 칩의 종류와 그 기능을 살펴보고, 경량화를 위하여 국내에서 연구되고, 논문으로 표출된 보안기능의 설계와 그에 따른 성능 개선 연구에 대해 소개하여 각자 필요한 솔루션을 선택할 수 있는 가이드가 되고자 한다.

II. 보안 - 경량암호화 기술

IoT의 특성상 종단 디바이스에서 사용자에게 서비스되는 모든 것이 연결되는 것이므로, 보안기술은 서비스 영역에 따라 IoT 서비스/플랫폼 보안, IoT 네트워크 보안, IoT 디바이스 보안으로 구성된다.

Trusted Computing Group(이하 TCG)에 의해 제정한 보안칩을 이용하여 암호키를 저장하고 관리하기 위한 규격으로 Trusted Platform Module(이하 TPM)이 제시되었다. I2C나 SPI 통신을 이용하여 TPM과 연결되어 사용되었으나, 요즘은 MCU내부에 보안 기능을 내장하여 디바이스 식별과 인증 그리고 암호화와 장치의 무결성을 보장하기 위한 시큐어부팅 기술이 가능하도록 하는 제품들이 출시되어 사용되고 있다. 시큐어부팅 과정에서 UEFI, OS 로더, 커널, 시스템 드라이버, 시스템 파일 등을 각각 암호화한 고유의 해시값을 TPM에 저장한다. 그 뒤 IoT 기기를 부팅하거나 새로운 실행 명령이 내려질 때마다 내부 소스코드에 대한 고유 해시값을 TPM에 저장한 해시값과 대조해 위·변조 여부를 확인한다. TPM의 인증이 폐쇄성을 가진다는 의견으로 그 대안으로 Advanced Encryption Standard(이하 AES)나 Error Correction Code(이하 ECC)와 같은 알고리즘 등을 적용한 소형 암호인증 전용 칩을 사용하거나 소프트웨어로 구현하여 사용하고 있다. 또한, 보안 기능에 따른 하드웨어적 사양이 크기 때문에 경량 암호화 기법^{[2][3]}에 대해서도 많은 연구가 지속되고 있다.

대표적으로 디바이스에서 사용되는 MCU인 ATtiny45(Microchips)를 기준으로 소프트웨어로 경량암호 알고리즘을 구현하여 적용해보면 그 성능은 다음과 같다^[4].



(그림 1) IoT 환경의 기술적 보안 위험 (출처 : "IoT 보안", KISA 전길수, 2016.11.03.)

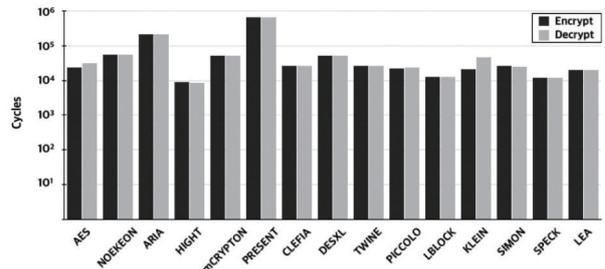
〈표 1〉 경량 암호화 기법⁽¹⁾국내 제안 경량암호기법

기법	블록 크기/Key 크기	Round수	GE 수	구조
AES	128/128,192,256	10,12,14	3,100	SPN
PRESENT	64/128	31	1,391	SPN
CLEFIA	128/128,192,256	18,22,26	4,950	GFN
PRINCE	64/128	12	3,286	SPN
SEA	96/96	93	449	Feistel
KLEIN	64/64,80,96	12/16/20	1,360/1,530/1,700	SPN
mCrypton	64/64,96,128	12	2,420/2,681/2,949	SPN
LED	64/64,128	32,48	1,265	SPN
DESLX	64/184	16	2,168	Feistel
KATAN	32,64/80	254	802/1,054	stream-cipher-like
IDEA	64/128	8,5		Lai-Massey
TEA	64/128	64	3,490	Feistel
LBlock	64/80	32	1,320	Feistel
SEED ⁽¹⁾	128/128	16		Feistel
HIGHT ⁽¹⁾	64/128	32	3,048	Feistel
ARIA ⁽¹⁾	128/128,192,256	12,14,16		Feistel
LEA ⁽¹⁾	32/128,192,256	24,28,32	3,826	ARX

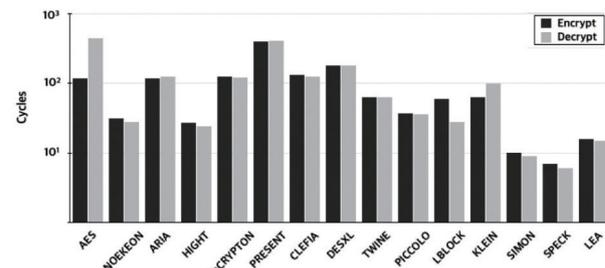
〈표 2〉 ATtiny45 기준 구현된 경량암호 기법 성능^[5]

Cipher	Block size (bits)	Key size (bits)	Code size (bytes)	RAM size (bytes)	Enc+key (Cycles)	Dec+key (Cycles)
AES	128	128	1,568	192	3,629	4,462
			2,606	0	6,637	7,429
DES	64	184	820	48	84,602	84,602
			3,192	0	8,531	7,961
HIGHT	64	128	402	32	19,503	20,159
			5,672	0	2,964	2,964
IDEA	64	128	836	232	8,250	2,272
			596	0	2,700	15,393
KLEIN	64	80	1,000	18	11,342	13,599
mCrypton	64	96	1,076	28	16,457	22,656
PRESENT	64	80	1,000	18	11,342	13,599
			936	0	10,723	11,239
SEA	96	96	426	24	41,604	40,860
			2,132	0	9,654	9,654
TEA	64	128	648	24	7,408	7,539
			1140	0	6271	6299

이상의 성능평가는 8비트 프로세스에서도 낮은 사양 (아두이노 사용 MCU는 ATtiny85)으로 구성한 것으로 LEA는 32비트 프로세서에 적합한 형태를 가진다.



〈그림 2〉 아두이노 성능 측정결과 - 알고리즘별 성능 비교^[6]



〈그림 3〉 라즈베리파이2 성능 측정결과 - 알고리즘별 성능비교^[6]

III. 보안칩 소개

앞서 살펴보았던 암호기법이 하드웨어적으로 구현되어 내장된 칩들에 대해 살펴보고자 한다. 보안엔진으로 명하여 암호의 인코딩과 디코딩을 지원하는 칩들과 ARM 코

〈표 3〉 보안 하드웨어 엔진 내장 칩

	칩셋	제조사	보안기능
보안지원	AT97SC320X	Microchips	RSA-2048/1024, SHA-1
	PLUTO RS1211	라닉스	LEA-128, AES-128, ARIA-128, TRNG
	DORCA-20	네오와인	AES-128
	STSAFE-A1SX	STMicroelectronics	AES-128
	ATAES132	Microchips	AES-128, Random Number Generator(RNG)
비 ARM 계열 MCU	C8051F96X	SiliconLabs	AES-128/192/256
	MSP430FR59XX	TI	AES-128/192/256, True Random Number Seed
	CC2541 ⁽¹⁾	TI	AES-128
	AT32UC3AXXX	Microchips	AES-128/192/256
	A700X ⁽²⁾	NXP	AES-128/192/256, RSA-2048, TRNG, DES, 3-DES, SHA-1, SHA-256
	ESP32 ⁽³⁾	Espressif Systems	AES-128, SHA-2, RSA-4096
	CSG01S ⁽²⁾	씨앤유글로벌	ARIA-128, ECC-193
ARM 계열 MCU	MG247X ⁽²⁾⁽⁴⁾	라디오필스	AES-128
	STM32L443	STMicroelectronics	AES-128/256, TRNG
	EFR32	SiliconLabs	AES-128/192/256, SHA-1, SHA-2, TRNG
	SIM3L1XX	SiliconLabs	AES-128/192/256
	EM358X/EM359X ⁽⁴⁾	SiliconLabs	AES-128, TRNG
	SAMA5	Microchips	AES-128/192/256, 3-DES, SHA-1/224/256/384/512, TRNG
	MX7D	NXP	SHA-256, RSA-2048, TRNG
	MK82FN256	NXP	AES-128/256, 3-DES, RNG
	MT7697	MEDIATEK	AES, DES, 3-DES, SHA-256/512
	MS500	이더블유비엠	AES-128/256, ARIA-128/192/256, SHA-1/SHA-256, TRNG
RN-MO-012	라닉스	AES-128, 3-DES, RSA-2048, TRNG	

⁽¹⁾BLUETOOTH, ⁽²⁾8051 계열, ⁽³⁾Tensilica Xtensa 32-bit LX6 microprocessor, ⁽⁴⁾2.4 GHz IEEE 802.15.4(Zigbee)
 * 칩셋의 보안 기능은 데이터시트 또는 제조사 홈페이지를 참조하였음.

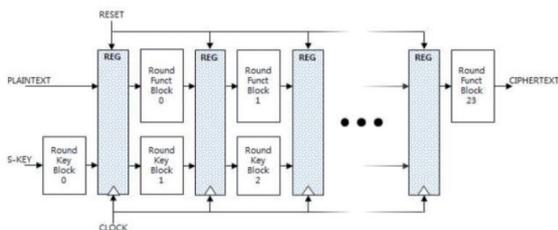
어플리케이션으로 보안기능을 내장한 MCU, 8051 IP 코어를 기반으로 보안엔진을 내장한 MCU로 구분할 수 있다.

FSM(Finite State Machine) 방식과 2, 3, 6, 8, 12, 및 24단계 파이프라인 방식의 다양한 구성으로 구현하였다.^[13]

IV. 경량암호기법 국내 연구 사례

1) LEA 구현 사례

128비트 LEA 암호화 알고리즘의 주요 블록인 키 스케줄 및 라운드 연산 블록을 설계하여 암호화 블록을



〈그림 4〉 24단계 파이프라인 LEA-128 암호화 블록 설계

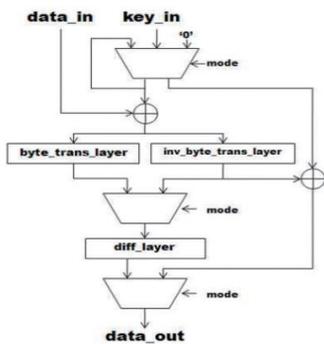
〈표 4〉 LEA-128 암호화 블록 합성 결과

Design	Max.Freq (MHz)	Clock cycles	Resource			Throughput (Mbps)
			FFs	LUTs	Slices	
FSM	323.55	25	552	616	775	1656.57
Pipeline2	274.77	12	679	1361	1445	2930.88
Pipeline3	310.04	8	936	1867	1948	4960.64
Pipeline6	317.15	4	1713	3529	3568	10148.8
Pipeline8	323.95	3	2257	4802	4837	13821.87
Pipeline12	333.30	2	3283	6612	6655	21331.2
Pipeline24	418.69	1	6426	7737	8819	53592.32

* Target device : Virtex5 XC5VLX50T

2) ARIA 구현 사례-1

기존 ARIA 알고리즘에서는 치환계층에서 3종류의 함수를 사용하지만, 제안된 방법에서는 3종류의 함수를 단일 블록함수로 통합하여 구현한다. 구현된 고속 암호 프로세서는 연산 속도가 보다 높아지며, 하드웨어 오버헤드도 감소하게 된다. 제안된 시스템은 저전력이 요구되는 스마트카드와 모바일 시스템 환경에 최적이 되도록 설계하였다^[14].



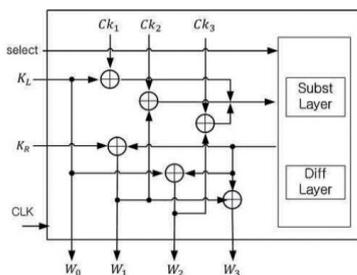
〈그림 5〉 제안한 F Block diagram

〈표 7〉 프로세서들의 성능비교

	Databus (bit)	Area	Freq. (MHz)	Throughput (Mbps)	Process
문헌[15]	128	1,491 slices	46,5	496	XCV-1600E
문헌[16]	32	13,893 GE	71	22	0.35um CMOS
문헌[17]	32	11,301 GE	467	215	0.25um CMOS
제안한 방식	128	9,217 slices	71.4	652	XCV-1600E

3) ARIA 구현 사례-2

키 초기화 과정 중 라운드 함수 내 공통으로 사용되는 치환 계층과 확산 계층을 공유하여 FPGA의 전체의 면적을 줄이는 설계방법을 제안하였다.^[18]



〈그림 6〉 개선된 키 초기화 모듈

〈표 8〉 키 초기화 방법의 성능비교

	슬라이스의 수	delay(nsec)
기존	3852	31.03
개선된 설계 방식	3465	8.3

〈표 9〉 ARIA 암호 프로세서의 성능비교

	슬라이스 수	주파수 (MHz)	Throught (Gbps)	Target Device
Method[19]	2,786	200	1.3	XC5V5X50T
제안한 방식	1,550	220.4	2.2	XC5V5X50T
Method[20]	22,778	192.9	2.5	XC2VP30-7
제안한 방식	6,647	162.9	1.9	XC2VP30-7

*[19], [20]에서 제안된 방식으로 구성하고, 각 논문에서 사용한 타겟 디바이스로 동등하게 평가.

V. 전망과 결론

본 기고에서는 최근까지 발표된 경량암호 기법의 특징과 구현에 따른 성능을 일부 살펴보았으며, AES만 구현된 것들이 대부분이지만 보안기능을 칩에 내장하여 보다 빠르고 편리하게 보안기능을 구현할 수 있는 칩들에 대해서도 소개하였다. 이곳저곳에서 발표되고 있는 것들을 모아놓은 것에 불과하지만, 각자가 활용하는 것에 도움이 될 수 있다고 생각하였으며 최대한 국내 칩도 소개하고자 하였다. IoT 디바이스의 특성상 ESP32로 소개된 중국 칩이 성능대비 가격이 저렴하고, 해당 제조사에서 적극적인 커뮤니티 지원, 개발지원등을 펼치고 있기 때문에 국내 출시된 칩들도 다양한 사이트에서 적용했으면 한다.

연구사례라고 기술한 국내 암호기법 구현 논문들에서와 같이 다양한 구현사례를 공유하여 연구된 내용을 기업 상용화의 기반으로 가져갔으면 한다. 지금도 다양한 경량 암호 기법은 계속 연구되고 있으므로, 지속적으로 연구현황, 칩 개발 현황 등의 모니터링을 통해 안전한 IoT 생태계를 형성해 나갔으면 한다.

참고 문헌

- [1] "사물인터넷 : 현재와 미래" Hewlett Packard Enterprise Aruba, 2017.
- [2] 서화정, 김호원, "사물인터넷을 위한 경량 암호 알고리즘 구현", 정보보호학회지 제25권 제2호, 2015.

[3] https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers

[4] AES specification, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>

[5] "Compact Implementation and Performance Evaluation of Block Ciphers in ATtiny Devices"

[6] 문시훈, 김민우, 권태경, "IoT 통신 환경을 위한 경량 암호 기술 동향", 한국통신학회지, 2016.

[7] Ahmad-Reza Sadeghi, Christian Wachsmann, Michael Waidner, "Security and Privacy Challenges in Industrial Internet of Things", Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE.

[8] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things", sony corporation, 2011.3.

[9] LED algorithm, <https://sites.google.com/site/ledblockcipher/design>

[10] Wenling wu and Lei Zhang, "LBlock: A Lightweight Block Cipher".

[11] Tung Chou, "QcBits: Constant-Time Small-Key Code-Based Cryptography"

[12] SEED/HIGHT/ARIA/LEA algorithms, <http://seed.kisa.or.kr>

[13] 윤기하, 박성모, "128 비트 LEA 암호화 블록 하드웨어 구현 연구", 스마트미디어저널 Vol.4, No.4, 2015.

[14] 강재석, "FPGA 기반 고속 ARIA 암호 프로세서 설계", 보안공학연구논문지, Vol.11, No.3, 2014.

[15] J.S.Park, S.Y.Kim, Y.D.Kim and Y.G.You, "Design and Implementation of ARIA Cryptic Algorithm", IEEK, Journal of IEEK, 2005

[16] Y.K. Yoo, et al., "Low Power Cryptographic Design based on Circuit Size Reduction", The Korea Contents Association, J. of Contents Association, 2007.

[17] ARIA-test Vector, "<http://seed.kisa.or.kr/>,알림마당/자료실/ARIA 소스코드 보급/ARIA.zip"

[18] 강재석, 강민섭, "개선된 키 스케줄링 기반 ARIA 암호 프로세서의 FPGA 구현", 보안공학연구논문지, Vol.13, No.6, 2016.

[19] 김동현, 신경욱, "4가지 운영모드와 3가지 마스터 키 길이를

지원하는 블록암호 알고리즘 ARIA의 효율적인 하드웨어 구현", 한국정보통신학회 논문지 제16권 제11호, 2012.

[20] Ha Seong-ju, Lee Chong-ho, "Design of High Speed Encryption/Decryption Hardware for Block Cipher ARIA", The Korean Institute of Electrical Engineers, 2008.

[21] 참조 제조사 사이트

TI, <https://www.ti.com>

SiliconLabs, <http://www.silabs.com>

Microchips, <http://www.microchip.com>, <http://www.atmel.com>

MEDiatek, <https://www.mediatek.com>

NXP, <http://www.nxp.com>

Espressif Systems, <http://espressif.com>

라닉스, <http://www.ranix.co.kr>

씨앤유글로벌, <http://www.cnuglobal.com>

이더블유비엠, <http://www.e-wbm.com>

네오와인, <http://neowine.com>

라디오펄스, <http://www.radiopulse.co.kr>



이재수

- 1993년 2월 강원대학교 공과대학 제어계측공학과 학사
- 1995년 2월 강원대학교 공과대학 제어계측공학과 석사
- 1995년 2월~1999년 6월 (주)셀파워 연구원
- 1999년 6월~2000년 8월 (주)셀라인 선임연구원
- 2001년 7월~2004년 1월 (주)세이뉴 선임연구원
- 2005년 4월~2008년 11월 (주)지이에치티 수석연구원
- 2008년 11월~2010년 8월 (주)테라솔텍 수석연구원
- 2010년 8월~2013년 6월 (주)지이에치티 수석연구원
- 2013년 6월~현재 (주)지엘큐 대표이사

<관심분야>

IoT, Security, Smart Home, Blockchain