정 보 보 호 학 회 지
제 29 권 제5호, 2019. 10

5G 보안을 위한 경량암호 기술 동향

김 우 환*, 권 대 성*

요 약

초고속, 초저지연, 초연결 특성으로 대표되는 5G 시대가 도래함에 따라 새로운 통신 환경과 서비스 환경에 적합한 암호기술이 요구되고 있다. IoT 환경 등 자원이 제약된 기기를 위한 저면적/저전력 암호기술, 자율 주행 등 실시간 처리를 위한 저지연 암호기술 등 경량암호에 대한 요구사항 또한 다변화되고 있다. 본 고에서는 SPECK/SIMON, LEA 등으로 대표되는 경량 블록암호와 초저지연 암호기술에 대해 살펴보고 NIST에서 진행 중인 경량암호 공모사업을 소개한다.

Ⅰ. 서 론

현대 암호기술은 다른 정보보호 기술과 달리 2000년 중반 이후 큰 변화를 겪지 않고 있다. 그 이면에는 우수한 안전성 및 성능을 가진 블록암호 AES (Rijndael)가 1990년대 후반에 개발되어 다양한 분야에 널리 쓰이고 있고, 인터넷에서의 전자 상거래, 서비스를 책임지면서 쉽게 바꿀 수 없는 특성을 지닌 공개키 암호 RSA, ECC가 있기 때문이었다.

최근, 센서 등을 비롯한 작은 디바이스와의 통신 보호가 필요한 IoT 환경이 늘어나면서, 경량 환경에서의 암호기술에 대한 연구가 진행되었다. 대표적인 국제표준화 기구인 ISO/IEC에서는 경량암호를 별도 분야로 분류하여 표준을 제정하였다.

대표적인 경량 블록암호로는 미국 NSA가 개발한 SPECK/SIMON[3]과 국가보안기술연구소가 개발한 LEA[7]를 들 수 있다. 그런데, 미국에서 제안한 경량암호는 ISO/IEC 표준화에 실패하였고, LEA는 금년 2019년말 ISO/IEC 경량암호로 제정될 예정이어서, 경량암호분야에서는 국내 암호기술이 세계적으로 앞서가는 발판을 마련하였다고 할 수 있다.

5G 환경에서는 경량 특성 외에도 초저지연 서비스를 지원할 수 있는 경량 초저지연 암호기술의 필요성이 대두되고 있다. 기존 경량암호들은 작게 구현될 수 있는 것을 우선 목표로 하고 있기 때문에, 저지연 특성은 주로 보유하고 있지 않다. 또 하나의 숙제는 SW 환경과 HW 환경 모두에서 경량과 저지연 특성 제공이 가능한가이다. 미국에서 SW 타겟으로 SPECK을, HW 타겟으로 SIMON을 제안한 것은 양쪽에서 모두 경량인 암호의 개발이 어렵기 때문이라고 생각된다.

경량암호 개발에서 가장 어려운 점은 단순한 연산으로 경량 특성을 제공하면서 동시에 안전성을 보장하는 것이다. 미국 NSA 암호들도 안전성면에서의 의구심이 표준화를 실패하게 만든 주된 이유이다.

경량 저지연 암호 개발은 5G 그리고 그 이후 이동통신 환경에서의 암호화를 위한 블록암호 기술 선점이라는 면에서 많은 연구가 필요한 부분이라고 할 수 있다.

본문에서는 경량 블록암호, 저지연 암호 기술 동향에 대하여 살펴보고, 이후 NIST에서 진행하고 있는 경량암호 공모사업 동향에 대하여 정리한다.

Ⅱ. 경량 블록암호

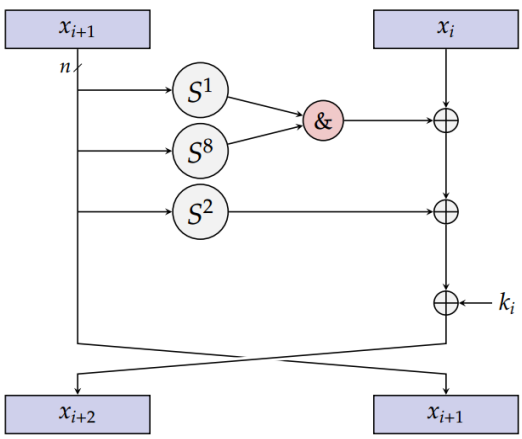
경량암호로서 요구되는 특성은 구현환경에 따라 다르며 크게 HW와 SW로 구분할 수 있다. HW에서는 FPGA 또는 ASIC에서의 저면적(low-area) 구현 측면이 주로 고려되고 있으며, SW에서는 AVR 등 경량 SW 플랫폼에서 코드 크기와 메모리 요구량이 작을수록 경량 특성이 우수하다. 이러한 자원 요구량과 함께 속도 또는 소요시간이 함께 고려되어 속도/면적 등의 FoM(figure of merit)을 이용하여 알고리즘의 성능을 비교할 수 있다.

* ETRI 부설연구소 (whkim5@nsr.re.kr, ds_kwon@nsr.re.kr)

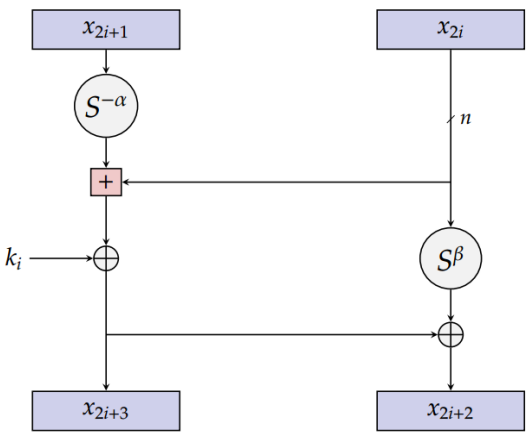
2013년 미국 NSA는 두 개의 경량 블록암호 SPECK/SIMON을 발표했다. SPECK과 SIMON의 라운드 함수는 각각 [그림 1], [그림 2]와 같다. 그림에서 S^m은 m비트 순환(rotation)을 의미한다.

이들은 기존의 블록암호들보다 상당히 우수한 경량 특성을 보유하고 있으며 NSA가 처음으로 공개 발표한 암호 알고리즘으로서 많은 관심을 받았다. 특히, 같은 구조로 다양한 크기(제안 시 32, 48, 64, 96, 128비트)의 입출력을 지원할 수 있다는 장점도 있어, 경량 환경에서 AES와 더불어 대표적인 블록암호로서 자리 잡을 것으로 예상되었다.

SPECK과 SIMON은 각각 SW 경량과 HW 경량에 주안점을 두고 설계되었다. SPECK은 AVR 등 경량 환경에서 FoM 면에서 기존 암호들보다 우수한 특성을 보이고, SIMON은 ASIC에서 1000GE 미만으로 구현 가능한 최초의 암호로 많은 관심을 받았다. 유사한 시기에 국내에서는 SW 환경에서 성능이 우수한 블록암호 LEA를 발표하였다. LEA의 라운드 함수는 [그림 3]과 같다.



〔그림 1〕 블록암호 SIMON 라운드 함수

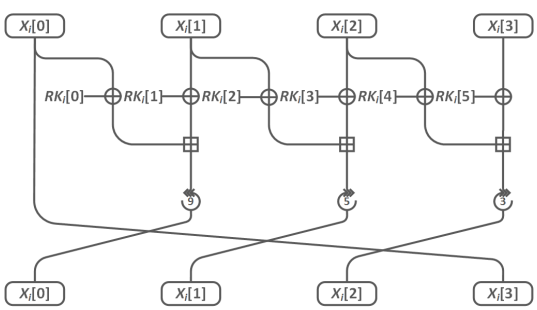


〔그림 2〕 블록암호 SPECK 라운드 함수

LEA의 특징은 32비트 CPU 환경에서 현 블록암호 중 가장 우수한 성능을 보이며, 1KB 미만으로 구현될 수 있다는 탁월한 경량 특성을 가지고 있다는 것이다. LEA는 SW 환경에서 우수한 구현 특성과 안전성을 확보하기 위해 구성 요소를 선택하였다. 그러나, HW 구현에서는 AES 등에 비하여, 작은 면적으로 구현하기 어려운 면이 존재한다.

SPECK/SIMON과 LEA의 공통점으로는, 기존 블록암호의 주요 논리인 S-box와, 행렬 연산을 이용한 AES 개발에서 비롯되어 널리 사용된 SPN (Substitution Permutation Network) 설계 기법을 탈피하여 덧셈, 논리곱 등으로 비선형성을 얻고 비트 회전 등을 활용하여 확산효과를 얻는 ARX(Addition, Rotation, Xor) 구조를 사용하여 경량화를 달성했다는 점이다. 그런데, ARX 구조는 기존 SPN 구조에 비하여, 안전성 보장이 어렵다는 단점을 갖고 있으며 이를 극복하기 위해 MILP, SAT solver 등 수학적 도구를 활용한 안전성 분석 기법이 주로 활용되고 있다.

2015년 룩셈부르크 대학의 암호 연구그룹인 CryptoLUX에서는 경량암호의 SW 성능을 평가하기 위해 FELICS(Fair Evaluation of Lightweight Cryptographic Systems) 프로젝트[11]를 진행하였다. 프로젝트에서는 세 가지 SW 플랫폼(8비트 AVR, 16비트 MSP, 32비트 ARM)을 대상으로 코드 크기, 메모리 사용량, 소요 시간 측면에서 알고리즘들의 성능을 비교하였으며 [표 1]과 같이 128비트 블록암호 중



〔그림 3〕 블록암호 LEA 라운드 함수

〔표 1〕 FELICS 주요 블록암호 구현 결과: 키 스케줄 및 암복호화 포함, CBC 운영모드, 센서 네트워크 등 IoT 기기를 고려한 128비트 데이터 처리 시나리오 가정(시나리오 1)

블록암호	블록 크기	키 크기	구현 결과									
			AVR			MSP			ARM			FOM
			코드 크기 (Byte)	RAM 사용량 (Byte)	시간 (Cycle)	코드 크기 (Byte)	RAM 사용량 (Byte)	시간 (Cycle)	코드 크기 (Byte)	RAM 사용량 (Byte)	시간 (Cycle)	
SPECK	64	128	864	300	45686	592	298	37850	402	312	17084	5.3
SIMON	64	128	1112	373	67040	780	374	53112	530	388	23404	7.2
LEA	128	128	1650	629	61755	1154	630	51582	496	664	17410	8.3
SKINNY	64	128	1086	337	92891	1006	342	112402	788	372	95924	13.9
HIGHT	64	128	1404	331	95348	1258	330	129188	1440	380	89382	14.8
AES	128	128	3000	406	58973	2684	408	87850	3052	452	72828	15.7

LEA가 가장 성능이 우수한 것으로 평가되었다. [표 1]에서 FOM은 다른 알고리즘들의 성능과 비교했을 때의 상대 수치이며 작을수록 성능이 우수함을 나타낸다.

미국 NSA가 제안한 SPECK/SIMON의 경우, LEA에 비하여 경량성이 좋도록 설계되었으나, 안전성 면에서는 많은 공격들이 발표되는 계기를 만들기도 하였다. 처음 제안되었을 때보다 개선된 공격들이 지속적으로 발표되었다. 이로 인해 발생한 안전성에 대한 의구심이 발단이 되어, ISO/IEC 표준화에 실패하였다.

반면, LEA의 경우, HW 경량 특성 등이 다소 미흡하지만 SW에서의 우수 성능과 안전성을 인정받아 ISO/IEC 표준화가 순조롭게 진행되고 있으며 금년 말 완료될 예정이다.

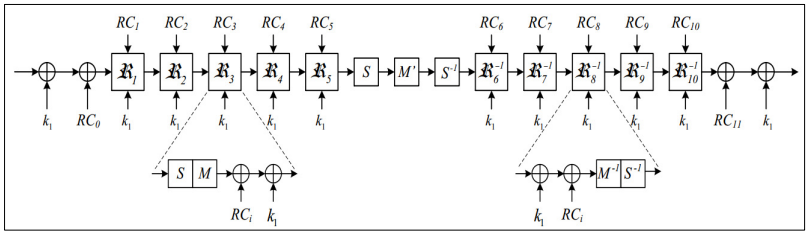
현재, ISO/IEC 경량 블록암호 표준으로는 HW 경량 특성이 있는 PRESENT(유럽), CLEFIA(일본)가 포함되어 있는데, LEA는 SW 경량 특성으로 차별화 되어, 대표적인 경량암호 국제 표준으로 자리매김할 것으로 기대한다.

Ⅲ. 저지연(low-latency) 암호

지연시간(latency)은 입력으로부터 출력을 얻는데까지 걸리는 시간을 의미한다. 저지연(low-latency) 암호는 다소 생소한 용어이지만 암호학계에서는 HW 구현 특성 측면에서 주로 논의되어 왔다. 지연시간이 짧은 암호를 저지연 암호라 부르며 5G와 같은 초저지연 통신 환경 및 서비스에서 초저지연 암호기술의 중요성과 활용도가 커지고 있다. 초저지연 암호기술이 필요한 분야로는 원격제어, 원격의료, 자율주행 등 실시간 서비스와 메모리 암호화[9]를 들 수 있다. 특히, 차량에 장착된 기기간의 통신은 짧은 지연시간이 요구된다. 메모리 암호화는 주요 적용 대상이 RAM(Random Access Memory)이며 FPGA의 RAM에 저장된 SW IP 보호에 활용될 수 있다.

블록암호 HW 구현에서는 파이프라인 구현 기법을 통해 고속 구현이 가능하지만 초기 지연시간이 있을 수 있음을 감안할 때 고속 구현과 저지연 구현의 개념은 다를 수 있다.

일반적으로 블록암호의 HW 구현에서 저지연 특성을 제공하기 위해서는 unrolled 구현을 해야 하며 비트 단위로 처리하는 bit-serial 구현과 라운드 단위로 처리하는 round-based 구현에 비해 면적이 크게 증가한다. 상대적으로 적은 면적으로 unrolled 구현이 가능하며 지연시간이 짧은 암호를 저지연 암호로 간주할 수 있으며 지금까지 발표된 알고리즘 중 저지연 특성을 강조한 블록암호로는 PRINCE[5]와 MANTIS[4]를 들 수 있다. PRINCE는 unrolled 구현을 고려하여 기존 블록암호에서 단순한 형태의 라운드 함수의 반복 구조로 설계한 것에서 벗어나 α-reflection 이라는 설계사상을 가지고 설계되었다. α-reflection이란 어떤 상수 α가 존재하여 비밀키 k에 대한 복호화가 비밀키 $k \oplus \alpha$에 대한 암호화와 동일한 성질을 의미하며 이로 인해 복호화를 별도로 구현할 필요가 없으므로 구현



〔그림 4〕 블록암호 PRINCE 전체 구조: α-reflection

면적을 줄일 수 있다. PRINCE의 전체 구조는 [그림 4]와 같다.

[표 2]에서는 단위 지연시간을 제한했을 때 PRINCE와 AES의 HW 구현 효율성을 비교한 결과로서 PRINCE가 AES에 비해 작은 면적으로 저지연 구현이 가능함을 보여준다.

〔표 2〕 AES와 PRINCE의 저지연 구현 효율성 비교

Unit Delay	1000	3162	10000
PRINCE	7,996 GE	7,996 GE	7,996GE
AES	421,997 GE	130,835 GE	118,522 GE

MANTIS는 SKINNY와 함께 발표된 저지연 블록암호로서 PRINCE의 α-reflection의 설계사상을 따르고 있으며 S-box 등 라운드 함수의 구성은 Midori[1]와 유사하다. 제안 논문에서는 대칭적인 부분의 라운드 수가 r일 때의 알고리즘을 MANTISr로 나타내고 있으며 [표 3]은 PRINCE와 MANTIS5를 unrolled 구현 했을 때의 비교 결과로서 MANTIS5가 조금 더 성능이 우수함을 알 수 있다.

〔표 3〕 PRINCE와 MANTIS5 unrolled 구현의 저면적, 저지연 구현 효율성 비교

	저면적 구현		저지연 구현	
	면적 (GE)	지연시간 (ns)	면적 (GE)	지연시간 (ns)
PRINCE	8,344	16.00	13,424	9.00
MANTIS5	8,544	15.95	17,693	9.00

저지연 특성에 맞춘 암호들의 연구는 아직 초기 단계여서 기존 HW 경량 블록암호에 비해 구현 면적이 크다는 것을 알 수 있다. 초저지연 특성이 5G의 주요 이슈로 대두되고 있는 만큼, 저지연 특성이 필요한 응용분야에서의 암호기술 요구사항 분석과 함께 기술 개발이 필요하다 할 수 있다.

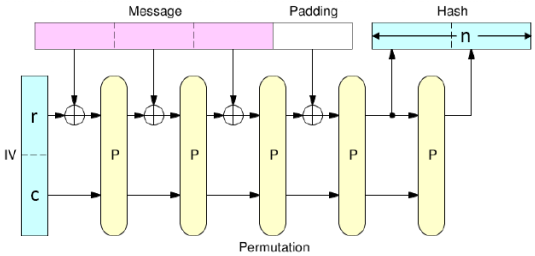
Ⅳ. NIST 경량암호 공모사업

미국 NIST는 자원이 제약된 환경에서 암호기술의 필요성이 증가함에 따라 2013년 기존 표준기술에 대한 경량 구현 기술과 전용 경량암호 기술에 대한 이해도를 높이기 위해 경량암호 프로젝트를 시작하였으며 2018년 인증암호화와 해쉬함수에 대한 경량암호 공모사업을 시작하였다. 경량암호에 대한 요구조건으로는 각종 암호학적 공격에 대해 112비트 이상의 안전성과 경량 환경에서 AES/CCM, AES/GCM, SHA-2/3 등 기존 NIST 표준 암호기술에 비해 성능이 월등히 우수할 것, 그리고 다양한 부채널 공격에 대한 대응기법 적용이 용이할 것을 명시하고 있다. 2019년 4월에 1차 라운드 후보 알고리즘이, 2019년 8월에 2차 라운드 후보 알고리즘이 발표되었다.

제출된 알고리즘들은 스폰지(sponge) 방식, 블록암호 운영모드 방식, 스트림암호 기반 등으로 분류할 수 있으며 1라운드와 2라운드 후보의 분류별 개수는 [표 4]와 같다.

가장 많이 제출된 스폰지 방식은 SHA-3로 채택된 Keccak의 기본 구조로서 해쉬함수 설계 뿐만 아니라 암호화와 인증 암호화에 응용되고 있으며 기반 논리인 치환함수의 안전성으로부터 이를 이용한 해쉬함수와 암호화 방식의 안전성이 증명 가능하다.

스폰지 구조 해쉬함수의 동작 과정은 [그림 5]와 같다. 스폰지 구조 해쉬함수에서 메시지와의 xor에 의해 직접 갱신되는 부분의 크기를 r(bit rate), 그 이외 부분을 c(capacity), 출력 해쉬값의 크기를 n이라 했을 때,



〔그림 5〕 스폰지 구조

〔표 4〕 NIST 경량암호 1라운드, 2라운드 후보 알고리즘 분류

분류	1라운드('19.4.)		2라운드('19.8.)	
	인증 암호화	해쉬함수	인증 암호화	해쉬함수
스폰지 기반	24	19	17	11
블록암호 기반	23	1	14	1
스트림암호 기반	6	2	1	0
기타	3	0	0	0
합계	56	22	32	12

치환함수가 랜덤하면 충돌쌍 공격과 역상 공격 및 제2 역상 공격에 대한 안전성이 증명 가능하며 제공 안전성은 [표 5]와 같다.

〔표 5〕 스폰지 방식 해쉬함수 제공 안전성

	비트 안전성
충돌 저항성	$\min(c/2,\ n/2)$
역상 저항성	$\min(c/2, n)$
제2 역상 저항성	$\min(c/2, n)$

스폰지 방식의 해쉬함수가 제안된 이후, "duplex construction"이라는 설계 기법을 이용하여 스폰지 방식에 기반을 둔 인증암호화가 제안되었으며 키 길이가 k이고 태그 길이가 t일 때, 안전성은 [표 6]과 같다.

스폰지 방식은 하나의 프리미티브(치환함수)로부터 인증 암호화와 해쉬함수의 기능을 제공할 수 있으며 증명가능한 안전성을 가진다는 점에서 주목받고 있다. 또한 기존 설계 기법과 달리 별도의 메시지 스케줄(해쉬함수) 또는 키 스케줄(인증 암호화)이 필요하지 않고

〔표 6〕 스폰지 방식 인증 암호화 제공 안전성

	비트 안전성
기밀성	$\min(k,\ c/2)$
위조불가능성	$\min(k,\ t,\ c/2)$

bit rate와 capacity 등 파라미터를 조절하여 선택적으로 안전성과 효율성을 제공할 수 있다는 장점을 가진다. 한편, 치환함수의 안전성을 충분히 담보하기 위해서는 더 많은 연구가 필요할 것으로 예상된다. [그림 6]은 스폰지 방식의 예로서 NIST에 제출된 인증 암호화 중 하나인 ASCON[6]의 전체 구조를 나타내고 있다.

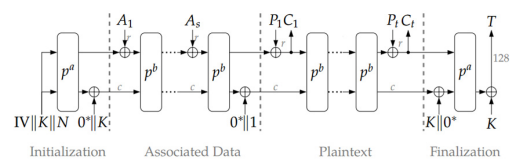
블록암호 운영모드 방식은 주로 인증암호화 분야에 한하여 제출되었으며 GIFT[2], SKINNY, SPECK, CHAM[8] 등 경량 특성이 우수한 블록암호를 특정하고 이를 이용한 인증암호화 알고리즘을 설계하였다. 예를 들어 COMET의 경우 경량 SW 특성을 위해 AES와 SPECK을 적용하고, 경량 HW 특성을 위해 CHAM을 적용하고 있다.

지난 2월 인증 암호화 공모사업 CAESAR[10]에서는 [표 7]과 같이 최종 포트폴리오를 발표하였으며 경량 부문에서는 스폰지 방식인 ASCON과 스트림암호 기반인 ACORN이 선정되었다. NIST 공모사업에서도 스폰지 방식이 강점을 가질 것으로 예상된다.

〔표 7〕 CAESAR 인증 암호화 최종 포트폴리오

분야	인증 암호화
경량 응용	ASCON, ACORN
고성능	AEGIS-128, OCB
고비도	Deoxys-II, COLM

NIST 공모사업에서는 SHA-3와 같이 단일 알고리즘을 선정하지 않고 CAESAR와 같이 몇몇 알고리즘들을 포함하는 포트폴리오를 선정하는 형태로 추진될



〔그림 6〕 스폰지 방식 인증암호화 ASCON 전체 구조

예정이며 제출된 알고리즘들에 대한 안전성 분석 등 다양한 논의들은 lwc-forum[12]에서 찾아볼 수 있다.

Ⅴ. 결 론

본 고에서는 5G 환경에서 요구되는 경량암호 기술 동향에 대해 정리하였다. 5G 환경에서는 기존의 저면적 위주의 HW 경량암호, 코드/메모리 SW 경량암호 외에 저지연 암호 등 추가적인 경량 특성의 암호기술이 요구되고 있다.

전통적으로 기밀성 제공에서 시작된 암호기술은 인증, 접근제어 뿐만 아니라 데이터 공유를 위한 응용기술 등으로 영역을 점차 넓혀가고 있으며 기밀성 위주의 비밀키 암호는 새로운 기능의 암호기술에 비해 상대적으로 주목받고 있지 못한 것이 현실이다. 하지만 비밀키 암호의 역할과 중요성은 정보보호의 필요성 증가와 함께 커질 수밖에 없으며 5G 시대의 다양한 요구에 부합하는 비밀키 암호기술은 지속적으로 연구 개발이 필요하다.

참 고 문 헌

[1] S. Banik et al., “Midori: A Block Cipher for Low Energy”, ASIACRYPT 2015, pp. 411-436, 2015.

[2] S. Banik, “GIFT: A Small Present”, CHES 2017, LNCS 10529, pp. 321-345, 2017.

[3] R. Beaulieu et al., “The SIMON and SPECK Families of Lightweight Block Ciphers”, Cryptology ePrint Archive: Report 2013/404.

[4] C. Beierle et al., “The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS”, CRYPTO 2006, LNCS 9815, pp. 123-153, 2016.

[5] J. Borghoff et al., “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications”, Asiacrypt 2012, LNCS 7658, pp. 208-225, 2012.

[6] C. Dobraunig et al., “Ascon v1.2”, https://competition.cr.yp.to/round3/asconv12.pdf.

[7] D. Hong et al., “LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors”, WISA 2013, LNCS 8267, pp. 3-27, 2014.

[8] B. Koo et al., “CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices”, ICISC 2017, LNCS 10779, pp. 3-25, 2018.

[9] M. Werner et al., “Transparent Memory Encryption and Authentication”, 2017 International Conference on Field Programmable Logic and Applications, 2017.

[10] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/

[11] FELICS, https://www.cryptolux.org.

[12] lwc-forum, https://list.nist.gov/lwc-forum.

〈저 자 소 개〉

김 우 환 (Woo-Hwan Kim)

1998년 2월 : 서울대학교 수학과 졸업
2000년 2월 : 서울대학교 수학과 석사
2004년 8월 : 서울대학교 수학과 박사
2004년 11월~현재 : ETRI 부설연구소 책임연구원/실장
<관심분야> 정보보호, 암호

권 대 성 (Daesung Kwon)

정회원

1992년 2월 : 서울대학교 수학과 졸업
1994년 2월 : 서울대학교 수학과 석사
1999년 2월 : 서울대학교 수학과 박사
2001년 3월~현재 : ETRI 부설연구소 책임연구원/센터장
<관심분야> 정보보호, 암호