정 보 보 호 학 회 지
제 30 권 제3호, 2020. 6

NIST 경량암호 공모사업 동향

백 승 준*, 전 용 진*, 김 한 기*, 김 종 성**

요 약

최근 사물인터넷 환경이 발달하면서 센서 네트워크, 헬스케어, 분산 제어 시스템, 가상 물리 시스템 등의 다양한 분야의 산업이 부상하고 있다. 이를 위한 소형 컴퓨팅 기기가 보편화되고 있지만, 해당 기기들은 제한된 리소스라는 공통의 약점을 가지고 있다. 제한된 환경에서 중요한 데이터들을 보호하기 위해서는 많은 리소스가 필요한 기존의 암호 알고리즘보다 적은 리소스로도 운용할 수 있는 경량암호 알고리즘이 필요하다. NIST에서는 2015년부터 제한된 환경에 적합한 경량암호 알고리즘을 표준화하기 위한 공모사업을 진행 중이다. 현재 2라운드 과정을 거치고 있으며 총 32종의 알고리즘에 대한 안전성, 효율성 분석이 이루어지고 있다. 이에 본 논문에서는 NIST 경량암호 공모사업 1, 2라운드 후보 알고리즘들을 특징별로 분석하고, 몇 가지 알고리즘들을 심층적으로 살펴본다. 또한 향후 전망과 계속 진행될 공모사업의 타임라인을 제시한다.

Ⅰ. 서 론

초기 인터넷 기술은 정보 공유 및 커뮤니케이션 위주의 유선 환경에서 발전하기 시작했다. 스마트폰 발달 이후 인터넷 영역이 모바일로 확장되었으며, 이용자들은 자신이 원하는 시간, 장소에서 인터넷에 접속할 수 있게 되었다. 최근에는 스마트폰뿐만 아니라 태블릿 PC, 자동차, 조명, 가전 등 다양한 사물들이 인터넷에 연결되어 인간에게 새로운 편의 혹은 가치를 부여한다. 한국인터넷진흥원(2012)은 사물인터넷 기술을 초연결사회의 기반 기술로서 사물 간 인터넷 혹은 개체 간 인터넷으로 정의했고, 고유 식별이 가능한 사물이 만들어낸 정보를 인터넷을 통해 공유하는 환경이라고 정의했다[1].

세계 사물인터넷(Internet of Things) 시장 규모는 빠르게 성장하고 있다. 주요 기관별로 시장 예측 규모 결과가 차이가 있지만, Machine Research는 세계 M2M(Machine to Machine) 시장이 2014년 45억 개에서 2024년 290억 개로 증가할 것이라고 예상하고 있으며[2], IDC(International Data Cor- poration)에서는 세계 사물인터넷 시장 규모가 2022년까지 연평균 12.8% 성장하면서 1조 1,933억 달러에 달할 것으로 전망한 바 있다[3]. 사물인터넷 기술의 발달로 인해 센서 네트워크, 헬스케어, 분산 제어 시스템, 가상 물리 시스템 등 다양한 분야의 산업이 함께 성장하고 있으며, 이를 위한 소형 컴퓨팅 기기가 보편화되고 있다. 해당 분야들은 사용자들의 편리성 및 유용성을 제공하기 위해 사용자들의 민감한 정보나 음성/영상 DB, 각종 생활 정보 등의 빅데이터를 이용하므로 다양한 형태의 해킹 및 크래킹에 노출된다. 하지만 소형 컴퓨팅 기기들의 가용한 리소스는 제한되므로, 기존 서버나 PC 환경에서 사용되는 암호 알고리즘을 그대로 사용 시 구현상의 문제점이 발생한다. NIST의 표준으로 등재된 인증 암호화 알고리즘 CCM[4], GCM[5]도 연산 부하의 문제점이 존재하므로 제한된 환경에 적합하지 않다. 따라서 기존 알고리즘보다 더 적은 비용으로 적정 수준의 안전성과 효율성을 보장할 수 있는 경량암호 알고리즘의 필요성이 높아지고 있다.

미국 국립표준기술연구소(The National Instit- ute of Standards and Technology, NIST)는 미 상무부 소속의 비 관리기관으로, 산업 기술, 측정 기술 및 표준의 개발을 통해 미국 경제 성장을 촉진할 목적으로 설립되었다. NIST에서는 암호 기술들의 표준화도 담당하고 있으며, 2015년 7월부터 제한된 환경에 적합한 경량암호 알고리즘을 공모 및 표준화하는 사업을 진행하고 있

본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.
* 국민대학교 금융정보보안학과 (대학원생, hellosj3@kookmin.ac.kr, idealtop18@kookmin.ac.kr, tiontta@kookmin.ac.kr)
** 국민대학교 금융정보보안학과, 정보보안암호수학과 (교수, jskim@kookmin.ac.kr)

〔표 1〕 NIST 경량암호 공모사업 타임라인

Date	Event
2015.7	1차 경량암호 워크숍 개최
2016.10	2차 경량암호 워크숍 개최
2018.8	경량암호 제안 알고리즘 요구 사항 및 평가 기준 공표
2019.2	경량암호 제출 마감(총 57종)
2019.4	1라운드 후보 알고리즘 선정(총 56종)
2019.8	2라운드 후보 알고리즘 선정(총 32종)
2019.11	3차 경량암호 워크숍 개최

다[6]. 2019년 4월, 1라운드 후보 알고리즘 선정을 시작으로 같은 해 8월에는 32종의 2라운드 후보 알고리즘 선정을 완료했으며 2라운드가 현재까지 진행되고 있다. 현재까지 진행된 NIST 경량암호 공모사업의 타임라인은 [표 1]과 같다.

본 논문에서는 NIST 경량암호 공모사업에 대해 조사했으며 내용 구성은 다음과 같다. 2장에서는 공모사업 1라운드 결과를 제시하고, 3장에서는 공모사업 2라운드 후보로 선정된 암호 알고리즘을 특징별로 분류한다. 4장에서는 2라운드 후보 암호 알고리즘 중 일부의 설계 사상과 분석을 제시한다. 마지막으로 5장에서는 향후 전망 및 일정을 제시하며 본 논문에 대한 결론을 맺는다.

Ⅱ. NIST 경량암호 공모사업 1라운드 결과

NIST는 2018년 8월 27일, 제안되는 경량암호 알고리즘에 대한 요구 사항 및 평가 기준을 공표했다[7]. 제출되는 알고리즘은 관련 데이터로 인증된 암호화(Authenticated Encryption with Associated Data, AEAD)를 기능적으로 지원해야 하며 선택적으로 해싱 기능을 지원할 수 있다. 총 23개국의 연구원들이 서로 협업하여 57종의 알고리즘을 제출했고, 2019년 4월에 최종적으로 56종의 알고리즘이 1라운드 후보로 선정되었다.

2019년 8월 30일, NIST는 2라운드 후보 알고리즘을 선정하며 1라운드 탈락 알고리즘을 발표했다. 이어서 10월 7일, NIST 경량암호 공모사업 1라운드에 대한 현황 보고서(NISTIR 8268)[8]를 발표했으며, 1라운드 탈락 알고리즘들이 갖는 취약점을 제시했다[표 2].

〔표 2〕 1라운드 후보 알고리즘에 대한 공격

Attacks & Observations	Candidates
Forgery attacks	Bleep64, CLAE, FlexAEAD, GAGE and InGAGE, HERN and HERON, Liliput-AE, Limdolen, Qameleon, Quartet, Remus, Simple, SIV-Rijndael256, SIV-TEM-PHOTON, SNEIK, Sycon, TGIF, Triad
Length-extension attacks	CiliPadi, FlexAEAD
Distinguishing attacks	Limdolen
Undesirable properties	LAEM, SNEIK, CLX, TRIFLE

위조 공격은 서로 다른 입력 쌍(메시지, 키, 논스, 인증 데이터)에 대한 동일한 인증값(태그)을 생성하여 검증을 우회하는 공격이다. 공격 과정은 일반적으로 메시지나 인증 데이터에 변화를 주어 같은 태그를 생성하는 방식으로 이루어진다. 길이 확장 공격은 메시지 또는 인증 데이터의 길이를 확장하여 암호 알고리즘에서 사용하는 패딩의 취약성을 이용하는 공격이다. 대표적으로 CBC 운영모드의 패딩을 공격한 패딩 오라클 공격이 있다. 많은 알고리즘이 위조 공격에 취약했으며 일부는 길이 확장 공격이나 구별 공격에 취약했다. 특히 Limdolen 알고리즘은 full-round 차분 구별자가 발견되어 구별 공격이 가능했고 LAEM, SNEIK, CLX, TRIPLE 알고리즘은 공격에 적용 가능한 성질들이 발견되어 취약한 알고리즘으로 판정받았다. Fountain, Yarará and Coral 알고리즘은 NIST 보안 요구 사항을 만족하지 못했고, 안전성 분석도 충분히 제시하지 않아 1라운드에서 탈락했으므로 [표 2] 목록에서는 제외되었다.

Ⅲ. NIST 경량암호 공모사업 2라운드 선정 암호의 특징별 분류

2라운드 후보 알고리즘들은 내부에 탑재되는 핵심

〔표 3〕 핵심 함수에 따른 2라운드 후보 알고리즘 분류

Inner core function	AEAD(with Hashing)	AEAD(only)
Permutation based	ACE, ASCON, DryGASCON, Gimli, KNOT, ORANGE, PHOTON-Beetle, SPARKLE(SCHWAEMM and ESCH), Subterranean 2.0, Xoodyak	Elephant, ISAP, Oribatida, SPIX, SpoC, WAGE
Block cipher based	Saturnin	COMET, GIFT-COFB, HyENA, mixFeed, Pyjamask, SAEAES, SUNDAE-GIFT, TinyJAMBU
Tweakable block cipher based	SKINNY-AEAD and SKINNY-HASH	ForkAE, ESTATE, LOTUS-AEAD and LOCUS-AEAD, Romulus, Spook
Stream cipher based	-	Grain-128AEAD

함수에 따라 치환 기반, 블록암호 기반, 트위커블(Tweakable) 블록암호 기반, 스트림 암호 기반 AEAD로 분류할 수 있다[표 3].

공모사업에 가장 많이 제출된 치환 기반 AEAD는 Sponge 구조에 기반을 두고 있으며, 두 가지 작동 과정으로 이루어진다. 먼저 흡수 단계(Absorbing Phase)에서는 메시지를 초기 상태(State), 치환을 거쳐 생성되는 내부 상태와 XOR 연산시킨다. 모든 메시지를 흡수한 후, 압착 단계(Squeezing Phase)에서는 내부 상태의 일부 비트들을 추출하여 출력값을 생성한다. Sponge 구조는 인증모드뿐만 아니라 해시모드와 같은 다른 기능에 유연하게 적용할 수 있으며, 메시지를 처리할 때 전체 메시지나 메시지 길이의 송신 여부와 독립적으로 병렬적인 온라인 연산이 가능하다. 복호화는 구조상 암호화와 같으므로 추가적인 구현이 적다. Sponge 구조의 안전성은 내부 상태의 길이에 의존하며 bitrate와 capacity를 적절히 설정하여 효율성과 안전성을 유연하게 조절할 수 있다[9]. 또한 키 스케줄이 불필요하므로 메모리 관점에서 이득을 볼 수 있어 경량 기기에 적합하다[10][표 4].

블록암호 기반 AEAD는 일반적으로 블록암호의 안전성에 기반하여 설계된다. 예를 들어 AES[11]와 같이 안전성이 충분히 검증된 블록암호를 AEAD의 내부 핵심 함수로 사용 시 일정 수준 이상의 안전성을 기대할 수 있다. AES와 GIFT[12] 알고리즘이 핵심 함수로 가장 많이 쓰인 것을 알 수 있다[표 5].

트위커블 블록암호는 일반적인 블록암호에서 트윅(Tweak)이라 불리는 입력을 추가한 알고리즘이다[13]. 기존의 비밀 키가 암호에 불확실성을 제공한다면, 트윅은 가변성을 제공한다. 트위커블 블록암호 기반 AEAD도 블록암호 기반 AEAD와 유사하게 기존에 제안된 SKINNY와 같은 트위커블 블록암호를 토대로 설계가 가능하다는 장점이 있다. 제안된 트위커블 블록암호 기

〔표 4〕 치환 기반 AEAD의 핵심 함수

AEAD	Core functions
ACE	ACE-320
ASCON	ASCON-320
DryGASCON	GASCON-128/256
Gimli	Gimli-384
KNOT	KNOT-256/384/512
ORANGE	PHOTON-256
PHOTON-Beetle	PHOTON-256
SPARKLE (SCHWAEMM)	Sparkle-256/384/512
Subterranean 2.0	Subterranean
Xoodyak	XOODOO-384
Elephant	Spongent-160/176, Keccak-200
ISAP	Keccak-400, ASCON-320
Oribatida	SimP-256-2/4, SimP-192-2/4
SPIX	sLiSCP-light-256
SpoC	sLiSCP-light-256
WAGE	WAGE-259

〔표 5〕 블록암호 기반 AEAD의 핵심 함수

AEAD	Core functions
Saturnin	Saturnin-256/256
COMET	AES-128, Speck-64/128, CHAM-128/128, CHAM-64/128
GIFT-COFB	GIFT-128
HyENA	GIFT-128
mixFeed	AES-128
Pyjamask	Pyjamask-96, Pyjamask-128
SAEAES	AES-128, AES-192, AES-256
SUNDAE-GIFT	GIFT-128
TinyJAMBU	JAMBU-128

〔표 6〕 트위커블 블록암호 기반 AEAD의 핵심 함수

AEAD	Core functions
SKINNY-AEAD	SKINNY-128-256
ForkAE	SKINNY-64-192, SKINNY-128-192, SKINNY-128-256, SKINNY-128-288
ESTATE	TweGIFT-128, TweAES-128, TweAES-128-6
LOTUS-AEAD and LOCUS-AEAD	TweGIFT-64
Romulus	SKINNY-128-256, SKINNY-128-384
Spook	Clyde-128

〔표 7〕 스트림 암호 기반 AEAD의 핵심 함수

AEAD	Core function
Grain-128AEAD	Grain-128a

반 AEAD 중 상당수가 핵심 함수로 SKINNY 알고리즘을 사용했음을 알 수 있다[표 6].

스트림 암호 기반 AEAD는 Grain-128AEAD[14]를 제외하고 모두 위조 공격에 취약하여 1라운드에서 탈락했다[표 5]. 스트림 암호는 블록암호와 달리 다양한 길이의 메시지를 허용할 수 있으며, 따라서 운영 모드가 필요하지 않게 된다. 또한 긴 메시지 암호화 시, 블록암호보다 에너지 측면에서 효율적이므로 리소스가 제한된 경량 기기에 더 적합하다[15].

Ⅳ. 2라운드 선정 알고리즘 일부의 구조 및 설계 논리

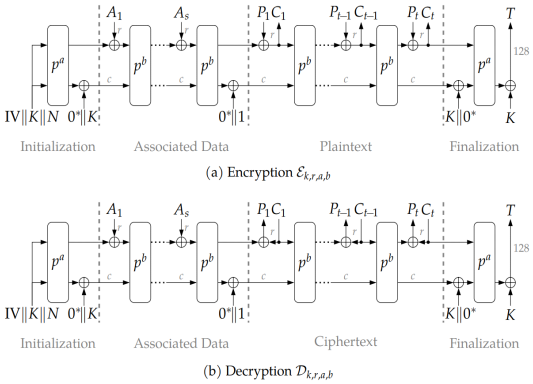
2012년부터 2018년까지 CAESAR 경진대회를 통해 경량성과 보안성을 갖춘 알고리즘들이 제안되었으며 최종적으로 경량 하드웨어 구현, 고속 소프트웨어 구현, 높은 안전성 측면에서 각 2종의 알고리즘이 최종 선정되었다[16]. 반면 NIST 경량암호 공모사업은 경량 인증암호 알고리즘에 초점을 맞추고 있으며, 이에 따라 CAESAR 경진대회에 참가한 알고리즘 중 알고리즘을 다소 수정하거나 추가하여 재참가한 알고리즘들이 존재한다. 본 장에서는 NIST 공모사업 2라운드 선정 알고리즘 중 CAESAR 경진대회에서 발표되었던 ASCON과 TinyJAMBU의 구조 및 설계 논리를 소개한다. 본 장의 내용은 CAESAR 경진대회 및 NIST 경량암호 워크숍에서 발표된 학술 자료를 근거로 한다[17].

4.1. ASCON

ASCON[18]은 CAESAR 경진대회에서 우승을 차지한 경량 인증암호 알고리즘이다. ASCON은 하드웨어와 소프트웨어의 각 환경에서 보안과 크기와 속도의 최상의 균형을 목표로 한다. NIST에 발표된 ASCON 패밀리는 인증암호와 함께 ASCON-Hash라는 256-비트 길이의 해시암호와 ASCON-Xof라는 가변길이의 해시암호를 추가하여 발표했다.

ASCON은 12라운드의 Sponge 구조를 채택했으며, 이는 SpongeWrap, MonkeyDuplex 구조[10]와 비슷하다[그림 1]. ASCON의 Sponge 구조에 사용된 블록암호는 SPN(Substitution Permutation Network) 구조이다. Substitution Layer에 사용된 S-box는 diffusion을 향상시키기 위해 SHA-3의 우승암호 Keccak[19]의 S-box에 아핀변환을 적용하여 얻은 새로운 S-box를 사용했으며, Permutation Layer는 SHA-2에서 사용된 Σ 함수와 유사한 선형함수를 사용했다.

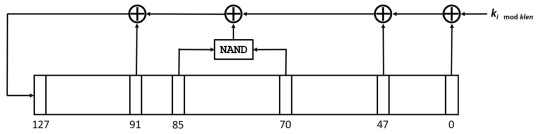
ASCON은 CAESAR 경진대회를 통해 검증된 암호알고리즘이므로, 안전성이 보장되어있다고 주장한다. 현재까지 가장 많은 라운드를 공격한 논문은 Cubic 공



〔그림 1〕 ASCON 인증암호의 암·복호화 과정

격을 응용하여 전체 12라운드 중 7라운드를 공격했다[20]. ASCON은 키를 사용한 초기 함수와 최종 함수가 포함된 Sponge 구조를 사용한다는 점에서 일반적인 Sponge 구조와 차별점을 갖는다. 따라서 일반적인 Sponge 구조는 부채널 공격 등의 이유로 공격자가 중간값을 얻게 되면 마스터키 복구나 위조 공격의 위험성이 커지지만, 키를 사용한 초기 함수와 최종 함수가 이를 방지해주므로 더 강한 안전성을 보장해준다.

효율성 관점에서도 ASCON은 64-비트 워드 내에서의 연산(NOT, AND, OR, XOR, rotation)만 사용하여 구현할 수 있으므로, 별도의 메모리가 필요 없다는 장점이 있다. 또한, 사용된 S-box와 선형함수는 모두 비트 슬라이싱 논리를 적용할 수 있고, 5개의 64-비트 워드로 병렬적으로 처리할 수 있어 속도 향상이 가능하다. 64-비트 워드를 사용하지 못하는 8-비트, 16-비트, 32-비트 프로세서와 같은 환경에서도 bit-interleaving 기술[21]을 사용하여 효율적인 병렬 처리가 가능하다. 키 스케줄, inverse permutation이 불필요하기 때문에 경량



〔그림 2〕 TinyJAMBU에서 사용하는 128-비트 NFSR

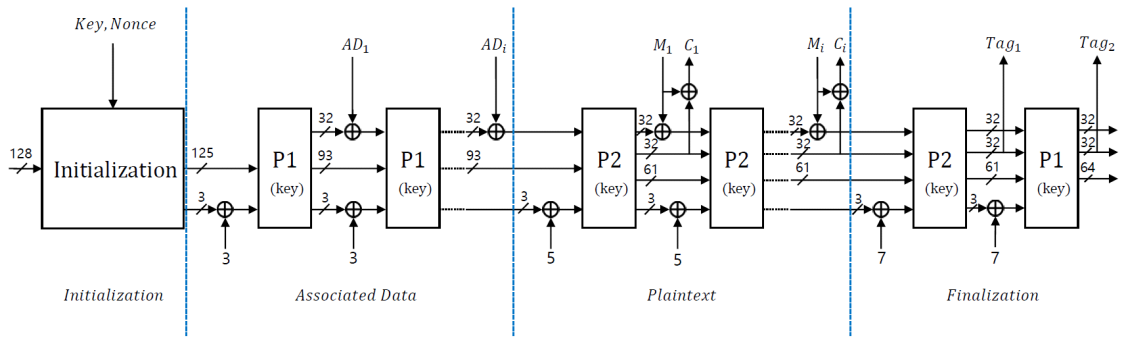
기기에 적합하다.

4.2. TinyJAMBU

JAMBU[22]는 CAESAR 경진대회의 3라운드 후보로 선정됐고, 해당 경진대회 제출 알고리즘 중 가장 작은 내부 블록 크기를 갖는 인증모드로 알려져 있다. JAMBU의 설계자들은 알고리즘을 약간 변경하여 128, 129, 256-비트 크기의 키를 지원하는 TinyJAMBU[23]를 제안했다.

TinyJAMBU는 MonkeyDuplex 구조를 채택했고, NFSR(Nonlinear Feedback Shift Register)[그림 2]을 기반으로 한 keyed permutation을 핵심 함수로 사용했다. 사용된 keyed permutation은 키 스케줄이 불필요하며 128-비트 키를 기준으로 초기, 최종 함수, 인증 데이터 처리 과정에서는 384번, 암호화, 복호화 과정에서는 1024번 반복해 사용한다. 또한 TinyJAMBU의 메시지 블록 크기와 내부 상태 크기는 JAMBU와 비교했을 때 각각 0.5, 1.5배이다[그림 3].

TinyJAMBU는 비밀 키가 기기에 저장된 기기에 최적화된 경량 인증암호를 제안하고 있다. 따라서 설계자들은 알고리즘을 논스, 인증 데이터, 메시지를 조절할 수 있는 공격자를 가정하여도 키 복구 공격을 계산적으로 불가능하게 하도록 설계하였다. 일반적으로 논스를 재사용하면 메시지에 대한 기밀성을 보장할 수 없지만,



〔그림 3〕 TinyJAMBU의 암호화 및 태그생성과정

TinyJAMBU는 논스가 재사용되더라도 비밀키를 탈취하기 위해 2^{112}의 연산이 필요하도록 설계하여 NIST의 안전성 요구사항을 충족했다. 그뿐만 아니라 논스 재사용 시 인증에 대한 위조 공격 가능성도 굉장히 낮도록 설계했다. 그러나 경량암호 3차 워크숍에서 TinyJAMBU에 대한 소프트웨어 구현 수치는 제시된 바 있지만[24], 안전성 관점에서의 암호분석은 설계자들의 제안논문을 제외하고는 찾아보기 어렵다. 향후 워크숍이나 논문을 통해 추가적인 분석이 제시되어야 할 것이다.

TinyJAMBU는 고정 키를 사용하는 하드웨어에 최적화된 경량 인증암호 알고리즘이다. 비밀 키가 기기에 이미 저장되어 있으면 keyed permutation을 사용하여 공격자가 오프라인으로 내부 상태를 계산하는 것을 방지할 수 있으므로 내부 상태를 작게 설계할 수 있다고 주장한다. 또한 keyed permutation의 기반이 되는 NFSR은 하드웨어 비용이 매우 낮으며, 효율적인 소프트웨어와 하드웨어 구현을 위해 여러 단계를 병렬 처리할 수 있도록 설계됐다. keyed permutation 내부에서 키 스케줄이 불필요하므로 키 스케줄에 대한 하드웨어 비용을 줄일 수 있다.

Ⅴ. 결 론

2019년 11월, NIST는 경량암호 3차 워크숍을 개최했고, 이 자리에서 1라운드 탈락 알고리즘들이 갖는 취약점 분석과 2라운드 선정 알고리즘들의 안전성 분석 및 효율성 분석 내용이 발표되었다[17]. NIST 경량암호 공모사업이 경량 인증암호 알고리즘에 초점을 맞추고 있는 만큼 향후 2라운드 선정 알고리즘들에 대한 하드웨어와 소프트웨어 등 여러 환경에서의 벤치마킹과 구현 효율성 분석이 집중적으로 이루어질 것으로 예상된다.

NIST는 2라운드 후보 알고리즘에 대한 분석을 1년 정도 진행할 것이며, 3라운드 후보로 총 8종의 알고리즘을 선정할 예정이라고 밝혔다[25]. 또한, 각 알고리즘의 장점을 취하기 위한 후보 간 알고리즘 결합은 해당 공모사업에서 진행하지 않으며, 공모사업 후에 경량암호 포럼 등을 통해 논의될 수 있다고 밝혔다. 향후 일정은 다음과 같다.

〈NIST 경량암호 공모사업 향후 일정〉

- ○ 3라운드 후보 알고리즘 선정
  (총 8종, 2020년 10월 예정)
- ○ 4차 경량암호 워크숍 개최
- ○ 최종 알고리즘 선정 (2021년 예정)

사물인터넷 환경의 발전에 따라 사용자들은 소형 컴퓨팅 기기들을 많이 사용하며 편리성을 추구하지만, 정보보안 측면에서는 안전하지 않은 경우가 많다. 이번 NIST 경량암호 공모사업을 통해 충분히 검증된 경량암호 알고리즘이 표준화된다면, 광범위한 시장에서 적용 가능할 것이며 사물인터넷 환경 보안에도 큰 기여를 할 것으로 예상된다.

참 고 문 헌

[1] 배상태, 김진경, “사물인터넷(IoT) 발전과 보안의 패러다임 변화,” KISTEP InI 14호, 2016.

[2] Press Release: Global Internet of Things market to grow to 27 billion devices, generating USD3 trillion revenue in 2025, Gartner, https://machinaresearch.com/news/press-release-global-internet-of-things-market-to-grow-to-27-billion-devices-generating-usd3-trillion-revenue-in-2025/, Visited on May 17. 2020.

[3] Internet of Things Ecosystem and Trends, IDC, https://www.idc.com/getdoc.jsp?containerId=IDC_P24793, Visited on May 18. 2020.

[4] Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality(SP 800-38D), NIST, https://csrc.nist.gov/publications/detail/sp/800-38c/final

[5] Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC(SP 800-38D), NIST, http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

[6] Lightweight Cryptography, NIST, https://csrc.nist.gov/Projects/lightweight-cryptography, Visited on May 18. 2020.

[7] Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process, NIST,

https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf

[8] Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process, NIST, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8268.pdf, Visdited on May 4. 2020.

[9] Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche, “Cryptographic sponge functions,” STMicroelectronics, 2011.

[10] Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche, “Permutation-based encryption, authentication and authenticated encryption,” STMicroelectronics, 2012.

[11] FIPS-197, NIST, “Advanced Encryption Standard,” Nov. 2001.

[12] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim and Yosuke Todo, “GIFT: A Small Present Towards Reaching the Limit of Lightweight Encryption,” CHES’17, LNCS 10529, pp.321-345, Sep. 2017.

[13] Moses Liskov, Ronald L. Rivest, David Wagner, “Tweakable block ciphers,”Advances in Cryptology, CRYPTO’02, LNCS 2442, pp.31-46, 2002.

[14] Grain-128AEAD, https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Grain_128AEAD-spec.pdf

[15] Subhadeep Banik, Vasily Mikhalev, Frederik Armknecht, Takanori Isobe, Willi Meier, Andrey Bogdanov, Yuhei Watanabe and Francesco Regazzoni, “Towards low energy stream ciphers,”IACR Transactions on Symmetric Cryptology, pp.1-19, Jun. 2018.

[16] Competition for Authenticated Encryption: Security, Applicability, CAESAR, and Robustness, http://competitions.cr.yp.to/caesar.html, Visited on May 4. 2020.

[17] Lightweight Cryptography Workshop 2019, https://csrc.nist.gov/events/2019/lightweight-cryptography-workshop-2019

[18] ASCON, https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf

[19] SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, NIST, “https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf,” Aug. 2015.

[20] Zheng Li, Xiaoyand Dong and Xiaoyun Wang, “Conditional Cube Attack on Round-Reduced ASCON,” IACR, Trans. Symmetric Cryptol, pp.175-202, Mar. 2017.

[21] Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche and Ronny Van Keer, “Keccak implementation overview,” STMicroelectronics, 2012.

[22] Hongjun Wu and Tao Huang, “The JAMBU Lightweight Authentication Encryption Mode,” Competition for Authenticated Encryption: Security, Applicability, CAESAR, and Robustness, 2016.

[23] TinyJAMBU, https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/TinyJAMBU-spec.pdf

[24] Benchmarking Software Implementations of 1st Round Candidates of the NIST LWC Project on Microcontrollers, https://csrc.nist.gov/Presentations/2019/benchmarking-software-implementations-of-1st-round

[25] NIST Lightweight Cryptography Standardization: Next Steps, https://csrc.nist.gov/Presentations/2019/nist-lightweight-cryptography-standardization-next

〈저자소개〉

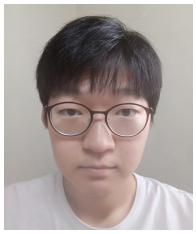
백 승 준 (Seungjun Baek)

학생회원

2019년 2월 : 국민대학교 수학과 졸업

2020년 3월~현재 : 국민대학교 금융정보보안학과 석사과정

<관심분야> 정보보호, 암호 알고리즘



전 용 진 (Yongjin Jeon)

학생회원

2018년 8월 : 국민대학교 수학과 졸업

2018년 9월~현재 : 국민대학교 금융정보보안학과 석사과정

<관심분야> 정보보호, 암호 알고리즘

김 한 기 (Hangi Kim)

학생회원

2016년 2월 : 국민대학교 수학과 졸업

2018년 2월 : 국민대학교 금융정보보안학과 석사

2018년 3월~현재 : 국민대학교 금융정보보안학과 박사과정

<관심분야> 정보보호, 암호 알고리즘

김 종 성 (Jongsung Kim)

종신회원

2000년 8월/2002년 8월 : 고려대학교 수학 전공 학사/이학석사

2006년 11월 : K.U.Leuven. ESAT/SCD-COSIC 정보보호 전공 공학박사

2007년 2월 : 고려대학교 정보보호대학원 공학박사

2007년 3월~2009년 8월 : 고려대학교 정보보호기술연구센터 연구교수

2009년 9월~2013년 2월 : 경남대학교 e-비즈니스학과 조교수

2013년 3월~2017년 2월 : 국민대학교 수학과 부교수

2014년 3월~현재 : 국민대학교 일반대학원 금융정보보안학과 부교수

2017년 3월~현재 : 국민대학교 정보보안암호수학과 부교수

<관심분야> 정보보호, 암호 알고리즘, 디지털 포렌식