NIST 경량암호 표준화 공모전 진행 동향

권혁동[1], 엄시우[2], 심민주[2], 서화정[2]
[1]한성대학교 정보컴퓨터공학과
[2]한성대학교 IT융합공학부
korlethean@gmail.com, shuraatum@gmail.com, minjoos9797@gmail.com,
hwajeong84@gmail.com

A Study on Progression of NIST lightweight cryptography standardization competition

Hyeok-Dong Kwon[1], Si-Woo Eum[2], Min-Joo Sim[2], Hwa-Jeong Seo[2]
[1]Dept. of Information Computer Engineering, Hansung University
[2]Dept. of IT Convergence Engineering, Hansung University

요 약

미국 국립표준기술연구소는 사물 인터넷 환경 상에서 원활하게 구동할 수 있는 경량암호의 표준화 공모전을 개최하였다. 경량암호 표준화 공모전은 2019년 Round 1 결과가 발표되었고, 2021년에는 최종 라운드 후보를 발표하였다. 최종 선정된 알고리즘은 총 10종이다. 선정된 알고리즘은 동작 방식에 따라서 순열 기반, 블록암호 기반, 트위커블 블록암호 기반, 그리고 스트림 암호 기반으로 분류된다. 또한 필수적으로 AEAD 기능을 제공할 것을 요구하며, 추가적으로 해시 기능을 제공하기도 한다. 본 논문에서는 국립표준기술연구소에서 진행한 경량암호 표준화 공모전의 최종 라운드에 대해서 확인해본다.

1. 서론

사물 인터넷 환경 상에서는 사용 가능한 자원이 제한되며 그에 따라 연산 능력이 줄어들게 된다. 일반적으로 암호 알고리즘은 복잡한 연산을 사용하기 때문에 사물 인터넷 환경에서는 원활한 가동이 어려울 수 있다. 이를 타개하기 위해서 경량암호가 제안되었다. 경량암호는 일반적인 암호 알고리즘에 비해 더 적은 연산량을 요구하여 암호화를 제공한다.

미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 경량암호 표준화 선정을 위해 경량암호 표준화 공모전을 개최하였다.

본 논문에서는 경량암호 표준화 공모전의 진행 사항과 최종 라운드의 후보군에 대해서 간단하게 살펴본다.

2. NIST 경량암호 공모전

NIST는 경량암호 공모전을 개최하며 평가 기준을 공개하였다[1]. 기본적으로 모든 알고리즘은 AEAD(Authenticated Encryption with Associated Data)를 제공해야 한다. 추가적으로 Hash를 제공해도 되지만 이는 필수항목은 아니다.

NIST 경량암호 공모전은 2019년에 Round 1 후보를 공지하였다[2]. Round 1 후보 알고리즘은 총 56종으로 표 1과 같이 정리된다.

<Table 1> Round 1 candidates of NIST lightweight cryptography standardization competition.

Base	AEAD+Hash	AEAD only
Permutation	ACE, ASCON, CLS and other 15 kinds	CiliPadi, Elephant, Fountain and other 5 kinds
Block cipher	Saturnin, SIV-Rijndael	COMET, FlexAEAD, GIFT_COFB and 10 kinds
Tweakable Block cipher	SKINNY-AEAD and SKINNY-Hash	ForkAE, ESTATE, Lilliput-AE and 6 kinds
Stream cipher	Triad	Bleep64, CLAE, Grain-128AEAD and 1 kind

NIST는 제안된 경량 암호의 내부 동작 원리에 따라 permutation 기반, block cipher기반, tweakable block cipher 기반, 그리고 stream cipher 기반으로 분류하였다. 전체적인 투고 결과, AEAD만 지원하는 알고리즘이 12개 더 많았다.

2019년에는 Round 2 후보 알고리즘을 공개하였다. 이때 탈락한 알고리즘은 표 2와 같은 사유로 탈락하였다[3].

<Table 2> Reason for dropping out of Round 1 algorithm.

Attack type	Algorithms
Forgery	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	CiliPadi, FlexAEAD
Distinguishing	Limdolen
Undesirable properties	LAEM, SNEIK, CLX, TRIFLE

탈락한 알고리즘은 취약점 분석을 통과하지 못한 알고리즘들로 총 4가지 사유가 존재한다. Forgery는 서로 다른 값을 입력하여 같은 인증 값을 생성하는 위조 공격이다. Length-extension은 지정된 입력 길이를 초과하여 입력할 때 적용되는 패딩의 취약점을 사용하는 공격이다. Distinguishing은 암호문과 난수와 구별되는 특성을 의미한다. 정상적인 경우에는 구분되지 않아야 한다. 마지막으로 Undesirable properties는 그 외에 공격이 적용 가능한 것을 뜻한다. 결과적으로 Round 2에 진출한 알고리즘은 표 3과 같다. Round 1에서 24개의 알고리즘이 탈락하여 총 32개의 알고리즘이 Round 2로 진출하였다[4].

Round 2 결과, 대부분의 알고리즘은 permutation 기반이다. 또한 stream cipher 기반 알고리즘은 Round 1 진출에서도 가장 적었는데, Round 2에서는 Grain-128 AEAD를 제외하고는 모두 탈락하였다. 따라서 stream cipher 기반 알고리즘은 hash를 제공하는 알고리즘도 진출하지 못했다.

<Table 3> Round 2 candidates of NIST lightweight cryptography standardization competition.

Base	AEAD+Hash	AEAD only
Permutation	ACE, ASCON, DryGASCON, Gimli, KNOT, ORANGE, PHOTON-Beetle, SPARKLE, Subterranean 2.0, Xoodyak	Elephant, ISAP, Oribatida, SPIX, SpoC, Spook, WAGE
Block cipher	SATURNIN	COMET, GIFT-COFB, HyENA, mixFeed, Pyjamask, SAEAES, SUNDAE-GIFT, TinyJAMBU
Tweakable Block cipher	SKINNY-AEAD and SKINNY-HASSH	ESTATE, ForkAE, LOTUS-AEAD and LOCUS-AEAD, Romulus, Spook
Stream cipher	-	Grain-128AEAD

2021년에는 Round 3가 발표되었다. NIST는 Round 3가 최종 라운드임을 공표하였다. Round 3에는 10개의 알고리즘이 진출하였으며, 전체적인 목록은 표 4와 같다. 표 4에서는 최종 라운드 후보 알고리즘의 목록과 해시 지원 여부, 기반 원리 및 사용하는 코어 함수에 대해서 확인할 수 있다.

제안된 알고리즘의 코어 함수를 확인해보면 기존에 사용되던 또는 제안되었던 알고리즘들이 있는 것을 확인할 수 있다. 이는 상당수의 알고리즘이 기존에 제안되었던 암호를 개량해서 투고되었음을 알 수 있다. 또한 TinyJAMBU와 같은 알고리즘은 Round 2에서는 block cipher 기반으로 분류되었지만 Round 3에서는 permutation 기반으로 재분류 되었다. 이는 NIST에서 투고된 후보 알고리즘을 검토하며 코어 함수의 종류 보다는 내부 동작 원리에 집중했다고 볼 수 있다.

<Table 4> Finalist candidates of NIST lightweight cryptography standardization competition.

Algorithm	Base	Hash	Core function
Grain-128AEAD	Stream cipher	X	Grain-128a
GIFT-COFB	Block cipher	X	GIFT-128
Romulus	Twekable block cipher	O	SKINNY-128-256, SKINNY-128-384
ASCON	Permutation	O	ASCON-320
ISAP	Permutation	X	Keccak-400, ASCON-320
PHOTON-Beetle	Permutation	O	PHOTON-256
Elephant	Permutation	X	Spongent-160/176, Keccak-200
SPARKLE	Permutation	O	Sparkle-256/384/512
TinyJambu	Permutation	X	JAMBU-128
Xoodyak	Permutation	O	Xoodoo-384

3. 결론

본 논문에서는 NIST에서 진행한 경량암호 공모전의 진행 과정에 대해서 간략하게 살펴보았다. 최초 56개의 알고리즘으로 시작한 본 공모전은 현재 10개의 알고리즘만 남아 경합을 벌이고 있다.

사물 인터넷 상에서의 보안 연구는 오래전부터 이어지고 있으며, 앞으로 사물 인터넷 산업이 발전할수록 더욱 요구될 것으로 전망된다[6]. 따라서 NIST의 경량암호 공모전의 결과는 사물 인터넷 보안 분야에 큰 영향을 끼칠 것으로 예상된다. 또한 경량암호는 요구하는 연산량이 적지만, 사물 인터넷 환경마다 통신에 필요한 자원이 얼마나 될 지는 알 수 없다. 때문에 경량암호를 사물 인터넷 환경에서 최적화 하는 연구도 지속되어야 할 것이다.

4. Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services).

참고문헌

[1] L. Bassham, Ç. Çalık, K. McKay, and M. S. Turan, “Submission requirements and evaluation criteria for the lightweight cryptography standardization process,” *US National Institute of Standards and Technology*, 2018.

[2] M. S. Turan, K. A. McKay, Ç. Çalik, D. Chang, and L. Bassham, “Status report on the first round of the NIST lightweight cryptography standardization process,” *National Institute of Standards and Technology*, Gaithersburg, MD, NIST Interagency/Internal Rep.(NISTIR), 2019.

[3] S. Baek, Y. Jeon, H. Kim, and J. Kim, “NIST Lightweight Crypto Competition Business Trend,” *Review of KIISC*, Vol. 30, No. 3, 17-24, 2020.

[4] M. S. Turan, K. McKay, D. Chang, C. Calik, L. Bassham, J. Kang, and J. Kelsey, “Status report on the second round of the NIST lightweight cryptography standardization process,” *National Institute of Standards and Technology Internal Report*, 8369(10.6028), 2021.

[5] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y. K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. S. Tone, “Status report on the third round of the nist post-quantum cryptography standardization process,” *US Department of Commerce, National Institute of Standards and Technology (NIST)*, 2022.

[6] J. N. Kim, and S. H. Jin, “Research on Internet of Things (IoT) security technology to respond to security threats in a hyper-connected environment,” *Information and Communications Magazine*, Vol. 34, No. 3, 57-64, 2017.