NIST 경량암호 공모전 동향

권혁동[1], 엄시우[2], 심민주[2], 서화정[2]
[1]한성대학교 정보컴퓨터공학과
[2]한성대학교 IT융합공학부

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

서론

NIST 경량암호 공모전

결론

서론

- IoT 디바이스의 발전에 따라 무선 보안의 중요성이 대두됨
  - 사물 인터넷과 같은 환경은 **대체로 가용 자원이 제한적**
  - **암호 알고리즘의 구동이 어려움**
- **요구 자원이 적은 경량암호**의 발전
- NIST에서는 경량암호 표준화를 위한 공모전을 개최
- 공모전의 현 진행 상황에 대해 정리

NIST 경량암호 공모전

- 2018년 공모전 개최 시작
- 요구사항
  - **AEAD(Authenticated Encryption with Associated Data) 모드 제공**
  - 일반적인 블록암호 운용 방식은 암호화와 인증을 동시에 제공하기 어려움
  - **AE는 암호문에 인증 값(태그)를 생성**하여 인증과 암호화를 동시에 제공
  - AEAD는 관련 데이터를 사용하여, **무결성까지 제공**
  - Hash는 선택 사항
- 최초 투고된 암호는 총 57종
- 2019년 Round 1 후보 공지
  - 56종 암호가 선정됨

NIST 경량암호 공모전

- 각각의 암호 알고리즘은 4가지 기반 원리로 분류됨
  - 순열(Permutation), 블록암호(Block cipher),
    트위커블-블록암호(Tweakable blolck cipher), 스트림 암호(Stream cipher)

Type	AEAD-Hash	AEAD only
Permutation	ACE, ASCON, CLX and 5 kinds	CiliPadi, Elephant, Fountain and 15 kinds
Block cipher	Saturnin, SIV-Rijndael	COMET, FlexAEAD, GIFT-COFB and 10 kinds
Tweakable block cipher	SKINNY-AEAD & SKINNY-Hash	ForkAE, ESTATE, Lilliput-AE and 6 kinds
Stream cipher	Triad	Bleep64, CLAE, Grain-128AEAD and 1 kind

NIST 경량암호 공모전

- Round 2 진행
  - 2019년 8월, 24종이 탈락하고 **32종의 알고리즘이 선정**
- 취약점을 4가지로 분류
  - **위조(Forgery)**: 서로 다른 입력 쌍으로 같은 태그 값 생성
  - **길이 확장(Length Extension)**: 입력 값을 늘렸을 때 발생하는 패딩 취약점
  - **구별(Distinguishing)**: 암호화된 데이터와 난수를 구분
  - **알고리즘 구성이 취약함(Undesirable properties)**

NIST 경량암호 공모전

- 32종의 알고리즘이 Round 2에 잔류
  - 추가적인 취약점을 분석하여 Round 3 진행

Type	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 & SKINNY-Hash	ESTATE, ForkAE, LOTUS-AEAD and LOCUS-AEAD, Romulus, Spook
Stream cipher	Triad	Grain-128AEAD

NIST 경량암호 공모전

- Round 3 진행
  - 2021년 3월 22종의 알고리즘이 탈락하고 **10종의 알고리즘**이 선정
- 각 기반의 특징
  - **블록 암호(트위커블-블록암호)**: 경량 블록 암호를 기반으로 동작
    기존 경량 암호를 활용했기에, 다른 기반에 비해 암호가 가벼움
  - **순열**: Sponge 구조를 사용하여 해시 제공에 유리함
    또한 Round 3에 가장 많이 남은 유형의 알고리즘
  - **스트림 암호**: 스트림 암호를 기반으로 동작
    하지만 Round 3에 가장 적은 수의 알고리즘만 남음

NIST 경량암호 공모전

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

결론

- NIST 경량암호 공모전의 진행에 대해서 간단히 살펴봄
- 현재 다른 암호 공모전에 비해 관심도가 저조함
  - 경량암호의 중요성이 상대적으로 떨어지기 때문
- 아직 많은 연구 결과가 존재하지 않으므로 연구 주제로 삼기 좋음
  - 경량암호의 구조는 단순한 편이기에 접근성도 높음
- 추후 최종 선정 알고리즘에 따라 새로운 연구 분야가 개척될 수 있음
  - 양자내성 공모전과 마찬가지로 추가 라운드도 진행 가능

Q & A