NIST 경량암호 공모전 TinyJAMBU의 기능적 고찰

A study of the NIST lightweight cryptography contest TinyJAMBU

권혁동*, 엄시우**, 심민주**, 서화정**
한성대학교 정보컴퓨터공학과*
한성대학교 IT융합공학부**

서론

- IoT 기기의 발전에 따라 경량암호의 중요성이 올라감
- NIST 에서는 경량암호 표준화 공모전을 개최
- 제출된 작품 중 TinyJAMBU에 대해서 분석

NIST 경량암호 공모전

- 2018년 개최된 경량암호 표준화 선정을 위한 공모전
- 2022년 현재 최종 라운드 진행 중
- 최종 라운드 후보군은 [표 1]에서 확인 가능
- 요구사항으로 AEAD(Authenticated Encryption with Associated Data) 기능을 필수로 제공해야 함
- 해시 기능 지원은 선택 사항

Table. 1. The finalists of NIST lightweight cryptography standardization.

Core function	AEAD + Hashing	AEAD only
Permutation	ASCO, PHOTON-Beetle SPARKLE, Xoodyak	Elephant, ISAP
Block Cipher	-	GIFT-COFB, TinyJAMBU
Tweakable Block cipher	-	Romulus
Stream Cipher	-	Grain-128 AEAD

TinyJAMBU

- JAMBU는 CAESAR 경진대회에서 제안된 암호
- CAESAR에서 가장 작은 블록 크기를 보유함
- TinyJAMBU는 JAMBU를 변형한 알고리즘
- 블록암호 기반의 내부 연산을 지원
- 하지만 **실제 동작은 스트림암호**와 유사
- 128-bit, 192-bit, 256-bit 세 종류의 키 사이즈 지원
- 96-bit의 논스 사용
- 키 스케쥴 없이 keyed permutation을 반복적으로 사용

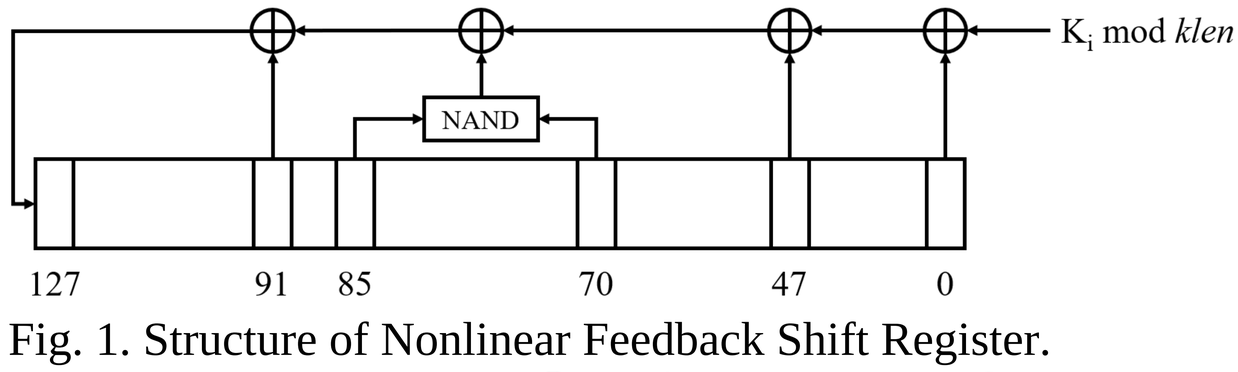

Fig. 1. Structure of Nonlinear Feedback Shift Register.

- Keyed permutation 연산을 위해 [그림 1]과 같은 NLFSR 사용
- Keyed permutation은 P_n으로 지칭되며 n은 [표 2]를 따름

Table. 2. The list of number of permutation.

Key length	128	192	256
Initialization Key	1024	1152	1280
Initialization Nonce	640	640	640
Processing Associated Data	640	640	640
Encryption Decryption	1024	1152	1280
Finalization	1024, 640	1152, 640	1280, 640
Verification	1024, 640	1152, 640	1280, 640

결론

- TinyJAMBU의 기능적인 면에 대해서 간단히 살펴봄
- Round 2에는 차분/선형 분석에 취약점이 존재
- Final에서는 keyed permutation 횟수를 늘려서 이를 해결
- 간단한 구조지만 너무 많은 keyed permutation이 필요
- 이를 최적화 하는 연구가 필요

참고문헌

1. D.S.Milojicic, V.Kalogeraki, R.Lukose,K.Nagaraja, J.Pruyne, B.Richard, S.Rollins and Z.Xu, Peer to Peer Computing, HP Laboratories Palo Alto HPL-2002-57, March, 2002.
2. H.J.Kim, J.H.Park, H.D.Kwon, and H.J.Weo, “A trend of NIST cryptography standardization contest,” Review of KIISC, 30(6), 117-123, 2020.
3. H.wu, and T.Huang, “JAMBU lightweight authenticated encryption mode and AES-JAMBU,” CAESAR competition proposal, 2014.
4. H.Wu, and T.Huang. “TinyJAMBU: A family of lightweight authenticated encryption algorithms (version 2),” Submission to the NIST Lightweight Cryptography Standardization P rocess, 2021.
5. S.J.Baek, Y.G.Jeon, H.G.Kim, and J.S.Kim, “Technology trend of NIST Lightweight Cryptography Competition,” Review of KIISC, 30(3), 17-24, 2020.
6. D.Saha, Y.Sasaki, D.Shi, F.Sibleyras, S.Sun, and Y.Zhang, “On the security margin of TinyJAMBU with refined differential and linear cryptanalysis,” IACR Transactions on Symmetric Cryptology, 152-174, 2020.

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB