NIST 경량암호 공모 최종 후보 양자회로 구현 동향

오유진 * 장경배 * 임세진 * 양유진 * 서화정 *†
* 한성대학교 대학원 융합보안학과

서 론

- 사물인터넷(Internet of Things, IoT)의 발전으로 초소형 스마트 기기의 보안성 문제가 대두됨 → 경량 암호 기술 연구
- 미국 국립표준기술연구소(The National Institute of Standard and Technology, NIST)에서는 경량 암호 표준화 공모전을 주최 (특히 AEAD (Authenticated Encryption with Associated Data) 형태의 암호) → 최종적으로 10개의 후보군이 선정
- 현재 암호시스템은 양자 컴퓨터의 발전으로 양자 알고리즘인 Grover 알고리즘을 통해 대칭 키 또한 키 전수 조사를 루트만큼 감소시킬 수 있음.
- 본 논문에서는 NIST 경량암호 표준화 공모전에 선정된 암호 중 ASCON, Sparkle, Grain-128AEAD에 대한 양자 회로 구현 동향에 대해 살펴보고 공격 비용을 비교함

관련 연구

● NIST 양자 후 보안 레벨

- NIST는 AES에 대한 양자 공격 복잡성을 기반으로 사후 양자 보안 기준을 수립하였다.
- Level 1,3,5는 AES-128,192,256에 대한 Grover 공격 비용에 의해 결정되며 (총 게이트 수 x 깊이)로 계산된다.

	[3]	[5]
Level 1(AES-128)	2^{170}	2^{157}
Level 3(AES-192)	2^{233}	2^{221}
Level 5(AES-256)	2^{298}	2^{285}

연구 동향

● ASCON-128

- Oh et al. 은 치환 계층에서 사용되는 64개의 S-box를 320(5x64)개의 보조 큐비트 할당을 통해 병렬로 구현
- 역연산을 수행하여 320개의 보조 큐비트를 매 라운드마다 재사용
- 선형계층에서는 naïve한 구현 출력 값을 저장할 큐비트들을 할당하여 병렬로 구현

● Sparkle SCHWAEMM

- Yang et al.은 순열 과정 중 Alzette 단계에서 CDKM 덧셈기를 사용하여 한개의 보조 큐비트만을 사용
- 4개의 Alzette 함수를 병렬로 구현
- 함수 내부의 사용되는 덧셈기를 병렬로 구현

● Grain-128AEAD

- Anand et al.은 3비트 및 4비트에 대한 토폴리 게이트를 구현하기 위해 compute-copy-uncompute 방법을 사용
- 각각 2개,3개의 보조 큐비트를 사용하여 결과값을 복사함으로써 구현.
- 초기화 단계와 키 스트림 생성 단계를 동시에 구현함으로써 최적화

● NIST 경량암호 공모 최종후보 회로 구현을 기반으로 추정한 Grover 양자 공격 비용

Cipher	Total gates	Total depth	Cost	Qubits
ASCON-128	$1.180 \cdot 2^{83}$	$1.574 \cdot 2^{73}$	$1.856 \cdot 2^{156}$	20064
Sparkle-SCHWAEMM	$1.732 \cdot 2^{83}$	$1.431 \cdot 2^{80}$	$1.239 \cdot 2^{164}$	613
Grain-128AEAD	$1.724 \cdot 2^{82}$	$1.820 \cdot 2^{80}$	$1.569 \cdot 2^{163}$	532

결론

- 암호 공격 비용이 NIST에서 제시하는 비용보다 높을 경우 → 해당 암호는 양자 컴퓨터 공격으로부터 안전
- NIST에서 제시하는 비용보다 현저히 낮을 경우 → 양자 공격으로부터 보안성 붕괴
- 본 논문에서는 NIST 경량암호 표준화 공모전에 선정된 암호 중 ASCON, Sparkle, Grain-128AEAD에 대한 양자 회로 구현 동향에 대해 살펴보고 공격 비용을 비교함.
- ASCON, Sparkle, Grain-128AEAD에 대한 공격 비용은 2^{157}이상이거나 그와 비슷함 → 보안 레벨 1을 달성