국산경량암호 양자 회로 구현 동향

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

요 약

● 양자 컴퓨터의 발전으로 Shor알고리즘의 공개키 암호 공격이 다항시간 내에 가능함이 밝혀지면서 NIST에서는 양자 내성 암호 공모전을 진행하였다. 또한 Grover 알고리즘으로 대칭키 암호 공격의 복잡도가 제곱근으로 감소될 수 있으며 이에 따라 대칭키 암호 역시 안전하다고 보기 어렵다. 그리하여, 안전한 양자 후 보안 시스템 구축을 위해 NIST는 양자 후 보안 강도를 추정하며 이에 맞춰 양자 암호 분석 연구가 활발 하게 수행되고 있다. 이에 본 논문에서는 국산 경량 암호에 대한 양자 회로 구현 동향을 살펴보고 NIST 보안 강도와 비교하여 평가한다.

관련연구

● NIST 양자 후 보안 레벨

NIST는 AES에 대한 양자 공격 복잡성을 기반으로 사후 양자 보안 기준을 수립하였다.[3,5].

Level 1,3,5 는 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

● CHAM

[7]에서는 라운드 키 생성에 사용되는 보조 큐비트를 줄이기 위해 키 스케줄에 두 가지 선형 레이어 최적화 기법을 적용

PLU 기법 - CNOT 게이트와 Swap 게이트만을 사용

FSE 기법 - CNOT게이트와 swap 연산은 논리적 swap을 사용

● LEA

[8] 에서는 큐비트 수 절약을 위해 라운드 키를 하나씩 업데이트하여 라운드 함수에 사용하는 on-the-fly 방식을 활용. 또한 키 스케줄에서 사용되는 연산들을 병렬로 처리함으로써 depth 측면에서 최적화

● HIGHT

[8]에서는 키 스케줄과 라운드 함수에서 최적화를 진행. 라운드 키(RK) 생성 시 초기 σ_0을 총 4개(σ_0~ σ_3) 할당하여 4개의 라운드 키를 병렬적으로 생성하여 라운드 함수에서 병렬 덧셈을 통해 depth를 최적화

● 국산 경량암호 회로 구현을 기반으로 추정한 Grover 양자 공격 비용

Cipher	Qubits	Total gates	Total depth	Cost
CHAM	409	2^{81}	2^{81}	2^{157}
HIGHT	457	2^{82}	2^{75}	2^{158}
LEA	389	2^{82}	2^{77}	2^{159}

결론

● 본 논문에서는 국산 경량암호들에 대한 양자 회로 구현 연구에 대해 살펴보고 그에 따른 Grover 양자 공격 비용 및 양자 후 보안 강도를 평가함

● 국산 경량 암호인 CHAM, HIGHT, LEA 모두 NIST가 정의한 양자 후 보안 레벨 1을 달성한 것을 확인함

● 미리 보안 강도를 평가하는 것은 향후 양자 컴퓨터가 실용화되기 전에 보안 시스템을 구축하는데 도움이 될 것으로 판단됨.