SPECK128/128 에서 SPECK128/256 으로의 안전한 마이그레이션을 위한 동형 트랜사이퍼링

이재연, 김영식*

대구경북과학기술원

{ljy8733, ysk}@dgist.ac.kr

Homomorphic Transciphering for Secure Migration from SPECK128/128 to SPECK128/256

Jaeyeon Lee, Young-Sik Kim*
DGIST

요 약

본 논문은 기존 SPECK128/128 암호문을 평문 노출 없이 SPECK128/256 암호문으로 변환하는 CKKS 기반 동형 트랜사이퍼링 프레임워크를 제안한다. 이 프레임워크는 양자 컴퓨터 환경에서 대칭키 보안 강도가 감소하는 문제에 대응하여 동형 암호를 활용한 안전한 키 전환 방법을 제시하며, V2X 환경에서 대량의 암호화된 차량 데이터를 보호하면서 키를 업그레이드하는 데 활용될 수 있다. 제안 방식은 (1) SPECK 의 64 비트 데이터를 CKKS 암호문에 비트 단위로 매핑하는 기법, (2) 회로 기반 모듈러 덧셈 구현, (3) 저차 노이즈 감쇄 다항식을 결합하여 구성된다. 실험 결과, SPECK128/128 에서 SPECK128/256 으로의 변환이 6.5s amortized 시간 내에 완료되었다.

Ⅰ. 서 론

V2X 통신은 자율주행 및 지능형 교통 시스템의 핵심 기술로서, 차량 간 및 차량-인프라 간 통신을 포함한다. V2X 환경에서는 실시간 데이터 교환과 함께 강력한 보안이 요구되며, 리소스 제약으로 인해 경량 블록 암호가 널리 사용된다. SPECK 은 NSA 에서 개발한 ARX(Addition, Rotation, XOR) 기반 경량 블록 암호로, 소프트웨어 환경에서 우수한 성능을 보인다[1].

그러나 양자 컴퓨터의 Grover 알고리즘은 대칭키 암호의 보안 강도를 절반으로 감소시킨다[2]. 이에 따라 SPECK128/128 은 양자 환경에서 64 비트 수준의 보안성만 제공하게 되므로, SPECK128/256 으로의 전환이 필요하다.

키 전환을 위한 기존 방식에는 두 가지가 있다. 첫째, SPECK128/128 을 복호화한 후 SPECK128/256 으로 재암호화하는 방식은 변환 과정에서 평문이 노출되는 보안 취약점을 지닌다. 둘째, SPECK128/128 을 SPECK128/256 으로 추가 암호화하는 방식은 키 관리 복잡성을 증가시키고 공격 위험을 높인다.

트랜사이퍼링은 동형 암호화된 상태에서 동형복호화 후 재암호화를 수행하는 기술로서, 평문 노출 없이 안전한 변환을 가능하게 한다[3]. 본 논문은 CKKS 를 사용해 SPECK128/128 에서 SPECK128/256 으로의 트랜사이퍼링 프레임워크를 제안한다.

Ⅱ. 배경 지식

2.1 SPECK 블록 암호

SPECK128 은 128 비트 블록과 각 128/192/256 비트 키를 지원하는 경량 블록 암호이다. 128 비트 블록은 두 개의 64 배트 워드 (x, y) 로 구성되며, 각 암호와 라운드는 다음과 같이 수행된다.

$$x \leftarrow \left((x \gg 8) \boxplus y\right) \oplus k, y \leftarrow (y \ll 3) \oplus x$$

$\oplus$ 는 비트 XOR, $\boxplus$ 는 모듈러 덧셈, >>와 <<는 각각 오른쪽/왼쪽 순환 이동, k 는 라운드 키를 나타낸다.

SPECK128/128, 128/192, 128/256 은 32, 33, 34 라운드를 수행한다.

2.2 CKKS 동형암호

CKKS 는 근사 연산을 지원하는 동형 암호 스킴으로, SIMD 구조를 통해 다수의 데이터를 병렬 처리할 수 있다. 덧셈, 곱셈, 회전의 제한된 연산을 지원한다[4].

Ⅲ. 제안 방식

3.1 트랜사이퍼링 프레임워크

클라이언트는 SPECK128/128 암호문과 CKKS 로 암호화된 마스터 키, 그리고 필요한 CKKS 키를 서버에 전송한다. 서버는 주어진 SPECK128/128 암호문을 CKKS 공개키로 암호화한 후, (1) CKKS 스킴 하에서 SPECK128/128 복호화를 수행하여 암호화된 평문을 얻고, (2) SPECK128/256 암호화를 수행하여 목표 암호문을 생성한다. 클라이언트는 결과 암호문을 CKKS 비밀키로 복호화하여 SPECK128/256 암호문을 얻는다. 이 과정에서 데이터는 항상 암호화된 상태로 유지된다.

3.2 비트 패킹

SPECK 의 64 비트 워드를 CKKS 슬롯에 비트 단위로 인코딩한다. N개의 슬롯에서 gap = $N/64$로 설정하여, 비트 i는 슬롯 $i \times gap$에 매핑된다. 이를 통해 하나의 암호문에서 gap개의 64 비트 워드를 병렬 처리한다.

3.3 ARX 연산

XOR 은 $x + y - 2xy$로 depth 1 로 평가되며, 회전은 CKKS 슬롯 회전으로 구현된다. 64 비트 모듈러 덧셈/뺄셈은 Kogge-Stone 가산기로 구현하여 로그 깊이의 캐리 전파를 달성한다. 또한 CKKS 근사 연산으로 인한 오차를 방지하기 위해 $f(x) = 3x^2 - 2x^3$ 노이즈 감쇄 함수를 적용한다.

Ⅳ. 실험 결과

실험은 AMD Ryzen Threadripper Pro CPU 에서 DesiloFHE 를 사용하여 32 스레드 병렬 모드로 수행하였다. CKKS 파라미터는 2^{15} 슬롯을 지원한다. Amortized 시간은 SIMD 병렬 처리되는 블록 수(512)로 총 시간을 나눈 값이다.

[표 1] SPECK 트랜사이퍼링 성능

Workload	Round (s)	Total(s)	Notes
SPECK128/128 Encrypt	0.099	3.17	32 Rounds
SPECK128/128 Decrypt	0.084	2.70	32 Rounds
SPECK128/256 Encrypt	0.112	3.80	34 Rounds
SPECK128/256 Decrypt	0.094	3.21	34 Rounds
Transcipher	-	**6.50**	**66 Rounds**

[표 1]은 트랜사이퍼링의 전체 성능을 보여준다. SPECK128/128 에서 SPECK128/256 으로의 변환은 6.5amortized 시간에 수행되었으며, 복호 시 실제 값과 동일함을 확인할 수 있었다. 이는 동형 암호를 이용해 평문 노출 없이 안전하게 256 비트 비밀키로 마이그레이션이 가능함을 보여준다.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. RS-2024- 00442085, 자율주행 차량 서비스 보호를 위한 V2X 무선통신 인프라 보안 핵심기술 개발).

참 고 문 헌

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers," Cryptology ePrint Archive, Report 2013/404, 2013.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proc. the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 212-219, 1996.

[3] I. Thakur, A. Karmakar, C. Li, and B. Preneel, "A survey on transciphering and symmetric ciphers for homomorphic encryption," Cryptology ePrint Archive, Report 2025/093, 2025.

[4] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," *Advances in Cryptology - ASIACRYPT 2017*, pp. 409-437, 2017.