전자서명을 활용한 동형암호 무결성 검증 프레임워크

이희수, 이용우
인하대학교
fromhslee@inha.edu, yongwoo@inha.ac.kr

A Signature-Embedded Transmission Framework for Homomorphic Encryption

Heesoo Lee, Yongwoo Lee
Inha Univ.

요 약

본 논문은 RLWE 기반 동형암호문에 격자 기반 전자서명 FALCON을 결합해, 키 교환 없이 공개 무결성 검증이 가능한 방식을 제안한다. 암호문을 입력으로 간주하여 생성한 서명을 함께 전송함으로써, 수신자는 암호문이 변조되지 않았음을 독립적으로 확인할 수 있다. 제안 방식은 공개된 환경에서도 동형암호문의 무결성을 검증할 수 있으며, 서명 크기가 작고 계산 효율이 높아 실용적인 통신량을 유지한다.

Ⅰ. 서 론

동형암호(Homomorphic Encryption)는 암호화된 상태에서도 덧셈, 곱셈과 같은 수학적 연산을 수행할 수 있는 암호 기법이다[1]. 이러한 특징은 사용자의 데이터가 외부에 노출되는 위험을 원천적으로 차단할 수 있으며, 이는 개인 정보가 중요한 환경에서 유용하게 활용된다.

동형암호 기술 중에서도 Ring Learning With Errors(RLWE) 문제를 기반으로 한 스킴은 양자 컴퓨터에 대해 안전성을 제공함으로써, 차세대 통신 보안 기술로 평가받고 있다[2]. RLWE 기반 동형암호는 민감한 데이터를 외부 서버로 전송하여 처리하는 구조에서도, 데이터의 기밀성을 유지할 채 계산이 가능하다는 장점을 갖는다.

그러나 암호화된 데이터가 외부에서 처리되는 구조는 기존 암호 시스템에서 고려되지 않았던 새로운 보안 문제를 야기할 수 있다. 예를 들어, 암호문이 전송 중 변조되거나 훼손되었을 경우, 수신자는 이를 인지하지 못한 채 잘못된 연산 결과를 신뢰할 가능성이 존재한다. 이는 전송 계층 보안 프로토콜인 Transport Layer Security(TLS)를 사용할 경우에도 완전히 해결되지 않는다. TLS는 세션 기반 암호화를 통해 전송 중의 무결성은 보장하지만, 암호문 자체에 대한 공개적이고 독립적인 무결성 검증은 지원하지 않기 때문이다.

본 논문에서는 이러한 문제를 해결하기 위해, 암호문 자체를 서명의 대상으로 간주하고 격자 기반 전자서명 스킴인 FALCON [3]을 적용하는 방식을 제안한다. 암호문 전송 시 서명을 함께 전송함으로써, 수신자는 암호문이 전송 중에 변조되지 않았음을 공개적으로 검증할 수 있으며, 이는 동형 연산의 안전성과 신뢰성을 향상시키는 데 기여한다.

Ⅱ. RLWE-based Homomorphic Encryption

동형암호(Homomorphic Encryption)는 암호문 위에서 직접 연산을 수행할 수 있도록 설계된 암호 방식이다. 그 중에서도 RLWE 기반 스킴은 암호화 과정에서 작은 잡음(noise)을 추가하여 암호학적 어려움을 제시함으로써 수학적으로 강력한 보안성을 제공한다. 이는 암호문을 더욱 안전하게 만드는 요소로 작용한다.

동형암호 시스템에서 사용되는 다항식 링은 $R_q = \mathbb{Z}_q[X]/(X^N+1)$로 정의된다. 여기서 q는 계수 모듈러이고 N은 링의 차수로, 일반적으로 2의 거듭제곱인 수로 설정된다.

동형암호에서 암호문은 보통 두 개의 다항식 $c=(c_0,c_1)\in R_q^2$로 구성되며, 암호화 과정은 다음과 같은 수식을 따른다:

$$c_0 = a\cdot r + e_1 + \Delta\cdot m,\ c_1 = b\cdot r + e_2$$

여기서 $a,b\in R_q$는 공개키, r,e_1,e_2는 잡음 다항식, m은 암호화할 메시지 다항식, Δ는 스케일링 계수이다.

Ⅲ. FALCON

Fast Fourier Lattice-based Compact Signature over NTRU(FALCON)은 Gentry-Peikert-Vaikuntanathan(GPV) 프레임워크 [4]를 기반으로 NTRU 격자 구조 위에 구현된 전자서명 스킴이다. 이 스킴은 수학적으로 짧은 서명 벡터 생성을 위해 Fast Fourier Sampling 기법을 채택하고, 서명의 압축성과 계산 효율성을 동시에 고려하여 설계되었다.

GPV 프레임워크는 공개키를 통해 정의되는 격자 Λ와, 이에 직교하는 $\Lambda_q^{\perp}$의 trapdoor를 비밀키로 활용하여, 해시 값 $H(m)$에 대응하는 짧은 벡터를 샘플링하는 방식으로 서명을 생성한다.

공개키는 $h = g\cdot f^{-1} \bmod q$로 표현되는 다항식이며, 비밀키는 NTRU 방정식 $fG-gF=q \mod (X^N+1)$을 만족하는 $f,g,F,G\in R_q$의 네 개의 다항식으로 구성된다. 메시지 m에 대한 서명은 난수 r과 함께 $H(r\|m)$으로부터 유도된 벡터에 의해, trapdoor를 이용한 샘플링 절차를 통해 계산된다.

Ⅳ. 제안 방식: FALCON 기반 RLWE 암호문 서명 기법

본 논문은 RLWE 기반 동형암호문의 무결성을 보장하기 위해, 암호문 자체를 서명의 대상으로 간주하고 격자 기반 전자 서명 스킴인 FALCON을 적용하는 방식을 제안한다. 제안 방식에서는 암호문에 대한 서명을 생성하고, 수신자는 이를 이용해 암호문이 변조되지 않았음을 검증할 수 있다.

구체적으로, RLWE 기반 동형암호 스킴에 따라 생성된 암호문 $c=(c_0,c_1)\in R_q^2$을 FALCON 서명의 입력으로 활용하기 위해, 암호문 c의 계수들을 이진 인코딩하여 $M\in\{0,1\}^*$으로 변환한 후, 난수 salt $r\in\{0,1\}^k$를 앞에 붙여 해시 함수 H에 적용하여 다음과 같이 해시값 d를 계산한다:

$$d=H(r\|M)$$

이어서 비밀키에 해당하는 NTRU trapdoor $B=\begin{bmatrix} g & -f \\ G & -F \end{bmatrix}$를 이용하여, 위 해시값 $d\in R_q$에 대응하는 짧은 벡터 $s=(s_1,s_2)\in R_q^2$를 샘플링한다. 이 벡터는 다음 조건을 만족해야 한다:

$$s_1+s_2\cdot h=d \mod q$$

샘플링된 벡터의 유클리드 노름 $\|s\|$는 사전 정의된 임계값 β를 초과하지 않아야 하며, 송신자는 암호문 c, salt r, 서명 벡터의 일부인 s_2를 함께 전송한다.

수신자는 수신한 암호문으로부터 송신 측과 동일한 방식으로 M을 복원하고, 이를 r과 함께 해시 함수에 적용하여 해시값 d를 계산한다. 이후 s_2와 공개키 h를 이용하여 s_1을 다음과 같이 복원한다:

$$s_1=d-s_2\cdot h \mod q$$

이때 복원된 벡터 (s_1,s_2)가 사전에 정의된 범위 $\|(s_1,s_2)\|^2\le\beta^2$를 만족하는지를 확인함으로써, 암호문이 변조되지 않았음을 검증한다. 검증에 실패한 경우 해당 암호문은 변조된 것으로 간주된다.

이와 같이 암호문 자체에 서명을 결합하는 방식은, 암호문을 단일 수신자에게만 일회성으로 전달하는 것을 넘어, 다자간 공유나 공개 검증이 요구되는 다양한 상황에서의 활용을 가능하게 한다. 예를 들어 암호문을 블록체인에 저장하거나 다수에게 브로드캐스트하는 경우에도 별도의 키 교환 없이 무결성 검증이 가능하다는 점에서 강점을 갖는다.

Ⅴ. 결론

본 논문에서는 RLWE 기반 동형암호문에 무결성을 부여하기 위한 방법으로, 암호문 자체를 서명의 대상으로 간주하고 격자 기반 전자서명 스킴인 FALCON을 적용하는 방식을 제안하였다. 암호문을 해시한 뒤, trapdoor 샘플링을 통해 짧은 서명을 생성함으로써, 수신자는 별도의 키 교환 없이도 암호문이 변조되지 않았음을 독립적으로 검증할 수 있다. 이는 암호문 연산의 신뢰성을 보장할 수 있으며, TLS 기반 보호 방식이 가지는 구조적 한계를 보완할 수 있다.

TLS는 세션 기반 암호화 방식으로 빠른 속도와 세션 단위의 기밀성 보장이라는 장점을 제공하지만, 암호문을 블록체인에 저장하거나 다수의 수신자에게 전송하는 환경에서는 별도의 키 교환 없이는 무결성 검증이 불가능하다는 제약이 있다. 특히 브로드캐스트 환경에서는 수신자마다 키를 개별적으로 교환해야 하므로, 오히려 통신량이 증가하고 적용이 어렵다. 이에 비해, 본 논문에서 제안한 방식은 암호문 자체에 전자서명을 결합함으로써, 제3자도 공개키만으로 무결성을 검증할 수 있다. 이러한 구조는 블록체인, 브로드캐스트, 스마트 컨트랙트 등 키 공유가 제한된 환경에서도 실용성을 높인다.

물론 서명 정보를 함께 전송해야 하므로 통신량이 증가한다는 단점이 존재한다. 그러나 본 논문에서 적용한 FALCON 스킴은 서명 크기가 약 656바이트로 매우 작고 연산 속도도 빠르기 때문에, 이러한 부담을 실질적으로 최소화할 수 있다. 예를 들어, 암호문 자체의 크기가 약 770KB인 경우, FALCON 서명을 결합하더라도 전체 전송량은 약 771KB에 불과하다. 이는 전체 데이터 크기 대비 약 0.08% 수준의 증가이다. 이러한 실험은 AMD Ryzen Threadripper PRO 3975WX CPU, 251GB RAM, Linux 6.8.0 기반 OS 환경에서 수행되었다. 실험에 사용된 암호문은 OpenFHE 라이브러리를 통해 생성하였으며, 이때 링 차수는 2^{14}, 암호문의 모듈러스는 약 2^{120} 수준으로 설정하였다.

	TLS	제안 방법
암호화 시간	약 0.16ms	약 10ms
데이터 전송량	770KB	771KB
키 교환	필요함	필요 없음

[표1] 실험 결과

암호문 전체를 서명의 입력으로 사용할 경우, 서버는 동형 연산 수행 전에 무결성 검증을 선행할 수 있으며, 변조된 암호문으로 인한 자원 낭비를 방지할 수 있다. 이와 동시에 동형암호문 자체가 데이터의 기밀성을 보장하므로, 복호화 없이도 무결성을 검증할 수 있다는 점에서 실용성과 보안성을 모두 만족시키는 구조를 제공한다. 이러한 특성은 동형암호의 활용 범위를 넓히고, 다양한 응용 환경에서 보다 안전하고 유연한 암호문 전달을 가능하게 한다.

ACKNOWLEDGMENT

이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.RS-2022-00155915, 인공지능융합혁신인재양성(인하대학교))

참 고 문 헌

[1] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009.

[2] Lyubashevsky, Vadim, Chris Peikert, and Oded Regev. "On ideal lattices and learning with errors over rings." Journal of the ACM (JACM) 60.6 (2013): 1-35.

[3] National Institute of Standards and Technology. "Module-Lattice-Based Digital Signature Standard." Federal Information Processing Standards Publication 204. August 13, 2024.

[4] Gentry, Craig, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions." Proceedings of the fortieth annual ACM symposium on Theory of computing. 2008.