래티스 기반 준동형 서명 기법의 비교[1)]

최락용* 김광조*

*카이스트 전산학부

Comparison of Homomorphic Signature Schemes over Lattices

Rakyong Choi* Kwangjo Kim*

*School of Computing, KAIST

요 약

서명에서의 준동형 성질이란 다수의 서명자 S_i가 각각의 데이터 m_i에 대해서 서명 σ_i를 하고 서버에 저장한다고 가정할 때, 어떤 데이터 수집가가 평균, 표준편차 등의 데이터의 함수 f를 요구할 경우 서버가 각 데이터에 대한 정보 공개 없이 서버 상에서 함수 값 $f(m_1, m_2, ..., m_n)$에 대한 올바른 서명 σ_f를 계산할 수 있게 되는 성질로 만족하는 함수의 성질에 따라 선형 준동형 성질 혹은 완전 준동형 성질을 만족한다고 한다. 본 논문은 이러한 준동형 성질을 가진 준동형 서명 기법 중 래티스 문제의 어려움에 의해 증명 가능하도록 설계된 최신 논문에 대해서 조사하고 앞으로의 발전 방향에 대해서 논의하고자 한다.

I. 서론

최근 정보통신 기술의 발달로 인해 클라우드, 빅데이터 등에서 프라이버시 보호는 점점 더 큰 문제가 될 것이라 염려되고 있다. 이를 해결하기 위해 기존 데이터에 대한 권한을 가지지 않은 서버가 준동형 암호(Homomorphic Encryption)를 이용하여 암호화된 데이터에 대한 계산을 해결하는 방법이 2009년 Gentry에 의해 제안된 이후[1], 2011년 MIT가 지정한 세계 10대 혁신 과제 중 하나로 클라우드 및 빅데이터 보안에 적합한 획기적인 연구 성과로 주목을 받고 있다.[2] 한편, 계산된 데이터의 서명 또한 기존의 서명을 이용하여 계산할 수 있는 준동형 서명의 필요성이 대두되었으며 최근 들어 Gorbunov, Vaikuntanathan, Wichs 등이 래티스 기반 수학적 난제에 기반한 최초의 완전 준동형 서명이 발표하였다.[3]

하지만 이렇게 준동형 성질을 이용한 준동형 암호와 준동형 서명에 대한 연구로 빠르게 발전해나가는 해외기술에 비해 클라우드, 빅데이터 상에서의 프라이버시 보호를 위한 국내 관련 연구는 아직 초보 단계에 불과하며, 선진국과의 격차를 최단시간에 줄여나가야 한다.

1.1 논문의 구성

본 논문의 구성은 다음과 같다. 우선 II장에서는 래티스와 준동형 성질의 정의와 앞으로 쓸 기호의 표기법에 대해서 정의한다. 이후 III장에서 기존의 준동형 서명들의 주요특성과 서명 기법의 안전성 검증 방법, 그리고 이 중 위조불가능성 증명의 기반이 되는 수학적 난제가 어떤 것인지에 대해 논의한다. 마지막으로 IV장에서는 기존 III장에서 다룬 기존의 준동형 서명을 표로 요약 및 비교하고 아직 해결되지 않은 문제들에는 어떤 것들이 있는지 논의한다.

1) 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [1391104001, 생체모방 알고리즘(Bio-inspired Algorithm)을 활용한 통신기술 연구]

II. 배경지식

최근 약 15년 간 미국, 유럽, 일본 등 선진국에서는 양자컴퓨터 출현에 대비하여 양자 암호에 대한 활발한 연구가 진행되고 있으며 그 중 RSA(Rivest, Shamir, Adleman) 공개키 암호, ElGamal 공개키 암호, Diffie-Hellman 키 교환 알고리즘 등 기존의 정수론 기반 어려움이 아닌 다른 수학적 어려운 문제에 근간을 둔 포스트 양자 암호(Post Quantum Cryptography, PQC)에 대한 연구가 이루어지고 있다.

래티스 기반 암호는 이러한 포스트 양자 암호의 한 가지로 주목받고 있으며 래티스와 래티스 기반 난제는 다음과 같다.

2.1 래티스 및 래티스 기반 난제

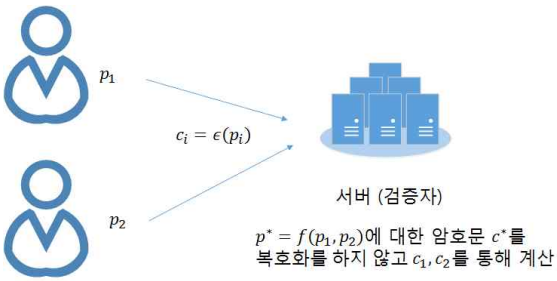
일반적으로 래티스란 어떤 실수 공간 $\mathbb{R}^m$ 상에 있는 기저(basis)를 통해 나오는 이산 부분군(discrete subgroup)을 칭하며, 만약 실수 공간이 아닌 정수 공간 $\mathbb{Z}^m$ 상에서는 정수 래티스(integer lattice)라고 명한다. 또한, 아이디얼 래티스(ideal lattice)는 이러한 래티스 중 아이디얼 성질을 만족하는 래티스를 지칭한다.

암호에서 많이 이용되는 대표적인 래티스 기반 어려운 문제로는 Learning With Errors(LWE) 문제와 Small Integer Solution(SIS) 문제가 있다. LWE 문제란 주어진 벡터 $a_1, a_2, \ldots, a_m$에서 임의의 작은 에러값 $e_1, e_2, \ldots, e_m$을 추출하여 벡터 $b_i = \langle s, a_i \rangle + e_i$를 각 $i = 1, 2, \ldots, m$에서 계산한 뒤, $\{\langle a_i, b_i \rangle\}_{i=1}^{m}$에서 비밀키 s를 찾아내는 문제로 작은 에러와 함께 유일한 해답 s가 나온다는 점에서 주로 공개키 암호, 완전 준동형 암호 등을 설계하는 기반이 된다.

SIS 문제란 주어진 벡터 $a_1, a_2, \ldots, a_m \in \mathbb{Z}^m$에 대해 $\sum_{i=1}^{m} z_i a_i = 0$을 만족하는 0이 아닌 $z_1, z_2, \ldots, z_m \in \{-1, 0, 1\}$를 찾는 문제로 유일해를 가지는 LWE 문제와 달리 많은 답이 나올 수 있어 개인 식별 및 디지털 서명의 위조불가능성을 증명하는데 주로 이용된다.

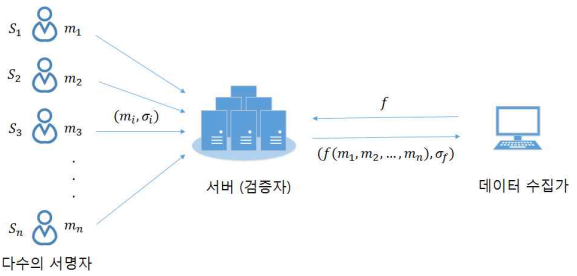
2.2 준동형 성질 및 준동형 서명

일반적으로 암호에서 말하는 준동형 성질(homomorphic property)이란 [그림 1]과 같이 두 평문 p_1, p_2와 이에 따른 암호문 c_1, c_2에 대해 어떤 함수 f가 있어 $p^* = f(p_1, p_2)$에 대한 암호문 c^*를 c_1, c_2의 복호화 과정 없이 계산할 수 있다는 것으로, 대표적으로 가장 널리 쓰이고 있는 RSA 암호시스템의 경우 곱셈에서의 준동형 성질을 가지며 ElGamal 암호시스템의 경우는 덧셈에서의 준동형 성질을 가진다.



[그림 1] 준동형 성질을 만족하는 암호

한편 서명 기법에서의 준동형 성질은 [그림 2]에서와 같이 어떤 서명 기법에 대해 다수의 서명자 S_i가 각각의 데이터 m_i에 대해서 서명 σ_i를 하고 서버에 저장한다고 가정한다.



[그림 2] 준동형 서명 기법

이 때, 어떤 데이터 수집가가 평균, 표준편차 등의 데이터의 함수식 f를 요구할 경우 서버가 각 데이터에 대한 정보 공개 없이 서버 상에서 데이터의 기존 서명을 이용하여 각 데이터의 함수 값 $f(m_1, m_2, \ldots, m_n)$에 대한 올바른 서명

σ_f를 계산할 수 있다면 이 서명 기법에 대해 준동형 성질을 만족한다고 하고 이러한 성질을 만족하는 서명 기법을 함수 f의 성질에 따라 선형 준동형 서명(linearly homomorphic signature) 혹은 완전 준동형 서명(fully homomorphic signature)이라고 칭한다.

III. 준동형 서명 기법

이번 장에서는 2011년 발표된 Boneh와 Freeman의 두 논문들(이하 BF11a, BF11b)과 최근 발표된 Gorbunov, Vaikuntanathan, Wichs의 논문(이하 GVW15)에 대한 주요특성을 확인하고 안전성 검증 방법에 대해서 간략하게 알아본다.

3.1 BF11a 논문[4]

이 논문은 Gentry, Peikert, Vaikuntanathan이 쓴 서명 기법 논문(이하 GPV08)[5]을 토대로 한 논문으로 태그 id, 메시지 m에 대한 서명 σ를 modulus q에서 정의된 래티스가 아닌 modulus $2q$에서 정의된 래티스에서 추출하면서 $\sigma = m \bmod 2$로 벡터의 정보를 얻음과 동시에 $\sigma \bmod q$를 통해 서명의 위조불가능성도 보일 수 있다는 장점이 있다. 본 기법의 안전성 검증을 위해서는 서명문의 정확성을 확인한 뒤 위조불가능성(unforgeability)과 weakly context hiding 성질을 만족해야 한다.

여기서 본 서명은 가우시안 분포의 샘플 크기를 제한하고 중국인의 나머지 정리를 이용하여 상수 횟수 덧셈 연산에 대해 선형 준동형 성질을 가지며 위조불가능성은 공격자가 서명을 하는 데이터 $v_{i1}, v_{i2}, ..., v_{ik} \in V$을 직접 정할 수 있는 상황에서 서명에 쓰이는 태그 id_i만 서명자가 결정하여 서명 σ_{ij}를 $j = 1, 2, ..., k$에 대해 얻을 수 있다고 할 때, 임의의 식별자 id^*에 대해 0이 아닌 벡터 y^*에 대한 올바른 서명 σ^*를 하는 게임을 가정한다. 단, 이 때 모든 i에 대해 식별자 $id^* \neq id_i$이거나 어떤 i에 대해 $id^* = id_i$인 경우에는 $y^* \notin V$를 만족해야 한다. 만약 이러한 게임에서 공격자 A가 승리할 확률이 보안 매개변수 n에 대해 무시 가능한 수준이면 선형 준동형 암호에 대해 위조불가능성을 가진다고 말하며 본 논문의 위조불가능성은 SIS 문제의 어려움으로부터 증명 가능하다.

또한 이 논문에서는 기존 데이터의 프라이버시 보호를 위해서 서로 다른 두 벡터 공간 V_1, V_2에서 함수 f_j에 대해 어떤 데이터 $(v_{i1})_{i=1}^k$, $(v_{i2})_{i=1}^k$가 $f_j\{(v_{i1})_{i=1}^k\} = f_j\{(v_{i2})_{i=1}^k\}$를 만족한다고 할 때, $f_j\{(v_{i1})_{i=1}^k\}$의 서명 σ_{j1}과 $f_j\{(v_{i2})_{i=1}^k\}$의 서명 σ_{j2}를 구분할 수 없다는 weakly context hiding 성질을 증명하였다.

3.2 BF11b 논문[6]

이 논문은 앞선 BF11a 논문과 마찬가지로 GPV08 논문을 토대로 하였으며 안전성 검증을 위해서도 비슷하게 위조불가능성과 weakly context hiding 성질을 증명하여야 한다. 하지만 BF11a 논문과 달리 숫자가 아닌 래티스 그 자체를 modulus 연산의 도구로 이용하였으며 그로 인해 상수 횟수가 아닌 다항식 횟수의 연산에 대해서도 선형 준동형 성질을 만족하며 일반적인 래티스를 아이디얼 래티스로 바꿀 경우에는 제한된 다항식 함수에 대해서도 준동형 성질을 만족하는 서명 기법을 설계할 수 있다.

안전성 증명은 두 래티스 Λ_1, Λ_2에 대하여 태그 τ, 메시지 m, 함수 f에 대한 서명 σ를 만들 때, 태그 τ에 대한 해시 함수 ω_τ가 있어 $\sigma = m \bmod \Lambda_1$, $\sigma = \omega_\tau(f) \bmod \Lambda_2$를 만족한다고 한다. 그러면 이 때, 적당한 해시 함수 ω_τ가 주어지면 준동형 성질을 증명할 수 있으며 SIS 문제의 어려움 등으로 위조불가능성과 weakly context hiding 성질 또한 증명 가능하다.

3.3 GVW15 논문[3]

이 논문은 Boneh 등이 작성한 2014년

EUROCRYPT 2014 논문(이하 BGG14)[7]에서 쓴 기술을 이용하여 준동형 트랩도어 함수(homomorphic trapdoor function)를 새롭게 정의하여 준동형 암호와 준동형 서명의 개념을 하나로 통합하였으며 SIS 문제의 어려움으로부터 얻은 준동형 트랩도어 함수를 이용하여 래티스 기반 완전 준동형 서명을 설계하였다.

이 논문에서의 완전 준동형 서명 기법의 안전성 검증은 서명의 정확성과 함께 공개 파라미터를 보지 않고 데이터를 선택하는 공격자를 가지는 모델에서의 선택적 안전성(selective security) 또는 공개 파라미터를 안 상태에서 데이터를 선택하는 공격자를 가지는 모델에서의 완전 안전성(full security)을 증명한다. 그리고 BF11a, BF11b 논문에서의 weakly context hiding과 비슷한 정의를 가지는 context hiding 성질의 검증을 통해 안전성 검증을 마무리한다.

IV. 결론

본 논문에서는 래티스와 준동형 성질의 기본 정의에 대해서 알아본 뒤 기존에 알려진 래티스 기반 준동형 서명 기법에 대한 주요특성과 안전성 검증 방법에 대해서 알아보았다. [표 1]은 각 논문의 준동형 서명 기법을 비교한 것으로 똑같은 수학적 난제인 SIS 문제에 이용하여 서명의 안전성을 증명하였으며 각자 다른 주요 특성을 가지고 선형 혹은 완전 준동형 성질을 증명하였다.

표 1. 래티스 기반 준동형 서명 방식의 비교

	BF11a	BF11b	GVW15
기반하는 서명 기법	GPV08	GPV08	BGG14
기반 문제	SIS	SIS	SIS
준동형 성질	선형	선형 (아이디얼 래티스는 완전)	완전
주요특성	modulus $2q$에서의 래티스	두 개의 서로 다른 래티스 사용	준동형 트랩도어 함수

추후 과제로는 우선 각 서명의 서명자가 단수가 아닌 그룹에 의한 서명인 경우에 대한 선형 혹은 완전 준동형 서명 설계를 생각할 수 있다. 또한 아이디얼 래티스 상에서의 어려운 래티스 문제에 기반한 완전 준동형 서명을 만드는 것도 하나의 도전적인 주제가 될 것이다.

[참고문헌]

[1] Craig Gentry, “A Fully Homomorphic Encryption Scheme,” Doctoral dissertation, Stanford University, 2009.

[2] “10 Breakthrough Technologies: Homomorphic Encryption,” MIT Technology Review, 2011. (http://www2.technologyreview.com/article/423683/homomorphic-encryption/)

[3] Sergey Gorbunov, Vinod Vaikuntanathan and Daniel Wichs, “Leveled Fully Homomorphic Signatures from Standard Lattices,” Proceedings of the 47th Annual ACM Symposium on Theory of Computing (STOC 2015), ACM, 2015.

[4] Dan Boneh and David Mandell Freeman, “Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures,” Public Key Cryptography - PKC 2011, Springer Berlin Heidelberg, 2011, pp. 1-16.

[5] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” Proceedings of the 40th annual ACM Symposium on Theory of Computing, 2008, pp. 197-206.

[6] Dan Boneh and David Mandell Freeman, “Homomorphic signatures for polynomial functions,” Advances in Cryptology - EUROCRYPT 2011, Springer Berlin Heidelberg, 2011, pp. 149-168.

[7] Dan Boneh, *et al.,* “Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits,” Advances in Cryptology - EUROCRYPT 2014, Springer Berlin Heidelberg, 2014, pp. 533-556.