준동형 집합 서명을 이용한 일반적인 준동형 다중서명 설계 방법[1)]

최락용* 김광조*

*카이스트 전산학부

Generic Construcition of Homomorphic Multisignatures from Homomorphic Aggregate Signatures

Rakyong Choi* Kwangjo Kim*

*School of Computing, KAIST

요 약

준동형 서명이란 주어진 서명 알고리즘을 이용해 다수의 개인 서명자 S_i가 각각의 메시지 m_i에 대해서 서명 σ_i를 하고 이 정보를 서버에 저장한다고 가정할 때, 어떤 데이터 수집가가 평균, 표준편차 등의 데이터 f를 요구할 경우 서버 상에서 함수 값 $f(m_1, m_2, ..., m_n)$에 대한 올바른 서명 σ_f를 계산할 수 있는 서명을 말한다. 본 논문은 임의의 데이터 m_j에 대한 서명자가 개인 서명자가 아닌 그룹 서명자라고 가정하여, 준동형 서명을 준동형 다중서명으로 확장하는 일반적인 방법을 제시하고, 구체적 사례를 제시한다.

I. 서론

최근 클라우드 시스템의 성장으로 인해 암호화된 메시지에 대한 계산 및 인증 방법을 어떻게 해결할 것인지가 문제로 제기되고 있다. 이 중 암호화된 메시지에 대한 계산은 2009년 Gentry의 완전 준동형 암호에 대한 논문[1] 이후 많은 연구가 진행되었으며, 이제 구현까지도 이루어지고 있다.

반면 암호화된 메시지의 계산식에 대해서 서명을 통해 인증하는 방법은 최근까지 활발한 연구가 진행되었으며 특히 2015년 Gorbunov 등은 래티스 기반 어려운 문제를 이용해 모든 암호화된 메시지의 계산식에 대해서 서명을 만들어주는 완전 준동형 서명을 발표하였다[2]. 하지만 현재까지의 논문은 개인 서명자에 의한 서명에 대해서만 생각한다는 단점이 있으며 이로 인해 회사, 정부 등 그룹 서명자가 존재하는 실제 클라우드 시스템에 준동형 서명을 적용하기에는 아직 무리가 있다.

따라서 본 논문에서는 기존의 준동형 서명에서 사용한 기법들을 분석하여, 그룹 사용자에 의해 암호화된 메시지에 대해서도 그룹 서명자에 의한 서명으로 인증하는 방법에 대해 제시한다.

1.1 논문의 구성

본 논문의 구성은 다음과 같다. 우선 II장에서는 래티스의 정의와 래티스 기반 어려운 문제를 설명한 뒤, 래티스 기반 알고리즘에는 어떤 것들이 있는지 알아본다. III장에서 기존에 알려진 래티스 기반 선형 준동형 서명(linearly homomorphic signature) 및 준동형 집합 서명(homomorphic aggregate signature)에는 어떤 것들이 있었는지 다루고, 준동형 집합 서명으로부터 그룹 서명자를 가질 수 있는 준동형 다중서명(homomorphic multisignature)으로 확장하는 방법에 대해서 알아본다. 마지막으로 IV장에서는 현재까지 진행 상황을 정리하고 추후 진행과제에는 어떤 것들이 있는지 제시한다.

1) 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2015R1A2A2A01006812).

II. 배경지식

양자컴퓨터 출현에 대비하여 암호학자들은 래티스 기반 암호, 코드 기반 암호, 다변수 이차 다항식 기반 암호, 해시 기반 암호 등 양자컴퓨터를 이용한 공격에 견딜 수 있는 포스트 양자 암호에 대한 활발한 연구를 진행하였다. 이 중 래티스 기반 암호는 최근 암호학에서 가장 많이 사용되는 도구로, 이번 장에서는 래티스의 정의와 래티스 기반 어려운 문제에 대해 설명하고 래티스 기반 알고리즘에는 어떤 것들이 있는지 다룬다.

2.1 래티스 및 래티스 기반 난제

일반적으로 래티스는 덧셈 연산을 가지는 임의의 군(group) G의 부분집합 중 이산 부분군(discrete subgroup)의 성질을 만족하는 집합을 말하며, 이러한 이산 부분군을 생성해주는 생성집합(generating set)을 기저(basis)라고 말한다. 특히 군 G가 정수 공간 $\mathbb{Z}^m$ 상에 있을 경우 정수 래티스(integer lattice)라고 지칭하며, 임의의 행렬 $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$에 대해 생성되는 래티스를 $\Lambda_q^{\perp}(\mathbf{A}) = \{e \mid A \cdot e = 0 \bmod q\}$라고 나타낸다.

이러한 래티스를 이용한 어려운 문제로는 대표적으로 Learning With Errors(LWE) 문제와 Small Integer Solution(SIS) 문제가 있으며 암호를 만드는 데 많이 이용된다. LWE 문제란 주어진 벡터와 임의의 작은 에러에서 비밀키를 찾는 문제로 유일한 해답이 존재하여 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 $z_1, z_2, \ldots, z_m \in \{-1, 0, 1\}$을 찾는 문제로 유일한 해 s를 가지는 LWE 문제와 달리 여러 가지 답이 나올 수 있어 디지털 서명 등에서 주로 이용된다.

2.2 래티스 기반 알고리즘

래티스 기반 암호는 비밀키 생성 과정에서 작은 기저를 비밀키로 가지며, 이를 위해서는 사이즈가 작은 트랩도어(trapdoor) 행렬을 생성하여야한다.

Alwen과 Peikert에 의해 제안된[3] 트랩도어(trapdoor) 생성 알고리즘 *TrapGen(n, m, q)*은 행렬 $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$에 의해 생기는 래티스 $\Lambda_q^{\perp}(\mathbf{A})$의 기저가 되는 사이즈가 작은 트랩도어 행렬 $\mathbf{T}$를 추출하는 알고리즘이다.

이 트랩도어 생성 알고리즘을 기반으로 Cash 등에 의해 행렬 $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$와 트랩도어 행렬 $\mathbf{T}$로부터 충분히 작은 사이즈를 가지는 임의의 기저 $\mathbf{T}^*$를 추출하는 임의 기저 알고리즘 *RandBasis(**T**, s)*와 행렬 $\mathbf{B}=\mathbf{A}|\mathbf{A}' \in \mathbb{Z}_q^{m \times (n+n')}$와 행렬 $\mathbf{A}$의 트랩도어 행렬 $\mathbf{T}$로부터 행렬 $\mathbf{B}$의 트랩도어 행렬 $\mathbf{S}$를 추출하는 기저 추출 알고리즘 *ExtBasis(**T**, **B**)*를 제안하였다[4].

한편 Gentry 등은 어떤 래티스와 그에 따른 트랩도어 행렬 $\mathbf{T}$가 주어졌을 때, 가우시안 분포 상에서의 벡터 σ를 생성해주는 가우시안 샘플링 알고리즘 *SamplePre(**A**, **T**, γ, **u**)*를 제안하였다[5].

III. 제안 방법

이번 장에서는 준동형 서명과 준동형 집합 서명에 대해서 소개하고, 준동형 집합 서명에서 사용한 아이디어를 변형하여 본 논문에서 제안하는 준동형 다중 서명을 만드는 방법에 대해서 제시한다.

3.1 준동형 서명 및 집합 서명[6]

임의의 서명 기법에 대해 다수의 서명자 S_i가 각각의 메시지 m_i에 대해서 서명 σ_i를 하고 서버에 저장한다고 가정한다. 이 때, 어떤 데이터 수집가가 평균, 표준편차와 같이 메시지 m_i에 대한 함수식 f를 요구할 경우 서버 상에서 각 메시지에 대한 정보 공개 없이 메시지의 기존 서명 σ_i을 통해 함수 값 $f(m_1, m_2, \ldots, m_n)$에 대한 올바른 서명 σ_f를 계산할 수 있다면 이 서명 기법은 준동형 성질을 만족한다. 준동형 성질(homomorphic property)을 만족하는 서명 기

법을 준동형 서명(homomorphic signature)이라고 부르며 함수 f의 차수에 따라 선형 준동형 서명 혹은 완전 준동형 서명(fully homomorphic signature)이라고 칭한다. 현재 알려진 래티스 기반 준동형 서명은 각 서명자가 같은 비밀키를 공유하고 있어야 한다.

한편, 집합 서명(aggregate signature)이란 메시지에 대한 계산 없이 서로 다른 메시지 m_i와 서명 σ_i에 대해서 하나의 서명으로 합쳐줄 수 있는 서명 기법으로 준동형 서명과 달리 메시지를 계산한 함수 값에 대해서는 서명을 제공하지 못하지만 각 서명자가 서로 다른 비밀키를 가진다.

3.2 Zhang 등의 준동형 집합 서명[7]

2012년 Zhang 등은 Boneh와 Freeman이 제안한 선형 준동형 서명[8]을 개선하여 준동형 서명의 성질과 집합 서명의 성질을 동시에 가지도록 하는 새로운 서명인 준동형 집합 서명을 제안하였다. 준동형 집합 서명은 서로 다른 비밀키를 가지는 사용자에 대해서도 준동형 성질을 만족하며 Zhang 등이 제안한 구체적인 프로토콜은 다음과 같은 다섯 가지 알고리즘으로 구성된다.

Setup(n, params): g명의 개인 서명자가 있을 때, 첫 번째 개인 서명자의 비밀키는 *TrapGen(n, m, q)* 알고리즘을 통해 나오는 행렬 **A**의 트랩도어 행렬 $\mathbf{T_1}$로 잡고, 다른 개인 서명자의 비밀키는 *RandBasis*($\mathbf{T_1}$, *s*) 알고리즘을 통해 나오는 행렬 **A**의 또 다른 기저 $\mathbf{T_2}$, $\mathbf{T_3}$, …, $\mathbf{T_g}$로 잡는다. 이 때 모든 서명자는 같은 공개키로 행렬 **A**를 가지며 해시 함수 H를 가진다.

Sign($sk, id,$ v): 서명 알고리즘으로 태그 id에 대해 **B=A**|$H(id)$를 계산하고, *ExtBasis*($\mathbf{T_i}$, **B**) 알고리즘으로 **B**의 기저 $\mathbf{S_i}$를 각각의 비밀키 $\mathbf{T_i}$에 대해 계산한다. 이후 **B**와 $\mathbf{S_i}$를 통해 서명 σ_i를 계산해준다.

AggMsg($pk, id, g, \{\alpha_i, m_i\}_{i=1}^{g}$): 같은 태그 id를 가지는 메시지 m_i에 대해 α_i가 m_i에 대한 가중치라고 할 때, $m_{agg} = \sum_{i=1}^{g} \alpha_i m_i$를 계산하는 알고리즘이다.

AggSig($pk, id, g, \{\alpha_i, \sigma_i\}_{i=1}^{g}$): 같은 태그 id를 가지는 서명 σ_i에 대해 α_i가 σ_i에 대한 가중치라고 할 때, $\sigma_{agg} = \sum_{i=1}^{g} \alpha_i \sigma_i$를 계산하는 알고리즘이다.

Verify($pk, id,$ **y**, σ): 서명이 올바른 서명인지 검증하는 알고리즘이다.

3.3 제안하는 확장 방법

Boneh와 Freeman의 논문과 비교하여 Zhang 등이 제안한 논문의 가장 큰 차이점은 *RandBasis* 알고리즘을 통해 각 서명자마다 다른 비밀키를 공유할 수 있다는 점이다. 하지만 Zhang 등이 제안한 논문 역시 한 메시지마다 하나의 서로 다른 비밀키를 가지는 개인 서명자가 있다는 점에서 서로 다른 비밀키를 가지는 그룹 서명자에 대해서는 설명하지 못한다. 따라서 Zhang 등이 제안한 논문을 복수 서명자를 가질 수 있는 서명으로 수정하여 다음과 같이 제안한다.

Setup(n, params): g명의 그룹 서명자가 있을 때, 그룹의 첫 번째 서명자의 비밀키는 *TrapGen(n, m, q)* 알고리즘을 통해 나오는 행렬 **A**의 트랩도어 행렬 $\mathbf{T_1}$로 잡고, 그룹의 다른 서명자의 비밀키는 *RandBasis*($\mathbf{T_1}$, *s*) 알고리즘을 통해 나오는 행렬 **A**의 또 다른 기저 $\mathbf{T_2}$, $\mathbf{T_3}$, …, $\mathbf{T_g}$로 잡는다. 이 때 그룹 내의 서명자는 같은 공개키로 행렬 **A**를 가지며 해시 함수 H를 가진다.

PreShare(g, v): 메시지 m에 각각의 멤버에 에러 $e_1, e_2, \cdots, e_g$를 더하여 $m_1, m_2, \cdots, m_g$로 그룹 내의 각 서명자에게 분배하는 알고리즘이다. 이 때, $m = \sum_{i=1}^{g} m_i$이 되도록 한다.

Sign($sk, id,$ $\mathbf{v_i}$): 그룹 내 서명자의 서명 알고리즘으로 Zhang 등의 논문과 동일하다.

Combine$(pk, id, g, \{\sigma_i\}_{i=1}^{g})$: 메시지 m의 서명을 계산하는 알고리즘으로 에러가 더해진 각각의 메시지 m_i에 대한 서명을 σ_i라고 할 때, m의 서명 $\sigma = \sum_{i=1}^{g} \sigma_i$를 계산하는 알고리즘이다.

LinCom$(pk, id, \{g_j, \sigma_j\}_{j=1}^{l})$: 같은 태그 id를 가지는 서명 σ_j에 대해 α_j가 σ_j에 대한 가중치라고 할 때, $\sigma_{lin} = \sum_{j=1}^{l} \alpha_j \sigma_j$를 계산하는 알고리즘이다. 이 때, l은 선형 준동형 성질을 만족하도록 해야 한다.

Verify$(pk, id,$ **y,** $\sigma)$: 서명이 올바른 서명인지 검증하는 알고리즘이다.

여기에서 일반적으로 **PreShare**$(g,$ **v**$)$ 알고리즘을 준동형 집합 서명에 적용하면 메시지를 사전에 분배함으로써, 준동형 집합 서명으로부터 간단히 준동형 다중서명을 만들어낼 수 있다.

IV. 결론

본 논문에서 우리는 기존에 소개된 래티스 기반 선형 준동형 서명 및 준동형 집합 서명에 대해 간단히 소개한 뒤, Zhang 등의 준동형 집합 서명 논문을 확장하여 선형 준동형 성질을 만족하는 준동형 다중서명을 설계하는 방법에 대해서 알아보았다. 이를 통해 정부, 회사 등 그룹 서명자가 있는 실제 클라우드 시스템에서도 제안하는 준동형 다중서명을 활용할 수 있을 것으로 예상된다.

추후 진행할 연구로는 우선 제안한 확장 방법의 안전성을 증명하고, 그룹 서명(group signature), 링 서명(ring signature) 등을 기반으로 더 효율적인 그룹 서명자 기반 선형 준동형 서명 기법을 개발하고 일반화된 방법을 연구할 예정이다. 또한 Gorbunov 등의 논문[2]을 확장하여 그룹 서명자를 가질 수 있는 완전 준동형 서명을 만들어볼 것이다.

[참고문헌]

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

[2] 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.

[3] Joël Alwen and Chris Peikert, "Generating Shorter Bases for Hard Random Lattices," Theory of Computing Systems, 48(3), 2011, pp. 535-553.

[4] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. "Bonsai Trees, or How to Delegate a Lattice Basis," Journal of Cryptology, 25(4), 2012, pp. 601-639.

[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] Giulia Traverso, Denise Demirel, and Johannes Buchmann, "Homomorphic Signature Schemes - A Survey," Cryptology ePrint Archive: Report 2015/954, 2015. avaliable at http://eprint.iacr.org/2015/954.

[7] Peng Zhang, Jianping Yu, and Ting Wang, "A Homomorphic Aggregate Signature Scheme Based on Lattice," Chinese Journal of Electronics, 21(4), 2012, pp. 701-704.

[8] 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.