다자간 복수키 래티스 기반 준동형 서명 방식의 분류[1)]

최락용* 김광조*

*카이스트 전산학부

Classification of Multi-key Multi-party Homomorphic Signature from Lattice

Rakyong Choi* Kwangjo Kim*

*School of Computing, KAIST

요 약

다자간 복수키 준동형 서명이란 하나의 비밀키를 이용하여 모든 데이터를 서명하는 기존의 양자간 단일키준동형 서명과 달리 복수 서명자에 따라 복수의 비밀키를 가질 수 있는 서명을 말한다. 다자간 복수키 준동형 서명을 통해 서버는 복수의 서명자로부터 받은 데이터에 대해 올바른 서명을 만들어줄 수 있다. 본 논문에서는 다자간 복수키 준동형 서명을 소개하고, 기존의 선형 준동형 서명 논문들을 분석하여 다자간 복수키 준동형 성질을 만족하는 서명 기법을 비교 분석하였다.

I. 서론

최근 클라우드 시스템 환경의 발전과 함께 클라우드 상에 올린 데이터 인증에 대한 연구가 정보보호의 한 가지 중요한 문제로 대두되고 있다. 이 중 준동형 서명이란 특정 데이터에 대한 함숫값 요청에 대해 서버가 서명자를 대신하여 이 결과가 서명자로부터 나왔음을 증명할 수 있는 서명 기법으로[1], 최근 모든 함수에 대해 준동형 성질을 만족하는 완전 준동형 암호가 Gorbunov 등에 의해 제안되었다[2]. 하지만 기존의 서명 기법은 비밀키를 하나만 가져 서로 다른 비밀키를 가진 복수의 서명자로부터 온 데이터에 대한 함숫값에는 서명을 할 수 없는 단점이 있었으며, 이를 복수의 서명자, 더 나아가 복수의 개인 서명자 및 그룹 서명자 모두에 대해서 서명이 가능하도록 하는 준동형 서명 방식이 필요하다.

1) 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2015R1A2A2A01006812).

1.1 논문의 구성

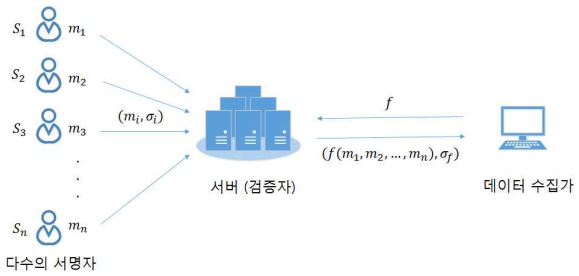
본 논문의 구성은 다음과 같다. 우선 II장에서는 준동형 성질 및 준동형 서명을 정의하고 다자간 복수키 준동형 서명에 대해 소개한다. 이어 III장에서는 기존에 알려진 래티스 기반 선형 준동형 서명을 다자간 복수키 준동형 성질을 만족하는지 여부에 따라 분류하며, IV장에서 각 방식의 비교와 추후 연구를 제시한다.

II. 다자간 복수키 준동형 서명

2.1 준동형 성질 및 준동형 서명

준동형 성질이란 [그림 1]과 같이 어떤 서명 기법에 대해 서명자 S_i가 각각의 데이터 m_i에 대해서 서명 σ_i를 하고 서버에 저장한다고 가정할 때, 어떤 데이터 수집가가 평균, 표준편차 등의 함수 f의 함숫값을 요구할 경우 서버가 각 데이터에 대한 정보 공개 없이 서버 상에서 데이터의 기존 서명을 이용하여 각 데이터의 함수 값 $f(m_1, m_2, ..., m_n)$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 또는 완전 준동형 서명이라 정의한다.



[그림 1] 준동형 서명 기법

2.2 다자간 복수키 준동형 서명

복수키 준동형 서명이란 준동형 성질을 만족하는 서명에서 서명을 만들 때 하나의 비밀키가 아닌 복수의 비밀키를 통한 데이터에 대해서도 준동형 성질을 만족하도록 서명을 만들어주는 서명을 말하며, 다자간 준동형 서명이란 서명 중에서 그룹 서명자로부터 생성된 서명이 있는 경우에도 준동형 성질을 만족하도록 하는 서명을 뜻한다.

따라서 다자간 복수키 준동형 서명을 통해 클라우드 서버는 개인이 올린 데이터에 대해서만 인증해주는 것만이 아니라, 다양한 그룹에서 올라온 데이터에 대한 서명 또한 할 수 있다.

III. 래티스 기반 선형 준동형 서명 분류

3.1 선형 준동형 서명

2011년 Boneh와 Freeman에 의해 두 종류의 래티스 기반 선형 준동형 서명 BF11a 방식[1], BF11b 방식[3]이 제안되었다. 두 논문 모두 Gentry 등이 사용한 서명 방식[4]을 토대로 한 논문으로 비밀키를 하나만 가지고 있다고 가정하여, 복수의 서명자가 다른 비밀키를 가지는 실제 상황에서 적용하기에는 어렵다.

3.2 복수키 선형 준동형 서명

2012년 Zhang 등이 제안한 집합 준동형 서명 ZYW12 방식[5]은 이하와 같은 5개의 알고리즘으로 구성된다.

Setup$(n,$ **params**$)$: g명의 서명자가 있을 때, 서명자의 비밀키를 트랩도어 생성 알고리즘을 통해 나오는 행렬 **A**의 트랩도어 행렬 $\mathbf{T_1}$과 임의의 기저 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**$)$: 태그 id에 대해 **B=A**$|H(id)$를 계산하고, 기저 확장 알고리즘으로 **B**의 기저 $\mathbf{S_i}$를 각각의 비밀키 $\mathbf{T_i}$에 대해 계산한 뒤, **B**와 $\mathbf{S_i}$를 통해 서명 σ_i를 생성.

AggMsg$(pk, id, g, \{\alpha_i, m_i\}_{i=1}^{g})$: 메시지의 합 $m_{agg} = \sum_{i=1}^{g} \alpha_i m_i$를 계산.

AggSig$(pk, id, g, \{\alpha_i, \sigma_i\}_{i=1}^{g})$: 메시지의 합 m_{agg}에 대한 서명 $\sigma_{agg} = \sum_{i=1}^{g} \alpha_i \sigma_i$를 계산.

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

이 때 ZYW12 방식은 Setup 알고리즘으로부터 서로 다른 비밀키를 복수의 서명자가 가지면서 준동형 성질을 만족하기 때문에 복수키 선형 준동형 서명이라고 볼 수 있다. 또한 Jing이 제안한 논문 Jing14 방식[6] 또한 복수키 선형 준동형 성질을 만족한다.

3.3 다자간 복수키 선형 준동형 서명

최근 Choi와 Kim이 제안한 준동형 다중서명 논문 CK16a 방식[7]은 다음의 6개의 알고리즘을 가진다.

Setup$(n, g,$ **params**$)$: g명의 그룹 서명자가 있을 때, 트랩도어 생성 알고리즘을 g번 실행하여 행렬 A_i와 트랩도어 행렬 T_i를 잡고, $A = A_1 \| A_2 \| \cdots \| A_g$, $H: \{0,1\}^* \rightarrow \mathbb{Z}_q^{l \times n}$로 잡아 각 그룹 내의 서명자의 공개키 $pk = (A, H)$와 비밀키 $sk = T_i$를 출력.

PreShare(g, m): 가우시안 샘플링 알고리즘을 이용해 메시지 m에 각각의 멤버에 노이즈 $e_1, e_2, \cdots, e_g$를 더하여 $m_1, m_2, \cdots, m_g$로 그룹 내의 각 서명자에게 분배하는 알고리즘. 이 때, $m = \sum_{i=1}^{g} m_i$이 되어야 한다.

Sign(sk_i, id, m_i): $B = A \| H(id)$로 잡고 B의 트랩도어 S_i를 기저 확장 알고리즘을 통해 찾고 가우시안 샘플링 알고리즘을 이용해 각 그룹 서명자의 부분서명 σ_i를 출력.

Combine$(pk, id, g, \{\sigma_i\}_{i=1}^{g})$: 메시지 m_i의 부분서명 σ_i에서 메시지 m의 서명 $\sigma = \sum_{i=1}^{g} \sigma_i$를 계산해주는 알고리즘.

LinCom$(pk, id, \{g_j, \sigma_j\}_{j=1}^{L_g})$: 같은 태그 id를 가지는 서명 σ_j에 대해 α_j가 σ_j에 대한 가중치 일 때, $\sigma_{lin} = \sum_{j=1}^{L_g} \alpha_j \sigma_j$를 계산하는 알고리즘이다. 단, L_g는 $\sum_{j=1}^{L_g} \alpha_j g_j \leq L$를 만족해야 한다.

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

여기서 CK16a 방식은 Sign 알고리즘과 Setup 알고리즘으로부터 그룹 서명자로부터 서명을 생성할 수 있으며, 각 서명자는 다른 비밀키를 가진다는 것을 확인할 수 있으므로 다자간 복수키 선형 준동형 서명이라고 할 수 있다. 이 밖에도 CK16b 방식[8] 또한 다자간 복수키 선형 준동형 성질을 만족한다.

IV. 비교 및 추후 연구

본 논문은 기존에 제안되었던 선형 준동형 서명 논문들을 다자간 복수키 준동형 개념을 이용하여 [표 1]과 같이 비교하였다.

차후 연구에는 다자간 복수키 준동형 서명에 대해 정확한 보안 모델을 잡고 기존 논문들이 보안 모델에 대해 적합한지에 대한 연구가 필요하다.

[표 1] 래티스 기반 선형 준동형 서명 분류

방식	준동형 성질	복수키 준동형	다자간 준동형
BF11a[1] BF11b[3]	O	X	X
ZYW12[5] Jing14[6]	O	O	X
CK16a[7] CK16b[8]	O	O	O

O: 만족 X: 불만족

[참고문헌]

[1] D. Boneh and D. M. 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.

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

[3] D. Boneh and D. M. Freeman. “Homomorphic signatures for polynomial functions,” Advances in Cryptology - EUROCRYPT 2011. Springer Berlin Heidelberg, 2011. pp. 149-168.

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

[5] P. Zhang, J. Yu, and T. Wang, “A Homomorphic Aggregate Signature Scheme Based on Lattice,” Chinese Journal of Electronics, 21(4), 2012, pp. 701-704.

[6] Z. Jing, “An efficient homomorphic aggregate signature scheme based on lattice,” Mathematical Problems in Engineering, 2014.

[7] R. Choi and K. Kim, “Lattice-based Multi-signature with Linear Homomorphism,” 2016 Symposium on Cryptography and Information Security (SCIS 2016), 2016.

[8] 최락용, 김광조, “래티스 기반 선형 준동형 다중서명 설계 방법,” 한국정보보호학회 하계학술대회(CISC-W'16), 2016.