메시지 다중화 기술 및 이를 적용한 격자 기반 문턱서명 방식1)

최락용* 김광조*

*KAIST 전산학과

Message Block Sharing and Its Application: Lattice-based Threshold Signature Scheme

Rakyong Choi* Kwangjo Kim*

*Department of Computer Science, KAIST

요 약

문턱서명(k-out-of-N Threshold Signature) 기술이란 N명의 복수 서명자가 하나의 메시지에 대해서 서명을 한 뒤 이 중 k명 이상의 서명자의 서명이 있어야 메시지에 대한 인증이 가능한 전자서명 방식이다. 본 논문에서는 기존에 쓰이던 문턱서명 기술에 쓰이던 메시지 서명 방식이 보안강도에 따라 서명 방식의 조정이 어려웠던 것을 보완한 새로운 문턱서명 방식을 만들기 위해 메시지 다중화 기술(Message Block Sharing)을 설명하고 이를 격자 기반 암호기술에 적용하여 양자컴퓨터 공격에 대응할 수 있는 보안강도 조절이 가능한 서명방식을 제안한다.

I. 서론

일반적으로 전자서명 방식은 서명자가 비밀키를 이용하여 서명을 하고 검증자가 공개키를 통해 서명이 메시지에 대한 올바른 서명인지 확인한다. 하지만 이 방식은 서명자의 권한이 지나치다는 문제가 있었고 이를 보완하기 위해 제안된 서명 방식으로 N명의 복수 서명자가 하나의 메시지에 대해서 서명을 한 뒤 이 중 k명 이상의 서명자의 서명이 있어야 메시지에 대한 인증이 가능한 문턱서명(k-out-of-N Threshold Signature) 방식이 제안되었으며 Desmedt의 논문을 통해 문턱서명의 일반적인 개념이 정립되었다[1].

한편 격자 기반 암호는 Ajtai의 논문[2]을 통해 제안된 이후, 양자컴퓨터 공격에 강한 암호이며 수학적 계산이 어려운 문제들을 기반으로 오늘날에는 다양한 함수형암호, 완전준동형암호 등 최신암호기술들이 격자 기반으로 제안되고 있다[3, 4, 5].

1.1 관련 연구

기존에 연구된 격자 기반 문턱서명 방식으로는 Feng 등이 제안한 NTRUSign 기법을 이용한 문턱서명 방식[6], Cayrel 등이 제안한 ring 문턱서명 방식[7], Bendlin 등이 제안한 격자 trapdoor를 공유하는 방법을 이용한 문턱서명 방식[8] 등이 있으나 논문[6]은 NTRUSign이 이미 가능한 공격이 알려진 기법이고, 논문[7]은 SIS(Small Integer Solution)를 이용한 서명은 LWE(Learning with Errors)를 이용한 서명보다 위조가 쉽다는 단점이 있다. 본 논문은 저자 등이 이러한 점을 보완하여 발표한 SCIS 2014 논문[9]를 수정한 연구이다.

1) 본 연구는 미래부가 지원한 2014년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음.

1.2 제안하는 기법에 이용되는 기술

다양한 격자 기반 서명 방식을 다룬 논문들 중 이 논문에서는 Gentry 등이 제안한 논문[10]과 Gordon 등이 제안한 논문[11]에 쓰인 기법을 응용하기로 한다. 특히 논문[10]의 Gaussian 확률 분포와 이를 이용한 효율적인 "해시 후 서명(hash-then-sign)"을 통한 서명 기술과 논문[11]의 직교 격자(Orthogonal Lattice)와 그의 trapdoor를 추출(sampling)하는 알고리즘을 이용한다.

1.3 논문의 구성

본 논문의 구성은 다음과 같다. 2장에서는 문턱서명 방식의 설계에 있어 기존에 알려진 보조정리 및 알고리즘에 대해 간단히 설명한다. 이어 3장에서는 메시지 다중화 기술을 어떻게 만들어내는지에 대해 설명하고 4장에서 격자 기반 문턱서명 방식의 정의 및 보안 요구사항(security requirement), 구현 등에 대해서 설명한다. 마지막으로 5장에서는 기존의 격자 기반 문턱서명 방식과 제안된 방식을 비교해본다.

II. 배경지식

본 장에서는 메시지 다중화 기술 및 격자 기반 문턱서명 방식의 설계에 필요한 여러 보조정리 및 알고리즘에 대해 설명한다.

2.1 직교격자와 Gaussian 확률 분포

직교격자란 어떤 행렬 $B \in Z_q^{n \times m}$에 대해 $B^T w \equiv 0 \pmod q$를 만족하는 $w \in Z^m$의 집합 $\Lambda^{\perp}(B)$를 말하며 Gaussian 확률 분포 중 격자에서는 이산 Gaussian 확률 분포라 하여 Gentry 등의 논문[10]에서 1.2에서 설명할 LWE 문제에 이용되는 에러 변수(error parameter) e를 잘 추출할 수 있다는 것을 보인다.

2.2 LWE(Learning with Errors) 문제

LWE 문제는 격자 기반 문제 중 가장 유명한 문제 중 하나이다. LWE 문제는 기존에 잘 알려진 유명한 문제인 "LPN(Learning Parity with Noise)" 문제를 격자 기반 문제로 일반화하여 Regev가 2005년 LWE 문제와 이를 활용한 암호 기법들에 대해 설명[12]하였고, 이후 다양한 분야에서 활용되고 있다[3, 4, 5].

2.3 직교격자와 trapdoor의 추출 방법

본 논문에서는 논문[11]과 마찬가지로 Alwen과 Peikert가 제안한 격자의 trapdoor 추출 알고리즘[13]과 논문[11]의 직교격자의 trapdoor 추출 알고리즘, 논문[10]의 trapdoor와 Gaussian 확률 분포를 통한 에러 생성 알고리즘을 이용한다.

보조정리 1[13]. $q \geq 2$이고 $m \geq 8n\log q$일 때, 격자의 trapdoor 추출 알고리즘 TrapSamp $(1^n, 1^m, q)$이 있어 $A \cdot T = 0 \pmod q$이고 $\|T\|$의 크기가 충분히 작은 행렬 $A \in Z_q^{n \times m}$와 trapdoor $T \in Z^{m \times m}$를 생성한다.

보조정리 2[11]. $q \geq 2$이고 $m \geq 8n\log q$일 때, 직교격자의 trapdoor 추출 알고리즘 OrthoSamp$(1^n, 1^m, q, B \in Z_q^{n \times m})$이 있어 $AB^T = 0 \pmod q$, $A \cdot T = 0 \pmod q$이고 $\|T\|$의 크기가 충분히 작은 행렬 $A \in Z_q^{n \times m}$와 trapdoor $T \in Z^{m \times m}$를 생성한다.

보조정리 3[10]. Gaussian 에러 생성 알고리즘 GPVInvert(A, T, s, u)가 있어 $At = u \pmod q$를 만족하는 t에서 에러 e를 생성한다.

III. 메시지 다중화 기술

본 장에서는 이항계수와 메시지를 나눈 메시지 블록을 이용한 메시지 다중화 기술에 대해서 설명하고 간단한 예와 메시지 블록 생성 알고리즘에 대해서 설명한다.

3.1 2-out-of-3 메시지 다중화 기술

3명의 그룹이 있어 이 중 2명이 모이면 메시지를 확인할 수 있다고 생각해본다. 여기에서 메시지 블록은 총 3개가 필요하고 개인에게는 2개의 메시지 블록만이 주어진다면 3명의 그룹

중 2명이 모여 메시지를 확인할 수 있다. ($\Gamma_1 = \{M_2, M_3\}, \Gamma_2 = \{M_1, M_3\}, \Gamma_3 = \{M_1, M_2\}$)

3.2 k-out-of-N 메시지 다중화 기술

3.1의 경우를 일반화하여 N명의 그룹이 있어 이 중 k명이 모이면 메시지를 확인할 수 있다고 생각해보면, 각 메시지 블록은 최대 $k-1$명의 멤버에게 들어있지 않을 수 있으며 각 멤버는 정확히 같은 개수의 메시지 블록을 가진다고 가정한다. 이 때 메시지 블록은 정확하게 $\binom{N}{k-1}$개가 나오며 각 멤버는 $\binom{N-1}{k-1}$개의 메시지 블록을 가진다.

여기서 k, N은 메시지의 비트 길이에 따라 달라지며 메시지 M의 비트 길이를 $l(M)$이라 할 때, 알고리즘 TParamExt($l(M)$)가 있어 보안 변수(security parameter) n과 그룹 크기 N, 검증에 필요한 서명자의 수 k, 그리고 각 멤버의 메시지 블록 Γ_i를 결정한다.

IV. 격자 기반 문턱서명 방식

본 장에서는 격자 기반 문턱서명 방식의 정의와 이에 대한 보안 요구사항에 대해서 설명하고 메시지 다중화 기술을 이용한 새로운 문턱서명 방식을 제안한다. 또한 제안한 방식이 기존의 문턱서명 방식의 보안 요구사항을 만족함을 증명한다.

4.1 문턱서명 방식

일반적인 문턱서명 방식은 다음과 같은 4개의 알고리즘으로 구성된다[14].

T.Param(M): 문턱서명을 위한 변수를 준비하는 알고리즘으로 메시지 M을 이용하여 시스템에서 사용될 보안 변수 n, 서명에 필요한 그룹의 크기 N, 검증에 필요한 서명자의 수 k를 생성한다.

T.KeyGen($1^n, 1^N, 1^k$): 문턱서명을 위한 키를 생성하는 알고리즘으로 T.Param에서 생성된 변수들을 이용하여 공개키 PK와 N개의 비밀키 gsk를 생성한다. 4.3에서 제안하는 알고리즘에서는 이 때 추가로 각 멤버의 메시지 블록 Γ_i를 추가로 계산한다.

T.Sign(gsk, M or $(\Gamma_i)_{i=1}^N$): 비밀키 gsk와 메시지 M(또는 본 논문의 경우 $(\Gamma_i)_{i=1}^N$)을 이용하여 서명 σ를 생성한다.

T.Verify(PK, M or $(\Gamma_i)_{i=1}^N, \sigma$): 공개키 PK와 메시지 M(또는 본 논문의 경우 $(\Gamma_i)_{i=1}^N$), 서명 σ를 통해 이 서명 σ를 받아들일 것인지 거절할 것인지 결정한다.

4.2 보안 요구사항

침입자에 공모하는 멤버의 수를 τ라고 할 때, 올바른 서명을 위해서는 반드시 $k > \tau$이며 $N - \tau \geq k$이어야한다. 또한 문턱서명은 다음의 두 가지 보안 요구사항을 만족해야한다.

타당성(Correctness). 만일 침입자 중 공모하는 멤버가 한 명도 없다면 어떤 k명의 서명자의 서명으로도 올바른 서명을 만들어낼 수 있어야한다.

위조불가능성(Unforgeability). 침입자가 서명을 위조(forge)할 수 있는 확률이 무시 가능할 때 문턱서명 방식을 위조불가능하다고(unforgeable) 부르며 서명 쿼리에 τ명의 공모자가 있을 때, 침입자가 올바른 서명을 만들어낼 수 있다고 하면 침입자가 서명을 위조하였다고 정의한다.

4.3 제안하는 기법

논문[11]을 응용하여 n을 보안 변수, $q = poly(n), m \geq 8n\log q$, s를 다른 변수들이라고 할 때 해시 함수 $H: \{0,1\}^* \rightarrow Z_q^n$가 있어 다음과 같이 계산한다.

T,Param(M):

- 메시지 M의 비트 길이 $l(M)$을 계산한 뒤 TParamExt($l(M)$)으로부터 (n, N, k)를 구한다.

- 각 멤버의 메시지 블록 집합 Γ_i 역시 이 때 계산하며 새로운 집합 $\{\Delta_j\} = \{\Gamma_i\}$를 두어 Γ_i를 임의의 순서로 공개한다.

T.KeyGen($1^n, 1^N, 1^k$):

- [보조정리 1]의 TrapSamp($1^n, 1^m, q$) 알고리즘에서 행렬 B_i를 얻고 [보조정리 2]의 OrthoSamp($1^n, 1^m, q, B \in Z_q^{n \times m}$) 알고리즘을 이용하여 행렬과 trapdoor (A_i, T_i)를 계산한다.

- A_i를 공개키로 하고 (B_i, T_i)를 비밀키로 이용한다.

T.Sign(gsk, M or $(\Gamma_i)_{i=1}^N$):

- 각각의 멤버들의 메시지 블록에 대해 해시 값 $h_i = H(\Gamma_i)$를 계산하고 [보조정리 3]의 GPVInvert(A_j, T_j, s, h_j) 알고리즘을 통해 e_j를 계산한다.

- $z_i = B_i^T s_i + e_i (\mathrm{mod} q)$를 계산하고 이를 멤버 i의 서명으로 이용한다.

T.Verify(PK, M or $(\Delta_i)_{i=1}^N, \sigma$):

- 어떤 Δ_{j_i}에 대해 $A_i z_i = H(\Delta_{j_i})$가 성립하는지 확인한다.

- $\Delta_{j_{i1}} \neq \Delta_{j_{i2}}$가 모든 $i_1 \neq i_2$에 대해 성립하는지 확인한다.

- 두 가지를 모두 만족하는 경우만 메시지 M에 대한 서명을 받아들인다.

4.4 보안 요구사항 증명

정리 1. 제안한 방식은 타당성을 만족한다.

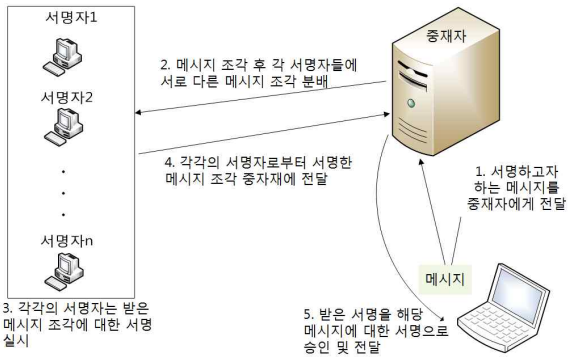
증명. 각각의 서명 z_i에 대해 $A_i z_i = A_i(B_i^T s_i + e_i) = A_i e_i = H(\Gamma_i) (\mathrm{mod} q)$가 성립하고 여기에서 어떤 j에 대해 $\Gamma_i = \Delta_j$이므로 z_i는 Γ_i에 대한 올바른 서명이다. 또한 $\bigcup_{i=1}^{k} \Gamma_i = M$이므로 k명의 서명자의 서명으로 올바른 서명을 만들어낼 수 있다.

정리 2. 제안한 방식은 위조불가능성을 만족한다.

증명. τ명의 공모자가 있다고 가정하더라고 $\tau < k$이므로 이를 공모자가 없을 경우 하나의 서명 z_i를 위조할 수 있는지에 대해 생각해볼 수 있다. 여기에서 LWE 문제의 어려움과 해시 함수의 선택에 의해 제안한 방식이 위조될 수 없다고(unforgeable) 할 수 있다.

V. 결론

본 논문은 메시지 다중화 기술을 제안하고 이를 격자 기반 암호기술에 적용해 양자컴퓨터 공격에 대응할 수 있으며 보안강도 조절도 가능한 서명방식을 제안하였다. [그림 1]은 제안한 방식의 간단한 동작과정 설명이다.



[그림 1] 메시지 다중화 기술을 이용한 격자 기반 문턱서명 방식의 동작과정

또한 [표 1]은 기존의 격자 기반 문턱서명 논문들[6, 7, 8]과 현재 제안한 방식을 비교하여 제안한 방식이 새로운 아이디어를 적용한 안전한 문턱서명 방식임을 확인할 수 있다.

	논문[6]	논문[7]	논문[8]	본 논문
격자	NTRU Lattice	**Ideal Lattice**	Lattice	Orthogonal Lattice
문제	CVP	SIS	**LWE**	**LWE**
알려진 공격	Y	N	N	N
idea	sequential signing	syndrome decoding	trapdoor sharing	message block

[표 1] 격자 기반 문턱서명 방식의 비교

추후 연구계획으로는 본 논문에 제안한 기법의 취약점에 대해서 분석하고 취약점에 대응할 수 있는 기법을 만들며 더 나아가 메시지 다중화 기술이 다른 어떤 암호 기법에 쓰일 수 있는지 분석하여 활용하고자 한다.

[참고문헌]

[1] Y. Desmedt, “Society and group oriented cryptography: a new concept,” *Advances in Cryptology – CRYPTO'87*, LNCS Vol.293, pp120-127, 1987

[2] Miklós Ajtai, “Generating hard instances of lattice problems,” *Proceedings of the twenty-eighth annual ACM Symposium on Theory of Computing*, ACM, pp99-108, 1996.

[3] Shweta Agrawal, David Mandell Freeman, and Vinod Vaikuntanathan, “Functional encryption for inner product predicates from learning with errors,” *Advances in Cryptology – ASIACRYPT 2011*, LNCS Vol.7073, pp21-40, 2011.

[4] Craig Gentry, Amit Sahai, and Brent Waters, “Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based,” *Advances in Cryptology – CRYPTO 2013*, LNCS Vol.8042, pp75-92, 2013

[5] Zvika Brakerski and Vinod Vaikuntanathan, “Efficient fully homomorphic encryption from (standard) LWE,” *Foundations of Computer Science (FOCS)*, IEEE, pp97-106, 2011.

[6] Tao Feng, Yongguo Gao, and Jianfeng Ma, “Changeable Threshold Signature Scheme Based on Lattice Theory,” *E-Business and E-Government (ICEE), 2010 International Conference on*, IEEE, pp1311-1315, 2010.

[7] Pierre-Louis Cayrel, Richard Lindner, Markus Rückert, and Rosemberg Silva, “A lattice-based threshold ring signature scheme,” *Progress in Cryptology – LATINCRYPT 2010*, LNCS Vol.6212, pp255-272, 2010.

[8] Rikke Bendlin, Sara Krehbiel, and Chris Peikert, “How to share a lattice trapdoor: threshold protocols for signatures and (H) IBE,” *Applied Cryptography and Network Security*, LNCS Vol.7954, pp218-236, 2013.

[9] Rakyong Choi and Kwangjo Kim, “Lattice-based Threshold Signature with Message Block Sharing,” *The 31st Symposium on Cryptography and Information Security*, Kagoshima, Japan, 2014.1.21-1.24

[10] 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*, ACM, pp197-206, 2008.

[11] S. Dov Gordon, Jonathan Katz, and Vinod Vaikuntanathan, “A group signature scheme from lattice assumptions,” *Advances in Cryptology – ASIACRYPT 2010*, LNCS Vol.6477, pp395-412, 2010.

[12] Oded Regev, “On lattices, learning with errors, random linear codes, and cryptography,” *Proceedings of the thirty-seventh annual ACM Symposium on Theory of Computing*, ACM, pp84-93, 2005.

[13] Joël Alwen and Chris Peikert, “Generating shorter bases for hard random lattices,” *Theory of Computing Systems*, Vol.48, Issue3, pp535-553, 2011

[14] Victor Shoup, “Practical threshold signatures,” *Advances in Cryptology – EUROCRYPT 2000*, LNCS Vol.1807, 207-220, 2000