학 사 학 위 논 문
Bachelor's Thesis

격자 기반 서명 암호화 방식과 인증 키 교환의 암호학적 특성 비교

A Comparison of Cryptographic Protocol between Lattice-based Signcryption and Generic Authenticated Key Exchange

2018

백 승 근 (白 承 根 Baek, Seung Geun)

한 국 과 학 기 술 원

Korea Advanced Institute of Science and Technology

학 사 학 위 논 문

격자 기반 서명 암호화 방식과 인증 키 교환의 암호학적 특성 비교

2018

백 승 근

한 국 과 학 기 술 원

전산학부

초 록

1997년 Zheng에 의해 제안된 서명 암호화(Signcryption)는 정보의 기밀성과 인증 기능을 동시에 제공하는 암호화 방식이다. 하이브리드 서명 암호화 모델의 일부로 인증 기능을 제공하는 KEM (Signcryption KEM, SKEM)이 제시되었으며, 여러 연구가 SKEM이 인증 키 교환(Authenticated Key Exchange, AKE)과 밀접히 연관되어 있음을 논증하고 있다. 양자 내성 암호 등장의 맥락에서, 본 논문은 알려진 격자 기반 서명 암호화 기법을 조사하고 AKE 등으로의 확장 가능성에 대해 전망하고자 한다.

핵 심 낱 말 서명 암호화, 인증 키 교환, 격자 기반 암호

Abstract

First proposed by Zheng on 1997, signcryption schemes are encryption modules that providing not only confidentiality but also authentication. The concept of hybrid signcryption brought the model of an authentication-providing signcryption KEM (SKEM). Researches have shown that SKEM has close relationship with Authenticated Key Exchange (AKE). In the context of post-quantum cryptography, I survey researches surrounding lattice-based signcryption and extend their usages toward AKE schemes.

Keywords Signcryption, Authenticated Key Exchange, Lattice-based Cryptography

차 례

제 1 장 머릿말

Zheng은 암호문의 기밀성과 송신자 인증 가능성을 동시에 만족하면서도, 비대칭 암호화와 전자서명을 별도로 수행하는 경우에 비해 더 적은 비용이 소모되는 서명 암호화의 개념을 최초로 제시하였다[Zhe97]. 일반적인 배경 이론이 Dent의 형식 체계를 통해 정의되었으며[Den05a][Den05b], Baek 등에 의해 다자간으로 확장되었다[BSZ07].

인증 키 교환 방식은 추후 대칭 키 암호화 등에 사용하기 위해, 양자간에 동일한 비밀 키를 공유하는 방식의 하나이다. 인증 키 교환 방식의 참여자들은 중도에 이루어지는 키 생성 요소의 통신 과정에서 상대방을 인증하여야 한다. 일반 키 교환 방식의 역사는 Diffie-Hellman 프로토콜까지 거슬러 올라가지만, 중간자 공격을 방지하기 위한 인증 키 교환 방식은 Bellare와 Rogaway에 의해 정립되었다[BR93].

Gorantla 등에 따르면, 서명 암호화를 이용한 KEM과 일방향 키 교환 방식은 특정한 조건을 만족할 때 서로 변환 가능하다[GBN07]. 이에 대한 자세한 사항은 3.2에서 논한다. 해당 결과는 서명 암호화를 이용하여 인증 키 교환 방식을 유도하고, 반대로 인증 키 교환 방식을 응용하여 서명 암호화 방식을 제작할 수 있는 가능성을 열어 두었다.

한편, 양자 컴퓨터 기술의 발달은 기존에 사용되는 암호체계를 위협하고 있다. 예를 들어, Shor의 알고리즘은 소인수분해, 이산 로그, 타원곡선 이산 로그 문제 등을 공격한다. 그 결과, 각각 RSA, Diffie-Hellman 키 교환, 타원곡선 암호 등의 안전성이 무효화될 수 있다. 양자 내성 암호 연구에서는 양자 컴퓨터에서도 어려울 것으로 예상되는 대안 문제들을 바탕으로 암호 체계를 제작하고 분석한다. 그 중 하나로서, 격자 기반 암호는 Learning With Errors (LWE), Short Integer Solution (SIS) 등 격자 관련 문제에 기반을 두고 있다.

이러한 맥락에서, 본 논문은 서명 암호화와 인증 키 교환에 관한 이론뿐만 아니라 격자 기반의 여러 설계 및 그 확장 가능성에 관하여 논한다.

제 2 장 이론적 배경

2.1 서명 암호화

서명 암호화는 다음 5개 다항 시간 알고리즘의 집합이다.

$param \leftarrow \mathbf{Setup}(1^k)$
$Setup$은 서명 암호화 방식에 사용될 공개된 인자 $param$을 생성한다.

$(pk_S, sk_S) \leftarrow \mathbf{KeyGen}_S(param)$
$KeyGen_S$는 송신자가 사용할 키의 쌍을 생성한다.

$(pk_R, sk_R) \leftarrow \mathbf{KeyGen}_R(param)$
$KeyGen_R$는 수신자가 사용할 키의 쌍을 생성한다.

$C \leftarrow \mathbf{Signcrypt}(\mu, pk_R, sk_S[, pk_S])$
송신자는 $Signcrypt$를 실행하여 μ의 암호문 C를 생성한다. 이 때 송신자의 비밀키 sk_S와 수신자 또는 쌍방의 공개키를 활용한다.

$\mu \leftarrow \mathbf{Unsigncrypt}(C, pk_S, sk_R[, pk_R])$
$Unsigncrypt$ 는 수신자가 실행하는 결정적 알고리즘으로, 송신자의 메시지 μ 또는 복호화 실패 메시지 $\perp$를 출력한다. $Unsigncrypt$는 수신자의 비밀키 sk_R과 송신자 또는 쌍방의 공개키를 활용한다.

2.1.1 기본적 설계([DZ10])

An과 Rabin이 [DZ10]에서 논한 것과 같이, 서명 암호화 방식은 전자 서명 방식 Sig와 공개키 암호 Enc를 세 가지 방법으로 조합하여 생성할 수 있다.

암호화 및 서명. 송신자는 전자 서명의 결과와 공개키 암호문을 단순 연결하여 $C = (Enc_{pk_R}(m), Sig_{sk_S}(m))$를 생성할 수 있다. 이 방식은 공격자가 서명을 검증함으로써 메시지를 구별할 수 있기 때문에 후술할 IND-CCA 안전성을 만족하지 못한다.

암호화 후 서명. 송신자는 메시지에 대한 공개키 암호문 $c = Enc_{pk_R}(m)$을 만들고, 공개키 암호문과 그에 대한 서명을 포함한 암호문 $C = (c, Sig_{sk_S}(c))$를 수신자에게 보낸다.

서명 후 암호화. 송신자는 메시지를 서명한 후($\sigma = Sig_{sk_S}(m)$) 평문과 함께 암호화한다. 그 결과 암호문 $C = Enc_{pk_R}(m||\sigma))$이 생성된다.

2.1.2 안전성 모델

기초 안전성 모델 ([DZ10]). 기밀성 요구조건을 위하여, 적응적 암호문 선택 공격에 대한 비구별성(IND-CCA2)을 공개키 암호에서와 유사한 방법으로 정의할 수 있다. IND-CCA2에 대한 game은 확률적 다항 시간 공격자가 제시한 μ_0, μ_1에서 $b \xleftarrow{\$} \{0,1\}$에 따라 선택된 암호문 C_b를 돌려받았을 때, b의 값을 맞히는

game이다. 이 때 공격자는 주어진 C_b를 복호화 오라클에 직접 질의하는 것 이외에 서명 암호화/복호화 오라클에 자유롭게 접근할 수 있다. 어떤 공격자에 대해서도 game에서 승리할 확률이 1/2와 무시할 수 있는 차이만을 가질 때, 해당 암호체계는 IND-CCA2를 만족하는 것으로 정의한다.

인증/무결성 요구조건을 위하여, 메시지 선택 공격에 대한 강한 위조 불가능성(sUF-CMA)을 전자 서명에서와 유사한 방법으로 정의할 수 있다. 어떠한 확률적 다항 시간 공격자도 무시할 수 없는 확률로 서명 암호화 오라클에서 응답한 결과 외에 복호화 과정을 통과할 수 있는 메시지($Unsigncrypt(C, ...) \neq \perp$)를 위조할 수 있어서는 안 된다. Dent는 무결성을 강조하여 이러한 안전성 모델에 대해 "INT-CCA"라고 지칭한다[Den05a].

비적응적으로 정의된 IND-CCA1과 존재적 위조 불가능성(eUF-CMA) 등 이보다 약한 안전성 모델도 유사하게 정의될 수 있다.

외부자/내부자 공격 안전성 ([Den05a][Den05b]). Dent의 정의에 따라, 외부 공격자와 내부 공격자는 주어진 정보가 다른 두 가지 종류의 공격자를 가리킨다. 외부 공격자는 송수신자 쌍방의 공개키를 이용하여 공격을 진행한다. 내부 공격자는 그 중 한 쪽의 비밀키를 추가로 이용할 수 있는데, sUF-CMA 안전성의 경우 수신자의 비밀키, IND-CCA2 안전성의 경우 송신자의 비밀키가 주어진다.

다자간 안전성 ([BSZ07]). 다자간 상황에서는 서명 암호화/복호화 오라클의 정의가 송신자나 수신자를 선택할 수 있도록 확장되어야 한다. Baek 등은 이러한 확장을 "유연한" 서명 암호화/복호화 오라클(FSO/FUO)이라 지칭한다[BSZ07].

다자간 상황의 여러 요소는 위에서 정의한 안전성 모델에 부합하지 않을 수 있다. 이에 따라 Baek 등은 안전성 모델과 공격자 모델의 네 가지 조합 모두에 대해 안전성을 엄밀하게 재정의하였다[BSZ07].

2.1.3 하이브리드 서명 암호화 ([Den05a][Den05b])

Cramer와 Shoup [CS03]는 KEM과 DEM, 두 개의 알고리즘으로 구성된 하이브리드 암호에 대해 최초로 논하였다. KEM은 키 은닉 메커니즘으로 공개키 암호 등을 통해 키를 안전하게 공유하는 데 초점이 맞추어져 있다. DEM은 데이터 은닉 메커니즘으로 KEM에서 공유한 키를 이용하여 (주로 대칭키 암호 등을 통해) 데이터를 안전하게 전송하는 방식에 대한 알고리즘이다. 서명 암호화는 키 은닉 방식에 기여할 수 있으므로, 서명 암호화 KEM (SKEM)의 개념을 자연스럽게 유도할 수 있다.

$SKEM = \{Setup, KeyGen_S, KeyGen_R, Encap, Decap\}$
$param \leftarrow Setup(1^k)$: 공개 인자 생성
$(sk_S, pk_S) \leftarrow KeyGen_S(param)$: 송신자의 키 생성
$(sk_R, pk_R) \leftarrow KeyGen_R(param)$: 수신자의 키 생성
$(K, C) \leftarrow Encap(pk_R, sk_S)$: 송신자의 공유되는 키 은닉
$K/\perp \leftarrow Decap(pk_S, sk_R, C)$: 수신자의 공유되는 키 복구

안전한 SKEM을 설계하기 위해서는 두 가지 비구별성 조건이 필요하다. 하나는 서명 암호화에서 정의되는 IND-CCA2 안전성이며, 다른 하나는 은닉한 키가 균일한 무작위 값(이상적인 키 은닉)과 구별되어서는 안 된다는 조건이다. 두 번째 조건을 엄밀하게 논하기 위해 left-or-right CCA (LoR-CCA) 안전성이 정의되어 있다.

2.2 인증 키 교환

키 교환은 참여자들이 동적인 커뮤니케이션을 통해 공통의 값을 유도해 내는 방식을 말한다. 그 과정에서 송신자와 수신자가 서로가 정당한 참여자임을 확인할 수 있도록 인증 효과를 부여하는 것이 인증 키 교환(Authenticated Key Exchange, AKE)이다. Bellare와 Rogaway는 [BR93]에서 커뮤니케이션 과정을 수학적으로 기술하여 "상호 인증"의 개념을 만들고, 그 과정에서 같은 값을 공유할 수 있도록 하여 인증 키 교환 방식으로 변형하였다.

2.2.1 인증 키 교환 방식의 종류

일반적인 키 교환과 달리, 인증 키 교환은 사전에 참여자 간 인증에 필요한 일부 정보가 공유되어야 한다. 어떠한 정보를 공유하는지에 대한 가정에 따라 인증 키 교환 방식의 모습도 달라질 수 있다.

비밀번호 기반 인간이 기억할 수 있을 정도의 짧은 비밀번호가 공유되었다고 가정한다. 비밀번호 기반 AKE는 공격자의 사전 공격을 막을 수 있어야 한다.

ID 기반 참여자들의 신분을 나타낼 수 있는 알려진 문자열을 공통의 정보로 사용한다.

PKI 기반 키 분배 센터에서 개인의 키를 분배받아서 사용할 수 있다. 서명 암호화에서 만든 키를 PKI와 유사한 방법으로 분배받아 사용하는 방식도 가능하다.

2.2.2 안전성 모델([CK01])

공격자 모델 Unauthenticated Links 공격자 모델에서는 공격자가 네트워크의 모든 요소를 수집/변조할 수 있으며 정의할 안전성 단계에 따라 상태 유출부터 키 유출 상황까지 폭넓은 행동이 허용된다. Authenticated Links 모델에서는 네트워크 상에서 이루어지는 통신에 대한 변조가 금지된다.

세션 키 보안 공격자는 세션 키를 무작위 값으로부터 구별할 수 없어야 한다. 이는 세션 키 k와 무작위 값 r가 $\{\mu_0, \mu_1\}$의 형태로 주어질 때, 어떤 다항 시간 공격자에 대해서도 $\mu_b = k$인 b의 값을 맞히는 확률이 $1/2$와 무시할 수 있는 차이만을 가진다면 해당 키 교환 방식은 세션 키 보안성을 갖는 것으로 정의한다.

Forward Secrecy 공격자는 참여자가 장기적으로 사용한 개인키를 유출하더라도, 이미 교환되고 만료된 세션 키의 정보를 알 수 없어야 한다.

2.3 격자 기반 암호

격자는 기저들의 정수 배 결합을 통해 생성되는 점들의 집합을 가리키는 수학적 구조이다.

정의 1. (격자)
행렬 $A \in \mathbb{Z}_q^{n \times m}$에 대해, 격자 $\Lambda_q(A) = \left\{A^T x : x \in \mathbb{Z}_q^m\right\}$는 A^T의 열에서 정의된 m개 기저로부터 발생하는 격자이다. 쌍대 격자로서의 격자 $\Lambda_q^{\perp}(A) = \{x : Ax \equiv 0 \ mod \ q\}$과 $\Lambda_q^u(A) = \{x : Ax \equiv u \ mod \ q\}$ 또한 정의될 수 있다.

2.3.1 격자 기반 문제

격자에서 정의된 다양한 문제가 양자 컴퓨터를 통한 공격에 안전할 것으로 추정되는 Shortest Independent Vector Problem(SIVP) 문제로 환원될 수 있음이 알려져 있다. 격자 기반 암호체계에는 Learning With Errors (LWE)와 Short Integer Solution (SIS) 문제가 자주 사용되고 있다.

정의 2. (LWE 분포)
행렬 $A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$, 균일하게 추출된 무작위 벡터 $x \xleftarrow{\$} \mathbb{Z}_q^m$, 이산 가우시안 분포에서 추출된 벡터 $e \in \mathbb{Z}_q^n \leftarrow D_{q,\alpha}$가 주어졌을 때, $(A, Ax + e)$의 분포는 LWE 분포이다.

정의 3. (Search-LWE 문제)
LWE 분포에서 추출된 표본 $(A, Ax + e)$에 대해, x의 값을 찾는 문제를 가리킨다.

정의 4. (Decision-LWE 문제)
값 (A, b)가 $A \in \mathbb{Z}_q^{n \times m}$, $b \in \mathbb{Z}_q^n$를 만족할 때, 이 값이 LWE 분포에서 추출된 표본인지 균일하게 추출된 무작위 값인지를 구별하는 문제이다.

정의 5. (SIS 문제)
행렬 $A \in \mathbb{Z}_q^{n \times m}$가 주어졌을 때, $||e|| < \beta$를 만족하는 격자점 $e \in \Lambda_q^{\perp}(A)$를 구하는 문제이다.

대수적인 기반을 변경한 격자 문제들도 활발하게 연구되고 있다. 일례로, 정수 계수 다항환 $\mathbb{Z}_q[x]/f(x)$과 같은 환에 대해 Ring-LWE 문제가 정의될 수 있으며, 간결함과 빠른 성능 등에 따라 그 활용도가 증가되고 있다.

2.3.2 격자 기반 Trapdoor

Trapdoor 함수는 trapdoor로 불리는 특정한 정보가 주어졌을 때에만 역방향 계산이 가능하며, trapdoor 없이는 해시 함수와 같이 일방향성 및 충돌 회피성을 가지는 함수를 가리킨다. 그 특성으로 인해, 다수의 격자 기반 서명 방식이 trapdoor를 활용하고 있다.

Preimage Sampleable Trapdoor ([GPV08]). Gentry 등은 격자 문제를 활용해 다음과 같은 trapdoor 함수를 설계하였다.

Trapdoor 함수 $f_A(v)$
Trapdoor 함수 $f_A(v)$는 함수 정보 행렬 A를 사용하여 trapdoor 없이 일방향성과 충돌 회피성을 갖도록 설계된 함수이다. 이러한 함수의 예 중 하나로 행렬 곱셈 $f_A(v) = Av$이 있으며, 특히 v가 오차 분포에서 추출된 경우 충돌 회피성은 SIS 문제의 난이도에 의해 유도될 수 있다.

$(A,T) \leftarrow \mathbf{TrapGen}(1^k)$
TrapGen은 $f_A(v)$의 사용을 위해 trapdoor 행렬 T와 함수 정보 행렬 A 의 쌍을 구하는 trapdoor 생성 함수이다.

$x \leftarrow \mathbf{SampleDom}(A,T)$
D를 벡터 x가 D에서 추출되었을 때 $f_A(x)$가 균일 분포하도록 하는 분포라고 한다면, SampleDom은 이러한 분포 D에서 벡터 x를 추출한다.

$x \leftarrow \mathbf{SamplePre}(A,T,y)$
f_A의 preimage y가 주어졌을 때, 위와 같이 정의된 분포 D에서 $f_A(x) = y$를 만족하는 벡터 x를 추출한다.

Gadget Trapdoor ([MP12]). Micciancio와 Peikert는 gadget trapdoor라 불리는 trapdoor의 일종을 제시하였으며, 격자 기반으로 이를 설계하였다.

$(A,R) \leftarrow \mathbf{GenTrap}^D(\overline{A},H)$
균일 추출된 $\overline{A} \in \mathbb{Z}_q^{n\times(m-w)}$와 태그 행렬 $H \in \mathbb{Z}_q^{n\times n}$를 이용하여, $\mathrm{GenTrap}^D$는 trapdoor 행렬 $R \leftarrow D$ 과 행렬 $A = [\overline{A}|HG - \overline{A}R] \in \mathbb{Z}_q^{n\times m}$를 생성한다. 이 과정에서 gadget이라 불리는 상수 행렬 $G \in \mathbb{Z}_q^{n\times w}$가 사용된다. Trapdoor R 없이 A는 균일 추출된 행렬과 구분될 수 없다.

$e \leftarrow \mathbf{SampleD}(R,A,u,s)$ SampleD는 trapdoor R을 활용하여 크기가 s에 따라 제한된 벡터 e를 격자 $\Lambda_A^{\mathbf{u}}$로부터 추출한다.

$(s,e) \leftarrow \mathbf{Invert}(R,A,b)$ 결정적 다항 시간 알고리즘 Invert는 trapdoor R을 이용하여 Search-LWE 문제 $b = A^T s + e$ 의 답을 구한다.

제 3 장 서명 암호화와 인증 키 교환 방식의 비교

3.1 두 방식의 연관성

원래 서명 암호화와 인증 키 교환은 그 의도하고자 하는 바가 다른 별개의 개념이다. 예를 들어, 인증(Authentication)은 수신자가 송신자의 메시지가 유효한 것으로 납득하기 위한 중요한 암호학적 조건 중 하나이다. 인증은 그 객체에 따라 메시지 인증(Message Authentication)과 개체 인증(Entity Authentication)으로 나뉜다. 메시지 인증은 메시지의 무결성과 직결되는 특성이 있으며, 개체 인증은 메시지의 송신자 또는 수신자가 정확한지에 관한 요소로 중간자 공격 방지와 직접적인 관련이 있다. 서명 암호화는 메시지 인증에, 인증 키 교환은 개체 인증에 그 의도가 맞추어져 있다.

표 3.1: 암호 체계별 안전성 범위

암호 체계	기밀성	무결성	인증		부인 방지
			메시지 인증	개체 인증	
전자 서명(DS)	X	O	O	서명자†	O
공개키 암호화(PKE)	O	X	X	X	X
서명 암호화(Signcryption)	O	O	O	△†	X
키 교환(KE)	△‡	X	X	X	X
인증 키 교환(AKE)	△‡	△†	△†	O	X

† 부수적 효과, ‡ 통신 정보로부터 교환된 키 유추 불가

흥미로운 점은, 부수적인 효과들을 고려했을 때 표 3.1과 같이 서명 암호화와 인증 키 교환이 의도하지 않은 상당한 유사성을 보인다는 것이다. 예를 들어, 둘 모두는 전달되는 메시지 또는 키에 대한 기밀성을 갖추고 있다. 서명 암호화는 외부인의 암호문 구별을 방지하기 위해 부인 방지 기능을 포기하는데, 부인 방지의 경우 인증 키 교환의 요구사항이 아니다. 서명 암호화는 암호화와 복호화 과정에서 상대방의 공개키를 사용하므로 적어도 해당 키에 대응하는 비밀키를 가진 쪽과 통신을 했음을 간접적으로 인증할 수 있다.

따라서 서명 암호화(및 이를 통해 유도된 SKEM)와 인증 키 교환의 상호 관계 및 유사성에 관한 선행 연구를 조사하고, 격자 기반 암호 체계에서 키를 공유하는 데 격자 기반 서명 암호화의 적용 가능성에 대해 논할 필요성이 있다.

3.2 일방향 키 교환과 SKEM ([GBN07])

서명 암호화와 키 교환의 상호 관계에 대하여 Gorantla 등은 주목할 만한 논증을 이끌어 내었다. 특히, Gorantla 등의 주요 연구 기여 중 하나는 SKEM이 일방향 키 교환 방식으로, 혹은 그 반대로 사용될 수 있는 조건을 엄밀하게 제시한 것이다[GBN07]. 그림 3.1은 SKEM과 키 교환의 대응과 그 조건에 대한 도식이다.

키 교환의 안전성은 Canetti-Krawczyk(CK) 모델에서 정의된 바 있다[CK01]. 그 중 Forward Secrecy는 키 생성을 위해 장기적으로 사용되는 키가 유출되더라도 공격자가 이전에 공유된 키를 복구할 수 없다는 성질을 의미한다. Krawczyk은 Diffie-Hellman 방식의 키 교환이 Forward Secrecy를 만족하기 위해 적어도 3회 이상의 통신이 필요함을 언급하고 있다[Kra05]. 이에 따라 Gorantla 등은 일방향 키 교환에 사용할 수 있는 완화된 Forward Secrecy로서 Sender Forward Secrecy를 제안하고 있다[GBN07].

인증 키 교환은 일반적인 키 교환과 다르게 사전에 약간의 값 공유가 필요하므로, 그에 대한 적절한 가정이 필요하다. 간단한 가정 중 하나는 서로가 유효한 서명 암호화 공개키를 직접 또는 키 분배 센터를 통

그림 3.1: 일방향 AKE와 SKEM의 대응 관계

일방향 키 교환		**서명 암호화 KEM**
송수신자 양측은 AKE 수행을 준비한다.		$Setup, KeyGen_S, KeyGen_R$
송신자는 공유 키 재료 C를 생성한다.		$(K, C) \leftarrow Encap(pk_R, sk_S)$
송신자는 C로부터 공유 키 K를 도출한다.		
송신자는 C를 수신자에게 전송한다.	$\Leftrightarrow$	송신자는 C를 수신자에게 전송한다.
수신자는 C로부터 공유 키 K를 도출한다.		$K \leftarrow Decap(pk_S, sk_R, C)$
요구사항		**요구사항**
- Sender Forward Secrecy 하에서의 세션 키 보안		- 내부자 공격 하에서의 기밀성
		- 외부자 공격 하에서의 위조 불가능성

하여 사전에 공유했다고 가정하는 것이다. 이 경우 공유된 정보는 모두 공개된 정보이고 공개키의 신뢰성에 대한 공격이 일어날 수 없다는 점에서 서명 암호화의 특성을 직접적으로 활용할 수 있다.

제 4 장 격자 기반 서명 암호화 방식

4.1 랜덤 오라클 모델 기반 방식

Wang 등이 제안한 서명 후 암호화 형태의 서명 암호화 방식은 격자 기반 GPV 서명 방식[GPV08]을 이용한다[WHW12]. Wang 등은 서명 결과를 암호화하기 위해 trapdoor가 적용된 LWE 문제를 포함한 다항 개수의 LWE 문제의 error vector에 서명 결과를 숨긴다.

Li 등의 방식은 더욱 간단한 방식의 서명 후 암호화 방식으로, Wang 등의 방식과 다르게 GPV 서명의 결과를 단일 LWE 문제에 숨긴다[LMKT13]. Trapdoor를 가지고 있는 수신자만이 LWE 문제를 풀어 메시지와 서명을 얻어낼 수 있다.

두 방식은 모두 IND-CCA2와 sUF-CMA 안전성을 논증하고 있다. 내부적으로 해시 함수를 사용하는 GPV 서명의 안전성은 랜덤 오라클 모델에서 유도되어 있으므로, 두 서명 암호화 방식의 안전성도 랜덤 오라클 모델에 기반하게 된다.

4.2 표준 모델 기반 방식

Yan 등의 방식은 표준 모델에서 안전성을 증명한 초기 격자 기반 서명 암호화 방식 중 하나이다[YWW+13]. 이 방식은 임의의 대칭 키 암호를 사용하고 있으며, gadget trapdoor 함수(SampleD)를 사용하여 sUF-CMA 안전성을 유도하였다. 반면, Lu 등의 방식은 preimage sampleable trapdoor 함수(SamplePre)를 사용하여 이보다 약한 eUF-CMA 안전성을 갖는다고 주장한다[LWJ+14].

한편, Yan 등이 주장한 sUF-CMA 안전성은 다자간 내부 공격자 상황에서 의문이 제기되고 있다. Sato와 Shikata는 MU-sUF-iCMA라 지칭한 이 위조 공격 가정에서 Yan 등이 제안한 방식의 안전성에 대해 부정적으로 언급하였으며, 다음 요약과 같이 동일한 gadget trapdoor를 활용한 서명 후 암호화 방식임에도 이를 만족하는 새로운 방식을 발표하였다[SS18].

$param \leftarrow \mathbf{Setup}(1^k)$
Setup은 서명 암호화를 위해 공유되어야 하는 여러 안전성 인자 및 변수를 설정한다.

$(pk_R, sk_R) \leftarrow \mathbf{KeyGen}_R(param)$
KeyGen_R은 $pk_R = A_R \leftarrow \text{GenTrap}^D(\overline{A}_R, O)$ (단, $\overline{A}_R \xleftarrow{\$} \mathbb{Z}_q^{n \times \overline{m}}$)를 통해 공개키를 생성하고, 그 trapdoor를 개인키로 한다. O의 역행렬이 존재하지 않으므로 이 키 생성 과정의 결과는 gadget trapdoor의 조건을 만족하지 않지만, 추후 O의 자리가 태그 행렬로 변경된 이후에는 제 기능을 다하게 된다.

$(pk_S, sk_S) \leftarrow \mathbf{KeyGen}_S(param)$
KeyGen_S는 $pk_S = A_S \leftarrow \text{GenTrap}^D(\overline{A}_S, I)$ from $\overline{A}_S \xleftarrow{\$} \mathbb{Z}_q^{n \times \overline{m}}$를 통해 공개키를 생성하고, 그 trapdoor를 개인키로 한다.

$C \leftarrow \mathbf{Signcrypt}(\mu, pk_R, sk_S, pk_S)$
오차 벡터 r_e를 이용해 생성된 정사각행렬 $H(t)$은 수신자 공개키 A_R에 해당 암호에 한한 태그 행렬로서 추가되어 $A_{R,t}$를 형성할 수 있다. 오차 벡터 r_e는 이후에 암호문의 일부가 되므로, 양측과 암호문을 본 공격자를 포함한 모두가 $A_{R,t}$를 계산할 수 있다.
송신자는 두 값 $\overline{c_0} \leftarrow s^T A_{R,t} + px_0^T, \overline{c_1} \leftarrow s^T U + px_1^T$을 준비한다. SampleD($sk_S$, ...)를 활용하여, 송신자는 두 값과 수신자의 공개키, 전송할 메시지에 대한 서명을 생성한다. 암호화 과정은 서명된 값과 변형된 메시지 $\lfloor \mu/2 \rfloor$를 $\overline{c_0}, \overline{c_1}$에 통계적으로 은닉하여 c_0, c_1를 생성하는 과정이다.

$m \leftarrow \mathbf{Unsigncrypt}(C, pk_S, sk_R, pk_R)$
$A_{R,t}$의 trapdoor를 보유하고 있는 수신자는 c_0, c_1과 관련된 모든 값들을 복구할 수 있다. Invert(sk_R, ...)의 사용을 통해 $A_{R,t}E = U$를 만족하는 E를 얻을 수 있으며, $\overline{c_0}, \overline{c_1}$에서 나타나는 오차값이 아닌 값 $s^T A_{R,t}, s^T U$를 소거할 수 있도록 한다. 결과적으로 $\lfloor \mu/2 \rfloor$를 통해 메시지를 복구할 수 있게 되며, 서명 또한 검증할 수 있게 된다.

4.3 AKE와 연관된 암호화 방식

일방향 AKE로부터의 서명 암호화 유도 Zhang 등의 Ring-LWE 기반 인증 키 교환 방식은 양방향 및 일방향으로 설계되었는데, 그 중 일방향 방식을 서명 암호화로 변환할 수 있는 가능성을 제시했다[ZZD+15]. 저자들은 해당 방식에 "평문 선택 공격에 안전한 대칭 키 암호와 MAC 생성 알고리즘을 표준 방식으로 결합함으로써"[ZZD+15] 서명 암호화 방식을 만들 수 있다고 주장한다. 논문은 이를 "deniable encryption"로 지칭하고 자세히 설명하지 않고 있지만, Gong과 Zhao는 이후에 논문의 주장이 서명 암호화와 동등한 것임을 확인하면서 그에 대한 공격까지 동시에 제시하였다[GZ16].

서명 암호화를 사용한 AKE 일반적인 SKEM과 일방향 인증 키 교환 방식의 관계가 알려졌음에도 불구하고, 격자 기반 서명 암호화 방식을 이용하여 AKE를 설계한 사례는 찾아보기 힘들다. 다만 Gupta와 Biswas는 서명 암호화에 기반하여 양방향 AKE를 설계하였는데, 이는 양측이 키 생성 재료를 서로에게 전달하는 과정을 서명 암호화를 통해 암호화한 것이다[GB18]. 이 방식은 SKEM의 범주에는 포함되지 않는다.

4.4 다자간으로의 확장

최초 요청자 L이 n-1명의 다른 인원 $p_j (0 < j < n)$과 키를 공유하려는 경우를 생각하자. 다자간으로 확장된 SKEM 방식은 다음과 같은 형태를 갖추어야 한다.

$MPSKEM = \{Setup, KeyGen_L, KeyGen, MultiEncap, Decap\}$
$param \leftarrow Setup(1^k)$: 키 교환을 위한 인자 생성
$(sk_L, pk_L) \leftarrow KeyGen_L(param)$: 최초 요청자의 키 생성
$(sk, pk) \leftarrow KeyGen(param)$: 다른 참여자의 키 생성
$(K, \{C_j\}^*) \leftarrow MultiEncap(\{pk_j\}^*, sk_L)$: 최초 요청자의 공유할 키 은닉
$K/\perp \leftarrow Decap(pk_L, sk_j, C_j)$: 다른 참여자의 키 복구

이를 기초로 한 프로토콜을 제작하기 위해서는, 동적 프로토콜을 위한 요소(참여, 이탈, 병합, 상하 구조 등)와 관리 규칙(상호 확인, 참여 거절 등) 등을 고려해야 한다. 이러한 키 교환 이후의 관리 상황까지 고려했을 때 최초 요청자 L을 n명의 인원을 대표하는 것으로 가정하는 방법이 있다. 서명 암호화가 메시지에 대한 인증을 내재적으로 제공하므로, 프로토콜의 수행 결과는 다자간 인증 키 교환의 결과와 동일할 것으로 보인다.

다자 수신 서명 암호화 다자 수신 서명 암호화는 수신자 여러 명이 동일한 암호문을 이용하여 평문을 복호화할 수 있는 서명 암호화의 변형이다. Lu 등은 격자의 기저를 대리하는 공통의 기저를 만드는 방법을 통해 격자 기반 다자 수신 서명 암호화 기법을 제시했다[LWJW13]. Zhang 등은 ID 기반 다자 수신 서명 암호화를 설계하면서, LWE/SIS 문제 기반으로 각각 IND-CCA2/eUF-CMA 안전성을 갖도록 구성하였다[ZXX18].

다자간의 키 교환에 사용되는 경우, 다자 수신 서명 암호화 방식은 암호문을 한 번만 네트워크 전체에 방송하면 되므로 더욱 간략한 통신을 기대할 수 있다.

제 5 장 맺음말

본 논문은 격자 기반의 서명 암호화와 그에 연관된 인증 키 교환을 일반적 이론과 함께 조사하였다. Gorantla 등에 의해 서명 암호화와 일방향 인증 키 교환의 일반적인 관계가 알려짐에 따라[GBN07], 서명 암호화와 SKEM을 통해 AKE와 그에 연관된 프로토콜을 설계하는 것이 가능해졌다. 특히, 다자간 인증 키 교환 방식를 설계하는 과정에서 다양한 서명 암호화의 변형을 사용하면 더욱 단순하지만 효율적인 다자간 방식을 얻을 수 있을 것으로 보인다. 다만 서명 암호화 기반 AKE 설계의 근본적이면서도 가장 큰 한계는 키 교환에서 요구하는 강한 단계의 보안인 Perfect Forward Secrecy를 만족하지 못하고 Sender Forward Secrecy에 머무를 수 밖에 없다는 것이다.

추가 연구. 서명 암호화와 일방향 인증 키 교환의 일반적인 관계는 양자 공격자 모델에서 추가로 검토되어야 할 필요가 있다. 대부분의 서명 암호화가 단순 LWE와 SIS 문제에 기초한 trapdoor 함수에 바탕을 두고 있으므로, Ring-LWE와 같은 더욱 효율적인 변형 문제를 사용한 서명 암호화 방식을 설계할 필요가 있다. 후행 연구에서 다양한 격자 기반 서명 암호화를 AKE로 변형한 사례를 활발하게 제시할 수 있을 것으로 보인다.

참 고 문 헌

[BR93] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In *Annual international cryptology conference*, pages 232–249. Springer, 1993.

[BSZ07] Joonsang Baek, Ron Steinfeld, and Yuliang Zheng. Formal proofs for the security of signcryption. *Journal of cryptology*, 20(2):203–235, 2007.

[CK01] Ran Canetti and Hugo Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 453–474. Springer, 2001.

[CS03] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003.

[Den05a] Alexander W Dent. Hybrid signcryption schemes with insider security. In *Australasian Conference on Information Security and Privacy*, pages 253–266. Springer, 2005.

[Den05b] Alexander W Dent. Hybrid signcryption schemes with outsider security. In *International Conference on Information Security*, pages 203–217. Springer, 2005.

[DZ10] Alexander W Dent and Yuliang Zheng. *Practical signcryption*. Springer Science & Business Media, 2010.

[GB18] Daya Sagar Gupta and GP Biswas. A novel and efficient lattice-based authenticated key exchange protocol in C-K model. *International Journal of Communication Systems*, 31(3):e3473, 2018.

[GBN07] M Choudary Gorantla, Colin Boyd, and Juan Manuel González Nieto. On the connection between signcryption and one-pass key establishment. In *IMA International Conference on Cryptography and Coding*, pages 277–301. Springer, 2007.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.

[GZ16] Boru Gong and Yunlei Zhao. Small field attack, and revisiting RLWE-based authenticated key exchange from Eurocrypt'15. *IACR Cryptology ePrint Archive*, 2016:913, 2016.

[Kra05] Hugo Krawczyk. Hmqv: A high-performance secure Diffie-Hellman protocol. In *Annual International Cryptology Conference*, pages 546–566. Springer, 2005.

[LMKT13] Fagen Li, Fahad T Muhaya, Muhammad Khurram Khan, and Tsuyoshi Takagi. Lattice-based signcryption. *Concurrency and Computation: Practice and Experience*, 25(14):2112–2122, 2013.

[LWJ+14] Xiuhua Lu, Qiaoyan Wen, Zhengping Jin, Licheng Wang, and Chunli Yang. A lattice-based signcryption scheme without random oracles. *Frontiers of Computer Science*, 8(4):667–675, 2014.

[LWJW13] Xiuhua Lu, Qiaoyan Wen, Zhengping Jin, and Licheng Wang. A lattice-based multi-receiver signcryption scheme for point to multi-point communication. 2013.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 700–718. Springer, 2012.

[SS18] Shingo Sato and Junji Shikata. Lattice-based signcryption without random oracles. In *International Conference on Post-Quantum Cryptography*, pages 331–351. Springer, 2018.

[WHW12] Fenghe Wang, Yupu Hu, and Chunxiao Wang. Post-quantum secure hybrid signcryption from lattice assumption. *Applied Mathematics & Information Sciences*, 6(1):23–28, 2012.

[YWW+13] Jianhua Yan, Licheng Wang, Lihua Wang, Yixian Yang, and Wenbin Yao. Efficient lattice-based signcryption in standard model. *Mathematical Problems in Engineering*, 2013, 2013.

[Zhe97] Yuliang Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature)+ cost (encryption). In *Annual International Cryptology Conference*, pages 165–179. Springer, 1997.

[ZXX18] Xiaojun Zhang, Chunxiang Xu, and Jingting Xue. Efficient multi-receiver identity-based signcryption from lattice assumption. *International Journal of Electronic Security and Digital Forensics*, 10(1):20–38, 2018.

[ZZD+15] Jiang Zhang, Zhenfeng Zhang, Jintai Ding, Michael Snook, and Özgür Dagdelen. Authenticated key exchange from ideal lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 719–751. Springer, 2015.