논문 2009-46CI-1-8

# DNF 정책을 가지는 속성 기반 서명

## ( Attribute-Based Signatures with DNF Policies )

이 광 수*, 황 정 연**, 김 형 중***, 이 동 훈**

( Kwangsu Lee, Jung Yeon Hwang, Hyoung-Joong Kim, and Dong Hoon Lee )

요 약

속성 기반 서명(Attribute-Based Signature) 기법이란 서명자의 비밀키에 속성 집합(Attribute Set)이 연관되고 서명에 접근 구조(Access Structure)가 연관되는 서명 기법이다. 속성 기반 서명 기법은 객체의 식별자가 속성 집합으로 표현되는 속성 기반 시스템(Attribute-Based System) 또는 권한 기반 시스템(Role-Based System)에서 서명자의 익명성과 접근 제어를 가능하게 하는 유용한 서명 기법이다. 본 논문에서는 속성 기반 서명 기법을 정의하고 서명에 포함되는 정책을 DNF(Disjunctive Normal Form) 수식으로 표현이 가능한 효율적인 속성 기반 서명 기법을 제시한다. 제시한 기법은 서명 검증시 상수번의 페어링 연산만이 필요한 최초의 안전한 기법이다. 그리고 증명이 가능한 속성 기반 서명 기법을 구성하기 위해서 새로운 interactive 가정을 소개하고 제안된 기법이 랜덤 오라클과 새로운 가정에서 안전함을 보인다.

Abstract

An attribute-based signature scheme is a signature scheme where a signer's private key is associate with an attribute set and a signature is associated with an access structure. Attribute-based signature schemes are useful to provide anonymity and access control for role-based systems and attribute-based systems where an identity of object is represented as a set of roles or attributes. In this paper, we formally define the definition of attribute-based signature schemes and propose the first efficient attribute-based signature scheme that requires constant number of pairing operations for verification where a policy is represented as a disjunctive normal form (DNF). To construct provably secure one, we introduce a new interactive assumption and prove that our construction is secure under the new interactive assumption and the random oracle model.

**Keywords**: attribute-based signature, disjunctive normal form, signer anonymity

## I. 서 론

전자 서명은 현대 암호학에서 가장 근본적이고 유용한 요소 중의 하나이다. 최초의 공개키 기반 암호시스템[10]이 소개된 이후로, 다양한 전자 서명 기법이 다양한 어플리케이션의 요구사항을 만족하기 위해서 제안되었다. 대표적 예는 전자 서명에 접근 구조를 결합하는 것으로 기존의 전통적인 전자 서명 기법은 단순히 서명이 서명자에 의해서 생성된 것임을 보장하지만 접근 구조가 포함된 서명은 추가로 서명자 익명서과 접근 제어 기능 등을 제공하는 것이 가능하다. 접근 구조와 결합된 전자 서명 기법은 서명자에 대한 정보를 접근 구조를 이용하여 유연하게 표현하는 것이 가능하여 멀티-서명, 링-서명, 메쉬-서명 등과 다양한 기법에 적용되었다[3, 6~7, 9, 11, 18, 21]. 하지만 컴퓨터 시스템과 네트워크의 발전으로 서명에 참여할 수 있는 객체의 수가 늘어남에 따라서 객체를 표현하는 인증서 또는 식별자만을 이용해서 접근 제어를 수행하는 경우 접근 구조의 크기 역시 늘어나서 효율적인 접근 제어가 점점 어려워지고 있다.

* 학생회원, ** 정회원, *** 평생회원,
고려대학교 정보경영공학전문대학원
(Korea University, Graduate School of Information Management and Security)

※ "이 연구에 참여한 연구자(의 일부)는 '2단계 BK21 사업'의 지원비를 받았음"
접수일자: 2008년12월10일, 수정완료일: 2009년1월12일

이와 같이 그 수가 빠르게 늘어나고 있는 객체에 대한 효율적인 접근 제어를 수행하기 위한 방법 중의 하나는 권한 기반 시스템 또는 속성 기반 시스템과 같이 객체를 다수의 권한 또는 속성들의 집합으로 표현하는 것이다[20, 23]. 권한 또는 속성 기반 시스템에서의 접근 제어는 개별 객체의 유일한 식별자 대신 객체의 권한 또는 속성들로 구성된 접근 구조를 이용해서 접근 구조 크기를 효율적으로 유지하면서도 충분히 효과적인 접근 제어가 가능하다. 본 논문에서는 권한 또는 속성 기반 시스템에 적합한 속성 기반 서명 기법을 정의하고 서명 검증시 상수번의 페어링 연산만 필요한 최초의 효율적인 속성 기반 서명 기법을 제안한다.

속성 기반 서명 기법은 권한 또는 속성 기반 시스템에 적합한 전자 서명 기법으로 기존의 속성 기반 암호(Attribute-Based Encryption) 기법[4, 12, 19]을 서명 기법으로 개념을 확장한 것 또는 아이디 기반 서명(Identity-Based Signature) 기법[8, 22]을 속성 집합으로 구성된 아이디로 확장한 것으로 볼 수 있다. 이때 올바른 속성 기반 서명 기법은 속성 집합이 서명자의 비밀키에 위치하고 접근 구조가 서명에 위치하는 속성-정책 속성 기반 서명 기법이다. 본 논문에서는 서명에 포함되는 정책을 DNF 수식으로 표현가능한 속성 기반 서명 기법을 다룬다.

속성 기반 서명 기법의 대표적인 응용은 권한 및 속성 기반 시스템에서 권한 및 속성을 이용한 서명 기법이다. 이것은 개별 객체의 식별자가 속성 집합으로 이루어지면 키생성 기관이 객체의 속성 집합에 대한 비밀키를 생성하여 객체에게 전달하고 개별 객체는 속성 집합에 대한 비밀키를 이용하여 속성에 대한 서명을 수행하는 것이 가능하다. 따라서 속성 기반 서명 기법을 이용하여 권한 및 속성 기반 시스템에서 속성별 서명이 가능하다. 또 다른 응용은 속성 기반 메시징 시스템에서 서명이다. 현재 널리 사용되고 있는 이메일은 메일링 리스트를 이용해서 다수의 사용자들에게 메시지를 전달한다. 하지만 메일링 리스트 기반 메시징 시스템은 메일링 리스트에 포함된 모든 사용자들에게 동일한 메시지를 전달하기 때문에 사용자 특성 및 취향에 따른 선별적 메시지 전달이 불가능하다. 속성 기반 메시징(Attribute-Based Messaging) 시스템은 이와 같은 문제점을 극복하기 위해서 사용자의 속성들을 저장하고 있는 리스트를 이용해서 송신자가 메시지 수신자에 대한 속성을 지정하는 경우 해당 속성을 만족하는 수신자들에게만 메시지가 전달되는 시스템이다[5]. 이런 속성 기반 메시징 시스템에서 일부 중요한 메시지의 경우 메시지의 송신자가 특정한 속성을 가지고 있음을 보장할 필요가 있다. 이 경우 속성 기반 서명을 이용하여 송신자가 특정 속성을 가지고 있음을 암호학적으로 보장하는 것이 가능하다.

본 논문에서는 먼저 권한 또는 속성 기반 시스템에 적합한 속성 기반 서명 기법을 정의하고 안전성 모델을 제시했다. 속성 기반 서명 기법은 위조 불가능성과 익명성, 그리고 기존 공개키 서명 기법과는 달리 공모 안전성(Collusion-Resistance)을 제공해야 한다. 위조 불가능성 모델은 기존 공개키 서명의 위조 불가능성 성질과 유사하지만 공모 안전성 제공하기 위해서 공격자가 개별 속성 집합에 대한 비밀키 생성 질의를 요청할 수 있도록 정의했다. 익명성 모델은 모든 비밀키가 노출되는 경우에도 익명성이 유지되도록 정의했다. 그런 다음 서명 검증시 상수번의 페어링 연산만을 요구하는 효율적인 속성 기반 서명 기법을 설계했다. 이를 가능하게 하기 위해서 본 논문에서는 접근 구조를 논리합과 논리곱으로 이루어진 DNF(Disjuctive Normal Form) 수식으로 변환하여 속성 기반 서명을 설계했다. 증명이 가능한 속성 기반 서명을 구성하기 위해서 본 논문에서는 사용자별 난수를 통한 비밀키 묶음 기법과, 새로운 interactive 가정의 고안을 통해서 속성 기반 서명 기법 설계의 어려운 문제점들을 해결했다.

권한 및 속성 기반 시스템에 적용이 가능한 암호 기법에 대한 연구는 속성 기반 암호(Attribute-Based Encryption) 기법으로 Sahai와 Waters에 의하여 처음 소개되었다[19]. 이후 Goyal 등은 일반적인 접근 권한 구조를 지원하는 키-정책 속성 기반 암호(Key-Policy Attribute-Based Encryption) 기법을 제안하였다[12]. 그리고 Bethencourt 등은 기존의 암호문에 접근 권한 구조를 지정하는 것이 가능한 암호문-정책 속성 기반 암호(Ciphertext-Policy Attribute-Based Encryption) 기법을 제안하였다[4]. 최근에는 접근 구조에 NOT 연산을 지원하도록 확장하거나 또는 속성 기반 암호 기법에 기반 키교환 기법이 연구되고 있다[1, 16].

암호 기법과 달리 속성 기반 시스템에 적용이 가능한 서명 기법에 대한 연구는 아직 미진하며 최근에서야 몇 가지 연구결과가 발표되었다. 먼저 Khader는 기존 그룹 서명과 유사하게 서명자의 아이디는 숨기고 서명 생성에 참여한 속성 정보는 노출하는 속성 기반

그룹 서명 기법을 제안했다[13]. 하지만 Khader가 제안한 서명 모델은 일반적인 서명 모델과 많이 다르기 때문에 올바른 속성 기반 서명으로 볼 수가 없다. Maji 등은 속성 기반 서명 기법을 정의하고 generic 그룹 모델에서 안전한 기법을 제안했다[15]. 하지만 이 기법은 서명 검증시 페어링 연산 횟수가 접근 구조 크기에 선형적으로 증가하는 문제점이 있기 때문에 실용적으로 사용되기에는 어려움이 있다. 최근 Li와 Kim은 속성 기반 링 서명 기법을 제안했다[14]. 이 기법 역시 서명 검증시 페어링 연산 횟수가 접근 구조 크기에 선형적으로 증가하는 문제점을 가지고 있다.

## Ⅱ. 속성 기반 서명 정의

이 절에서는 속성 기반 서명 기법을 정의하고 속성 기반 서명 기법이 만족해야 하는 안전성 모델을 정의한다.

### 1. 접근 구조

접근 구조(Access Structure)[2]는 다음과 같이 정의된다. 먼저 $\{P_1, P_2, \cdots, P_n\}$를 개체들의 집합이라고 하자. 이때 모임 $A \subseteq 2^{P_1, P_2, \cdots, P_n}$에서 모든 집합 $B, C$에 대하여 만일 $B \in A$이고 $B \subseteq C$이면 $C \in A$ 만족하는 경우 모임 $A$를 단조라고 한다. 접근 구조 (또는 단조 접근 구조)는 $\{P_1, P_2, \cdots, P_n\}$ 집합의 공집합이 아닌 부분 집합의 모임으로 정의된다. 즉, $A \subseteq 2^{\{P_1, P_2, \cdots, P_n\}} \setminus \{\varnothing\}$. $A$ 모임의 원소 집합을 권한 집합이라 하고, $A$ 모임의 원소 집합이 아닌 집합을 비권한 집합이라고 정의한다.

### 2. 속성 기반 서명 정의

속성 기반 서명 기법은 접근 구조가 서명에 위치하는 서명-정책 속성 기반 서명(Signature-Policy Attribute-Based Signature)이 올바른 속성 기반 서명이다. 속성 기반 서명 기법은 다음과 같은 알고리즘으로 정의된다.

- $Setup(1^k)$: 설정 알고리즘은 입력으로 보안 파라미터 $1^k$ 값을 받고, 공개 파라미터 $PP$ 값과 마스터 비밀키 $MK$ 값을 출력한다.

- $KeyGen(w, MK, PP)$: 비밀키 생성 알고리즘은 입력으로 속성 스트링 $a_i$ 값으로 이루어진 속성 집합 $w = \{a_1, \cdots, a_l\}$, 마스터 비밀키 $MK$, 그리고 공개 파라미터 $PP$ 값을 받고, 사용자의 비밀키 $SK_w$ 값을 출력한다.

- $Sign(M, AS, SK_w, PP)$: 서명 알고리즘은 입력으로 메시지 $M$, 접근 구조 $AS$, 사용자의 비밀키 $SK_w$, 그리고 공개 파라미터 $PP$ 값을 받고, 사용자의 속성 집합이 $w \in AS$ 조건을 만족하는 경우 서명 $\sigma$ 값을 출력한다.

- $Verify(\sigma, M, AS, PP)$: 검증 알고리즘은 입력으로 서명 $\sigma$, 메시지 $M$, 접근 구조 $AS$, 그리고 공개 파라미터 $PP$ 값을 받고, 서명의 올바름 여부에 따라서 "accept" 또는 "reject" 값을 출력한다.

### 3. 안전성 정의

속성 기반 서명 기법은 다음과 같은 위조 불가능성(Unforgeability) 게임, 그리고 익명성(Anonymity) 게임으로 정의된다.

위조 불가능성 (Unforgeability). 위조 불가능성은 챌린저 $C$ 와 공격자 $A$ 간의 다음과 같은 게임으로 정의된다.

Setup: 먼저 챌린저 $C$는 설정 알고리즘을 수행하여 마스터 비밀키 $MK$ 값은 자신이 보관하고 공개 파라미터 $PP$ 값을 공격자 $A$에게 전달한다.

Queries: 공격자는 다음과 같은 질의들을 챌린저에게 요청할 수 있다.

- 해쉬 질의: $A$는 속성 $a$에 대한 해쉬 값을 요청하고, $C$는 해쉬 값을 답변한다.

- 비밀키 생성 질의: $A$는 속성 집합 $w = \{a_1, \cdots, a_l\}$에 대한 비밀키 생성 질의 요청하고, $C$는 이에 해당하는 비밀키 $SK_w$ 생성하여 답변한다.

- 서명 질의: $A$는 메시지 $M$과 접근 구조 $AS$에 대한 서명을 요청하고, $C$는 이에 대한 서명 $\sigma$ 생성하여 답변한다.

Output: 마지막으로 공격자 $A$는 $(\sigma^*, M^*, AS^*)$ 값을 출력하고 다음의 조건이 만족되는 경우 게임에 승리한다. 조건은 (1) $A$는 접근 구조 $AS^*$에 속하는 속성 집합 $w$에 대한 비밀키 생성 질의를 요청하지 않아야 한다.; (2) $A$는 메시지 $M^*$과 접근 구조 $AS^*$에 대한 서명 질의 요청하지 않았어야 한다.; (3) 공격자가 출력한 서명에 대해서 $Verify(\sigma^*, M^*, AS^*, PP) = accept$

성립해야 한다.

사건 $Succ$는 공격자 $A$가 앞에서 정의된 게임을 이기는 사건으로 정의된다. 공격자 $A$의 이득은 $Adv_A^{ABS-UF} = \Pr[Succ]$ 값으로 정의된다.

익명성 (Anonymity). 익명성은 챌린저 $C$와 공격자 $A$ 간의 다음과 같은 게임으로 정의된다.

Setup: 먼저 챌린저 $C$는 설정 알고리즘을 수행하여 마스터 비밀키 $MK$ 값은 자신이 보관하고 공개 파라미터 $PP$ 값을 공격자 $A$에게 전달한다.

Queries: 공격자는 다음과 같은 질의들을 챌린저에게 요청할 수 있다.

- 해쉬 질의: $A$는 속성 $a$에 대한 해쉬 값을 요청하고, $C$는 해쉬 값을 답변한다.
- 비밀키 생성 질의: $A$는 속성 집합 $w = \{a_1, \cdots, a_l\}$에 대한 비밀키 생성 질의 요청하고, $C$는 이에 해당하는 비밀키 $SK_w$ 생성하여 답변한다.
- 서명 질의: $A$는 메시지 $M$과 접근 구조 $AS$에 대한 서명을 요청하고, $C$는 이에 대한 서명 $\sigma$ 생성하여 답변한다.

Challenge: 공격자 $A$는 $(M, AS, w_0, w_1)$ 값을 챌린저에게 제공한다. 이때 두 속성 집합 $w_0, w_1$는 $w_0 \neq w_1$이고 $w_0, w_1 \in AS$ 조건을 만족한다. 챌린저 $C$는 랜덤 값 $c \in \{0,1\}$ 선택하여 서명 값을 $\sigma \leftarrow Sign(M, AS, SK_{w_b}, PP)$와 같이 계산하고, 그 서명 $\sigma$ 값을 $A$에게 전달한다.

Output: 마지막으로 공격자 $A$는 랜덤 값 $c$에 대한 추측 값인 $c'$값을 출력하고 $c = c'$ 성립하는 경우 게임에 승리한다.

사건 $Succ$는 공격자 $A$가 앞에서 정의된 게임을 이기는 사건으로 정의된다. 공격자 $A$의 이득은 $Adv_A^{ABS-AN} = |\Pr[Succ] - 1/2|$ 값으로 정의된다.

## III. 배경지식 및 가정

이 절에서는 본 논문을 이해하기 위한 배경지식으로 bilinear 그룹, 그리고 제안된 서명 기법의 안전성에 대한 바탕이 되는 새로운 interactive 가정을 설명한다.

### 1. Bilinear 그룹

먼저 $G$, $G_T$는 소수 위수 $g$를 갖는 곱셈 순환군이다. 그리고 $g$는 $G$의 생성원이고, $e$는 bilinear 함수로 $e : G \times G \rightarrow G_T$로 정의되고 다음의 성질을 가지는 함수이다.

- Bilinearlity: 모든 $u, v \in G$와 $a, b \in Z_p^*$에 대해서 $e(u^a, v^b) = e(u,v)^{ab}$가 성립한다.
- Non-degeneracy: 모든 $u, v \in G$에 대해서 $e(u,v) \neq 1$이 성립한다.

만일 $G$에서의 그룹 연산과 bilinear 함수 $e$의 연산을 효율적으로 계산 가능한 경우 $G$를 bilinear 그룹이라고 한다. 그리고 $e(u^a, v^b) = e(u,v)^{ab} = e(u^b, v^a)$ 수식이 성립하기 때문에 $e$함수는 대칭성을 가지고 있다.

### 2. Interactive 가정

먼저 그룹 $G$는 소수 $g$를 윗수로 가진 곱셈 순환군이다. 이때 bilinear 그룹 $G$에서 interactive 가정은 다음과 같은 문제를 무시할 수 없는 확률 이득 이상으로 해결 가능한 확률적인 다항시간(Probabilistic Polynomial-Time) 알고리즘 $A$가 존재하지 않는 것이다. 알고리즘 $A$는 초기 입력으로 bilinear 그룹에 대한 정보와 해쉬 함수 정보가 포함된 $((p, G, G_T, e), g, g^s, H)$ 값이 주어지고, 외부의 오라클 $O_S(\cdot)$ 이용하여 속성 집합 $w_i = \{a_{i,1}, \cdots, a_{i,l}\}$ 값에 대한 답변 $(H(a_{i,1})^{s \cdot t_i}, \cdots, H(a_{i,l})^{s \cdot t_i}, g^{s \cdot t_i}, g^{t_i})$ 값을 얻을 수 있다. 최종적으로 알고리즘 $A$는 외부 오라클에 요청했던 모든 속성 집합 $w_i$ 대하여 $w^* \not\subseteq w_i$ 조건을 만족하는 $(w^* = a_1^*, \cdots, a_l^*, \prod_{i \in w^*} H(a_i^*)^{s \cdot t'}, g^{s \cdot t'}, g^{t'})$ 값을 출력한다. 이때 $A$의 확률 이득은 $Adv_G^{IA}(A)$ 값으로 표현되고, 공격자가 앞의 조건을 만족하는 결과를 출력한 확률로 정의된다.

## IV. 속성 기반 서명 기법

이 절에서는 효율적인 속성 기반 서명 기법을 제시하고, 제시한 기법의 안전성을 증명한다.

### 1. 설계 원리

속성 기반 서명 기법의 설계 아이디어는 서명에 포함되는 접근 구조를 DNF 수식으로 표현하는 것이다. 즉, 속성 집합을 속성들의 논리곱($\wedge$)으로 표현하고 속성 집합의 모임을 논리합($\vee$)으로 표현하는 DNF 수식

을 사용한다. 이와 같이 논리곱과 논리합으로 표현되는 DNF 수식을 이용하는 경우, 논리곱은 멀티 서명(Multi-Signature) 기법을 이용하여 구현할 수 있고 논리합은 링 서명(Ring Signature) 기법을 이용하여 구현할 수 있다. 하지만 단순한 아이디 기반 멀티 서명 기법과 아이디 기반 링 서명 기법을 확장은 공모 공격에 안전하지 않고 안전성 모델의 차이로 인해서 증명 역시 속성 기반 서명 기법에서 동작하지 않는다. 따라서 본 논문에서는 이들 두 가지 핵심적인 어려움을 해결하기 위해서 사용자별 난수를 이용하는 기법과 새로운 interactive 가정을 이용하여 속성 기반 서명 기법의 안전성을 증명한다.

## 2. DNF 수식

논리 연산자 $\psi$가 다수 논리곱의 논리합($\vee$)으로 표현되고, 논리곱($\wedge$)은 다시 다수의 리터럴로 이루어진 경우 논리 연산자는 논리합 정규형 (Disjunctive Normal Form)이라고 정의된다. 이때 리터럴은 기본 명제 또는 그의 부정으로 구성된다. 여기 DNF 수식 $\psi$는 논리 연산자에서 리터럴이 단지 속성 스트링으로만 이루어지는 논리합 정규형 논리 연산자로 정의한다. 즉, DNF 수식은 $\psi = \vee_{i=1}^{m} \wedge_{j=1}^{n_i} a_{i,j}$ 식으로 표현되고 이때 $a_{i,j}$ 값은 속성 스트링 값이다.

접근 구조 $AS$는 DNF 수식 $\psi$으로 표현이 가능하다. 즉, DNF 수식 $\psi$의 논리곱과 논리합은 각각 접근 구조 $AS$의 개체의 부분집합과 부분집합의 모임을 표현할 수 있다.

## 3. 기법 설명

$Setup(1^k)$: 설정 알고리즘은 먼저 소수 $p$를 윗수로 가지는 bilinear 그룹 $G$ 생성한다. 이때 소수 $p$는 랜덤 소수로 $k$ 비트 길이를 가진다. 알고리즘은 그룹 생성원 $g \in G$ 랜덤하게 선택하고, 랜덤 값 $s \in Z_p$ 선택한다. 마지막으로 알고리즘은 두 해쉬 함수 $H_1 : \{0,1\}^* \rightarrow G$와 $H_2 : \{0,1\}^* \rightarrow Z_p^*$를 선택한다. 이때 공개 파라미터 $PP$와 마스터 비밀키 $MK$는 다음과 같이 설정된다.

$$PP = ((p, G, G_T, e), g, g_1 = g^s, H_1, H_2), \quad MK = s.$$

$KeyGen(w, MK, PP)$: 마스터 비밀키 $MK$ 이용하여 속성 집합 $w = \{a_1, \cdots, a_l\}$에 대한 비밀키 생성하기 위해서 키 생성 알고리즘은 랜덤 값 $t_1 \in Z_p^*$ 선택한 후 다음과 같은 비밀키 생성한다.

$$SK_w = (H_1(a_1)^{s \cdot t_1}, \cdots, H_1(a_l)^{s \cdot t_1}, g_1^{t_1}, g^{t_1}).$$

$Sign(M, \psi, SK_w, PP)$: 서명 알고리즘은 입력으로 메시지 $M$, DNF 수식 $\psi = \vee_{i=1}^{m} \wedge_{j=1}^{n_i} a_{i,j}$, 그리고 비밀키 $SK_w$를 받는다. 이때 인덱스 $i^*$ 값은 모든 $j \in \{1, \cdots, n_{i^*}\}$에 대하여 $a_{i^*,j} \in w$ 조건이 성립하는 값이라고 정의하자. 서명 생성 과정은 다음과 같다.

1. 먼저 알고리즘은 난수 $t_2 \in Z_p^*$ 선택하여 비밀키에 대한 재-난수화 과정을 수행하여 $T_1 = g_1^t = g_1^{t_1 \cdot t_2}$ 값과 $T_2 = g^t = g^{t_1 \cdot t_2}$ 값을 계산한다. 이때 $t = t_1 \cdot t_2$ 라고 설정하자.
2. 알고리즘은 $i^*$ 제외한 모든 인덱스 $i \in \{1, \cdots, m\} \setminus \{i^*\}$에 대하여 난수 $R_i \in G$ 선택하고 $h_i = H_2(M, \psi, R_i, T_1, T_2)$값을 계산한다.
3. 인덱스 $i^*$의 경우, 먼저 난수 $r_{i^*} \in Z_p^*$ 선택하고 $Y_i = \prod_{j=1}^{n_i} H_1(a_{i,j})$라고 설정한 후 $R_{i^*} = (Y_{i^*}^{r_{i^*}}) / (\prod_{1 \le i \ne i^* \le m} (R_i \cdot Y_i^{h_i}))$ 값과 $h_{i^*} = H_2(M, \psi, R_{i^*}, T_1, T_2)$ 값을 계산한다.
4. 비밀키에 포함된 속성 집합 $w$는 DNF 수식 $\psi$ 만족하기 때문에 인덱스 $i^*$에 대한 비밀키 요소 $\{H_1(a_{i^*,j})^{s \cdot t_1}\}_{1 \le j \le n_{i^*}}$ 값들이 존재한다. 알고리즘은 이들 비밀키 요소들을 이용하여 $V = (\prod_{j=1}^{n_{i^*}} H_1(a_{i^*,j})^{s \cdot t_1})^{t_2 \cdot (r_{i^*} + h_{i^*})}$ 값을 계산한다.
5. 마지막으로 알고리즘은 다음의 값을 서명으로 출력한다.

$$\sigma = (V, R_1, \cdots, R_m, T_1, T_2) \in G^{m+3}.$$

$Verify(\sigma, M, \psi, PP)$: 검증 알고리즘은 입력으로 서명 $\sigma$, 메시지 $M$, 그리고 DNF 수식 $\psi = \vee_{i=1}^{m} \wedge_{j=1}^{n_i} a_{i,j}$ 값을 받는다. 알고리즘은 모든 $i$ 값에 대하여 $Y_i = \prod_{j=1}^{n_i} H_1(a_{i,j})$ 라고 설정하고, 해쉬 $h_i = H_2(M, \psi, R_i, T_1, T_2)$ 계산 후 다음의 두 수식이

성립하는지 체크한다.

$$e(g,V)=e(T_1,\prod_{i=1}^{m}(R_i\cdot Y_i^{h_i})) \quad \wedge$$
$$e(g,T_1)=e(T_2,g_1).$$

만일 위의 두 수식이 성립하는 경우 "accept" 출력하고, 그렇지 않은 경우 "reject" 출력한다.

## 4. 올바름

속성 기반 서명 기법의 올바름은 다음 식을 통해서 확인할 수 있다. 이때 난수는 $t=t_1\cdot t_2$라고 정의하자.

$$\begin{aligned}e(g,V)&=e(g,\prod_{j=1}^{n_{i^*}}H_1(a_{i^*,j})^{st(r_{i^*}+h_{i^*})})\\&=e(g^{st},Y_{i^*}^{r_{i^*}}\cdot Y_{i^*}^{h_{i^*}})\\&=e(g^{st},R_{i^*}\cdot\prod_{1\le i\ne i^*\le m}(R_i\cdot Y_i^{h_i})\cdot Y_{i^*}^{h_{i^*}})\\&=e(T_1,\prod_{i=1}^{m}(R_i\cdot Y_i^{h_i})),\end{aligned}$$

$$e(g,T_1)=e(g,g_1^t)=e(T_2,g_1).$$

## 5. 안전성 증명

*정리 1. 본 논문에서 기술된 속성 기반 서명 기법은 랜덤 오라클 모델과 interactive 가정 하에서 위조 불가능성을 제공한다.*

증명) 속성 기반 서명 기법의 위조 불가능성을 공격하는 공격자 $A$가 존재한다고 가정하자. 공격자 $A$를 이용해서 interactive 가정을 공격하는 알고리즘 $B$는 다음과 같이 기술된다. 먼저 $B$는 입력으로 bilinear 그룹 정보 $(p,G,G_T,e)$와 $(g,g^s)$ 값들이 주어지고 외부 오라클을 통해서 해쉬 함수 $H_1$ 계산과 $O_s$ 오라클 계산이 가능하다. 그리고 $B$는 공격자 $A$와 다음과 같은 방식으로 상호 작용한다.

Setup: 먼저 알고리즘 $B$는 공개 파라미터 $PP=((p,G,G_T,e),g,g_1=g^s)$ 설정하고 이 값을 $A$에게 전달한다.

Queries: 공격자 $A$의 질의에 대한 답변은 다음과 같이 수행한다.

- $H_1$ 해쉬 질의: $A$가 $H_1$ 해쉬 질의 요청하는 경우 $B$는 interactive 가정에서 주어지는 $H_1$ 해쉬 오라클 이용하여 답변한다.
- $H_2$ 해쉬 질의: $A$가 $(M,\psi,R,T_1,T_2)$ 입력에 대한 $H_2$ 해쉬 질의 요청하는 경우 $B$는 다음과 같이 답변한다. 만일 $(M,\psi,R,T_1,T_2)$ 값이 이전 $H_2-List$ 테이블에 존재하는 경우, $B$는 $(M,\psi,R,T_1,T_2,h)$ 값을 $H_2-List$ 테이블에서 $h$ 값을 복구하여 답변한다. 그렇지 않은 경우, $B$는 랜덤 $h\in Z_p^*$ 값을 선택하여 $(M,\psi,R,T_1,T_2,h)$ 값을 $H_2-List$ 테이블에 추가 후 $h$ 값을 답변한다.
- 비밀키 생성 질의: $A$가 속성 집합 $w=\{a_1,\cdots,a_l\}$에 대한 비밀키 생성 질의를 요청하는 경우 $B$는 외부에 주어진 오라클 $O_S$이용하여 $D=(H_1(a_1)^{s\cdot t},\cdots,H_1(a_l)^{s\cdot t},g_1^t,g^t)$ 값을 얻어온 후 이 값을 $A$에게 답변한다.
- 서명 질의: $A$가 메시지와 DNF 수식 $\psi=\vee_{i=1}^{m}\wedge_{j=1}^{n_i}a_{i,j}$로 이루어진 입력 $(M,\psi)$ 값에 대한 서명 질의를 요청하는 경우 $B$는 다음과 같이 답변한다.

1. 먼저 $B$는 $1\le i^*\le m$ 조건을 만족하는 임의의 인덱스 $i^*$ 값을 선택한다. 그리고 랜덤 $t\in Z_p^*$ 값을 선택하여 $T_1=g_1^t$, $T_2=g^t$ 값들을 계산한다.

2. $B$는 $1\le i\ne i^*\le m$ 조건을 만족하는 모든 인덱스 $i$에 대하여 랜덤 $R_i\in G$ 값을 선택하고 $h_i=H_2(M,\psi,R_i,T_1,T_2)$ 값을 계산한다. 만일 $(M,\psi,R_i,T_1,T_2,h_i)$ 값을 $H_2-List$ 테이블에 저장할 때 충돌이 발생하는 경우 $R_i$ 값을 다시 선택한 후 계산을 수행하여 충돌이 발생하지 않도록 설정한다.

3. $B$는 $i^*$ 인덱스에 해당하는 값들을 계산하기 위하여 랜덤 $h_{i^*}\in G$와 $x\in Z_p^*$ 값을 선택하고 $Y_i=\prod_{j=1}^{n_j}H_1(a_{i,j})$라고 설정 후 $R_{i^*}=(g^x/(Y_{i^*}^{h_{i^*}}))/(\prod_{1\le i\ne i^*\le m}(R_i\cdot Y_i^{h_i}))$ 값을 계산한다. 만일 $(M,\psi,R_{i^*},T_1,T_2,h_{i^*})$ 값을 $H_2-List$ 테이블에 저장할 때 충돌이 발생하는 경우 새로운 난수 $h_{i^*},x$ 다시 선택한 후 계산을 수행하여 충돌이 발생하지 않도록 설정한다.

4. $B$는 $V=(g_1^t)^x$ 값을 계산하고 $\sigma=(V,R_1,\cdots,R_m,T_1,T_2)$ 값을 $A$에게 답변한다. 이때 $B$가 생성한 서명은 다음 수식에 의해서 올바름을 알 수 있다.

$$V=(g^x)^{st}=(R_{i^*}\cdot Y_{i^*}^{h_{i^*}}\cdot \prod_{1\le i\ne i^*\le m}(R_i\cdot Y_i^{h_i}))^{st}$$
$$=(Y_{i^*}^{r_{i^*}}\cdot Y_{i^*}^{h_{i^*}})^{st}=\prod_{j=1}^{n_{i^*}}H_1(a_{i^*,j})^{st(r_{i^*}+h_{i^*})}.$$

Output: 마지막으로 공격자 $A$는 $(\sigma^*,M^*,\psi^*)$ 값을 출력한다. 이때 위조 서명은 $\sigma^*=(V^*,R_1^*,\cdots,R_{m^*}^*,T_1^*,T_2^*)$ 값이고, 공격자가 선택한 DNF 수식은 $\psi^*=\vee_{i=1}^{m^*}\wedge_{j=1}^{n_i^*}a_{i,j}^*$ 값으로 표현된다.

만일 공격자 $A$가 출력한 위조 서명이 위조 불가능성 게임에서 정의된 조건을 만족하지 못하는 경우, 공격자 $A$는 성공적으로 공격을 수행하지 못했기 때문에 $B$는 시뮬레이션을 중지한다.

Forking Lemma[17] 이용하여 알고리즘 $B$는 공격자 $A$를 이용하여 메시지 $M$과 DNF 수식 $\psi=\vee_{i=1}^{m}\wedge_{j=1}^{n_i}a_{i,j}$에 대하여 서명 $V\ne V'$ 조건을 만족하는 두 서명 $\sigma=(V,R_1,\cdots,R_m,T_1,T_2)$, $\sigma'=(V',R_1,\cdots,R_m,T_1,T_2)$ 값들을 얻는 것이 가능하고 인덱스 $i^*$ 이용하여 다음과 같이 $U$ 값을 계산한다.

$$U=(V/V')^{(h_{i^*}-h_{i^*}')^{-1}}$$
$$=\prod_{j=1}^{n_{i^*}}H_1(a_{i^*,j})^{st(h_{i^*}-h_{i^*}')\cdot(h_{i^*}-h_{i^*}')^{-1}}$$
$$=\prod_{j=1}^{n_{i^*}}H_1(a_{i^*,j})^{st}.$$

그런 후 $B$는 속성 집합 $w=\{a_{i^*,1},\cdots a_{i^*,n_{i^*}}\}$ 값과 $(U,T_1,T_2)$ 값을 interactive 가정의 해답으로 출력하고 종료한다. 공격자 $A$는 DNF 수식 $\psi$ 만족하는 속성 집합에 대한 비밀키 생성 질의 요청하지 않았기 때문에 알고리즘 $B$가 출력하는 속성 집합 $w$은 $\forall i: w\not\subseteq w_i$ 조건이 성립한다. 그러므로 $B$가 출력하는 값은 올바른 interactive 가정의 해답이다. □

*정리 2. 본 논문에서 기술된 속성 기반 서명 기법은 통계적 익명성을 제공한다.*

증명) 제안된 속성 기반 서명 기법이 자원 사용에 제한이 없는 공격자에 대해서 익명이라는 것을 보이기 위해서는 챌린저 $C$가 Challenge 단계에서 공격자 $A$에게 전달하는 서명 $\sigma$ 값이 서명 생성에 사용된 실제 서명자의 속성 정보와 통계적으로 독립임을 보이면 된다.

먼저 챌린저 $C$는 속성 기반 서명 기법의 설정 알고리즘 이용하여 공개 파라미터 $PP$와 마스터 비밀키 $MK$ 생성하여 익명성 게임을 수행한다. 이때 $C$는 마스터 비밀키 알고 있기 때문에 $A$가 요청하는 모든 질의에 대한 답변을 수행하는 것이 가능하다. Challenge 단계에서 $A$는 $(M,\psi,w_0,w_1)$ 값을 선택하면 $C$는 랜덤 $c\in\{0,1\}$ 선택하여 속성 집합 $w_c$의 비밀키 $SK_{w_c}$ 생성하고 이를 이용해서 $\psi=\vee_{i=1}^{m}\wedge_{j=1}^{n_i}a_{i,j}$ 수식에 대한 서명 $\sigma=(V,R_1,\cdots,R_m,T_1,T_2)$ 생성하여 $A$에게 전달한다.

공격자 $A$의 질의에 대한 답변은 Challenge 단계 이전에 수행되기 때문에 이들 답변은 챌린지 서명의 실제 서명 속성에 대한 어떠한 정보도 제공하지 않는다. 따라서 실제 서명 속성에 관련된 정보는 챌린지 서명 $\sigma=(V,R_1,\cdots,R_m,T_1,T_2)$ 값에만 포함된다. 챌린지 서명이 실제 서명자의 속성 정보와 통계적으로 독립임을 보이기 위해서 챌린지 서명 값이 공격자가 예상하는 어떠한 속성 정보 $w$에 대해서도 유효한 서명 값이 됨을 보이도록 하자.

1) 첫 번째로 서명에 포함된 $T_1,T_2$ 값은 실제 서명 속성 정보를 노출하지 않음을 보이자. 공격자 $A$는 두 값으로부터 $s\cdot t=dlog_g(T_1), t=dlog_g(T_2)$ 계산할 수 있다. 그리고 두 값은 실제 서명자 비밀키 요소에 추가 난수 $t_2$ 값을 지수승한 것이다. 실제 서명자의 비밀키에 사용되었던 난수가 $t_1$이라면 $t=t_1\cdot t_2 \bmod p$ 수식이 성립한다. 하지만 모든 $t_1$ 값에 대해서 이 수식이 성립하는 유일한 난수 $t_2$ 값이 존재하기 때문에 $A$는 $t_1$ 정보를 얻을 수 없다. 따라서 $T_1,T_2$ 두 값은 실제 서명 속성 정보를 노출하지 않는다.

2) 두 번째로 서명의 $V,R_1,\cdots,R_m$ 값들이 실제 서명 속성 정보를 노출하지 않음을 보이자. 먼저 DNF 수식 $\psi=\vee_{i=1}^{m}\wedge_{j=1}^{n_i}a_{i,j}$에서 서명 생성에 사용된 속성 집합과 관련된 인덱스가 $i^*$라고 가정하자. $C$가 챌린지 서명 생성에 사용한 난수가 $r_1^*,\cdots,r_{i^*}^*,\cdots,r_m^*$이라

고 하고, $Y_i = \prod_{j=1}^{n_i} H_1(a_{i,j})$라고 정의하자. 그러면 챌린지 서명 값들은 다음과 같이 표현된다.

$$V = Y_{i^*}^{st(r_{i^*}^* + h_{i^*})},\ \{R_i = g^{r_i^*}\}_{1 \le i \ne i^* \le m},$$
$$R_{i^*} = Y_{i^*}^{r_{i^*}^*} / \left( \prod_{1 \le i \ne i^* \le m} (R_i \cdot Y_i^{h_i}) \right)$$

공격자 $A$는 이산 대수 계산할 수 있기 때문에 $s = dlog_g(g_1),\ \forall i:\ y_i = dlog_g(Y_i)$ 계산이 가능하고, $v = dlog_g(V), u_i = dlog_g(R_i), t = dlog_g(T_2)$라고 정의하면 공격자는 서명 값에서 다음 수식을 얻을 수 있다.

$$v = y_{i^*} \cdot st \cdot (r_{i^*}^* + h_{i^*}),\ \{u_i = r_i^*\}_{1 \le i \ne i^* \le m},$$
$$u_{i^*} = y_{i^*} \cdot r_{i^*}^* - \sum_{1 \le i \ne i^* \le m} (r_i + y_i \cdot h_i)$$

만일 공격자 $A$가 DNF 수식의 인덱스 $\tilde{i}\,(\ne i^*)$에 해당하는 속성 집합의 비밀키를 이용해서 챌린지 서명이 생성되었다고 추측한다고 고려해 보자. 그리고 이때 공격자의 추측을 합리화하는 난수 값들을 $\tilde{r}_1^*, \cdots, \tilde{r}_{\tilde{i}}^*, \cdots, \tilde{r}_m^*$라고 하자. 그러면 $R_1, \cdots, R_m$ 값들로부터 다음을 얻을 수 있다.

$$\{u_i = r_i^* = \tilde{r}_i\}_{1 \le i \ne i^*, i \ne \tilde{i} \le m},$$
$$u_{i^*} = y_{i^*} \cdot r_{i^*}^* - \sum_{1 \le i \ne i^* \le m} (r_i^* + y_i \cdot h_i) = \tilde{r}_{i^*},$$
$$u_{\tilde{i}} = r_{\tilde{i}}^* = y_{\tilde{i}} \cdot \tilde{r}_{\tilde{i}} - \sum_{1 \le i \ne \tilde{i} \le m} (\tilde{r}_i + y_i \cdot h_i)$$

위의 수식을 다시 정리하면 다음과 같이 공격자의 추측을 합리화하는 난수들을 구할 수 있다.

$$\tilde{r}_i = r_i^*{}_{1 \le i \ne i^*, i \ne \tilde{i} \le m},$$
$$\tilde{r}_{i^*} = y_{i^*} \cdot r_{i^*}^* - \sum_{1 \le i \ne i^* \le m} (r_i^* + y_i \cdot h_i),$$
$$\tilde{r}_{\tilde{i}} = (r_{\tilde{i}}^* + \sum_{1 \le i \ne \tilde{i} \le m} (\tilde{r}_i + y_i \cdot h_i)) / y_{\tilde{i}}$$

참고로 $r_i^*$ 난수들은 $Z_p^*$ 상의 랜덤 값이기 때문에 $\tilde{r}_i$ 난수들 역시 $Z_p^*$ 상의 랜덤 값임을 확인할 수 있다.

이제 앞에서 구한 난수들을 이용하여 공격자가 예상하는 서명의 $\tilde{v} = dlog_g(\tilde{V})$ 값을 계산하여 이 값이 챌린지 서명의 $v = dlog_g(V)$ 값과 동일함을 다음과 같이 보이자.

$$\begin{aligned}
\tilde{v} &= y_{\tilde{i}} \cdot st \cdot (\tilde{r}_{\tilde{i}} + h_{\tilde{i}}) \\
&= st \cdot (r_{\tilde{i}}^* + \sum_{1 \le i \ne \tilde{i} \le m} (\tilde{r}_i + y_i h_i) + y_{\tilde{i}} h_{\tilde{i}}) \\
&= st \cdot (r_{\tilde{i}}^* + y_{\tilde{i}} h_{\tilde{i}} + \tilde{r}_{i^*} + y_{i^*} h_{i^*} + \sum_{1 \le i \ne i^*, i \ne \tilde{i} \le m} (\tilde{r}_i + y_i h_i)) \\
&= st \cdot (r_{\tilde{i}}^* + y_{\tilde{i}} h_{\tilde{i}} + (y_{i^*} r_{i^*}^* - (r_{\tilde{i}}^* + y_{\tilde{i}} h_{\tilde{i}}) \\
&\qquad - \sum_{1 \le i \ne i^*, i \ne \tilde{i} \le m} (r_i^* + y_i h_i)) + \\
&\qquad y_{i^*} h_{i^*} + \sum_{1 \le i \ne i^*, i \ne \tilde{i} \le m} (r_i^* + y_i h_i)) \\
&= st \cdot (y_{i^*} r_{i^*}^* + y_{i^*} h_{i^*}) \\
&= y_{i^*} \cdot st \cdot (r_{i^*}^* + h_{i^*}) \\
&= v
\end{aligned}$$

따라서 공격자가 어떠한 속성 집합을 추측하더라고 이를 만족하는 난수 $\{\tilde{r}_i\}$ 값들이 존재하고 이들 난수를 이용하여 생성한 서명은 챌린지 서명의 $V$ 값과 동일하므로 $V, R_1, \cdots, R_m$ 값들은 실제 서명 속 집합에 대한 정보를 노출하지 않는다. □

## V. 결 론

본 논문에서는 권한 및 속성 기반 시스템에 적합한 속성 기반 서명의 정의와 안전성 모델을 제시하고 서명에 포함된 정책을 DNF 형식으로 표현이 가능한 효율적인 속성 기반 서명 기법을 제안하였다. 제안된 기법은 서명 검증시 상수번의 페어링 연산만을 사용하기 때문에 현실적으로 사용이 가능한 기법이다.

## 참 고 문 헌


[1] G. Ateniese, M. Blanton, and J. Kirsch. Secret Handshakes with Dynamic and Fuzzy Matching. In *Network and Distributed System Security Symposuim (NDSS '07)*. 2007.

[2] A. Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[3] A. Bender, J. Katz, and R. Morselli. Ring signatures: Stronger denitions, and constructions without random oracles. In *TCC 2006*, volume 3876 of LNCS, pages 60-79. Springer-Verlang, 2006.

[4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Proceeding of the IEEE Symposium on Security and Privacy*, pages 321-334. 2007.

[5] R. Bobba, O. Fatemieh, F. Khan, C.A. Gunter, and H. Khurana. Using Attribute-Based Access Control to Enable Attribute-Based Messaging. In *IEEE Annual Computer Security Applications Conference (ACSAC '06)*, 2006.

[6] X. Boyen. Mesh signatures How to leak a secret with unwitting and unwilling participants. In *EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 210-227. Springer-Verlang, 2007.

[7] E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In *CRYPTO 2002*, volume 2442 of *LNCS*, pages 465-480. Springer-Verlang, 2002.

[8] J.C. Cha and J.H. Cheon. An identity-based signature from gap diffie-hellman groups. In *PKC 2003*, volume 2567 of *LNCS*, pages 18-30. Springer-Verlang, 2003.

[9] S.S.M. Chow, S.M. Yiu, and L.C.K. Hui. Efficient identity based ring signature. In *ACNS 2005*, volume 3531 of *LNCS*, pages 499-512. Springer-Verlang, 2005.

[10] W. Diffie and M.E. Hellman. New directions in cryptography. In *IEEE Transactions on Information Theory*, volume IT-22, no. 6, pages 644-654. 1976.

[11] C. Gentry and Z. Ramzan. Identity-based aggregate signatures. In *PKC 2006*, volume 3958 of *LNCS*, pages 257-273. Springer-Verlang, 2006.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute based encryption for fine-graned access control of encrypted data. In *ACM conference on Computer and Communications Security (ACM CCS)*, pages 89-98. 2006.

[13] D. Khader. Attribute-based group signatures. Cryptology ePrint Archive, Report 2007/159, 2007. http://eprint.iacr.org/.

[14] J. Li and K. Kim. Attribute-based ring signatures. Cryptology ePrint Archive, Report 2008/394, 2008. http://eprint.iacr.org/.

[15] H. Maji, M. Prabhakaran, and M. Rosulek. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. Cryptology ePrint Archive, Report 2008/328, 2008. http://eprint.iacr.org/.

[16] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *ACM conference on Computer and Communications Security (ACM CCS)*, pages 195-203. 2007.

[17] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. In *Journal of Cryptology*, volume 13, no 3, pages 361-396. 2000.

[18] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552-565. 2001.

[19] A. Sahai and B. Waters. Fuzzy identity based encryption. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457-473. Springer-Verlang, 2005.

[20] R.S. Sandhu, E.J. Coyne, and C.E. Youman. Role-based access control models. In *IEEE Computer*, volume 29, no 2, pages 38-47. 1996.

[21] H. Shacham and B. Waters. Efficient ring signatures without random oracles. In *PKC 2007*, volume 4450 of *LNCS*, pages 166-180. Springer-Verlang, 2007.

[22] A. Shamir. Identity-based cryptosystems and signaure shcemes. In *CRYPTO 1984*, volume 196 of *LNCS*, pages 47-53. Springer-Verlang, 1984.

[23] L. Wang, D. Wijesekera, and S. Jajodia. A Logic-Based Framework for Attribute-Based Access Control. In *ACM Workshop on Formal Methods in Security Engineering (FMSE '04)*, 2004.

## 저 자 소 개


**이 광 수**(학생회원)
1998년 연세대학교 컴퓨터과학과 졸업.
2000년 한국과학기술대학원 전산학과 석사.
2007년~현재 고려대학교 정보경영전문대학원 박사 과정 재학중.
<주관심분야 : 암호이론, 정보보호>

**김 형 중**(평생회원)
1978년 서울대학교 제어계측공학과 공학사.
1986년 서울대학교 제어계측공학과 공학석사.
1989년 서울대학교 제어계측공학과 공학박사.
1990년~2006년 강원대학교 교수.
2006년~현재 고려대학교 정보경영공학전문대학원 교수.
2008년~현재 대한전자공학회 컴퓨터소사이어티 회장
<주관심분야 : Parallel Computing, Image Hashing, Data Compression, Steganography>

**황 정 연**(정회원)
1999년 고려대학교 수학과 졸업.
2003년 고려대학교 정보보호대학원 석사 졸업.
2006년 고려대학교 정보보호대학원 박사 졸업.
2008년~현재 고려대학교 BK21 유비쿼터스 정보보호 사업단 연구교수
<주관심분야 : 암호프로토콜, 정보보호이론>

**이 동 훈**(정회원)
1983년 고려대학교 경제학과 졸업.
1987년 University of Oklahoma 전산학과 공학석사.
1992년 University of Oklahoma 전산학과 공학박사.
1993년~현재 고려대학교 정보경영공학전문대학원 교수.
<주관심분야 : 프로토콜이론, 정보보호>