情報保護學會論文誌
第11券 第6號, 2001. 12

그룹 서명 기법에서의 효율적이고 안전한 구성원 탈퇴 방법*

김 현 정*, 임 종 인**, 이 동 훈**

Efficient and Secure Member Deletion in Group Signature Scheme

Hyun-Jeong Kim*, Jong-In Lim**, Dong-Hoon Lee**

요 약

그룹 서명 기법은 익명성을 보장해주면서 그룹 구성원들로 하여금 그룹을 대표해서 서명을 할 수 있도록 하는 방법으로 분쟁이 발생하는 경우에는 지정된 그룹 관리자만이 구성원의 신원을 확인할 수 있다. 최근 수 년 동안, 그룹 서명 기법은 집중적으로 연구되어 왔으며 다양한 응용분야에 적용되고 있다. 그러나 그룹의 구성원이 소속된 그룹에서 탈퇴하기를 원하거나 불법행위 등의 이유로 그룹에서 강제 탈퇴되어야 하는 경우가 발생했을 때, 이 상황에 적합한 방법이 구체적으로 제시되어 있지 않다. [3]에서 언급한 바에 의하면 구성원 탈퇴에 따른 복잡도는 그룹 서명을 실생활에 적용하는데 있어 걸림돌이며 따라서 시급히 해결해야 할 문제이다. 이 논문에서 그룹 공개키와 서명 길이는 그룹 크기에 독립적이면서 구성원의 자유로운 탈퇴를 허용하는 효율적인 그룹 서명 기법을 제안한다. 제안한 그룹 서명 기법의 안전성은 RSA 가정에 기반하고 있다. 더 나아가 특정한 구성원이 생성한 서명을 추적해 낼 수 있는 방법도 더불어 제안한다.

ABSTRACT

Group signature schemes allow a group member to sign messages anonymously on behalf of the group. In case of dispute, only a designated group manager can reveal the identity of the member. During last decade, group signature schemes have been intensively investigated in the literature and applied to various applications. However, there has been no scheme properly handling the situation that a group member wants to leave a group or is excluded by a group manager. As noted in[3], the complexity of member deletion stands in the way of real world applications of group signatures and the member deletion problem has been a pressing open problem. In this paper, we propose an efficient group signature scheme that allows member deletion. The length of the group public key and the size of signatures are independent of the size of the group and the security of the scheme relies on the RSA assumption. In addition, the method of tracing all signatures of a specific member is introduced.

keyword : *group signature, revocation, user-tracing, signature-tracing*

Ⅰ. 서 론

그룹 서명 기법의 개념은 D.Chaum과 van Heyst[9]에 의해 처음으로 제시되었다. 그룹 서명 기법에서 그룹 구성원에게 서명 권한을 부여하는 것은 그룹 관리자에 의해 이루어지며 각 구성원이 발행하는 서

* 본 연구는 한국과학재단 목적기초연구(r01-2001-00537) 지원으로 수행되었음.
** 고려대학교 정보보호연구센터(CIST)(khj@cist.korea.ac.kr)
*** 고려대학교 정보보호연구센터(CIST)({jilim,donghlee}@tiger.korea.ac.kr)

명에 대해서는 익명성이 보장된다. 이때 서명된 문서는 그룹의 공개키에 의하여 정당성이 확인되며 분쟁이 발생하는 경우에는 권한이 부여된 그룹 신원 관리자만이 구성원의 신원을 밝혀 낼 수 있도록 한다. 이때 그룹 관리자와 그룹 신원 관리자는 동일할 수도 있고 그룹 관리자의 권한을 최소화하기 위해 분리되어 구성 될 수도 있다. 일반적으로 그룹 서명 기법은 다음과 같은 과정으로 구성되어 있다.

- 초기구성(Setup) : 그룹 관리자의 키와 시스템 매개변수를 생성한다.
- 가입(Join) : 그룹에 가입하고자 하는 새로운 구성원이 그룹 관리자로부터 그룹 서명을 생성할 수 있는 권한(멤버쉽 키)을 얻는다.
- 서명(Sign) : 권한을 부여받은 구성원이 그룹을 대표하는 서명을 생성한다.
- 검증(Verify) : 그룹키를 이용하여 주어진 서명이 정당한 그룹 구성원에 의해 생성된 것인지 확인한다.
- 추적(Tracing) : 부적절한 서명이 발생하는 경우 그룹 신원 관리자는 해당 서명을 발행한 그룹 구성원의 신원을 밝혀 낸다.

지금까지 서명의 길이와 그룹의 공개키가 그룹 크기에 독립적일 수 있는 보다 효율적인 기법을 고안하기 위해 다양한 그룹 서명 기법들이 연구되었다. 그 결과 [5,9,10,12]에서 제시된 그룹 서명 기법들은 길이에 대한 요구조건을 만족시키지 못했지만 [2,6~8]에서 제시된 기법들은 이 조건을 수용하고 있다.

또한 그룹 서명 기법은 구성원 공모 공격에도 견딜 수 있어야 한다. 그룹 관리자를 포함한 구성원 일부가 공모하여 추적 불가능한 서명을 생성하거나 혹은 다른 구성원의 신원으로 잘못 밝혀질 수 있는 불법 서명을 생성할 수 없어야 하는 것이다. [2,6]은 구성원 공모 공격에 대해 증명 가능한 안전성을 제공하는 기법을 다루고 있다.

이처럼 효율적이고 안전한 그룹 서명 기법의 발달에 따라 그룹 서명 개념은 전자 화폐 시스템, 경매 시스템, 투표 시스템 등 다양한 응용분야에 적용되고 있다. 그러나 이러한 실용분야에 적용되기 위해서 해결되어야 할 몇 가지 문제점들이 남아 있는데 그 중 가장 중요한 것은 구성원 탈퇴에 대한 효율적인 운영이다.

실생활에서 그룹은 유동적이다. 구성원들은 승진 등의 다양한 이유로 인해 자발적으로 그룹을 떠날 수도 있고 구성원이 불법행위를 저지른 경우는 그룹 관리자에 의해 강제 탈퇴될 수도 있다. 이런 경우 다른 구성원들의 익명성은 그대로 보존하면서 불법 행위를 벌인 그 구성원이 생성했던 서명들을 추적해 내야 하는 경우가 생길 수도 있다. [3]에서 언급했듯이 효율적이고 안전한 구성원 탈퇴가 해결되어야 할 문제로 남아 있다. [4]에서는 [6]에 기반하여 그룹 구성원 탈퇴방법을 제시하였으나 서명의 길이가 탈퇴 인원수에 비례하여 증가하는 문제점을 지니고 있다. 이 외에 지금까지 그룹 서명 기법에 있어서 구체적으로 구성원 탈퇴 기법을 제안한 논문은 거의 없다.

이 논문에서는 구성원 탈퇴를 허용하면서 서명 길이는 구성원의 수나 탈퇴 인원수에 독립적인 그룹 서명 기법을 제안한다. 제시하는 기법은 Camenisch와 Michels이 제시했던 그룹 서명 기법[6]에 기반하여 구성원 탈퇴 과정을 구성하고 더 나아가 특정 구성원에 의해 생성된 서명을 추적하는 방법을 새롭게 제안한다.

본 논문의 구성은 다음과 같다. 2절에서는 그룹 서명 기법에서 구성원 가입/탈퇴를 허용하기 위해 제시한 기법의 모델과 접근방식에 대해 설명하고 기존 기법과 비교해 본다. 3절에서는 제시한 그룹 서명 기법의 안전성을 위해 필요한 가정들을 설명한다. 4절에서는 제시하는 기법을 구체적으로 구현하고 그 안전성 분석을 5절에서 다룬다. 마지막으로 6절에서 이 논문에 대한 결론을 논하고자 한다.

II. 새로운 기법의 개념 및 관련 연구

이 절에서는 제안 기법의 개념과 접근 방식에 대해 간략히 설명한다. 또한 기존에 제안된 기법과 새롭게 제안하는 기법을 비교, 분석한다.

2.1 제안 기법의 모델 및 접근 방식

본 논문에서 제안되는 모델의 큰 특징은 구성원 탈퇴 과정과 추적 과정이다. 지금까지의 추적 과정은 특정 서명과 관련된 해당 구성원의 신원을 추적하는 것만을 다루고 있으나 여기서는 특정 구성원이 생성한 서명을 추적하는 방법을 추가로 제안한다.

구성원 탈퇴는 [1]의 브로드캐스트 암호화 기법을

사용함으로써 보다 안전하고 효율적으로 이루어진다. 브로드캐스트 암호화 기법은 암호화 메시지를 브로드캐스트하면 사전에 권한이 부여된 구성원만이 메시지를 복호화 할 수 있도록 하는 것이다. 특히 [1]에서 제안된 기법은 권한이 박탈된 사용자는 더 이상 브로드캐스트되는 암호화 메시지를 복호화 할 수 없도록 하는 기능이 포함되어 있다.

2.1.1 모델

제안하는 그룹 서명 기법은 다음과 같은 단계로 구성된다.

- **초기구성(Setup)** : 그룹 관리자와 그룹 신원 관리자 에 의해 이루어진다. 이 과정에서 그룹 관리자의 비밀키 x_M, 공개키 y_M과 그룹 신원 관리자의 비밀키 x_R, 공개키 y_R이 생성된다.
- **가입(Join)** : 그룹 관리자와 그룹 구성원이 되고자 하는 사용자 사이에서 이루어지는 프로토콜로써 그룹 관리자가 다음과 같은 키를 생성한다. 새로운 그룹 구성원의 비밀키 x_G, 공개키 y_G, 비밀 소속키 U_G와 그룹의 공개 소속키 U_M, 그리고 그룹의 공개 갱신키 U_N이 생성된다. 또한 가입하는 그룹 구성원은 구성원 탈퇴시 브로드캐스트 기법을 통하여 암호화되서 공개되는 $E(U_N)$을 복호화하기 위한 개인키를 얻는다.
- **탈퇴(Delete)** : 그룹 관리자는 입력 정보인 탈퇴 구성원의 공개키 y_G에 기반하여 그룹의 공개 소속키 U_M과 그룹의 공개 갱신키 U_N을 갱신한 후, 탈퇴하는 구성원이 복호화할 수 없도록 [1]의 기법으로 암호화된 $E(U_N)$을 생성한다.
- **서명(Sign)** : 서명 생성 알고리즘은 그룹 구성원이 수행하는 것으로 메세지 m과 x_G, y_G, y_M, y_R, U_G을 입력값으로 하여 서명값 σ을 생성한다.
- **검증(Verify)** : 검증 알고리즘은 메세지 m, 서명값 σ, y_M, y_R 그리고 U_M에 대해서 σ가 정당한 그룹 구성원에 의해 생성된 것인지에 대해 검증하고 유효하다고 판단되면 1을 출력한다.
- **구성원 추적(User-Tracing)** : 이 알고리즘을 통해 그룹 신원 관리자는 서명값 σ, 메세지 m, x_R, y_R을 바탕으로 σ를 생성한 그룹 구성원의 신원을 찾는다.
- **서명 추적(Signature-Tracing)** : 이 알고리즘은 그룹 신원 관리자에 의해 수행되는 것으로 특정 구성원의 공개키 y_G와 그룹 신원 관리자의 비밀키 x_R를 이용하여 서명값 σ가 특정한 그룹 구성원에 의해 생성되었음이 입증되는 경우 1을 출력한다.

제안기법에서는 다음과 같은 안전성이 필요하다.

- **서명 위조 불가능성** : 오직 현재 그룹에 소속되어 있는 구성원만이 정당한 서명을 생성할 수 있다. 더 나아가서 그렇게 생성된 서명 값은 필요시 그룹 신원 관리자에 의해 추적이 가능하다. 특히, 그룹을 탈퇴한 구성원은 더 이상 정당한 서명을 생성해 낼 수 없어야 한다.
- **익명성** : 그룹 신원 관리자 이외에는 주어진 서명을 생성한 구성원의 신원을 확인하는 것이 어렵다.
- **서명 연계 불가능성** : 두 개 이상의 서명이 주어졌을 때 그룹 신원 관리자를 제외하고는 그 누구도 그 서명이 동일한 그룹 구성원에 의해 생성된 것인지 아닌지 판단하기 어렵다.
- **공모 위조 불가능성** : 그룹 관리자를 포함하여 그룹 구성원 일부가 공모하여 공모에 가담하지 않은 다른 구성원에 의해 생성된 것처럼 보이는 서명을 생성해 낼 수 없다. 더 나아가서 공모자들이 그룹을 이미 탈퇴한 구성원을 대신해서 정당하게 보이는 서명을 생성할 수 없다.
- **구성원 추적 위조 불가능성** : 주어진 서명에 대해 그룹 신원 관리자가 그 서명 생성자의 신원을 거짓으로 밝힐 수 없다.
- **서명 추적 위조 불가능성** : 그룹 신원 관리자가 특정한 그룹 구성원에 의해 생성된 것이 아닌 서명에 대해 거짓으로 그 구성원이 생성한 것이라고 증명할 수 없다.

이와 같이 본 논문에서 제안한 기법의 구성과 Camenisch 기법[6] 구성의 차이점을 비교해보면 다음 표와 같다.

[표 1] 제안 기법과 [6] 기법의 비교

항목 / 기법	구성원 가입	구성원 탈퇴	구성원 추적	서명 추적
[6]	○	×	○	×
제안기법	○	○	○	○

3.1.2 접근방식

구성원 변경 관리를 위한 핵심 개념은 다음과 같다. 그룹 내 구성원의 변경사항 처리를 위해 그룹 관리자는 그룹의 공개 소속키 U_M과 그룹의 공개 갱신키 U_N을 관리한다. 또한 새로운 구성원이 가입하는 경우 그룹 관리자는 그 구성원의 비밀 소속키 U_G를 생성한다.

가입 또는 탈퇴의 경우 그룹 관리자는 먼저 그룹의 공개 소속키 U_M과 그룹의 공개 갱신키 U_N을 변경하고 가입의 경우 U_M과 U_N을 그대로 공개, 탈퇴의 경우 U_M과 브로드캐스트 기법을 이용하여 암호화된 $E(U_N)$을 공개한다. 이때 [1]의 브로드캐스트 암호화 기법에 따라 탈퇴에 관련되지 않은 정당한 그룹 구성원만이 그룹의 공개 갱신키 U_N을 복호화 할 수 있다. U_N을 얻은 그룹 구성원은 정당한 서명 생성을 위해 그룹의 공개 갱신키 U_N를 이용하여 각자 자신의 비밀 소속키 U_G를 변경하고 새로 변경된 자신의 비밀 소속키가 정당한지 그룹의 공개 소속키 U_M를 이용하여 확인한다. 또한 누군가가 주어진 서명값이 정당한지 확인하고자 한다면 그룹의 공개 소속키를 이용하여 확인해야 한다. 이때 그룹을 이미 탈퇴한 사람이 자신이 가지고 있던 이전의 비밀 소속키를 이용하여 정당하게 보이는 서명을 생성하려 하는 것은 계산적으로 어려운 문제이다.

이상 설명한 내용에 따르면 그룹 관리자는 각 구성원의 비밀키에 대해 오직 새로 가입하는 구성원의 비밀키만을 생성해주면 되고 기존 구성원들의 비밀키는 각 개인이 관리하도록 되어있음을 알 수 있다. 따라서 그룹 구성원 변동에 따라 발생하는 계산량은 각 구성원들에게 분산되어진다.

2.2 관련연구

여기서는 제안하는 새로운 기법과 관련된 기존 연구에 대해 비교, 분석하고자 한다.

2001년 PKC에 E. Bresson과 J. Stern에 의해 발표된 "Efficient Revocation in Group Signatures[4]" 이전에 그룹 서명 기법에서 구성원의 탈퇴 과정을 구체적으로 논의한 경우는 거의 없다. 이 논문 역시 여기서 제시하고 있는 기법과 마찬가지로 Camenisch와 Michels의 그룹 서명 기법[6]에 기반하고 있다. 따라서 먼저 [6]의 논문을 살펴보고 [4]와 본 논문의 제안 기법을 비교해 보도록 한다.

[6]에서는 Modified Strong RSA 가정에 기반한 새로운 그룹 서명 기법을 제안하고 있다. 앞서 그룹 구성원 크기에 독립적인 서명을 처음으로 제시하였던 [8]의 기법과 마찬가지로 독립적인 그룹 서명 길이를 유지하고 있으면서 [8]보다 계산적으로 효율적인 방법을 구성함으로써 구성원 수가 많은 큰 그룹에 적용이 용이하도록 하였다. 그러나 이 논문에서도 다른 연구 결과들과 마찬가지로 구성원 탈퇴 문제에 대해서는 다루고 있지 않다.

[4]는 위의 [6]에서 제시된 그룹 서명 기법에 기반하여 구성원 탈퇴가 가능하도록 하는 새로운 기법을 제시하였다. 이 기법의 경우 구성원 탈퇴시 그룹 관리자는 공개키 기반 구조에서 탈퇴 사용자 리스트를 관리하는 것과 마찬가지로 탈퇴 구성원의 공개키 리스트를 관리하게 된다. 정당한 그룹 구성원들은 서명을 생성할 때 자신의 공개키가 탈퇴 구성원의 공개키 중 어떤 것과도 일치하지 않음을 보이는 서명을 덧붙혀 생성해야만 한다. 따라서 탈퇴 인원수에 따라 서명생성을 위한 계산량뿐만 아니라 서명길이도 증가하게 되고 서명을 확인하는 단계의 계산량도 함께 증가한다.

본 논문에서 제안하는 기법에서는 그룹 관리자는 [6]에서 보다 두 개가 더 증가한 세 개의 그룹키를 관리한다. 그룹 공개 소속키와 갱신키가 이에 해당하며 이 키를 이용하여 탈퇴 인원의 공개키를 관리하게 된다. 새로운 구성원이 가입하거나 혹은 기존 구성원이 탈퇴하는 경우 각 구성원이 소유한 멤버쉽 키의 재발급 없이 그룹의 공개 정보와 구성원의 비밀키 일부만을 수정하면 된다. 이를 위해 그룹 관리자의 경우 두 번의 모듈러 지수승, 두 번의 모듈러 역수 계산, 그리고 변경 인원수에 따른 모듈러 곱이며 각 그룹 구성원의 경우는 오직 한 번의 모듈러 곱이 필요하다. 그룹 구성원 탈퇴시에는 그룹 공개 갱신키를 위한 브로드캐스트 암호화/복호화 기법의 연산이 포함된다. 이때 그룹의 공개키, 구성원의 비밀키, 서명은 일정한 크기를 유지하며 구성원 등록과 탈퇴에 대한 계산 복잡도는 그룹 크기와 관련이 있지만 계산부담이 각 구성원에게 분산되어 있다. 그리고 그 이외 과정의 계산 복잡도는 그룹 크기에 독립적이다. 서명 검증 또는 서명 추적을 위해서는 [6]에서 제안된 연산량에 테이블 검색이 추가될 뿐이다. 테이블 크기를 m이라 할 때 검색시 $O(\log m)$ 정도가 걸린다. 이처럼 탈퇴과정을 제공하는 기법을 구현하는데 있어서 서명길이를 항상 일정하게 유지하기 위해 각 과정마다 [6]의 기법에서 요구되는 연

산량에 덧붙혀 추가적으로 연산량이 다소 증가하게 됨을 알 수 있고 이를 표현하면 다음과 같다.

〔표 2〕 본 기법에서 〔6〕의 연산량에 대해 증가되는 연산량 : k-가입 또는 탈퇴 구성원수, m-탈퇴구성원 테이블 길이, MUL-모듈러곱, INV-모듈러 역수계산, EXP-모듈러 지수승

항목 / 대상	구성원 가입	구성원 탈퇴	서명 검증
그룹 관리자	2 INV +2 EXP + k MUL	2 INV+2 EXP + k MUL+ 브로드캐스트 암호화	·
구성원	1 MUL	1 MUL+ 브로드캐스트 복호화	·
서명 검증자	·	·	2 MUL+ O(logm)

이처럼 다소 연산량이 증가하지만 서명의 길이는 계속해서 일정하게 유지될 수 있다는 측면에서 본 논문에서 제시하는 모델은 〔4〕보다 효율적이며 구성원의 변화가 수시로 발생하는 큰 그룹에 적합한 해결책이 될 것이다. 더 나아가서 불법 행위를 행한 특정 구성원이 생성한 모든 서명 추적이 가능한 방법을 추가로 제시하고 있다.

Ⅲ. 기본 가정

이 절에서는 제안한 그룹 서명 기법을 구현하기 위해 필요한 암호학적 가정들을 살펴본다. 제안된 기법은 Camenisch와 Michels의 방법〔6〕에 기반하여 구성원 탈퇴 과정을 수행하고 있기 때문에 여기서는 그들이 제안한 기법과 관련한 내용만을 간략히 언급하고 〔6〕의 제 4절에 설명된 암호학적 기반들에 대해서는 생략하도록 한다. 그 암호학적 기반들은 증명 시스템으로써 이를 이용하여 한 사용자가 다른 사람들에게 자신이 정확한 자료를 지니고 있다는 사실을 정보의 누출없이 증명할 수 있도록 되어 있다. 이는 메세지에 대한 서명과 동시에 비밀키에 대한 증명을 수행할 수 있기 때문에 이러한 증명 시스템을 "signatures based on a proof of knowledge", 줄여서 SPK라 칭한다. 앞으로 이 논문에서 SPK가 사용될 때마다 증명하고자 하는 비밀키가 무엇인지 세부적인 내용은 〔6〕와 〔11〕를 참조한다.

l_g를 안전성 매개변수라 하고 G는 길이가 l_g인 위수를 가진 군이라 하자. 이때 위수는 길이 $(l_g-2)/2$인 두 개의 소수로 인수분해 되어진다.

■ **문제 1(RSA 문제)** G와 $(z, e)\in G/\{\pm 1\}\times Z$가 주어졌을 때, $u^e=z$를 만족하는 $u\in G$를 찾는 문제.

T를 입력값 1^{l_k}에 대해 G와 $z\in G/\{\pm 1\}$를 출력하는 키 생성자라 하자.

■ **가정 1(RSA 가정)** 모든 확률적인 다항식 시간 알고리즘 A, 모든 다항식 $p(\cdot)$, 그리고 충분히 큰 l_g에 대해 다음을 만족하는 확률적인 알고리즘 T가 존재한다.

$$\Pr[z=u^e|(G,z,e):=T(1^{l_k}),\ u:=A(G,z,e)]<\frac{1}{p(l_g)}$$

다음에 나오는 두 가정은 〔5〕에서 인용한 것이다. 이 논문에서는 Fujisaki와 Okamoto 〔10〕에 의한 "Strong RSA 가정"을 변형한 "Modified Strong RSA 가정"을 제안하였다. k, l_1, $l_2<l_g$와 $\varepsilon>1$를 안전성 매개변수라 하고 $\tilde{l}=\varepsilon(l_2+k)+1$라 하자. 또한 $z\in G$에 대해 $M(G,z)=\{(u,e)|x=u^e,\ u\in G,\ e\in\{2^{l_1}-2^{l_2},\cdots,2^{l_1}+2^{l_2}\},\ e\text{: prime}\}$라 하자.

■ **문제 2(Modified Strong RSA 문제)** G, $z\in G$와 $|M|=O(l_g)$인 $M\subset M(G,z)$가 주어졌을 때, $u^e=z$, $e\in\{2^{l_1}-2^{\tilde{l}},\cdots,2^{l_1}+2^{\tilde{l}}\}$를 만족하면서 M에 속하지 않는 한 쌍의 $(u,e)\in G\times Z$를 찾는 문제.

■ **가정 2(Modified Strong RSA 가정)** 모든 확률적인 다항식 시간 알고리즘 A, 모든 다항식 $p(\cdot)$, 충분히 큰 l_g, $|M|=O(l_g)$인 모든 $M\subset M(G,z)$, 그리고 적절하게 선택된 l_1, l_2, k와 ε에 대하여 다음을 만족하는 확률적인 알고리즘 T가 존재한다.

$$\Pr[z=u^e\wedge e\in\{2^{l_1}-2^{\tilde{l}},\cdots,2^{l_1}+2^{\tilde{l}}\}\wedge(u,e)\notin M|(G,z):=T(1^{l_k}),(u,e):=A(G,z,M)]<\frac{1}{p(l_g)}$$

〔6〕에서 기술된 것처럼, 만일 $z=u^e=u'^{e'}$인 두 개의 쌍 (u,e), (u',e')와 $\gcd(e,e')=1$이 알려진다면 "extended Euclidean 알고리즘"을 이용하여 $z=\hat{u}^{ee'}$를 만족하는 $\hat{u}$를 쉽게 찾을 수 있다. 그러나 적절히 선택된 매개변수 l_g, l_1, l_2, ε, k에 대해서 $ee'\notin\{2^{l_1}-2^{\tilde{l}},\cdots,2^{l_1}+2^{\tilde{l}}\}$이기 때문에 ee'는 요구

되는 범위를 만족시키지 못한다. 그러므로 "Modified strong RSA 가정"에 기반한 그룹 서명 기법은 공모 공격에 강하다. 또한 "Modified Strong RSA 문제"가 최소한 "Strong RSA 문제"만큼 어려운 문제임을 [6]와 [13]를 통해 알 수 있다.

"Modified Strong RSA 가정"에 덧붙여 Camenish와 Michels의 그룹 서명 기법은 Diffie-Hellman Decision(DHD)가정에 기반한다. 이 가정에 대해 설명하기에 앞서 먼저 다음 두 집합을 정의하도록 하자.

$$DH(G)=\{(g_1,y_1,g_2,y_2)\in G^4 \mid ord(g_1)=ord(g_2)=n',\ \log_{g_1}y_1=\log_{g_2}y_2\}$$

$$Q(G)=\{(g_1,y_1,g_2,y_2)\in G^4 \mid ord(g_1)=ord(g_2)=ord(y_1)=ord(y_2)=n'\}$$

이때 $n'|O(G)$이고 $|n'|=l_g-2$이다.

- **가정 3(Diffie-Hellman Decision 가정)** 모든 확률적인 다항식 시간 알고리즘 A와 충분히 큰 l_g에 대해 다음 두 확률분포

  $\Pr[a=1|G=T(1^{l_k}),K\in_R DH(G),a=A(K)]$와
  $\Pr[a=1|G=T(1^{l_k}),K\in_R Q(G),a=A(K)]$

  를 계산적으로 구별해내기 어려운 확률적인 알고리즘 T가 존재한다.

n이 RSA-modulus인 $G=Z_n^*$의 경우에 대해 DHD 가정을 고려해 보자. 이런 경우 어떤 $g_1,g_2,y_1,y_2\in G$에 대해서는 $\log_{g_1}y_1$와 $\log_{g_2}y_2$에 관한 정보가 Jacobi-symbol에 의해 누출될 수 있으므로 일반적으로 DHD가정은 성립하지 않는다. 예를 들면, 만일 $\left(\frac{g_1}{n}\right)=\left(\frac{g_2}{n}\right)=\left(\frac{y_2}{n}\right)=-1$ 이고 $\left(\frac{y_1}{n}\right)=1$ 이면, $\log_{g_1}y_1\neq\log_{g_2}y_2$이다.

- **주 1** n이 RSA-modulus인 $G=Z_n^*$의 경우 $G=\langle g\rangle$를 $\left(\frac{g}{n}\right)=1$ 인 $G=Z_n^*$의 부분군으로 정의하면 DHD가정은 성립한다.

Ⅳ. 제안된 기법

이제 제시하는 그룹 서명 기법에 관하여 설명하도록 한다. 제안하는 기법의 안전성은 가정 1,2,3에 기반하고 있다. 특히, 구성원 탈퇴를 위해 사용되는 그룹 소속키와 그룹 갱신키에 대한 안전성은 가정 1에 기반한다. 여기서는 구성원의 가입 및 탈퇴에 촛점을 두고 제안 방식을 기술해 나갈 것이다.

4.1 시스템 초기 구성(Setup)

먼저 그룹 관리자와 그룹 신원 관리자는 각자 공개키와 비밀키를 생성한다.

그룹 관리자는 다음과 같은 과정을 수행한다.

1. 군 $G=\langle g\rangle$을 선택하고 동일한 위수($\approx 2^{l_k}$)를 가지면서 가정 2,3을 만족하는 두 개의 임의의 값 $z,h\in G$을 선택한다. 또한 군 G의 위수는 비밀로 한다.
2. 임의의 큰 소수 p와 $q(\approx 2^{l_k/2})$를 선택한다. 이때 소수 p',q'에 대해 $p=2p'+1$, $q=2q'+1$ 형태이고 $p,q\neq 1$, $p\neq q \pmod 8$를 만족하도록 한다.
3. p와 q는 비밀키로 하고 $n=pq$는 공개한다.
4. n이 RSA-mod일 때 $e_N d_N\equiv 1(\bmod \phi(n))$인 공개키 e_N와 비밀키 d_N를 선택한다.
5. z,g,h,G,e_N와 l_g를 공개하고 g,h와 z가 동일한 위수가 됨을 증명한다.

또한 그룹 관리자는 해쉬함수 $H:\{0,1\}^*\rightarrow\{0,1\}^k$와 안전성 매개변수 $\tilde{l}$, l_1, l_2, ε을 선택, 공개한다.

그룹 신원 관리자는 다음 과정을 수행한다.

1. 비밀키 $x_R\in\{0,\cdots,2^{l_k}-1\}$을 임의로 선택한다.
2. $y_R=g^{x_R}$을 공개한다.

4.2 가입(Join)

이것은 그룹 관리자와 그룹의 새로운 구성원이 되고자 하는 Alice 간에 수행되는 상호 프로토콜이다.

Alice는 다음과 같이 수행한다.

1. $\hat{x}_G x_G\neq 1 \pmod 8$와 $\hat{x}_G\neq x_G \pmod 8$을 만족하는 임의의 소수 $\hat{x}_G, x_G\in_R\{2^{\tilde{l}-1},\cdots,2^{\tilde{l}}-1\}$을 선택한다.
2. $\grave{x}_G=x_G\,\hat{x}_G$와 $\grave{z}=z^{\hat{x}_G}$을 계산한다.

3. $\tilde{x}_G$, $\tilde{z}$와 이에 대한 commitment 값을 그룹 관리자에게 보낸다.
4. 다음에 대한 상호증명 프로토콜을 그룹 관리자와 함께 수행한다.

$$W = SPK\{(\tau, \varrho) | z^{\widetilde{x_G}} = \tilde{z}^{\tau} \wedge \tilde{z} = z^{\varrho} \wedge (2^{l_1} - 2^{\varepsilon(l_2+k)+1} < \tau < 2^{l_1} + 2^{\varepsilon(l_2+k)+1})\}(\tilde{z})$$

W는 $x_G \in \{2^{l_1} - 2^{\varepsilon(l_2+k)+1}, \cdots, 2^{l_1} + 2^{\varepsilon(l_2+k)+1}\}$와 $\tilde{z}^{x_G} = z^{\widetilde{x_G}}$를 만족하는 정수 x_G와 $\tilde{z}(= z^{\widetilde{x_G}})$의 이산대수 지식에 관한 통계적인 영지식 증명에 기반하고 있다. 따라서 그룹 관리자는 증명 W를 통하여 Alice가 $\tilde{x}_G$와 $\tilde{z}$를 정확히 선택하였음을 신뢰한다.

$C = \{G_1, G_2, \cdots, G_{m-1}\}$을 현재 그룹에 소속되어 있는 구성원들 집합이라 하고 G_m을 새로 가입하는 구성원 Alice라 하자. y_{G_i}는 각 구성원의 공개키를 의미한다. Alice가 그룹에 가입하기 전 상태에서의 그룹 공개 소속키는 $U_M = y_{G_1} \cdots y_{G_{m-1}} y'$라 하자. 이때 $y' \in G$는 임의의 값이다.

그룹 관리자는 다음을 수행한다.

1. Alice의 공개키 $y_{G_m} = \tilde{z}^{1/\widetilde{x_G}}$을 생성한다.
2. 그룹의 공개 소속키 $U_M = y_{G_1} \cdots y_{G_{m-1}} y_{G_m} y''$를 재생성한다. 이때 $y'' \in_R G$이다.
3. 그룹의 공개 갱신키 $U_N = \left(\frac{y_{G_m} y''}{y'}\right)^{d_N}$을 계산한다.
4. 새로운 구성원 G_m의 비밀 소속키 $U_{G_m} = (y_{G_1} y_{G_2} \cdots y_{G_{m-1}} y'')^{d_N}$을 생성한다.

그룹 관리자는 U_M과 U_N을 공개하고 새로운 구성원의 공개키 y_{G_m}과 비밀 소속키 U_{G_m}을 Alice에게 보낸다. 또한 구성원 탈퇴가 발생하는 경우 암호화된 $E(U_N)$을 복호화하기 위해 필요한 개인키를 전송한다. 이때 (x_{G_m}, y_{G_m})가 Alice의 멤버쉽 키가 된다. 새로운 구성원 Alice(G_m)는 자신의 공개키 y_{G_m}과 비밀 소속키 U_{G_m}을 각각 $y_{G_m}^{x_{G_m}} = z$와 $(U_{G_m})^{e_N} y_{G_m} = U_M$을 확인함으로써 검증할 수 있다. 새로운 구성원 G_m을 제외한 각 구성원 $G_i (1 \le i \le m-1)$은 그의 비밀 소속키 U_{G_i}을 $U_{G_i} = U_{G_i} \cdot U_N$로 변경한다. 즉,

$$U_{G_i} = (y_{G_1} \cdots y_{G_{i-1}} y_{G_{i+1}} \cdots y_{G_m} y')^{d_N} \times (y_{G_m} y'' / y')^{d_N} = (y_{G_1} \cdots y_{G_{i-1}} y_{G_{i+1}} \cdots y_{G_{m-1}} y_{G_m} y'')^{d_N}$$

각 그룹 구성원은 새로 갱신한 키 U_{G_i}을 $U_M = (U_{G_i})^{e_N} y_{G_i}$을 이용하여 검증할 수 있다.

4.3 탈퇴(Delete)

이 프로토콜은 가입 프로토콜과 유사하다. 그룹 구성원 G_j의 탈퇴를 위해 그룹 관리자는 그룹의 공개 소속키 U_M에서 해당 구성원의 공개키 y_{G_j}를 제거해야 하고 다른 그룹 구성원들은 그들의 비밀 소속키를 갱신하면 된다.

현재 그룹의 공개 소속키를 $U_M = y_{G_1} \cdots y_{G_m} y''$이라 하자. 이때 $y'' \in G$는 임의의 값이다.

그룹 관리자는 다음과 같이 탈퇴 프로토콜을 수행한다.

1. $y''' \in_R G$인 $U_M = U_M \cdot \frac{y'''}{y_{G_j} y''}$를 계산한다.
   즉, $U_M = y_{G_1} \cdots y_{G_{j-1}} y_{G_{j+1}} \cdots y_{G_m} y'''$
2. $U_N = \left(\frac{y'''}{y_{G_j} y''}\right)^{d_N}$를 계산한다.

그룹 관리자는 브로드캐스트 기법을 이용하여 탈퇴 구성원 G_j는 복호화 할 수 없도록 암호화한 $E(U_N)$을 U_M과 함께 공개한다.

각 그룹 구성원은 각자의 개인키를 이용하여 U_N을 복호화 한 후, 자신의 비밀 소속키 U_{G_i}를 $U_{G_i} = U_{G_i} \cdot U_N$로 변경한다. 즉, $i < j$ 일 때

$$U_{G_i} = (y_{G_1} \cdots y_{G_{i-1}} y_{G_{i+1}} \cdots y_{G_m} y'')^{d_N} \cdot (y''' / y_{G_j} y'')^{d_N} = (y_{G_1} \cdots y_{G_{i-1}} y_{G_{i+1}} \cdots y_{G_{j-1}} y_{G_{j+1}} \cdots y_{G_m} y''')^{d_N}$$

각 그룹 구성원은 변경된 U_G을 $(U_G)^{e_N} y_G = U_M$을 통하여 검증한다.

4.4 서명(Sign)

먼저, 그룹 서명에 대해 정의하도록 한다.

■ **정의** 1 ε, l_1, l_2을 $l_2 < \frac{l_g - 2}{\varepsilon} - k, \varepsilon > 1, l_2 < l_1 < l_g$을 만족하는 안전성 매개변수라 하자. 메시지 $m \in \{0,1\}^*$에 대한 그룹 서명은 다음을 만족한다.

$(c, s_1, s_2, s_3, a, b, d, \alpha, \beta) \in \{0,1\}^k$
$\times \{-2^{l_2-\epsilon}, \cdots, 2^{\epsilon(l_2+k)}\}$
$\times \{-2^{l_4+l_2+k}, \cdots, 2^{\epsilon(l_4+l_2+k)}\}$
$\times \{-2^{l_4+k}, \cdots, 2^{\epsilon(l_4+k)}\} \times G^5$

$c = H(g \| h \| y_R \| z \| a \| b \| d \| \beta \| z^c b^{s_1 - c2^{l_1}} / y_R^{s_2}$
$\| a^{s_1 - c2^{l_1}} / g^{s_2} \| a^c g^{s_3} \| d^c g^{s_1 - c2^{l_1}} h^{s_3}$
$\| \beta^c y_R^{s_3} h^{s_3 e_N} \| m)$

■ **Remark 1** 이와 같은 그룹 서명은 다음과 같이 표현될 수 있다.

$L = SPK\{(\theta, \lambda, \mu) : z = b^\theta / y_R^\lambda \wedge 1 = a^\theta / g^\lambda$
$\wedge a = g^\mu \wedge d = g^\theta h^\mu \wedge \beta = Y_R^\mu h^{\mu e_N}$
$\wedge (2^{l_1} - 2^{\epsilon(l_2+k)+1} < \theta < 2^{l_1} + 2^{\epsilon(l_2+k)+1})\}(m)$

L에 대한 비상호 증명 프로토콜은 $y_G = g^{x_G}$와 $x_G \in \{2^{l_1} - 2^{\epsilon(l_2+k)+1}, \cdots, 2^{l_1} + 2^{\epsilon(l_2+k)+1}\}$을 만족하는 정수 x_G와 a의 이산대수 지식에 관한 통계적인 영지식 증명에 기반한다.

$m \in \{0,1\}^*$에 서명하기 위해, 그룹 구성원은 다음과 같은 과정을 수행한다 .

1. 정수 $w \in_R \{0,1\}^{l_R}$을 선택하고, $a = g^w$, $b = y_G y_R^w$, $d = g^{x_G} h^w$, $\alpha = U_G h^w$, $\beta = y_R^w h^{we_N}$을 계산한다.
2. $r_1 \in_R \{0,1\}^{\epsilon(l_2+k)}$, $r_2 \in_R \{0,1\}^{\epsilon(l_4+l_2+k)}$ 그리고 $r_3 \in_R \{0,1\}^{\epsilon(l_4+k)}$을 선택한다.
3. $t_1 = b^{r_1}(1/y_R)^{r_2}$, $t_2 = a^{r_1}(1/g)^{r_2}$, $t_3 = g^{r_1}$, $t_4 = g^{r_1} h^{r_3}$, $t_5 = y_R^{r_1} h^{r_3 e_N}$을 계산한다.
4. $c = H(g \| h \| y_R \| z \| a \| b \| d \| \beta \| t_1 \| t_2 \| t_3 \| t_4 \| t_5 \| m)$를 계산한다.
5. $s_1 = r_1 - c(x_G - 2^{l_1})(\in Z)$, $s_2 = r_2 - cwx_G (\in Z)$, $s_3 = r_3 - cw (\in Z)$.

메시지 m에 대한 서명의 결과는 $(c, s_1, s_2, s_3, a, b, d, \alpha, \beta)$이다.

4.5 서명검증, 구성원 추적, 서명 추적

검증 과정은 [6]에 있는 방법에 덧붙여 서명이 생성될 당시의 그룹 공개 소속키를 이용한 검증 단계를 추가한 것이다. 구성원 추적 과정은 [6]의 방식을 따르고 있다. 서명 추적 과정은 이 논문에서 처음으로 제시하는 새로운 단계로써 주어진 서명에 대해 서명 추적을 통하여 그 서명이 지목된 특정 구성원에 의해 생성되었는지 여부를 판별하는 것이다. 마치 이것은 전자 화폐 시스템에서 코인-추적 과정과 유사하다고 볼 수 있다. 참고로 서명 검증과 서명 추적 프로토콜 수행 시에는 그룹의 공개 소속키 히스토리를 검색하여 서명이 생성된 시점에 사용된 그룹의 공개 소속키를 이용하여야 한다. 이는 서명에 생성날짜를 첨부하고 그룹 소속키 히스토리 테이블을 관리함으로써 해결할 수 있다. 이때 서명의 길이는 여전히 일정하며 테이블을 검색하는데는 테이블 사이즈를 m이라 할 때 $O(\log m)$정도가 걸린다.

■ **서명 검증 :** 주어진 서명에 대해 먼저 정의1을 만족하는지 확인하다. 이를 만족하면 검증자는 서명자가 정당한 멤버쉽 키를 사용하였고, 임의의 수 w를 정직하게 선택하였으며 $\beta = y_R^w h^{we_N}$의 형태로 이루어져 있음을 신뢰할 수 있다. 그 다음 $\left(\frac{U_M}{e_N}\right)\beta = b$이 성립하는지 체크한다. 이 등식이 성립한다는 것은 서명이 정당한 그룹 구성원(즉, 탈퇴하지 않은 현 구성원)에 의해 생성되었다는 것을 의미한다.

■ **구성원 추적 :** 메세지 m에 대해 주어진 서명 $\sigma = (c, s_1, s_2, s_3, a, b, d, \alpha, \beta)$의 서명자를 밝히기 위해서 그룹 신원 관리자는 먼저 서명을 검증한 후 $y_G = b/a^{x_R}$을 계산한다. 구성원 추적 위조 불가능성을 증명하기 위하여 관리자는 $P = SPK\{(\rho) : y_R = g^\rho \wedge b/y_G = a^\rho\}(y_G \| \sigma \| m)$을 생성하고 $\arg = y_G \| P$을 드러낸다. 이 SPK는 y_R와 b/y_G에 대한 두 개의 이산대수가 동일함을 보이는 것이다. 그리고 이는 $y_R (= g^{x_R})$의 이산대수 지식에 관한 통계적 영지식 증명에 기반하고 있다. 관리자는 그룹 구성원 목록에서 y_G와 일치되는 y_G를 검색한다.

■ **서명 추적 :** 서명 $\sigma = (c, s_1, s_2, s_3, a, b, d, \alpha, \beta)$가 특정한 (불법) 구성원에 의해 생성되었는지 여부를 밝히기 위해 그룹 관리자는 $(a, y_G^{d_X}\alpha, \beta)$을 그

룹 신원 관리자에게 전달한다. 이때 y_G는 지적된 특정 구성원의 공개키이다. 그룹 신원 관리자는 $(y_G^{d_N} \cdot \alpha)^{e_N} / (\beta / a^{x_R})$을 계산하고 그 결과가 U_M과 동일한지 체크한다. 만일 이 값이 동일하다면 그 서명이 특정 구성원에 의해 생성되었다고 판단하고 1을 그룹 관리자에게 전송한다. 이때 주어진 서명이 특정 구성원에 의해 생성된 서명이 아니라면 그룹 신원 관리자는 서명이 해당 구성원에 의한 것이 아니라는 사실 이외에 어떠한 정보도 얻을 수 없다.

V. 안전성 분석

이 장에서는 제안된 기법의 안전성에 대해 논한다. 탈퇴하는 구성원이 브로드캐스트 암호화 기법을 통하여 암호화된 그룹의 공개 갱신키를 복호화하는 것이 어렵다는 것은 [1]에 기반한다. 또한, 탈퇴로 인해 그룹의 공개키를 한 번이라도 복호화하지 못한 구성원은 그 이후에 공개되는 그룹의 공개 갱신키를 이용하여 자신의 비밀 소속키를 정당하게 변경하는 것이 불가능함을 알 수 있다. 만일 그룹 구성원이 아니거나 이미 탈퇴한 구성원이 서명을 위조할 수 있다면 이는 RSA 문제를 해결하는 것과 동일한 것임을 다음의 정리를 통하여 보일 것이다.

■ **정리 1** 입력값 y_R, y_G, h, G_M, e_N에 대해 $\beta = y_R^w h^{we_N}$과 $b = y_G y_R^w$인 $(U_M / \alpha^{e_N})\beta = b$를 만족하는 (w, α)를 찾는 확률적인 알고리즘이 존재한다는 것은 이 알고리즘이 RSA 문제를 해결한다는 것과 동치이다.

(증명)

y_R, y_G, h, G_M과 e_N이 주어졌을 때, 확률적인 다항식 시간 알고리즘 A가 $(U_M / \alpha^{e_N})\beta = b$를 만족하는 유효한 (w, α)을 찾아 낼 수 있다고 가정하자. 그러면 우리는 다음을 알수 있다.

$$U_M \beta = b\alpha^{e_N} \quad (1)$$

식 (1)로 부터, 다음 등식을 얻는다.

$$(U_M / y_G)^{1/e_N} = \alpha / h^w \quad (2)$$

즉, 이것은 A가 식 (2)를 만족하는 쌍 (w, α)를 찾아 낼 수 있음을 의미한다. $m \in G$인 m^{e_N}가 주어질 때 식 (2)에서 (U_M / y_G)를 m^{e_N}으로 치환하면 다음과 같다.

$$(m^{e_N})^{1/e_N} = \alpha / h^w \quad (3)$$

그러므로 $m = \alpha / h^w$를 찾을 수 있고 이는 RSA 문제를 풀 수 있다는 것을 의미하고 있다.

역으로, RSA 문제를 풀 수 있는 알고리즘 A'가 존재한다고 하면 $w \in_R G$에 대해 A'는 입력값 쌍 $(U_M \beta / b, e_N)$으로 부터 $U_M \beta / b = \alpha^{e_N}$ 즉, $(U_M / \alpha^{e_N})\beta = b$을 만족하는 α을 생성할 수 있다. □

이제부터 서명 위조 불가능성과 서명 추적 위조 불가능성에 대한 안전성에 대해 설명한다. 그 외의 안전성은 [6]와 동일하므로 여기서는 생략한다.

■ **서명 위조 불가능성 :** 오직 정당한 그룹 구성원만이 그룹 신원 관리자에 의해 구성원 추적 및 서명 추적이 가능한 합법적인 서명을 생성할 수 있다. (가정 2에 기반하여, 군의 위수를 알지 못하는 누군가가 정당한 멤버쉽 키를 생성해 내기는 어렵다. 그러므로 오직 그룹 관리자와 함께 하는 가입 프로토콜을 통해서만 그룹의 구성원이 될 수 있다. 더 나아가서 그룹 신원 관리자는 그의 비밀키를 이용하여 서명의 (a, b)를 복호화하고 $y_G = b / a^{x_R}$을 계산함으로써 서명자의 공개키를 밝혀 낼 수 있다.[6]) 또한, 정리 1로부터 그룹을 탈퇴한 과거의 구성원이 정당한 서명을 생성해 내는 것은 RSA 문제를 푸는 것과 동치임을 알 수 있다.

■ **서명 추적 위조 불가능성 :** 주어진 $(a, y_G^{d_N} \alpha, \beta)$에 대해 그룹 신원 관리자가 그룹 관리자에게 1을 전달한다면, 그룹 관리자는 $\alpha^{e_N} b / U_M \beta$을 계산함으로써 위조 여부를 쉽게 판별할 수 있다. 이 계산 값이 1이라면 이는 그룹 신원 관리자가 정확하게 추적 과정을 수행하였음을 의미하는 것이다.

VI. 결 론

그룹 서명 기법에서 구성원 탈퇴에 관한 복잡도는 그룹 서명을 실제로 적용하는데 큰 장애물이 되어왔다. 이 논문에서 보다 효율적으로 구성원 탈퇴가 가능한 그룹 서명 기법을 제안하였다. 이 기법은 탈퇴

인원수가 제한되는 [1]의 브로드캐스트 기법을 이용하고 있음에도 불구하고 탈퇴 인원수에 제한이 없는 그룹 서명 기법을 구성하였다. 이 기법은 [6]에서 제안된 기법의 확장으로 볼 수 있다. 그룹의 공개키나 서명의 크기는 구성원 수나 탈퇴 인원수와 무관하게 일정하며 효율적인 방법이다.

그러나 제안한 방식은 [6]에 기반하고 있으며 다른 그룹 서명 기법에는 확장 적용되지 않는다. 또한 각 서명마다 서명 일자가 있어야 하고 그룹 공개키 히스토리 관리가 요구되어 진다. 따라서 향후 연구 방향은 좀 더 실용적이고 일반적이면서 구성원 탈퇴가 자유로운 그룹 서명 기법에 대한 연구일 것이다.

참 고 문 헌

[1] J. Anzai, N. Matsuzaki and T. Matsumoto, "A Quick Group Key Distribution Scheme with Entity Revocation", *Proc. Advances in Cryptology - ASIACRYPT '99*, Vol. 1716 of Lecture Notes in Computer Science, pp. 333~347, Springer Verlag, 1999.

[2] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme", *Proc. Advances in Cryptology - CRYPTO 2000*, Vol. 1880 of Lecture Notes in Computer Science, pp. 255~270, Springer Verlag, 2000.

[3] G. Ateniese and G. Tsudik, "Group signatures a la carte", In *ACM Symposium on Discrete Algorithms*, 1999.

[4] E. Bresson and J. Stern, "Efficient Revocation Group signatures", In PKC 2001, Vol. 1992 of Lecture Notes in Computer Science, pp. 190~206, 2001.

[5] J. Camenisch, "Efficient and generalized group signatures", In W. Fumy, editor, *Advances in Cryptology - EUROCRYPT '97*, Vol. 1233 of Lecture Notes in Computer Science, pp. 465~479, Springer Verlag, 1997.

[6] J. Camenisch and M. Michels, "A group signature scheme based on an RSA-variant", Tech. Rep. RS-98-27, BRICS, Dept. of Comp. Sci., University of Arhus, preliminary version in *Advances in Cryptology - ASIACRYPT '98*, Vol. 1514 of Lecture Notes in Computer Science, Springer Verlag, 1998.

[7] J. Camenisch and M. Michels, "Proving in zero-knowledge that a number is the product of two safe primes", In *Advances in Cryptology - EUROCRYPT '99*, Vol. 1592 of Lecture Notes in Computer Science, pp. 107~122, Springer Verlag, 1999.

[8] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups", In *Advances in Cryptology - CRYPTO '97*, Vol. 1296 of Lecture Notes in Computer Science, pp. 410~424, Springer Verlag, 1997.

[9] D. Chaum, and E. van Heyst, "Group Signatures", *Proc. Advances in Cryptology - EUROCRYPT '91*, Vol. 547 of Lecture Notes in Computer Science, pp. 257~265, Springer Verlag, 1991.

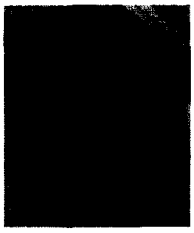
[10] L. Chen and T. P. Pedersen, "New group signature schemes", In A. De Santis, editor, *Advances in Cryptology - EUROCRYPT '94*, Vol. 950 of Lecture Notes in Computer Science, pp. 171~181, Springer Verlag, 1995.

[11] E. Fujisaki and T. Okamoto, "Statistical zero knowledge protocols to prove modular polynomial relations", In B. Kaliski, editor, *Advances in Cryptology - CRYPTO '97*, Vol. 1294 of Lecture Notes in Computer Science, pp. 16~30, Springer Verlag, 1997.

[12] H. Petersen, "How to convert any digital signature scheme into a group signature scheme", In M. Lomas and S. Vaudenay, editors, *Security Protocols Workshop*, Paris, 1997.

[13] A. Shamir, "On the generation of cryptographically strong pseudorandom sequences", In *ACM Transaction on Computer Systems*, Vol. 1, pp. 38-44, 1998.

〈著者紹介〉



김 현 정 (Hyun-Jeong Kim) 학생회원
1994년 2월 : 경희대학교 수학과 졸업
1994년 1월~1999년 12월 : 삼성SDS 근무
1999년 9월~2001년 8월 : 고려대학교 수학과 석사
2001년 9월~현재 : 고려대학교 정보보호 대학원 박사과정
〈관심분야〉 암호이론, 암호 프로토콜, 정보은닉

임 종 인 (Jong-In Lim) 정회원
1980년 : 고려대학교 수학과 졸업
1982년 : 고려대학교 수학과 석사
1986년 : 고려대학교 수학과 박사
1986년~현재 : 고려대학교 수학과 교수
2000년~현재 : 고려대학교 정보보호 대학원 원장
〈관심분야〉 암호이론, 암호 프로토콜, 정보이론

이 동 훈 (Dong Hoon Lee) 정회원
1984년 : 고려대학교 경제학과 졸업
1987년 : Oklahoma Univ. 전산학과 석사
1992년 : Oklahoma Univ. 전산학과 박사
1993년~현재 : 고려대학교 전산학과 교수
2000년~현재 : 고려대학교 정보보호 대학원 교수
〈관심분야〉 암호이론, 암호 프로토콜, 정보이론