[UCI]I804:24011-200000232903

*2006*년 *8*월

박사학위논문

모바일 환경에서 *Fiat-Shamir*방식을 적용한 안전한 그룹키 갱신 메커니즘

조선대학교 대학원

전자계산학과

탁 동 길

모바일 환경에서 *Fiat-Shamir* 방식을 적용한 안전한 그룹키 갱신 메커니즘

A Secure Renewal Mechanism of Group Key Employing the Fiat-Shamir Method on Mobile Environment

*2006*년 *8*월 일

조선대학교 대학원

전자계산학과

탁 동 길

모바일 환경에서 *Fiat-Shamir* 방식을 적용한 안전한 그룹키 갱신 메커니즘

지도교수 정 일 용

이 논문을 이학박사학위신청 논문으로 제출함.

*2006*년 *4*월 일

조선대학교 대학원

전자계산학과

탁 동 길

탁동길의 박사학위논문을 인준함

위원장 조선대학교 교수 _____ 인

위 원 광주대학교 교수 _____ 인

위 원 조선대학교 교수 _____ 인

위 원 조선대학교 교수 _____ 인

위 원 조선대학교 교수 _____ 인

*2006*년 *6*월 일

조선대학교 대학원

목 차

Ⅰ. 서 론 ····· 1

A. 연구배경 및 목적 ····· 1

B. 연구 내용 및 구성 ····· 4

Ⅱ. 키 분배 방식 및 보안시스템을 위한 기반 기술 ····· 6

A. 디지털 이동 통신망의 기본 구성 ····· 6

B. 키분배 방식 ····· 9

C. 키분배 프로토콜 공격 유형 ····· 11

D. 안전한 그룹키 분배 및 갱신 프로토콜 설계시 요구사항 ····· 16

E. 보안시스템을 위한 기반기술 ····· 21

Ⅲ. 그룹 키 분배 및 갱신 프로토콜 설계 ····· 27

A. 기존 그룹키 갱신 프로토콜 ····· 27

B. 새로운 그룹 키 갱신 방식의 제안 ····· 39

C. 제안 방식의 안전성 검토 ····· 49

Ⅳ. 실험 및 평가 ····· 52

A. 기존 프로토콜과의 비교 분석 ····· 52

B. 각 방식별 비교 분석 결과 ····· 53

Ⅴ. 결론 및 향후 연구 ····· 61

참 고 문 헌 ····· 63

그림 목차

[그림 2.1] 디지털 이동 통신망의 시스템 구성도 ····· 8

[그림 2.2] 키분배 프로토콜에 대한 공격들 ····· 12

[그림 2.3] 디지털 서명(Digital signature) ····· 22

[그림 3.1] 대칭키 그룹키 분배 ····· 27

[그림 3.2] 비대칭키 그룹키 분배 방식 ····· 28

[그림 3.3] MA 방식 (그룹 비밀키 준비단계) ····· 29

[그림 3.4] MA방식 (그룹 비밀키 갱신단계) ····· 31

[그림 3.5] SPW 방식 (그룹 비밀키 준비단계) ····· 33

[그림 3.6] SPW 방식 (그룹 비밀키 갱신단계) ····· 34

[그림 3.7] PL 방식 (그룹 비밀키 준비단계) ····· 36

[그림 3.8] PL 방식 (그룹 비밀키 갱신단계) ····· 37

[그림 3.9] 제안된 그룹키 방식 (키분배 센터 준비단계 1) ····· 41

[그림 3.10] 제안된 그룹키 방식 (키분배 센터 준비단계 2) ····· 42

[그림 3.11] 제안된 그룹키 방식 (키분배 터미널 준비단계) ····· 43

[그림 3.12] 제안된 그룹키 방식 (키분배 터미널 갱신 준비단계 1) ····· 44

[그림 3.13] 제안된 그룹키 방식 (키분배 터미널 갱신 준비단계 2) ····· 45

[그림 3.14] 제안된 그룹키 방식 (키분배 터미널 갱신 준비단계 3) ····· 45

[그림 3.15] 제안된 그룹키 방식 (키분배 터미널 갱신단계) ····· 46

[그림 3.16] 제안된 그룹키 방식 (단말기 확인단계 1) ····· 47

[그림 3.17] 제안된 그룹키 방식 (단말기 확인단계 2) ····· 48

[그림 3.18] 제안된 그룹키 방식 (센터 최종 단말기 확인단계 3) ····· 49

[그림 4.1] MA 방식 그룹키 갱신 준비단계 ····· 53

[그림 4.2] MA 방식 그룹키 갱신 단계 (단말기 2 배제) ····· 54
[그림 4.3] MA방식 (단말기 4 배제 후 배제된 단말기 2 그룹키 갱신발생) ····· 54
[그림 4.4] SPW 방식 (그룹키 갱신 Center 준비단계) ····· 55
[그림 4.5] SPW 방식 (그룹키 갱신 단말기 준비단계) ····· 55
[그림 4.6] SPW 방식 (그룹키 갱신 단말기 3 배제) ····· 56
[그림 4.7] SPW 방식 (단말기 5 배제 후 배제된 단말기 3 그룹키 갱신발생) ··· 56
[그림 4.8] 제안된 그룹키 갱신 준비단계 ····· 57
[그림 4.9] 제안된 그룹키 갱신단계(단말기 2 배제) ····· 57
[그림 4.10] 제안된 그룹키 갱신(단말기 2,4 연속 배제) ····· 58
[그림 4.11] 제안된 그룹키 갱신(단말기 2,4,5 연속 배제) ····· 58
[그림 4.12] 각 방식별 통신횟수와 통신량 (준비단계) ····· 59
[그림 4.13] 각 방식별 통신횟수와 통신량 (갱신단계) ····· 59
[그림 4.14] 각 방식별 비교 분석 결과 ····· 60

표 목 차

[표 2.1] I_i 의 조건 ····· 25

[표 3.1] MA 방식 (시스템 계수) ····· 30

[표 3.2] SPW 방식 (시스템 계수) ····· 32

[표 3.3] PL 방식 (시스템 계수) ····· 36

[표 3.4] 제안된 그룹키 갱신 방식 (시스템 계수) ····· 40

ABSTRACT

A Secure Renewal Mechanism of Group Key Employing the Fiat-Shamir on Mobile Environment

Dong-Kil Tak

Advisor : Prof. Il-Yong Chung, Ph.D.

Department of Computer Science,

Graduate School of Chosun University

The number of remote, computer-based conferences have been increasing, and the supply of mobile terminals and the use of Mobile Radio Communication have been increasing in an alarming way. Simultaneously, the requirement for securing safe communication channels also has been steadily increasing . In order to protect the terminals from the illegal use, technologies that keep off the surreptitious use of conversation and protect the legal terminal by utilizing formal identification have been developed. In this paper, we proposed an improved scheme for renewing and distributing a group key in order to secure the safety of the remote conferences and digital mobile communication

systems. It is a security service based on the group key which is necessary for encryption and authentication. It is an efficient and safe scheme for renewing and distributing a group key by using a digital signature and a key distribution scheme based on a secure ID technique.

The proposed protocol is so designed as to create a new secret key within the group when the center wants to renew the group key for any reason, when the terminal losses the group key or the secret information, when any user losses their terminal, or when the center wants to exclude specific terminals from the security service.

For example, in the case of excluding a specific terminal from the group, the protocol must be able to keep off illegal tapping or the surreptitious use of the conversation from the excluded terminal. Therefore, in this case, the key distribution center must re-share the group key as fast as possible and must make normal communication possible and must have no influence upon the existing communication and must prevent the excluded terminal from intercepting the new group key when re-sharing it. The proposed protocol can keep off the illegal change of the transmission information and illegal key renewal because it employs the safety scheme based on the ID-based key distribution scheme and Fiat-Shamir's digital signature. In particular, while the existing scheme can be disclosed to the various attacks, our protocol can cope with them because it adds a digital signature. Also it can prevent the transmission information from being changed or can verify the authority of the digital

signature of the center that this information is transmitted by the key distribution center.

The proposed protocol doesn't have more distinguished advantages about an amount of computation and the number of communications than the existing one. However, it can be effectively managed even if the terminals have small storage capacity and computing power, and can consecutively renew the group key more than two times. Even if many terminals are simultaneously excluded from the group, the center can reflect the various changes and can create the secret information in a lump and can handle the various changes at once. It can easily renew the group key when it intends to alter the group key without the change of terminals.

Ⅰ. 서 론

A. 연구배경 및 목적

이동 무선통신의 시스템의 발전으로 인한 정보 통신망은 새로운 형태의 디지털 정보사회를 만들어가고 있다. 이는 인간 문명 전반에 획기적인 변환의 시대로 현대 사회의 정보화 현상은 산업구조 및 사회 일반에 광범위한 컴퓨터의 보급 확산과 통신 서비스의 발전을 통해 확대되고 있다. 이러한 서비스의 발전은 인간 친화적인 정보기기를 구성하기 위한 것으로서 휴대성과 편의성을 개선시키기 위하여 언제, 어디서나 컴퓨팅을 실현할 수 있어야 하며, 항시 들고 다닐 수 있을 정도의 소형 컴퓨팅 기기를 통하여 유비쿼터스(Ubiquitous) 컴퓨팅 서비스를 제공할 수 있으며, 컴퓨팅 기능이 주위환경에 내재되어 이로부터 정보를 획득하여 활용하거나 사용자가 인식하지 못하는 상태에서도 컴퓨팅 기능을 수행할 수 있는 기술이 되고 있는 실정이다. 이러한 기술은 그 응용분야도 급속히 확대되고 있는 분야로 이동통신의 휴대성으로 인한 개인성과 인터넷 서비스의 폭발적 요구로 인해 여러 단체나 기업에서는 무선 인터넷 표준안들을 제시하고 있다. 에릭슨, 노키아 등이 주도하는 WAP(Wireless Application Protocol), 마이크로소프트사의 ME(Mobile Explorer), SUN의 J2ME(Java2 Micro Edition) 등이 바로 그것이다. 이러한 무선 인터넷을 위한 표준들은 기존의 음성 서비스에 국한되지 않고 좀더 고급 서비스들을 제공하여 사용자들의 욕구를 충족시키고 있는데 전 국민의 70%가 이동전화에 가입하고, 초고속 인터넷 가입자가 1천만 명을 돌파함으로써 IT 강국으로서 손색이 없는 수준의 정보통신 인프라를 확보하게 되었다. 그리고 무선 LAN (WLAN)의 대중화로 정지 및 이동 중에 언제 어디서나 저렴한 가격으로 고속의 인터넷 접속 서비스를 제공받고 싶은 욕구가 자연스럽게 표출되고 있다.

이동통신환경은 아날로그 셀룰러 이동 통신 서비스단계로 음성통화 위주의 1세

대, 디지털 셀룰러 이동통신 서비스 단계로 음성위주의 서비스와 저속의 데이터 통신을 제공하는 2세대, 유럽의 UMT와 미국의 IMT-2000 에 해당하는 것으로 고속의 데이터 통신 멀티미디어 서비스 및 다양한 응용분야를 제공하는 3세대 그리고 향후 2010년 대비, 고속데이터수용 및 대용량, 신규 서비스에 대한 유연한 수용등을 목표로 하고 있는 4세대 이동 통신은 현재 이동통신망 및 인터넷 망을 통합하여 음성, 동영상 및 인터넷 서비스 등을 포함한 광대역 멀티미디어 서비스를 제공하기에 이르렀다. 이동 통신망의 전송매체는 대기 중에서 이루어지므로 근본적으로 정보 보호 면에서 취약하여 유선을 이용하는 통신에 비해 정보의 유출, 불법 수정 등이 용이하다. 이러한 점을 개선하기 위해서는 암호를 사용하는 것이 안전하고 효율적으로 알려져 있다[9,15,36,40].

아날로그 방식을 사용하는 1세대 통신은 도청 등에 의한 정보의 유출이 발생하기가 용이하였다. 2세대 통신에서는 디지털 이동통신을 사용하였는데 1세대 통신의 채널의 보안성 문제를 해결하고, 사용자 인증 및 키 분배를 위하여 주로 대칭암호 시스템을 사용하였다. 그러나 대칭암호 시스템은 공개키 암호 방식에 비해 계산량이 적다는 장점이 있으나, 인증 및 키 분배시 항상 홈 인증 센터를 필요로 하며, 부인봉쇄 서비스를 위한 디지털 서명을 제공하기가 용이하지 않다. 이에 반해 공개키 암호 방식은 온라인 서버를 필요로 하지 않으며, 이동 통신환경에서의 전자상거래를 위한 서명을 제공하기가 용이하여 이동통신 환경에서의 암호 시스템으로 사용된다. 이동 단말기의 보급 증대와 이동 무선통신의 확대로 컴퓨터를 이용한 원격회의의 증가 및 이동 단말기의 보급 증대와 이동 무선통신의 확대로 인한 통화 참여자간의 안전한 통신채널의 확보가 요구되고 있는 실정에서 불법 도청과 침해, 이동통신 시스템에서의 복제 단말기를 이용한 통화 도용이나 도청 등이 증가하고 있는 추세이다. 이에 디지털 이동통신 시스템의 대표적인 시큐리티 서비스로 가입자의 단말기 복제 등으로 인한 불법 위조 사용을 방지하기 위한 인증기술, 무선통화 내용을 불법적인 도청으로부터 보호하기 위한 암호기술 그리고 통신 상대방 또는 그룹내의 비밀키 공유를 위한 키 공유나 분배 기술이 다루어져 왔으며 많은

연구가 이루어지고 있으며 이러한 불법적 사용으로부터 통화자를 보호하기 위하여 인증 절차를 통한 통화 도용을 막고 정당한 통화자를 보호하려는 기술들이 개발되고 있는데 미국의 CDMA(Code Division Multiple Access)방식이나 유럽의 GSM(Global System for Mobile Communication)등의 이동 통신 표준 방식에서는 이미 인증을 포함한 보안 서비스를 권고하여 사용 중이다[8,22].

본 논문에서는 디지털 이동 통신 시스템에서 한정된 그룹내의 단말기 분실 또는 단말기의 비밀 정보 유출에 의한 도청이나 통신 도용과 같은 경우를 예방하기 위해서 특정 단말기를 배제하고 신속하게 그룹 비밀키를 갱신할 수 있으며 또한 계속적으로 안전하게 사용할 수 있는 효율적인 그룹 비밀키 갱신 방식을 제안한다.

B. 연구 내용 및 구성

급속한 네트워크 발전으로 이동통신을 통해서 각종 정보를 공유하는 일들이 많아지고 있다. 특히, 화상회의(Video Conference), 공동 작업장(Collaborative Workspaces), 쌍방향 대화(Interactive Chat), 온라인 게임(On-line Games)등과 같은 그룹단위 응용프로그램(Group-oriented Applications)들의 사용빈도는 점점 증가하고 있다. 이에 따라, 여러 가지 그룹단위 응용프로그램들은 그룹 구성원들이 안전하게 송수신할 수 있는 통신 서비스를 제공해야 하며, 그룹에 속해 있지 않은 멤버는 특정 그룹에 제공되는 정보를 얻지 못하도록 해야 한다. 이를 안전한 그룹통신(Secure Group Communication)이라고 하며, 이는 그룹에 속하지 않는 사람들에게는 정보를 유출하지 않고 그룹 구성원들에게만 안전하면서도 비밀스러운 서비스를 받을 수 있도록 보장하는 것이다[34].

일반적으로 이동 통신 시스템은 그룹 내에 속하는 모든 단말기의 통신을 제어하는 일종의 센터로 구성된 스타형 네트워크를 이루고 있다. 암호 기능을 제공할 경우, 센터와 단말기 간에 비밀리에 사전 분배된 그룹 비밀 키를 이용하여 모든 정보를 암호화하여 동시에 모든 단말기들에 동보 전송하여 특정 그룹 내에서 무선 암호 통신을 수행하고 있다[29]. 그러나 이동 통신에서 신호 교환은 무선 채널을 통해서 대기 중에 수행되므로, 도청이나 그 밖의 신뢰하지 못할 요소들로부터 위조나 불법적인 변경들과 같은 위협들에 대해서는 취약성을 갖고 있다. 또한 무선 단말기의 분실이나 무선 단말기의 비밀 정보 불법적인 취득은 그룹 소속 단말기들의 공유 정보 노출뿐만 아니라 불법적인 시스템의 사용을 야기 시킨다[35]. 따라서 그룹에 가입한 사용자를 제외한 다른 불법적인 사용자들로부터 기밀성과 안전성을 확보하기 위한 암호화 시스템이 활발하게 연구되고 있다. 그러나 특정 그룹 간 비밀 키 공유로 인한 암호화 통신 기법은 널리 알려져 있으나, 특정 그룹 간에 공유하여 사용되고 있는 그룹 비밀 키의 변경이 필요한 경우에 대한 연구는 많이 알려져 있지 않다[29,41].

본 논문의 제안 방식에서는 회의장 등과 같이 특정한 공간에서 소규모 그룹회의를 고려한 쉬운 키 생성과 갱신을 위주로 오직 사전에 허가된 사용자만이 그룹키를 이용하여 디지털 정보를 얻을 수 있게 하며 사용자가 탈퇴나 새로운 가입 시에 효율적인 키 캥신을 제안한다. 이는 그룹 내의 특정 단말기 또는 불법 단말기를 배제하고자 할 경우, 예를 들어서 단말기의 분실 및 단말기의 비밀 정보의 불법적인 유출로 인한 도청이나 통신 도용과 같은 경우를 방지하기 위해서는 센터는 가능한 빨리 도청이나 통신 도용을 감지하고 신속하게 분실 단말기나 비밀 정보 유출 단말기를 제외한 다른 모든 단말기의 그룹 비밀 키를 갱신해야 한다. 이러한 갱신은 일반 통신에 영향을 미치지 않으면서 신속하게 이루어져야 한다. 또한 분실 단말기나 비밀 정보 유출 단말기들이 갱신 시 또는 갱신 이후로는 결코 그룹 비밀 키를 알 수 없게 해야 한다. 본 연구에서는 이러한 조건에 합당하면서 기존 그룹 키 갱신 방법들의 문제점을 해결할 수 있는 효율적인 그룹 비밀 키 갱신 방식을 제안하였다.

본 논문은 II장에서 디지털 이동통신의 환경 및 키 분배 방식 및 보안 시스템을 위한 기반 기술 그리고 기존 연구들에서 제안된 그룹 비밀 키 분배 및 갱신 방식들에 대해서 살펴본다. III장에서는 본 연구가 제안하고자하는 그룹 비밀 키 갱신 방식 및 특정 단말기를 배제하고 그룹 비밀 키를 갱신하여 그룹 비밀 키를 재공유하는 절차 및 불법 단말기의 확인을 위한 절차 등을 제안한다. Ⅳ 장에서는 제안 방식의 안전성 분석 및 기존 방식들과 비교 평가 하고 제안 방식의 장점을 분석 기술하였다. V장에서 결론 및 향후 연구과제에 대하여 논하였다.

Ⅱ. 키 분배 방식 및 보안시스템을 위한 기반 기술

A. 디지털 이동 통신망의 기본 구성

디지털 이동 통신망의 기본 장치별 구성은 이동통신 교환국(MSC), 홈스위치 등록 레지스터(HLR),게이트웨이 이동 교환국(GMSC), 기지국(BS), 이동국(MS), 방문 위치 등록 레지스터(VLR), 운용 보전국(OMC)등으로 각각의 기능은 다음과 같다.

1. 이동통신 교환국(MSC : Mobile Switching Center)

고정 전화망과 연동(Interworking)하여 이동통신 가입자들에게 회선교환서비스를 제공하며, 무선자원의 관리, 이동국의 위치를 추적하여 항상 서비스가 가능하도록 하는 기능과 통화중 이동국이 이동하더라도 통화를 지속시켜주는 기능(Handover)을 수행한다.

2. 홈스위치 등록 레지스터(HLR : Home Location Register)

이동단말기를 계약할 때에 가입자 데이터를 보존하고, 그 단말기의 위치 관리를 행하는 홈로케이션 레지스터로 이동국에서 셀을 연결시켜 주거나, 그 밖의 이동통신 서비스를 제공하기위하여 필요한 이동국의 모든 영구적인 정보를 저장하고 있는 데이터베이스이다. HLR이 저장하고 있는 정보 가운데 가장 중요한 정보는 이동국의 현재 위치에 대한 정보이다.

3. 게이트웨이 이동 교환국(GMSC : Gateway Mobile Switching Center)

이동 통신망와는 다른 공중전화망(PSTN) 등의 고정된 네트워크와의 상호 접속 접속을 행한다.

4. 기지국(BS : Base Station)

무선과 유선 네트워크의 인터페이스를 갖는 무선기지국으로 이동 통신시스템에서는 무선채널의 효율적인 이용을 위하여, 커다란 지역을 셀이라는 작은 지역으로 나눈 뒤 하나 혹은 그 이상의 셀에 기지국을 두고, 기지국으로 하여금 이동국과의 무선통신을 담당하게 한다. 따라서 기지국은 자신이 관할하는 셀 내에 있는 이동국에서 발신한 신호를 무선채널로 수신하여 이동통신 교환국으로 전송하고, 역으로 이동국으로 보내기 위하여 이동통신 교환국으로부터 오는 신호를 무선 채널을 통하여 이동국에 송신하는 기능을 담당한다.

5. 이동국(MS : Mobile station)

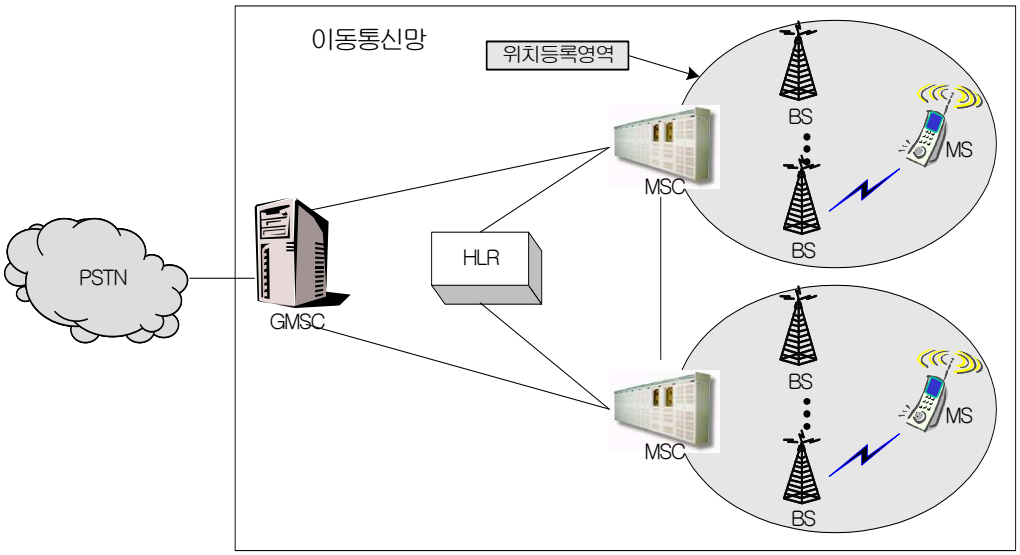
가입자 쪽 종단에 위치한 무선 인터페이스로써, 가입자에게 서비스를 제공하기 위한 단말기 기능이 포함된다.

6. 방문 위치 등록 레지스터(VLR : Visitor Location Register)

이동국이 관할 지역에 들어 왔을 때, 그 이동국에 대한 가입자 정보를 일시적으로 저장하는 데이터베이스이다. 대부분의 정보는 위치 등록시 HLR로부터 전송되어 보관되므로, HLR에 대한 부분 중복 로컬 데이터베이스(Partically Replicated Local Database)의 역할을 한다. 따라서 공중 육상 이동 통신망내의 각 구성 요소들이 이동국에 대한 정보를 요구할 때 마다 HLR에 질의하는 것을 피할 수 있게 한다.

7. 운용 보전국(OMC : Operation and Maintenance Center)

공중 육상 이동 통신망내의 각 요소를 운용하고 유지 보전하는 기능을 갖고 있으며, 모든 요소와 연결되어 있다. OMC는 무선 부문을 담당하는 OMCR과 교환 부분을 담당하는 OMCS로 나눌 수 있다.



[그림 2.1] 디지털 이동 통신망의 시스템 구성도

일반적으로 하나의 MSC(Mobile Switching Center)에는 복수의 BS(Base Station)가 접속되고, 각각의 BS의 전파가 도달하는 범위가 그 MSC의 '서비스 영역'이 된다. 또 각각의 MSC 서비스 영역을 합친 전체를 '오퍼레이터가 통신 서비스를 제공하는 영역'이라고 한다. 이와 같은 네트워크의 구성 중에서 이동 단말기의 위치는 '위치등록 영역'이라고 하는 범위를 단위로 하여 인식된다.

본 연구에서는 [그림 2.1]과 같이 기지국(BS)과 단말기(MS)들 간에 그룹 비밀키 분배 및 갱신 방식에 관해서 다룬다.

B. 키분배 방식

1. 키 분배 프로토콜

a. Diffie-Hellman의 키 분배 방식

Diffie-Hellman은 1976년 유명한 공개키 암호 논문에서 공개키 암호의 원리와 함께 현재 Diffie-Hellman 키 분배 (Diffie-Hellman Key-Distribution)이라는 키 분배 방식을 발표했다[24]. 이 방식은 도청의 가능성이 있는 통신로를 통해서 A와 B가 암호화 키를 비밀로 공유할 수 있는 방식을 이산대수 문제를 이용하여 실현하였다.

(1) 키 분배 절차

[파라메터 생성] 시스템은 소수 p를 생성하고 GF(p)의 원시근 g를 구하여, 이런 값들을 시스템 공통의 파라메터로 공개한다.

다음의 절차에 의해 도청되어도 무방한 통신로를 사용하여 이용자 A와 이용자 B간에 키를 공유한다.

- 시스템의 공개 정보 : 소수 p 및 원시근 g
- A의 비밀키 : x_A
- B의 비밀키 : x_B

[$A \rightarrow B$] A는 $y_A \equiv g^{x_A} \bmod p$ 를 계산하여 y_A를 B에게 보낸다.

[$B \rightarrow A$] B는 $y_B \equiv g^{x_B} \bmod p$ 를 계산하여 y_B를 A에게 보낸다.

[A] A는 $K_{AB} \equiv g^{x_A x_B} \bmod p$

$\equiv y_B^{x_A} \bmod p$ 를 계산하여 B 와의 공통키로 한다.

[B] B는 $K_{AB} \equiv g^{x_A x_B} \bmod p$

$\equiv y_A^{x_B} \bmod p$ 를 계산하여 A 와의 공통키로 한다.

A, B는 모두 공통키 K_{AB}를 얻어 A, B사이에서의 키의 공유가 가능하게 된다.

b. ID를 이용한 키 분배

Okamoto는 Diffie-Hellman의 키 분배 방식을 변형시켜 ID를 이용한 키분배 방식으로 제안하였다[26].

(1) 키 발급 절차

키 발급센터는 다음과 같은 키를 생성한다.

① 두 개의 소수 p, q를 랜덤하게 생성하여 $N = p \cdot q$를 만든다.

② $\Phi(N) = (p-1)(q-1)$ 이다.

③ $\gcd(e, \Phi(N)) = 1$과 $ed = 1 \bmod \Phi(N)$인 d를 계산한다.

④ GF(p)와 GF(q)의 원시근 g를 구한다.

⑤ 각 통화자 j는 자신의 개인 식별 정보 ID_j를 키 발급센터에 등록하고 키 발급센터로부터 $V_j = ID_j^{\,d} \bmod N$ 을 계산하여 받는다.

⑥ 키 발급센터는 N, e, g, ID_j 값을 모든 고용자에게 공개하고, V_j는 통화자 j만 보유하며, p, q는 center만 보유한다.

(2) 세션키 공유

위에서 생성된 키를 사용하여 A와 B는 다음과 같이 키를 공유한다.

① A는 랜덤한 수 k_A를 임의로 선택하여,

$C_A \equiv V_A \cdot g^{k_A} \bmod N$ 을 B에게 보낸다.

② B는 랜덤한 수 k_B를 임의로 선택하여,

$C_B \equiv V_B \cdot g^{k_B} \bmod N$을 A에게 보낸다.

③ B는 $y \equiv (C_A^e / ID_A)^{k_B} \bmod N \equiv g^{e \cdot k_A \cdot k_B} \bmod N$

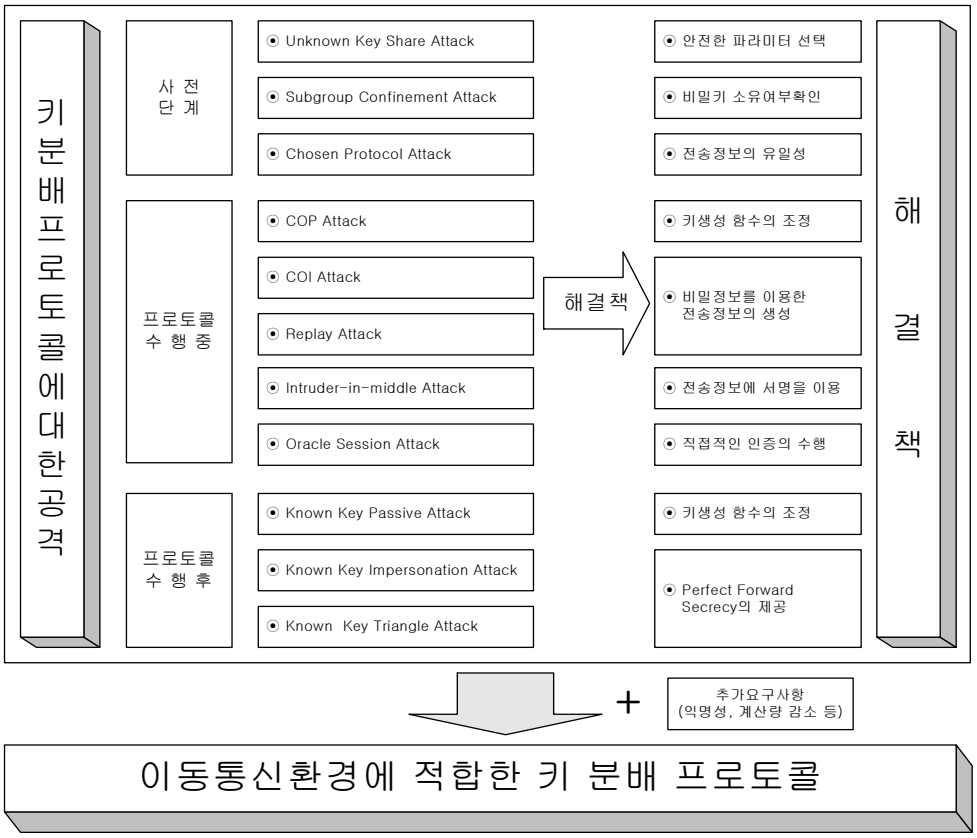
④ A도 같은 방법으로 $g^{e \cdot k_A \cdot k_B}$를 얻는다.

⑤ A와 B는 $g^{e \cdot k_A \cdot k_B}$를 공유키로 한다.

위의 방식은 통화자 j가 비밀키 파라메터 k_j를 center를 통하지 않고 쉽게 변경할 수 있으며, 또한 키 발급센터 조차도 각 통화자 A와 B간의 공유키를 알 수 없는 특징을 갖는다.

C. 키분배 프로토콜 공격 유형

프로토콜의 기반이 되는 수학적 문제들의 안전성이 보장되고, 공개 파라미터들의 안전한 선택이 이루어져도 프로토콜의 설계방식에 따라 다양한 형태의 공격 방법이 존재하게 된다. 즉, 키분배 프로토콜의 안전성은 프로토콜의 설계방식에 크게 의존한다[32].



[그림 2.2] 키분배 프로토콜에 대한 공격들

프로토콜에 대한 공격은 공격자들이 취득할 수 있는 정보 및 그들의 공격형태에 따라 다양한 공격이 있다. [그림 2.2]는 키분배 프로토콜들에 대한 공격방법을 공격 시점에 따라, 사전단계, 프로토콜 수행중, 프로토콜 수행후로 분류하고, 각 시점에 따라 해결책을 제시한 것이다. 키분배 프로토콜의 안전성은 공격자들이 취득할 수 있는 정보 및 그들의 공격형태에 따라 여러 가지로 분류할 수 있다.

1. 사전 단계에 가능한 공격

a. Unknown key share 공격

Unknown key share 공격은 공격자가 공격을 수행한 결과, 사용자는 공격자와

정당한 프로토콜을 수행한 것으로 믿도록 인증만을 속이며, 실제로는 정당한 사용자와 세션키를 생성하고 공격자는 생성된 세션키를 모르므로 Unknown key share 공격이라고 부른다. 이 공격은 크게 공격자가 사용자들의 공개키를 자신의 공개키로 등록하는 경우와 다른 사용자들의 공개키를 변형하는 경우로 나눌 수 있다 [3,20,25].

두 가지 경우 모두 공격자가 전송정보중의 사용자들의 인증서를 치환함으로써 발생한다. 따라서 이를 막기 위해서는 공격자는 세션키를 생성할 수 없다는 점을 이용해서 사용자들이 자신의 인증서와 세션키의 해쉬값을 전송정보에 포함시켜 세션키를 모르는 공격자가 사용자들의 인증서를 바꿀 수 없도록 함으로써 막을 수 있다.

b. Subgroup confinement 공격

잘못된 공개 파라미터의 선택에 의해서 발생하는 공격으로 암호 프로토콜 설계시 많이 이용되는 수학문제인 이산대수 문제를 사용하는 키분배 프로토콜에 적용될 수 있는 공격으로, 소수의 형태에 따라 Z_p^* 상에서 작은 크기의 위수를 갖는 원시 원소들이 있으며, 이 원소들은 각기 작은 서브 그룹들을 만들고, 공격자들은 그러한 서브 그룹상에서 이산대수문제를 쉽게 풀 수 있다는 성질을 이용한다. 이러한 서브 그룹을 이용하는 공격의 형태는 다양하게 존재하며, 키분배 프로토콜의설계시 중요하게 고려되어야 한다[5].

이러한 공격을 막기 위해서는 공격자가 서브 그룹을 이용하는 것을 막기 위해서는 모듈러 p의 형태를 p-1이 작은 소수들만의 곱들로 이루어지지 않도록 p를 선택함으로써 공격자가 이산대수문제를 풀 수 없도록 하는 방법과 큰 소수 위수를 갖는 기저를 선택함으로써 계산 효율성과 안전성을 함께 유지할 수 있도록 하여야 한다.

c. Chosen protocol 공격

P와 Q가 두개의 다른 프로토콜이고, 각각이 동일한 키를 사용하여 다른 일을 수행할 때, 프로토콜 P에서 생성된 정보가 프로토콜 Q를 공격하는데 성공적으로 사용될 수 있을 때, '프로토콜이 Interactive 하다'라고 한다[10].

Chosen protocol 공격은 이러한 프로토콜의 Interaction을 이용하여 공격하기를 원하는 프로토콜과 Interactive 한 프로토콜을 선택 또는 설계하여 공격을 수행한다. 이러한 공격이 가능한 이유는 암호학적 API가 널리 퍼짐에 따라 많은 프로토콜들이 보안을 위해 암호를 채용하고 있으나, 키의 저장에 사용되는 스마트 카드의 저장용량이 적기 때문에, 인증서의 형태로 발행된 하나의 공개키가 여러 프로토콜에 사용될 수 있기 때문이다.

이러한 공격을 막기 위해서는 동일한 키가 여러 프로토콜에 사용되는 것을 막기 위해 발급된 키마다 사용할 수 있는 프로토콜의 수를 제한하거나, 각 응용 프로토콜, 버전, 프로토콜 단계의 전송정보가 유일한 식별자를 갖도록 하여, 다른 프로토콜 및 단계에 사용될 수 없도록 해야 한다.

2. 키 분배 프로토콜 수행중의 공격 방법

a. Ciphertext-only 공격

Ciphertext-only 공격은 공격자가 공개된 정보만을 이용하여 키와 관련된 중요한 정보나 세션키를 알아내는 공격으로, 도청 등으로 획득한 전송정보와 사용자의 공개키와 같은 공개정보만을 이용하여 세션키를 알아내려는 Ciphertext-only passive 공격[31]과 전송되는 정보를 수정하여 세션키를 알아내려고 시도하는 Ciphertext-only impersonation 공격으로 나눌 수 있다[30].

Ciphertext-only passive 공격은 공격자가 수행가기에 가장 쉬운 공격이나 공개 파라미터가 안전하게 선택되었다면 기존에 나와 있는 프로토콜은 모두 이 공격에

안전하다고 할 수 있다[30]. Ciphertext-only impersonation 공격은 공격자가 유효한 전송정보를 발생시킬 수 없도록 전송정보에 사용자의 비밀키를 포함시키거나, 세션키 생성함수의 조정 또는 서명 등을 사용하여 막을 수 있다.

b. Replay 공격

공격자가 합법적인 사용자로 위장하거나 정당한 사용자와 세션키를 설정하기 위하여 이전 프로토콜에서 사용된 메시지를 재사용하는 공격을 Replay 공격이라고 한다[30]. 이러한 Replay 공격은 과거의 프로토콜에서 기록된 메시지를 재사용하는 방법과 현재 수행되고 있는 프로토콜에서 생성된 메시지를 재사용하는 방법이 있다[39]. 또한 재사용된 메시지를 수신하는 사람에 따라, 송신자의 메시지가 송신자에게 되돌아가는 Reflection 공격과 제 3자에게 사용되는 Interleaving 공격등이 있다[2,17].

일반적으로 각 프로토콜의 특성에 따라 메시지의 재전송을 막기 위한 방법은 다양하며, 이산대수문제에 기반한 키 동의 프로토콜에서는 주로 Key freshness를 제공함으로써 한쪽 사용자가 키 토큰을 재전송하더라도 세션키의 생성에 영향을 줄 수 없도록 설계한다. 또한, Challenge-response 기법을 사용하여 재전송을 막을 수도 있다.

c. Intruder-in-the-middle 공격

이 공격은 통신 선로상의 중간에 위치한 공격자가 합법적인 사용자들 사이에 전송되는 정보들을 불법으로 도청 변경하여 전송함으로써 두 사용자간의 세션키를 구해내는 공격을 말한다. 이러한 공격은 전송정보에 디지털 서명 등을 사용하여 전송정보의 변경이 있을시 이를 탐지할 수 있도록 하거나, 암호화 등을 사용하여 정보의 누출이 일어나지 않도록 프로토콜을 설계함으로써 해결할 수 있다[18].

이외에도 공격자 E가 사용자 B에게 자신을 사용자 A로 위장하기 위해 필요한 전송정보를 A로부터 얻어내는 oracle session 공격 등이 있다[4,31].

3. 키 분배 프로토콜 수행 후의 공격

키분배 프로토콜 수행후의 공격은 합법적인 사용자들 사이에 한번 이상의 키분배 프로토콜이 수행된 이후, 공격자가 이전 세션에서 얻은 정보를 이용한 공격으로, 기한이 만료되어 공개되거나 부주의로 인해 노출된 이전 세션의 세션키를 이용하여 해당 세션의 세션키를 얻어내는 공격인 Known key 공격이 있다. 이 Known key 공격은 과거의 키와 현재의 전송정보를 관찰하여 세션키를 획득하려는 Known key passive 공격과 과거의 세션키와 현재의 전송정보를 수정하여 세션키를 생성하려는 Known key impersonation 공격, Known key impersonation 공격을 3자 이상으로 확대한 Known key triangle 공격으로 나눌 수 있다[12,30].

만일 프로토콜이 Known key 공격에 의해서 공격당하기 쉽다면, 현재 및 미래의 세션키를 비밀로 보관해야 한다. 따라서 보관해야 하는 키의 수는 프로토콜을 수행함에 따라 늘어나게 된다. 이러한 공격을 막기 위해서는 서명, 랜덤수 등을 사용하여 공격자가 유효한 전송정보를 생성할 수 없도록 프로토콜을 설계하거나, 과거의 세션키와 현재의 세션키가 상호 연관 관계가 없고, 세션키에 고정된 비밀정보로만 이루어지지 않도록 세션키 생성함수를 설계해야 한다.

D. 안전한 그룹키 분배 및 갱신 프로토콜 설계시 요구사항

모든 암호 프로토콜은 분배된 키를 사용하므로, 키의 안전한 분배 및 갱신은 매우 중요며 특정 분야에 적합한 키분배 프로토콜 설계에는 응용분야에 대한 요구사항은 고려해야 한다. 예를 들어, 본 논문에서의 모바일 환경에서의 그룹 통신을 위한 키분배 프로토콜은 일반적인 키분배 프로토콜의 요구사항 뿐만 아니라, 이동통신환경의 특징인 Mobile station의 이동성이나 안전한 그룹 통신이 되기 위한 그룹

키 분배 및 갱신의 안전성 그리고 통신 계산량의 최소화 등의 특징을 고려해야 한다. 모든 공개 파라미터와 인증서의 발급이 정상적으로 이루어졌다는 가정하에 안전하고, 이동통신환경의 특성을 만족시키는 그룹키 분배 및 갱신 프로토콜의 설계 원칙에 대하여 다룬다.

1. 그룹키의 안전성(Security)

그룹 멤버가 가입(Join) 혹은 탈퇴(Leave)등의 이유로 그룹에 변화를 발생시키면, 그룹에 관한 데이터와 그룹키의 안전성을 보장하기위해서 그룹키를 갱신해야 한다. 안전한 그룹 통신이 되기 위해서는 그룹키 안전성에 중요한 다음 속성들을 만족해야 한다.

a. 그룹키 비밀성(Group Key secrecy)

가장 기본적인 속성으로, 어떤 특정 그룹에서 사용되었던 혹은 사용중인 그룹키는 그룹의 구성원들만이 알 수 있어야 한다.

b. 전방 비밀성(Forward Secrecy)

그룹 멤버의 변화로 어떤 멤버가 더 이상 그룹 멤버가 아니거나 수동적인 적(Passive adversary)이 옛 그룹키의 서브셋을 알더라도 앞으로 그룹에서 사용할 새로운 그룹키에 대해서 알 수 없어야 한다.

c. 후방 비밀성(Backward Secrecy)

그룹 멤버의 변화로 새로운 멤버가 그룹에 가입되거나 수동적인 적이 그룹키의 서브셋을 알더라도 이전에 그룹 통신에 사용된 그룹키에 대해서 알 수 없어야 한다.

d. 키 독립성(Key Independence)

가장 강한 속성으로, 어떤 그룹이 사용하고 있는 그룹키에 대해서, 수동적인 적이 그룹키의 일부 서브셋을 알고 있더라도 그룹키에 대해서 알 수 없어야 한다.

전방 비밀성과 후방 비밀성은 그룹키 비밀성에 포함되고, 키 독립성은 나머지 세 가지를 포괄한다.

2. 상대방에 대한 명시적인 인증

사용자는 상대방으로부터의 전송정보의 유효성을 검사하기 위하여 통신상대방이 자신이 프로토콜을 수행하고자 하는 사람인지를 확인하는 명시적 인증이 필요하다. 일반적으로 공격자의 Impersonation을 이용한 공격을 막기 위해 통신 상대방에 대한 명시적인 인증을 수행한다. 이는 전송정보에 대한 디지털 서명을 사용하여 수행되거나, 키 분배를 하는 두 객체가 상호 정당한 사람만이 키를 생성할 수 있다는 확신을 갖는 묵시적 인증과 세션키가 올바르게 생성되었는지를 확인하는 키 확인(Key confirmation)을 결합하여 수행된다.

3. 전송정보에 대한 메시지 인증

메시지 인증으로 전송정보의 변경을 막는다. 전송정보에 대한 디지털 서명, MAC 등을 사용하여 메시지 인증을 제공함으로써 공격자의 전송정보에 대한 내용변경, 순서변경, 삭제여부 등을 확인하여 메시지의 변경에 의한 공격을 막는다.

4. 재전송 방지

각각의 전송정보에 유일성을 부여하고, 상호연관관계를 맺어 다른 프로토콜에 사용되거나 프로토콜 수행 후에 재전송되는 것을 막는다.

키분배 프로토콜들에서의 대부분의 공격들은 전송정보를 기록하고 그 전송정보

나 일부분을 다른 세션에 재사용하는 경우에 발생한다. 따라서 이러한 공격들을 막기 위해서는 전송정보의 재사용을 막을 수 있는 방법이 필요하다. 이는 주로 각 라운드의 전송정보들이 다른 구조를 갖도록 하거나, 각 라운드들의 메시지들이 연관성을 갖게 함으로써 이 요구사항을 만족시킬 수 있다.

5. 키 확인의 제공

두 사용자간에 동일한 세션키를 가지고 있는지를 확인하는 키 확인을 수행한다. Unknown key share 공격과 같은 경우 키 분배 프로토콜 수행단계에서 사용자간에 동일한 세션키를 생성했는지를 확인하여 쉽게 막을 수 있다. 또한, 묵시적 인증을 수행한 경우, 키 확인을 수행하여 명시적 인증을 수행할 수 있다.

6. 키생성 함수의 선택

세션키의 생성에 항상 값이 고정되는 항이나 다른 항과 별도로 분리되는 항이 존재하지 않도록 함으로써 Known key 공격에 안전할 수 있다.

Known key 공격은 키 생성 함수에 사용자들의 비밀키로만 이루어진 항이 존재하는 경우 비밀키에 해당하는 세션의 세션키가 노출될 때 발생한다. 따라서 키생성 함수에 다른 항과 분리되거나 세션에 상관없이 항상 고정된 항이 존재하지 않도록 세션키 생성함수를 선택해야만 한다. 일반적으로 해쉬 함수를 이용한 세션키를 생성하여 Known key 공격을 막을 수 있다.

7. 전송정보의 량 및 패스의 수 최소화

이동통신에서의 프로토콜은 전송정보의 량 및 프로토콜의 패스의 수를 최소화시킨다. 일반적으로 이동통신환경의 특징인 무선통신은 유선통신에 비하여 낮은 대역폭과 높은 에러율을 나타낸다. 따라서 이동통신환경의 무선통신 환경에서의 프로토콜들은 메시지의 량과 패스의 수가 최소화 되도록 설계한다[17].

8. Mobile Station 계산량의 최소화

일반적으로 Mobile station의 계산능력은 Base station에 비해 낮으므로 Mobile station의 계산량을 최소화하도록 프로토콜을 설계해야 한다. 이동통신 기기는 사용자의 휴대성을 높이기 위하여 소형화 및 경량화 되고 있다. 따라서 이동통신기기는 낮은 계산능력과 적은 자원을 가지므로, 상대적으로 높은 계산량과 많은 자원을 가진 base station이 보다 많은 계산을 수행하고 Mobile station은 최소의 계산을 수행하도록 프로토콜을 설계해야 한다. 예를 들어, Park의 프로토콜에서는 Mobile station의 계산을 최대한 Base station으로 이동시킴으로써, Mobile station의 계산량을 최소화하고자 했다[5].

9. 익명성 보장

이동통신환경에서는 사용자의 위치정보가 알려질 경우 개인의 프라이버시가 침해될 여지가 있으므로 익명성을 보장해야 한다. 사용자의 위치가 항상 고정된 유선통신과는 달리, 이동통신환경에서는 개인의 전송정보의 보호도 중요하지만, 개인의 위치정보가 노출되는 경우 개인의 프라이버시의 침해를 가져올 수 있다. 따라서 의도된 상대만이 통신하고 있는 상대가 누구인지를 알 수 있는 사용자에 대한 익명성을 보장해야 하며, 이러한 익명성의 보장은 Base station의 공개키로 Mobile station의 인증정보를 암호화하여 보내거나, 둘 사이에 세션키 생성 후 Mobile station의 인증정보를 암호화시켜 보냄으로써 수행할 수 있다.

10. 인증정보의 핸드오프

Mobile station의 이동성 및 유용성을 높이기 위하여 인증정보의 핸드오프를 제공해야 한다. 이동통신환경에서 이동통신기기는 여러 도메인을 이동하며, 다른 도메인(Foreign domain)에서 서비스를 받기 위해서는 홈 도메인(Home domain)에서 다른 도메인으로 인증정보를 제공해야만 한다. 따라서 프로토콜 설계 시에는 인증

정보의 핸드오프를 고려하여 설계해야 한다. 주로 X.509 형식의 인증서를 사용하여 온라인 인증서버의 도움 없이 인증 정보의 핸드오프를 해결할 수 있다.

11. 송신정보의 부인 불가

Mobile station은 자신이 전송한 정보에 대하여 차후에 부인할 수 없어야 한다. 현재 진행 중인 ASPeCT 등의 제 3세대 이동통신을 위한 프로젝트에서는 이동통신을 활용한 전자상거래를 고려하여 프로젝트를 수행하고 있다[11]. 따라서 소비자가 판매자로부터 물건을 구입하는 경우나 어떠한 서비스를 사용한 경우, 나중에 이를 부인할 수 없어야 한다. 이러한 부인불가 서비스는 디지털 서명을 사용하여 구현되고 있다.

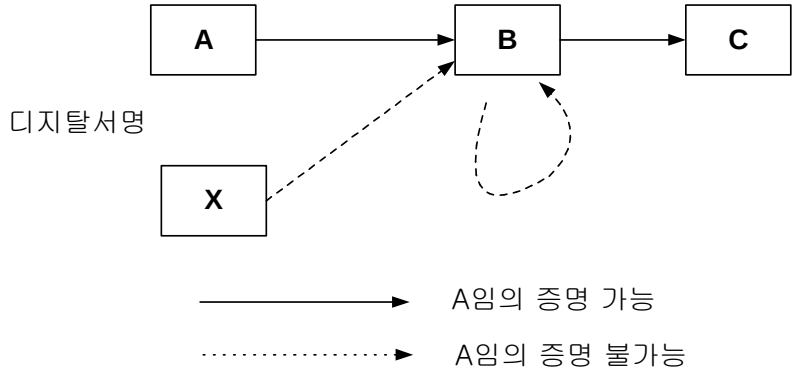
E. 보안시스템을 위한 기반기술

1. 디지털 서명*(Digital Signature)*

a. 디지털 서명의 개념

컴퓨터 통신 기술에 근거하여 정보 교환이 이루어지게 됨에 따라 상대방과 직접 대화를 통하여 부수적으로 얻게 되는 개인 고유의 특성인 음성 및 모습 등에 대한 정보를 얻는 비대면 환경에서 전자적인 방법으로 거래가 이루어짐에 따라 정보가 교환되는 상대가 누구인지, 송신된 메시지가 정확하게 전달되었는지, 제 3자의 개입은 없었는지, 의사전달이 정확히 전달이 되었는지 등을 확인할 수 있는 방법이 요구되었다. 이와 같은 확인 기능인 인증 기능은 암호 기법(cryptographic scheme)을 이용하여 시스템을 구성한다[33].

인증은 메시지 인증(message authentication), 사용자 인증(entity authentication), 디지털 서명(digital signature)으로 분류된다. 메시지 인증은 정보가 변경되지 않고 본래의 정보 그대로임을 보증하는 기능이며, 사용자 인증은 정보시스템에서 정보의 생성, 전송, 처리, 기억, 판단 등의 행위에 관여한 사용자 A의 일치성을 보증하는 기능이다.



[그림 2.3] 디지털 서명(Digital signature)

메시지 인증과 사용자 인증을 모두 지원하는 디지털 서명은 사용자 인증 관점에서 보면 “사용자 X가 B에게, B가 C에게, B가 B 자신에게조차도 사용자 A임을 증명할 수 없다”는 조건을 만족하는 경우로 [그림 2.3]과 같다.

b. 디지털 서명의 방식

(1) 공통키 기반 디지털 서명 방식

공개키 암호 시스템의 계산량이 많다는 단점을 보완하기 위한 방법으로 주로 제안되었다. 공통키 서명 방식은 DES(Digital Encryption Standard)가 안전하다고 할 때 제3자는 주어진 값으로부터 $h(key)$를 계산할 수 없다는 점에 착안된 ‘Lamport 공통키 서명 방식’, 메시지의 압축된 형태를 암호 키로 암호화하

여 서명문을 생성하는 방식인 'Rabin 공통키 서명 방식', Trusted authority가 요구되는 '중재 서명 방식' 등이 있다.

(2) **공개키 기반 디지털 서명 방식**

공개키 암호 시스템을 적용하는 인증 시스템은 제약 조건이 강하여 공통키 암호 시스템으로 실현 할 수 없는 개인 식별과 디지털 서명을 실현하는데 사용된다. 공개키 기반의 디지털 서명 방식은 소인수분해 문제에 기반 한 'RSA 디지털 서명 방식', 이산대수 문제에 기반 한 'ElGamal 디지털 서명 방식' 등이 있다.

(3) ID **기반 디지털 서명 방식**

ID를 이용한 암호시스템에서는 공개키에 해당하는 ID와 ID에 대응되는 비밀키가 있으며, 비밀키를 만들어 주는 키 발급 센터가 존재한다. 키 발급 센터만이 비밀키를 생성할 수 있는 능력을 갖고 있으므로 키 발급 센터이외에는 누구도 ID를 변경할 수 없다. 이 방식은 Shamir가 1984년 기본 개념을 처음 제안하였다[19]. ID 기반의 디지털 서명 방식은 Fiat-Shamir의 ID를 이용한 서명 방식과 Ohta의 ID를 이용한 개인 식별이 있다.

2. ID 기반 디지털 서명 방식

a. 공통키, 공개키 디지털 서명 방식의 특성

서명의 바람직한 특성은 위조하기 어렵고 증명하기 쉬워야 한다. 디지털 서명은 심볼들의 스트링으로 구성되는데 이것은 손으로 쓴 서명과는 다르게 서명할 때마다 다르다. 이는 각 디지털 서명이 서명하는 메시지의 함수가 되고 time stamp와 함께 사용함으로써 실현 가능하다. 또한 각 서명자에게 유일성은 보장하고 위조를 방지하기 위하여 각 디지털 서명은 서명자에게 유일한 비밀키에 의존하는 것이 바람직하다. 검증자는 서명자의 비밀키를 알지 못하더라도 서명을 쉽게 검증할 수 있어야 한다.

공통키 암호 시스템을 이용한 디지털 서명 방법은 서명자와 검증자 간의 공통인

비밀키에 의해서 서명을 생성 검증하기 때문에 검증자가 서명 메시지를 변조하여 서명을 할 수 있다. 따라서 공통키 암호 시스템에 의한 서명은 분쟁의 문제가 발생하였을 때 분쟁을 해결하기 어려우므로 서명에 효과적이지 못하다. 그럼에도 불구하고 공통키 암호 시스템을 이용한 서명 시스템에 대한 많은 시도가 있었다. 공개키 암호 시스템의 계산량이 많다는 단점을 보완하기 위한 방법으로 주로 제안되었다.

공개키 암호 시스템의 특징은 키 분배가 용이하며, 관리할 키의 수가 적고, 디지털 서명이 가능하다는 점이다. 공개키 시스템을 이용한 서명의 특성은 본인만이 할 수 있으며 어느 누구라도 위조 불가능해야 하며 누구나 확인할 수 있어야 한다는 서명의 특성을 만족시키면서 전자적으로 실현할 수 있다. 공개키 암호 시스템은 공통키 암호 시스템 보다 키 관리가 용이하고 보다 많은 정보 서비스를 제공할 수 있다고 하여도 상대를 인증하기 위해서는 공개키를 인증해야 하는 문제가 발생한다. 공개키는 제 3자에게 노출된다고 하여도 암호 시스템의 안전성에 영향을 주지 않으나, 공개키 내용이 불법적으로 변경되어서는 안되므로 인증된 공개키를 공개 기록집으로 만들어 항시 보유해야만 된다.

*b. Fiat-Shamir*의 *ID*를 이용한 디지털 서명 방식

공개키 방식에서 나타나는 공개 인증 문제로 인하여 1984년 Shamir를 시초로, 주소, 성명 등 각 개인을 식별할 수 있는 ID를 이용한 암호시스템이 등장하였다. ID를 이용한 암호시스템에서는 ID를 공개키로 사용하기 때문에 공개키를 인증할 필요가 없다. 따라서 공개 기록집을 작성하지 않아도 된다[18].

ID를 이용한 암호 시스템에서는 공개키에 해당하는 ID와 ID에 대응되는 비밀키가 있으며, 비밀키를 만들어 주는 키 발급 센터가 존재한다. 키 발급 센터만이 비밀키를 생성할 수 있는 능력을 갖고 있으므로 키 발급 센터 이외에는 누구도 ID를 변경할 수 없는 장점을 가지고 있다. Fiat와 Shamir는 ID를 이용한 개인 식별에서 사용하였던 방법을 이용하여 ID를 이용한 디지털 서명 방법을 제안하였다[1,27,33].

(1) **키 발급 절차**

① 키 발급센터는 서로 다른 큰 소수 p, q를 랜덤하게 생성하여 그들의 곱 $N = p \cdot q$를 계산한다.

② f는 단방향 함수이다.

③ 통화자 A의 개인식별 정보 ID_A를 이용하여 $I_i = f(ID_A, i)$ 를 계산한다. ($i = 1, 2, \cdots, k$) 여기서 I_i는 [표 2.1]을 만족한다.

[표 2.1] I_i 의 조건

$I_i \in QR_N$
QR_N은 modulus N에 대하여 이차 잉여인 집합 전체

④ I_i를 이용하여 $I_i^{-1} = S_i^{2} \pmod N$ $i = 1, 2, \cdots, k$ 인 $S_1, S_2, \cdots, S_k$를 계산한다.

⑤ 키 발급센터는 N, f, ID_A를 모든 통화자에게 공개하고, $S_1, S_2, \cdots, S_k$를 A에게만 분배하고, p, q는 키 발급센터만 비밀리에 보유한다.

(2) **서명절차**

① A는 t개의 랜덤한 수 r_1, r_2, $\cdots$, r_t $(0 < r_t < n)$을 생성하여 $x_i = r_i^{2} \bmod N$ 을 계산한다.

② A는 $f(M, x_1, x_2, \cdots, x_t)$를 계산하여 상위 kt비트를 e_{ij} $(1 \le i \le t, 1 \le j \le k)$로 한다.

③ A는 $y_i = r_i \cdot \prod_{e_{ij}=1} S_{ij} \pmod N$, $(1 \le i \le t)$ 을 계산하여 ID_A, M, $t \times k$의 행렬 $[e_{ij}]$, y_i $(1 \le i \le t)$를 B에게 보낸다.

(3) 검증 절차

통화자 A는 통화자 B에게 자신이 A임을 다음과 같은 암호 프로토콜을 사용하여 증명할 수 있다.

① B는 $I_j = f(ID_A, j)$, $(1 \le j \le k)$ 를 계산한다.

② B는 $Z_i = y_i^{\,2} \cdot \prod_{e_{ij}=1} I_j \bmod N$, $(1 \le i \le t)$를 계산한다.

③ B는 $f(M, Z_1, Z_2, \cdots, Z_t)$를 계산하여 상위 kt비트를 e_{ij}와 같은가 확인한다.

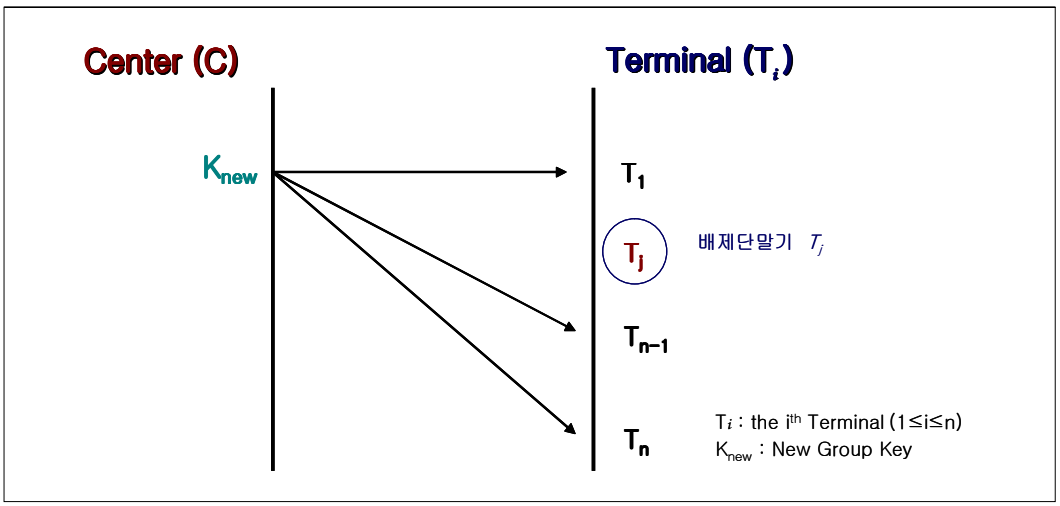
A와 B가 위와 같은 프로토콜을 실행할 수 있다면 B는 $t \times k$ 행렬 $[e_{ij}]$와 $y_i (1 \le i \le t)$로써 메시지 M의 서명이 됨을 확인할 수 있으며, A의 서명으로부터 A의 비밀키 S_1, S_2, …, S_k에 대한 어떤 정보도 얻을 수 없다. 이 방식은 고속처리와 ID에 근거하기 때문에 RSA에 근거한 서명 방식보다 효율적이다.

Ⅲ. 그룹 키 분배 및 갱신 프로토콜 설계

A. 기존 그룹키 갱신 프로토콜

디지털 이동 통신시스템의 특정 그룹 내에서 공유되어 사용되고 있는 비밀 키를 공개된 통신망을 통해 그룹 내의 일부 가입자에 의한 분실 등의 이유로 새로운 그룹 비밀 키를 공유하고자 할 때의 기술은 많이 알려져 있지 않다[37,38].

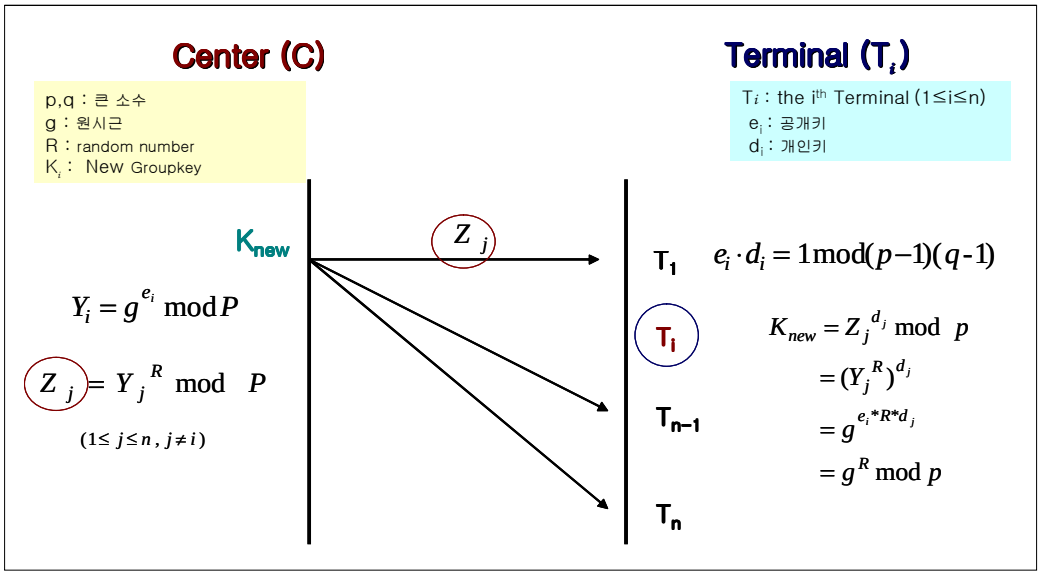
1. 대칭키 암호화를 이용한 그룹키 분배 방식



[그림 3.1] 대칭키 그룹키 분배

각 단말기 $T_i(1 \le i \le n)$는 그들의 비밀 키 K_i를 가지고 있으며, 그룹 비밀 키 생성 및 분배를 담당하는 센터 C는 모든 사용자의 비밀 키를 비밀리에 보관한다. [그림 3.1]과 같이 단말기 T_i를 배제하고자하는 경우, 센터는 T_i를 제외한 모든 다른 단말기에게 새로운 그룹 비밀 키 K_{new}를 자신이 보유하고 있는 각 단말기의 비밀 키를 이용하여 단말기들에게 개별적으로 암호화하여 분배한다[21].

이 방식에서는 배제되는 단말기 T_i를 식별하고 새로운 그룹 비밀 키 K_{new}를 암호화하여 분배하는데 $n-1$회의 통신이 필요하게 된다. 센터가 많은 수의 단말기를 관리하는 경우 그룹 비밀 키 전송에 많은 시간이 요구된다.



[그림 3.2] 비대칭키 그룹키 분배 방식

2. 비대칭키 암호화를 이용한 그룹키 분배 방식

이 방식은 공개키를 전제로 하므로 다음과 같은 과정을 통해 새로운 그룹 비밀 키를 갱신하게 된다[24]. 먼저 각 단말기 $T_i(1 \le i \le n)$ 는 자신의 공개키 E_i를 다음과 같이 생성한 후 공개한다.

$$E_i \cdot D_i = 1 \bmod (P-1),\ \text{단 } P\text{는 큰 소수}$$

센터는 다음의 정보를 생성하여 안전하게 저장한다.

$$Y_i = G^{E_i} \bmod P$$

그룹 비밀 키 갱신이 필요한 경우 센터는 랜덤 값 R을 생성하여 배제하고자 하는 단말기 T_i를 제외한 모든 단말기에게 다음의 정보를 전송한다.

$$Z_j = Y_j^R \bmod P, \ (1 \le j \le n, j \ne i)$$

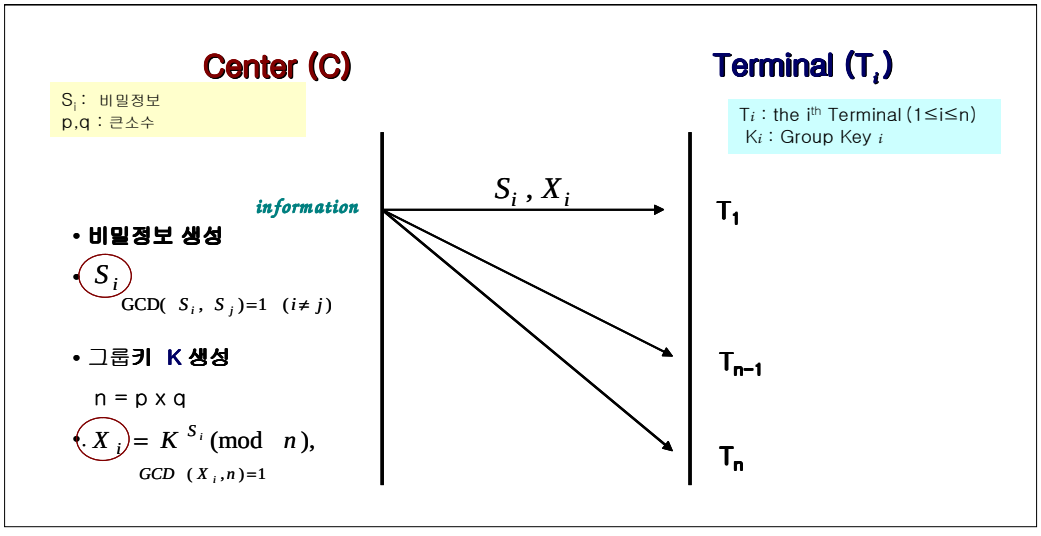
각 단말기 T_j는 다음과 같이 새로운 그룹 비밀 키를 갱신한다.

$$K_{new} = Z_j^{D_j} \bmod P$$

이 방식은 센터가 사용자의 비밀정보를 알 수 없으므로 보안의 측면에서는 바람직할 것이다. 그러나 그룹 비밀 키 K_{new}를 암호화하여 분배하는데 $n-1$회의 통신이 필요하게 된다.

3. *Matsuzaki-Anzai(MA)* 방식을 이용한 그룹키 분배방식

Matsuzaki-Anzai는 디지털 이동통신 시스템에 적합한 효율적이고 새로운 그룹 비밀키 재 공유 방식을 처음으로 소개하였다[13].



[그림 3.3] MA 방식 (그룹 비밀키 준비 단계)

이 방식은 그룹 비밀 키 갱신 시 사용자의 수에 의존하지 않는 특징을 가지고 있다. 이 방식은 기지국이 복수의 단말기를 관리하는 스타형 이동 통신 시스템에 있어서 그룹 내의 공유 비밀키를 사용해서 동보 암호 통신을 행하는 경우를 말한다. 이 방식은 그룹으로부터 특정 단말기를 배제하고 새로운 그룹 비밀 키를 가능한 빨리 갱신하기 위한 것이다.

[표 3.1] MA 방식 (시스템 계수)

- $T_i (1 \le i \le n)$: 각 사용자의 단말기
- S_i: 그룹 키 갱신을 위한 각 단말기의 비밀정보
- p, q: 센터가 생성하는 큰 소수
- K: 새로 갱신될 그룹 비밀키

a. 준비 단계

① 센터는 $GCD(S_i, S_j) = 1 (i \neq j)$이 되도록 각 단말기 비밀정보 S_i를 생성하여 비밀리에 보관하고, 각 단말기로 비밀리에 전송한다.

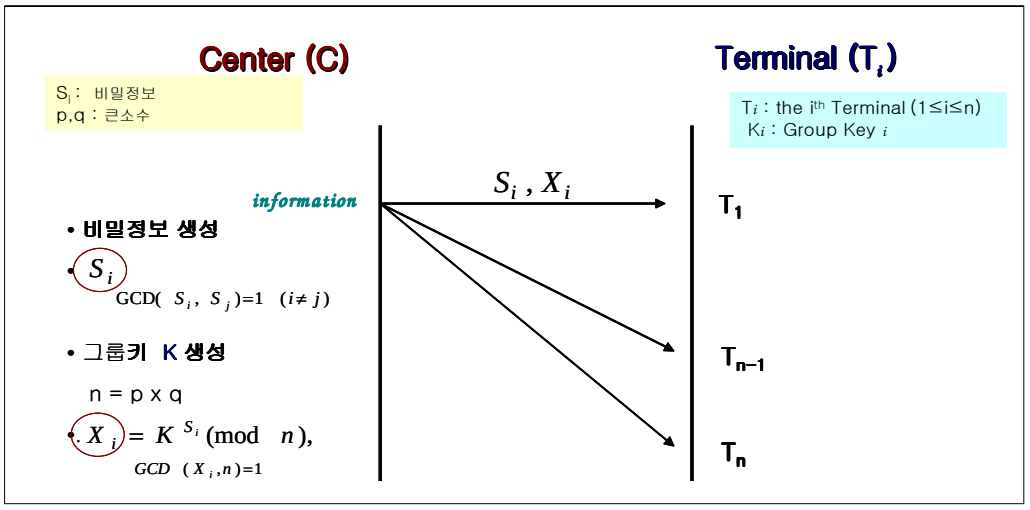
② 센터는 새로운 새로 갱신될 그룹 비밀 키 K를 랜덤하게 발생하고 비밀리에 보관한다.

③ 센터는 큰 소수 p, q를 생성한 후, $N = p \times q$를 계산하고 비밀리에 보관한다.

④ 센터는 각 단말기의 비밀 정보를 이용하여 $X_i = K^{S_i} \ (mod\ N), GCD(X_i, N) = 1$을 계산하여 안전하게 보관한 후, 각 단말기 안전하게 전송한다.

⑤ 각 단말기 T_i는 센터로 수신된 S_i, X_i를 비밀리에 보관한다.

c. 그룹 비밀 키 갱신 단계



[그림 3.4] MA방식 (그룹 비밀키 갱신단계)

① 센터가 단말기 T_i를 배제하고자 하는 경우 터미널 T_i와 관련된 정보 (S_i, X_i, N)을 모든 단말기에게 동보 전송한다.

② 단말기 T_j는 수신된 정보를 이용하여

$a \cdot S_i + b \cdot S_j = 1$을 만족하는 a, b 찾는다. 정수 a, b는 확장 유클리드 알고리즘을 이용하여 polynomial time에 계산이 가능하다.

③ 단말기는 다음과 같이 그룹 비밀 키를 갱신한다.

$a < 0$이면, $K = (X_i^{-1})^{-a} \cdot X_j^{\,b} \bmod N$

$b < 0$이면, $K = X_i^{a} \cdot (X_j^{-1})^{-b} \bmod N$

MA 방식은 터미널 T_i의 경우 수신된 정보가 자신의 비밀 키이므로 정확한 a, b를 생성할 수 없게 된다. 즉, 분실 단말기를 불법적으로 취득한 경우는 새로운 그룹 공유키 K를 생성 할 수 없게 된다. 이 방식은 N을 각 단말기가 알게 되는 경

우에 단말기들 간의 결탁을 방지할 수 없다. 즉, 특정 단말기 T_i, T_j가 각각의 비밀 정보 S_i, X_i와 S_j, X_j를 서로 주고받아 별도의 그룹 비밀 키를 센터의 도움 없이 계산한 후, 모든 다른 단말기들을 배제할 수 있다. 불법 단말기 T_k가 정당한 단말기 T_i의 비밀 정보 S_i, X_i를 취득하여 불법적인 도청을 하고 있고, 센터가 알게 되었다고 하자. 이 경우 센터는 T_i의 비밀 정보 S_i, X_i를 모든 단말기에 전송함으로써 T_k의 불법적인 도청을 막을 수 있다. 그러나 센터가 또 다른 단말기 T_j를 배제하기 위해서 T_j의 비밀 정보 S_j, X_j를 모든 단말기에 동보전송하게 되면 T_k의 경우 T_i의 비밀 정보를 이용하여 새로운 그룹 비밀 키를 생성할 수 있다. 이러한 위험에 대처하기 위해서 MA 방식은 RSA 공개키 암호화를 이용한다. 즉 불법 취득한 정보를 이용한 새로운 그룹 비밀 키를 계산하는 어려움은 RSA 안전성에 의존한다[11]. MA 방식은 단 1회의 그룹 공유 비밀 키 갱신만이 가능하다. 2회 이상 연속하여 그룹 비밀 키를 갱신하려면 준비 단계부터 다시 시작해야 한다[30,35]. 또한 역수 값의 계산이 단말기에서 수행되므로 약간의 계산상의 비효율성이 존재하게 된다[35].

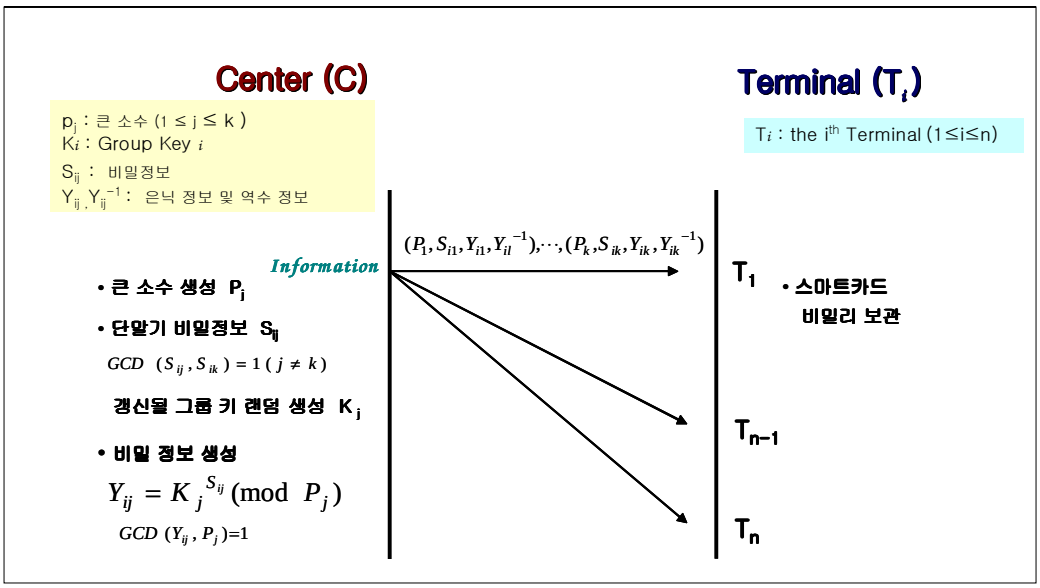
4. *Sim-Park-Won(SPW)* 방식

MA 방식의 문제점을 해결하기 위해서 SPW 방식이 제안되었다[29]. SPW 방식은 스마트카드를 이용하여 다수의 갱신될 그룹 비밀 키 정보와 역수 정보를 은닉하여 각 단말기에게 배포한다.

[표 3.2] SPW 방식 (시스템 계수)

- $T_i (1 \le i \le n)$: 각 사용자의 단말기
- $P_j (1 \le j \le k)$: 센터가 생성하는 큰 소수
- K_j: 새로 갱신될 그룹 비밀키
- S_{ij}: 각 사용자 T_i의 그룹 키 갱신을 위한 비밀 정보
- Y_{ij}, Y_{ij}^{-1}: 각 사용자 T_i의 그룹 키 갱신을 위한 은닉 정보 및 역수 정보

a. 준비 단계



[그림 3.5] SPW 방식 (그룹 비밀키 준비 단계)

① 센터는 큰 소수 $P_j(1 \le j \le k)$를 생성한 후, 비밀리에 보관한다.

② 센터는 $GCD(S_{ij}, S_{ik}) = 1\,(j \ne k)$이 되도록 각 단말기 비밀정보 S_{ij}를 생성하여 비밀리에 보관한다.

③ 센터는 새로운 새로 갱신될 그룹 비밀 키 K_j를 랜덤하게 발생하고 비밀리에 보관한다.

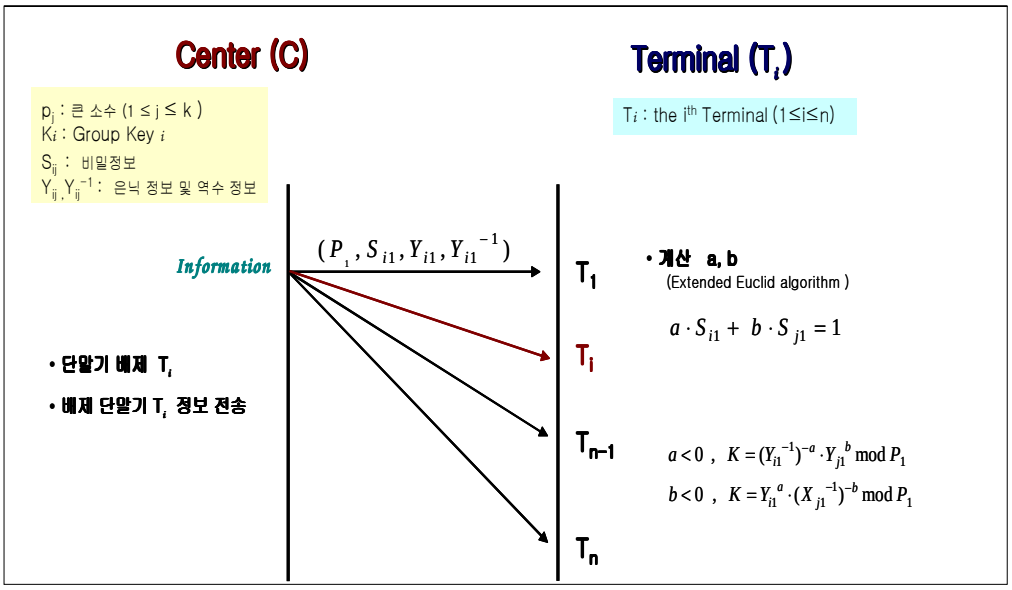
④ 센터는 그룹 비밀 키 은닉 정보 및 역수 정보를 각 단말기의 비밀 정보를 이용하여 계산하고 비밀리에 보관한다.

$$Y_{ij} = K_j^{S_{ij}} (mod\ P_j),\ GCD(Y_{ij}, P_j) = 1$$

⑤ 센터는 각 단말기 T_i에게 $(P_1, S_{i1}, Y_{i1}, Y_{i1}^{-1}), \cdots, (P_k, S_{ik}, Y_{ik}, Y_{ik}^{-1})$를 스마트카드에 저장하여 안전하게 전송한다.

⑥ 각 단말기 T_i는 센터로 수신된 스마트카드를 비밀리에 보관한다.

c. 그룹 비밀 키 갱신 단계



[그림 3.6] SPW 방식 (그룹 비밀키 갱신 단계)

① 센터가 단말기 T_i를 배제하고자 하는 경우 터미널 T_i와 관련된 정보 $(S_{i1}, Y_{i1}, Y_{i1}^{-1}, P_1)$을 모든 단말기에게 동보 전송한다.

② 단말기 T_j는 수신된 장보를 이용하여 $a \cdot S_{i1} + b \cdot S_{j1} = 1$을 만족하는 a, b 찾는다. 정수 a, b는 확장 유클리드 알고리즘을 이용하여 Polynomial time에 계산이 가능하다.

③ 단말기는 다음과 같이 그룹 비밀 키를 갱신한다.

$a < 0$이면 $K_1 = (Y_{i1}^{-1})^{-a} \cdot Y_{j1}^{b} \bmod P_1$

$b < 0$이면 $K_1 = Y_{i1}^{a} \cdot (Y_{j1}^{-1})^{-b} \bmod P_1$

SPW 방식에서는 Y_{j1}^{-1}이 미리 계산되어 스마트카드에 저장되어 내장되어 있으므로 별도의 역수 계산이 필요 없다[29]. MA방식과 마찬가지로, SPW 방식 역시 터

미널 T_i의 경우 수신된 정보가 자신의 비밀 키이므로 정확한 a, b를 생성할 수 없게 된다. 즉, 분실 단말기를 불법적으로 취득한 경우는 새로운 그룹 공유키 K를 생성 할 수 없게 된다.

이 방식은 그룹 공유키를 갱신하기 위한 정보가 스마트카드에 저장되어있으므로 2회 이상의 갱신 시 준비 단계부터 새롭게 수행하지 않아도 된다[29]. 그러나 스마트카드를 사용하기 때문에 또한 단말기의 경량화가 어려워질 수 있으며, 갱신의 횟수가 스마트카드의 용량에 따라 제한된다. 사용자간 단합에 의한 그룹 비밀 키 유출을 막을 수 없다. 또한 Modular 정보를 미리 제공하기 때문에 2개 이상의 단말기를 동시에 분실하였을 때 단말기들이 그룹 비밀 키를 생성할 수 있거나, 그들의 단합에 의해 그들 간에 그룹 비밀 키를 공유할 수 있다[35].

SPW 방식 역시 스마트카드의 정보를 불법으로 취득한 불법 단말기를 1회는 배제할 수 있지만 2회부터는 배제할 수 없다는 문제를 내포하고 있다. 이러한 위험에 대처하기 위해서 SPW 방식은 카드 내의 정보를 암호화해 두거나 접근 제어기능과 같은 추가적인 보호대책이 필요하다[29]. 단합에 의한 그룹 비밀 키 유출을 예방하기 위해서 P_j값을 스마트카드에 저장하여 배포하지 않고 매 갱신 때마다 서로 다른 P_j를 전송하는 것이 가능하지만, P_j를 미리 발생하여 센터가 안전하게 보관해야 하고, 이러한 방식만으로 불법 단말기가 그룹 비밀 키를 생성하는 것을 영구히 예방할 수는 없다.

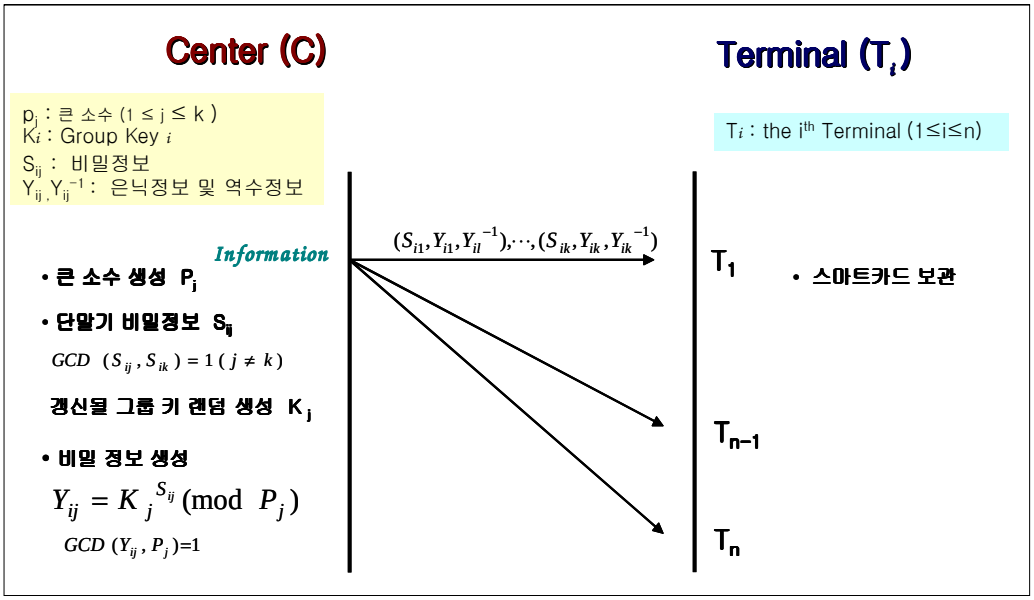
5. Park-Lee(PL) 방식

PL 방식은 SPW 방식에서 문제가 되는 2개 이상의 단발기의 동시 배제의 문제를 해결하기 위해서 제안되었다. SPW와 마찬가지로, PL 방식 역시 스마트카드를 이용하여 그룹 비밀 키 갱신을 위한 정보들을 미리 배포한다[35].

[표 3.3] PL 방식 (시스템 계수)

- $T_i (1 \le i \le n)$: 각 사용자의 단말기
- $P_j (1 \le j \le k)$: 센터가 생성하는 큰 소수
- K_j: 새로 갱신될 그룹 비밀 키
- S_{ij}: 각 사용자 T_i의 그룹 키 갱신을 위한 비밀 정보
- Y_{ij}, Y_{ij}^{-1}: 각 사용자 T_i의 그룹 키 갱신을 위한 은닉 정보 및 역수정보

a. 준비 단계



[그림 3.7] PL 방식 (그룹 비밀키 준비 단계)

① 센터는 큰 소수 $P_j (1 \le j \le k)$를 생성한 후, 비밀리에 보관한다.

② 센터는 $GCD(S_{ij}, S_{ik}) = 1 (j \neq k)$ 이 되도록 각 단말기 비밀정보 S_{ij}를 생성하여 비밀리에 보관한다.

③ 센터는 새로운 새로 갱신될 그룹 비밀 키 K_j를 랜덤하게 발생하고 비밀리에 보관한다.

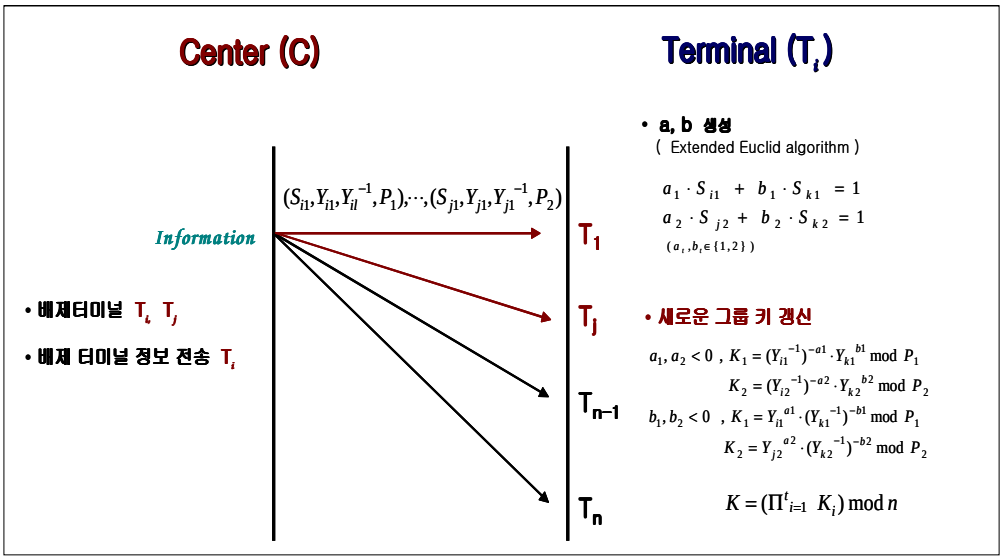
④ 센터는 그룹 비밀 키 은닉 정보 및 역수 정보를 각 단말기의 비밀 정보를 이용하여 계산하고 비밀리에 보관한다.

$$Y_{ij} = K_j^{S_{ij}} (mod\ P_j),\ GCD(Y_{ij}, P_j) = 1$$

⑤ 센터는 각 단말기 T_i에게 $(S_{i1}, Y_{i1}, Y_{i1}^{-1}), \cdots, (S_{ik}, Y_{ik}, Y_{ik}^{-1})$를 스마트카드에 저장하여 안전하게 전송한다.

⑥ 각 단말기 T_i는 센터로 수신된 스마트카드를 비밀리에 보관한다.

c. 그룹 비밀 키 갱신 단계



[그림 3.8] PL 방식 (그룹 비밀키 갱신 단계)

① 센터가 단말기 T_i, T_j를 동시에 배제하고자 하는 경우 터미널 T_i, T_j와 관련된 정보 $(S_{i1}, Y_{i1}, Y_{i1}^{-1}, P_1)$, $(S_{j1}, Y_{j1}, Y_{j1}^{-1}, P_2)$을 모든 단말기에게 동보 전송한다.

② 단말기 T_k는 수신된 장보를 이용하여 다음을 만족하는 $a_t, b_t (t \in \{1,2\})$를 찾는다.

$$a_1 \cdot S_{i1} + b_1 \cdot S_{k1} = 1$$

$$a_2 \cdot S_{j1} + b_2 \cdot S_{k2} = 1$$

③ 단말기 T_k는 다음과 같이 그룹 비밀 키를 갱신한다.

$$\text{if } a_1, a_2 < 0,\ K_1 = (Y_{i1}^{-1})^{-a_1} \cdot Y_{k1}^{b_1} \bmod P_1$$
$$K_2 = (Y_{j2}^{-1})^{-a_2} \cdot Y_{k2}^{b_2} \bmod P_2$$

$$\text{if } b_1, b_2 < 0,\ K_1 = Y_{i1}^{a_1} \cdot (Y_{k1}^{-1})^{-b_1} \bmod P_1$$
$$K_2 = Y_{j2}^{a_1} \cdot (Y_{k2}^{-1})^{-b_1} \bmod P_2$$

④ 단말기 T_k는 계산된 정보를 이용하여 새로운 그룹 비밀 키를 갱신 한다

$$K = (\Pi_{i=1}^{t} K_i) \bmod n$$

PL 방식 역시 Y_{j1}^{-1}이 미리 계산되어 스마트카드에 저장되어 내장되어 있으므로 별도의 역수 계산이 필요 없다. PL 방식 역시 터미널 T_k의 경우 수신된 정보가 자신의 비밀 키이므로 정확한 a, b를 생성할 수 없게 된다. 즉, 분실 단말기를 불법적으로 취득한 경우는 새로운 그룹 공유키 K를 생성 할 수 없게 된다. PL 방식은 P_i를 스마트카드에 저장하여 배포하지 않고 갱신 시마다 전송함으로써 단합에 의한 그룹 비밀키 생성의 문제를 해결하였다. 또한 배제되는 단말기들의 갱신을 위한 정보를 동시에 전송하고 그들의 연산을 통해서 그룹 비밀 키를 생성함으로써 동시 배제의 문제를 해결하였다[35]. PL 방식은 SPW의 장점을 그대로 가지고 있지만, SPW의 문제점도 그대로 가지고 있다. 즉, 스마트카드를 사용하기 때문에 또한 단말기의 경량화가 어려워질 수 있으며, 갱신의 횟수가 스마트카드의 용량에 따라 제한된다. SPW 방식과 마찬가지로, PL 방식도 스마트카드의 정보를 불법으로 취득한 불법 단말기를 1회는 배제할 수 있지만 2회부터는 배제할 수 없다는 문제를 내포하고 있다[28]. 이러한 위험에 대처하기 위해서 PL 방식은 도한 카드 내의 정보를 암호화해 두거나 접근 제어기능과 같은 추가적인 스마트카드 보호대책이 필요

하다. 또한 $K=(\Pi_{i=1}^{t}K_i)\bmod n$의 연산을 위해 n값을 임의의 큰 수로 결정해야하는데 이것에 대한 정확한 정의가 없다. n은 센터에 의해 미리 결정되어 각 단말기에 안전하게 저장되어야 할 것이다.

B. 새로운 그룹 키 갱신 방식의 제안

본 논문에서 제안하는 방식은 디지털 이동 통신 시스템에서 특정한 공간에서 소규모 그룹회의를 고려한 쉬운 키 생성과 갱신을 위주로 키센터에서 관리되는 단말기들 간의 통신의 안전성을 확보하기 위해서 필요한 그룹 비밀 키를 공유하는 방식이다. 본 연구는 그룹 비밀 키 공유 및 분배 방식은 이동 통신의 일반적인 특징인 소형 경량의 이동 단말기와 계산 능력이 큰 키센터를 충분히 고려하였으며, 동보통신을 수행하는 스타형 네트워크를 대상으로 하였다. 키센터를 중심으로 동일한 그룹 내에서 안전한 통신을 하고자하는 경우 먼저 고려해야 할 것은 그룹 내의 비밀 키의 문제이다. 그러나 단말기를 분실하였을 때 이 단말기의 공유 그룹 비밀 키나 비밀 정보를 이용하여 그룹 내의 통신을 쉽게 도청하거나 허위 정보를 유포할 수 있다. 공유 그룹 비밀 키를 이용한 도청이나 허위 정보 유포는 그룹 비밀 키의 갱신을 통해서 예방할 수 있지만, 비밀정보를 이용한 도청이나 허위 정보 유포는 단순한 그룹 비밀 키의 갱신을 통해서 예방하기는 어려운 점이 있다. 특히 동보통신이 이루어지고 있는 상황에서는 더욱 심각하다.

기존 방식들은 특정 단말기 내에 있는 그룹 키를 갱신을 위한 비밀정보를 불법적으로 취득한 불법 사용자를 1회의 그룹 키 갱신을 통해서 배제할 수 있지만, 2회부터는 배제할 수 없다는 문제를 가지고 있다. 따라서 본 연구에서는 이러한 문제점을 해결하고, 소형 경량의 이동 단말기를 위해 스마트카드와 같은 부가적인 장치

의 없이 그룹 비밀 키를 갱신할 수 있는 방식을 제안하였다.

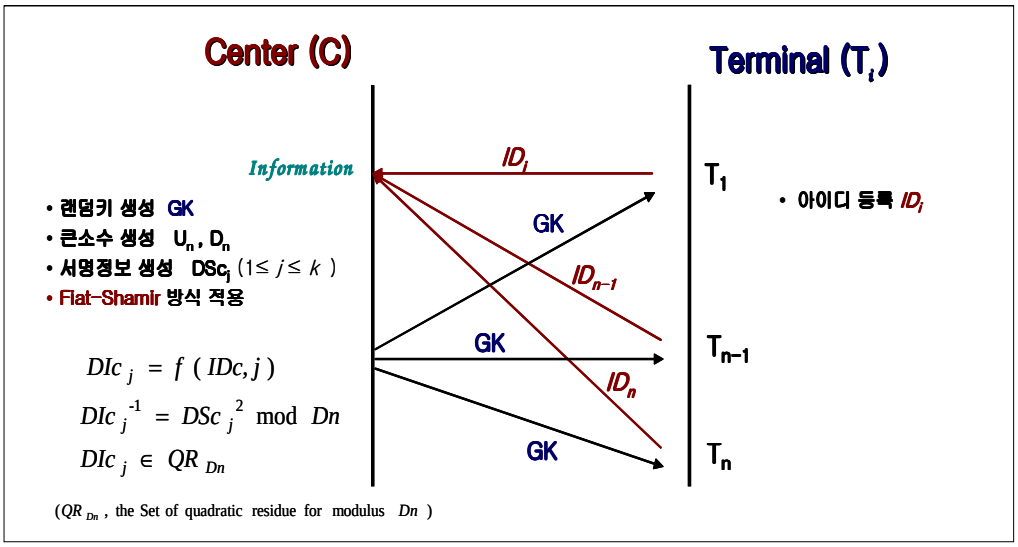
제안 방식은 ID 보안 기술에 기반을 둔 디지털 서명, 키분배 기법을 이용하여 그룹 비밀키의 분배와 갱신을 위한 효율적인 프로토콜을 제안한다. 제안된 프로토콜의 안전성은 Fiat-Shamir의 ID 기반의 디지털 서명과 Diffie-Hellman의 키 분배 방식을 이용하여 이산대수 어려움에 근거하고 있으며 단말기의 저장능력과 처리의 능력이 적을 경우도 적절하게 운영될 수 있고,단말기의 변동 없이 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있도록 설계하였다. 그리고 그룹 내에서 제외하고자 하는 통화자가 동시에 여러 명일 경우에도 적용할 수 있다. 이는 동일한 그룹 내의 가입자가 비밀 키나 비밀 정보를 분실하였을 때, 단말기를 분실하였을 때 또는 키센터가 불법적인 사용이 의심되는 특정 단말기를 그룹 내의 통신에서 배제하고자 할 때, 그룹 내의 비밀 키를 안전하게 갱신할 수 있는 효율적인 방식이며 최대의 장점은 불법적인 정보에 의한 불법 도청 단말기를 영구적으로 배재할 수 있다는 점이다. 새로운 그룹키 갱신 방식의 시스템 계수는 [표 3.4]와 같다.

[표 3.4] 제안된 그룹키 갱신 방식 (시스템 계수)

- C : 키 분배 센터
- $T_i (1 \le i \le n)$: 각 사용자의 단말기
- GK : 공유 그룹 비밀 키
- UK : 새로 갱신될 그룹 비밀 키
- $US_i (1 \le i \le n)$: 그룹 키 갱신을 위한 각 단말기의 비밀 정보
- $UX_i (1 \le i \le n)$: 갱신될 그룹키 은닉한 정보
- $ID_i (1 \le i \le n)$: 사용자 i의 ID정보
- f, h: 공개된 단 방향 함수
- Un: 그룹 키 갱신을 위한 큰 소수
- Dn: 디지털 서명을 위한 큰 소수

1. 준비 단계

a. 키 분배 센터



[그림 3.9] 제안된 그룹키 방식 (키분배 센터 준비단계 1)

① 키분배 센터(C)는 각 단말기 T_i로부터 식별정보 ID_i를 등록 받은 후 최초 그룹 비밀 키 GK를 랜덤하게 발생한다. 그리고 비밀리에 보관한 후 각 단말기에게 안전하게 배포한다.

② 센터는 커다란 소수 Un을 발생 후, 비밀리 보관한다.

③ $DSc_j (1 \le j \le k)$ 를 계산한 후, 안전하게 보관하며 이것은 비밀리에 보관하지 않아도 된다.

$DIc_j = f(ID_c, j)$

$DIc_j^{-1} = DSc_j^2 \bmod Dn$

$DIc_j \in QR_{Dn}$, (QR_{Dn}은 modulus Dn에 대한 이차잉여 집합전체)

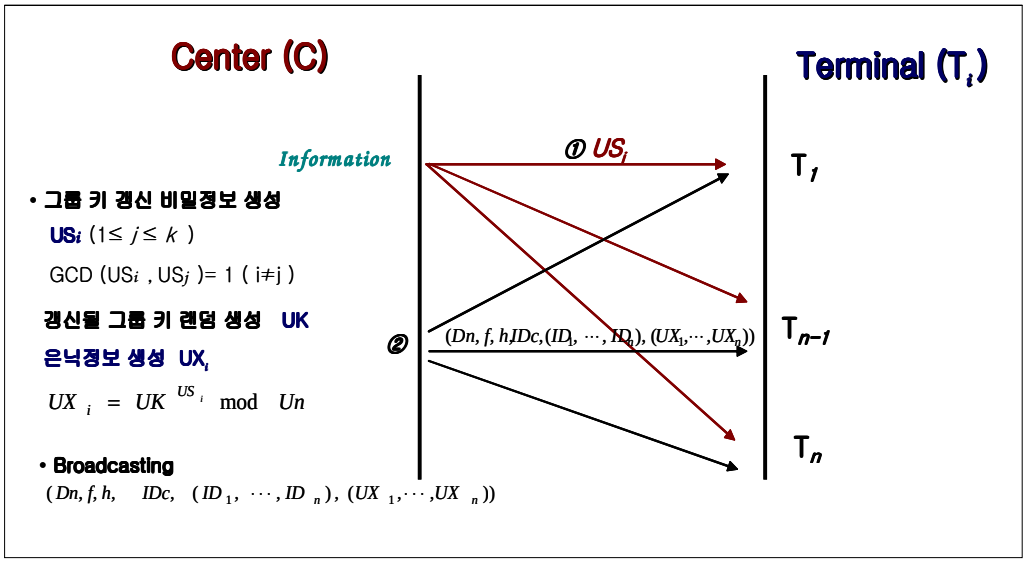
④ 그룹 키 갱신을 위한 단말기들의 비밀정보 $US_i (1 \le i \le n)$를 발생한 후, 비밀리에 보관하고 각 단말기들에게 안전하게 배포한다.

$GCD(US_i, US_j) = 1, i \neq j$

⑤ 새로 갱신될 그룹 비밀키 UK를 랜덤하게 발생한 후,비밀리에 보관한다.

⑥ 그룹 키 갱신을 위한 단말기들의 공개정보 UX_i을 계산한다. 이 단계에서 UX_i는 비밀리에 보관하지 않아도 된다.

$$UX_i = UK^{US_i} \bmod Un$$



[그림 3.10] 제안된 그룹키 방식 (키분배 센터 준비단계 2)

⑦ 모든 단말기들에게 다음 정보를 공개적으로 동보전송(broadcasting) 분배한다.

$$(Dn, f, h, ID_c, ID_1 \cdots ID_n, UX_1 \cdots UX_n)$$

b. 각 단말기

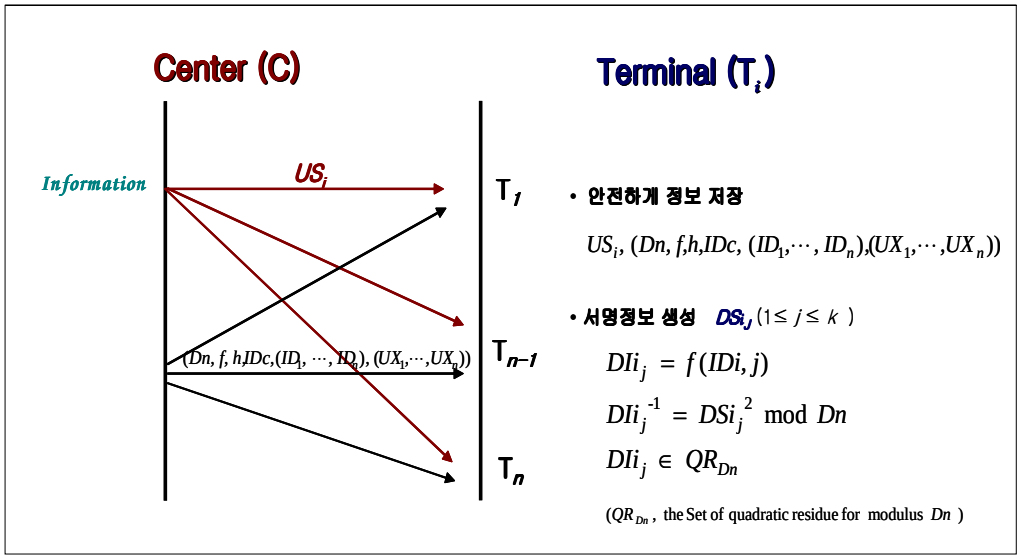
① 센터로부터 수신된 US_i, UX_i와 Dn,ID_c, ID_i, $\cdots$ ID_n를 안전하게 보관한다.

② $DSi_j (1 \le j \le k)$를 계산한 후, 안전하게 보관한다. 이것은 비밀리에 보관하지 않아도 된다.

$$DKi_j = f(IDi, j)$$

$$DKi_j^{-1} = DSi_j^2 \bmod Dn$$

$DKi_j \in QR_{Dn}$, (QR_{Dn}은 modulus Dn에 대한 이차잉여 집합전체)



[그림 3.11] 제안된 그룹키 방식 (키분배 터미널 준비단계)

2. 그룹 키 갱신 단계

a. 키 분배 센터

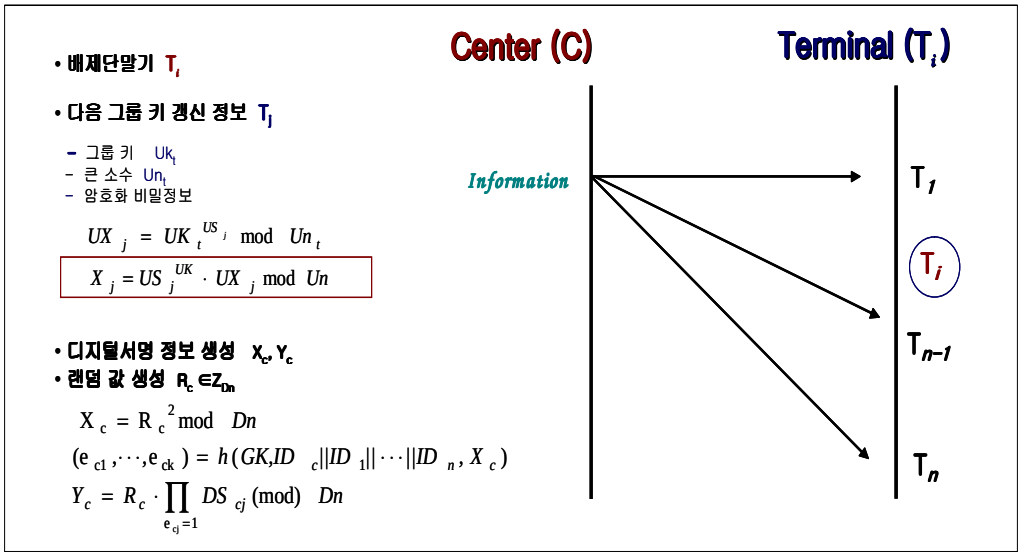
① 키 분배 센터가 어떤 사유로 인해 단말기 T_i를 배제하고자 한다.

② 일차 갱신되는 UK 이후, 갱신을 위한 그룹 비밀 키 UK_t를 생성하고 다음 갱신에 사용할 커다란 소수 Un_t을 발생한다.

③ 다음 갱신을 위한 단말기 $T_j(j \neq i)$의 단말기의 정보 UX_j를 은닉한다.

$$UX_j = UK_t^{US_j} \bmod Un_t$$

$$X_j = US_j^{UK} \cdot UX_j \bmod Un$$



[그림 3.12] 제안된 그룹키 방식 (키분배 터미널 갱신 준비단계 1)

④ 서명 정보 X_c, Y_c 생성한다.

ㄱ. 무작위 수 $R_c \in Z_{Dn}$을 생성

ㄴ. $X_c = R_c^2 \bmod Dn$

ㄷ. $(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$

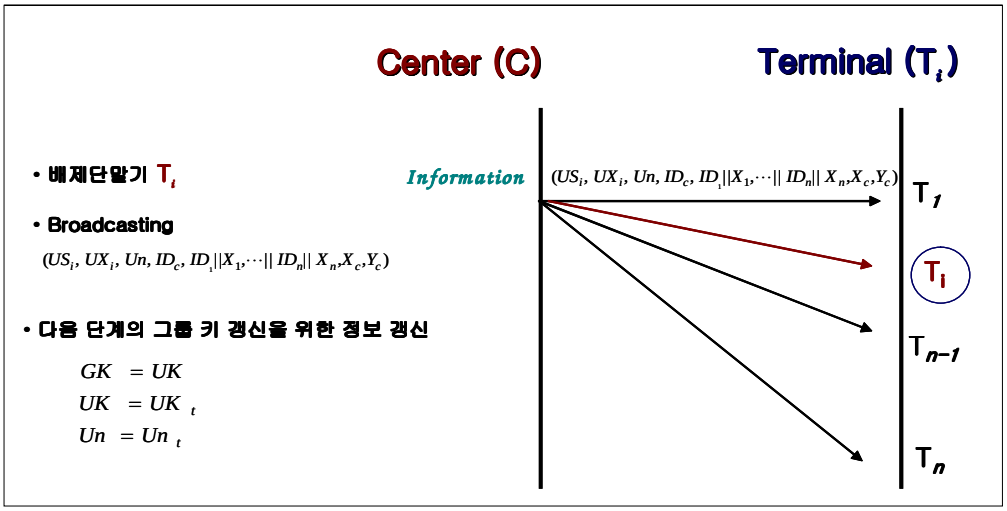
ㄹ. $Y_c = R_c \cdot \prod_{e_{c_j}=1} DSc_j \,(mod)\, Dn$

⑤ 다음 정보를 모든 터미널에 동보전송 한다.

$$(US_i,\ UX_i,\ Un,\ ID_c, ID_1 \| X_1, \cdots \| ID_n \| X_n, X_c,\ Y_c)$$

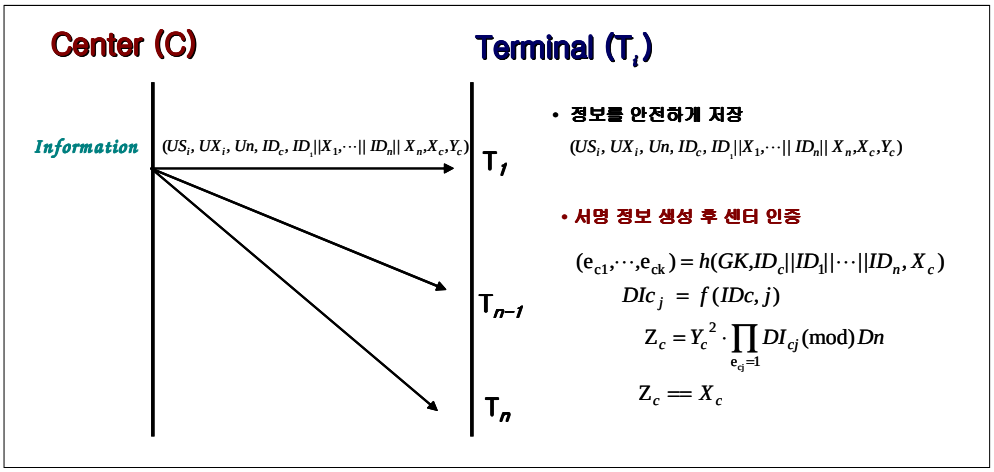
⑥ 다음의 그룹키 갱신을 위해 정보를 비밀리에 보관한다.

$$GK = UK,\ UK = UK_t,\ Un = Un_t$$



[그림 3.13] 제안된 그룹키 방식 (키분배 터미널 갱신 준비단계 2)

b. 각 단말기



[그림 3.14] 제안된 그룹키 방식 (키분배 터미널 갱신 준비단계 3)

① 터미널(T_j)는 아래의 정보를 센터로부터 수신한 후, 정당한 센터로부터 온 정보임을 확인 한다.

$$(US_i,\ UX_i,\ Un,\ ID_c,\ ID_1 \parallel X_1,\cdots \parallel ID_n \parallel X_n,\ X_c,\ Y_c)$$

ㄱ. $(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$

ㄴ. $DIc_j = f(IDc, j)$

ㄷ. $Z_c = Y_c^2 \cdot \prod_{e_{c_j}=1} DIc_j \,(mod)\, Dn$

ㄹ. $Z_c = X_c$를 만족하는지 검사하여 메시지를 인증한다.

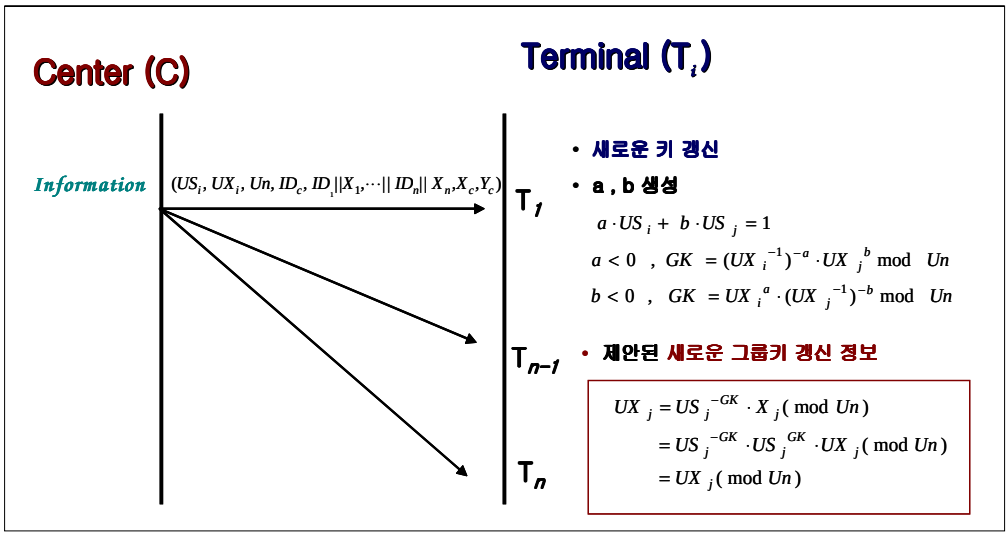
② 그룹 비밀키를 갱신 하고 $a \cdot US_i + b \cdot US_j = 1$을 만족하는 a, b 찾는다.

$$(a < 0),\ GK = (UX_i^{-1})^{-a} \cdot UX_j{}^{b} \bmod Un$$

$$(b < 0),\ GK = UX_i^{a} \cdot (UX_j^{-1})^{-b} \bmod Un$$

③ 다음 그룹 비밀 키 갱신을 위한 단말기의 정보를 갱신한다.

$$\begin{aligned} UX_j &= US_j^{-GK} \cdot X_j \ (mod\ Un) \\ &= US_j^{-GK} \cdot US_j^{GK} \cdot UX_j \ (\bmod Un) \\ &= UX_j \ (mod\ Un) \end{aligned}$$



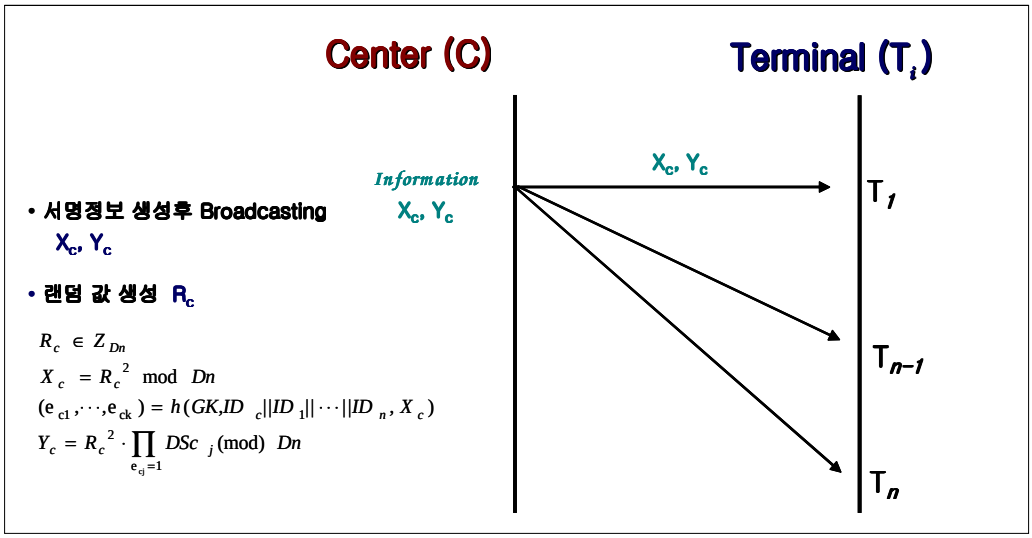
[그림 3.15] 제안된 그룹키 방식 (키분배 터미널 갱신 단계)

본 방식은 터미널 T_i의 경우 수신된 정보가 자신의 비밀 키이므로 정확한 a, b를 생성할 수 없게 된다. 즉, 분실 단말기를 불법적으로 취득한 경우는 새로운 그룹

공유키 GK를 생성 할 수 없게 된다. 또한 정당한 그룹 공유키를 생성하지 못한 단말기 T_i는 다음번 그룹 공유키 생성을 위해 필요한 UX_i를 올바르게 생성할 수 없게 되므로, 이 후의 그룹 공유키 경신 과정에서 영구히 배제된다. 따라서 단말기 T_i의 비밀 정보를 취득한 불법 사용자는 영구히 배제된다. 그리고 키 갱신 시마다 새로운 Un값을 배포하고 폐기하므로 단말기들이 서로의 비밀 정보 UX_i와 UX_i를 주고받아 그룹 공유키를 계산한 후 다른 모든 단말기를 배제하는 경우가 없게 된다.

3. 단말기 확인단계

디지털 서명을 이용함으로써 제인 방식은 불법적인 사용을 주기적으로 확인 및 인증하여 임의적으로 배제할 수 있다.



[그림 3.16] 제안된 그룹키 방식 (단말기 확인 단계 1)

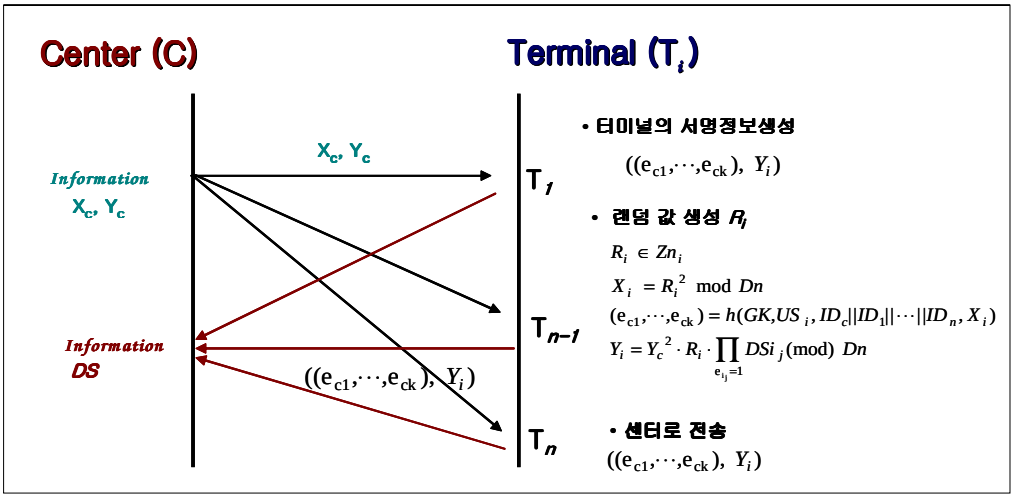
① 키 분배센터는 서명정보 X_c, Y_c를 생성 후, 모든 터미널에 동보 전송한다.

② 무작위 수 $R_c \in Z_{Dn}$을 생성한다.

$$X_c = R_c^2 \bmod Dn$$

$$(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$$

$$Y_c = R_c \cdot \prod_{e_{c_j}=1} DSc_j \,(mod)\, Dn$$



[그림 3.17] 제안된 그룹키 방식 (단말기 확인 단계 2)

③ 각 단말기 T_i은 자신의 서명정보$((e_{i_1}, \cdots, e_{i_K}), Y_i)$를 생성한 후, 센터에게 전송한다.

④ 무작위 수 $R_i \in Z_{N_1}$을 생성한다.

$$X_i = R_i^2 \bmod Dn$$

$$(e_{i_1}, \cdots, e_{i_K}) = h(GK, US_i, ID_c \| ID_1 \| \cdots \| ID_n, X_i)$$

$$Y_i = Y_c \cdot R_i \cdot \prod_{e_{i_j}=1} DSi_j \,(mod)\, Dn$$

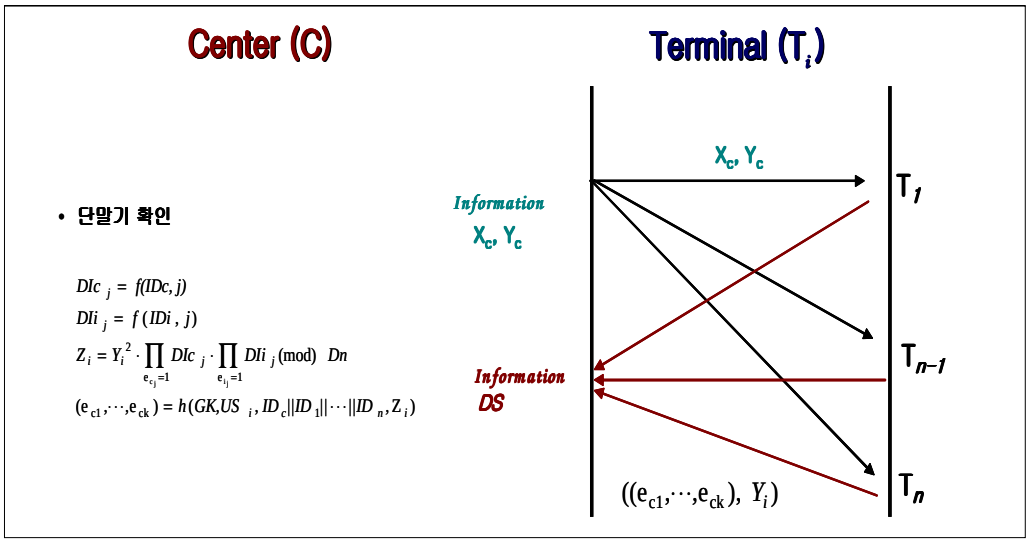
⑤ 키 분배 센터는 각 단말기 T_i의 서명정보로부터 정당한 터미널인지 검사한다.

ㄱ. $DIc_j = f(IDc, j)$

ㄴ. $DIi_j = f(IDi, j)$

ㄷ. $Z_i = Y_i^2 \cdot \prod_{e_{c_j}=1} DIc_j \cdot \prod_{e_{i_j}=1} DIi_j \ (mod)\ Dn$

ㄹ. $(e_{i_1}, \cdots, e_{i_K}) == h(GK, US_i, ID_c \| ID_1 \| \cdots \| ID_n, Z_i)$를 만족하는지 검사 후 인증 한다.



[그림 3.18] 제안된 그룹키 방식 (센터 최종 단말기 확인 단계 3)

C. 제안 방식의 안전성 검토

1. 준비 단계의 안전성

키 분배 센터가 안전하다고 가정하였을 때, 준비 단계에서 어떠한 단말기도 새로운 그룹 공유 비밀 키를 계산할 수 없어야 한다[30].

제안 방식에서는 각 단말기가 다른 단말기의 비밀정보를 알아냈거나, 단말기 간의 결탁에 의해 서로의 비밀정보를 알게 될지라도 연산을 위해서 필요한 Un을 알지 못하기 때문에 센터가 그룹 비밀 키 갱신을 위해 Un을 각 단말기에게 전송하기

전까지 각 단말기는 그룹 비밀 키를 알아낼 수 없다. 이것은 이산대수문제를 해결하는 것과 같기 때문이다.

2. 갱신 단계의 안전성

먼저 배제된 특정 단말기가 센터로부터 동보 전송되는 정보를 이용하여 새로운 그룹 비밀 키를 계산할 수 있는 지 검토한다[30].

제안한 방식은 키 갱신 단계에서 센터로부터 전송되는 정보는 1회의 갱신을 위해 필요한 배제된 단말기 T_i의 비밀정보 US_i, 은닉 정보 UX_i와 모듈라 연산의 제수 Dn 그리고 다음 번 갱신을 위해 사용될 단말기들의 은닉정보를 은닉한 정보 X_i이다. 먼저, 배제된 단말기는 자신의 비밀 정보 이외에 다른 정보를 알 수 없기 때문에 유클리드 알고리즘에 의한 계산이나 그룹의 새로운 공유키를 계산하는 것은 사실상 불가능하다. 다음으로, 정확한 그룹 비밀 키를 계산하지 못한 단말기는 다음 번 그룹 키 갱신을 위해 필요한 은닉정보 UX_i를 X_i로부터 구할 수 없다. 이것은 이산대수문제에 근거한다.

3. 제안 방식 장점

제안 방식은 그룹 비밀 키의 정당한 갱신이 가능한 단말기만이 다음 번 갱신을 위한 은닉 정보를 알 수 있기 때문에 불법적으로 특정 단말기의 비빌 정보를 취득하여 불법적인 도청을 하는 불법 사용자를 영구히 그룹 내의 통신으로부터 배제할 수 있다. 또한 다음과 같은 장점들이 있다.

첫째, 본 방식 준비 단계 이후 대부분의 정보 전송이 동보통신을 통해서 이루어진다.

둘째, 본 방식은 디지털 서명을 이용함으로써 키 센터로 위장한 불법 사용자가 불법적인 키 갱신 정보를 단말기들에게 송신하는 것을 예방할 수 있다.

셋째, 본 방식은 불법적인 사용이 의심되는 사용자를 키 센터가 서명을 이용하여 임의적으로 확인하여 배제할 수 있다.

넷째, 본 방식은 스마트카드와 같은 별도의 장치를 사용하여 그룹 키 갱신을 위한 다량의 정보를 미리 분배하는 것이 아니라 단말기가 그룹 키 갱신을 위한 정보를 단말기 내에서 연산을 통해서 갱신 한다. 따라서 소형 경량의 이동 단말기의 특성을 만족한다.

다섯째, 본 방식에서 그룹 키 갱신 시 전달되는 갱신을 위한 정보들은 이산 대수 문제에 의한 안전한 방식을 사용한다.

여섯째, 본 방식은 새로운 그룹 키 갱신 시 별도의 준비 단계를 필요로 하지 않고 연속하여 안전하고 효율적으로 사용 할 수 있으면, 새로운 단말기가 그룹 내에 진입하는 경우에도 준비과정부터 다시 시작할 필요가 없다.

일곱째, 본 방식은 불법 단말기들이 불법적인 정보로부터 그룹 비밀 키를 계산하는 것을 예방하기위한 추가적인 보호 대책이 필요하지 않다.

Ⅳ. 실험 및 평가

A. 기존 프로토콜과의 비교 분석

첫 번째로 고려해볼 수 있는 키를 재분배하는 방식이다. 이러한 방식에는 대칭키 암호화를 이용하는 방식과 비대칭 암호화 기법을 이용하는 방식이 있다[21,24]. 그러나 이러한 방식은 센터가 많은 회수의 키 분배를 해야 하고 키 전송에 많은 시간이 소요되므로 정상적인 통신을 방해할 수 있고 또한 무선을 기반으로 동보 암호화 통신을 수행하는 하는 디지털 이동 통신 시스템에는 적합하지 않을 수 있다[31,41]. 다음으로 동보 암호화 통신을 통해 그룹 비밀 키 갱신을 위한 정보를 모든 단말기에 동보 전송하는 방식이다. 이러한 방식에는 Matsuzaki-Anzai(MA)방식,Sm-Park-Won(SPW) 방식 그리고 Park-Lee(PL) 방식이 있다[16,29,35]. 특히 이들 방식중 SPW 방식 및 PL 방식은 스마트 카드를 이용하여 다수의 갱신될 그룹 비밀키 정보와 역수 정보를 은익하여 각 단말기에 배포한다. 그러나 이 방식은 단말기의 경량화가 어려워질 수 있으며 갱신의 횟수가 스마트 카드의 용량에 따라 제한된다. 또한 SPW 방식은 사용자간 단합에 의한 그룹 비밀키 유출을 막을 수 없다. 또한 Modular 정보를 미리 제공하기 때문에 2개 이상의 단말기를 동시에 분실 하였을 때 단말기들이 그룹 비밀키를 생성할 수 있거나, 그들의 단합에 의해 그들 간에 그룹 비밀 키를 공유 할 수 있다[29]. 반면에 PL방식은 Modular 정보는 스마트 카드에 저장하여 배포하지 않고 갱신할 때 마다 전송함으로써 단합에 의한 그룹 비밀키 생성의 문제를 해결하였다. 또한 배제되는 단말기들의 갱신을 위한 정보를 동시에 전송하고 그들의 연산을 통해서 그룹 비밀 키를 생성함으로써 동시 배제의 문제를 해결하였다[35]. 하지만 단말기 경량화의 문제와 갱신의 횟수는 스마트 카드의 용량에 따라 제한되는 문제가 따른다. 그러나 이 방식들은 그룹 비밀 키 갱신을 위해 필요한 통신 횟수가 적고 단말기들이 그룹 비밀 키를 자체적으로 갱신하므로, 디지털 이동 통신 시스템에 적합하다고 할 수 있다[42,43].

B. 각 방식별 비교 분석 결과

*1.*각 방식별 키 생성 비교 분석표

각 방식별 키 생성을 위한 데이터는 임의로 컴퓨터가 발생한 랜덤한 소수 값을 이용 5개의 단말기를 가정하여 실험하였다. 먼저 MA 방식에서는 MA방식 수식을 적용하였을 때 [그림 4.2]와 같이 단말기 2번째 배제 후 그룹키 갱신하고 이어서 단말기 4번째를 배제했을 때 기존 배제되어진 단말기가 그룹키 재 갱신이 되어버리는 단점을 보여준다. 마찬가지 스마트 카드를 이용하는 예로 SPW방식을 대표로 실험 했을 때 카드의 슬롯 정보는 갱신 횟수 총 10번으로 가정하고 단말기 3번째를 배제한 경우 [그림 4.6]과 바로 단말기 5번째를 배제한 경우 역시 배제된 단말기가 그룹키를 재 갱신 해버리는 경우가 발생하는 결과를 보여준다. 제안된 그룹키 방식은 [그림 4.10]과 [그림 4.11]에서 보는 결과와 같이 연속해서 배제가 되는 경우에도 일단 한번 배제된 단말기는 그룹키를 재 갱신할 수 없는 결과를 보여준다.

CENTER			
ID	GK 그룹키	Center 비밀정보	연 산 식
568	0	P = 127, Q = 53 ,N = 2459, K = 165 S[5] = 7, 127, 67, 197, 101, X[5] = 1496, 289, 454, 1740, 2453	GCD(S[i], S[j]) = 1 GCD(X[i], N) = 1 X[i] = pow(K, S[i]) mod N

	T1	T2	T3	T4	T5
ID	1734	62	1088	1443	1068
G K	0	0	0	0	0
배포된 정보	$S_i = 7$ $X_i = 1496$ N = 2459	$S_i = 127$ $X_i = 289$ N = 2459	$S_i = 67$ $X_i = 454$ N = 2459	$S_i = 197$ $X_i = 1740$ N = 2459	$S_i = 101$ $X_i = 2453$ N = 2459
배제 단말기	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$
계산된 값	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1a = 0$, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0
연 산 식	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N

[그림 4.1] MA 방식 그룹키 갱신 준비단계

CENTER			
ID	K 그룹키	Center 비밀정보	연 산 식
568	165	P = 127, Q = 53 ,N = 2459, K = 165 S[5] = 7, 127, 67, 197, 101, X[5] = 1496, 289, 454, 1740, 2453	GCD(S[i], S[j]) = 1 GCD(X[i], N) = 1 X[i] = pow(K, S[i]) mod N

	T1	T2	T3	T4	T5
ID	1734	62	1088	1443	1068
K	165	1379	165	165	165
배포된 정보	S_i = 7 Xj = 1496 N = 2459	S_j = 127 Xj = 289 N = 2459	S_i = 67 Xj = 454 N = 2459	S_i = 197 Xj = 1740 N = 2459	S_i = 101 Xj = 2453 N = 2459
배제 단말기	S_i = 127 X_i = 289	S_i = 127 X_i = 289	S_i = 127 X_i = 289	S_i = 127 X_i = 289	S_i = 127 X_i = 289
계산된 값	a * S_i + b * S_j = 1 a = 1, b = −18	a * S_i + b * S_j = 1 a = 0, b = 1	a * S_i + b * S_j = 1 a = 19, b = −36	a * S_i + b * S_j = 1 a = −76, b = 49	a * S_i + b * S_j = 1 a = 35, b = −44
연 산 식	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N

[그림 4.2] MA 방식 그룹키 갱신 단계 (단말기 2 배제)

CENTER			
ID	K 그룹키	Center 비밀정보	연 산 식
568	165	P = 127, Q = 53 ,N = 2459, K = 165 S[5] = 7, 127, 67, 197, 101, X[5] = 1496, 289, 454, 1740, 2453	GCD(S[i], S[j]) = 1 GCD(X[i], N) = 1 X[i] = pow(K, S[i]) mod N

	T1	T2	T3	T4	T5
ID	1734	62	1088	1443	1068
K	165	165	165	2099	165
배포된 정보	S_i = 7 Xj = 1496 N = 2459	S_i = 127 Xj = 289 N = 2459	S_i = 67 Xj = 454 N = 2459	S_j = 197 Xj = 1740 N = 2459	S_i = 101 Xj = 2453 N = 2459
배제 단말기	S_i = 197 X_i = 1740	S_i = 197 X_i = 1740	S_i = 197 X_i = 1740	S_i = 197 X_i = 1740	S_i = 197 X_i = 1740
계산된 값	a * S_i + b * S_j = 1 a = 1, b = −28	a * S_i + b * S_j = 1 a = 49, b =−76	a * S_i + b * S_j = 1 a = −17, b = 50	a * S_i + b * S_j = 1 a = 0, b = 1	a * S_i + b * S_j = 1 a = 20, b = −39
연 산 식	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_j, a) * pow(inv(X_i), -b) mod N

[그림 4.3] MA방식 (단말기 4 배제 후 배제된 단말기2 그룹 키 재갱신 발생)

CENTER			
ID	GK 그룹키	Center 스마트 카드 정보	연 산 식
1175	0	스마트 카드 슬롯의 개수 10 센터가 생성한 스마트카드 정보 터미널 i(=1): K, P, T, Y, inv(Y)	i =스마트카드 번호, j = 슬롯의 번호 GCD(T[i] [j], T[i] [k]) = 1 Y[i] [j] = pow(K[i] [j], T[i] [j]) mod P[i] [j]

	T1	T2	T3	T4	T5
	K, P, T, Y, inv(Y)	K, P, T, Y, inv(Y)	K, P, T, Y, inv(Y)	K, P, T, Y, inv(Y)	K, P, T, Y, inv(Y)
Slot 1	1045, 3571, 1277, 1967, 1574	1045, 3571, 431, 1388, 548	1045, 3571, 1913, 1166, 1761	1045, 3571, 131, 20, 1607	1045, 3571, 281, 799, 1895
Slot 2	187, 23447, 283, 3456, 22314	187, 23447, 1657, 16249, 14134	187, 23447, 127, 19380, 1424	187, 23447, 1609, 9408, 9154	187, 23447, 1733, 17598, 7356
Slot 3	365, 499, 1087, 104, 24	365, 499, 19, 487, 291	365, 499, 1973, 291, 487	365, 499, 1601, 118, 351	365, 499, 1483, 110, 186
Slot 4	1107, 15031, 1613, 6409, 2418	1107, 15031, 727, 1461, 7212	1107, 15031, 1217, 12658, 12529	1107, 15031, 457, 173, 2259	1107, 15031, 607, 6940, 3095
Slot 5	498, 29153, 127, 26383, 4073	498, 29153, 1493, 19261, 23969	498, 29153, 761, 18825, 1019	498, 29153, 1657, 7765, 23833	498, 29153, 1399, 18965, 5062
Slot 6	1346, 8059, 479, 3868, 3019	1346, 8059, 1531, 4160, 1513	1346, 8059, 59, 7216, 3010	1346, 8059, 1423, 1056, 7914	1346, 8059, 89, 1384, 4967
Slot 7	950, 8741, 431, 5835, 7601	950, 8741, 373, 7821, 4380	950, 8741, 1811, 1715, 8583	950, 8741, 107, 6943, 5722	950, 8741, 487, 3052, 7730
Slot 8	1608, 19889, 907, 4661, 4489	1608, 19889, 1511, 13505, 1997	1608, 19889, 593, 8891, 16925	1608, 19889, 503, 5352, 18488	1608, 19889, 547, 8501, 2859
Slot 9	1775, 12659, 787, 6516, 9910	1775, 12659, 1163, 9778, 6402	1775, 12659, 1373, 1500, 10642	1775, 12659, 1811, 7864, 2545	1775, 12659, 1823, 9767, 731
Slot 10	1728, 32707, 383, 31978, 19023	1728, 32707, 709, 8511, 25711	1728, 32707, 353, 27771, 17036	1728, 32707, 89, 6776, 19100	1728, 32707, 719, 20996, 24901

[그림 4.4] SPW 방식 (그룹키 갱신 Center 준비단계)

CENTER			
ID	GK 그룹키	Center 스마트 카드 정보	연 산 식
1175	0	스마트 카드 슬롯의 개수 10 센터가 생성한 스마트카드 정보 터미널 i(=1): K, P, T, Y, inv(Y)	i =스마트카드 번호, j = 슬롯의 번호 GCD(T[i] [j], T[i] [k]) = 1 Y[i] [j] = pow(K[i] [j], T[i] [j]) mod P[i] [j]

	T1	T2	T3	T4	T5
ID	1348	1940	643	1893	1580
K	0	0	0	0	0
배포된 스마트 카드 정보	P, Tj, Yj, inv(Yj) S1: 3571,1277,1967,1574 S2: 123447,283,3456,22314 :	P, Tj, Yj, inv(Yj) S1: 3571,431,1388,548 S2: 23447,1657,16249, 14134 :	P, Tj, Yj, inv(Yj) S1: 3571,1913,1166,1761 S2: 23447,127,19380,1424 :	P, Tj, Yj, inv(Yj) S1: 3571,131,20, 1607 S2: 23447,1609, 9408,9154 :	P, Tj, Yj, inv(Yj) S1: 3571, 281, 799, 1895 S2: 23447,1733,17598, 7356 :
배제 단말기	Slot : P, T_j, Y_j, inv(Y_j) 0, 0, 0, 0	Slot : P, T_j, Y_j, inv(Y_j) 0, 0, 0, 0	Slot : P, T_j, Y_j, inv(Y_j) 0, 0, 0, 0	Slot : P, T_j, Y_j, inv(Y_j) 0, 0, 0, 0	Slot : P, T_j, Y_j, inv(Y_j) 0, 0, 0, 0
계산된 값	$a * T_i + b * T_j = 1$ a = 0, b = 0	$a * T_i + b * T_j = 1$ a = 0, b = 0	$a * T_i + b * T_j = 1$ a = 0, b = 0	$a * T_i + b * T_j = 1$ a = 0, b = 0	$a * T_i + b * T_j = 1$ a = 0, b = 0
연산식	a<0, K = pow(inv(Y_i), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_i), -b) mod P	a<0, K = pow(inv(Y_i), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_i), -b) mod P	a<0, K = pow(inv(Y_i), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_i), -b) mod P	a<0, K = pow(inv(Y_i), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_i), -b) mod P	a<0, K = pow(inv(Y_i), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_i), -b) mod P

[그림 4.5] SPW 방식 (그룹키 갱신 단말기 준비단계)

CENTER			
ID	GK 그룹키	Center 스마트 카드 정보	연 산 식
1175	1045	스마트 카드 슬롯의 개수 10 센터가 생성한 스마트카드 정보 터미널 i(=1): K, P, T, Y, inv(Y)	i =스마트카드 번호, j = 슬롯의 번호 GCD(T[i] [j], T[i] [k]) = 1 Y[i] [j] = pow(K[i] [j], T[i] [j]) mod P[i] [j]

	T1	T2	T3	T4	T5
ID	1348	1940	643	1893	1580
K	**1045**	**1045**	**2692**	**1045**	**1045**
배포된 스마트 카드 정보	P, Tj, Yj, inv(Yj) S1: 3571,1277,1967,1574 S2: 123447,283,3456,22314 :	P, Tj, Yj, inv(Yj) S1: 3571,431,1388,548 S2: 23447,1657,16249, 14134 :	P, Tj, Yj, inv(Yj) S1: **3571,1913,1166,1761** S2: 23447,127,19380,1424 :	P, Tj, Yj, inv(Yj) S1: 3571,131,20, 1607 S2: 23447,1609, 9408,9154 :	P, Tj, Yj, inv(Yj) S1: 3571, 281, 799, 1895 S2: 23447,1733,17598, 7356 :
배제 단말기	Slot1 : P, Tj, Yj, nv(Yj) **3571,1913,1166,1761**	Slot1 : P, Tj, Yj, nv(Yj) **3571,1913,1166,1761**	Slot1 : P, Tj, Yj, nv(Yj) **3571,1913,1166,1761**	Slot1 : P, Tj, Yj, nv(Yj) **3571,1913,1166,1761**	Slot1 : P, Tj, Yj, nv(Yj) **3571,1913,1166,1761**
계산된 값	$a * T_j + b * T_j = 1$ a = 255, b = −382	$a * T_j + b * T_j = 1$ a =187, b = −830	$a * T_j + b * T_j = 1$ a = 0, b = 1	$a * T_j + b * T_j = 1$ a = −63, b = 920	$a * T_j + b * T_j = 1$ a = 26, b = −177
연산식	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P

[그림 4.6] SPW 방식 (그룹키 갱신 단말기 3 배제)

CENTER			
ID	GK 그룹키	Center 스마트 카드 정보	연 산 식
1175	187	스마트 카드 슬롯의 개수 10 센터가 생성한 스마트카드 정보 터미널 i(=1): K, P, T, Y, inv(Y)	i =스마트카드 번호, j = 슬롯의 번호 GCD(T[i] [j], T[i] [k]) = 1 Y[i] [j] = pow(K[i] [j], T[i] [j]) mod P[i] [j]

	T1	T2	T3	T4	T5
ID	1348	1940	643	1893	1580
K	**187**	**187**	**187**	**187**	**19232**
배포된 스마트 카드 정보	P, Tj, Yj, inv(Yj) S1: 3571,1277,1967,1574 S2: 123447,283,3456,22314 :	P, Tj, Yj, inv(Yj) S1: 3571,431,1388,548 S2: 23447,1657,16249, 14134 :	P, Tj, Yj, inv(Yj) S1: 3571,1913,1166,1761 S2: 23447,127,19380,1424 :	P, Tj, Yj, inv(Yj) S1: 3571,131,20, 1607 S2: 23447,1609, 9408,9154 :	P, Tj, Yj, inv(Yj) S1: 3571, 281, 799, 1895 S2: **23447,1733,17598, 7356** :
배제 단말기	Slot2 : P, Tj, Yj, nv(Yj) **23447,1733,17598,7356**	Slot2 : P, Tj, Yj, nv(Yj) **23447,1733,17598,7356**	Slot2 : P, Tj, Yj, nv(Yj) **23447,1733,17598,7356**	Slot2 : P, Tj, Yj, nv(Yj) **23447,1733,17598,7356**	Slot2 : P, Tj, Yj, nv(Yj) **23447,1733,17598,7356**
계산된 값	$a * T_j + b * Tj = 1$ a = −97, b = 594	$a * T_j + b * Tj = 1$ a =−109, b = 114	$a * T_j + b * Tj = 1$ a = −48, b = 655	$a * T_j + b * Tj = 1$ a = −532, b = 573	$a * T_j + b * Tj = 1$ a = 0, b = 1
연산식	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P	a<0, K = pow(inv(Y_j), -a) * pow(Y_j, b) mod P b<0, K = pow(Y_j, a) * pow(inv(Y_j), -b) mod P

[그림 4.7] SPW 방식 (연속 단말기 5 배제후 배제된 단말기 3 그룹키 재갱신 발생)

CENTER			
ID	K 그룹키	Center 비밀정보	연 산 식
491	157	P =127, Q = 97, N = 12319, K = 293 S0[5] = 0,0,0,0,0 X0[5] = 0,0,0,0,0 S[5] = 191,149,431,419,83 X[5] = 1019,1972,9167,9786,4451	GCD(S[i], S[j]) = 1 GCD(X[i], N) = 1 X[i] = pow(K, S[i]) mod N

	T1	T2	T3	T4	T5
ID	948	1707	733	1342	1686
K	**157**	**157**	**157**	**157**	**157**
이전 배포된 정보	$S0_i = 0$ $X0_i = 0$	$S0_i = 0$ $X0_i = 0$	$S0_i = 0$ $X0_i = 0$	$S0_i = 0$ $X0_i = 0$	$S0_i = 0$ $X0_i = 0$
현재 배포된 정보	$S_i = 191$ $X_i = 1019$ N = 12319	$S_i = 149$ $X_i = 1972$ N = 12319	$S_i = 431$ $X_i = 9167$ N = 12319	$S_i = 419$ $X_i = 9786$ N = 12319	$S_i = 83$ $X_i = 4451$ N = 12319
배제 단말기	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$	$S_i = 0$ $X_i = 0$
계산된 값	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1a = 0$, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0
연 산 식	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N

[그림 4.8] 제안된 그룹키 갱신 준비단계

CENTER			
ID	K 그룹키	Center 비밀정보	연 산 식
491	**293**	P =127, Q = 97, N = 12319, K = 367 S0[5] = 191,149,431,419,83 X0[5] = 1019,1972,9167,9786,4451 S[5] = 307,3607,439,12197,9787 X[5] = 7818,3696,9225,860,3671	GCD(S[i], S[j]) = 1 GCD(X[i], N) = 1 X[i] = pow(K, S[i]) mod N

	T1	T2	T3	T4	T5
ID	948	1707	733	1342	1686
K	**293**	**5541**	**293**	**293**	**293**
이전 배포된 정보	$S0_i = 191$ $X0_i = 1019$	**$S0_i = 149$** **$X0_i = 1972$**	$S0_i = 431$ $X0_i = 9167$	$S0_i = 419$ $X0_i = 9786$	$S0_i = 83$ $X0_i = 4451$
현재 배포된 정보	$S_i = 307$ $X_i = 7818$ N = 12319	$S_i = 2897$ $X_i = 3696$ N = 12319	$S_i = 439$ $X_i = 9225$ N = 12319	$S_i =12197$ $X_i = 860$ N = 12319	$S_i = 9787$ $X_i = 3671$ N = 12319
배제 단말기	**$S_i = 149$** **$X_i = 1972$**	**$S_i = 149$** **$X_i = 1972$**	**$S_i = 149$** **$X_i = 1972$**	**$S_i = 149$** **$X_i = 1972$**	**$S_i = 149$** **$X_i = 1972$**
계산된 값	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1a = 0$, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0
연 산 식	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N

[그림 4.9] 제안된 그룹키 갱신단계(단말기 2 배제)

CENTER			
ID	K 그룹키	Center 비밀정보	연 산 식
491	367	P =127, Q = 97, N = 12319, K = 367 S0[5] = 307,3607,439,12197,9787 X0[5] = 7818,3696,9225,860,3671 S[5] = 12157,9511,4327,8081,7823 X[5] =7557,5525,8144,5747,4322	GCD(S[i], S[j]) = 1 GCD(X[i], N) = 1 X[i] = pow(K, S[i]) mod N

	T1	T2	T3	T4	T5
ID	948	1707	733	1342	1686
K	367	5541	367	293	367
이전 배포된 정보	$S0_i$ = 307 $X0_i$ = 7818	$S0_i$ = 2897 $X0_i$ = 3696	$S0_i$ = 439 $X0_i$ = 9225	$S0_i$ = 12197 $X0_i$ = 860	$S0_i$ = 9787 $X0_i$ = 3671
현재 배포된 정보	S_i = 12157 X_i = 7557 N = 12319	S_i =8147 X_i = 5525 N = 12319	S_i = 4327 X_i = 8144 N = 12319	S_i =6733 X_i = 5747 N = 12319	S_i = 7823 X_i = 4322 N = 12319
배제 단말기	S_i = 12197 X_i = 860	S_i = 12197 X_i = 860	S_i = 12197 X_i = 860	S_i = 12197 X_i = 860	S_i = 12197 X_i = 860
계산된 값	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1a = 0$, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0
연 산 식	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N

[그림 4.10] 제안된 그룹키 갱신(단말기 2,4 연속 배제)

CENTER			
ID	K 그룹키	Center 비밀정보	연 산 식
491	397	P =127, Q = 97, N = 12319, K = 41 S0[5] = 12157,9511,4327,8081,7823 X0[5] =7557,5525,8144,5747,4322 S[5] = 5471,3181,5501,10037,9689 X[5] =750,2711,5349,1666,8268	GCD(S[i], S[j]) = 1 GCD(X[i], N) = 1 X[i] = pow(K, S[i]) mod N

	T1	T2	T3	T4	T5
ID	948	1707	733	1342	1686
K	397	10161	397	9303	6352
이전 배포된 정보	$S0_i$ = 12157 $X0_i$ = 7557	$S0_i$ = 8147 $X0_i$ = 5525	$S0_i$ = 4327 $X0_i$ = 8144	$S0_i$ = 6733 $X0_i$ = 5747	$S0_i$ = 7823 $X0_i$ = 4322
현재 배포된 정보	S_i = 5471 X_i = 750 N = 12319	S_i =6607 X_i = 2711 N = 12319	S_i = 5501 X_i = 5349 N = 12319	S_i =641 X_i = 1666 N = 12319	S_i = 12203 X_i = 8268 N = 12319
배제 단말기	S_i = 7823 X_i = 4322	S_i = 7823 X_i = 4322	S_i = 7823 X_i = 4322	S_i = 7823 X_i = 4322	S_i = 7823 X_i = 4322
계산된 값	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0	$a * S_i + b * S_j = 1a = 0$, b = 0	$a * S_i + b * S_j = 1$ a = 0, b = 0
연 산 식	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N	a<0, K = pow(inv(X_i), -a) * pow(X_j, b) mod N b<0, K = pow(X_i, a) * pow(inv(X_j), -b) mod N

[그림 4.11] 제안된 그룹키 갱신(단말기 2,4,5 연속 배제)

2. 통신횟수와 통신량

a. [준비단계] - 센터가 보냄 (k : 갱신횟수, n : 단말기대수)

(K : 스마트 카드 정보 내 가능 갱신 횟수) , n : 단말기 개수)

System	준 비 단 계			
	통신횟수	통신량	전 송 데 이 터	합계
M A	n	2	S_i, X_i	2n
S P W	n	4 * k	S_{ij}, Y_{ij}, Y_{ij}^{-1}, P_j	4 kn
P L	n	3 * k	S_{ij}, Y_{ij}, Y_{ij}^{-1}	3 kn
제안 방식	1	2	UX_i , US_i	2 n

[그림 4.12] 각 방식별 통신횟수와 통신량 (준비단계)

b. [갱신단계] : 배제하고자하는 단말기 1

(C: 배제 단말기 개수 , n : 단말기 개수)

System	갱 신 단 계			
	통신횟수	통신량	전 송 데 이 터	합계
M A	n	3	S_{i1}, X_{i1}, n	3n
S P W	n	4	S_{i1}, Y_{i1}, Y_{i1}^{-1}, P_j	4n
P L	n	4 * c	S_{i1}, Y_{i1}, Y_{i1}^{-1}, P_j	4cn
제안 방식	c	4	US_i, UX_i, Un, X_i	4cn

[그림 4.13] 각 방식별 통신횟수와 통신량 (갱신단계)

3. 각 방식별 비교 분석 결과

제안 방식은 그룹 비밀키의 정당한 갱신이 가능한 단말기만이 다음 번 갱신을 위한 은닉정보를 알 수 있기 때문에 불법적으로 특정 단말기의 비밀정보를 취득하여 불법적인 도청을 하는 불법 사용자를 영구히 그룹내의 통신으로부터 배제 할 수 있다. 그러므로 다른 기존 방식과는 달리 그룹키의 갱신은 횟수에 관계없이 갱신이 가능하며 기존의 문제가 되었던 부분인 2명이상의 그룹키를 연속하여 갱신할 수 있다. 이는 그룹키 분배 및 갱신 프로토콜 설계시 중요한 요구사항중 그룹 멤버의 변화로 어떤 멤버가 더 이상 그룹 멤버가 아니거나 수동적인 적(Passive adversary)이 옛 그룹키의 서브셋을 알더라도 앞으로 그룹에서 사용할 새로운 그룹키에 대해서 알 수 없어야 하는 전방 비밀성(Forward Secrecy), 그룹 멤버의 변화로 새로운 멤버가 그룹에 가입되거나 수동적인 적이 그룹키의 서브셋을 알더라도 이전에 그룹 통신에 사용된 그룹키에 대해서 알 수 없어야 하는 후방 비밀성(Backward Secrecy)을 만족한다 할 수 있다. 또한 기존에 없었던 Fiat-Shamir 방식을 적용하여 인증을 요하는 Mobile 환경에 효과적인 방식을 도입하여 인증으로 인한 불법 단말기 자동배제를 하여 발전된 그룹키 갱신 방식을 제안하였다.

Comparative \ System	MA	SPW	PL	제안 방식
Forward Secrecy	X	X	X	O
Backward Secrecy	X	X	X	O
단합 해결	X	X	O	O
확인 및 인증	X	X	X	O
암호화 통신	O	O	O	O

[그림 4.14] 각 방식별 비교 분석 결과

V. 결론 및 향후 연구

본 논문은 디지털 이동 통신에서 사용되는 그룹키 갱신 및 보안 문제를 해결하고자 하였다. 이를 위해 먼저 기존의 방식들의 고찰을 통하여 그룹키 갱신의 문제점을 분석하였다. 이동 통신 환경에 있어서 그룹키 갱신의 문제는 통신 단말기를 분실하였을 때 이 단말기의 공유 그룹비밀 키나 비밀 정보를 이용하여 그룹 내의 통신을 쉽게 도청하거나 허위 정보를 유포할 수 있다. 공유 그룹 비밀 키를 이용한 도청이나 허위 정보 유포는 그룹 비밀 키의 갱신을 통해서 예방할 수 있지만, 비밀 정보를 이용한 도청이나 허위 정보 유포는 단순한 그룹 비밀 키의 갱신을 통해서 예방하기는 어려운 점이 있다. 특히 동보통신이 이루어지고 있는 상황에서는 더욱 심각하다. 기존 방식들은 특정 단말기 내에 있는 그룹 키를 갱신을 위한 비밀정보를 불법적으로 취득한 불법 사용자를 1회의 그룹 키 갱신을 통해서 배제할 수 있지만, 2회부터는 배제할 수 없다는 문제를 가지고 있다.

본 제안 방식은 ID 보안 기술에 기반을 둔 디지털 서명, 키분배 기법을 이용하여 그룹 비밀키의 분배와 갱신을 위한 효율적인 프로토콜을 제안한다. 제안된 프로토콜의 안전성은 Fiat-Shamir의 ID 기반의 디지털 서명과 Diffie-Hellman의 키 분배 방식을 이용하여 이산대수 어려움에 근거하고 있으며 단말기의 저장능력과 처리의 능력이 적을 경우도 적절하게 운영될 수 있고,단말기의 변동 없이 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있도록 설계하였다. 이는 소형 경량의 이동 단말기를 위해 스마트카드와 같은 부가적인 장치의 없이 그룹 비밀 키를 갱신할 수 있는 방식이며 디지털 서명을 이용함으로써 키센터로 위장한 불법 사용자가 키 갱신 정보를 단말기들에게 송신하는 것을 예방 할 수 있다. 또한 이를 이용하여 사용자들을 인증함으로써 불법적인 단말기를 배제할 수 있다. 그리고 특정한 공간에서 소규모 그룹회의를 고려한 쉬운 키 생성과 갱신을 위주로 오직 사전에 허가된 사용자만이 그룹키를 이용하여 디지털 정보를 얻을 수 있게 함

으로써 사용자가 탈퇴나 새로운 가입 시 효율적인 키 캥신 메커니즘이다. 중요한 것은 그룹 키 갱신을 위해 필요한 비밀 정보가 그룹 키 갱신 시마다 동시에 갱신되므로 단말기의 안전성을 보장할 수 있고 불법 단말기들이 영구적으로 정확한 그룹 비밀 키를 갱신할 수 없게 할 수 있다는 점이다. 이는 그룹 비밀 키 생성을 위한 스마트카드와 같은 부가적인 장치가 필요 없으며 준비 단계이후 계속적으로 안전하게 그룹 비밀 키를 갱신하면서 그룹 내의 통신을 수행할 수 있는 효과적인 방식이다.

본 논문에서 제시한 새로운 그룹키 갱신 메커니즘은 소규모 회의 시스템에서부터 Ad-hoc 네트워크, 센서 네트워크등 다양한 환경에서 사용이 가능하다. 그러나 현재 활발히 연구가 진행 중인 유비쿼터스 센서 네트워크 환경에도 적용은 가능하나 센서 네트워크 노드에 사용되는 하드웨어 처리능력의 기술적인 한계로 인해 본 논문에서 제안한 방식을 그대로 사용할 경우 동보 전송으로 인하여 발생되는 데이터의 오버헤드로 인해 어려움이 따른다. 따라서 향후 제안한 방식을 적용하기 위해서는 이 환경에 적합하고 안정적인 데이터 구성에 관한 연구가 선행되어야 할 것이다.

참 고 문 헌

[1] A. Fiat and A. Shamir, “How to prove yourself : Practical Solutions to identification and signature problems,” Proceedings of Crypto, LNCS 263, pp. 186-194, 1986.

[2] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, pp. 103-113, 1997.

[3] A. Menezes, M.Qu and S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication,” Workshop on Selected Area in Cryptography, pp. 22-32, 1995.

[4] B. Bird, I. Goa, A. Herzaberg, P. Janson, S. Kutte, R. Molva and M. Yung, "Systematic design of a family of Attack-resistant authentication protocols,” IEEE Journal on Selected Areas in Communications, vol. 11, no. 5, pp. 679-693, 1993.

[5] C. H. Lim and P. J. Lee, "A Key Recovery Attack on discrete log-based schemes using a prime order subgroup,” Proceedings of Crypto, LNCS 1294, pp. 249-463, 1997.

[6] C. S. Park, “On Certificate-Based Security Protocol for Wireless Mobile Communication Systems,” IEEE Network, vol. 11, no. 5, pp. 50-55, 1997.

[7] C. S. Park, K. Kaoru, T. Okamoto and S. Tsujii, "On Key Distribution and Authentication in Mobile Radio Networks,” Proceedings of Eurocrypt, LNCS 765, pp. 461-465, 1993.

[8] ETSI-RES, European Telecommunication Standard, ETS 300 175-7, DECT, Common Interface, part 7: Security features, 1992.

[9] George H. Forman and John Zahorjan, "The Challenges of Mobile Computing,”

Technical Report 93-11-03, Department of Computer Science and Engineering, University of Washington, December 1993.

[10] J. Kelsey, B. Schneier and D. Wagner, "Protocol Interactions and the Chosen Protocol Attack," Proceedings of the 5th International Workshop on Security Protocols, pp. 233-246, April 1998.

[11] Keith Martin and Chris Mitchell, "Evaluation of Authentication Protocols for Mobile Environment Value-Added Services," Draft, Available on-line as http://isg.rhbnc.ac.uk/cjm/EOAPFM.ZIP, 1998.

[12] M. Burmester, "On the risk of opening distribution keys," Proceedings of Crypto, LNCS 839, pp. 308-317, 1994.

[13] M. Tatebayashi, N. Matsuzaki, and D. B. Newman, Jr., "Key distribution Protocol for digital mobile communication systems," Proceedings of Crypto, LNCS 435, pp. 324-334, 1989.

[14] M. J. Beller, L. Chang, and Y. Yacobi, "Privacy and Authenticaion on a Portable Communications System," IEEE Global Telecommunications Conference, pp. 1922-1927, 1988.

[15] N. Asokan, "Security Issues in Mobile Computing", CS 690B- Research Proposal, April 1995. Available on-line as http://www.semper.org/sirene/people/asokan/research/proposal.ps.gz.

[16] N. Matsuzaki and J. Anzai, "A Group Key Renewal Method Suitable for Mobile Telecommunications," Proceedings of SCIS, 5.2.E., 1998.

[17] R. Anderson and S. Vaudenay, "Minding your p's and q's," Proceedings of Asiacrypt, LNCS 1163, pp. 15-25, 1996.

[18] R. L. Rivest and A. Shamir, "How to expose an eavesdropper," Communications of the ACM, vol. 27, no. 4, pp. 393-395, 1984.

[19] Shamir, A. "Identity-based cryptosystem and signature scheme," Proceedings of Crypto, LNCS 196, pp. 47-53, 1984.

[20] Simon Blake Wilson and Alfred Menezeds, "Unknown Key-share Attacks on the station-to station(STS) Protocol," University of Waterloo Dept. of Combinatorics and Optimization, Research Report, CORR 98-42, 1998.

[21] T. Hwang, "Scheme for Secure Digital Mobile Communications based on Symmetric Key Cryptography," Information Processing Letters, vol. 48, pp. 35-37, 1993.

[22] TIA/EIA Telecommunications Systems Bulletin, Cellular Radio telecommun ications Intersystem Operations: Authentication, Signaling Message Encryption and Voice Privacy, TSB 51, 1995.

[23] W. Adams and L.Goldstein, "Introduction to Number Theory," Prentice Hall, 1976.

[24] W. Diffie and M. Hellman. "New Directions in Cryptography," IEEE Transaction. Information. Theory, vol. 22, pp. 644-654, 1976.

[25] W. Diffie, P. C, .Oorschot and M.J.Wiener, "Authentication and Authenticated Key Exchange," Designs, Codes and Cryptography, vol. 2, no. 2, pp. 107-125, 1992.

[26] 강창구, "디지털 다중서명 방식과 응용에 관한 연구," 충남대학교 공학박사학위논문, 1993.

[27] 김성열, "ID기반의 디지털 서명 기술을 이용한 이동 에이전트 보안 시스템에 관한 연구," 조선대학교 이학박사학위논문, 2000.

[28] 문태욱, 박상우, 이정숙, 조성준. "디지털 이동통신 시스템에서 스마트 카드를 이용하는 키 분배 프로토콜," 한국통신정보보호학회논문지, 제4권, 제2호, pp. 3-16, 1994.

[29] 심주걸, 박춘식, 원동호. “디지털 이동통신시스템에 적합한 그룹 공유키 경신 방식,” 한국통신정보보호학회논문지, 제10권, 제3호, pp. 69-76, 2000.

[30] 이필중, 임채훈, “일반화된 Diffie-Hellman 키분배 방식의 안전성 분석,” 한국정보통신학회논문지, 제16권, 제7호, pp. 575-597, 1997.

[31] 임채훈, 이필중, “상호 신분 인증 및 디지털 서명기법에 관한 연구,” 통신정보보호학회논문지, 제2권, 제1호, pp. 16-33, 1992.

[32] 조동욱, 최연이, 김희도, 원동호. “이동통신환경에 적합한 상호인증을 제공하는 키분배 프로토콜의 설계,” 한국통신정보보호학회논문지, 제10호, 제2호, pp. 21-29, 2000.

[33] 한국전자통신연구소, “현대암호학,” pp. 157-170, 1991.

[34] 박영희, “Diffie-Hellman 키 교환을 이용한 구성원의 계층적 구조에 기반한 그룹키 동의 프로토콜,” 카이스트 석사논문, 2002.

[35] 박희운, 이임영, “효율적인 이동통신 그룹키 갱신 방식 제안,” 한국정보과학회논문지, 제8권, 제1호, pp. 367-370, 2001.

[36] 조동욱, “다중 통신환경에 적합한 상호인증을 제공하는 키 분배 프로토콜에 관한 연구,” 성균관대학교 석사논문, 1999.

[37] 이덕규, 이임영, “브로드캐스트 암호화에서의 효율적인 키 캥신 방법에 관한 연구,” 한국정보보호학회 논문집, 제13권, 제1호, pp. 263-267, 2003.

[38] 남정현, 이진우, “안전성이 증명 가능한 효율적인 동적 그룹 키 교환 프로토콜,” 정보보호 학회 논문지, 제14권, 제4호, pp. 163-165, 2004.

[39] P.Syverson, ″ A Taxonomy of Replay Attacks,” Proceedings of the 7th IEEE Computer Security Foundations Workshop, pp. 131-136, 1994.

[40] 박영호, 이경현, “ 이동 네트워크 환경에서의 그룹키 관리 구조,” 정보보호학회논문지, 제12권, 제2호, pp. 89-91, 2002.

[41] 황정연, 최규영, 이동훈, 백종명, “ 효율적인 패스워드 기반 그룹키 교환 프로토콜,” 정보보호학회 논문지, 제14권, 제1호, pp. 59-60, 2004.

[42] 탁동길, 정일용, “ 효율적인 모바일 통신을 위한 그룹 키 갱신 메커니즘의 설계,” 전자정보통신연구소 논문지, 제8권, 제2호, pp. 113-122, 2005.

[43] 탁동길, 정일용, “ Fiat-Shamir 방식을 적용한 디지털 모바일 통신 그룹키 갱신 메커니즘,” 한국 해양정보통신학회 논문지, 제10권, 제3호, pp. 571-577, 2006.