이동 에이전트에 대한 신뢰 센터 기반 단방향 엔티티 인증 기법

이 기 현† · 노 환 주††

요 약

이동 에이전트와 같은 분산 이동 객체를 사용한 전자상거래 시스템인 경우 원격 이동 엔티티에 대한 정확하고 안전한 신분 확인 및 신원 검증 과정을 필요로 한다. 본 연구에서는 기존의 양방향 기반 이동 에이전트 인증 기법에 대한 성능 분석 및 안전성 분석을 통해 이산 대수 기법에 기반한 Schnorr형 인증 기법을 개선하고 ElGamal기법을 변형 발전시킨 인증 기법을 제시하였다. 제안한 기법은 이동 에이전트 서버에 기반한 컴퓨팅 시스템에 적용하기 위해 불확정 전송 기반 단방향 인증 기법으로 분산 이동 컴퓨팅 환경에서의 에이전트 인증에 적합한 성능과 안전성을 제공한다.

Trusted Third Party(TTP) Based Mono-directional Entity Authentication Scheme in Mobile Agent

Kee-Hyun Lee† · Hwan-Joo Noh††

ABSTRACT

Electronic commerce system based on distributed mobile object such as mobile agents need both precise identification and secure authentication scheme on remote mobile entities. In this paper, existing discrete logarithm based Schnorr like entity authentication schemes are improved by the analysis of performance and security on the bi-directional interactive proofs. And ElGamal like schemes are also proposed. Then, these are enhanced with oblivious transfer based mono-directional authentication schemes based on trusted third party for applying to the mobile agent based computing systems. Therefore, proposed schemes provide compatible performance and safety on mobile entity authentication processes.

1. 서 론

이동 컴퓨팅 환경에서 각종 서비스를 제공하고자 할 때 가장 중요한 것은 이동 엔티티의 신원을 확인하는 과정이다. 이동 객체에 의한 분산 이동 에이전트 기반 컴퓨팅 구조 또는 셀룰러 이동 통신 기반 시스템인 경우 원격 엔티티에 대한 정확한 신분 확인 및 신원 검증 과정이 필요하다[1-6]. 유선망 기반 네트워크 시스템 환경과 마찬가지로 무선망 기반 이동 컴퓨팅 환경 역시 명확한 인증 과정이 반드시 제공되어야 한다.

본 연구에서는 기존의 인증 기법에 대한 분석을 바탕으로 이동 컴퓨팅 환경에 적합한 엔티티 인증 기법을 제시한다. Schnorr기법[7] 및 Okamoto기법[8] 기법과 같은 양방향(bi-directional) 인증 방식을 개선하고 변형된 ElGamal기법[14]을 적용하여 성능과 안전성을 개선하였다. 또한 불확정 전송[18] 방식과 접목한 단방향(mono-directional) 인증 기법을 제시하였고 이를 단방

† 종신회원 : 명지대학교 컴퓨터공학과 교수
†† 종신회원 : 동국대학교 전자계산원 전임교원
논문접수 : 1999년 10월 15일, 심사완료 : 1999년 11월 12일

향 증명으로 발전시켰다. 본 연구에서 제시하는 단방향 인증 기법은 안전성 분석 및 성능 비교 분석을 바탕으로 이동 엔티티 인증 분야에 직접 적용할 수 있다. 본 연구의 구성은 다음과 같다. 2장에서 기존의 이동 에이전트에 대한 고찰을 통해 3장에서는 엔티티에 대한 인증 기법을 고찰한다. 4장에서는 양방향 증명 방식과 이를 확장한 단방향 증명 방식에 대해 살펴보고, 5장에서는 기존의 기법을 개선한 단방향 엔티티 인증 기법을 제시한다. 6장과 7장에서는 본 연구에서 제시한 기법에 대한 안전성 분석 과정과 성능에 대한 비교 분석 결과를 제시하고, 결론 및 향후 연구 방향을 제시한다.

2. 이동 에이전트의 인증

2.1 이동 에이전트에 대한 고찰

이동 에이전트(mobile agent)는 자발성, 자율성, 사회성, 반응성을 갖는 독립된 프로그램을 의미하며, 에이전트를 조합하여 구성되는 시스템인 경우 일반 엔티티에게 편리하고 향상된 기능을 제공한다. 그러나 개발자 측면에서는 에이전트 시스템에서 요구하는 각종 기능 및 제약 규칙을 따라야 하기 때문에 여러 가지 문제점과 어려움이 따른다[25, 26].

에이전트는 사용자를 대신하여 사용자가 필요로 하는 작업을 대신하여 자동적으로 수행하는 소프트웨어이다. 객체 지향(object-oriented) 기술과 지능(intelligent) 기술 및 네트워크 기술을 결합한 것이다. 현재의 인터넷 기반 정보 체계는 급속도로 변화하고 있으며 각종 데이터들이 대규모 가상 공간에 분산되어 있는 형태이다. 각종 정보에 대한 분산 정도 및 이에 따르는 검색 난이도는 날로 증가할 것이다. 따라서 기존의 프로토콜을 사용하거나 기존의 정보 관리 및 검색 체계를 통해서는 효율적으로 대처하기 어렵다. 인터넷 기반 전자 상거래를 구현하기 위해서는 분산되어 있는 상거래 정보를 자동 가공하여 사용자에게 제공할 수 있어야 한다. 결국 대단위 인터넷을 여러 개의 에이전트가 이동하면서 관련되는 정보를 수집할 수 있어야 하는데 에이전트에 대한 보안 문제가 해결되어야 한다[27].

2.2 이동 에이전트에서의 보안

이동에이전트 시스템은 분산 어플리케이션의 구성에 유연한 환경을 제공해 주지만 심각한 보안 문제를 야기한다. 첫째는 불완전한 통신 채널을 이용하는 것에 대한 기본적인 보안 문제가 있으며, 둘째는 에이전트가 행하는 불법적인 행위나 공격에 대한 호스트 컴퓨터와 에이전트 서버의 보호문제이고, 셋째는 에이전트 서버가 행하는 에이전트공격에 대한 보안 문제이다.

안전하지 못한 네트워크 채널의 보안을 위해서는 호스트 컴퓨터에 대한 인증, 에이전트 코드와 데이터의 기밀성 및 무결성을 제공하여야 하며, 에이전트 전송을 통한 부인방지 기능을 제공하여야 한다. 호스트 컴퓨터에 대한 보안 기능을 제공하기 위해서는 에이전트에 대한 안전한 인증과 접근제어 기능을 제공하여야 한다. 마지막으로 이동에이전트 보안을 위해서는 에이전트 실행 상태의 변화에 대한 감사 및 인증 기능을 제공하여야 한다.

이동 에이전트에 대한 인증은 크게 인증을 원하는 부분과 인증을 수행하는 부분으로 나눌 수 있다. 인증을 원하는 엔티티를 증명자(prover)라고 하고, 인증을 수행하는 부분을 검증자(verifier)라고 한다. 이동 에이전트 기반 컴퓨팅 환경에 접목하여 고찰하였을 경우 이동 에이전트 자체는 증명자에 해당하고, 이동 에이전트가 접속하고자 하는 호스트 서버는 검증자에 해당한다. 이동 에이전트와 서버간의 인증에서의 부정 행위를 감찰하고 불법적 행동이 발생하였을 경우 이를 감시할 수 있는 기관이 필요한데 이러한 역할을 신뢰 센터(Trusted Third Party : TTP)가 담당한다. TTP는 공개적인 검증 기능을 통해서 증명자 및 검증자에 대한 역기능을 방지할 수 있는 엔티티이다.

본 연구에서는 이동 에이전트 기반 시스템에서 가장 필수적인 보안 기능에 대해 고찰하고, 시스템에 대한 안전성을 향상시킴과 동시에 에이전트가 지닌 계산 능력의 단점을 보완하면서 인증 과정을 수행할 수 있는 개선된 이동 에이전트 인증 기법을 제시하고자 한다.

3. 엔티티 인증 기법

엔티티에 대한 인증은 사용자에 대한 인증에 포함되며 유사한 의미로 사용된다[9, 10]. 사용자 인증이란 사용자 A가 사용자 B에게 A 자신을 증명할 수 있으나, B 자신을 포함한 A 이외의 어떤 제 3의 사용자도 C에게 A임을 증명할 수 없는 암호 기법을 의미한다. 엔티티 인증은 전자 서명과 달리 분쟁을 일으키는 메시지를 포함하지 않는다. 다만 요청 받은 서비스를 제공할

것인지 아닌지를 실시간 내에 결정하여 처리할 수 있도록 하는 기본 암호 시스템이다. 만일 이동 에이전트에 대한 인증이 인증서 기반으로 수행될 경우 방대한 인증서 정보를 이동 엔티티가 대화형으로 확인하여야 한다. 따라서 이동 에이전트의 성능 및 안전성 측면에서 개선할 수 있는 인증 기법이 필요하다.

3.1 기존의 인증 기법에 대한 분석

공개키에 기반한 엔티티 인증 기법은 이동 컴퓨팅 환경과 분산 전자 상거래 분야 및 시스템 접근 제어 기법과 같이 광범위한 분야에 활용 가능하다[5, 6, 15]. 엔티티 인증 기법은 일반적인 영지식 증명(zero knowledge proofs)에 해당한다[16]. 영지식 증명에 기반한 여러 가지 기법[7, 8, 11, 12, 13, 17]이 제시되었다. FFS기법[12]는 영지식 기반 양방향 증명 방법을 통해서 반복 회수를 $O(\log_2 n)$으로 하였다. 이는 어떠한 노출 정보도 제공하지 않는 방식이다. FFS기법인 경우 메모리 측면에서 단점을 지니고 있다. Schnorr기법과 GQ기법[13]인 경우에 정보의 크기 및 메모리 크기는 동시에 FFS기법보다 작다. 그러나, 이 두 방식은 확실한 안전성을 제공하지 못한다는 단점이 있다.

FFS기법은 연산 회수에서 가장 성능이 좋으나 증명자의 비밀키가 복수 개의 난수 $s_1, s_2, ..., s_k$를 사용할 경우 검증자 또한 k개 비트 $e_1, e_2, ..., e_k$를 랜덤하게 선택하여 증명자에게 전송하여야 하기 때문에 전체 키의 크기가 방대해 질 수 있다는 단점이 있다. 키 크기가 제일 작은 것은 Schnorr기법이므로 시스템 메모리 및 한정된 계산 능력을 갖는 시스템에 적합하다.

Schnorr기법인 경우 전체 성능 측면에서도 만족할 만하다. 전체적인 성능 평가 과정에서 이산 대수에 근거한 엔티티 인증 알고리즘을 기반으로 개선된 이동 에이전트 인증 알고리즘을 개발한다면 더욱 향상된 성능을 제공할 수 있을 것이다. 특히 Schnorr기법과 Okamoto 기법과 같은 이산 대수 기반 증명 기법은 인증 과정에서의 전처리 과정에서 사전 계산 과정을 수행하고, 이동 에이전트에 해당하는 증명자 부분의 처리 부하가 0인 것을 알 수 있다. 또한 호스트 컴퓨터에 해당하는 검증자 부분에 처리 부하가 집중되기 때문에 이동 에이전트에 대한 인증에 적용할 수 있다는 장점이 있다. 구체적인 특성 및 성능 비교는 아래 <표 1>, <표 2>와 같다.

<표 1> 엔티티 인증 기법의 특성

기 법 / 비교 항목	FFS 기법	GQ 기법	Schnorr 기법	Okamoto 기법
확실한 안전성 제공 측면	○	×	×	○
근본 안전성 기반	소인수분해	RSA[15]	이산대수	이산대수
시스템 파라메터 크기(비트)	0	20	1164	1676
공개키 크기(비트)	1024	1024	512	512
비밀키 크기(비트)	1024	512	140	280
키 크기 합계(비트)	2048	1556	1816	2468

<표 2> 엔티티 인증 기법의 계산량 비교

기 법 / 비교 항목	FFS 기법	GQ 기법	Schnorr 기법	Okamoto 기법
통신량(비트)	1044	1044	672	812
전처리 과정(증명자 측면)	1	30	210	245
온라인 처리량(증명자 측면)	10	31	0	0
온라인 처리량(검증자 측면)	11	35	210	248
연산 회수 합계 512비트 mod 곱셈 연산수	22	96	420	493

3.2 기존 프로토콜 기반 성능 개선 방향

이산 대수 문제에 근거한 기존의 Schnorr기법 및 이를 보완한 Okamoto기법이 지니고 있는 장점 및 성능 측면을 활용할 수 있는 개선된 기법이 필요하다. 결국 FFS기법과 Schnorr 및 Okamoto기법을 접목하여 전체 키의 크기를 최소화하면서 안전성도 향상시킬 수 있는 기법이 필요하다. 다른 측면에서의 해결 방법으로는 기존의 다양한 암호화 기법과 접목하는 것이다. 구체적인 방법으로는 양방향 영지식 증명을 단방향 기법으로 발전시키는 것이며, 안전성 측면에서는 불확정 전송(oblivious transfer) 기법[18]과 같은 추가적인 암호화 기법과 접목하는 것이 필요하다. 따라서 본 연구에서는 양방향 영지식 증명 방법에 대한 특징을 고찰하고 이의 변형인 불확정 전송 기법에 대한 분석 및 관련성을 제시한다. 특히 이동 컴퓨팅 환경에 적합한 대역폭을 제공하기 위해서 양방향 기법을 개선한 단방향 인증 기법을 제시하고자 한다.

4. 양방향 및 단방향 증명 기법

4.1 양방향 증명 기법

엔티티 또는 사용자 인증은 증명자와 검증자 사이에서 상호 작용을 통해서 증명자에 대한 신원을 검증자에게 증명하는 것이다. 이와 같이 두 엔티티에 대한 상

호 증명 및 인증 기법으로 사용되는 것이 영지식 증명이다. 각 엔티티는 공개적으로 신뢰할만한 데이터베이스에 자신만이 알고 있는 정보를 저장시켜 놓는다. 임의의 엔티티가 로그인하고자 할 때 영지식 증명에 기반한 검증 단계를 수행한다. 영지식 증명 단계는 데이터베이스에 저장된 각 개인의 비밀 정보에 대한 노출 없이도 자신임을 증명할 수 있다. FFS기법 및 GQ기법에 의해서 제시된 방법은 엔티티 인증 및 개인 식별 기능을 제공하는 영지식 증명 시스템이다[11, 12, 13, 16, 17]. 양방향 증명 기법의 구성 방식은 (그림 1)과 같은 도전-응답(challenge-response) 과정이다.

4.2 단방향 증명 기법

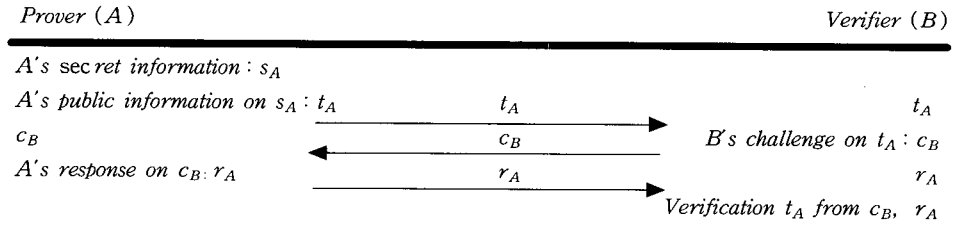
이동 컴퓨팅 환경은 방대하고 다양한 암호화 프로토콜을 적용할 수 있다. 프로토콜 중에서도 영지식 증명은 매우 중요한 암호화 프로토콜에 해당한다. 그러나 영지식 증명에서 사용하는 양방향 기반 증명 방식은 많은 자원을 사용한다는 단점이 있다. 따라서 단방향 영지식 증명 방식을 사용하여 이동 컴퓨팅 기반 암호화 프로토콜에서의 통신 비용을 줄일 수 있다. 단방향 증명 기법의 구성 방식은 아래 (그림 2)와 같은 특성을 나타낸다.

4.2.1 단방향 영지식 증명(zero knowledge proofs)

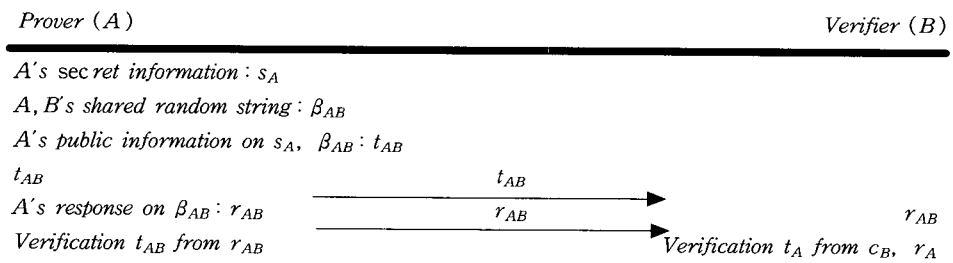
단방향 영지식 증명[20]은 증명자와 검증자가 랜덤 문자열을 공유한 상태로 증명자가 자신을 단방향 방식으로 증명하는 기법이다. 단방향 영지식 증명 시스템은 두 단계로 구성된다. 첫 단계에서는 양방향 작업이 수행된다. 양방향 방식을 사용하여 증명자와 검증자에게 필요한 개인 정보 및 필요 정보를 설정하는 단계이다. 두 번째 단계에서는 증명자가 첫 단계에서 생성된 정보를 사용하여 영지식에 기반하여 검증자에게 증명하는 단계이다. 이때 증명이 수행되는 과정은 단방향 방식으로 수행된다[21-23]. 단방향 영지식 증명 기법은 증명자가 검증자에게 자신의 비밀 정보에 대한 노출 없이도 자신에 대한 신원을 증명하는 것을 의미한다. 본 연구에서 제시한 기법 역시 증명자에 해당하는 이동 에이전트의 고유 비밀 정보를 검증자인 서버에 노출시키지 않은 상태에서 인증을 수행하는 것을 목적으로 한다.

4.2.2 단방향 불확정 전송(oblivious transfer protocol)

불확정 전송 방법은 Rabin[18]에 의해서 제시되었다. 이 기법은 A가 B에게 메시지 m 비트를 전달하고자 할 때 1/2의 확률로 전달하는데 A 자신은 어떠한 비트가 전달되었는지 모르는 경우를 의미한다. 불확정 전송(oblivious transfer : OT) 기법에서 A는 B의 공개키 P_B를 사용하여 자신이 가지고 있는 문자열 s_0와 s_1 및 메시지 m을 암호화한 후 B에게 전달한다. B는 자신의 비밀키를 사용하여 복호화 한다. 이때 A는 B가



(그림 1) 양방향 증명 기법의 도해



(그림 2) 단방향 증명 기법의 도해

m이외에 s_0와 s_1 중에서 어떠한 문자열을 받았는지를 모르는 경우를 의미한다.

Bellare와 Micali[19]는 양방향 방식으로 수행되는 불확정 전송 방식을 단방향 방식으로 발전시켰다. 엔티티 B에 해당하는 공개키 P_B와 비밀키 S_B가 있을 때, 엔티티 A는 B에게 감지 불가 방식에 기반하여 데이터를 보낸다. B는 어떠한 데이터도 보내지 않는 단방향 방식이다.

4.3 개선 방향에 대한 고찰

기존의 단방향 영지식 증명 기법은 증명자와 검증자가 랜덤 문자열을 공유하여 단방향으로 증명하는 기법이다. 그러나, 만일 다른 검증자에게 증명하고자 할 경우에 또 다른 랜덤 문자열을 공유하여야 한다는 단점이 있기 때문에 다중 엔티티 환경에는 부적합하다. 또한 기존의 단방향 영지식 증명 기법은 전이(transitive)가 가능하다. 결국 기존의 단방향 영지식 증명은 다중 엔티티 환경에 적합하도록 변형되어야 하며 전이 불가 기능을 제공하여야 한다. 해결 방법으로는 단방향 영지식 증명 방법의 전처리 단계에 불확정 전송 기법을 적용하는 것이다.

본 연구에서 제시한 기법 역시 증명자에 해당하는 이동 에이전트의 고유 비밀 정보를 검증자인 서버에 노출시키지 않은 영지식 증명이면서 동시에 단방향 불확정 전송의 특성을 이용하여 전체적으로 단방향적인 인증을 수행하며 단방향 영지식 증명 기법의 초기 단계에서는 불확정 전송 방식을 사용한다. 이는 증명자에 해당하는 이동 에이전트의 계산 능력이 서버와 비교하였을 경우에 많은 차이가 있기 때문에 균등한 계산량을 보이는 기존의 양방향 인증 기법의 문제점을 개선할 필요가 있다. 서버 측면에서 인증에 필요한 대부분의 계산 과정을 수행하는 방식을 적용할 경우 이동 에이전트 기반 시스템의 성능을 효율적으로 향상시킬 수 있기 때문이다. 따라서 본 연구에서는 이동 에이전트에 대한 전체 인증 과정의 전처리 단계에서 공개키에 기반한 단방향 불확정 전송 방식을 수행한다.

5. 제안한 단방향 인증 기법

본 연구에서는 양방향 인증 기법을 제안하고 이를 단방향 기법으로 발전시킨다. 제안하는 기법은 Schnorr형 인증 기법을 개선하였으며 ElGamal기법을 적용하였다. 이동 에이전트에 대한 보안 및 검증 기능을 수행하기 위해 각 에이전트는 신뢰 센터에 사전 등록을 수행한다. 등록 단계에서는 단방향 인증을 수행하기 위한 전처리 과정에 해당한다.

5.1 신뢰 센터에 대한 등록 단계

본 연구에서 제안하는 단방향 인증을 위해서 에이전트와 해당 네트워크 기반 이동 시스템은 신뢰 센터에 등록하는 과정을 수행한다. 제안한 기법은 우선 신뢰 센터에 대한 등록 단계를 수행한 인증 단계에서 필요로 하는 정보를 할당받는다. 우선 A는 신뢰 센터 J의 비밀키 x_J에 대한 공개키 정보 $y_J \equiv g^{x_J} \bmod p$를 바탕으로 아래와 같은 등록 단계를 수행한다.

단계 1 : 등록 요청 단계

단계 1-1 : 전송자 A는 랜덤 비밀 정보 $s_A \in Z_q$를 생성한다.

단계 1-2 : A는 $\delta \equiv g^{s_A} \bmod p$를 만족하는 δ와 신원 정보 ID_A를 신뢰 센터 J에게 전송하여 등록을 요청한다.

단계 2 : 등록 단계

단계 2-1 : 신뢰 센터 J는 난수 $w_J \in G(q)$에 대한 $t_J \equiv g^{w_J} \bmod p$를 생성한다.

단계 2-2 : J는 자신의 데이터베이스에 A에 대한 정보 ID_A, δ와 서명 해지 키에 해당하는 w_J를 저장한다.

단계 2-3 : J는 해쉬 함수를 적용하여 $c = h(\delta \| t_J)$를 생성한다.

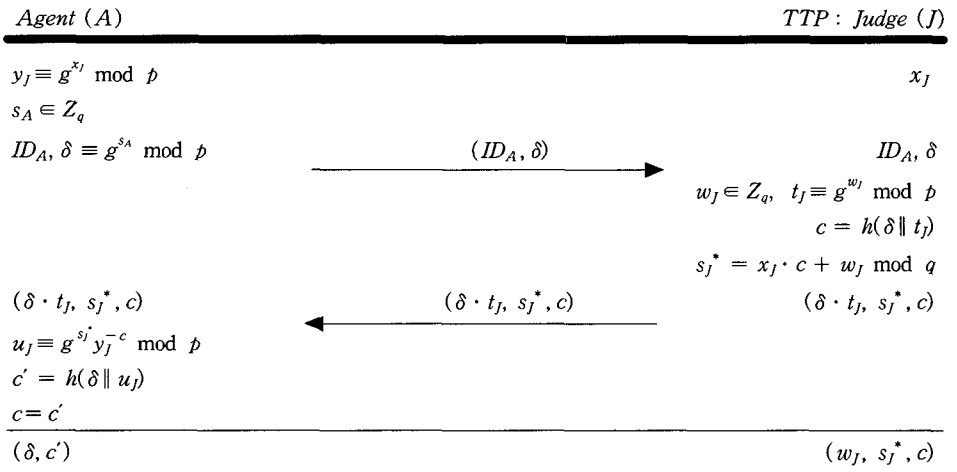
단계 2-4 : 신뢰 센터는 Schnorr 기반 알고리즘을 통해서 s_J^*를 생성하고 A에게 메시지 $(\delta \cdot t_J, s_J^*, c)$를 전달한다.

단계 3 : 등록 확인 단계

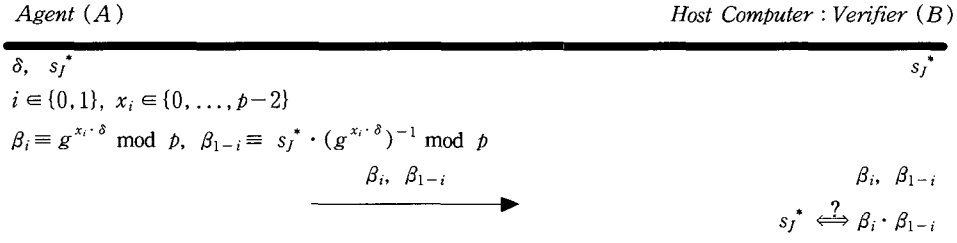
단계 3-1 : A는 $u_J \equiv g^{s_J^*} y_J^{-c} \bmod p$를 만족하는 u_J를 생성한다.

단계 3-2 : 등록 단계에서 전달되는 c과 $c' = h(\delta \| u_J)$에 대해 $c = c'$일 경우 등록이 정확하다는 것을 확인하게 된다.

제안하는 등록 단계에 대한 구체적인 과정은 다음 (그림 3)과 같다.



(그림 3) 신뢰 센터 J에 대한 등록 프로토콜



(그림 4) 공유 정보 할당 프로토콜

(증명) $u_J \equiv g^{s_J^*} y^{-c} \bmod p$에 기반한 $c = c'$에 대한 증명

$$u_J \equiv g^{s_J^*} y^{-c} \equiv g^{x_J \cdot c + w_J} g^{x_J \cdot -c} \equiv g^{w_J} \equiv t_J \bmod p$$
$$\therefore\ c' = h(\delta \| u_J) = h(\delta \| t_J) = c$$

등록 단계 이후에 이동 시스템은 신뢰 센터로부터 해당 에이전트에 대한 공개 등록 정보 δ, s_J^*를 얻을 수 있다. s_J^*를 사용하여 에이전트 A는 검증자인 B에게 자신만의 비밀 정보 $x_i \in \{0, \ldots, p-2\}$를 사용하여 β_i, β_{1-i}를 생성한다. 생성된 정보는 검증자에게 전달된다. 구체적인 공유 난수 정보 할당 프로토콜 과정은 위 (그림 4)와 같다.

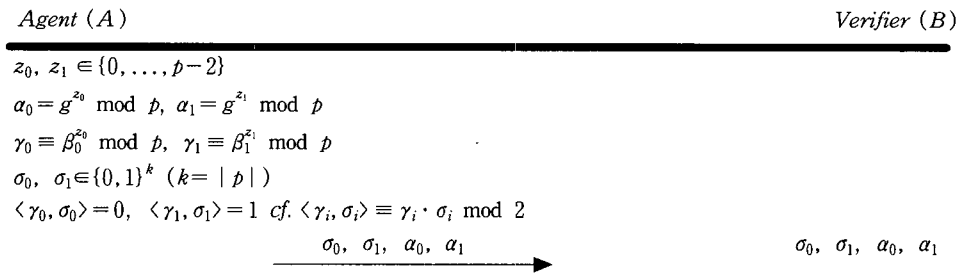
이와 같은 공유 정보 할당 프로토콜을 통해 이동 에이전트는 접근하고자 하는 호스트 시스템에게 전처리 과정에서 해당 정보를 전송할 수 있고, 추후에 단방향 이동 에이전트 인증 과정을 요청할 수 있다. 인증 요청에 대해 호스트 시스템은 시스템 보호 기능을 수행하면서 각 에이전트에 대한 접근 제어(access control) 기능을 제공하게 된다.

5.2 단방향 엔티티 인증 단계

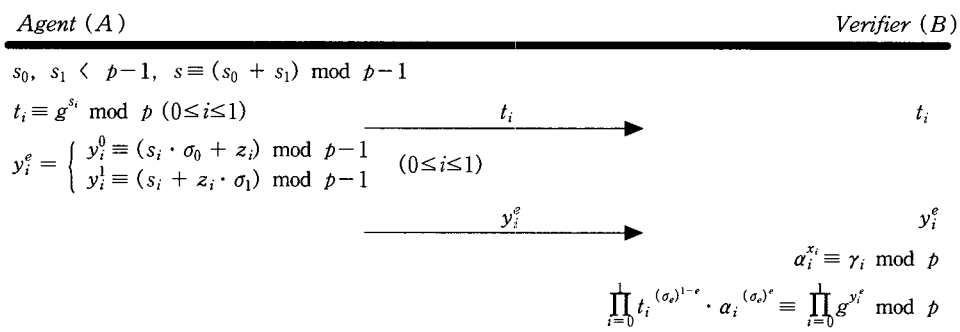
5.2.1 제안한 Schnorr형 단방향 엔티티 인증 기법

이동 에이전트 기반 컴퓨팅 환경이 지니고 있는 네트워크 대역폭을 고려하고 이동 단말 및 이동 객체가 지니고 있는 계산량의 한계 및 성능 측면을 고려할 때, 위에서 제시한 엔티티 인증 프로토콜이 단방향 및 단방향으로 수행된다면 훨씬 향상된 성능을 제공할 수 있을 것이다.

본 연구에서는 개선된 Schnorr 기반 양방향 엔티티 인증 알고리즘에서의 양방향성을 제거한다. 단방향 증명 단계를 수행하기 위해서 단방향 불확정 전송 기법을 적용한다. β_i, β_{1-i}를 사용하여 A는 임의의 두 비밀 난수 z_0, z_1을 선택한 후에 γ_0, γ_1을 생성한다. $\langle \gamma_0, \sigma_0 \rangle = 0$과 $\langle \gamma_1, \sigma_1 \rangle = 1$를 만족하도록 σ_0, $\sigma_1 \in \{0,1\}^k$ ($k = |p|$)을 설정한다. 선정된 σ_1, σ_2는 단방향 증명



(그림 5) 단방향 엔티티 인증을 위한 초기화 단계



(그림 6) Schnorr형 단방향 엔티티 인증 알고리즘($MDEA_{Sch}$)

기법에서 증명자와 검증자가 공통으로 공유하게 되는 참조 문자열 σ에 해당한다. 참조 문자열을 공유하게 됨으로써 증명자는 검증자로부터의 도전 e, c가 필요 없다. σ를 사용하여 증명자는 전체 전송 데이터량의 최소화와 성능의 최적화를 유도할 수 있다

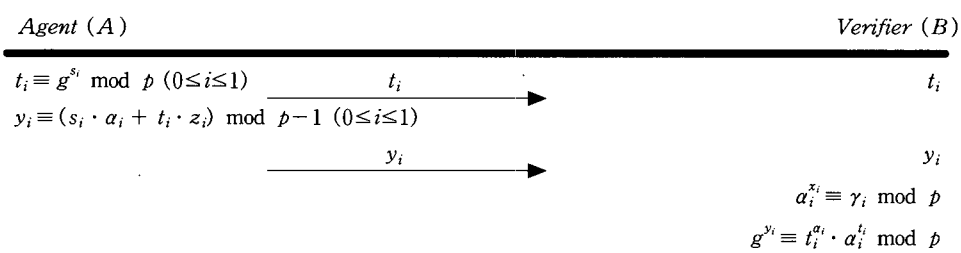
불확정 전송 기반 단방향 엔티티 인증을 위해 z_0, $z_1 \in \{0, \ldots, p-2\}$에 대한 $\alpha_0 = g^{z_0} \bmod p$ 및 $\alpha_1 = g^{z_1} \bmod p$를 생성한다. 비밀 정보 s에 대해 s_0와 s_1으로 이분화 하여 $t_i \equiv g^{s_i} \bmod p\ (0 \le i \le 1)$를 생성한 후에 아래 수식 (1)을 만족하는 y_i^e를 계산한다. 제안한 기법은 비밀 분산 기법을 접목한 것으로 다중 에이전트 환경에도 적용할 수 있는 특성을 제공한다.

$$y_i^e = \begin{cases} y_i^0 \equiv (s_i \cdot \sigma_0 + z_i) \bmod p-1 \\ y_i^1 \equiv (s_i + z_i \cdot \sigma_1) \bmod p-1 \end{cases} \quad (0 \le i \le 1) \quad (1)$$

인증을 위한 초기화 단계를 수행한 후 구체적인 불확정 전송 기반 최적화된 단방향 엔티티 인증 알고리즘은 아래 (그림 4)와 같다.

5.2.2 ElGamal형 단방향 엔티티 인증 기법

또한 ElGamal기법을 기반으로 변형된 $y_i \equiv (s_i \cdot \alpha_i + t_i \cdot z_i) \bmod p-1\ (0 \le i \le 1)$수식을 통해 단방향으로 인증을 수행할 수 있다. (그림 5)와 같은 초기화 단계를 공통적으로 수행한 후에 아래 (그림 7)과 같이 ElGamal 기법을 적용한 단방향 엔티티 인증을 수행할 수 있다.



(그림 7) ElGamal형 단방향 엔티티 인증 알고리즘($MDEA_{EIG}$)

6. 안전성 분석 및 성능 평가

6.1 제안한 $MDEA_{Sch}$ 기법의 안전성 분석

$MDEA_{Sch}$ 기법은 불확정 전송 기법을 적용함으로써 증명자와 검증자는 공통된 참조 문자열 σ_i $(0 \le i \le 1)$을 공유할 수 있었다. 또한 최적 증명을 위해서 Schnorr 기법에서의 비밀 분산 기법에 해당하는 비밀 정보를 s_1과 s_2를 사용하였기 때문에 Okamoto기법에서의 안전성과 동일한 측면의 안전성을 제공한다. 또한 이산 대수 문제[14]에 근거하고 있기 때문에 전체적인 안전성에서도 기존의 기법과 동일한 안전성을 제공한다. 또한 제시한 기법은 단방향 증명에 기반한 영지식 증명 프로토콜에 해당한다. 단방향 증명 방식에서 e에 대한 검증자의 검증 단계는 아래와 같다.

(증명-1) $\prod_{i=0}^{1} t_i^{(\sigma_e)^{1-e}} \cdot \alpha_i^{(\sigma_e)^e} \equiv \prod_{i=0}^{1} g^{y_i^e} \bmod p$ 에 대한 증명

if $e = 0$ *then*

$$\prod_{i=0}^{1} t_i^{(\sigma_e)^{1-e}} \cdot \alpha_i^{(\sigma_e)^e} \equiv \prod_{i=0}^{1} t_i^{(\sigma_0)^1} \cdot \alpha_i^{(\sigma_0)^0}$$

$$\equiv \prod_{i=0}^{1} g^{s_i \cdot \sigma_0} \cdot \alpha_i \equiv g^{s_0 \cdot \sigma_0} \cdot \alpha_0 \cdot g^{s_1 \cdot \sigma_0} \cdot \alpha_1$$

$$\equiv g^{(s_0+s_1) \cdot \sigma_0} \cdot \alpha_0 \cdot \alpha_1 \equiv g^{s \cdot \sigma_0} \cdot \alpha_0 \cdot \alpha_1$$

$$\equiv t^{\sigma_0} \cdot \alpha_0 \cdot \alpha_1$$

if $e = 0$ *then*

$$\prod_{i=0}^{1} g^{y_i^e} \bmod p \equiv \prod_{i=0}^{1} g^{y_i^0} \bmod p \equiv \prod_{i=0}^{1} g^{s_i \cdot \sigma_0 + z_i}$$

$$\equiv g^{s_0 \cdot \sigma_0 + z_0} \cdot g^{s_1 \cdot \sigma_0 + z_1} \equiv g^{(s_0+s_1) \cdot \sigma_0} \cdot g^{(z_0+z_1)}$$

$$\equiv g^{s \cdot \sigma_0} \cdot g^{(z_0+z_1)} \equiv t^{\sigma_0} \cdot \alpha_0 \cdot \alpha_1$$

if $e = 1$ *then*

$$\prod_{i=0}^{1} t_i^{(\sigma_e)^{1-e}} \cdot \alpha_i^{(\sigma_e)^e} \equiv \prod_{i=0}^{1} t_i^{(\sigma_1)^0} \cdot \alpha_i^{(\sigma_1)^1} \equiv \prod_{i=0}^{1} t_i \cdot \alpha_i^{\sigma_1}$$

$$\equiv g^{s_0} \cdot \alpha_0^{\sigma_1} \cdot g^{s_1} \cdot \alpha_1^{\sigma_1} \equiv g^{(s_0+s_1)} \cdot (\alpha_0 \cdot \alpha_1)^{\sigma_1}$$

$$\equiv g^{s} \cdot g^{(z_0+z_1) \cdot \sigma_1} \equiv t \cdot (\alpha_0 \cdot \alpha_1)^{\sigma_1}$$

if $e = 1$ *then*

$$\prod_{i=0}^{1} g^{y_i^e} \bmod p \equiv \prod_{i=0}^{1} g^{y_i^1} \bmod p \equiv \prod_{i=0}^{1} g^{s_i + z_i \cdot \sigma_1}$$

$$\equiv g^{s_0 + z_0 \cdot \sigma_1} \cdot g^{s_1 + z_1 \cdot \sigma_1} \equiv g^{(s_0+s_1)} \cdot g^{(z_0+z_1) \cdot \sigma_1}$$

$$\equiv g^{s} \cdot g^{(z_0+z_1) \cdot \sigma_1} \equiv t \cdot (\alpha_0 \cdot \alpha_1)^{\sigma_1}$$

$$\therefore \prod_{i=0}^{1} t_i^{(\sigma_e)^{1-e}} \cdot \alpha_i^{(\sigma_e)^e} \equiv \prod_{i=0}^{1} g^{y_i^e} \bmod p$$

6.2 제안한 $MDEA_{ElG}$ 기법의 안전성 분석

$MDEA_{ElG}$ 기법 역시 이산 대수 문제의 안전성에 근거하고 있으며, 비밀 분산 기법에 기초하기 때문에 복잡성에 기초한 안전성을 향상시킬 수 있다. 또한 시스템 파라메터 $i(0 \le i \le 1)$값으로 설정으로 인해 증명자로부터 전달된 y_i에 대한 검증 과정에서 ElGamal 알고리즘에 제공하는 계산량의 향상을 얻을 수 있었으며, 단방향 불확정 전송 기법에 기반하기 때문에 기존의 양방향 기반 알고리즘보다 이동 에이전트가 수행하여야 할 계산량을 감소시켜 주므로 전체적인 성능을 향상시킬 수 있었다. 결국 증명 단계가 단방향으로 수행되므로 이동 컴퓨팅 환경과 같은 원격 컴퓨팅 환경에서 한정된 대역폭을 갖는 경우에 적합하다. $MDEA_{ElG}$ 기법의 무결성을 검증하기 위해서는 우선 검증자에게 전달된 γ_0, γ_1와 α_0, α_1에 대해 $MDEA_{Sch}$ 기법과 동일한 방식으로 불확정 전송 과정에 대한 증명을 수행하고 단방향 ElGamal기법에 대한 증명을 수행한다. 구체적인 검증 단계는 아래와 같다.

(증명-2) $g^{y_i} \equiv t_i^{\alpha_i} \cdot \alpha_i^{t_i} \bmod p$에 대한 증명

$$g^{y_i} \equiv g^{s_i \cdot \alpha_i + t_i \cdot z_i} \equiv (g^{s_i})^{\alpha_i} \cdot (g^{z_i})^{t_i} \equiv t_i^{\alpha_i} \cdot \alpha_i^{t_i} \bmod p$$

6.3 제안한 기법의 성능 비교 분석

본 연구에서 제시한 기법인 경우 신뢰 센터에 대한 등록 결과를 바탕으로 단방향 인증을 수행하기 때문에 인증 과정에서 전이가 발생하였을 경우 신뢰 센터에 의해서 이중 사용된 인증 정보를 검출할 수 있다. 신뢰 센터에 의해서 수행되는 서명 정보 $s_J^* = x_J \cdot c + w_J \bmod q$는 에이전트에 의해서 검증자에게 전달될 때에 아래와 같은 수식에 의해 포함되어 전달된다.

$$\beta_i \equiv g^{x_i \cdot \delta} \bmod p, \ \beta_{1-i} \equiv s_J^* \cdot (g^{x_i \cdot \delta})^{-1} \bmod p$$

따라서 불법적으로 전이된 인증 정보에 대해서는 신뢰 센터에 의해서 추후에 검증될 수 있다. 결국 본 연구에서 제시한 기법인 경우에 전이 문제를 해결할 수 있다.

공격자의 입장에서 얻을 수 있는 정보는 아래와 같은 프로토콜에서의 t_i와 y_i^e 정보이다. y_i^e인 경우 기존의 Schnorr기법보다 복잡성이 증대된 응답(response)을 생성하게 된다.

$$y_i^e = \begin{cases} y_i^0 \equiv (s_i \cdot \sigma_0 + z_i) \bmod p-1 \\ y_i^1 \equiv (s_i + z_i \cdot \sigma_1) \bmod p-1 \end{cases} \quad (0 \le i \le 1)$$

$$y_i \equiv (s_i \cdot \alpha_i + t_i \cdot z_i) \bmod p-1 \ (0 \le i \le 1)$$

ElGamal형 단방향 인증인 경우에도 i 값에 따라서 서로 다른 정보가 전달되기 때문에 공격자가 얻을 수 있는 정보는 기존의 Schnorr 기법 및 ElGamal 기법보다 계산 측면에서 더욱 복잡한 형태로 전달된다. 따라서 제시한 기법은 기존의 기법보다 외부로부터의 공격에 더욱 효과적이다.

기존의 단방향 방식으로 단방향 불확정 전송 기법과 단방향 영지식 증명 기법을 본 연구에서 제시한 단방향 기반 증명 기법인 $MDEA_{Sch}$, $MDEA_{EIG}$ 및 NIOT 기법과 비교 분석한다. 기존의 단방향 불확정 전송 기법은 엔티티 인증 시스템에 적용할 수 없거나 판정 불가능한 상태이나, 본 연구에서 제시하는 기법인 경우에 이동 컴퓨팅 환경에서 필요한 엔티티 인증 시스템에 접목할 수 있다. 이산 대수에 근거한 기법으로서 수학적인 안전성을 보장할 수 있으며[14], 이동 컴퓨팅 환경에서의 ID 기반 인증 시스템으로도 발전 시킬 수 있다. 또한 제시한 기법은 이동 에이전트 시스템에서 발생할 수 있는 부정 행위 및 불법적인 침입이 발생하였을 경우 공개적인 검증이 가능한 공정 암호화 시스템(fair cryptosystem)으로 발전시킬 수 있다. <표 3>은 제안한 기법에 대한 성능 평가이다.

〈표 3〉 제안한 기법의 성능 비교

기법 / 비교 항목	NIOT[19]	$MDEA_{Sch}$	$MDEA_{EIG}$
공유 참조문자열 크기(비트)	$2 \cdot k$	$2 \cdot k$	$2 \cdot k$
전처리 과정(증명자 측면)	$2 \cdot p \cdot m$	$2 \cdot p \cdot m$	$2 \cdot p \cdot m$
온-라인 처리(증명자 측면)	0	0	0
온-라인 처리(검증자 측면)	$2 \cdot p \cdot m$	$2 \cdot p \cdot m$	$2 \cdot p \cdot m$
연산 회수 합계	$4 \cdot p \cdot m$	$4 \cdot p \cdot m$	$4 \cdot p \cdot m$

($k = |p|$)인 관계이고 m은 상수에 해당

<표 3>과 같이 단방향 인증을 위한 공유 참조 문자열의 크기는 일반적으로 $2 \cdot k$로 동일하다. 전체적인 연산 회수에서는 동일한 성능을 나타낸다. 제시한 기법 역시 증명자 측면에서의 온라인 처리량이 모두 0이므로 이동 에이전트와 같은 한정된 계산 능력을 갖는 엔티티의 인증 시스템에 적당하다.

7. 결 론

다양한 암호화 프로토콜을 적용하여 이동 에이전트 기반 컴퓨팅 환경에서의 안전성을 증대하고자 하는 노력이 계속되고 있다. 기존의 프로토콜들은 대부분 클라이언트 서버 개념에 기반한 양방향 증명 시스템에 해당한다. 안전한 신원 확인 프로토콜이나 엔티티 인증 기법을 통해 안전한 이동 컴퓨팅 환경을 제공할 수 있다. 그러나 기존의 양방향 인증 기반 증명 방식은 많은 대역폭을 필요로 한다는 단점이 있다.

본 연구에서는 Schnorr와 Okamoto 양방향 기반 인증 기법에 대한 성능 분석 및 안전성 분석을 통해 안전성과 성능 측면에서 이동 컴퓨팅 환경에 적합한 인증 기법을 제시하였다. 또한 ElGamal기법을 적용한 형태도 제시하였다. 이동 컴퓨팅 시스템에 적용하기 위해 불확정 전송 기반 단방향 인증 기법으로 개선하였다.

제안한 인증 기법은 증명자로부터의 단방향 증명 과정을 통해서 엔티티 인증 과정이 수행되므로 안전성과 통신량 측면에서 향상된 성능을 제공한다. 따라서 이동 컴퓨팅 시스템과 분산 전자 상거래 분야 및 시스템 접근 제어 분야와 같은 광범위한 분야에 활용 가능하다. 향후 연구 과제로는 비밀 정보에 대한 분산을 통해 공개적으로 증명 가능하고 공정한 검증이 가능한 기법으로 더욱 개선하고, 분산 컴퓨팅 환경에 적합한 공정 인증 기법으로 발전시키는 것이다.

참 고 문 헌

[1] R. Gray, D. Kotz, S. Nog, D. Rus and G. Cybenco, "Mobile Agents for Mobile Computing," Proc. of the 2nd Aizu Int'l Symposium on Parallel Algorithm/Architecture Synthesis (pAs97), Fukushima, Japan, Mar., 1997.

[2] J. Vitek. M. Serrao and D. Thanos, "Security and Communication in Mobile Agents Systems," Mobile Object Systems, Springer-Verlag, pp.177-199, 1996.

[3] K. Kato, "Safe and Secure Execution Mechanisms for Mobile Objects," Mobile Object Systems, Springer-Verlag, pp.201-211, 1996.

[4] G. J. Simmons, "A Survey of Information Authentication," *Proceedings of the IEEE*, Vol.76, No.5, pp.603-620, May, 1988.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol.IT-22, No.6, pp.472-492, Nov. 1976.

[6] W. Diffie, "The First Ten Years of Public-Key Cryptography," *Proceedings of the IEEE*, Vol. 76, No.5, pp.560-577, 1988.

[7] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," *Advances in Cryptology, Proceedings of Crypto'89, Springer-Verlag*, pp.239-252, 1990.

[8] T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," *Advances in Cryptology, Proceedings of Crypto'92, Springer-Verlag*, pp.31-53, 1993.

[9] B. Schneier, *Applied Cryptography, 2nd Edition*, John Wiley & Sons Press, 1996.

[10] A. J. Menezed, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, *CRC Press*, 1996.

[11] A. Fiat and A. Shamir, "How to Prove Yourself : Practical Solution to Identification and Signature Problems," *Advances in Cryptology, Proceedings of CRYPTO'86, Springer-Verlag*, pp.186-199, 1987.

[12] U. Feige, A. Fiat, A. Shamir, "Zero Knowledge Proofs of Identity," Proceedings of the 19th Annual ACM Symposium of Theory of Computing, pp.210-217, 1989.

[13] L. C. Guillou and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory," *Advances in Cryptology, Proceedings of Eurocrypt'88, Springer-Verlag*, pp.123-128, 1989.

[14] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," *IEEE Transactions on Information Theory, Vol.IT-30, No.4, pp.469-472, Jul. 1985.*

[15] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol.21, No.2, pp.120-126, 1978.

[16] S. Goldwasser, S. Micali, C. Rackoff, "The Knowledge Complexity of Interactive Proofs," SIAM Journal of Computing, Vol.18, No.1, pp.186-208, 1989.

[17] K. Ohta and T. Okamoto, "A Modification of the Fiat-Shamir Scheme," *Advances in Cryptology, Proceedings of Crypto'88, Springer-Verlag*, pp.232-243, 1989.

[18] M. Rabin, "How to exchange secrets by oblivious transfer," Technical Reports TR-81, Harvard Aiken Computation Laboratory, 1981.

[19] M. Bellare, S. Micali, "Non-Interactive Oblivious Transfer and Applications," Advances in Cryptology - Crypto 89, Lecture Notes in Computer Science, Vol.435, Springer-Verlag, 1989.

[20] M. Blum, P. Feldman, S. Micali, "Non-Interactive Zero-Knowledge Proof Systems and Applications," *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, 1988.

[21] A. D. Santis, G. D. Crescenzo, P. Persino, "Randomness-Efficient Non-Interactive Zero Knowledge," ICALP'97 Conference, 1997.

[22] A. D. Santis, S. Micali, G. Persiano, "Non-Interactive Zero-Knowledge Proof-Systems," *Advances in Cryptology - Crypto'87*, Vol.293, 1988.

[23] A. D. Santis, S. Micali, G. Persiano, "Non-Interactive Zero-Knowledge Proof-Systems with Preprocessing," *Advances in Cryptology - Crypto'88*, Vol.403, 1989.

[24] S. Micali, "Fair Cryptosystems," Technical Reports MIT/LCS/TR-579-b, 1993.

[25] C. G. Harrison, D. M. Chess and A. Kershenbaum, "Mobile Agents : Are they a good idea?" Technical Report, IBM T. J. Watson Research Center, Mar., 1995.

[26] M. R. Genesereth and S. P. Ketchpel, "Software Agents," Communication of the ACM, Vol.37, No.7, pp.48-53, July, 1994.

[27] V. Giovani, "Protecting Mobile Agents through Tracing," Accepted paper for the Mobile Object Systems ECoop Workshop'97.

이 기 현

e mail : khlee@wh.myongji.ac.kr

1960년 성균관대학교 경상대학 경제학과 졸업

1972년 성균관대학교 경영대학원 정보처리학과 졸업(경영학 석사)

1986년 광운대학교 대학원 전자계산학과 졸업(이학 석사)

1993년 광운대학교 대학원 전자계산학과 졸업(이학 박사)

1975년 총무처 행정전산 계획실 전산처리관

1980년 대한손해보험협회 전산실장

1993년 한국정보처리전문가협회(IPAC) 회원

1995년 한국정보처리학회 부회장

1996년 캘리포니아 주립대학교(Sancramento) 객원교수

1982년~현재 명지대학교 컴퓨터공학과 교수, 정보지원처장

노 환 주

e-mail : nhj@cakra.dongguk.ac.kr

1982년 광운대학교 전자계산학과 졸업(이학사)

1986년 동국대학교 경영대학원 졸업(경영학 석사)

1994년 강원대학교 대학원 전자계산학과 졸업(이학 석사)

1998년 명지대학교 대학원 컴퓨터공학과 박사과정 수료

1999년 현재 동국대학교 전자계산원 전임교원