Mobile IP 를 위한 공개키 기반 인증 프로토콜

이병래, 장경아, 김태윤
고려대학교 컴퓨터학과
e-mail : brlee@netlab.korea.ac.kr

Public Key based Authentication Protocol for Mobile IP

Byung-Rae Lee, Kyung-Ah Chang, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University.

요 약

Mobile IP[1]환경에서 *MN* (Mobile Node)[1]는 *FA* (Foreign Agent)[1]와 *HA* (Home Agent[1])간에 컨트롤 메시지들을 주고 받으며 이러한 컨트롤 메시지들은 인증을 받아야 한다. 그러나 기존의 Mobile IP 에서는 키 분배 문제를 고려하지 않고 메시지 인증만을 다루고 있으며 [2,3]에서는 등록 키를 생성하기 위하여 몇 가지 방법을 제시하고 있지만 구체적인 인증 프로토콜은 다루지 않고 있다. 본 논문에서는 Mobile IP 환경에서의 *MN* 와 *FA* 간에 공개키 기반 인증 프로토콜을 제안한다. 제안된 인증 프로토콜은 *MN* 와 *FA* 간의 상호 인증 단계를 거치며, 서로간에 비밀 세션키를 생성하여 데이터의 기밀성을 보장할 수 있다. 또한 공개키에 기반 하므로 전자서명을 통한 메시지의 부인방지 기능을 얻을 수 있다.

1. 서론

MN 의 이동성을 네트워크 계층에서 지원하기 위해 고안된 것이 Mobile IP 이다. Mobile IP 를 지원하기 위해서 각 지역 네트워크 망에는 이동성을 지원하는 *FA* (Foreign Agent)가 있고 이동 호스트의 현재 위치를 나타내는 care-of-address[1]를 이용해서 데이터 전송이 이루어 진다.

[2,3]은 RFC 2002 의 Mobile IP 자체의 비효율적인 데이터그램 라우팅 방식을 효율적으로 개선하기위해서 제안된 방식이다. *FA* 는 컨트롤 메시지를 기반으로 해서 *MN* 의 위치를 바인딩 캐쉬에 가지고 가지고 있으며 이를 이용해서 *MN* 와의 직접적인 통신을 가능하게 한다. 모든 Route Optimization 메시지들은 기존의 Mobile IP 와 같은 방식으로 인증을 받게 된다. 이 같은 인증은 사전에 성립된 SA(Security Association)에 의존하여 이루어 진다. 그러나 대개 *MN* 가 *FA* 와 등록을 할 경우 대개의 경우에 *FA* 와의 SA 는 존재하지 않는다. *FA* 는 *MN* 가 보내주는 컨트롤 메시지는 예전의 *FA* 로부터 새로운 *FA* 로 핸드오프를 지원해 준다. 이 같은 핸드오프는 예전의 *FA* 로부터의 메시지에 의존하며 인증을 필요로 한다.

본 논문에서는 이동 통신 시스템에서의 인증 프로토콜을 기반으로 하여 Mobile IP 를 위한 공개키 기반 인증 프로토콜을 제안한다. 제안한 인증 프로토콜은 Mobile IP 환경에서의 *MN* 와 외부 도메인에 위치한 *FA* 가 상호 인증 할 수 있도록 허용한다.

본 논문의 구성은 다음과 같다. 2 장에서 Mobile IP 의 등록 프로토콜[1]과 [3]에서 제시한 등록키 생성 방식을 설명한다. 3 장에서는 이동 통신 환경에서의 인증 프로토콜에 대한 요구 사항을 고찰하고 공개키 기반 구조에 대하여 살펴본다. 4 장에서는 제안한 인증 프로토콜을 설명한다. 5 장에서는 제안한 프로토콜에 대한 성능 분석이 있으며 마지막으로 6 장에서는 결론을 제시한다.

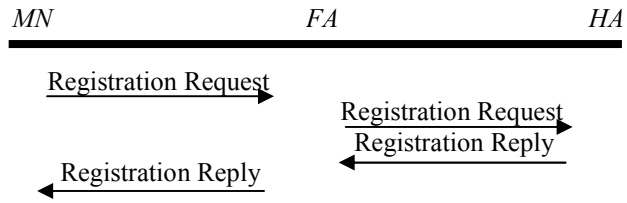
2. Mobile IP

본 장에서는 Mobile IP 의 등록 프로토콜과 [3]에서 제시된 등록 키를 생성하는 방식을 고찰한다.

2.1 Mobile IP

Mobile IP 설계의 기본 요구 조건은 투명성, 병립성, 그리고 보안성이다. 즉, *MN* 는 계속 자신의 홈 주소를 사용하면서 어느 지점을 통해서라도 네트워크에 접속할 수 있어야 한다. 또한 기존의 보통 호스트와 라우터에는 아무 변화가 없으며 *MN* 는 어떤 종류의 호스트와도 자유롭게 통신할 수 있어야 한다. 마지막으로 모든 등록 메시지는 인증을 받아야 한다.

Mobile IP 에서 제시하고 있는 등록 과정은 다음과 같다. *MN* 가 자신의 *HA* 가 아닌 다른 *FA* 가 관리하는 네트워크로 이동하였을 경우, *MN* 는 이 *FA* 에 등록을 하고 *FA* 는 이 사실을 *HA* 에게 알림으로써 *MN* 는 이동 호스트의 현재 위치를 알려주게 된다.



<그림 1> Mobile IP 등록 과정

MN 로 전송되는 데이터는 우선 *HA* 로 보내진다. *HA* 가 이 데이터를 터널링을 통해 *FA* 로 보내주면 *FA* 가 최종적으로 데이터를 *MN* 로 전송해 주게 된다. 이때 *MN* 의 현재 위치를 나타내는 care-of-address 는 *FA* 자신의 IP 주소 일 수도 있고, DHCP 등을 통해 할당 받은 *MN* 의 지역 주소일 수도 있다[1].

현재 Mobile IP 에서의 *MN* 의 등록 과정을 개선하고자 하는 여러 가지 노력이 있었다[6,7,8,9]. 하지만 등록에 대한 개선안을 다루고 있을 뿐, 분산 이동 컴퓨팅 환경을 고려한 등록키를 생성하는 방법에 있어서는 단점을 많이 드러내고 있다.

2.2 Route Optimization for registration key

[3]에서는 Route Optimization 에서 이용되는 등록키를 생성해내기 위한 여러 가지 방법을 제시하고 있다. 그 방법은 세가지이며 다음과 같다.

- *HA* 를 키 분배 센터로 이용하는 방법
- *FA* 를 키 분배 센터로 이용하는 방법
- Diffie-Hellman[4] 키 교환 방식에 근거하여 *MN* 와 *FA* 간에 등록 단계 중 키를 생성해 내는 방법

HA 를 키 분배 센터로 이용하는 방법은 *HA* 가 *MN* 와 *FA* 간에 사용될 등록키를 생성해서 전송하는 방식이다. *FA* 를 키 분배 센터로 이용하는 방법은 일반적으로 *FA* 자체를 신뢰할 수 있는 문제가 있으며, *FA* 의 안전성에 대한 고려가 있어야 한다. Diffie-Hellman 키 교환 방식은 다른 방법에 비하여 개선된 안정성을 가지고 있지만 상대방의 공개키에 대한 인증 문제는 고려하지 않고 있다. 위에 제시된 기법들은 상대방의 엔티티 인증에 관한 문제는 고려하지 않고 있으며 단지 키 공유 방식만을 언급하고 있다.

3. 이동 통신 환경에서의 공개키 기반 프로토콜

3.1 이동 통신 환경에서의 인증 프로토콜 요구 사항

안전한 이동 컴퓨팅 환경을 구현하기 위해서는 각 사용자에 대한 완벽하고 성능 측면에서 향상된 인증 프로토콜이 제시되어야 한다. 이동 통신 환경에서의 인증 프로토콜의 주요 요구 사항은 다음과 같다.

- 무선 인터페이스에서의 기밀성
- 사용자 신원의 익명성
- 네트워크의 사용자 인증

위와 같은 특징들이 이미 기존의 이동 통신 보안 시스템에서 제공되고 있지만 더욱 개선된 다른 요소들이 필요하다. 이동 컴퓨팅 환경에 있어서 중요한 또 다른 요소로 사용자는 침입자가 네트워크 오퍼레이터(network operator) 또는 서비스 제공자(service provider) 임을 가장하는 것을 방지하기 위하여 반드시 네트워크를 인증하여야 한다는 것이다[10,11,12].

- 사용자의 네트워크 인증

이동 통신에서는 이동 노드의 컴퓨팅 능력을 고려하여 인증과 키 분배 프로토콜을 설계하여야 한다. 이동 노드는 이동성을 고려한 장치이므로 사용 전력과 계산 능력이 제한적이기 때문에 정보 보호를 위한 키 분배 방식도 제한적일 수 밖에 없다. 즉, 메시지 교환 회수는 많아서는 안되며, 계산량 또한 적어야 한다.

3.2 공개키 암호 시스템

공개키 기반 암호화 알고리즘이 대칭키 기반의 알고리즘보다 계산량이 크고 복잡하지만, 하드웨어의 발전과 효율적인 공개키 암호 시스템으로 공개키 기반의 암호화가 가능해지고 있다. 일반적으로 대칭키 기반의 암호 알고리즘은 Mobile IP 와 같은 이동 통신 환경에 적용하기에는 다음과 같은 단점을 가지고 있다.

- 대칭키 기반 암호 시스템은 네트워크의 신뢰를 필요로 하므로 확장성 문제가 발생한다. 따라서 이동 통신 환경에는 적합하지 않다.
- 일반적으로 부인 방지 서비스(non-repudiation)는 공개키 암호 시스템을 이용한 전자서명 알고리즘으로만 가능하다. 인터넷을 이용한 서비스 이용이 활발해지므로 부인 방지 서비스가 많이 요구될 것이다.
- 일반적으로 공개키에 기반 한 서비스는 각 세션마다의 새로운 세션키를 생성해낼 수 있어서 개선된 안전성을 보장할 수 있다.

기존의 공개키 암호 알고리즘은 이동 컴퓨팅 환경

에 응용하기에는 어려움이 있다. 제한된 계산 능력을 가지고 있는 이동 단말에게 있어서 계산량의 문제와 메시지 길이가 이동 컴퓨팅 환경에는 적합하지 않았다.

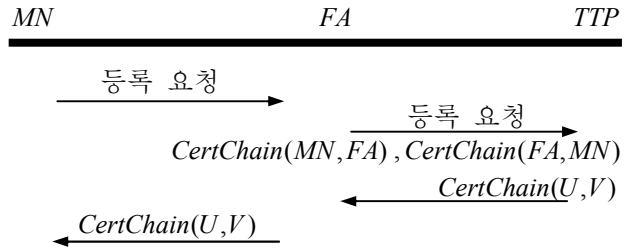
그러나 하드웨어의 발전으로 인하여 이동 단말의 연산 능력이 개선되었으며, 타원 곡선 암호 시스템은 다른 공개키 암호 알고리즘과 비교할 때 적은 비트수와 빠른 연산속도를 제공한다.

3.3 공개키 기반 인증 프로토콜

이동 환경을 고려한 초기의 프로토콜은 Tatebayashi, Matsuzaki, 그리고 Newman 에 의해 제안되었으며 TMN 프로토콜로 널리 알려져 있다[13].

Beller 등이 제안한 알고리즘은 다른 공개키 암호 시스템에 비하여 효율적인 암호화 방식을 기반으로 한 암호 시스템에 의존하고 있다. 이러한 공개키 암호화 방식은 Rabin[14]에 의하여 제안된 것으로서 modulo squaring 과 MSR(modulo square root)를 찾아내는 방식에 근거하고 있다.

인증서 체인[15]은 프로토콜에 참여하는 동일한 *TTP* 를 가지고 있지 않거나, 각자의 *TTP* 에 온-라인 접근이 가능하지 않을 때 사용될 수 있다. 인증서 체인은 다음과 같다. $CertChain(X,Y)$ 는 $c_0, c_1, \ldots, c_n$ 와 같은 인증서의 배열로 이루어져 있다. 여기서 인증서 c_0 의 전자서명을 한 것은 X 의 인증 기관(CA)이며 c_i 의 대상은 c_{i+1} 의 전자서명을 한 기관이다. c_n 의 전자서명을 한 것은 Y 의 인증기관(CA)이다.



<그림 2> 인증서 체인 분배 과정

우선 *MN* 는 *FA* 에게 등록 요청을 한다. *FA* 는 이를 신뢰센터인 *TTP* 에게로 보내준다. *TTP* 는 *MN* 가 *FA* 의 공개키를 검증할 수 있도록 $CertChain(U,V)$ 를 생성하고 *FA* 가 *MN* 와 *TTP* 의 인증서를 검증할 수 있도록 각각

Mobile IP 와 같은 이동 통신 환경에서 *MN* 와 *FA* 는 서로간의 전자서명을 검증할 공개키를 소유할 수 있는 가능성은 적다. 비밀 세션키 계산에 있어서 상대방으로부터 오는 공개키가 올바른 상대방의 공개키인지를 검증하려면 상대방의 인증서를 검증하여야 한다.

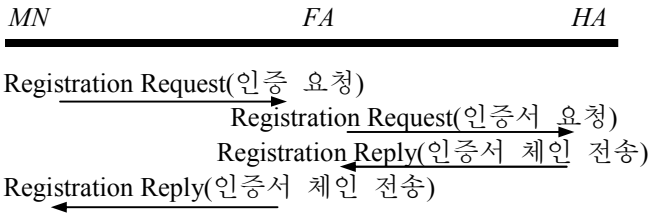
본 논문에서 제안한 인증 프로토콜은 *MN* 의 *HA* 가 *MN* 와 *FA* 에게 서로간의 전자서명을 검증할 수 있는 공개키를 인증서 체인 형식을 이용하여 전달한다.

4. 제안한 인증 프로토콜

본 장에서는 공개키 기반 인증 구조를 기술하고 MSR 기반 프로토콜과 [11,12]에 제시된 이동 통신 환경에서의 신뢰기관과 연계하여 수행되는 인증 프로토콜을 변형하여 제안된 인증 프로토콜을 설명한다.

4.1 인증 기반 구조

제안한 프로토콜에서는 공개키 기반 인증 구조를 Mobile IP 환경에 도입하기 위하여 인증기관(CA)를 도입한다. 본 논문에서는 *MN* 의 *HA* 가 인증기관의 역할을 한다고 가정한다. *HA* 는 엔티티들의 인증서에 접근할 수 있으며 제안한 인증 프로토콜에서 *FA* 는 *MN* 의 인증 기관인 *HA* 와의 통신을 한다.본 논문에서는 *HA* 가 인증서 리스트에 접근할 수 있는 사용자의 신뢰센터의 역할을 한다고 가정한다.



<그림 3> 제안한 인증 프로토콜 개요

Mobile IP 에서 사용되는 FA 와의 등록키를 생성해내기 위한 제안한 인증 프로토콜의 구조는 아래 그림과 같다. *MN* 는 새로운 라우팅 도메인에 들어가게 되면 *FA* 에게 인증 요청을 하게 된다. *FA* 는 *MN* 의 신뢰센터의 역할을 하는 *HA* 와의 통신을 통해 *MN* 와 *HA* 의 공개키를 얻을 수 있는 인증서 체인을 얻는다. 세션키를 생성해내는 알고리즘은 Diffie-Hellman 과 ElGamal[5] 기법을 사용한다.

4.2 제안한 인증 프로토콜

제안한 인증 프로토콜의 참가자는 *MN* , *FA* 그리고 *HA* 이다. *HA* 는 *MN* 의 신뢰센터의 역할을 한다. *HA* 는 *MN* 와 *FA* 의 공개키에 대한 인증서 취소 여부를 파악할 수 있으며 인증서 체인을 생성할 수 있는 기능이 있다. 인증 프로토콜에서 *MN* 와 *FA* 는 서로간의 신원을 인증하고 비밀 세션키를 성립한다. *MN* 는 *FA* 와는 Diffie-Hellman 기법을 사용하며 *HA* 와는 ElGamal 기법과 유사한 방법을 이용한다. 제안된 인증 프로토콜은 이산 대수 문제(Discrete Logarithm Problem)가 어렵다는 가정을 두고 있다. 우선 큰 소수 p 와 위수가 $p-1$ 인 곱셈상의 Z_p^* 군의 생성자 g 가 요구된다.

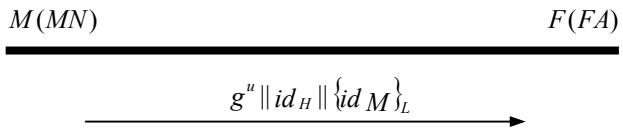
제안한 프로토콜의 목적은 다음과 같다.

- *MN* 와 *FA* 간에 명확한 상호 인증
- *MN* 와 *FA* 간에 상호 키 인증과 비밀 세션키의 성립
- *MN* 와 *FA* 간에 상호 키 확인
- *MN* 와 *FA* 간에 새로 생성되는 키에 대한 상호 확인
- *MN* 가 *FA* 에게 보내는 데이터의 부인 방지
- *MN* 가 *FA* 에게 보내는 데이터의 기밀성 보장

제안한 인증 프로토콜의 시작전의 가정은 다음과 같다.

- *MN* 와 *FA* 는 HA 의 전자서명을 검증할 수 있는 공개키를 가지고 있다.
- *HA* 는 *MN* 와 *FA* 의 공개키에 관련된 최신의 인증서 취소 리스트를 접근할 수 있다.
- *HA* 는 비밀-공개키 설정 쌍인 (w, g^w)을 가지고 있다.
- *FA* 는 비밀-공개키 설정 쌍인 (s, g^s)를 가지고 있다.
- *MN* 는 *HA* 의 ElGamal 공개키 g^w를 가지고 있다.

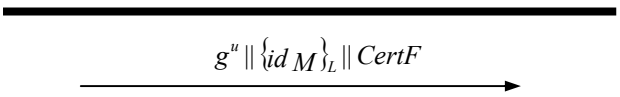
제안한 인증 프로토콜의 표기 형식은 다른 암호 시스템으로의 응용을 위하여 일반적인 방식을 이용하였다. id_X 는 X 의 신원을 의미하며, *CertX* 는 X 의 인증서를 뜻한다. *MN*, *FA*, *HA* 의 메시지 M 에 대한 전자서명 알고리즘은 각각 $Sig_M(M)$, $Sig_F(M)$, $Sig_H(M)$로 표기된다. 세션키 K 로 암호화된 메시지 M 은 $\{M\}_K$ 로 나타내어진다.



<그림 4> 제안한 인증 프로토콜 – 1

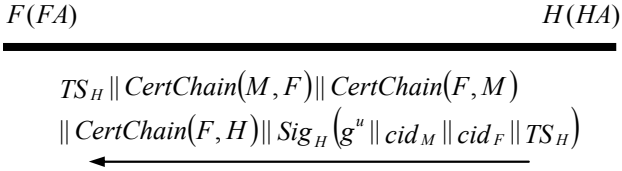
프로토콜(<그림 4>)이 시작되면 *MN* 는 난수 u 를 생성하고 ElGamal 공개키 g^u 를 생성하고 *HA* 의 공개키 g^w 와 같이 세션키 $L=(g^u)^w$ 을 계산한다. 이와 같이 자신의 *HA* 의 신원 id_H, 그리고 자신의 신원 id_M 를 세션키 L 을 이용해서 암호화해서 *FA* 에게 보낸다 id_M 를 암호화해서 보내는 이유는 사용자의 익명성을 보장하기 위해서이다.

<그림 5>에서 *FA* 는 *MN* 로 부터 전송 받은 g^u, id_M 를 자신의 인증서 *CertF* 와 같이 *HA* 에게로 보낸다.



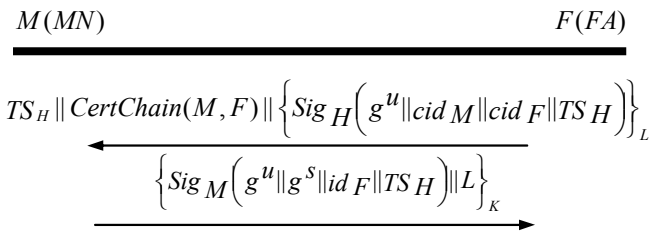
<그림 5> 제안한 인증 프로토콜 – 2

<그림 6>을 보면 *HA* 는 *MN* 의 ElGamal 공개키 g^u 와 같이 세션키 $L=(g^w)^u$ 을 계산한다. *HA* 는 *FA* 로부터 전송 받은 id_M 를 이용하여 *MN* 의 인증서를 찾아내고 인증서 체인 $CertChain(F,H)$ 을 생성한다. 마찬가지로 *HA* 는 *CertF* 에 기반해서 $CertChain(M,F)$ 을 만들어내고 g^u 를 이용하여 $CertChain(F,H)$ 를 계산한다. *HA* 는 타임스탬프 TS_H 를 생성해낸다. *HA* 는 *MN* 의 ElGamal 공개키 g^u 와 인증서 식별 번호 g^u, cid_M, cid_F, TS_H 에 전자서명을 수행한다.



<그림 6> 제안한 인증 프로토콜 – 3

<그림 7>을 보면 *FA* 는 $CertChain(F,H)$ 를 검증하여 *HA* 의 서명을 검증할 수 있는 공개키를 얻고 이를 이용하여 전자서명을. 그리고 $CertChain(F,M)$ 을 이용하여 *MN* 의 전자서명을 검증할 수 있는 공개키를 얻는다. *FA* 는 *MN* 의 공개키 g^u 를 이용하여 세션키 $K=(g^s)^u$ 를 계산해 낸다.



<그림 7> 제안한 인증 프로토콜 – 4

MN 는 *FA* 로부터 받은 $CertChain(M,F)$ 를 이용하여 *FA* 의 전자서명을 검증할 수 있도록 공개키를 복구해낸다. 그리고 *FA* 의 ElGamal 공개키 g^s 를 이용하여 *FA* 와의 세션키 $K=(g^u)^s$ 를 계산해낸다. 전자서명을 세션키 K 로 암호화하는 것은 다음의 두가지 이유

가 있다. 첫째, 전자서명을 하는 *MN* 이 세션키 *K* 를 알고 있다는 것을 확인시키며 둘째, *MN* 의 신원을 보호하기 위해서이다.

5. 성능 평가 및 분석

제안한 공개키 기반 인증 프로토콜은 *MN* 와 *FA* 간의 상호 인증과 비밀 세션키 설정을 허용한다. 표 1 은 제안한 인증 프로토콜과 Mobile IP 와의 성능 평가를 나타낸다. 제안한 프로토콜은 상대방의 신원을 상호 인증할 수 있으며 이동 통신 환경에서의 키 분배 문제를 공개키 암호 시스템을 이용하였다.

<표 1> 제안한 프로토콜 성능 비교

프로토콜 / 항목	Mobile IP	Route-Optimization	제안한 프로토콜
Entity Authentication	No	No	Yes (Mutual)
Key Distribution	Manual	Not stated	Public Key
Session Key Establishment with FA	No	Yes	Yew (Diffie-Hellman)
Session Key Establishment with HA	No	No	Yes (ElGamal)
Anonymity	No	No	Yes
perfect forward secrecy	No	No	Yes

제안한 인증 프로토콜은 *MN* 의 계산량을 네트워크 쪽으로 이전시켜서 *MN* 의 제한된 계산 능력을 고려하였으며 *MN* 의 신원을 세션키 *L* 로 암호화해서 보내므로 익명성이 보장된다. 또한 공개키에 기반하여 세션마다의 다른 세션키를 설정할 수 있으므로 perfect forward secrecy 가 보장될 수 있다.

6. 결론

본 논문에서는 Mobile IP 환경의 이동성을 지원할 수 있는 인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 공개키에 기반하여 이동 컴퓨팅 환경에서의 키 분배 문제를 고려하였으며 *MN* 와 *FA* 간에 상호 인증을 가능하게 하였다. 제안된 인증 프로토콜은 *MN* 와 *FA* 간에 비밀 세션키를 생성하여 사용자의 데이터에 대한 기밀성을 보장할 수 있다. 또한 Mobile IP 의 이동 컴퓨팅 환경을 고려하여 공개키를 기반으로 인증서 체인을 사용하였다.

참고문헌

[1] C. Perkins, Editor, “IP Mobility Support,” RFC 2002, October, 1996.

[2] C. Perkins, and D. B. Johnson, “Route Optimization in Mobile IP,” Internet Draft, February, 1999.

[3] C. Perkins, and D. B. Johnson, “Registration Keys for Route Optimization,” Internet Draft, November, 1997.

[4] W. Diffie and M. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, 1976.

[5] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Transactions on Informatio Theory, Vol. IT-31, No.4, pp.469-472, 1985.

[6] S. F. Foo, and K. C. Chua, “Region Aware Foreign Agent (RAFA) for Fast Local Handoffs,” Internet Draft, November, 1998.

[7] L.A. Sanchez, and G.D. Troxel, “Rapid Authentication for Mobile IP,” Internet Draft, November, 1997.

[8] M.C. Chua, and Y. Li, “Distributed Registration Extension to Mobile IP,” Internet Draft, October, 1997.

[9] S. Jacobs, “Mobile IP Public Key Based Authentication,” Internet Draft, March, 1999.

[10] ACTS AC095, ASPeCT Deliverable D20 – Project final report and results of trials, 1998.

[11] G. Horn and B. Preneel, “Authentication and payment in future mobile systems,” ESORICS LNCS 1488, pp. 469-472 1998.

[12] K.M. Martin, B. Preneel, C. Mitchell, H.J. Hitz, G. Horn, A. Poliakova and P. Howard, “Secure billing for mobile information services in UMTS,” IS&98, LNCS 1430, pp. 535-548, 1998

[13] M. Tatebayashi, N. Matsuzaki and D.B. Newman Jr., “Key Distribution Protocol for Digital Mobile Communications Systems,” *Advances in Cryptology – Crypto ’89*, Springer-Verlag, pp. 324-333 1990.

[14] M.O. Rabin, “Digitalized Signatures and Public-Key Functions as Intractable as Factorization,” MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[15] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, 1997.