ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

WP-IBE 적용 Mobile IPSec 연구☆

Study on WP-IBE compliant Mobile IPSec

최 정 현1*
Cheong Hyeon Choi

요 약

무선 인터넷에서 IPSec의 사용은 제한이 많다. MIPv4 IPSec 경로는 동적 무선링크를 포함하지 못한다. 즉 무선 인터넷의 IPSec은 Host-to-Host 경로 전체를 보호할 수 없다. 또한 무선 환경은 고정경로가 유지될 시간을 줄이지만 IPSec SA 합의를 위한 IKE의 지연시간은 상대적으로 길고, IPSec PKI 보안의 인증서 관리는 수행부담이 크다. 이는 무선 인터넷에서 IPSec 사용은 매우 불리하다는 의미이다. 본 논문은 무선링크까지 보호하는 Host-to-Host Transport Mode를 제공하면서 성능이 우수한 WP-IBE 보호방식을 적용하여 무선 인터넷에 유리한 Mobile IPSec을 구축하는 것이 목표이다. 이를 위해 Mobile IPSec은 무선링크를 포함하는 동적경로에 대한 라우팅이 필요하다. FA (Foreign Agent) Forwarding 방안은 동적으로 변경되는 경로를 FA가 확장하는 라우팅 방안이다. FA Forwarding을 위한 FA IPSec SA는 Source Routing 기반 Bind Update를 통해서 동적경로 변경 정보로 갱신된다. IPSec의 수행성능을 높이기 위해 효율적이고 강력한 차세대 Identity Based Weil Pairing (WP) Bilinear Elliptic Curve Cryptography인 WP IBE 방식을 적용했다. 본 논문은 WP-IBE 방식의 6개 암호 관련 알고리즘을 Mobile IPSec에 적용하는 변형 프로토콜을 제안하였다. 특별히 이 알고리즘을 ESP Datagram 구성에 적용하는 프로토콜에 집중하였다.

주제어 : 모바일 IPSec, 모바일 IPv4, 타원곡선암호기법, ID 기반 암호기법

ABSTRACT

In the wireless Internet, it is so restrictive to use the IPSec. The MIPv4 IPSec's path cannot include wireless links. That is, the IPSec of the wireless Internet cannot protect an entire path of Host-to-Host connection. Also wireless circumstance keeps a path static during the shorter time, nevertheless, the IKE for IPSec SA agreement requires relatively long delay. The certificate management of IPSec PKI security needs too much burden. This means that IPSec of the wireless Internet is so disadvantageous. Our paper is to construct the Mobile IPSec proper to the wireless Internet which provides the host-to-host transport mode service to protect even wireless links as applying excellent WP-IBE scheme. For this, Mobile IPSec requires a dynamic routing over a path with wireless links. FA Forwarding is a routing method for FA to extend the path to a newly formed wireless link. The FA IPSec SA for FA Forwarding is updated to comply the dynamically extended path using Source Routing based Bind Update. To improve the performance of IPSec, we apply efficient and strong future Identity based Weil Pairing Bilinear Elliptic Curve Cryptography called as WP-IBE scheme. Our paper proposes the modified protocols to apply 6 security-related algorithms of WP-IBE into the Mobile IPSec. Particularly we focus on the protocols to be applied to construct ESP Datagram.

☞ keyword : Mobile IPSec, Mobile IPv4, Elliptic Curve Cryptography, Identity Based Encryption

1. 서 론

최근 국내 기업에서 내부 직원이 핵심기술을 타국으로 유출하려다 검거된 사건이 보도되어 기업들은 기술의 보안에 관심을 기울이기 시작했다. 검거되지 않은 불법유출까지 포함한다면 그 피해 규모는 클 것으로 예측된다. 핵심기술을 보유한 기업들은 기술정보를 저장한 컴퓨터와 유통 네트워크에 대한 시스템 보안을 강화하고, 철저한 내부자 접근통제를 감독하는 보안 전담조직을 신설하고, 정보보호를 위한 행동수칙 및 강제규정 등을 정기적으로 교육하고 일상 업무에서 숙지케 하며, 사후 감시하는 보안실무를 일상화하여 정보보안의 실효성을 높이고 있다 [1].

그러나 현실은 대다수 기업들은 통합적 보안실무의 필요성을 공감하면서도 비용문제 때문에 이미 알려진 보안 취약점조차 충분히 대비하지 못하고 있다 [1].

기업 기술정보 불법유출의 일차 통로는 기업 네트워크를 인터넷에 연결하므로 발생하지만, 특히 접근통제가 어

1 MIS Dept., Kwangwoon Univ., Seoul, 139-701, Korea
* Corresponding author (chchoi@kw.ac.kr)
☆ 본 논문은 2011년도 광운대학교 교내연구비 지원에 의해 작성되었다.
[Received 30 July 2013, Reviewed 5 August 2013, Accepted 5 September 2013]

려운 무선 인터넷의 무선링크는 해커의 침입과 도청, 내부 아이디를 사용한 외부접속을 쉽게 하는 불법유출의 주요 통로가 되고 있다. 최근 무선 인터넷의 위험은 크게 증가했다 [2].

무선 인터넷의 정보유출에 대한 기본적 보안은 기술정보서버와 연결에 대한 접근통제와 사용통제이다. 이런 통제를 효과적으로 수행하려면 다음 사항들이 기본적으로 보장되어야한다 [1,2].

① 무선 인터넷에서 정보교환의 연결설정, 정보전송, 연결해제에서 무선링크의 노드는 신뢰확보를 위한 상호인증이 필요함 [13].
② 기술정보는 Host-to-Host 전체 경로에서 100% 안전한 암호화와 무결성 인증을 가지고 유통되어야 함 [1].
③ 암호키 및 암호 파라미터의 노출을 방지할 전방 기밀성 (forward secrecy) 보장이 필요함 [3].

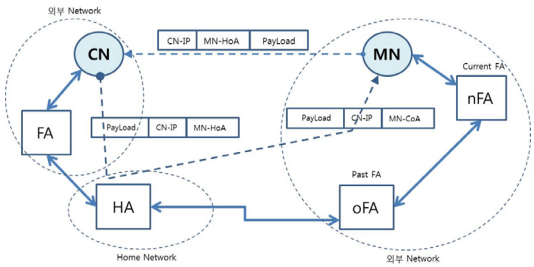
1.1 연구 범위와 목적

무선 인터넷에서 이런 보안성 보장은 IPSec의 ESP (Encapsulation Security Protocol)로 보호된 Host-to-Host Transport Mode 연결로 가능하다고 판단된다 [5][6][18]. 그러나 IPSec 보안방식은 수행성능이 낮기 때문에, IPSec 보안성능을 향상시킬 수 있는 강력하고 효율적인 타원곡선 기반 암호방식을 적용한다면 불법유출방지의 IPSec 기반 안전채널 구축은 가능할 것이다.

현재 IPSec은 IPv4의 고정경로 라우팅을 기반으로 설계되었기 때문에 무선 환경의 로밍(roaming) 호스트로 인한 동적경로 라우팅이 요구되는 무선 인터넷에서는 새로운 라우팅 방안이 필요하다 [9,14]. 다시 말하면 MIPv4 기반 IPSec은 동적 Host-to-Host Transport Mode 연결을 사용할 수 없다는 의미이다. 현재는 고정 호스트 또는 중간 게이트웨이 사이 Tunnel Mode 연결만을 허용하고 있다 [14].

또한 IPSec의 RSA 기반 공개키 방식은 연결설정에서 지연이 크고, 암호화와 인증에서 많은 계산을 필요로 하는 성능문제가 있다 [3]. 이런 IPSec 암호기법의 낮은 성능은 무선 환경에서는 더 악화된다. 따라서 MIPv4 IPSec에서 효율적인 적합한 암호기법은 매우 중요한 고려사항이라고 할 수 있다.

이를 위해 효율적 Bilinear Map 알고리즘이 존재하는 WP (Weil Pairing) ECC (Elliptic Curve Cryptography - 타원곡선 암호기법) [23]과 공개키 인증서의 관리 부담이 없는 IBE (Identity based Encryption) 방식을 연동하여 성능이 우수한 WP-IBE 방식에 주목했다 [24].



(그림 1) Triangle Routing Problem
(Figure 1) Triangle Routing Problem

WP-IBE는 공개키 기반 방식이므로 IPSec의 기존 공개키 방식과 연동하는 것에 큰 문제는 없다 [12][13]. WP-IBE 인증절차는 기존 인증방식과는 다르지만 오히려 서명이 쉽고 검증이 간단하므로 저성능 노드도 실행할 수 있는 장점이 있다 [23]. 이외에도 WP-IBE 방식에는 IKE (Internet Key Exchange)가 불필요하므로 키 합의 교환 지연이 없고, 효율적이고 강력한 ECC (타원곡선 암호기법) 방식으로 보안성능이 우수한 장점이 있다 [10][12].

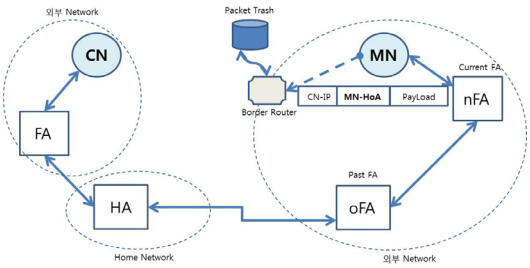
본 논문의 목적은 무선 인터넷에서 IPSec이 동적경로 라우팅을 할 수 있는 Mobile IPSec을 제안함으로써 Transport Mode 연결을 제공할 수 있게 하고, WP-IBE 방식을 Mobile IPSec ESP 보호에 사용하여 향상된 성능을 가진 알고리즘과 프로토콜을 구축하는 것이다.

1.2 동적 경로 라우팅의 방해 요소

무선 인터넷에서 동적 호스트로 인한 동적경로 라우팅 문제는 고정경로 라우팅 기반 MIPv4에서는 삼각 라우팅 (Triangle Routing) 기법으로 해결하고 있다 [9]. (그림 1)

(그림 1)의 삼각 라우팅을 보면, 만일 Datagram에 모바일 노드 (MN) 주소로 동적 임시주소 CoA (Care-of Address)를 사용하면, MN의 로밍(Roaming) 때, 그 임시주소가 변경되는 동적 문제가 있어서 'Host Unreachable' (배달 불능)을 야기할 수 있고 재전송도 증가하여 배달 지연도 커진다.

따라서 MIPv4는 Source/Destination Address에 MN의 위치주소보다는 고유주소 HoA (Home Address)를 사용한다. 단 MN의 위치주소는 배달에서 필수이므로 주소등록 BU (Bind Update) 과정에서 MN 관리자 HA (Home Agent)에 그 위치주소 CoA를 등록한다.



(그림 2) Ingress Filtering Problem
(Figure 2) Ingress Filtering Problem

(그림 1)을 보면, MN-방향 트래픽은 MN의 고유주소 HoA로 전송되므로 Home Network Gateway HA에 먼저 도착한다. 만일 해당 MN이 Home Network에 있으면 HA는 해당 트래픽을 MN에게 배달하면 된다. 반면 Foreign (외부) Network에 있으면 관리자 HA는 MN의 위치주소 CoA로 그 트래픽을 중계해야 하고, FA (Foreign Agent)에 배달하게 된다 [14]. (그림 1)에서 점선의 양방향 경로는 HA를 통과하는 삼각형을 형성하므로 삼각 라우팅이라 부른다 [9,27].

(그림 2)를 보면, MIPv4에서 MN 고유주소 HoA 사용이 또 다른 문제를 야기한다. 이는 경계 라우터의 Ingress Filtering 기능 때문이다. MIPv4에서 Foreign Network의 경계 라우터는 Source Address가 MN의 HoA인 Datagram을, 외부 네트워크 주소를 가졌다는 이유로, Spoofing Datagram으로 판단하고 제거하는 문제이다 [27].

현재 Filtering 문제의 일시적 해법으로 MIPv4에서는 Home Address Option을 두어 Source Address가 HoA인 Datagram은 Filtering을 중지해달라고 요청한다 [9,27]. 차세대 MIPv6에서는 Auto Configuration 주소변환 기법으로 CoA와 HoA의 네트워크 주소 구분을 없애므로 Filtering 문제를 해결한다 [9,27].

1.3 도전 과제

이런 문제로 MIPv4 IPSec에서 이동 호스트 간 Host-to-Host Transport Mode 연결을 사용할 수 없는 점에 주목하라 [14]. 이를 위한 우리의 첫 개선안은 무선 인터넷에서 이동 호스트 간 Host-to-Host Transport Mode 연결을 사용할 수 있도록 Datagram의 Address 필드에는 위치주소 CoA를 사용하게 하는 방안이다.

먼저 동적 CoA로 인해 형성되는 동적경로에 대한 Datagram 라우팅이 가능해야한다. 이를 위해 우리는 *FA Forwarding* 방식이라는 IPSec 동적 라우팅 기법을 제안하고 있다. 이 방안은 Old FA (ie. oFA)에 배달된 Datagram을 New FA (ie. nFA)로 *Forwarding* 하게 하는 방안으로 IPSec SA를 이용하여 IPSec이 직접 동적 라우팅을 수행하는 Mobile IPSec 방안이다.

*FA Forwarding*을 위해 oFA(Old FA) IPSec SA의 Source/Destination Interface Address를 갱신할 수 있도록 동적경로의 변경 정보를 제공해야한다. 본 논문은 새로운 주소등록 방식인 *Source Routing Bind Update (SRBU)*를 사용하여 관련된 FA에 동적경로의 변경 정보를 제공한다.

*SRBU*와 연동하는 *FA Forwarding* 방안은 Mobile IPSec에서 배달실패를 걱정하지 않는 동적 라우팅을 가능하게 한다 (그림 3). 특별히 *SRBU*의 정보 변경에서 고려할 보안사항은 nFA(New FA)와 oFA(Old FA)의 상호인증을 통한 확장된 경로의 신뢰보장이다.

우리의 둘째 도전은 WP-IBE 방식의 시스템 파라미터 생성과 분배, 키 생성과 분배, 메시지 암복호화 및 메시지/노드 인검증 알고리즘과 그 프로토콜들을 우리 Mobile IPSec에 적합하게 수정하여 제안하는 것이다. 이 알고리즘을 적용한 Mobile IPSec ESP (Encapsulation Security Protocol) Datagram의 구성방안도 제안하고, 동적 라우팅에 관련된 여러 종류의 IPSec SA 구성을 제안하고, 각 SA마다 필요한 암복호 및 인검증 알고리즘, 암복호키 및 다이제스트 생성 알고리즘을 제안한다.

본 논문의 구성은 2장에서 현재 MIPv4와 IPSec의 특성과 동작방식, 그리고 IBE (Identity Based Encryption)와 ECC (타원곡선 암호기법)의 수학적 이론과 암복호 및 인검증 알고리즘을 논한다. 3장에서는 MIPv4의 한계를 극복할 FA Forwarding 방안과 Source Route Bind Update 방안의 프로토콜을 제안한다. 4장에서는 우리의 Mobile IPSec에 WP-IBE 방식을 적용하는 프로토콜을 제안하고, 5장에서는 Mobile IPSec ESP Transport Mode에 WP-IBE 적용 방식을 제안한다. 6장에서 우리가 제안한 Mobile IPSec의 수행성능과 안전성 비교분석을 한다. 마지막으로 추후 연구에 대해 논한다.

2. 관련 연구

2.1 MIPv4와 IPSec

최근 WLAN (Wireless LAN) 확산으로 MIPv4 (Mobile IPv4) 기반 무선 인터넷 사용이 크게 증가하였다. 특별히 무선 인터넷의 무선링크는 스푸핑(spoofing) 공격에 매우

취약하다. 모바일 환경에서 모바일 노드 (MN)가 무선 AP(Access Point)의 FA로 로밍(roaming)할 때, AP의 FA와 MN 간 무선링크로 정보유출 위험이 커진다 [15].

WLAN은 무선링크를 보호하기 위해 단순 인증과 대칭키 암호방식을 주로 사용한다. 최근 AP와 MN 간 무선링크의 신뢰확보를 위한 Open-System 인증은 사실 보호기능이 없고, 공유키(Shared-Key) 인증방식은 Security Level이 낮고, 공개키 방식에 비해 안전성이 떨어지는 대칭키 방식으로 여전히 안전하지 않다. 또 무선링크의 암호화 방식인 WEP, TKIP, WPA 모두 스트링 암호 대칭키 방식으로 여전히 취약하다 [6,13].

따라서 보안이 취약한 IPv4 기반 연결에 강력한 보호를 제공하는 것이 IPSec이다. IPSec의 보호방식은, 첫째는 AHP (Authentication Header Protocol) 방식으로 Datagram Payload는 암호화 하지 않고, 인증정보만 담은 Authentication Header로 메시지 무결성을 보호하는 방식이다. 둘째는 ESP (Encapsulation Security Protocol) 방식으로 메시지 무결성 인증정보는 ESP Authentication Trailer에 담고, Datagram Payload는 암호화로 보호하는 방식이다 [11].

IPSec 연결의 시/종점 관점에서 보면, IPSec 연결의 출발 노드에서 암호화와 인증 처리를 수행하여 종점 노드까지 메시지를 보호된 상태로 전송하고 종점 노드에서 복호화/검증하여 메시지를 복구한다. 이런 IPSec 연결은 보호 정도와 범위에 따라서 Tunnel Mode와 Transport Mode로 구분된다 [8].

Tunnel Mode는 주로 고성능 노드 (Gateway 라우터 포함) 사이에 보호된 Tunnel을 형성하는 방식이고, 그 Tunnel 내에서 IP Datagram 전체를 메시지 암호화와 인증으로 전송 내용을 외부에 숨기는 방식이다. 이 Tunnel Mode는 두 단말 호스트 사이 전체를 보호하는 방식에는 사용되지 않는다 [11]. 이에 비해 Transport Mode는 메시지를 두 단말 호스트 사이에 Host-to-Host IPSec 연결을 설정할 수 있다. Datagram의 원래 IP Header는 그대로 두고, IPSec 연결 정보는 IPSec Header에 담는다. 특히 암호화는 Datagram Payload만 보호하고, Payload만 가지고 다이제스트를 계산하여 인증정보를 생성하고 이를 AHP Authentication Header 또는 ESP Authentication Trailer에 담는 방식이다 [11].

IPSec 기반 VPN에서 전체 연결 보호를 보장하는 방식은 ESP Transport Mode 연결방식이다 [6]. IPSec Transport Mode 연결의 두 단말 호스트는 동일 암호기법과 동일 키(key) 관련 정보를 가져야 한다. 이 암호기법 정보와 키 관련 정보를 담고 있는 것이 IPSec SA (Security Association)이다. IPSec SA는 IPSec Datagram 보안에 사용되고 IPSec 라우팅에서도 사용된다. IPSec SA의 합의는 키 교환 프로토콜이 IKE (Internet Key Exchange)에서 이루어진다. IKE의 Phase-2인 IPSec SA 합의과정에서 키 정보 노출을 방지하기 위해 IPSec SA의 키 정보를 암호화 전송할 때 사용할 암호정보는 IKE의 Phase-1의 Diffie Hellman Shared Key 합의로 된 ISAKMP SA이다 [10,11].

IKE의 수행부담을 보면, IPSec SA 합의까지 메시지 교환의 횟수로 본 지연은 IKE Phase-1에서 Main Mode는 6회이고 Aggressive Mode는 3회이다. IKE Phase-2은 Quick Mode에서 3회로 IPSec SA가 합의에 이른다. 따라서 IKE은 전체적으로 6~9회 메시지 교환의 지연이 발생한다 [12].

IPSec SA의 보안정보는 암/복호 알고리즘 및 암/복호키, 인/검증 알고리즘 및 인/검증키, 메시지 다이제스트 생성 해쉬 알고리즘의 암호기법 관련 정보이다. IPSec 보안연결을 의미하는 IPSec SA는 SPI (Security Parameter Index)로 식별되고 연결 경로의 시작주소와 종점주소를 가진다 [12]. 본 논문의 Mobile IPSec 동적 라우팅은 이 정보를 확장하여 사용한다. 이는 Mobile IPSec FA Forwarding이다.

MIPv4 IPSec 동적 라우팅은 삼각 라우팅을 통한다고 전술했다. HA의 중계를 통해서 동적 노드의 현재 주소로 IPSec Datagram을 배달하는 동적 라우팅 방식은 사실 MN의 이동성(mobility)에 적합하지 않다. 이와 같은 MIPv4 IPSec의 삼각 라우팅 때문에 IPSec이 제공하는 모든 연결 모드와 보호방식을 전부 사용할 수는 없다. 이런 이유로 무선 인터넷에서 MIPv4 IPSec은 대중적으로 사용되지 않는다 [15].

2.2 Weil Pairing EC Cryptography

본 논문의 Mobile IPSec에서 사용할 암호기법 WP-IBE의 암호화 및 인증 알고리즘 구축과 성능분석 및 보안성 분석을 위해 WP (Weil paring) Elliptic Curve (EC - 타원곡선) Cryptography와 IBE (Identity based Encryption) 방식의 특성은 아는 것은 중요하다 [19]. 먼저 WP EC (타원곡선) 암호기법에서 나타나는 수식은 특별히 명기하지 않아도 정수론 Modulo에 근거하는 점을 유념해야 한다 [21].

Pairing Based Cryptography에서 Bilinear Map은 중요하지만 이론적으로만 논의되었다. Bilinearity 속성을 만족하는 그룹(Group) 연산은 최근 Weil Pairing과 Tate Pairing Elliptic Curve에서 나온 Projective Group 연산으로 가능하게 되었고, 효율적인 Pairing Based Bilinear Map을 구현하

였다. 이런 효율적 Bilinear Map 알고리즘을 가진 현실적 암호기법이 Weil Pairing EC Cryptography이다 [19,21].

Miller [24]는 Weil Pairing EC Cryptography를 위한 두 그룹을 소개하였다. 첫 그룹 G_1^+는 Weil 타원곡선 $E: y^2 (\mathrm{mod} q) = x^3 + 1 (\mathrm{mod} q)$의 정수 좌표점 $(x,y) \in E(F_p)$, $p = 12q-1$을 원소로 구성되고, G_2^*는 Field F_{p^2}에서 구성된 Subgroup이다. 그 그룹의 특성을 요약하면 다음과 같다.

① 그룹 G_1^+: Order가 $q = |G_1^+|$이고 그룹 Generator는 P라면 $G_1 = \langle P \rangle = \{aP\}$, $a \in Z_q$, $p = 12q-1$이다.
② 그룹 G_2^*: Order가 q이고, 그룹 Generator는 $\hat{e}(P,P) = g$이고 $G_2 = \langle g \rangle = \{bg\}$, $b \in Z_q$이다.

Miller는 다음 속성을 만족하는 Polynomial Time bound Weil Pairing Bilinear Map $\hat{e}: G_1 \times G_1 \rightarrow G_2$을 제안하였다 [24].

① Bilinearity: $\hat{e}(aP,bP) = \hat{e}(P,P)^{ab}$
② Non-degeneracy: $\hat{e}(P,P) \neq 1$, $\hat{e}(P,P) = g$은 G_2의 generator가 된다.
③ 효율적 polynomial time bound 알고리즘이 존재: Boneh's 알고리즘 $\hat{e}(P,Q) = \frac{f_P(A_Q)}{f_Q(A_P)}$ [23]

이 Bilinear Map은 Additive Cyclic 그룹 G_1^+을 Multiplicative Cyclic 그룹 G_2^*으로 전환하는 역할을 한다. 여기서 $A_P = (P) - (O)$, f_P $((f_P) = nA_P)$이고 그 Complexity는 $O(\log p)$이다. 구체적 Group 연산은 생략한다. 자세한 것은 [23]을 참조하라.

이 암호기법의 장점을 살펴보면, Diffie Hellman (DH) 프로토콜에서 Alice와 Bob은 임의 정수 $a,b \in Z_q$ 선정하여 그룹 G_1에서 각각 $A = aP$, $B = bP$를 계산한 후, 상대에게 서로 각각 A와 B를 전송한다. G_2의 Generator가 $g(= \hat{e}(P,P))$라 하면, Alice와 Bob은 $\hat{e}(aP,bP) = \hat{e}(P,P)^{ab} = g^{ab}$ 계산하여 Shared Secret Key g^{ab}를 얻게 된다 [22].

그러나 도청자 Eve는 A, B 모두를 도청해도 g^{ab}를 계산한다는 것은 어려운 문제에 속한다. 이 문제를 Discrete Logarithm Problem (DLP) $a = Log_P A$, $b = Log_P B$ 을 푸는 문제이고 수학적으로 어려운(hard) 문제에 속한다. 다시 말하면 Eve가 Shared Secret Key를 얻을 수 있는 효율적 알고리즘은 존재하지 않는다는 의미이다. 이런 Bilinear Pairing-Based Cryptography에서 Diffie Hellman 프로토콜은 해킹되기 어려운 문제에 속한다. 이런 어려운 문제라는 가정을 Bilinear DH (BDH) assumption이라 부른다. 위 암호기법에서 Eve가 해당 Shared Key를 해킹하기 위해 요구되는 계산 문제를 Computational BDHP (CBDHP) 라고 부른다. 이 CBDHP은 DLP와 동일한 어려움(hard)에 속한 문제로 분류된다 [22].

WP ECC의 Security는 바로 BDH assumption에 근거한다. 악의적 해커는 도청한 부분적 암호정보로는 키를 알아내는 것이 불가능하다는 의미를 가진다. A, B, $C = abP$, $D = cP$, P가 주어져 있을 때 $C = D$ 여부를 알아내는 문제는 a, b, c 값 모두를 계산해야 알 수 있는 CBDHP 문제이다. 반면 WP ECC 방식에서는 $\hat{e}(P,C) = \hat{e}(P,D)$ 계산으로 알 수 있는 쉬운 문제에 속한다. 이 문제를 CBDHP와 구분하여 Decisional BDHP (DBDHP) 문제라고 부른다. 이는 Pairing-based Cryptography에서 인증과 검증에 사용하는 방식으로 큰 장점이다 [21,22].

2.3 WP IBE 암호기법 알고리즘

일반적으로 암호기법은 5가지 알고리즘을 정의한다. 그것은 암호, 복호, 인증서명, 검증 알고리즘과 다이제스트 생성 알고리즘이다. 그러나 IBE 방식은 Identity로부터 공개키와 개인키를 생성하는 키 생성 알고리즘이 추가된다 [21].

WP ECC에서 인증 서명과 검증은 Bilinearity 특성으로부터 어려운 CBDHP가 쉬운 DBDHP로 변환되는 장점이 있는 것은 전 Section에서 이미 언급했다. Menezes [21]은 인증과 검증의 알고리즘을 다음과 같이 제안했다.

서명(signature)

임의 정수 $a \in Z_q$를 비밀키로 선정하고, 공개키 $A = aP$ (mod q)를 생성한다. 메시지 m의 다이제스트 $M = Hash(m)$을 생성하고, $S = aM$ (mod q)으로 서명을 생성한다. 그리고 인증 Tuple (P,A,S,M)을 전송한다. 이 인증 Tuple이 알려져도 DLP로서 $a \in Z_q$를 알아낼 수 없다. 여기서 P는 시스템 파라미터의 일부이므로 생략해도 된다 [17,21].

검증(verification)

인증 Tuple (P,A,S,M)에서 $\hat{e}(P,S) = \hat{e}(P,aM) = \hat{e}(aP,M) = \hat{e}(A,M)$이므로 $\hat{e}(P,S) \equiv \hat{e}(A,M)$ 검사로 메시지 무결성 여부 검증을 수행한다. 해커가 해당 인증 Tuple의 조작을

위해 필요한 정수 $a \in Z_q$를 계산하는 것은 어려운 DLP (Discrete Logarithm Problem)이다 [17,21].

Boneh과 Frankliv [23]은 WP-IBE에서 Public Identity (ID)를 사용한 암/복호 알고리즘을 다음과 같이 제안하였다.

시스템 파라미터 설정

PKG (Private Key Generator) 서버는 초기 셋업(setup) 단계에서 두 Hash 함수 $H_1: \{0,1\}^* \rightarrow G_1$, $H_2: G_2 \rightarrow \{0,1\}^l$을 정의하고 시스템 비밀키 $t \in Z_q$ 선정하고, 공개키 $T = tP \pmod q$을 생성하여, 시스템 파라미터 $(G_1, G_2, \hat{e}, P, T, q, H_1, H_2)$를 생성한다 [23].

공개/개인키(key) 생성

PKG는 호스트 i의 Identity인 ID_i로부터 Identity 노출에도 안전한 공개키 $Q_i = H_1(ID_i, h^*)$를 생성하고, 개인키 $d_i = tQ_i \pmod q$를 계산한다. 개인키 d_i는 안전채널을 통해 호스트 i에게 보내진다. 여기서 h^*는 호스트 i의 관련 지역정보로서 길이 제한이 없고 반복 적용도 가능하다 [23].

암호화(Encryption)

임시 비밀키 $r \in Z_q$를 선정 후 $R = rP \pmod q$ 계산한다. 암호문은 $c = m \oplus H_2(\hat{e}(Q_i, T)^r)$ 방식으로 생성하고 암호 메시지는 (R, c)이다 [23,24].

복호화(Decryption)

$\hat{e}(Q_i, T)^r = \hat{e}(Q_i, tP)^r = \hat{e}(tQ_i, rP) = \hat{e}(d_i, R)$ 이므로 $H_2(\hat{e}(Q_i, T)^r) \oplus H_2(\hat{e}(d_i, R)) = 1$이 성립하므로 결국 $c \oplus H_2(\hat{e}(d_i, R)) = m$ 방식으로 메시지가 복원된다 [23,24].

일반적으로 WP-IBE가 수행하는 6개 암호 알고리즘의 입력 파라미터와 응답정보를 요약하면 다음과 같다 [23].

① *Setup*$(k) = (G_1, G_2, \hat{e}, P, T = tP, q, H_1, H_2)$
② *Key_Extract*$(ID_i) = < Q_i, d_i >$
③ *Encrypt*$(m, ID_i) = c$
④ *Decrypt*$(c, ID_i) = m$
⑤ *Sign*$(m) = (P, A, S, M)$
⑥ *Verify*$(P, A, S, M) =$ *true* | *false*

ID_i는 공개 Identity, Q_i는 공개키, d_i는 개인키, m는 메시지, c는 암호문, t는 시스템 비밀키이다.

이상 6개 알고리즘은 Mobile IPSec의 암호기법 WP-IBE의 알고리즘으로 사용하기 위해 본 논문에서 변형될 것이다 [24].

2.4 IBE Random Oracle Model 보안성

일반적으로 IBE (Identity Based Encryption) 방식에서 저성능 노드가 공개 시스템 파라미터를 가지고 공개/개인키 생성을 충분히 할 수 있다고 해도, 키 관리에서 노출위험이 높으므로 각 노드가 모든 암호 알고리즘을 직접 수행하는 것은 비효율적이다. 따라서 노출위험을 낮추기 위해서 보통 IBE 방식은 PKG 만 위 5개 암호 알고리즘을 수행할 수 있도록 하고, 다른 노드들로부터 알고리즘 수행 질의를 받아서 결과를 응답하는 방식인 Random Oracle Model (ROM)로 운용하는 방안이 이론적으로 논의되고 있다 [25].

ROM 방안은 알고리즘의 세부사항 노출위험을 줄일 수 있지만 악의적 해커 질의까지 응답해야 하는 문제가 있다. 알고리즘 수행 질의에 응답 정보만으로는 암호분석에 필요한 어떤 정보가 전혀 예측할 수 없어야 하는 Semantical Security(SS) 조건이 만족되어야 한다. Semantical Security는 Indistinguishability (IND) 조건과 Non-Malleability (NM) 조건으로 다시 나누어 볼 수 있다. 이 조건들의 수학적 의미는 다음과 같다 [26].

① **IND 조건:** 일반 평문 x와 그 암호문 y 사이의 관계에 대해서 어떤 정보도 얻을 수 없어야 한다는 조건이고, 기밀성을 의미한다 [26].
② **NM 조건:** 평문 x와 그 암호문 y 쌍 (x, y)을 알아도 변형된 새로운 쌍 (x', y')을 생성할 수는 없다는 조건이고, 불법적 조작이 불가능하다는 무결성을 의미한다 [26].

Bellare와 Rogaway [26]는 다음 특성 Trapdoor Permutation과 Random Hash의 조합으로 암호문 생성에 적용하면, IND과 NM 조건을 만족시킬 수 있다고 제안하였다.

① **Trapdoor Permutation:** $f(x) = y$에서 y만으로 x의 한 비트도 알아낼 수 없도록 만드는 함수 $f()$를 Trapdoor Permutation이라 하고, 역함수 $f^{-1}()$가 존재한다 [24].
② **Random Hash:** Hash의 특성으로 Hash의 출력은

Random 해야 하고, 동일 입력에 대해서는 Hash 값은 동일해야 한다 [24].

암호화 방식 $E^{G,H}(m)=f(r)\,\|\,G(r)\oplus m\,\|\,H(m)$은 암호문 $c=E^{G,H}(m)$을 생성한다. 이 방식은 IND-security와 NM-security를 만족한다 [26].

여기서 $H:\{0,1\}^{*}\rightarrow\{0,1\}^{k}$와 $G:\{0,1\}^{*}\rightarrow\{0,1\}^{\infty}$은 Random Hash이고, m은 메시지, c는 암호문이다. 우리의 WP-IBE 암호화 방식의 보안성 분석에서 사용할 것이다.

3. SRBU와 FA Forwarding 방안

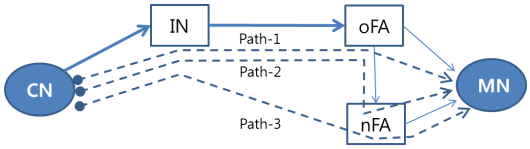
지금까지 언급된 IPSec에서 동적경로 라우팅에 관련한 문제를 요약해 보면 다음과 같다.

(1) IP주소와 라우팅 : IPv4 Datagram의 Address 필드는 고정 IP주소이므로 IPv4 라우팅은 고정 경로에 대한 것이다.
(2) MN에 관련 두 개의 IP주소 : 모바일 환경에서 MN은 고유주소로 등록된 IP주소 HoA (Home Address)와 FA (Foreign Agent)로부터 할당된 임시 IP주소 CoA (Care-of Address)가 관련된다 [14].
(3) IPSec과 삼각 라우팅 : MIPv4 동적 라우팅을 고정경로 기반 삼각 라우팅으로 해결한다. MN-방향 Datagram이 MN 관리자 HA (Home Agent)의 중계로 배달하는 방식이다 [14].
(4) IPSec Datagram Filtering : 경계 라우터의 Ingress Filtering 방식은 현재 IPSec Datagram의 Address 필드와 충돌한다.

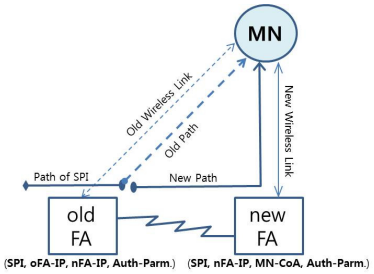
우리 논문의 관심은 이 문제들이 Mobile IPSec의 동적 Host-to-Host Transport Mode 연결을 사용할 수 없게 한다는 점이었다 (그림 3, 4).

우리의 첫째 개선안은 Datagram의 Source와 Destination Address에 Foreign Agent (FA) 할당 임시주소 CoA를 사용토록 하는 방안이었다. 이 방안은 Ingress Filtering 문제를 완전히 해결한다. MN의 이동성으로 어디에 위치해도 해당 네트워크에서 합법적 주소인 CoA를 Datagram의 주소 필드에 사용하였기 때문이다.

(그림 3)에서 Host-to-Host 연결에서 MN의 로밍으로 FA가 변경될 때, MN-oFA 무선링크가 MN-nFA 무선링크로 변경된다. (그림 3)을 좀 더 구체적으로 보면 MN의 로



(그림 3) IPSec Host-to-Host 연결
(Figure 3) IPSec Host-to-Host Connection



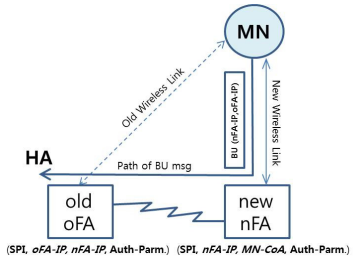
(그림 4) FA Forwarding
(Figure 4) FA Forwarding

밍(Roaming)으로 AP(Access Point) FA가 oFA에서 nFA로 변경되는 경우, 기존 MIPv4 IPSec의 라우팅은 경로 'Path-1' (CN, IN, oFA, MN)에서 경로 'Path-3' (CN, IN, nFA, MN)로 변경된다. 그러나 이런 CN-to-MN 경로의 변경에 적응하는 동적 라우팅이 없어서 Mobile IPSec Transport Mode가 정상적으로 제공되지 못한 것이다.

이를 위한 우리의 두 번째 개선안은 이미 형성된 IPSec 경로 'Path-1'은 그대로 두고, Old FA (ie. oFA)에서 New FA (ie. nFA)로 Datagram을 Forwarding 하는 방법으로 경로 'Path-1'을 확장하여 연장된 경로 'Path-2'를 형성하게 하는 방안이다. 이런 MN-방향 Datagram을 oFA가 nFA로 Forwarding 하므로 FA Forwarding 방안이라 부르겠다 (그림 4).

우리의 FA Forwarding 방안은 MN의 이동을 따라 기존 경로를 연장하는 방법으로 동적 라우팅을 하는 것이다. 기존 IPSec 게이트웨이가 IPSec SA를 따라 경로를 스위치 (switch) 하는 방식과 동일하다. 따라서 이를 구현하는 것은 기존 방식의 확장이다.

IPSec Transport Mode의 경로는 출발지와 도착지 사이에 먼저 설정되고 그 경로상의 라우터와 양쪽 호스트는 동일 보안방식과 동일 암호기법을 IKE 단계에서 합의하여 IPSec SA를 생성한다. 이런 IPSec compliant 노드들은 IPSec SA를 처리하고 암호 알고리즘을 수행할 능력이 있다고 가정한다. 우리의 FA Forwarding을 하는 FA도 IPSec



(그림 5) Source Route Bind Update
(Figure 5) Source Route Bind Update

Host Mobile IPSec SA for MN-bound Traffic

SPI	Source CN	Destination MN CoA	Route FA list (CN,oFA,nFA,MN)	Crypto-Parm.

FA IPSec SA in old FA

SPI	Source oFA	Destination nFA	none	Auth-Parm.

FA IPSec SA in current FA

SPI	Source oFA	Destination MN CoA	none	Auth-Parm.

(그림 6) IPSec SA 종류
(Figure 6) IPSec SA Sorts

compliant 하다고 가정한다.

그러나 우리의 IPSec compliant FA에서 필요한 암호 파라미터는 메시지와 노드 인/검증에 사용할 일부 파라미터만으로 충분하다. 이는 IPSec 경로의 양쪽 호스트와 중간 라우터에 있는 IPSec SA와 다르다. 우리는 이를 FA IPSec SA라 부른다. 우리 FA IPSec SA 구성은 아래와 같다 (* 본 논문의 FA Forwarding만을 위한 첨부한 정보). (그림 6 참조)

① SA Identifier/SN : IPSec 연결을 식별하는 SPI (Security Parameter Index)와 IPSec Datagram의 SN (Sequence Number)를 가진다.
② SA Source(시점) Interface (I/F) Address : FA에서 IPSec Datagram이 해당 FA로 들어오는 I/F 주소이다. New FA에는 Old FA의 IP주소이고 Old FA에는 변화가 없다.
③ SA Destination(종점) I/F Address : FA에서 IPSec Datagram이 나가는 I/F 주소이다. Old FA에는 New FA의 IP주소를, New FA에는 MN의 CoA 주소를 가진다.
④ *SA Valid-timer**: 해당 FA가 Forwarding을 수행할 유효기간의 타이머이다. FA IPSec SA는 해당 IPSec 경로와 유효기간과 다르다. New CoA의 주소등록이 HA와 CN까지 완료되면, CN은 MN-방향 트래픽에 New CoA를 사용하므로 Old FA의 Forwarding은 더 이상 이루어지지 않는다. 따라서 FA IPSec SA 유효기간이 IPSec 연결보다 작다.
⑤ *인증서명 알고리즘, 인증 파라미터**: FA간 SRBU 메시지 인증과 노드 인증 서명에 사용하여 신뢰관계 확보한다.
- 인증서명 알고리즘 : $Sign(H_3(m))$
- 인증 파라미터 : $(\hat{e}(), P, q, H_3)$

Mobile IPSec 동적 라우팅 프로토콜은 다음과 같다 (그림 3).

(1) FA가 IPSec Datagram 수신
(2) 그 Datagram의 AHP/ESP Header에 포함된 SPI 발췌/탐색, FA IPSec SA 선택
(3) 그 Datagram을 FA IPSec SA의 Destination I/F Address로 Forwarding 수행

우리의 FA Forwarding은 (그림 3)에서 경로 'Path-2'의 두 개의 FA (ie. oFA와 nFA)가 가진 FA IPSec SA의 Source/Destination I/F Address를 경로 연장에 적합한 주소로 변경하면, FA는 변경된 Destination I/F Address로 자동 Forwarding 하므로 Mobile IPSec은 경로 연장을 통한 동적 경로 라우팅이 가능하다. 따라서 FA (ie. oFA와 nFA) IPSec SA의 Source/Destination I/F Address를 변경하는 절차가 필요하다.

이 변경절차는 주소등록 과정을 통해서 구현된다. 기존 주소등록 Bind Update (BU) 메시지에 Source Routing Option을 사용하여 CN-to-MN 경로의 역방향 MN-to-CN으로 BU 메시지가 전달된다. FA는 IP Source Routing 처리에서처럼 BU 메시지의 Source Route Option 주소 리스트에서 자신의 주소를 확인하고 Timestamping을 한다. 여기서 주소 리스트를 확인하여 FA IPSec SA를 변경한다. 이 방안을 Source Routing Bind Update (SRBU)라 부른다. (그림 5)

SRBU 메시지는 IP Header의 Source Route Option에 SRBU의 경유 노드 리스트를 기록한다. SRBU 수신한 Old FA는 SPI로 식별한 FA IPSec SA의 Source I/F Address를 노드 리스트에서 자신의 주소 직전에 Timestamping된 New FA 주소로 변경한다 [14] (그림 5).

SRBU에 의한 FA IPSec SA 변경 프로토콜은 다음과 같다 [14] (그림 5).

(1) SA Source I/F Address ← SRBU의 Source Route Option에서 자신 IP주소 다음에 나오는 IP주소
(2) SA Destination I/F Address ← SRBU의 Source Route Option에서 자신 IP주소 직전에 나오는 IP주소

SRBU의 Source Route Option은 기존 IP Source Route Option 형식과 같다.

- *코드(0x89; 길이; 포인트; 노드 리스트=(MN,* FA_n, FA_o, N_i for $i \in [1,k]$, *CN)*

노드 리스트의 각 주소항목은 IP주소(32비트)와 Timestamp(32비트)로 구성된다. Timestamping은 해당 노드가 자신의 주소항목의 처리완료를 의미하는 처리시간을 기록하는 것이다.

New FA FA_n의 Datagram Incoming 주소인 Source I/F Address는 Old FA의 주소 FA_o이다. 중간 노드 N_j의 Source I/F Address는 N_{j-1} 이고 Destination I/F Address는 N_{j+1}가 된다.

FA 신뢰보장의 노드 인증은 FA IPSec SA 변경 전에 확인해야 할 필수 조건이다. SRBU에는 메시지 인증과 노드 인증을 위한 다이제스트를 계산하고 서명이 된 인증 Tuple을 포함시킨다.

노드의 메시지 인증과 노드 인증의 프로토콜은 다음과 같다. 여기서 노드 N_j가 인증 프로토콜을 수행한다고 가정하고, *Source*는 IPSec SA의 Source I/F Address를, *Destination*은 Destination I/F Address를 의미한다고 가정한다.

(1) Search for IPSec SA with SPI of SRBU.
(2) Extract $\Sigma_{N_{j-1}} = < A_{N_{j-1}}, S_{N_{j-1}}, M_{N_{j-1}} >$ from SRBU.
(3) If *Verify*($\Sigma_{N_{j-1}}$) is true, do (4); Otherwise exit;
(4) If *Source* is not N_{j+1}, *Source*←N_{j+1}; do (5);
(5) If *Destination* is not N_{j-1}, *Destination*←N_{j-1}; do (6);
(6) Change *Source Route Option* of SRBU as Timestamping as IP source routing protocol was.
(7) Make N_j's *Signature* $\Sigma_{N_j} = < A_{N_j}, S_{N_j}, M_{N_j} >$ as
  (가) Select random $a \in Z_q$.
  (나) Compute $A_{N_j} = aP \pmod q$.
  (다) Compute $M_{N_j} = H_3(SRBU \| IP_{N_j})$.
  (라) Compute $S_{N_j} = aM_{N_j}$.
(8) Attach Σ_{N_j} to SRBU, Then send SRBU to the next node N_{j+1}.

이상에서 다이제스트 M_{N_j}는 Timestamped Source Route Option을 가진 SRBU 메시지 전체를 Hashing 하여 생성된 것이다. 이 다이제스트는 두 Factor 즉 SRBU 메시지와 Timestamped 노드 리스트를 모두 포함하므로 SRBU 메시지 인증과 노드 인증에 사용하기 적합하다고 볼 수 있다.

4. Mobile IPSec WP-IBE 구축

공개키 방식을 사용한 경우 기존 IPSec의 시점과 종점 IPSec SA의 보안정보 구성은 아래와 같다 [11,12].

① *SA Identifier SPI (Security Parameter Index)*
② *SA Source I/F Address*
③ *SA Destination I/F Address*
④ *암호 알고리즘과 암호키*
⑤ *Digest 계산 해쉬 방식*
⑥ *인증 알고리즘과 인증키*

이미 언급한 FA IPSec SA와 비교하면 특별히 FA IPSec SA의 *Valid-timer*가 Host IPSec SA에는 필요 없다. Host IPSec SA는 연결해제 요청으로만 해제될 수 있기 때문이다. 반면 공개키 방식의 Host IPSec SA는 암호화와 인증서명을 위해 공개키와 개인키가 필요하다 [12]. MN-to-CN 연결의 Host IPSec SA에서 MN은 암호 알고리즘과 공개키를, CN은 복호 알고리즘과 개인키를 담는다. 그리고 인증 알고리즘, 다이제스트 생성 해쉬와 인증키로 RSA 공개키 방식에서는 개인키이고, 대칭키 방식에서는 비밀키를 IPSec SA에 담는다.

이미 언급한 것처럼 우리의 Mobile IPSec 방안의 암호기법은 WP (Weil Pairing) IBE (Identity based Encryption) 암호기법이다. WP IBE 방식을 기존 공개키 방식과 비교하면 서론에서 소개한 장점을 포함한 여러 강점을 가진다. 다시 강조하면, 첫째는 WP IBE 방식은 IKE와 같은 키 정보 교환 프로토콜이 불필요하다. 둘째는 Identity를 암/복호화 공개/개인키 생성에 사용하므로, 공인 인증서 교환이 불필요하다. 셋째는 인/검증방식은 쉬운 Decisional Bilinear DHP에 근거하므로 인증키가 불필요하다.

4.1 키 합의와 변경 프로토콜

Section 2.4에서 언급한 IBE 방식은 6개 암호 알고리즘에 대한 질의를 받으면 수행한 후 응답하는 ROM 방식으로 동작한다. 반면 IPSec의 기존 보안방식에서는 암호 알고리즘의 수행과 보호책임이 호스트나 라우터에 있다.

ROM PKG 서버 방식을 사용하려면 질의와 응답이 모든 사용자에게 공개되므로 질의응답 정보의 노출로 인한 보안문제를 충분히 고려해야 한다. 일반적으로 ROM PKG 방식은 제한된 경우에만 사용되는 것이 보편적이다.

우리의 방안은 키 생성만 ROM PKG 방식으로 수행하는 Key Escrow PKG 방식을 사용한다. 키 생성 시기는, 최초로는 MN이 HA에 등록될 때 이루어지고, 그 다음은 새로운 IPSec 연결이 설정될 때, Host IPSec SA가 합의될 때마다 새로운 키 생성이 이루어진다. 그러나 새로 생성된 키는 과거 암호키로 암호화하여 분배하므로 전방 기밀성을 만족한다. 이는 키 노출 확률을 줄이는 목적을 가진다.

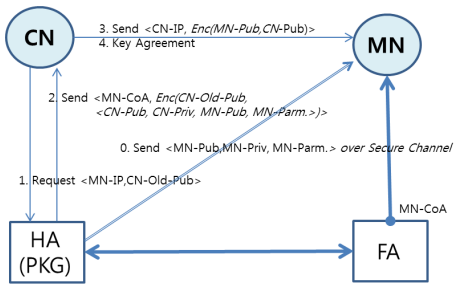
(그림 7)에서 우리가 제안한 키 생성과 분배의 프로토콜은 다음과 같다.

(1) 최초 키 생성 후 분배 (그림 7의 '0. Send <MN-Priv, MN-parm>') : 최초 MN에 WP IBE 암호기법에서 사용할 개인키 MN-Priv와 시스템 파라미터 MN-parm을 MN에 분배한다.

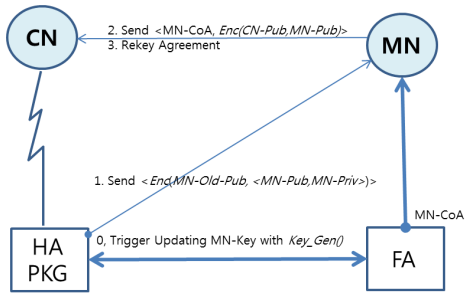
(2) CN의 연결요청 (그림 7의 '1. Request <MN-IP, CN-IP, CN-Old-Pub>') : 일방향 CN-to-MN 통신은 CN이 MN HA에 연결요청을 보내면서 시작된다. MN-IP는 MN HoA를 말한다.

(3) CN의 공개키와 개인키 생성 분배 및 MN 공개키 분배 (그림 7의 '2. Send <MN-CoA, *Enc(CN-Old-Pub, <CN-Pub, CN-Priv, MN-Pub, MN-parm>)*>') : PKG가 연결요청 CN의 공개키와 개인키를 Identity인 CN-IP로부터 생성하여, CN 키 쌍 (CN-Pub, CN-Priv), MN 공개키 MN-Pub와 시스템 파라미터 MN-parm를 CN Old 공개키 CN-Old-Pub으로 암호화하여 전송한다. 현재 CN 공개키는 본 메시지에 포함되어 있다. 전방 기밀성 보장을 위한 것이다.

(4) CN 공개키 MN에 분배 (그림 7의 '3. Send <CN-IP, *Enc(MN-Pub, CN-Pub)*>') : 역방향 MN-to-CN 통신을 위한 CN의 IP주소와 CN 공개키를 MN 공개키로 암호화하여 MN에 전송하여, IPSec 연결에 대한 MN의 Host IPSec SA를 합의한다.



(그림 7) 키 합의
(Figure 7) Key Agreement



(그림 8) Rekey Process
(Figure 8) Rekey Process

최초 MN 개인키의 분배는 Home Network의 안전채널을 통해서 이루어진다고 가정한다. 새로운 IPSec SA 설정이 필요하면, PKG는 MN 공개키와 개인키를 새로 생성하며, MN에 그 개인키를 분배하는 과정은 키 전방 안전성 보장을 위해서 MN Old-공개키로 암호화하여 분배한다.

키 변경(Rekey)은 *Key_Extract()* 수행요청과 같은 의미이다. 키 변경의 시작은 (그림 8)에서 나타난 '0 Trigger Updating MN-Key'라는 사건에 의해 촉발된다. 대표적 사건은 MN Key의 노출이 의심되는 경우, MN이 키 변경을 위해 *Key_Extract()* 수행요청을 PKG에 보내면 시작된다. 전방 기밀성을 위해서 변경된 개인키는 MN Old-공개키로 암호화하여 분배된다. 키 변경 프로토콜은 다음과 같다.

(1) 키 변경 요청 (그림 8. '0. Trigger Updating MN-Key') : 위 언급한 조건이 발생하면 MN의 *Key_Extract()* 요청으로 촉발된다.

(2) 키 생성 및 분배 (그림 8. '1. Send *<Enc(MN-Old-Pub, <MN-Pub, MN-Priv>)>*') : Identity MN-IP로 MN 개인키와 공개키 쌍을 MN-Old-Pub으로 암호화하여

MN에 배달한다.

(3) CN에 공개키 분배 (그림 8. '2. Send <MN-CoA, *Enc(CN-Pub, MN-Pub)*>') : 변경된 MN 공개키를 CN 공개키로 암호화하여 CN에 분배한다.

4.2 암복호 및 인검증 알고리즘

현재 IPSec의 암호기법은 대칭키 방식과 공개키 방식을 사용한다. 인증에도 개인키 서명방식과 비밀키 서명방식을 모두 사용하고 있다. WP IBE방식도 공개키 방식이므로 단순히 추가하면 된다. IPSec compliant 노드는 보안을 위해 암/복호 알고리즘과 인/검증 알고리즘, 해당 암호키와 인증키, 다이제스트 생성 해쉬함수가 상호 합의되어야 IPSec SA가 생성된다.

그러나 우리의 WP IBE 방식에서는 암호키는 Key Escrow PKG로부터 자동 생성되고 요청한 노드로 분배된다. 또한 인증키가 필요 없다. 암/복호와 인/검증 알고리즘은 Bilinear Map $\hat{e}$를 적용하는 것이 핵심이므로 WP IBE 방식의 *Setup()* 과정에서 생성된 암호 파라미터 (G_1, G_2, $\hat{e}$, P, T, q, k, l, H_1, H_2, H_3)로 충분히 수행된다. 키 생성을 제외한 암호화와 인증은 이 중 일부 파라미터로 충분하다 [23].

(그림 9)는 기존 키 합의 그림 7에서 MN-방향 IPSec 연결에서 사용할 MN-parm을 CN PKG에도 등록하는 과정이 포함되어 있다. 이는 MN-to-CN의 역방향 CN-to-MN 연결요청에서 사용하도록 한 것이다.

Section 2.3에서 논의된 알고리즘을 우리의 WP IBE 방식에 적합하게 변형하였다. 시스템 파라미터 생성, 키 생성과 암/복호와 인/검증 알고리즘은 다음과 같이 변형하였다 [4,17,22].

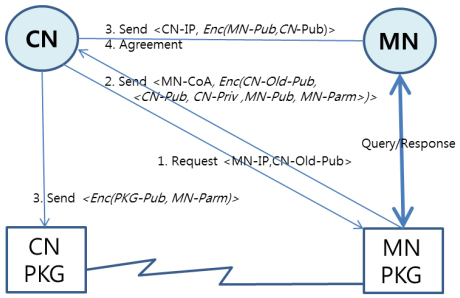
(1) *Setup()* ::== $(G_1, G_2, \hat{e}, P, T, q, k, H_1, H_2, H_3)$
where $T = tP$ (mod q) $t \in Z_q$, $G_1 = <P>$ of order q and $k = |H_3()|$

(2) *Key_Extract(ID)* ::== (d, Q)
where $Q = H_1(ID, h^*)$ and $d = t\,Q$ (mod q) at $t \in Z_q$

(3) *Sign(m)* ::== (R, S, M)
where $r \in Z_q$, $R = rP$ (mod q), $M = H_3(m)$ and $S = rM$ (mod q).

(4) *Verify(R,S,M)* ::==
if $\hat{e}(P,S) \equiv \hat{e}(R,M)$ then true else false

(5) *Encrypt(Q, m)* ::== (c, R, S, M)



(그림 9) Setup System Parameter 합의
(Figure 9) Setup System Parameter Agreement

(c, *Sign(m)*) where $c = m \oplus H_2(\hat{e}(Q_i, T)^r)$ and Q is a public key.

(6) *Decrypt*(d, (c, R, S, M)) ::==
if *Verify*(R, S, M) then m else failure, where $m = c \oplus H_2(\hat{e}(d, R))$ and d is a private key.

위 알고리즘을 보면, IPSec Host-to-Host 연결에서 암/복호와 인/검증 알고리즘에 필요한 시스템 파라미터는 일부분 ($\hat{e}()$, P, T, q, H_2, H_3)이면 충분하다. *Key_Extract()*에서 생성되어 일방향 CN-to-MN 통신을 위해 CN에게는 MN 공개키를, MN에게 자신 개인키를 분배한다. 이 공개키와 개인키는 그림 7, 8에서 언급한 방식으로 분배된다.

5. WP-IBE ESP Transport Mode

Mobile IPSec ESP Transport Mode 연결은 시점 호스트가 암호화, 메시지 인증, 노드 인증을 수행한다. 보안정보를 담은 ESP Datagram 구성은 다음과 같다 [12].

① IP Header : 기존 IP Datagram Header를 그대로 복사한다.
② ESP Header : IPSec SA의 식별자 SPI를 가진다.
③ Ciphered Payload : IP Header를 제외한 IP Payload 부분만 암호화된다.
④ ESP Trailer : 길이 조정을 위한 Padding Bits를 가진다.
⑤ ESP Authentication Trailer : 메시지 인증정보를 담는다.

다시 한 번 요약하면, IPSec ESP Datagram의 IP Header

에 Source/Destination Address로 CoA를 사용했고, 여기서 Mobile IPSec의 동적 라우팅을 위해 SRBU로 FA IPSec SA를 생성하여 FA Forwarding으로 경로를 연장하여 가능하게 했다. 동시에 WP IBE 방식으로 Ciphered Payload와 Authentication Trailer를 생성했다.

우리의 최종목표인 Mobile IPSec WP-IBE ESP Transport Mode 연결을 제공하는 방식을 WP-IBE Mobile IPSec라고 부르면서 논의를 계속하겠다.

5.1 WP-IBE Mobile IPSec SA

WP-IBE Mobile IPSec 방안은 일방향 CN-to-MN 연결에서 단말 호스트 CN과 MN의 Host Mobile IPSec SA 정보를 다음과 같이 확장한다 (그림 6, 10).

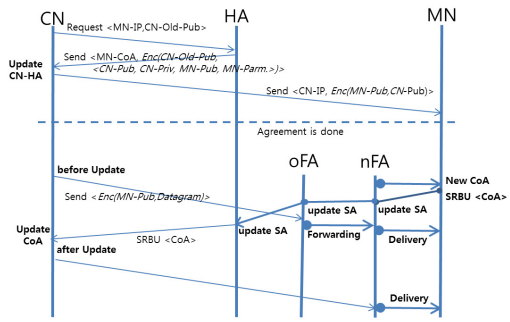
① *SA Header 정보* : 기존 SA 3개 정보
- 기존 SA SPI
- Source I/F Address
- Destination I/F Address

② *SA 라우트** : Source에서 Destination까지 연결 경로에 있는 노드 리스트 L_{node}=(MN, FA_n, FA_o, N_i for $i \in [1,k]$, CN) 는 IPSec 라우팅 경로이다.

③ *시스템 파리미터, 암복호키* : 이 필드는 단말 호스트에서만 사용되고 FA IPSec SA에서는 불필요하다.
- WP IBE 시스템 파라미터 : 일부 ($\hat{e}()$, P, T, q, H_2, H_3) 사용한다.
- 암복호키 : CN은 암호화용 MN의 공개키 Q_{MN}과 복호화용 CN의 개인키 d_{CN} 이고, MN에게 암호화용 CN의 공개키 Q_{CN}과 복호화용 MN의 개인키 d_{MN} 이다.

④ *인검증 알고리즘, 노드 Identity, 다이제스트 생성 알고리즘* : 여기서 IPA는 자신의 IP주소이고 호스트의 Identity이다.
- 인증서명 알고리즘: $Sign(Digest)$
- Digest 알고리즘: $Digest = H_3(m \| IPA)$

위 ②, ③, ④는 우리 방안의 Host Mobile IPSec SA만의 정보이다. ②의 '*SA 라우트*' 정보에 포함되어야 할 주 관심대상은 동적 FA들이다. 이 리스트에는 시점 호스트에서 종점 호스트까지의 경로에 상호인증으로 신뢰 확보된 중간 FA만 포함한다. 최초 무선링크의 MN과 FA의 상호인증은 그 FA의 주소할당과정에서 안전하게 수행되었다고 가정한다.



(그림 10) Mobile IPSec Operation
(Figure 10) Mobile IPSec Operation

특히 4장에 언급한 FA IPSec SA의 '*SA Valid-timer*'는 MN의 주소등록 SRBU 메시지가 CN까지 도착하여 주소갱신이 완료될 때까지 소요될 예측시간으로 설정된다. *Valid-timer*가 종료되었다는 의미는 그 FA가 FA Forwarding 할 필요가 없어졌다는 의미이다. 즉 CN은 MN-방향 Datagram의 Destination Address에 New CoA를 사용하므로 Old FA로 배달될 Datagram이 없다는 의미이다 (그림 10).

(그림 10)에서 보면 'after update'라는 것은 SRBU 주소갱신이 CN까지 완료되었다는 의미이고, 이 후 전송하는 Datagram은 oFA(Old FA)를 거치지 않게 된다. 한 번 더 주목할 것은 SRBU를 통한 FA IPSec SA의 시점과 종점주소를 변경할 때, 3장에서 제안한 프로토콜을 따라서 oFA(Old FA)와 nFA(New FA) 사이 상호인증이 수행된다는 것이다.

5.2 WP-IBE ESP 프로토콜

우리의 WP-IBE 방식을 Mobile IPSec ESP에 적용한 ESP Datagram 생성 프로토콜은 다음과 같다.

(1) IP Header 생성 : IP Option을 포함한 IP Header 정보를 복사한다.

(2) ESP Header 생성 : Mobile IPSec SA의 SPI 식별자와 SN (Sequence Number)로 구성된다.

(3) Ciphered Payload 생성 :
- *Encrypt*(Q,m) = ($<c>$,$<R,S,M>$) 수행 (Section 5.4 참조)
- $<c>$ 발췌, Ciphered Payload로 사용

(4) ESP Trailer 생성 : 길이 조정을 위한 Padding Bits를 계산하여 붙인다.

(5) ESP Authentication Trailer 생성 :

- *Encrypt*(Q,m) = (<c>,<R,S,M>) 수행 (Section 5.4 참조)
- <R,S,M> 발췌, ESP Authentication Trailer에 인증 Tuple로 사용

6. WP-IBE Mobile IPSec 강점 분석

우리의 개선방안들을 포함한 Mobile IPSec의 강점 분석은 수행성능 분석과 보안성 분석으로 나눈다.

6.1 수행성능 분석

먼저 기존 공개키 암호기법과 우리의 WP-IBE Mobile IPSec 방식의 수행성능 비교로 분석해 보자. 특히 두 방식의 전송과정에서 필요한 Trip Time 횟수를 단위로 분석한다.

기존 IPSec은 키 정보 교환 프로토콜 IKE를 통해서 IPSec SA를 합의한다. IKE Phase-1 ISAKMP SA 합의에서 Main Mode를 사용할 때 6 TDs (Trip Delay)가 소요되고, Aggressive Mode를 사용하면 3 TDs가 소요된다. IKE Phase-2 IPSec SA 합의에서 ISAKMP SA를 이용하는 Quick Mode를 사용할 때 3 TDs가 소요된다 [18]. 따라서 IKE 완료에 필요한 최소 지연은 6~9 TDs이다. 반면 그림 10에서 보면 우리의 개선방안은 Key Agreement까지 3 TDs 지연이 소요된다.

일반적 고정 라우팅은 CN-MN 왕복 지연으로 2 TDs가 요구되지만, 기존 MIPv4에서 삼각 라우팅으로 인한 지연은 3 TDs가 필요하다 (그림 1). 우리 방안은 모바일 환경에도 불구하고 항상 2 TDs 지연이 필요하고, 이는 고정 라우팅의 지연과 동일하다 (그림 10 참조).

기존 MIPv4에서는 이동성 MN의 FA 변경으로 인해 추가적 지연이 발생한다. MN의 로밍으로 FA가 변경될 때 주소등록 BU 메시지를 HA로 보낸다. HA에서 주소등록이 완료되기 전에 Old FA로 이미 전송된 미도착 Datagram은 배달 불능 에러로 처리된다. 그 Old FA는 Host-Unreachable ICMP 메시지를 전송자 CN에게 보내고, 그것을 수신하면 해당 Datagram을 재전송한다.

이 과정의 지연을 보면, FA 변경 후 MN의 주소등록 BU 메시지가 HA에 도착할 때까지 추가로 최소 1 TD 지연이 소요되고, 주소등록 후에 재전송이 가능하다.

기존 방식에서 Old CoA가 유효하거나 New CoA 주소등록이 완료된 후, Datagram 전송이 발생할 확률을 $p_s \le 1$라 하고, 1 TD 지연시간을 t_d라고 하면, 일방향 CN-to-MN에서 CN의 성공적 전송은 삼각 라우팅으로 2 TDs 지연이 필요하다. 만일 배달 불능으로 전송이 실패하면, 처음 실패한 전송에 2 TDs의 지연, Host-Unreachable ICMP 메시지로 배달로 2 TDs의 지연, 재전송으로 2 TDs의 지연이 소요되고, 실패한 전송은 재전송 성공까지 총 6 TDs의 지연이 발생한다.

기존 MIPv4 삼각 라우팅 방식의 평균 지연 계산식은 $(2t_d)p_s + (6t_d)(1-p_s)$이고 평균 지연시간은 $(6-4p_s)t_d$이다. 모바일 환경에서 빠른 이동성은 전송 성공확률 p_s을 낮추므로, 평균 지연시간은 증가하게 된다. 결론적으로 Mobile IPSec SA 설정 후 보안전송 프로토콜의 지연은 (표 1)로 요약할 수 있다. 단위는 TD이다.

(표 1) IPSec 전송 지연 비교 (p_s 성공확률)
(Table 1) IPSec Delay Comparison (p_s Success Probability)

구분	기존 방식			우리방식
	best	average	worst	
Key Agreement 전	6		9	3
CN→MN 전송	2	$6-4p_s$	6	1

본 논문에서 사용한 WP ECC는 효율적 암호방식으로 기존 공개키 암호방식 RSA 또는 DH (Diffie-Hellman) 보다 월등한 수행성능을 보여준다 [20].

(표 2) Key Size for Security Level [20,28]
(Table 2) Key Size for Security Level [20,28]
(2/3TDEA: 2/3-key Triple DES with 112/168-bit)

Security Level (Symm Key)	RSA/DH Key Size	EC Key Size	Ration RSA/EC
80 (2TDEA)	1024	180	5.7
112 (3TDEA)	2048	224	9.0
128 (AES)	3072	256	12.0
192 (AES)	7580	384	19.7
256 (AES)	15360	521	29.4

NSA [20]는 (표 2)에서 보면 다음과 같은 비교를 하고 있다. 동일한 키 길이 라면 그 Security Level은 Security Strength를 의미하는 것으로 일명 Security Bit라고도 한다. 만일 Security Level이 n 이면 컴퓨터에서 해당 Cryptography에 대한 어떤 값을 얻기 위해 최소 2^n operations이 요구된다는 의미이다 [28].

(표 2)에서 ECC의 Security Level을 RSA와 비교하면 최대 30배 키 길이 차이가 난다. (표 3)에서 보면 기존 DH 방식과 비교한 EC의 수행성능은 최대 64배의 차이를 알 수 있다. 또한 (표 2)에서 키 크기는 암호방식의 수행성능 $O(2^k-1)$ (k는 키 크기)과 관련된다 [20,28].

(표 3) Cost 비교 for Security Level [20]
(Table 3) Cost Comparison for Security Level [20]

Security Level	DH cost : EC cost
80	3 : 1
112	6 : 1
128	10 : 1
192	32 : 1
256	64 : 1

우리의 Mobile IPSec은 기존 MIPv4 IPSec IKE로 인한 지연이 없고, 삼각 라우팅이 필요 없어 전송지연이 없다. IBE 방식으로 공인 인증서 관리 부담이 없다. 이에 더하여 효율적 ECC 방식인 WP ECC 방안은 공개키 방식임에도 불구하고 높은 수행속도와 안전성을 보여준다. 우리 보안방식의 핵심 $\hat{e}()$의 수행성능 $O(\log p)$으로 최적이다 [23]. 결론은 우리 Mobile IPSec 방안은 매우 높은 수행성능을 보여준다고 할 수 있다.

6.2 보안성 분석

3.3절에서 언급한 ROM IBE 방식의 안전성 조건은 기밀성 IND-security와 무결성 NM-security 이다. IBE ROM 방식에 대한 공격자의 가장 강력한 공격은 ID-based Adaptive Ciphertext를 통한 공격인 ID-CCA2이다. 이 강력한 ID 기반 공격에 대한 안전성 조건은 IND-ID-CCA2과 NM-ID-CCA2이다. 어떤 암호기법이 이를 만족한다면 그 암호화 방안은 안전하다고 말할 수 있다 [7,25,26].

Section 2.4에서 언급한 IND/NM 조건을 만족시키는 암호화 알고리즘은 $f(r) \| G(r) \oplus m \| H(m)$ 이다. Section 4.2의 우리의 보안방안 WP-IBE 암호 알고리즘 *Encrypt()*가 이것과 일치하는지를 보면 다음과 같다.

① $G(r) \oplus m$: Random Generator $G(r)$은 우리의 $c = m \oplus H_2(\hat{e}(Q_i, T)^r)$에서 $\hat{e}(Q_i, T)^r$와 구조적 의미가 일치하므로 우리 암호화 방안은 Random Generator를 가진다.

② $H(m)$: 우리의 해쉬 $H_2()$와 일치하므로 우리 암호화 방식에는 두 번째 Random Generator도 존재한다.

③ Trapdoor Permutation $f(r)$: 우리 방식의 $r \in Z_q$, $R = rP$ (mod q)과 일치한다. Additive Group의 $R + Q = 0$에서 역함수 $Q = -rP$ (mod q)가 존재하므로 우리의 방식에는 Trapdoor Permutation 특성이 존재한다.

그러므로 우리의 암호화 방식은 IND와 NM 조건 모두를 만족시킨다고 할 수 있고 안전하다고 할 수 있다.

마지막으로 추후 연구를 살펴보면 본 논문의 Mobile IPSec은 구현이 가능한 방안이다. 우리는 본 Mobile IPSec을 구현하려고 하고 있다. 또한 WP ECC의 암호 알고리즘들의 수학적 Complexity 분석이 필요하다. 특히 WP ECC의 시스템 파라미터 생성 및 키 생성 수행시간 분석이 필요하다. 현재 우리는 시뮬레이션 모델, 성능분석 테스트 베드의 구축 연구를 하고 있다.

참 고 문 헌(Reference)

[1] Cheong H. Choi, “Study of Document Distribution System Architecture for Digital Secret Document Leakage Prevention,” Journal of Korean Society for Internet Information, Vol.11, No4, Aug. 2010, pp 143-158

[2] Cheong H. Choi, “The Study on Design and Implementation of MSEC-based Group Key Management Protocol for Corporate Secret Distribution,” Journal of Korean Society for Internet Information, Vol.11, No6, Dec. 2010, pp 87-110

[3] Cheong H, Choi, “Study on IBE-based Crypto-Module Functional Architecture,” 2010 Proceedings of the Korean Society for Internet Information Conference, pp. 419-422, Jeju Habitchi Resort, Jesus, Jun-25, 2010

[4] Cheong H. Choi, “IBE based Mobile IP Security,” Proceedings for ICONI & APIC-IST 2010, pp. 115-118, Mactan Island, Philippines, 2010-12-17

[5] Torsten Braun and Marc Danzelsen, “Secure Mobile IP Communication,” LCN ’01 Proceedings of the 26th Annual IEEE Conference on Local Computer Networks, p. 586, IEEE Computer Society, Washington

DC, USA, 2001

[6] Wei Qu and Sampalli Srinivas, “IPSec-based secure wireless virtual private network,” MILCOM 2002 Proceedings, Vol. 2, pp. 1107 – 1112, Oct. 7-10, 2002

[7] Daniel B. Faria, and David R. Cheriton, “Detecting Identity-based Attacks in Wireless Networks Using Signalprints,” WiSe’06, September 29, 2006, Los Angeles, California, USA. pp. 43-52

[8] Craig A. Shue, Minaxi Gupta, Steven A. Myers, “IPSec: Performance Analysis and Enhancements,” ICC 2007 Proceedings, IEEE 2007, pp. 1527-1532

[9] Salem Itani, “Use of IPSec in Mobile IP,” Report ID#20011003, The American Univer- sity of Beirut, May 21, 2001

[10] D. Harkins, and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409, Nov. 1998

[11] S. Kent and R. Atkinson, “IP Encapsulat- ing Security Payload (ESP),” RFC 2406, Nov. 1998

[12] C. Kaufman, Ed, “Internet Key Exchange (IKEv2) Protocol,” RFC 4306, May 2005

[13] C. Perkins and P. Calhoun, “Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4, “ RFC 3957, March 2005

[14] S. Vaarala and E. Klovning, “Mobile IPv4 Traversal across IPsec-Based VPN Gateways,” RFC 5265, June 2008

[15] H. Choi, H. Song, G. Cao and T. F. La Porta, “Mobile multi-layered IPsec,” Journal of Wireless Networks, Volume 14, Issue 6, pp. 895-913, December 2008

[16] G. Appenzeller and B. Lynn, “Minimal-Overhead IP Security using Identity Based Encryption,” http://citeseerx.ist.psu.edu/viewdoc/doi=10.1.1.10.3124

[17] K. G. Paterson, “ID-based signatures from Pairings on Elliptic Curves,” http://eprint.iacr.org/2002/004.pdf

[18] A. Alshamsi and T. Saito, “A Technical Comparison of IPSec and SSL,” 19th Interna-tional Conference on AINA 2005, 28-30 March 2005, Vol. 2, pp. 395-398

[19] Anoop MS, “Elliptic Curve Cryptography,” MS Anoop - An Implementation Guide, Jan. 2007, http://www.infosecwriters.com/text_resources/pdf/Elliptic_Curve_AnnopMS.pdf

[20] NCSA, “The Case for Elliptic Curve Cryptography,” http://www.nsa.gov/business/prog-rams/elliptic_curve.shtml, Jan. 2013

[21] A. Menezes, “An introduction to pairing-based cryptography,” Notes from lectures (2005) in http://www.cacr.math.uwaterloo.ca/~ajmeneze/public

[22] D. Boneh (1998), ″The Decision Diffie – Hellman Problem″. ANTS-III: Proceedings of the Third International Symposium on Al-gorithmic Number Theory (Springer-Verlag): pp. 48-63, 1998

[23] D. Boneh and Matthew Frankliny, “Identity-Based Encryption from the Weil Pairing”, SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[24] V. S. Miller, “The Weil Pairing, and Its Efficient Calculation,” J. Cryptology (2004) 17: pp. 235 – 261, 2004

[25] M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols,” Proc. First Annual Conf-erence on Computer and Communications Security, ACM, 1993

[26] M. Bellare, A. Desaiy, D. Pointchevalz, P. Rogaway, “Relations Among Notions of Security for Public-Key Encryption Schemes,” Advances in Cryptology, CRYPTO ’98, Lecture Notes in Computer Science, Vol. 1462, H. Krawczyk ed., Springer-Verlag, 1998

[27] F. Baker and P. Savola, “Ingress Filtering for Multihomed Networks,” RFC 3704, March 2004

[28] NSA, “Suite B Implementer’s Guide to NIST SP 800-56A,” http://www.nsa.gov/ia/_files/SuiteB_Implementer_G-113808.pdf, July 28, 2009

◐ 저 자 소 개 ◑

최 정 현

1984년 서울대학교 컴퓨터공학과(공학사)
1988년 미국 조지아공과대학교(GIT) 대학원 컴퓨터학과(이학석사)
1992년 미국 알라바마(Alabama) 주립 어번(Auburn)대학교 대학원 컴퓨터공학과(공학박사)
1994년~현재 광운대학교 경영대학 경영정보학과 교수
관심분야 : 인터넷 프로토콜, 정보보안, 암호학 etc.
E-mail : chchoi@kw.ac.kr