情報保護學會論文誌
第13券 第1號, 2003. 2

WAP에서 사용 가능한 ElGamal 기반의 비대화형 불확정 전송 프로토콜

정 경 숙*, 홍 석 미**, 정 태 충***

Non-Interactive Oblivious Transfer Protocol based on ElGamal in WAP

Kyoung Sook Jung*, Seok Mi Hong**, Tae Choong Chung***

요 약

인터넷이 무선 구간으로 확대됨에 따라 보안측면에서도 효율적이고 안전한 새로운 보안 프로토콜이 필요하게 되었다. 본 논문에서는 이러한 요구를 해결하기 위해 통신량이 적을 뿐만 아니라 신뢰 기관이 비밀키를 보유함으로 인해서 발생하는 문제점을 해결할 수 있는 새로운 프로토콜을 제안하고자 한다. 이 프로토콜은 비대화형 불확정 전송 프로토콜로서 기존의 안전도가 검증된 ElGamal 공개키 알고리즘을 기반으로 하였다. 제안된 프로토콜은 불확정 전송 프로토콜이므로 서버와 클라이언트간의 통신량을 줄일 수 있고, 챌린지 선택 비트(challenge selection bit)를 사용하여 클라이언트가 서버에 인증되는 확률을 줄임으로서 프로토콜의 효율성을 높였다. 또한 이중지수승(double exponentiation)을 사용함으로써 메시지를 복호화 할 경우 기존의 이산대수나 소인수문제보다 어렵게 되므로 프로토콜의 안정성을 높일 수 있다.

ABSTRACT

As the Internet moves to mobile environment, one of the most serious problems for the security is to required a new security protocol with safety and efficiency. To solve the problem, we propose a new protocol that reduces the communication traffic and solves the problem associated with the private security keys supplied by the trusted third party. The protocol is a non-Interactive oblivious transfer protocol, based on the ElGamal public-key algorithm. Due to its Non-Interactive oblivious transfer protocol, it can effectively reduce communication traffic in server-client environment. And it is also possible to increase the efficiency of protocol through the mechanism that authentication probability becomes lower utilizing a challenge selection bit. The protocol complexity becomes higher because it utilizes double exponentiation. This means that the protocol is difficult rather than the existing discrete logarithm or factorization in prime factors. Therefore this can raise the stability of protocol.

Keyword : *WAP(Wireless application protocol), oblivious transfer, ElGamal function*

Ⅰ. 서 론

무선 인터넷 서비스의 수요는 세계적으로 크게 증가하고 있으며, 2003년경에는 전 세계 무선 인터넷의 사용 인구는 6억명 이상으로 추정된다. 무선 인터넷 서비스를 위한 프로토콜은 현재 개발 중에 있으나

* 경희대학교 컴퓨터공학과 인터넷 & 지능시스템연구실 박사 수료(jungks@iislab.kyunghee.ac.kr)
** 경희대학교 컴퓨터공학과 인터넷 & 지능시스템연구실 박사 수료(smhong@iislab.kyunghee.ac.kr)
*** 경희대학교 컴퓨터공학과 교수(tcchung@khu.ac.kr)

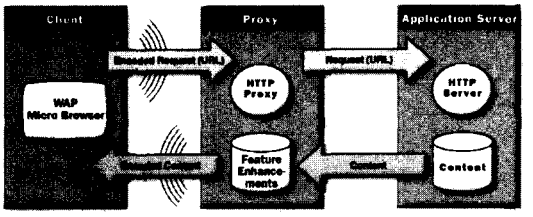
아직 표준화가 확립되지 않은 상태이다. 또한 전자상거래 서비스를 원활히 하기 위해서는 유선 인터넷과 마찬가지로 보안 문제가 해결되어야 하지만, 아직 국제적인 표준화가 진행중이다. 유선 인터넷에서 무선 인터넷으로의 확장은 WAP 1.0인 경우 휴대 단말기와 인터넷 서버 사이에 WAP Gateway를 두고, WAP 체계와 인터넷 TCP/IP 체계 사이의 변환 역할을 수행하도록 하였다. 그러나 WAP2.0에서는 WAP Gateway를 WAP Proxy로 대신하게 하고, 클라이언트와 서버 사이의 통신은 HTTP/1.1을 사용할 수 있게 하였다.[1] 그리고 WAP proxy로 하여금 통신 프로세스를 최적화하고, 이동 서비스의 향상을 제공할 수 있도록 하였다. WAP(Wireless Application Protocol)은 이동 전화나 PDA 등 소형 무선 단말기 상에서 인터넷 데이터를 이용할 수 있도록 하는 통신 규약이다. WAP은 이동 전화나 노트북을 이용해 인터넷을 사용할 수 있는 것에서부터, 인터넷 데이터의 가공 처리, 전용 브라우저 등에 대한 내용이 포함된 WML이 있다. WAP Forum의 목표는 이동 전화나 PDA 등의 무선 단말기에 인터넷 내용과 고급 데이터 서비스를 제공하고자 한다. 또한 모든 무선 네트워크 기술에 맞는 범용 무선 프로토콜 스펙을 작성하고, 다양한 단말기, 통신 회사 망에 통용되는 내용과 어플리케이션 제작이 가능하도록 노력하고 있다. 이러한 무선 인터넷 환경에서의 정보 보호는 가장 중요한 요소 기술 중의 하나이다. 그러나 무선 인터넷의 경우는 일반 PC와는 달리 많은 제약 조건이 따르고 있다. 휴대폰이나 PDA 단말기 내부의 작은 프로세서들은 메모리 및 장치의 한계 때문에 PC와 유선 망의 암호화 및 인증을 사용하는 것은 불가능하다. 따라서 본 논문에서는 무선 인터넷에 합당한 효율적이고 안전한 암호화 프로토콜을 제안하고자 한다. 본 논문의 구성은 2장에서 여러 가지 관련 연구에 대해 조사하였으며, 3장에서는 제안하는 프로토콜을 설명하였다. 그리고 4장에서는 프로토콜 분석을 하였으며 5장은 결론 및 향후 연구에 대해 논한다.

II. 관련 연구

2.1 WAP의 개요

WAP은 무선 단말기와 네트워크 서버 사이의 통신을 가능하게 하는 표준 컴포넌트의 집합으로 정의할 수 있으며, 다음과 같은 특징을 가지고 있다.[2]

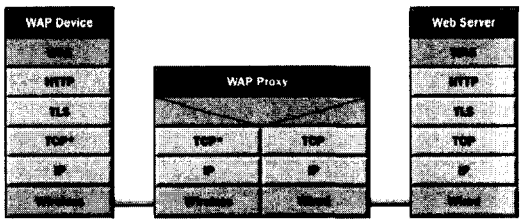
- 표준 네이밍 모델(Standard Naming Model) : 웹 표준 URL은 웹 서버 상에 있는 WAP 콘텐츠를 인식하는 데 사용되고, 또한 이것은 장치 안에 있는 지역 자원을 인식하는 데 사용된다.
- 컨텐츠 타이핑(Content Typing) : 모든 WAP 내용은 웹 타입과 호환되는 특별한 타입을 가지며, 따라서 WAP 클라이언트는 웹 타입을 기초로 하여 작성된 모든 내용을 정확하게 처리할 수 있다.
- 표준 컨텐츠 형식 : WAP 컨텐츠 형식은 웹 기술에 기초를 두고 있으며, 화면 표시용 마크업(Markup), 달력 정보, 전자 비즈니스 카드, 이미지 그리고 스크립터 언어 등을 포함한다.
- 표준 통신 프로토콜 : WAP 통신 프로토콜은 휴대 무선 장비로부터 네트워크에 연결된 웹 서버와의 통신을 가능하게 한다.



〔그림 1〕 WAP 시스템의 개요

WAP 구조는 무선 단말기를 위한 응용 프로그램 개발을 위해 확장 가능한 프로토콜 환경과 전체 네트워크의 계층화된 구조를 제공한다. WAP 구조에서 각각의 계층은 상위 계층에 의해서 접근될 수 있으며, 다른 서비스나 응용 프로그램에 의해서도 이용될 수 있다. 외부 응용 프로그램은 세션, 트랜잭션, 보안 그리고 트랜스포트 계층에 직접 접근할 수 있다. WAP 2.0의 주요 특성은 WAP 환경에서의 인터넷 프로토콜의 사용이다. 이것은 무선 네트워크가 고속이 되고, IP가 직접 무선 장치에 제공됨으로써 가능하게 되었다. Wireless Profiled HTTP(WP-HTTP)은 무선 환경에서의 HTTP이며, 완전하게 HTTP/1.1과 상호 운용 가능한 것이다. WAP 장치와 WAP proxy/WAP Server와의 상호 작용의 기본 모델은 HTTP request/response 트랜잭션이다. WP-HTTP는 응답의 전체 압축 메시지를 지원한다. Transport Layer Security(TLS) 프로토콜의 무선 윤곽은 안전한 트랜잭션을 위한 상호 작용을 하게 하는 것이다. TLS에서의 이 윤곽은 암호화, 인증 형식, 서명 알고리즘, 세션 요약 정보 등을 포함한다. 이것은 또한 트랜스포트 레벨에서의 종단간

안전을 지원하는 TLS 터널링을 위한 방법을 정의하고 있다. Wireless Profiled TCP(WP-TCP)는 연결성 지향 서비스를 제공한다. 이것은 무선 환경에서 최적화되어 있고, 인터넷의 표준 TCP 실행과 완전하게 상호 작용한다. TCP 최적화에 관한 연구는 성능을 개선하는 메커니즘의 수에 달려있다.



〔그림 2〕 WAP의 구조

2.2. ElGamal 공개키 암호 프로토콜

ElGamal 공개키 암호 시스템은 ElGamal이 Diffie-Hellman 키 분배 방식을 이용한 이산 대수 문제의 어려움에 바탕을 둔 공개키 암호 시스템이다.[3,11] Bob이 Alice에게 메시지 $(M)(1 \le M \le p-1)$을 보낸다고 가정할 때 프로토콜은 <키 생성 단계>, <암호화 단계>, <복호화 단계>로 나누어지며, 수행 절차는 다음과 같다.

• 키 생성 단계

[단계 1] Alice는 큰 임의의 소수(large random prime number) p와 Z_p^*의 생성원 g(modulo p의 원시근)을 하나 선택한다. 임의의 정수 $(x)(1 \le x \le p-1)$를 선택하고 $y = g^x \pmod p$를 계산 후 결과값 (p, y, g)을 신뢰할 수 있는 기관(TTP : Trusted Third Party)에게 전송하고 자신의 비밀키 (x)를 비밀리에 보관한다.

[단계 2] TTP는 Alice로부터 받은 결과값 (p, y, g)을 저장하고, 공개한다.

• 암호화 단계

[단계 3] Bob은 Alice의 공개키 (p, y, g)를 TTP로부터 받는다. 메시지 $(M)(M \in \{1, 2, \ldots, p-1\})$을 선택하고, 임의의 정수 $(k)(1 \le k \le p-1)$을 선택하여 $W = g^k \pmod p$와 $Z = M \cdot y^k \pmod p$을 계산하고 암호문 $(C) = (W, Z)$을 Alice에게 송신한다.

• 복호화 단계

[단계 4] Alice는 Bob으로부터 수신한 암호문 $(C) = (W, Z)$을 자신의 비밀키 (x)를 이용하여 $Q = W^{-x} \pmod p = g^{-xk} \pmod p$를 계산하고, 메시지 (M)를 다음과 같이 복호화 한다.

$$M = Q \cdot Z = g^{-xk} \cdot (M \cdot y^k) \pmod p$$
$$= g^{-xk} \cdot (Mg^x) \pmod p$$
$$= g^{-xk} \cdot Mg^{xk} \pmod p = M$$

2.3 불확정 전송 프로토콜

암호학이나 통신망 여러 분야에서의 비밀 정보 및 정당한 사용자에 대한 보호 대책을 일반적으로 모두 총칭하여 정보보호 프로토콜이라 정의하며, 이 중 암호 기술이 적용된 정보 보호 프로토콜을 암호화 프로토콜이라 정의할 수 있다. 암호화 프로토콜의 요구사항들 중에서 공평한 비밀 정보 교환 문제는 매우 중요하며, 공평한 비밀 정보 교환이란 여러 사람이 각각 자신이 가지고 있는 비밀 정보를 공평하게 교환할 수 있도록 하는 프로토콜이다.[4,13] 예를 들어 서로 신뢰하지 않는 두 당사자간에 전자 계약이나 합의 문서에 서명을 할 때 어느 한 쪽이 먼저 서명을 하여 보냄으로써 발생할 수 있는 문제점이 많다. 이러한 문제점을 해결하기 위하여 공평한 비밀 정보 교환을 위한 불확정 전송(Oblivious Transfer : OT) 프로토콜에 대한 연구가 요구되고 있다. 불확정 전송 프로토콜은 일반적으로 암호화 프로토콜을 설계하기 위한 기본적인 도구로서 유용하게 사용되는 서브 프로토콜이다. OT는 Rabin에 의해 소개되었으며, 일반적으로 OT 프로토콜은 두 참여자에게 적용되는 프로토콜로서 사용자 B는 사용자 A에 의해 전송된 두 개의 메시지 중에서 오직 하나의 메시지만을 선택할 수 있다[5]. 더불어 사용자 A는 사용자 B가 어느 메시지를 선택하였는가를 알지 못하게 된다. 이것은 사용자 B가 임의의 메시지를 선택할 확률이 1/2이 됨을 의미하는 것이며, OT_2^1로 표기된다.[6~8]

불확정 전송 프로토콜을 적용할 비밀 정보의 수에 따라 분류하면 적용할 비밀 정보의 수가 한 개인 경우의 일반 불확정 전송 프로토콜, 적용할 비밀 정보의 수가 두 개의 경우의 1-out-of-2 불확정 전송 프로토콜, 적용할 비밀 정보의 수가 n개의 경우의 1-out-of-n 불확정 전송 프로토콜, 적용할 비밀 정보의 수가 n개의 비밀 정보 중 (n-1)개의 비밀 정보만을 불확정 전송할 경우의 (n-1)-out-of-n 불확정 전송 프로

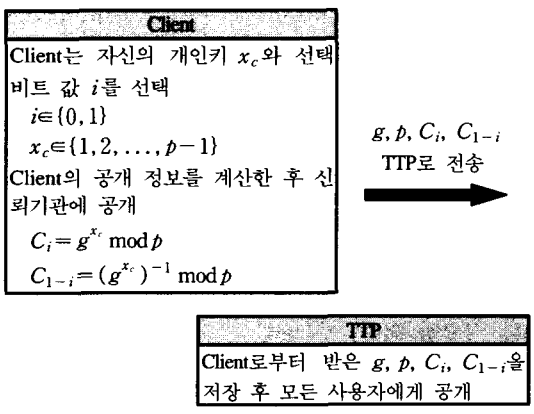
토콜로 분류할 수 있다.

불확정 전송 프로토콜을 비밀 정보 교환 방식에 따라 분류하면 프로토콜의 형태가 대화 형식으로 진행되며 송수신자간에 자신의 비밀 정보에 대하여 몇 번의 상호 교환을 통해 이루어지는 대화형 불확정 전송 프로토콜(Interactive OT : IOT)프로토콜과 송신자에 의한 수신자로의 일방향 통신만이 존재하는 프로토콜로써 송수신자간에 통신 횟수가 급격히 감소하기 때문에 실제 응용시 불확정 전송 프로토콜에 의한 통신로 상의 과부하(overhead)를 줄일 수 있는 비대화형 불확정 전송(Non-Interactive OT : NIOT) 프로토콜로 분류할 수 있다.

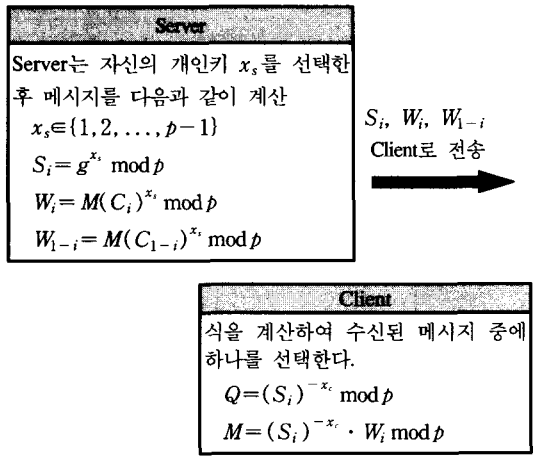
2.3.1 비대화형 OT_2^1 프로토콜

소수 $p \in Z_p^*$, Z_p^*의 생성원 g일 때, [그림 3]과 [그림 4]는 비대화형 OT_2^1 프로토콜을 나타낸 것이다. [그림 3]에서 i는 클라이언트의 선택 비트(selection bit)이고, x_c는 클라이언트의 개인키(private key)이다.

[그림 3]의 프로토콜을 수행하기 전에 클라이언트는 우선 선택 비트 $i \in \{0,1\}$를 결정하고, 자신의 개인키로 사용될 $x_c \in \{1,2,\ldots,p-1\}$를 임의로 선택한다. 그런 이후 클라이언트의 공개 정보를 계산하여 신뢰 기관에 정보를 제공함으로써, 모든 사용자에게 이 정보를 공개한다. 서버는 신뢰 기관에 공개된 정보를 이용하여 [그림 4]와 같이 보내고자 하는 정보를 계산한다. x_s는 서버의 개인키이며, 이것을 이용하여 보내고자 하는 메시지들을 계산한다. 서버는 [그림 4]에 나타난 과정을 계산하고, 클라이언트로 S_i, W_i, W_{1-i}을 전송한다. 클라이언트는 수신된 S_i, W_i, W_{1-i}와 자신만이 비밀스럽게 유지한 개인키 x_c을 통해 M를 계산할 수 있다.



〔그림 3〕 공개키 전송 단계



〔그림 4〕 메시지 전송 단계

이 경우 불확정 전송의 특성에 따라 클라이언트가 비밀 정보를 정확하게 알게 될 확률이 1/2이고, 비밀 정보에 대한 아무런 정보를 얻을 수 없는 확률이 1/2이다. 이 프로토콜은 g^x와 g^y가 주어지더라도, x와 y가 주어지지 않으면 g^{xy}를 계산하기 어렵다는 Diffie-Hellman 문제에 바탕을 두고 있고 또한 Goldreich-Leven 이론을 이용한 것이다.[9]

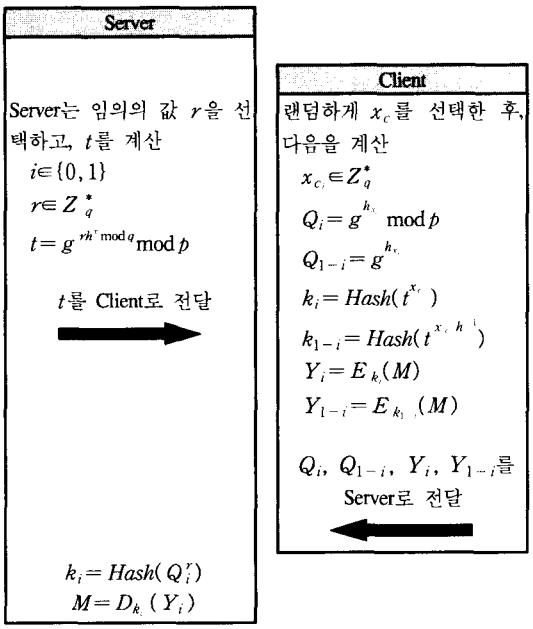
2.3.2 대화형 프로토콜 OT_2^1 프로토콜

대화형 1-out-of-2 OT도 역시 서버가 클라이언트에 의해 보내진 두 메시지 중에 하나를 선택하는 프로토콜로서 수신자는 오직 하나의 메시지만을 선택할 수 있으며, 송신자는 수신자가 어떤 메시지를 선택하였는지를 알 수 없다. 대화형 프로토콜 OT_2^1 프로토콜은 S.Even과 M. Stadler에 기본을 두고 있다.

[그림 5]의 대화형 OT_2^1는 서버가 p, q값을 만들어서 공개함으로써 서버와 클라이언트가 동일하게 p, q값을 알고 있다.[10,14]

그리고 암호화 함수 E_k와 복호화 함수 D_k를 이용하여 각각 암호와 복호를 하여 메시지 전송이 됨을 의미한다. 서버는 r, i값을 선택한 후, $t = g^{r h' \bmod q} \bmod p$를 계산하여 클라이언트에게 전송한다. 클라이언트에서는 x_c를 임의로 선택한 후 Q_i, Q_{1-i}, k_i, k_{1-i}, Y_i, Y_{1-i}를 계산한다. 그리고 Q_i, Q_{1-i}, Y_i, Y_{1-i}을 서버로 전달함으로써 키 교환이 이루어진다[12].

이 프로토콜의 안전성은 역시 Diffie-Hellman 문제에 바탕을 둔다. 기존 논문[14]의 경우 대화형 프로토콜에서 이중지수승을 이용하고 있기 때문에 일방향 함수를 이용함에도 불구하고 통신량이 증가됨을 알



〔그림 5〕 대화형 OT 프로토콜

수 있다. 본 논문에서는 이러한 단점을 보안하고자 하였다.

Ⅲ. 제안한 프로토콜

본 논문에서는 다음과 같은 두 공개 그룹을 사용한다. r이 큰 소수(large prime number)라고 할 때, $q = 2r+1$과 $p = kq+1$도 역시 소수가 되는 r, k가 존재한다. 이것은 T.Okamoto에 의해 이와 같은 소수들을 어렵지 않게 찾을 수 있음을 보였다[9]. $h \in Z_q^*$는 order r의 원소이고, H는 h에 의해 생성된 multiplicative 그룹이라고 하고, 또한 $g \in Z_p^*$는 order q의 원소이고, G는 g에 의해 생성된 multiplicative 그룹이라고 할 때, 다음과 같은 형태의 식을 갖는다.

$$h^r \equiv 1 \bmod q,\ g^q \equiv 1 \bmod p$$

여기서 밑수(base) h와 g의 이산 대수를 계산하는 것은 불가능하다고 가정한다. 본 논문에서는 이중지수승(double exponentiation)을 이용하여 비대화형 불확정 전송 프로토콜을 설계하고자 한다. 이 기법은 밑수 h와 g의 이중지수승을 통해 $x \in Z_r$에서 y로 대응됨을 의미한다.

$$y = (g^{h^x \bmod q}) \bmod p$$

본 논문에서 사용된 기호는 다음과 같은 의미를 갖는다.

WS : Web server의 공개 정보
x_s : Web Server의 비밀키
x_c : WAP Client의 비밀키
M : 암호화하는 메시지
WC : WAP Client의 공개 정보

제안된 프로토콜의 동작은 다음과 같다.

[1단계]

우선 Web Server는 개인키 x_s와 선택비트 $i \in \{0,1\}$를 선택한다. $x_s \in \{1,2,...,p\text{-}1\}$이고, p는 큰 소수(large prime number)이다.

[2단계]

Web Server는 자신의 개인키 x_s로 이중지수승을 이용하여 Web Server의 공개 정보인

$$\left\{ \begin{array}{l} WS_i = (g^{h^{x_s} \bmod q}) \bmod p \\ WS_{1-i} = (g^{-h^{x_s} \bmod q}) \bmod p \end{array} \right\}$$

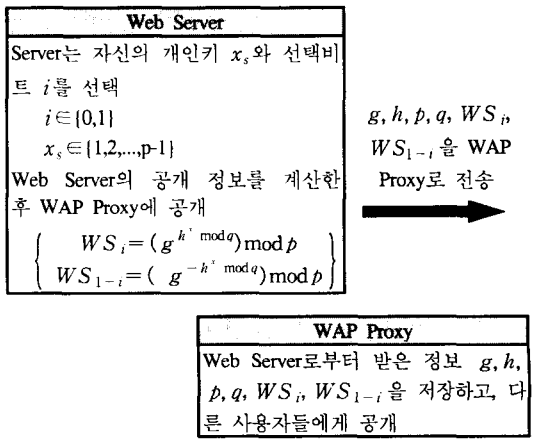
을 계산한다.

[3단계]

$g, h, p, q, WS_i, WS_{1-i}$을 WAP Proxy로 전송한다.

[4단계]

WAP Proxy는 Web Server로부터 받은 정보 $g, h, p, q, WS_i, WS_{1-i}$을 저장하고, 다른 사용자들에게 공개한다.



〔그림 6〕 웹 서버의 공개 정보

[5단계]

WAP Client는 자신의 개인키 x_c와 전달한 메시지 M을 다음과 같이 계산한다.

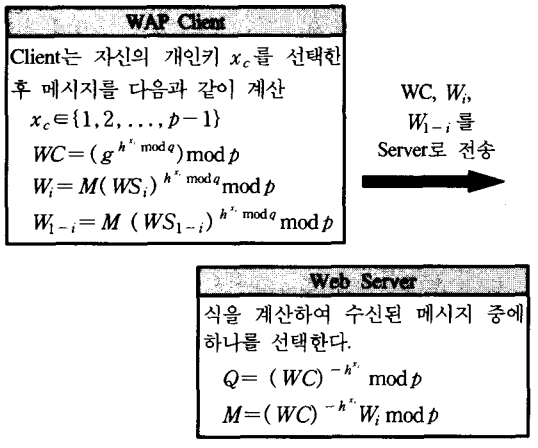
$$x_c \in \{1,2,\ldots,p-1\}$$
$$WC = (g^{h^{x_c} \bmod q}) \bmod p$$
$$W_i = M\,(WS_i)^{h^{x_c} \bmod q} \bmod p$$
$$W_{1-i} = M\,(WS_{1-i})^{h^{x_c} \bmod q} \bmod p$$

[6단계]

WAP Client 는 WC, W_i, W_{1-i}를 Web Server에게 보낸다.

[7단계]

Web Server는 메시지를 획득하기 위해 $Q=(WC)^{-h^{x_c}} \bmod p$로 정의한 후, 수신된 정보를 이용하여 Q와 $M=(WC)^{-h^{x_c}} W_i \bmod p$을 계산함으로써 WAP Client가 보낸 메시지를 얻을 수 있다.



〔그림 7〕 웹 서버의 메시지 전송 과정

Ⅳ. 프로토콜 분석

4.1 메시지 처리 과정

이 논문에서 설계한 프로토콜은 Web Server가 생성한 개인키로 h와 g의 이중지수승을 이용하여 서버의 정보를 계산한다. 그리고 WAP Proxy에 공개한다. WAP Client는 W_i, W_{1-i}를 계산하여 Web Server로 보내게 된다. Web Server는 자신이 가지고 있는 정보를 이용하여 원하는 메시지를 얻을 수 있다. 여기서 Web Server는 챌린지 선택 비트(challenge selection bit) $i \in \{0,1\}$를 선택하게 되고, 이 경우 서버는 $i \in \{0,1\}$의 두 가지 경우에 대해서만 메시지를 복호화 하게 된다. 따라서 정확한 메시지를 받을 수 있는 확률은 1/2이다. 또한 WAP Client가 Web Server에게 WC, W_i, W_{1-i}의 정보만을 전송하게 되고, Web Server는 WAP Client에게 아무런 정보를 전달하지 않기 때문에 비대화형 불확정 전송이다.

정리1)

만약 WAP Client가 WC, W_i, W_{1-i}의 정보를 전달하면 Web Server는 메시지 M을 얻을 수 있다.

증명)

Web Server가 WAP Client로부터 받은 정보는 다음과 같다.

$$WC=(g^{h^{x_c} \bmod q}) \bmod p$$
$$W_i=M\,(WS_i)^{h^{x_c} \bmod q} \bmod p$$
$$W_{1-i}=M\,(WS_{1-i})^{h^{x_c} \bmod q} \bmod p$$

그리고 Q를 다음과 같이 계산할 수 있다.

$$Q=(WC)^{-h^{x_c}} \bmod p$$

이것을 이용하여 서버는 자신이 가지고 있는 정보를 이용하여 다음과 같이 얻을 수 있다.

$$\begin{aligned} M &= Q \cdot W_i \bmod p \\ &= (WC)^{-h^{x_c}} W_i \bmod p \\ &= (WC)^{-h^{x_c}} M\,(WS_i)^{h^{x_c} \bmod q} \bmod p \\ &= g^{(h^{x_c}-h^{x_c}) \bmod q} M\, g^{h^{x_c} h^{x_c} \bmod q} \bmod p \\ &= M \end{aligned}$$

위와 같이 전달하고자 하는 메시지 M을 얻을 수 있다. ■

4.2 프로토콜의 비교

기존의 대화형 불확정 전송, 비대화형 불확정 전송 방식과 이중지수승을 이용한 ElGamal 기반의 비대화형 불확정 전송 방식을 비교하면 [표 1]과 같다.

본 논문에서 제안하는 프로토콜은 ElGamal 공개키 암호 방식의 이산대수 문제의 어려움에 근거하므

〔표 1〕 IOT, NIOT와 이중 지수승의 NIOT 전송 방식 비교

비교내용	IOT	일반적 NIOT	이중지수승의 NIOT
프로토콜 수행시 메시지 노출 가능성	X	X	X
송수신자 부정행위 가능성	O	O	O
부정 행위 탐지 기능	X	X	O
송신 사실 추후부인 해결 가능성	X	X	많음
수신 사실 추후부인 해결 가능성	X	X	X
통신량	많음	적음	적음
안전성, 효율성	낮음	낮음	높음

로 주어진 공개키로 비밀키를 아는 것은 불가능하다. 따라서 메시지 노출 가능성을 해결하였다. 또한 본 논문에서 제안한 ElGamal 기반의 비대화형 불확정 전송프로토콜은 WAP Proxy가 비밀키를 보유하지 않으므로 WAP Proxy와 제 3자간의 부정행위 가능성을 사전에 제거하였으며[14], WAP Server는 WAP Client의 부정 행위를 사전에 탐지할 수 있다.[3]

또한 제안된 프로토콜은 불확정 전송 프로토콜이므로 서버와 클라이언트간의 통신량을 줄일 수 있고, 챌린지 선택 비트(challenge selection bit)를 사용하여 클라이언트가 서버에 인증되는 확률을 줄임으로서 프로토콜의 효율성을 높였다. 그리고 송신 사실 추후 부인 해결을 위해서는 메시지 송신시 송신자의 정보를 추가하여 전송함으로써 일반적인 불확정 전송 프로토콜에서 해결하지 못한 점을 해결하고자 하였다.

프로토콜의 이론적 안전도는 시스템의 기반이 되는 수학적 문제를 얼마나 많이 푸는 것을 요구되는가를 분석하는 것이다. 본 논문에서 제안하는 프로토콜은 ElGamal 기반의 비대화형 불확정 전송 방식을 사용하고 있으므로 이것의 안전성은 이산 대수 문제의 어려움에 기인한다. 또한 이중지수승을 사용하고, 비대화형의 불확정 전송 프로토콜을 사용함으로써 WAP Server가 WAP Client를 인증하여 메시지를 복원하는 확률은 1/2로 낮아진다. 이것은 기존의 이산 대수나 소인수문제보다 어렵다는 것을 의미하므로 프로토콜의 안정성을 높이는 역할을 한다.

V. 결 론

본 논문에서는 무선 인터넷 통신에서 사용 될 수 있는 통신량이 적을 뿐만 아니라 신뢰 기관이 비밀키를 보유함으로 인해서 발생하는 문제점을 해결할 수 있는 새로운 프로토콜을 제안하였다. 이 프로토콜은 비대화형 불확정 전송 프로토콜로서 기존의 안전도가 검증된 ElGamal 공개키 알고리즘[8][11]을 기반으로 하였다. 제안된 프로토콜은 불확정 전송 프로토콜이므로 서버와 클라이언트간의 통신량을 줄일 수 있고, 챌린지 선택 비트(challenge selection bit)를 사용하여 클라이언트가 서버에 인증되는 확률을 줄임으로서 프로토콜의 효율성을 높였다. 또한 이중지수승(double exponentiation)을 사용하여 기존의 이산대수나 소인수문제보다 어렵다는 것을 의미하므로 프로토콜의 안정성을 높일 수 있다. 현재 무선 인터넷 통신 프로토콜은 여러 가지 방향으로 표준화가 진행중이므로 본 연구가 여러 가지 대안 중의 하나로 제시될 수 있으리라 본다. 또한 본 프로토콜을 이용한 다양한 컨텐츠 개발에 관한 연구가 요구된다.

참 고 문 헌

[1] WAP Forum, Wireless Application Protocol Technical White paper, January 2002

[2] Weekly Electronics Information. Vol. 3. No. 36, 2000. 10.

[3] T. ElGamal, A Public key Cryptosystem and Signature Scheme Based on Discrete Logarithm, IEEE Trans. Information Theory, Vol. 31, No. 44, pp. 469~472, 1985.

[4] M. Blum, How to Exchange Secret Keys, ACM Trans. Compute System, pp. 175~193, May 1983.

[5] M. O. Rabin, How to Exchange secrets by oblivious transfer, Technical Report Tech. Memo TR-81, aiken Computation Labs, Harvard Univ, 1981.

[6] Goldreich and L. A. Levin, A hard-core predicate for all one-way functions, In proceeding of the twenty first Annual ACM Symposium on theory of Computing, p. 25~32, Seattle, Washington, May 1989.

[7] M. Bellare, R. Canetti, and H. Krawczyk, A modular approach to the design and analysis of authentication an key exchange protocol, In Crypto '89. pp. 547~557.

[8] M. Blum, Coin Flipping by Telephone, IEEE, COMPCON, pp. 133~137, September 1982.

[9] S. Even, O.Goldreich, A. Lempel, A Randomized Protocol for Signing Contracts, Communications of the ACM, pp. 637~647, 1985.

[10] T. Okamoto, Threshold key recovery system for RSA, In Proceedings of 1997 Security protocol Workshop. Paris, April 1997.

[11] T. El-Gamal, A Public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory, Vol. IT-31, pp. 469~472, 1985.

[12] M. Stadler, J. M. Piveteau, and J. Camenisch, Fair Blind Signatures, Advances in Cryptology-EUROCRYPT '95, Lecture notes in Computer Science v.921, pp. 209~219, Springer Verlag, 1995.

[13] 박영호, 박호상, 정수환, ECDSA를 적용한 ID 기반의 사용자 인증 및 키 교환 프로토콜, 정보보호학회 논문지, Vol. 12, No. 1, 2002.

[14] 현상우, 류종호, 염홍렬, 불확정 전송을 이용한 패스워드 기반 인증 프로토콜, CISC2000, 2000.11.

〈著者紹介〉

정 경 숙 (Kyoung-sook Jung)
1995년 2월 : 경희대학교 수학과 졸업
1997년 8월 : 경희대학교 컴퓨터공학과 석사
1999년 3월~현재 : 경희대학교 컴퓨터공학과 박사수료
<관심분야> 인공지능, 정보보호, 전자상거래, 기계학습

홍 석 미 (Seok-mi Hong)
1994년 2월 : 상지대학교 전자계산공학과 졸업
1997년 2월 : 경희대학교 컴퓨터공학과 석사
1998년 3월~현재 : 경희대학교 컴퓨터공학과 박사수료
<관심분야> 인공지능, 기계학습, 멀티 에이전트, 정보보호

정 태 충 (Tae-choong Chung)
1980년 2월 : 서울대학교 전자공학과 졸업
1982년 2월 : 한국과학기술원 전자계산공학과 석사
1987년 2월 : 한국과학기술원 전자계산공학과 박사
1987년 9월~1988년 3월 : KIST 시스템 공학센터 선임 연구원
1988년 3월~현재 : 경희대학교 컴퓨터공학과 정교수
<관심분야> 인공지능, 자연어처리, 로봇 에이전트, 정보보호