情報保護學會論文誌
第17卷 第5號, 2007. 10

완전한 전방향 안전성을 제공하는 실용적인 전자우편 프로토콜*

이 창 용,[1†] 김 대 영,[2] 심 동 호,[3] 김 상 진,[4] 오 희 국[1‡]
[1]한양대학교, [2](주)엠파스, [3](주)누리비젼, [4]한국기술교육대학교

Practical Secure E-mail Protocols Providing Perfect Forward Secrecy

Changyong Lee,[1†] Daeyoung Kim,[2] Dongho Shim,[3] Sangjin Kim,[4] Heekuck Oh[1‡]
[1]Hanyang University, [2]Empas Co.,Ltd., [3]Nurivision Co.,Ltd., [2]Korea University of Technology and Education

요 약

전자우편을 사용할 때 고려해야 하는 중요한 보안 이슈 중 하나는 사용자 프라이버시이다. 현재 PGP(Pretty Good Privacy), S/MIME(Secure/Multipurpose Internet Mail Extension) 등의 여러 가지 전자우편 보안 프로토콜이 제안되어 사용되고 있으나, 이들 프로토콜은 안전성을 향상시킬 수 있는 요구사항인 전방향 안전성을 보장하지 못한다. 최근 이 특성을 만족하기 위한 전자우편 프로토콜들이 제안되었으나 실용성과 효율성 측면에서 개선이 필요하고, 일부 프로토콜은 실질적으로 완전한 전방향 안전성을 제공하고 있지 못하다. 이 논문에서는 실용성을 갖춘 효율적인 전자우편 보안 프로토콜을 제안한다. 제안하는 프로토콜은 기존의 전자우편 시스템에 영향을 주지 않는 실용적인 모델을 사용하며, 타원곡선 기반의 signcryption 기법을 사용하여 효율적으로 메시지를 인증한다. 추가적으로, 다수의 사람에게 전자우편을 전송할 때에도 적용할 수 있다는 장점이 있다.

ABSTRACT

One of the most important security issues of e-mail service is user privacy. Currently, various security protocols, like PGP(Pretty Good Privacy), S/MIME(Secure/Multipurpose Internet Mail Extension), have been proposed. These protocols, however, do not provide forward secrecy. Recently, some security protocols that provide forward secrecy were proposed. But all of them require changes to the current e-mail infrastructure. Moreover, contrary to authors' intention, some of them do not actually provide perfect forward secrecy. In this paper, we propose a new practical e-mail security protocol. The proposed protocol provides perfect forward secrecy and uses a practical e-mail model that dose not require any changes to existing e-mail servers. It encrypts and authenticates messages efficiently using elliptic curve based signcryption scheme. In addition, we provide a way to send secure group e-mails.

Keywords : *E-mail, Forward Secrecy, Privacy*

접수일: 2007년 4월 02일; 채택일: 2007년 9월 05일
* 본 연구는 한국기술교육대학교 교수현장연구학기제의 지원으로 수행된 과제임
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성, 지원사업의 연구결과로 수행되었음
† 주저자, chylee@infosec.hanyang.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr

Ⅰ. 서 론

정보통신 사회에서 전자우편은 가장 널리 사용되고 있는 인터넷 서비스이다. 이에 따라 전자우편의 역할 또한 개인 간 기본 통신 수단에서 벗어나 기업 간 혹은 개

인 간의 중요한 정보 교환의 수단으로 발전되었다. 또한 전자우편이 정보 데이터베이스로 활용되고, 금융 결제, 전자 상거래에서 필수 요소로 사용됨에 따라 전자우편 보안에 대한 요구가 증대되고 있다. 하지만 전자우편의 사용자들은 보안에 대한 인식이 매우 낮아 중요한 기밀 데이터나 개인적 내용의 전자우편을 평문 상태로 교환하는 경우가 많다. 가장 기본적인 전자우편 프로토콜인 SMTP(Simple Mail Transfer Protocol)[1]의 경우 송신자에 대한 인증이 배제되어 있고, 수신자에게 단순히 평문을 전달하는 등 아무런 보안 서비스를 제공하지 않는다.

이를 보완하기 위해 전자우편 보안 프로토콜들이 제안되었고 대표적으로 PGP[2]와 S/MIME[3]가 사용되고 있다. 이들 기법에서 송신자는 전자우편을 전송할 때마다 새로운 세션키를 생성하고 이 키로 메시지를 암호화한다. 그리고 미리 확보해 둔 수신자의 공개키로 세션키를 암호화하여 수신자에게 암호화된 메시지와 함께 전달하는 방식을 사용한다. 이와 같은 방법으로 송신자는 제3자에게 전자우편의 내용을 노출시키지 않고 안전하게 전자우편을 수신자에게 송신할 수 있다. 하지만 이 기법들은 모두 전방향 안전성을 제공하지 못한다. 만약 공격자가 이전에 교환된 모든 메시지를 저장하고 있고, 장기간 사용되는 수신자의 개인키를 알아낸다면 이전에 사용되었던 모든 세션키를 알 수 있다. 결국 이전에 교환된 모든 전자우편의 내용이 공격자에게 그대로 노출된다. Open PGP의 전방향 확장 명세[4]에서 이러한 점을 보완하여 전방향 안전성을 제공하는 PGP 프로토콜을 제안했지만, 이는 수신자의 개인키 수명을 짧게 설정하여 자주 바꾸어 주는 방식으로 비용 측면에서 비효율적이다.

전방향 안전성이란 송/수신자의 장기간 암호키가 노출되더라도 이전에 사용된 세션키들이 노출되지 않아야 하는 보안 요구조건을 말하는 것으로, 크게 부분 전방향 안전성과 완전한 전방향 안전성으로 구분된다. 부분 전방향 안전성은 일부 참여자의 장기간 키가 노출되어도 전방향 안전성이 보장되지만, 다른 일부 참여자의 장기간 키가 노출되었을 때는 전방향 안전성을 만족하지 못하는 수준을 가리킨다. 완전한 전방향 안전성은 모든 참여자의 장기간 키가 노출되어도 전방향 안전성이 보장되는 경우를 말한다.

지금까지 전방향 안전성을 보장하는 많은 키 확립 프로토콜이 제안되었지만 전자우편 프로토콜은 상태를 유지해야 하는 프로토콜이 아니며, 송신자와 수신자가 직접 통신을 하지 않는 프로토콜이다. 따라서 기존 암호프로토콜들을 그대로 전자우편에 적용할 수 없다.

이와 관련하여 전방향 안전성을 보장하기 위한 전자우편 프로토콜들이 제안되었다. 2005년에 Sun 등이 완전한 전방향 안전성을 보장하는 전자우편 프로토콜을 두 가지 제안하였지만, 완전한 전방향 안전성을 보장하지 못하거나, 전자우편 송/수신을 위해 특수한 하드웨어를 필요로 하는 문제점이 있었다[5]. 이를 개선하여 같은 해 김범한 등이 제안한 프로토콜은 특수한 하드웨어 휴대의 문제점은 해결했지만 지수 연산을 많이 필요로 하여 효율성 측면에서 문제점이 있었고, 저자의 주장과 달리 완전한 전방향 안전성을 보장하지 못했다[6]. 또한 이 프로토콜들은 송신자와 수신자의 전자우편 서버를 동일한 서버로 가정하여 그 실용성이 떨어지는 문제점을 가지고 있다.

이 논문에서는 다음 사항들을 충족하는 전자우편 서비스를 위한 키 동의 프로토콜을 제안한다.

- 전자우편의 특수한 환경을 고려한다. : 송/수신자는 동시에 온라인 상태에서 프로토콜을 수행할 수 없으며, 같은 서버를 사용하지 않는다.
- 전자우편의 송/수신 과정에서 완전한 전방향 안전성이 보장되어야 한다.
- 수신자는 송신자를 인증할 수 있어야 한다.

제안하는 프로토콜은 기존 전자우편 송/수신 서버와 독립적인 신뢰 서버를 추가하여 기존의 전자우편 시스템과 높은 호환성을 가지는 모델을 사용한다. 이 모델에서는 송신자만 신뢰 서버에 가입되어 있으면 수신자의 가입여부와 상관없이 안전한 전자우편 전송이 가능하다. 또한 DH(Diffie-Hellman) 키 동의 기법을 활용하여 전송되는 전자우편에 대해 완전한 전방향 안전성을 보장한다. 그리고 타원곡선 기반의 signcryption 기법[8]을 적용하여 효율적으로 메시지의 암호화와 송신자 인증을 수행한다. 제안하는 프로토콜은 일대일의 전자우편 전송뿐 아니라 한 명의 송신자가 다수의 수신자에게 전자우편을 전송할 때에도 적용이 가능하다는 장점이 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 제안된 전자우편 보안 프로토콜에 대해 살펴보고 제안하는 프로토콜의 수학적 배경을 설명한다. 3장에서는 제안하는 프로토콜에 대해 자세히 기술하고, 4장에서는 제안하는 프로토콜의 안전성을 분석한다. 5장에서는 결론과 향후 연구를 제시한다.

Ⅱ. 연구배경

2.1. 표기법

이 논문에서는 〔표 1〕에 기술된 표기법을 사용한다.

〔표 1〕 표기법

표 기	의 미
A, B	송/수신자
S	사용자의 전자우편 서버
T	신뢰 서버
q	충분히 큰 소수
G	위수가 q인 타원곡선의 덧셈군
Z_q^*	q를 법으로 하는 곱셈군
P	G의 랜덤한 생성자
a, b	Z_q^*의 랜덤한 원소
K	대칭키
$+K_X, -K_X$	X의 개인키와 공개키
$\{M\}_K$	키 K를 이용한 메시지 M의 암호화
$MAC_K(M)$	키 K를 이용한 메시지 M에 대한 MAC값
$Sig_K(M)$	키 K를 이용한 메시지 M에 대한 서명

2.2. 수학적 배경

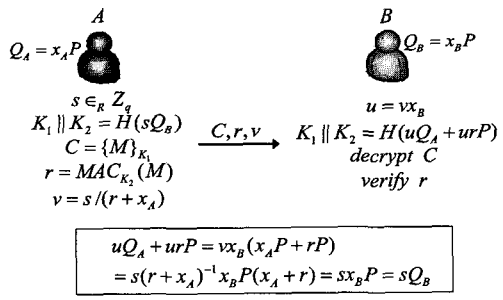
본 절에서는 제안하는 프로토콜의 바탕이 되는 수학적 배경에 대해 알아본다.

정의 1 〔이산대수 문제(DLP, Discrete Logarithm Problem)〕. 군 G의 원소 P와 aP가 주어졌을 때, a를 계산하는 문제를 말한다.

정의 2 〔계산적 Diffie-Hellman 문제 (CDHP, Computational Diffie-Hellman Problem)〕. 군 G의 원소 P, aP, bP가 주어졌을 때, abP를 계산하는 문제를 말한다.

현재까지 DLP, CDHP를 다항시간 내에 계산하는 것은 계산적으로 어렵다고 알려져 있다. 이 논문에서 제안하는 프로토콜의 안전성은 위의 문제들을 다항시간 내에 계산하는 것이 어렵다는 가정에 기반하고 있다.

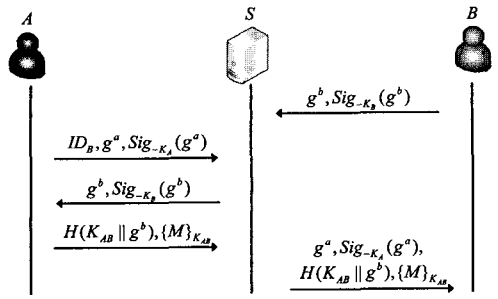
제안되는 프로토콜은 Zheng과 Imai가 제안한 타원곡선 기반의 signcryption 기법[8]을 사용하여 메시지 암호화와 인증을 수행한다. Signcryption 기법은 공개키를 이용한 서명과 암호화를 각각 별도로 하는 것보다 상대적으로 적은 비용으로 암호화와 서명을 동시에 수행할 수 있도록 해준다. 서명자는 자신의 개인키와 수신자의 공개키를 사용하여 메시지를 서명, 암호화하며, 이 과정을 signcryption이라 한다. 확인자는 자신의 개인키와 서명자의 공개키로 메시지를 복호화하며, 이 과정을 unsigncryption이라 한다. 제안되는 프로토콜은 서명자와 확인자의 개인키를 모르는 상태에서 signcryption을 공격하는 것은 수학적으로 어렵다는 가정에 기반하고 있다. 〔그림 1〕은 Zheng과 Imai의 signcryption 과정을 보여준다. 여기서 서명자 A는 자신의 개인키 x_A와 확인자 B의 공개키 Q_B를 이용하여 메시지 M에 대한 signcryptioon을 수행하며, 그 결과 $<C, r, v>$를 얻는다.



〔그림 1〕 Zheng과 Imai의 signcryption 기법

2.3. 관련 연구

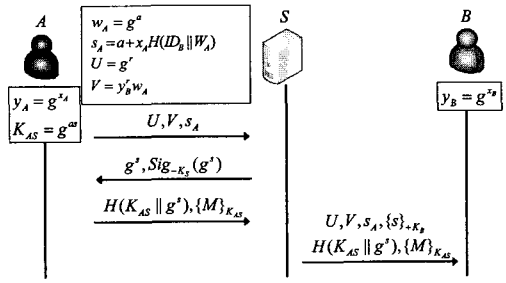
Sun 등은 2005년 전방향 안전성을 제공하는 두 종류의 전자우편 보안 프로토콜을 제안하였다. 첫 번째는 스마트카드를 이용하는 프로토콜로 〔그림 2〕와 같다. 이 프로토콜은 전자우편 메시지의 전방향 안전성 보장을 위해 DH 키 동의 기법을 사용한다. 수신자는 DH 키 동의를 위한 일회용 공개키를 미리 서버에 전송해 놓는다. 송신자는 전자우편을 전송하고자 할 때 서버에 자신의 일회용 공개키를 전송하고 서버로부터 수신자의 일회용 공개키를 전송 받아 세션키를 생성한다. 송신자는 생성된 세션키를 사용하여 전자우편을 수신자에게 전달한다. 수신자는 서버로부터 전자우편을 수신할 때 송신자의 일회용 공개키를 함께 전송 받아 송신자와 동일한 방법으로 세션키를 생성하고, 이 세션키를 사용하여 전자우편을 복호화한다. 이 프로토콜에서 송/수신자는 DH 키 동의 기법을 사용하여 생성한 세션키로 메시지를 암호화하므로 장기간 개인키가 노출되어도 세션키를 계산할 수 없다. 즉, 전자우편의 전방향 안전성이 보장



〔그림 2〕 Sun 등이 제안한 스마트 카드를 사용한 안전한 전자우편 프로토콜

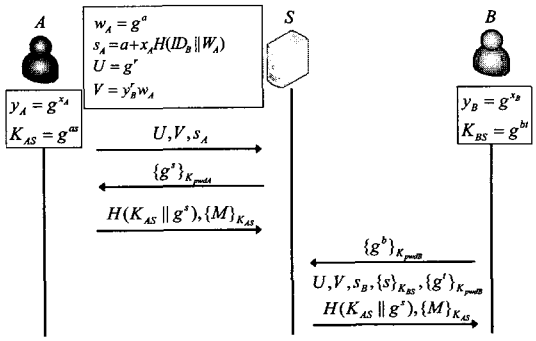
된다. 이 프로토콜을 수행하기 위해서는 수신자는 자신이 생성한 $<b, g^b>$쌍을 안전하게 보관하고 있어야하고, 항상 특정한 컴퓨터에서 전자우편을 수신하는 것이 아니라면 이 값들을 안전하게 휴대할 수 있어야 한다. 이에 따라 수신자는 전자우편의 수신을 위해 스마트카드를 사용해야 한다. 게다가, 이 프로토콜은 이메일의 송신자와 수신자가 동일한 전자우편 서버를 사용한다는 가정 하에 제안되었다. 결국, 수신자가 항상 특수한 하드웨어를 휴대해야 한다는 점과, 송/수신자가 동일한 서버를 사용한다는 가정은 비현실적인 것이어서 실용성 측면에서 문제가 있다.

Sun 등의 두 번째 프로토콜은 스마트카드를 사용하지 않는 프로토콜로 〔그림 3〕과 같다. 이 프로토콜에서 $<w_A, s_A>$쌍은 ID_A에 대한 송신자의 Schnorr 전자서명이며, $<U, V>$쌍은 수신자의 공개키를 이용한 ElGamal 암호이다. 저자는 수신자가 미리 일회용 공개키를 서버에 전송하고 휴대하여야 하는 문제점 해결을 위해 전자우편 서버가 수신자 대신 일회용 공개키를 생성하여 송신자에게 전달하도록 하였다. 하지만 서버가 자신이 생성한 일회용 공개키로 메시지의 내용을 열어볼 수 있으므로 송신자가 선택한 일회용 공개키는 서버에게 전달하지 않고 수신자의 공개키로 암호화하여 전달함으로써 서버가 그 내용을 볼 수 없게 하였다. 그러나 Dent는 이 프로토콜에서 $<w_A, s_A>$를 계산하는 방식의 문제점과 결정적으로 완전한 전방향 안전성이 보장되지 않는다는 문제점을 지적하였다[7]. 송신자의 장기간 개인키의 노출은 이전 메시지의 복호화에 영향을 주지 않지만 수신자의 장기간 개인키가 노출되면 서버가 선택한 s를 얻을 수 있고, ElGamal 암호를 복호화하여 송신자의 일회용 공개키를 얻을 수 있다. 즉, 수신자의 장기간 키가 노출되면 이전 메시지의 내용이 모두 노출되는 문제점을 가지고 있다. 따라서 이를 해결하기 위해서는 B가 DH 일회용 공개키를 만들어 서버에 전달해야 하며, 서버는 이를 이용하여 전방향 안전성이 보장되는 키를 확립하고 이 키를 이용하여 s를 암호화하여 B에게 전달해야 한다.



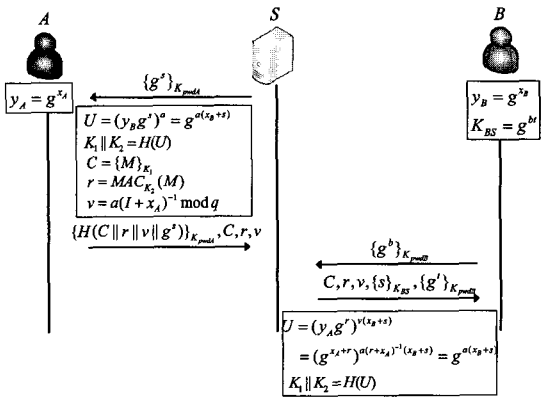
〔그림 3〕 Sun 등이 제안한 스마트 카드가 필요없는 안전한 전자우편 프로토콜

김범한 등은 Sun 등의 프로토콜의 문제점을 해결한 전자우편 보안 프로토콜을 두 가지 제안하였다[6]. 첫 번째 프로토콜은 〔그림 4〕와 같다. 이 프로토콜에서 송신자와 수신자는 각각 전자우편 서버와 패스워드 $pwdA$, $pwdB$를 공유한다. 송/수신자는 이 패스워드를 이용하여 일회용 공개키를 암호화하고 이를 전자우편 서버와 안전하게 교환하여 DH 키 동의 프로토콜을 수행한다. 이 프로토콜은 송신자와 수신자가 모두 전자우편 서버와 DH 키 동의 프로토콜을 수행하여 전방향 안전성을 보장하고 있으며, 서버가 수신자를 대신하여 일회용 공개키를 생성하는 방식을 통해 스마트카드와 같은 특수 하드웨어의 필요성을 제거하였다. 하지만 역시 송/수신자가 같은 전자우편 서버를 사용한다는 환경을 가정하고 있어서 비현실적이라는 문제점이 있다.



〔그림 4〕 김범한 등이 제안한 안전한 전자우편 프로토콜

김범한 등은 signcryption을 이용한 REP(a Robust E-mail protocol with Enhanced Privacy) 프로토콜을 추가로 제안하였다. 프로토콜의 동작은 [그림 5]와 같다[6]. 이 프로토콜에서는 signcryption을 이용하여 암호화와 인증을 동시에 수행하고자 하였으며, 송/수신자의 계산량을 줄이고자 하였다. 하지만 저자의 주장과 달리 완전한 전방향 안전성을 보장하지 못한다는 문제점을 가지고 있다. 완전한 전방향 안전성을 보장하기 위해서는 장기간 비밀키인 x_A, x_B, $pwdA$, $pwdB$가 노출되었을 경우 이전 사용된 세션키를 알 수 없어야 한다. 하지만 만약 공격자가 송신자의 장기간 개인키인 x_A와 $pwdA$를 알고 있고, 도청을 통해 $\{g^s\}_{pwdA}$, C, r, v를 알고 있다고 가정하면, $v=a(r+x_A)^{-1}$에서 x_A, r를 알고 있기 때문에 a를 알 수 있고, $\{g^s\}_{pwdA}$에서 $pwdA$를 알고 있기 때문에 g^s값을 알 수 있다. 결국, 공격자는 얻어진 a와 g^s를 이용하여 세션키 $K_1\|K_2$를 계산해낼 수 있다. 이와 같이 REP 프로토콜은 완전한 전방향 안전성을 제공하지 못하고 있으며, 이를 해결하기 위해서는 송신자와 서버 간에 s가 암호화되어 전송되어야 하며, 수신자와 서버 간에는 v와 s가 암호화 되어 전송되어야 한다. 즉, 프로토콜 내 두 번째 전송 메시지인 C, r, v, $\{H(C\|r\|v\|g^s)\}_{K_{pwdA}}$는 $\{H(C\|r\|v\|g^s)\|g^a\}_{K_{pwdA}}$, C, r, $\{v\}_{K_{AS}}$로 수정되어야 하며, 네 번째 전송 메시지인 C, r, v, $\{s\}_{K_{BS}}$,$\{g^t\}_{K_{pwdB}}$는 C, r, $\{s\|v\}_{K_{BS}}$,$\{g^t\}_{K_{pwdB}}$로 수정되어야 한다.



[그림 5] 김범한 등이 제안한 signcryption을 이용한 전자우편 프로토콜

Ⅲ. 제안하는 프로토콜

앞서 제안된 전자우편 보안 프로토콜들은 안전성과 효율성 측면에서의 문제를 보인 것 이외에 기존의 전자우편 시스템과의 호환성 부분에서도 큰 문제를 보여 그 실용성이 부족했다. 앞서 제안된 프로토콜들은 기존의 SMTP 서버와 POP 서버를 수정해서 사용해야 하고, 송/수신자가 같은 전자우편 서버를 사용해야 했다. 그리고 근래에 많이 사용되는 웹 전자우편 서비스에 적용하는 것이 불가능했다.

이 논문에서 제안하는 프로토콜은 기존의 전자우편 시스템을 그대로 유지하면서 추가로 신뢰할 수 있는 키 분배 서버를 추가하는 모델을 사용한다. 사용하는 모델에서 송신자는 신뢰 서버와 DH 키 동의 프로토콜을 수행하여 세션키를 생성하고 이를 바탕으로 signcryption을 수행하여 메시지를 암호화하고 서명한다. 송신자는 메시지 복호화에 필요한 정보를 수신자의 공개키로 암호화하여 암호화된 메시지와 함께 기존의 전자우편 시스템을 이용하여 전송하기만 하면 된다. 메시지를 받은 수신자는 신뢰서버와 DH 키 동의 프로토콜을 수행하여 세션키를 확보하고 자신이 받은 메시지에 대해 unsigncryption을 수행한다. 이 과정에서 송신자만 신뢰 서버에 미리 가입이 되어 있으면 수신자는 신뢰 서버에 가입되어 있지 않더라도 자신이 받은 메시지를 안전하게 복호화할 수 있다. 이 모델은 기존의 전자우편 시스템에 대한 수정이 없고 단지 송/수신자가 신뢰 서버와 통신을 통해 암호화된 메시지를 생성해주는 추가적 소프트웨어만 설치하면 되므로 기존의 POP 기반의 전자우편 서비스는 물론 웹기반의 전자우편 서비스에도 적용될 수 있다.

Sun 등의 첫 번째 프로토콜의 문제점 중 하나는 스마트카드와 같은 특수 하드웨어가 필요하다는 것이다. 제안하는 프로토콜의 경우도 여러 장치에서 안전하게 전자우편을 전송하거나 수신하기 위해서는 사용자가 자신의 공개키 쌍, 서버와 공유하고 있는 비밀키와 카운터 값이 필요하다. 하지만 Sun 등의 프로토콜의 문제점과는 성질이 다르다. Sun 등의 프로토콜은 특정 메일을 읽기 위해 이전에 서버에 제출한 여러 $<b, g^b>$ 쌍 중 해당 메일에 사용된 쌍을 가지고 있어야 한다. 즉, 장기간 키들 뿐만 아니라 단기간 키들을 유지해야 한다. 그런데 장기간 키를 안전하게 보관하고 휴대하는 것은 비단 제안하는 프로토콜만의 요구사항이 아니다. 대부분의 암호 프로토콜의 요구사항이다.

3.1. 프로토콜의 가정

제안하는 프로토콜은 다음과 같은 상황을 가정한다.

- 전자우편의 송신자는 수신자에게 전자우편을 보내기 전에 미리 신뢰 서버에 가입되어 있다.
- 신뢰 서버에 가입된 송신자 A는 서버와 대칭키 K_{AT}와 카운터 C_A를 공유하고 있다.
- 송신자와 수신자는 서로의 인증된 공개키를 알고 있다.
- 한 명의 수신자에게 전자우편을 보낼 때, 송신자와 수신자는 모두 같은 타원곡선 군 G로부터 생성된 공개키 쌍을 가지고 있어야 한다.
- 여러 명의 수신자에게 전자우편을 보낼 때, 송신자는 미리 모든 수신자의 인증된 공개키를 서버 데이터베이스에 등록해 놓아야 한다.

제안하는 프로토콜을 수행하기 위해서는 송신자가 서버와 첫 단계에서 통신하기 위해 대칭키를 가지고 있어야하고, 카운터 C_A를 이용해 메시지의 최신성을 검사하므로 C_A값을 공유하고 있어야 한다. 송/수신자 측에는 신뢰 서버와 통신하여 signcryption과 unsigncryption이 적용된 메시지를 생성하는 소프트웨어가 설치되어 있어야 하며, 송/수신자가 모두 동일한 키를 계산해 내기 위해서는 xP의 형태를 가진 공개키를 사용해야 한다. 단, 여러 명의 수신자에게 전자우편을 보낼 때는 송신자가 signcryption 과정에서 신뢰 서버가 생성해 준 공개키를 사용하므로 이와 같은 가정이 필요없다.

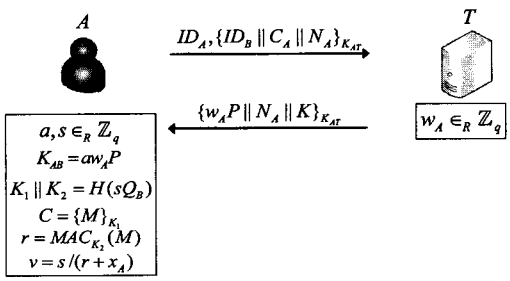
3.2. 수신자가 한 명인 경우의 프로토콜

제안하는 프로토콜은 크게 메시지 준비 단계, 메시지 전송 단계, 메시지 수신 단계의 세 단계로 나뉜다. 이 프로토콜에서 송신자 A와 수신자 B는 각각 signcryption과 unsigncryption을 수행하기 위해 개인키로 x_A, x_B를, 공개키로 $Q_A = x_A P$, $Q_B = x_B P$를 사용한다.

3.2.1. 메시지 준비 단계

메시지 준비 단계에서 송신자 A는 신뢰 서버 T와의 통신으로 세션키를 확립하고 signcryption을 수행한다. [그림 6]은 수신자가 한 명인 경우 메시지 준비 단계의 동작을 보여준다.

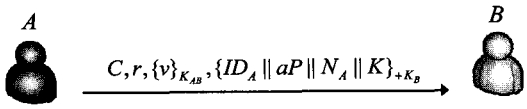
- A는 암호화된 메시지 생성을 위해 T에 자신이 생성한 난스 값 N_A와 수신자 B의 식별자인 ID_B, 카운터 값인 C_A를 A와 T가 미리 공유하고 있던 대칭키 K_{AT}로 암호화하여 전송한다. 이때 A는 자신의 식별자인 ID_A를 함께 전송하며, T는 A의 ID와 K_{AT}의 소유 여부를 이용하여 송신자를 인증한다. 여기서 ID는 각 사용자의 전자우편 주소이며 카운터는 메시지의 최신성을 보장하기 위해 사용한다.
- T는 메시지를 복호화하여 C_A값이 자신이 가지고 있던 C_A값보다 큰지 여부를 확인한다. C_A값이 자신의 값 보다 크다면 T는 A와의 카운터 값 동기화를 위해 카운터 값을 증가시킨다. 그 후 T는 DH 키 동의 프로토콜 수행을 위한 값 $w_A \in_R Z_q^*$와 향후에 T가 수신자 B를 인증하기 위한 랜덤한 대칭키 값 K를 생성한다. N_A, ID_B, K, w_A는 T의 데이터베이스에 저장되며 향후에 N_A를 식별자로 활용하여 검색한다. 마지막으로, T는 $w_A P$, N_A, K를 K_{AT}로 암호화하여 A에게 전송한다.
- A는 T로부터 받은 메시지를 복호화하고 N_A를 검사해 메시지 최신성을 확인한다. 최신성이 확인되면, A는 a, $s \in_R Z_q^*$를 선택하고, 선택한 a값을 이용하여 $K_{AB} = aw_A P$를, s값을 이용하여 sQ_B를 생성한다. $aw_A P$는 메시지 전달에 사용되는 세션키이며, sQ_B는 signcryption에 사용되는 키이다. A는 sQ_B를 사용하여 메시지 M에 대한 signcryption을 수행한다. 과정이 완료되면 T와의 카운터 값 동기화를 위해 C_A를 증가시킨다.



[그림 6] 수신자가 한 명일 경우 제안하는 프로토콜의 메시지 준비단계

3.2.2. 메시지 전송 단계

메시지 전송 단계에서는 A가 메시지 준비 단계에서 생성된 메시지를 B에게 전달한다. [그림 7]은 수신자가 한 명인 경우 메시지 전송 단계의 동작을 보여준다.



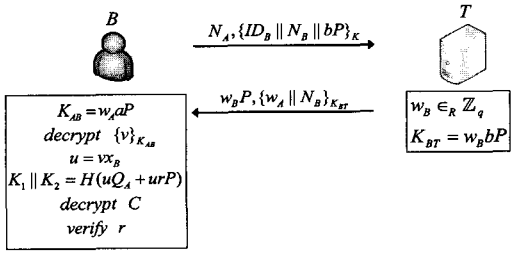
〔그림 7〕 수신자가 한 명일 경우 제안하는 프로토콜의 메시지 전송단계

- A는 signcryption을 수행해 생성된 C, r, v 중 v를 세션키 K_{AB}를 이용하여 암호화한다. C, r 값은 이미 암호화 되어있으므로 다시 암호화할 필요는 없다. 그리고 ID_A, aP, N_A, K를 B의 공개키 $+K_B$로 암호화 한다. ID_A는 A의 식별자이며, aP는 DH 키 동의 프로토콜을 통하여 K_{AB}를 생성하기 위한 값이다. B는 T에 가입되어 있지 않기 때문에 B가 정당한 사용자임을 T가 검증할 수 있도록 N_A, K 값을 같이 암호화한다. 향후에 B가 T에 N_A를 제출하면 T는 이를 식별자로 K값을 검색해내고, B가 동일한 K값을 가지고 있는지 검사하여 B를 인증한다. 암호화가 다 되었으면 A는 일반적인 전자우편 시스템을 이용하여 전자우편에 $\{ID_A \| aP \| N_A \| K\}_{+K_B}$, C, r, $\{v\}_{K_{AB}}$를 첨부하여 B에게 전달한다.

3.2.3. 메시지 수신 단계

메시지 수신단계에서 B는 A 로부터 받은 메시지를 바탕으로 T와 통신하여 필요한 정보를 얻어 unsigncryption을 수행한다. 〔그림 8〕은 수신자가 한 명인 경우 메시지 수신 단계의 동작을 보여준다.

- A 로부터 메시지를 수신한 B는 $b \in_R Z_q^*$를 선택하여 DH 키 동의 프로토콜 수행을 위한 값 bP를 생성하고, 메시지 최근성 보장을 위한 난스 값 N_B를 생성한다. 그리고 T에게 $\{ID_B \| N_B \| bP\}_K$ 와 N_A를 전송한다.
- T는 N_A를 식별자로 이용하여 자신의 데이터베이스에서 K를 검색하고 이 값으로 B로부터 받은 메시지에 대한 복호화를 시도한다. 성공하면 T는 B가 A로부터 메시지를 수신한 정당한 사용자임을 인증할 수 있다. T는 $w_B \in_R Z_q^*$를 선택하고 $K_{BT} = w_B bP$를 생성한다. 그리고 $w_B P$, $\{w_A \| N_B\}_{K_{BT}}$를 B에게 전송한다. B는 $w_B P$ 와 b값을 이용하여 K_{BT} 값을 생성할 수 있고 이 키를 사용하여 복호화한 값 w_A와 A 로부터 받은 aP 를 이용하여 K_{AB}를 생성할 수 있다.
- K_{AB}를 얻은 B는 v값을 복호화한 다음 C, r, v를 이용하여 unsigncryption을 수행한다.



〔그림 8〕 수신자가 한 명일 경우 제안하는 프로토콜의 메시지 수신단계

3.3. 수신자가 그룹인 경우의 프로토콜

이 절에서는 제안하는 프로토콜을 이용하여 여러 명의 수신자에게 그룹 전자우편을 보내는 과정을 살펴본다. 전체적인 과정은 수신자가 한 명인 경우의 프로토콜과 거의 유사하며, n명의 사용자에게 보낼 메시지를 n번 signcryption하는 비효율성을 없애기 위해 T가 생성한 x를 개인키로, xP를 공개키로 사용한다. 그룹 전자우편의 경우에도 프로토콜은 크게 메시지 준비 단계, 메시지 전송 단계, 메시지 수신 단계의 세 단계로 나뉜다.

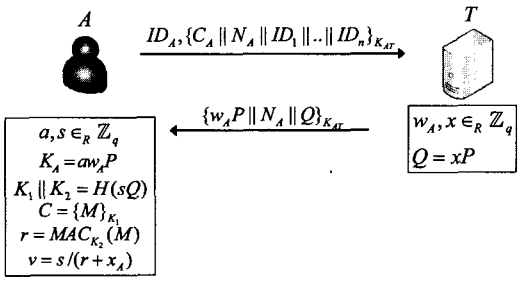
3.3.1. 메시지 준비 단계

〔그림 9〕는 수신자가 그룹인 경우 메시지 준비 단계의 동작을 보여준다.

- A 는 난스 N_A를 생성하고 수신자들의 식별자인 $ID_1, ID_2, \cdots, ID_n$, 카운터 값인 C_A와 함께 A 와 T가 미리 공유하고 있던 대칭키 K_{AT}로 암호화한다. 암호화된 메시지는 A의 ID인 ID_A와 함께 T에게 전송된다.
- T는 메시지를 복호화 하여 C_A값과 자신의 카운터 값을 비교한다. 그 후 T는 DH 키 동의 프로토콜 수행을 위한 값 $w_A \in_R Z_q^*$와 signcryption에 사용될 수신자의 개인키인 $x \in_R Z_q^*$를 선택하고 수신자의 공개키 $Q = xP$를 생성한다. T는 각 수신자의 ID 등과 N_A, x, w_A를 데이터베이스에 저장하며 향후에 N_A를 식별자로 활용하여 검색한다. 마지막으로, T는 $w_A P$, N_A, Q를 K_{AT}로 암호화하여 $w_A P$와 함

께 A에게 전송한다.

- A는 T로부터 받은 메시지를 복호화하고 N_A를 검사해 메시지 최신성을 확인한다. 최신성이 확인되면, A는 $a, s \in_R Z_q^*$를 선택하고, 선택한 a값을 이용하여 $K_A = aw_A P$를, s값을 이용하여 sQ를 생성한다. $aw_A P$는 메시지 전달에 사용되는 세션키이며, sQ는 signcryption에 사용되는 키이다. A는 sQ를 사용하여 M에 대한 signcryption을 수행한다. 과정이 완료되면 T와의 카운터 값 동기화를 위해 C_A를 증가시킨다.

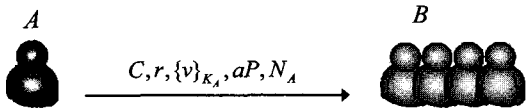


〔그림 9〕 수신자가 그룹일 경우 제안하는 프로토콜의 메시지 준비단계

3.3.2. 메시지 전송 단계

〔그림 10〕은 수신자가 그룹인 경우 메시지 전송 단계의 동작을 보여주며, 다음과 같이 이루어진다.

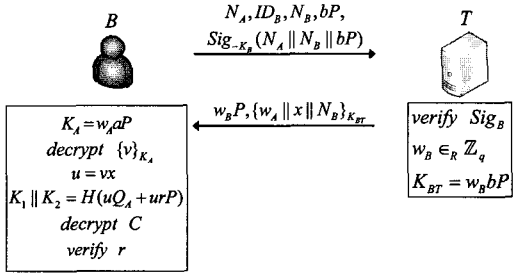
- A는 생성된 C, r, v 중 보호해야할 값인 v를 세션키 K_A를 이용하여 암호화 한다. 이 값들을 aP, N_A와 함께 전자우편에 첨부하여 일반적인 전자우편 시스템을 통하여 해당 그룹의 사용자에게 전달한다.



〔그림 10〕 수신자가 그룹일 경우 제안하는 프로토콜의 메시지 전송단계

3.3.3. 메시지 수신 단계

여러 명의 수신자가 메시지를 수신하지만 모든 수신자의 메시지 열람 방법이 같으므로 그 중 한 명인 수신자 B가 메시지를 수신하는 단계를 설명한다. 〔그림 11〕은 수신자가 그룹인 경우 메시지 수신 단계의 동작을 보여준다.



〔그림 11〕 수신자가 그룹일 경우 제안하는 프로토콜의 메시지 수신단계

- B는 $b \in_R Z_q^*$를 선택하여 DH 키 동의 프로토콜 수행을 위한 값 bP를 생성하고, 메시지 최근성 보장을 위한 난스 값 N_B를 생성한다. 이 값들과 자신의 식별자인 ID_B, N_A, 이들을 서명한 서명값인 $Sig_{-K_B}(N_A \| N_B \| bP)$를 T에게 전송한다.
- T는 네 번째 가정에 따라 미리 가지고 있던 B의 공개키로 서명을 확인하고, N_A를 식별자로 데이터베이스를 검색한다. T는 검색된 N_A와 비트결합되어있는 $ID_1, ..., ID_n$ 중에서 ID_B를 찾아내면 수신자를 인증할 수 있다. T는 $w_B \in_R Z_q^*$를 선택하고 $K_{BT} = w_B bP$를 생성한다. 그리고 $w_B P, \{w_A \| x \| N_B\}_{K_{BT}}$를 B에게 전송한다. B는 $w_B P$ 와 b값을 이용하여 K_{BT} 값을 생성할 수 있고 이 키를 사용하여 복호화한 값 w_A와 A로부터 받은 aP 를 이용하여 K_A를 생성할 수 있다.
- K_A를 얻은 B는 v값을 복호화 해 내고 C, r, v를 이용하여 unsigncryption을 수행한다.

IV. 프로토콜 분석

이 장에서는 제안하는 프로토콜의 안전성과 효율성을 분석한다. 전자우편의 가장 기본적인 보안 요구사항은 크게 기밀성과 인증이다[6]. 전자우편의 기밀성이란 전자우편의 전달 과정에서 전자우편의 내용이 제3자에게 노출되지 않아야 한다는 것을 말하며, 인증이란 수신자가 전자우편의 송신자를 확인할 수 있어야 한다는 것을 말한다. 이 외에 부인방지 등 추가적인 보안 요구사항이 있을 수 있으나 이 논문에서는 전자우편의 기밀성과 인증을 제공하는 것을 목적으로 프로토콜을 제안하

고 있으며, 기밀성을 향상시키기 위해 전방향 안전성을 추가로 제공하고자 하고 있다.

4.1. 수신자가 한 명인 경우의 프로토콜 안전성

제안하는 프로토콜은 크게 두 가지 요소로 구성되어 있다. 하나는 전자우편의 내용을 signcryption하는 부분이고, 다른 하나는 전방향 안전성을 제공하기 위한 부분이다. 수신자가 한 명인 경우의 프로토콜에서 후자의 요소들은 signcryption 자체의 안전성에는 아무런 영향을 주지 않는다. 즉, 전자우편을 signcryption만 하여 그 결과 값을 전달하면 기본적으로 기밀성과 인증이 제공된다는 것이다. 그런데 이와 같이 전달하면 전방향 안전성이 보장되지 않아 전방향 안전성이 보장되도록 참여자들 간에 키 확립을 하여 signcryption한 값을 다시 암호화하여 전달하고 있다. 따라서 제안하는 프로토콜은 이 논문에서 제공하고자 하였던 기밀성과 인증은 보장된다. 자세한 프로토콜의 안전성은 다음과 같다.

- **기밀성** : 메시지 M은 키 K_1으로 암호화 되어 메시지의 기밀성을 보장한다. 신뢰 서버의 경우도 w_A 값은 알고 있지만 aP값을 알 수 없으므로 메시지의 내용을 복호화 할 수 없다.
- **인 증** : 송신자와 신뢰 서버간에는 대칭키 K_{AT}를 이용하여 상호 인증할 수 있고, 수신자 B는 송신자 A의 공개키를 가지고 있고 A의 개인키 x_A로 signcryption 했으므로 수신자는 송신자를 인증할 수 있다. 또한 수신자와 신뢰 서버간에는 신뢰 서버가 생성한 키 값인 K를 이용하여 상호 인증한다. 신뢰 서버는 송신자가 정당한 수신자에게만 K를 전달할 것을 믿으며 수신자 또한 정당한 서버만이 K를 가지고 있다고 믿으므로 수신자와 신뢰 서버의 상호 인증이 가능하다.
- **완전한 전방향 안전성** : 이 프로토콜에서 장기간 키는 x_A, x_B, K_{AT} 이다. 사용된 signcryption이 안전하다고 가정하면 signcryption에 사용된 s나 정상적인 unsigncryption을 할 때 필요한 x_B를 알아야 메일의 내용을 볼 수 있다. s는 노출되는 정보가 아니지만, x_B는 전방향 안전성 공격자에게는 노출된 정보이다. 그런데 제안하는 프로토콜에서는 v가 K_{AB}로 암호화되어 전달되므로 공격자는 K_{AB}가 추가로 필요하다. K_{AB}는 타원곡선 기반의 DH 키 동의 기법에 의해 생성되는 값이므로 이 값을 알기 위해서는 a또는 w_A값을 알아야 한다. 이 산대수의 어려움 때문에 aP나 w_AP로부터 이 값을 얻을 수는 없지만 제안하는 프로토콜에서 w_A 값은 K_{BT}로 암호화 되어 전송된다. 하지만 K_{BT} 또한 타원곡선 기반의 DH 키 동의 기법에 의해 생성되는 값이고 여기에 사용되는 값 w_B, b는 외부로 노출되는 경우가 없으므로 안전하다. 따라서 장기간 키인 x_A, x_B, K_{AT}의 노출은 세션키의 계산에 아무런 영향을 주지 않으므로 완전한 전방향 안전성을 보장한다.

4.2. 수신자가 그룹인 경우의 프로토콜 안전성

수신자가 그룹인 경우에도 프로토콜의 안전성은 수신자가 한명인 경우와 거의 동일하다. 다만 수신자가 그룹인 경우에는 수신자의 공개키를 이용하여 signcryption을 하지 않고 있기 때문에 수신자들에게만 기밀성을 제공할 수 없으며, 신뢰서버도 전자우편의 내용을 볼 수 있다. 특히, 수신자들은 신뢰서버로부터 일회성 공개키에 대응되는 개인키를 받아야 송신자로부터 받은 전자우편을 unsigncryption할 수 있다. 만약 공격자도 교환되는 일회성 개인키를 확보할 수 있으면 전자우편의 기밀성을 제공할 수 없다. 하지만 신뢰서버는 수신자의 전자서명을 확인한 후에 타원곡선 Diffie-Hellman 키를 이용하여 개인키를 전달하여 주기 때문에 제3자가 이 값을 확보하는 것은 계산적으로 어렵다.

- **기밀성** : 메시지 M은 키 K_1으로 암호화 되어 메시지의 기밀성을 보장한다. 다만 이 프로토콜에서는 모든 메시지를 각각 수신자의 공개키로 암호화 할 수 없으므로 aP값이 평문으로 노출된다. 공격자는 w_A값을 알 수 없으므로 메시지를 복호화할 수 없지만 신뢰 서버의 경우는 w_A값은 알고 있으므로 메시지의 내용을 복호화 할 수 있다.
- **인 증** : 송신자와 서버간에는 대칭키 K_{AT}를 이용하여 상호 인증할 수 있고, 수신자 B는 송신자 A의 공개키를 가지고 있고 A의 개인키 x_A로 signcryption 했으므로 수신자는 송신자를 인증한다. 송신자는 신뢰 서버가 생성한 일회용 공개키를 사용하여 signcryption을 수행하지만 서버는 송신자를 대신하여 signcryption을 할 수 없기 때문에 수

〔표 2〕 제안하는 프로토콜의 효율성 비교

프로토콜	참여자	지수연산	서명생성	서명확인	지수연산 내용
Sun 등의 프로토콜 1	송신자	2	1	1	g^a, g^{ab}
	수신자	2	1	1	g^b, g^{ab}
	서 버	0	0	0	-
Sun 등의 프로토콜 2	송신자	3	1	1	g^{as}, g^r, y_B^r
	수신자	4	1	2	U^{x_B}, g^b, g^{bt}, g^{as}
	서 버	3	2	0	g^s, g^t, g^{bt}
김범한 등의 프로토콜 1	송신자	3	1	0	g^{as}, g^r, y_B^r
	수신자	4	0	1	U^{x_B}, g^b, g^{bt}, g^{as}
	서 버	3	0	0	g^s, g^t, g^{bt}
김범한 등의 프로토콜 2 (REP)	송신자	2	1	0	g^a, g^{as}
	수신자	2	0	1	g^b, g^{bt}
	서 버	4	0	0	g^s, g^{as}, g^t, g^{bt}
제안하는 프로토콜 단일 수신자	송신자	2	1*	0	aP, aw_AP
	수신자	3	0	1*	bP, aw_AP, bw_BP
	서 버	3	0	0	w_AP, w_BP, bw_BP
제안하는 프로토콜 그룹 수신자	송신자	2	1*	0	aP, aw_AP
	수신자	3	0	1*	bP, aw_AP, bw_BP
	서 버	3	0	0	w_AP, w_BP, bw_BP

* 타원곡선 기반의 signcryption 기법으로 기존의 서명에 비해 비용이 저렴하다. 단위 : 횟수

신자는 송신자를 인증할 수 있다. 또한 신뢰 서버는 송신자가 미리 등록해 놓은 수신자의 공개키를 신뢰하며 이를 바탕으로 수신자의 서명을 검증하여 수신자를 인증할 수 있고, 수신자는 unsigncryption을 위한 w_A값을 정당한 신뢰 서버만 가지고 있다고 믿으므로 서버로부터 w_A를 받아 unsigncryption이 성공적으로 수행되면 신뢰 서버를 인증할 수 있다.

- **완전한 전방향 안전성** : 이 프로토콜에서는 공격자가 메시지를 복호화 하기 위해 b 대신 x를 알아내야 한다는 점이 수신자가 한 명일 경우의 프로토콜과 다르다. 하지만 x 또한 타원곡선 기반의 DH 키 동의 기법에 의해 생성되는 값 K_{BT}로 암호화 되어 전송되므로 공격자는 x값을 알 수 없다. 따라서 제안하는 프로토콜은 수신자가 그룹인 경우에도 완전한 전방향 안전성을 제공한다.

4.3. 프로토콜의 효율성

전자우편의 송신자와 수신자, 신뢰 서버는 타원곡선 기반의 DH 키 동의 프로토콜 과정에서 일정량의 지수연산을 수행하고, 타원곡선 기반의 signcryption과 unsigncryption을 통해 메시지를 서명하고 서명을 확인한다. 이 과정에서의 계산 비용을 현재까지 제안된 프로토콜과 비교하면 〔표 2〕와 같다. 효율성 비교는 이전 제안된 프로토콜의 틀린 부분을 수정했을 때를 기준으로 계산하였으며, 표에 명시된 숫자의 단위는 프로토콜 수행중의 해당 연산의 수행 횟수를 의미한다.

제안된 프로토콜은 현재까지 제안된 현재까지 제안된 프로토콜 중 가장 효율적인 REP 프로토콜과 유사한 연산량을 보여주고 있으나, 타원곡선 기반의 DH 키 동의 기법과 signcryption으로 저렴한 비용의 지수연산과 서명 생성/확인을 수행한다. 또한 제안된 프로토콜은 기존의 전자우편 시스템 구조를 변경하지 않고 그대로 사용하므로 기존 프로토콜에 비해 실용적이며, 그룹 전자우편을 지원하는 장점을 가지고 있다.

V. 결 론

이 논문에서는 완전한 전방향 안전성을 제공하는 전자우편 보안 프로토콜을 제안하였다. 제안하는 프로토

콜은 기존의 전자우편 시스템에 아무런 영향을 주지 않고 동작하므로 그 실용성이 뛰어나고, 웹기반의 전자우편 서비스에도 적용이 가능하다. 그리고 송신자만 신뢰 서버에 가입되어있으면 수신자는 신뢰 서버에 미리 가입되어 있지 않더라도 한 명 또는 여러 명의 수신자에게 쉽게 비밀성이 요구되는 메시지를 전달할 수 있다. 제안하는 프로토콜의 가정에서 수신자가 한 명인 경우 송신자와 수신자가 반드시 같은 타입의 공개키와 개인키 쌍을 가지고 있어야 한다고 가정하였는데, 모든 수신자가 송신자와 같은 타입의 공개키 쌍을 가지기는 어렵다. 따라서, 송신자와 다른 타입의 공개키 쌍을 가진 수신자에게 안전하게 전자우편을 전달하는 기법을 고려할 예정이다.

참고문헌

[1] J. Postel, "Simple Mail Transfer Protocol," RFC 821, 1982.

[2] J. Callas, L. Donnerhacke, H. Finney, R. Thayer, "OpenPGP Message Format," RFC 2440, 1998.

[3] B. Ramsdell, "Secure/Multipurpose Internet Mail Extensions(S/MIME) Version 3.1 Message Specification," RFC 3851, 2004.

[4] I. Brown, "Forward Secrecy Extensions for Open PGP," draft-brown-pgp-pfs-04, http://www.links.org/dnssec/draft-brown-pfp-04.html.

[5] H. Sun, B. Hsieh, H. Hwang, "Secure E-mail Protocols Providing Perfect Secrecy," IEEE Communication Letters, Vol.9, No.1, pp.58-60, 2005.

[6] 김범한, 구재형, 이동훈, "완전한 전방향 안전성을 보장하는 이메일 프로토콜," 한국정보보호학회 충청지부 학술대회, pp.37-48, 2005.

[7] A. W. Dent, "Flaws in an E-Mail Protocol of Sun, Hsieh, and Hwang," IEEE Communication Letters, Vol.9, No.8, pp.718-719, 2005.

[8] Y. Zheng, H. Imai, "How to Construct Efficient Signcryption Scheme on Elliptic Curves," Information Processing Letters, Vol.68, pp.227-233, 1998.

[9] K. Moore, "SMTP Service Extension for Delivery Status Notifications," RFC 1891, 1996.

〈著者紹介〉

이 창 용 (Changyong Lee) 학생회원
2004년 2월 : 강원대학교 전기전자정보통신공학부(학사)
2006년 3월~현재 : 한양대학교 컴퓨터공학과 석사과정
<관심분야> 네트워크 보안

김 대 영 (Daeyoung Kim) 학생회원
2005년 2월 : 한양대학교 전자컴퓨터공학부(학사)
2007년 2월 : 한양대학교 컴퓨터공학과(석사)
2007년 3월~현재 : (주)엠파스 시스템본부 시스템개발부 ECS개발팀
<관심분야> 네트워크 보안
URL : http://kzero.net

심 동 호 (Dongho Shim) 정회원
1996년 2월 : 한양대학교 전자계산학과(학사)
2000년 6월 : 뉴욕시립대학교 Computer Science(석사)
2006년 3월~현재 : 남부대학교 디지털경영정보 박사과정
2003년 7월~현재 : (주)누리비전 대표이사
<관심분야> 정보보호, 전자우편 보안

김 상 진 (Sangjin Kim) 종신회원
1995년 2월 : 한양대학교 전자계산학과(학사)
1997년 2월 : 한양대학교 전자계산학과(석사)
2002년 8월 : 한양대학교 전자계산학과(박사)
2003년 3월~현재 : 한국기술교육대학교 인터넷미디어공학부 조교수
<관심분야> 암호기술 응용
URL:http://infosec.kut.ac.kr/sangjin

오 희 국 (Heekuck Oh) 종신회원
1983년 : 한양대학교 전자공학과(학사)
1989년 : 아이오와주립대학 전자계산학과(석사)
1992년 : 아이오와주립대학 전자계산학과(박사)
1993년~1994년 : 한국전자통신연구원 선임연구원
1995년 3월~현재 : 한양대학교 컴퓨터공학과 부교수
<관심분야> 암호프로토콜, 네트워크 보안
URL:http://infosec.hanyang.ac.kr/~hkoh/