(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0005975
(43) 공개일자 2009년01월14일

(51) Int. Cl.
G06Q 50/00 (2008.03)
(21) 출원번호 10-2008-0064377
(22) 출원일자 2008년07월03일
심사청구일자 2008년07월03일
(30) 우선권주장
1020070069365 2007년07월10일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
권정옥
서울 광진구 중곡1동 234-12번지
정익래
광주 북구 오치2동 로얄아파트 102동 101호
(뒷면에 계속)
(74) 대리인
현종철

전체 청구항 수 : 총 20 항

(54) 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법 및이를 기록한 기록매체

(57) 요 약

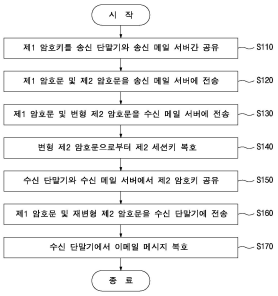
기밀성과 전방향 안전성을 제공하는 이메일 전송 방법 및 이를 기록한 기록매체가 개시된다.

본 발명에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법은,

이메일 메시지를 전송하고자 하는 송신 단말기에서 수신 메일 서버와 제 1 세션키를 미리 공유한 송신 메일 서버에 로그인하면, 상기 송신 단말기에서 선택된 제 1 난수와 상기 송신 메일 서버에서 선택된 제 2 난수를 이용하여 상기 송신 단말기와 상기 송신 메일 서버간에 공유되는 제 1 암호키를 각각 생성하고 상기 제 1 암호키를 공유하는 단계; 상기 송신 단말기에서 제 3 난수를 선택하고, 상기 선택된 제 3 난수에 따라 생성된 제 2 세션키를 이용하여 상기 송신 단말기에서 전송하고자 하는 이메일 메시지를 암호화한 제 1 암호문 및 상기 제 1 암호키를 이용하여 상기 제 2 세션키를 암호화한 제 2 암호문을 상기 송신 메일 서버에 전송하는 단계; 상기 송신 메일 서버에서 상기 제 1 암호키를 이용하여 상기 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 제 1 세션키를 이용하여 상기 제 2 세션키를 암호화하여 변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 변형 제 2 암호문을 수신 메일 서버에 전송하는 단계; 상기 수신 메일 서버에서 상기 제 1 세션키를 이용하여 상기 변형 제 2 암호문으로부터 상기 제 2 세션키를 복호하는 단계; 수신 단말기가 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기와 상기 수신 메일 서버 간의 제 2 암호키를 각각 생성하고, 상기 수신 단말기와 상기 수신 메일 서버에서 상기 제 2 암호키를 공유하는 단계; 상기 수신 메일 서버에서 상기 제 2 암호키를 이용하여 상기 제 2 세션키를 암호화하여 재변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 재변형 제 2 암호문을 상기 수신 단말기에 전송하는 단계; 및 상기 수신 단말기에서 상기 제 2 암호키를 이용하여 상기 재변형 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 복호된 상기 제 2 세션키를 이용하여 상기 제 1 암호문으로부터 상기 이메일 메시지를 복호하는 단계를 포함한다.

본 발명에 의하면, 사용자의 패스워드 또는 메일 서버의 비밀키가 노출된 경우에도 공개키 인증서의 필요 없이 이메일 계정의 패스워드만을 이용하여 이메일 메시지의 기밀성과 전방향 안전성을 제공하는 효과가 있다.

대 표 도 - 도1



(72) 발명자

이동훈

경기 고양시 일산서구 일산3동 후곡 동신 808-804

임종인

서울 종로구 내수동 95 삼성파크팰리스 101-901

특허청구의 범위

청구항 1

이메일 메시지를 전송하고자 하는 송신 단말기에서 수신 메일 서버와 제 1 세션키를 미리 공유한 송신 메일 서버에 로그인하면, 상기 송신 단말기에서 선택된 제 1 난수와 상기 송신 메일 서버에서 선택된 제 2 난수를 이용하여 상기 송신 단말기와 상기 송신 메일 서버 간에 공유되는 제 1 암호키를 각각 생성하고 상기 제 1 암호키를 공유하는 단계;

상기 송신 단말기에서 제 3 난수를 선택하고, 상기 선택된 제 3 난수에 따라 생성된 제 2 세션키를 이용하여 상기 송신 단말기에서 전송하고자 하는 이메일 메시지를 암호화한 제 1 암호문 및 상기 제 1 암호키를 이용하여 상기 제 2 세션키를 암호화한 제 2 암호문을 상기 송신 메일 서버에 전송하는 단계;

상기 송신 메일 서버에서 상기 제 1 암호키를 이용하여 상기 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 제 1 세션키를 이용하여 상기 제 2 세션키를 암호화하여 변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 변형 제 2 암호문을 수신 메일 서버에 전송하는 단계;

상기 수신 메일 서버에서 상기 제 1 세션키를 이용하여 상기 변형 제 2 암호문으로부터 상기 제 2 세션키를 복호하는 단계;

수신 단말기가 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기와 상기 수신 메일 서버 간의 제 2 암호키를 각각 생성하고, 상기 수신 단말기와 상기 수신 메일 서버에서 상기 제 2 암호키를 공유하는 단계;

상기 수신 메일 서버에서 상기 제 2 암호키를 이용하여 상기 제 2 세션키를 암호화하여 재변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 재변형 제 2 암호문을 상기 수신 단말기에 전송하는 단계; 및

상기 수신 단말기에서 상기 제 2 암호키를 이용하여 상기 재변형 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 복호된 상기 제 2 세션키를 이용하여 상기 제 1 암호문으로부터 상기 이메일 메시지를 복호하는 단계를 포함하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 2

제 1 항에 있어서,

상기 제 1 암호키를 공유하는 단계는

상기 송신 단말기에서 선택된 제 1 난수에 따라 생성된 송신 단말 메시지를 송신 메일 서버로 전송하고, 상기 송신 메일 서버에서 선택된 제 2 난수에 따라 생성된 송신 메일 서버 메시지를 상기 송신 단말기에 전송하는 단계;

상기 송신 단말기에서 상기 송신 메일 서버 메시지를 이용하여 제 1 공유 메시지 인증 코드키를 생성하고, 상기 제 1 공유 메시지 인증 코드키를 이용하여 송신 단말기의 메시지 인증 코드값을 생성하여 상기 송신 메일 서버에 전송하는 단계;

상기 송신 메일 서버에서 상기 송신 단말 메시지를 이용하여 상기 제 1 공유 메시지 인증 코드키를 생성하고, 상기 제 1 공유 메시지 인증 코드키를 이용하여 상기 송신 메일 서버의 메시지 인증 코드값을 생성하여 상기 송신 단말기에 전송하는 단계;

상기 송신 단말기에서 상기 제 1 공유 메시지 인증 코드키를 이용하여 상기 송신 메일 서버의 메시지 인증 코드값을 검증한 후, 상기 송신 메일 서버 메시지를 이용하여 제 1 암호키를 생성하는 단계; 및

상기 송신 메일 서버에서 상기 제 1 공유 메시지 인증 코드키를 이용하여 상기 송신 단말기의 메시지 인증 코드값을 검증한 후, 상기 송신 단말 메시지를 이용하여 상기 제 1 암호키를 생성하는 단계를 포함하는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 3

제 2 항에 있어서,

상기 제 2 암호키를 공유하는 단계는

상기 수신 단말기에서 선택된 수신 단말 난수에 따라 생성된 수신 단말 메시지를 상기 수신 메일 서버로 전송하고, 상기 수신 메일 서버에서 선택된 수신 메일 서버 난수에 따라 생성된 수신 메일 서버 메시지를 상기 수신 단말기에 전송하는 단계;

상기 수신 단말기에서 상기 수신 메일 서버 메시지를 이용하여 제 2 공유 메시지 인증 코드키를 생성하고, 상기 제 2 공유 메시지 인증 코드키를 이용하여 수신 단말기의 메시지 인증 코드값을 생성하여 상기 수신 메일 서버에 전송하는 단계;

상기 수신 메일 서버에서 상기 수신 단말 메시지를 이용하여 상기 제 2 공유 메시지 인증 코드키를 생성하고, 상기 제 2 공유 메시지 인증 코드키를 이용하여 상기 수신 메일 서버의 메시지 인증 코드값을 생성하여 상기 수신 단말기에 전송하는 단계;

상기 수신 단말기에서 상기 제 2 공유 메시지 인증 코드키를 이용하여 상기 수신 메일 서버의 메시지 인증 코드값을 검증한 후, 상기 수신 메일 서버 메시지를 이용하여 제 2 암호키를 생성하는 단계; 및

상기 수신 메일 서버에서 상기 제 2 공유 메시지 인증 코드키를 이용하여 상기 수신 단말기의 메시지 인증 코드값을 검증한 후, 상기 수신 단말 메시지를 이용하여 상기 제 2 암호키를 생성하는 단계를 포함하는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 4

제 2 항에 있어서,

상기 송신 단말 메시지 X_A는

상기 제 1 난수가 x_A이고, 오더(order)가 q 인 유한 순환군의 서로 다른 두 개의 생성자가 g_1, g_2이고, 상기 송신 단말기의 아이디가 A 이고, 송신 메일 서버의 아이디가 S_A이고, 상기 송신 단말기의 패스워드가 pw_A이고, $H()$는 해쉬함수이고, p는 $2q+1=p$를 만족하는 소수일때, 하기의 식 1에 의해 생성되는 것을 특징으로 하는 기밀성과 전방향 안정성을 제공하는 이메일 전송 방법.

$$X_A = g_1^{x_A} g_2^{H(A||S_A||pw_A)} \bmod p \quad (1)$$

청구항 5

제 2 항에 있어서,

상기 송신 메일 서버 메시지 X_{S_A}는

g_1, g_2는 오더가 q인 유한 순환군의 서로 다른 두 개의 생성자이고, y_A는 상기 송신 메일 서버에서 생성된 제 2 난수이고, A는 상기 송신 단말기의 아이디이고, S_A는 상기 송신 메일 서버의 아이디이고, pw_A는 상기 송신 단말기의 패스워드이고, $H()$는 해쉬 함수이며, p는 $2q+1=p$를 만족하는 소수일 때, 하기의 식 2에 의해 결정되는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

$$X_{S_A} = g_1^{y_A} g_2^{H(A||S_A||pw_A)} \bmod p \quad (2)$$

청구항 6

제 2 항에 있어서,

상기 제 1 공유 메시지 인증 코드키는

X_{S_A}는 송신 메일 서버 메시지이고, g_1, g_2는 오더가 q인 유한 순환군의 생성자이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, pw_A는 송신 단말기의 패스워드이고, $H()$는 해쉬 함수이며, x_A가 상기 제 1 난수이고, y_A가 상기 제 2 난수일 때, 하기의 식 3에 의해 상기 제 1 공유 메시지 인증 코드키 k_A가 생성되는 것을 특징으로 하는 기밀성과 전방향 안정성을 제공하는 이메일 전송 방법.

$$k_A=\left(X_{S_A}/g_2^{H(A||S_A||pw_A)}\right)^{x_A}=g_1^{x_Ay_A} \quad (3)$$

청구항 7

제 2 항에 있어서,

상기 송신 단말기의 메시지 인증 코드값 τ_A는

$Mac.G$가 메시지 인증 코드값 생성 함수이고, k_A가 상기 제 1 공유 메시지 인증 코드키이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, X_A는 송신 단말 메시지이고, X_{S_A}는 송신 메일 서버 메시지일 때, 하기의 식 4에 의해 생성되는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

$$\tau_A=Mac.G_{k_A}(A||S_A||X_A||X_{S_A}) \quad (4)$$

청구항 8

제 7 항에 있어서,

상기 송신 메일 서버의 메시지 인증 코드값 τ_{S_A}는

하기의 식 5에 의해 생성되는 것을 특징으로 하는 기밀성과 전방향 안정성을 제공하는 이메일 전송 방법.

$$\tau_{S_A}=Mac.G_{k_A}(S_A||A||X_A||X_{S_A}) \quad (5)$$

청구항 9

제 8 항에 있어서,

상기 제 2 세션키 SK는

$H()$는 해쉬 함수이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, sid는 세션 아이디이며 $sid=X_A||X_{S_A}||\tau_A||\tau_{S_A}$에 의해 연산되고, sk는 제 3 난수일 때, 하기의 식 6에 의해 생성되는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

$$SK=H(A||S_A||sid||sk) \quad (6)$$

청구항 10

제 2 항에 있어서,

상기 제 1 암호키를 생성하는 단계는

상기 제 1 공유 메시지 인증 코드키 k_A를 이용하여 상기 송신 메일 서버의 메시지 인증 코드값 τ_{S_A}가 $Check\ Mac.V_{k_A}(\tau_{S_A})$이 '1'의 값을 출력하는 지의 여부에 따라 검증하되,

'1'의 값이 출력되면 상기 송신 메일 서버로부터 전송된 송신 메일 서버 메시지 X_{S_A}를 유효한 메시지 인증 코드값으로 판단하고, '0'의 값이 출력되면 유효하지 않은 메시지 인증 코드값으로 판단하여 전송된 송신 메일 서버 메시지 X_{S_A}를 버리는 단계를 포함하는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 11

송신 단말기에서 송신 단말 일회용 공개키와 송신 단말 비밀키로 이루어진 송신 단말 데이터 쌍을 저장하고, 송신 메일 서버에서 송신 단말 아이디 및 상기 송신 단말 일회용 공개키로 이루어진 송신 메일 서버 데이터 쌍을 메일 서버 리스트에 저장하며, 수신 단말기에서 수신 단말 일회용 공개키와 수신 단말 비밀키로 이루어진 수신 단말 데이터 쌍을 저장하고, 수신 메일 서버에서 수신 단말기의 아이디 및 수신 단말 일회용 공개키로 이루어진 수신 메일 서버 데이터 쌍을 메일 서버 리스트에 미리 저장하는 단계;

이메일 메시지를 전송하고자 하는 상기 송신 단말기에서 상기 수신 메일 서버와 제 1 세션키를 미리 공유한 상기 송신 메일 서버에 로그인하면, 상기 송신 단말기에서 선택된 제 1 난수와 상기 송신 메일 서버에서 선택된 제 2 난수를 이용하여 상기 송신 단말기와 상기 송신 메일 서버간에 공유되는 제 1 암호키를 각각 생성하고 상기 제 1 암호키를 공유하는 단계;

상기 수신 메일 서버에서 상기 송신 메일 서버와 미리 공유한 제 1 세션키 및 상기 수신 메일 서버 리스트에 저장된 수신 단말 일회용 공개키를 이용하여 수신 서버 암호문을 생성하여 상기 송신 메일 서버에 전송하는 단계;

상기 송신 메일 서버에서 상기 수신 서버 암호문으로부터 상기 수신 단말 일회용 공개키를 복호하고, 상기 복호된 수신 단말 일회용 공개키 및 상기 제 1 암호키를 이용하여 송신 서버 암호문을 생성하여 상기 송신 단말기에 전송하는 단계;

상기 송신 단말기에서 상기 제 1 암호키를 이용하여 제 1 암호문을 생성하여 상기 송신 메일 서버로 상기 제 1 암호문을 전송하는 단계;

상기 송신 메일 서버에서 상기 제 1 암호키를 이용하여 상기 제 1 암호문으로부터 상기 송신 단말 암호문을 복호한 후, 복호된 상기 송신 단말 암호문에 상기 제 1 세션키를 이용하여 제 2 암호문을 생성하여 상기 수신 메일 서버에 전송하는 단계;

상기 수신 메일 서버에서 상기 제 1 세션키를 이용하여 상기 제 2 암호문으로부터 상기 송신 단말 암호문을 복호하는 단계;

상기 수신 단말기에서 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기와 상기 수신 메일 서버에서 제 2 암호키를 생성하여 상기 수신 단말기 및 상기 수신 메일 서버에서 공유하는 단계;

상기 수신 메일 서버에서 상기 제 2 암호키를 이용하여 상기 송신 단말 암호문을 암호화하여 제 3 암호문을 생성하여 상기 수신 단말기에 전송하는 단계; 및

상기 수신 단말기에서 상기 제 2 암호키를 이용하여 상기 제 3 암호문으로부터 상기 송신 단말 암호문을 복호하고, 복호된 상기 송신 단말 암호문으로부터 상기 수신 단말 비밀키를 이용하여 상기 이메일 메시지를 복호하는 단계를 포함하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 12

제 11 항에 있어서,

상기 송신 메일 서버로 상기 제 1 암호문을 전송하는 단계는

상기 송신 서버 암호문으로부터 상기 수신 단말 일회용 공개키를 복호하고, 상기 복호된 수신 단말 일회용 공개키를 이용하여 상기 이메일 메시지를 암호화하여 송신 단말 암호문을 생성하고, 상기 송신 단말 암호문에 상기

제 1 암호키를 이용하여 제 1 암호문을 생성하는 단계를 포함하는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 13

제 11 항에 있어서,

상기 이메일 메시지를 복호하는 단계는

상기 수신 단말기에서 상기 수신 단말 일회용 공개키와 수신 단말 비밀키를 갱신하는 단계를 더 포함하는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 14

송신 단말기에서 제 1 난수를 생성하고, 송신 메일 서버에서 상기 송신 단말기의 아이디 및 상기 송신 메일 서버에서 생성한 생성자에 상기 제 1 난수를 지수승한 송신 메일 서버의 메시지로 이루어진 데이터 쌍을 송신 메일 서버 리스트에 저장하고, 수신 단말기에서 제 2 난수를 생성하고, 수신 메일 서버에서 상기 수신 단말기의 아이디 및 상기 수신 메일 서버에서 생성한 생성자에 상기 제 2 난수를 지수승한 수신 메일 서버의 메시지로 이루어진 데이터 쌍을 수신 메일 서버 리스트에 저장하는 단계;

이메일 메시지를 전송하고자 하는 상기 송신 단말기에서 상기 송신 메일 서버와 로그인 프로토콜을 수행하여 생성된 제 1 암호키를 상호 공유하는 단계;

상기 송신 메일 서버에서 수신 메일 서버와 키 교환 프로토콜을 수행하여 제 1 세션키를 상호 공유하고, 상기 수신 메일 서버에서 상기 수신 메일 서버의 메시지 및 상기 제 1 세션키를 이용하여 상기 수신 메일 서버의 메시지를 암호화한 수신 메일 서버의 메시지 인증 코드값을 상기 송신 메일 서버로 전송하는 단계;

상기 송신 메일 서버에서 상기 수신 메일 서버의 메시지 인증 코드값이 유효한 지의 여부를 검증하고, 상기 송신 메일 서버에서 수신 메일 서버의 메시지, 상기 제 1 암호키를 이용하여 상기 수신 메일 서버의 메시지를 암호화한 송신 메일 서버의 제 1 메시지 인증 코드값을 상기 수신 단말기에 전송하는 단계;

상기 송신 단말기에서 상기 송신 메일 서버로부터 전송된 상기 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한지의 여부를 판단하고, 제 3 난수를 선택하여 생성된 송신 단말 메시지 및 상기 송신 단말 메시지 및 상기 제 2 난수를 이용하여 생성된 제 2 세션키를 연산하는 단계;

상기 송신 단말기에서 상기 제 2 세션키로 상기 이메일 메시지를 암호화한 암호문, 상기 송신 단말 메시지, 및 상기 제 1 암호키를 이용하여 상기 송신 단말 메시지를 암호화한 송신 단말의 메시지 인증 코드값을 상기 송신 메일 서버로 전송하는 단계;

상기 송신 메일 서버에서 상기 송신 단말기로부터 전송된 송신 단말의 메시지 인증 코드값이 유효한지의 여부를 판단하고, 상기 송신 메일 서버에서 상기 암호문, 상기 송신 단말 메시지 및 상기 제 1 세션키로 상기 송신 단말 메시지를 암호화한 송신 메일 서버의 제 2 메시지 인증 코드값을 상기 수신 메일 서버로 전송하는 단계;

상기 수신 메일 서버에서 상기 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 지의 여부를 판단하고, 상기 수신 메일 서버에서 상기 암호문 및 상기 송신 단말 메시지를 저장하는 단계;

상기 수신 단말기가 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기 및 상기 수신 메일 서버에서 로그인 프로토콜을 수행하여 제 2 암호키를 공유하는 단계;

상기 수신 메일 서버에서 상기 송신 단말기의 아이디, 상기 암호문, 상기 송신 단말 메시지 및 상기 제 2 암호키로 상기 송신 단말 메시지를 암호화한 수신 단말의 메시지 인증 코드값을 상기 수신 단말기에 전송하는 단계; 및

상기 수신 단말기에서 상기 수신 단말의 메시지 인증 코드값이 유효한지의 여부를 판단하고, 상기 제 2 난수를 이용하여 상기 제 2 세션키를 추출하고, 상기 제 2 세션키를 이용하여 상기 암호문으로부터 상기 이메일 메시지를 추출하는 단계를 포함하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 15

제 14 항에 있어서,

상기 수신 메일 서버의 메시지 인증 코드값이 유효한 지의 여부는

상기 제 1 세션키 k_{SS}를 이용하여 상기 수신 메일 서버의 메시지 인증 코드값 τ_1이 유효한지의 여부를 $Check\ Mac\ V_{k_{SS}}(\tau_1)$에 의해 검증하며, 검증값이 '1'이 출력되면 수신 메일 서버의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어, 수신된 수신 메일 서버의 메시지 인증 코드값을 버리는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 16

제 14 항에 있어서,

상기 송신 메일 서버로부터 전송된 상기 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한지의 여부는

상기 제 1 암호키 K_A를 이용하여 상기 송신 메일 서버의 제 1 메시지 인증 코드값 τ_2이 유효한지의 여부를 $Check\ Mac\ V_{K_A}(\tau_2)$에 의해 검증하며, 검증값이 '1'이 출력되면 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어 수신된 송신 메일 서버의 제 1 메시지 인증 코드값을 버리는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 17

제 14 항에 있어서,

상기 송신 단말의 메시지 인증 코드값이 유효한지의 여부는

상기 제 1 암호키 K_A를 이용하여 상기 송신 단말의 메시지 인증 코드값 τ_3가 유효한지의 여부를 $Check\ Mac\ V_{K_A}(\tau_3)$에 의해 검증하며, 검증값이 '1'이 출력되면 상기 송신 단말의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어 수신된 상기 송신 단말의 메시지 인증 코드값을 버리는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 18

제 14 항에 있어서,

상기 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 지의 여부는

상기 제 1 세션키 k_{SS}를 이용하여 상기 송신 메일 서버의 제 2 메시지 인증 코드값 τ_4가 유효한지의 여부를 $Check\ Mac\ V_{k_{SS}}(\tau_4)$에 의해 검증하며, 검증값이 '1'이 출력되면 상기 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어, 수신된 상기 송신 메일 서버의 제 2 메시지 인증 코드값을 버리는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 19

제 14 항에 있어서,

상기 수신 단말의 메시지 인증 코드값이 유효한지의 여부는

상기 제 2 비밀키 K_B를 이용하여 상기 수신 단말의 메시지 인증 코드값 τ_5가 유효한지의 여부를 $Check\ Mac\ V_{K_B}(\tau_5)$에 의해 검증하며, 검증값이 '1'이 출력되면 상기 수신 단말의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어, 수신된 상기 수신 단말의 메

시지 인증 코드값을 버리는 것을 특징으로 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법.

청구항 20

제 1 항 내지 제 19 항 중 어느 한 항의 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 기록매체.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법 및 이를 기록한 기록매체로써, 특히 이메일 계정의 패스워드를 이용해서 암호화된 이메일을 전송하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법 및 이를 기록한 기록매체에 관한 것이다.

배 경 기 술

<2> 이메일은 오늘날 많은 사람들이 사용하는 수많은 통신수단 가운데 하나이다. 이메일은 컴퓨터를 이용해서 뿐 아니라 휴대하고 다니는 모바일기기를 이용해서도 언제 어디서나 전송 가능하고 확인 가능하다. 실제로 이러한 요구에 맞추어 모바일 이메일 서비스를 제공하고 있다.

<3> 이메일 전송 시스템이 이메일을 인터넷과 같은 안전하지 않은 통신로를 통해 전송할 경우, 허가되지 않은 수신 단말기도 이메일 내용을 쉽게 변경하거나 열어볼 수 있다. 이러한 문제를 해결하기 위하여 이메일 메시지를 암호 알고리즘을 이용하여 암호화하게 된다. 이메일의 기밀성뿐 아니라 전자우편의 전방향 안전성 (forward securecy)에 대한 연구도 활발히 이뤄지고 있다. 전방향 안전성을 제공하는 이메일 시스템이란 이메일 사용자들과 이메일 서버들의 비밀키 (long-term key)가 노출되었을 경우에도 비밀키 노출 시점 이전에 이메일 사용자가 전송한 이메일 메시지에 대한 내용을 알 수 없음을 의미한다.

<4> 종래에 전방향 안전성을 제공하는 암호화된 이메일 전송을 위한 기술들이 있다. 이러한 기술들에서는 암호화된 이메일 서비스를 이용하기 위해서 이메일 사용자가 공개키 인증서를 발급받아야 한다. 그리고 사용자 측에서는 상대방의 공개키 인증서의 유효성 판단을 하기 위해 인증서 검증 절차를 거치게 된다.

<5> 따라서 사용자가 인증서 발급 기관에 가서 인증서를 발급받아야 하는 번거로움이 있으며, 암호화된 이메일을 전송하고 수신받기 위해서 사용자 측에서 인증서 검증 연산(공개키 서명검증)을 수행해야 하기 때문에 효율성 측면에서 개선이 요구되는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<6> 따라서, 본 발명이 해결하고자 하는 첫 번째 과제는 송신자가 전송하고자 하는 이메일 메시지를 암호화하여 송신 메일 서버와 수신 메일 서버를 거쳐 수신자의 수신 단말에 안전하게 전송할 수 있도록 하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 제공하는 것이다.

<7> 본 발명이 해결하고자 하는 두 번째 과제는 상기 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 컴퓨터에서 수행할 수 있도록 프로그램을 기록된 기록매체를 제공하는 것이다.

과제 해결수단

<8> 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<9> 이메일 메시지를 전송하고자 하는 송신 단말기에서 수신 메일 서버와 제 1 세션키를 미리 공유한 송신 메일 서버에 로그인하면, 상기 송신 단말기에서 선택된 제 1 난수와 상기 송신 메일 서버에서 선택된 제 2 난수를 이용하여 상기 송신 단말기와 상기 송신 메일 서버간에 공유되는 제 1 암호키를 각각 생성하고 상기 제 1 암호키를 공유하는 단계; 상기 송신 단말기에서 제 3 난수를 선택하고, 상기 선택된 제 3 난수에 따라 생성된 제 2 세션키를 이용하여 상기 송신 단말기에서 전송하고자 하는 이메일 메시지를 암호화한 제 1 암호문 및 상기 제 1 암호키를 이용하여 상기 제 2 세션키를 암호화한 제 2 암호문을 상기 송신 메일 서버에 전송하는 단계; 상기 송신

메일 서버에서 상기 제 1 암호키를 이용하여 상기 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 제 1 세션키를 이용하여 상기 제 2 세션키를 암호화하여 변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 변형 제 2 암호문을 수신 메일 서버에 전송하는 단계; 상기 수신 메일 서버에서 상기 제 1 세션키를 이용하여 상기 변형 제 2 암호문으로부터 상기 제 2 세션키를 복호하는 단계; 수신 단말기가 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기와 상기 수신 메일 서버 간의 제 2 암호키를 각각 생성하고, 상기 수신 단말기와 상기 수신 메일 서버에서 상기 제 2 암호키를 공유하는 단계; 상기 수신 메일 서버에서 상기 제 2 암호키를 이용하여 상기 제 2 세션키를 암호화하여 재변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 재변형 제 2 암호문을 상기 수신 단말기에 전송하는 단계; 및 상기 수신 단말기에서 상기 제 2 암호키를 이용하여 상기 재변형 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 복호된 상기 제 2 세션키를 이용하여 상기 제 1 암호문으로부터 상기 이메일 메시지를 복호하는 단계를 포함하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 제공한다.

<10> 한편, 상기 제 1 암호키를 공유하는 단계는 상기 송신 단말기에서 선택된 제 1 난수에 따라 생성된 송신 단말 메시지를 송신 메일 서버로 전송하고, 상기 송신 메일 서버에서 선택된 제 2 난수에 따라 생성된 송신 메일 서버 메시지를 상기 송신 단말기에 전송하는 단계; 상기 송신 단말기에서 상기 송신 메일 서버 메시지를 이용하여 제 1 공유 메시지 인증 코드키를 생성하고, 상기 제 1 공유 메시지 인증 코드키를 이용하여 송신 단말기의 메시지 인증 코드값을 생성하여 상기 송신 메일 서버에 전송하는 단계; 상기 송신 메일 서버에서 상기 송신 단말 메시지를 이용하여 상기 제 1 공유 메시지 인증 코드키를 생성하고, 상기 제 1 공유 메시지 인증 코드키를 이용하여 상기 송신 메일 서버의 메시지 인증 코드값을 생성하여 상기 송신 단말기에 전송하는 단계; 상기 송신 단말기에서 상기 제 1 공유 메시지 인증 코드키를 이용하여 상기 송신 메일 서버의 메시지 인증 코드값을 검증한 후, 상기 송신 메일 서버 메시지를 이용하여 제 1 암호키를 생성하는 단계; 및 상기 송신 메일 서버에서 상기 제 1 공유 메시지 인증 코드키를 이용하여 상기 송신 단말기의 메시지 인증 코드값을 검증한 후, 상기 송신 단말 메시지를 이용하여 상기 제 1 암호키를 생성하는 단계를 포함하는 것을 특징으로 한다.

<11> 그리고, 상기 제 2 암호키를 공유하는 단계는 상기 수신 단말기에서 선택된 수신 단말 난수에 따라 생성된 수신 단말 메시지를 상기 수신 메일 서버로 전송하고, 상기 수신 메일 서버에서 선택된 수신 메일 서버 난수에 따라 생성된 수신 메일 서버 메시지를 상기 수신 단말기에 전송하는 단계; 상기 수신 단말기에서 상기 수신 메일 서버 메시지를 이용하여 제 2 공유 메시지 인증 코드키를 생성하고, 상기 제 2 공유 메시지 인증 코드키를 이용하여 수신 단말기의 메시지 인증 코드값을 생성하여 상기 수신 메일 서버에 전송하는 단계; 상기 수신 메일 서버에서 상기 수신 단말 메시지를 이용하여 상기 제 2 공유 메시지 인증 코드키를 생성하고, 상기 제 2 공유 메시지 인증 코드키를 이용하여 상기 수신 메일 서버의 메시지 인증 코드값을 생성하여 상기 수신 단말기에 전송하는 단계; 상기 수신 단말기에서 상기 제 2 공유 메시지 인증 코드키를 이용하여 상기 수신 메일 서버의 메시지 인증 코드값을 검증한 후, 상기 수신 메일 서버 메시지를 이용하여 제 2 암호키를 생성하는 단계; 및 상기 수신 메일 서버에서 상기 제 2 공유 메시지 인증 코드키를 이용하여 상기 수신 단말기의 메시지 인증 코드값을 검증한 후, 상기 수신 단말 메시지를 이용하여 상기 제 2 암호키를 생성하는 단계를 포함하는 것을 특징으로 한다.

<12> 한편, 상기 송신 단말 메시지 X_A는 상기 제 1 난수가 x_A이고, 오더(order)가 q 인 유한 순환군의 서로 다른 두 개의 생성자가 g_1, g_2이고, 상기 송신 단말기의 아이디가 A 이고, 송신 메일 서버의 아이디가 S_A 이고, 상기 송신 단말기의 패스워드가 pw_A이고, $H()$는 해쉬함수이고, p는 $2q+1=p$를 만족하는 소수일때, 수학식 $X_A = g_1^{x_A} g_2^{H(A\|S_A\|pw_A)} \bmod p$ 에 의해 생성되는 것을 특징으로 한다.

<13> 그리고, 상기 송신 메일 서버 메시지 X_{S_A}는 g_1, g_2는 오더가 q인 유한 순환군의 서로 다른 두 개의 생성자이고, y_A는 상기 송신 메일 서버에서 생성된 제 2 난수이고, A는 상기 송신 단말기의 아이디이고, S_A는 상기 송신 메일 서버의 아이디이고, pw_A는 상기 송신 단말기의 패스워드이고, $H()$는 해쉬 함수이며, p는 $2q+1=p$를 만족하는 소수일 때, 수학식 $X_{S_A} = g_1^{y_A} g_2^{H(A\|S_A\|pw_A)} \bmod p$ 에 의해 결정되는 것을

특징으로 한다.

<14> 그리고, 상기 제 1 공유 메시지 인증 코드키는 X_{S_A}는 송신 메일 서버 메시지이고, g_1, g_2는 오더가 q인 유한 순환군의 생성자이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, pw_A는 송신 단말기의 패스워드이고, $H()$는 해쉬 함수이며, x_A가 상기 제 1 난수이고, y_A가 상기 제 2 난수일 때, 수학식 $k_A=\left(X_{S_A}/g_2^{H(A\|S_A\|pw_A)}\right)^{x_A}=g_1^{x_A y_A}$ 에 의해 생성되는 것을 특징으로 한다.

<15> 또한, 상기 송신 단말기의 메시지 인증 코드값 τ_A는 $Mac.G$가 메시지 인증 코드값 생성 함수이고, k_A가 상기 제 1 공유 메시지 인증 코드키이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, X_A는 송신 단말 메시지이고, X_{S_A}는 송신 메일 서버 메시지일 때, 수학식 $\tau_A=Mac.G_{k_A}(A\|S_A\|X_A\|X_{S_A})$에 의해 생성되는 것을 특징으로 한다.

<16> 그리고, 상기 송신 메일 서버의 메시지 인증 코드값 τ_{S_A}는 수학식 $\tau_{S_A}=Mac.G_{k_A}(S_A\|A\|X_A\|X_{S_A})$에 의해 생성되는 것을 특징으로 한다.

<17> 아울러, 상기 제 2 세션키 SK는 $H()$는 해쉬 함수이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, sid는 세션 아이디이며 $sid=X_A\|X_{S_A}\|\tau_A\|\tau_{S_A}$에 의해 연산되고, sk는 제 3 난수일 때, 수학식 $SK=H(A\|S_A\|sid\|sk)$에 의해 생성되는 것을 특징으로 한다.

<18> 여기서, 상기 제 1 암호키를 생성하는 단계는 상기 제 1 공유 메시지 인증 코드키 k_A를 이용하여 상기 송신 메일 서버의 메시지 인증 코드값 τ_{S_A}가 $Check\ Mac.V_{k_A}(\tau_{S_A})$이 '1'의 값을 출력하는 지의 여부에 따라 검증하되, '1'의 값이 출력되면 상기 송신 메일 서버로부터 전송된 송신 메일 서버 메시지 X_{S_A}를 유효한 메시지 인증 코드값으로 판단하고, '0'의 값이 출력되면 유효하지 않은 메시지 인증 코드값으로 판단하여 전송된 송신 메일 서버 메시지 X_{S_A}를 버리는 단계를 포함하는 것을 특징으로 한다.

<19> 한편, 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<20> 송신 단말기에서 송신 단말 일회용 공개키와 송신 단말 비밀키로 이루어진 송신 단말 데이터 쌍을 저장하고, 송신 메일 서버에서 송신 단말 아이디 및 상기 송신 단말 일회용 공개키로 이루어진 송신 메일 서버 데이터 쌍을 메일 서버 리스트에 저장하며, 수신 단말기에서 수신 단말 일회용 공개키와 수신 단말 비밀키로 이루어진 수신 단말 데이터 쌍을 저장하고, 수신 메일 서버에서 수신 단말기의 아이디 및 수신 단말 일회용 공개키로 이루어진 수신 메일 서버 데이터 쌍을 메일 서버 리스트에 미리 저장하는 단계; 이메일 메시지를 전송하고자 하는 상기 송신 단말기에서 상기 수신 메일 서버와 제 1 세션키를 미리 공유한 상기 송신 메일 서버에 로그인하면, 상기 송신 단말기에서 선택된 제 1 난수와 상기 송신 메일 서버에서 선택된 제 2 난수를 이용하여 상기 송신 단말기와 상기 송신 메일 서버간에 공유되는 제 1 암호키를 각각 생성하고 상기 제 1 암호키를 공유하는 단계; 상기 수신 메일 서버에서 상기 송신 메일 서버와 미리 공유한 제 1 세션키 및 상기 수신 메일 서버 리스트에 저장된 수신 단말 일회용 공개키를 이용하여 수신 서버 암호문을 생성하여 상기 송신 메일 서버에 전송하는 단계; 상기 송신 메일 서버에서 상기 수신 서버 암호문으로부터 상기 수신 단말 일회용 공개키를 복호하고, 상기 복호된 수신 단말 일회용 공개키 및 상기 제 1 암호키를 이용하여 송신 서버 암호문을 생성하여 상기 송신 단말기에 전송하는 단계; 상기 송신 단말기에서 상기 제 1 암호키를 이용하여 제 1 암호문을 생성하여 상기 송신 메일 서버로

상기 제 1 암호문을 전송하는 단계; 상기 송신 메일 서버에서 상기 제 1 암호키를 이용하여 상기 제 1 암호문으로부터 상기 송신 단말 암호문을 복호한 후, 복호된 상기 송신 단말 암호문에 상기 제 1 세션키를 이용하여 제 2 암호문을 생성하여 상기 수신 메일 서버에 전송하는 단계; 상기 수신 메일 서버에서 상기 제 1 세션키를 이용하여 상기 제 2 암호문으로부터 상기 송신 단말 암호문을 복호하는 단계; 상기 수신 단말기에서 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기와 상기 수신 메일 서버에서 제 2 암호키를 생성하여 상기 수신 단말기 및 상기 수신 메일 서버에서 공유하는 단계; 상기 수신 메일 서버에서 상기 제 2 암호키를 이용하여 상기 송신 단말 암호문을 암호화하여 제 3 암호문을 생성하여 상기 수신 단말기에 전송하는 단계; 및 상기 수신 단말기에서 상기 제 2 암호키를 이용하여 상기 제 3 암호문으로부터 상기 송신 단말 암호문을 복호하고, 복호된 상기 송신 단말 암호문으로부터 상기 수신 단말 비밀키를 이용하여 상기 이메일 메시지를 복호하는 단계를 포함하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 제공한다.

<21> 여기서, 상기 송신 메일 서버로 상기 제 1 암호문을 전송하는 단계는 상기 송신 서버 암호문으로부터 상기 수신 단말 일회용 공개키를 복호하고, 상기 복호된 수신 단말 일회용 공개키를 이용하여 상기 이메일 메시지를 암호화하여 송신 단말 암호문을 생성하고, 상기 송신 단말 암호문에 상기 제 1 암호키를 이용하여 제 1 암호문을 생성하는 단계를 포함하는 것을 특징으로 한다.

<22> 그리고, 상기 이메일 메시지를 복호하는 단계는 상기 수신 단말기에서 상기 수신 단말 일회용 공개키와 수신 단말 비밀키를 갱신하는 단계를 더 포함하는 것을 특징으로 한다.

<23> 한편, 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<24> 송신 단말기에서 제 1 난수를 생성하고, 송신 메일 서버에서 상기 송신 단말기의 아이디 및 상기 송신 메일 서버에서 생성한 생성자에 상기 제 1 난수를 지수승한 송신 메일 서버의 메시지로 이루어진 데이터 쌍을 송신 메일 서버 리스트에 저장하고, 수신 단말기에서 제 2 난수를 생성하고, 수신 메일 서버에서 상기 수신 단말기의 아이디 및 상기 수신 메일 서버에서 생성한 생성자에 상기 제 2 난수를 지수승한 수신 메일 서버의 메시지로 이루어진 데이터 쌍을 수신 메일 서버 리스트에 저장하는 단계; 이메일 메시지를 전송하고자 하는 상기 송신 단말기에서 상기 송신 메일 서버와 로그인 프로토콜을 수행하여 생성된 제 1 암호키를 상호 공유하는 단계; 상기 송신 메일 서버에서 수신 메일 서버와 키 교환 프로토콜을 수행하여 제 1 세션키를 상호 공유하고, 상기 수신 메일 서버에서 상기 수신 메일 서버의 메시지 및 상기 제 1 세션키를 이용하여 상기 수신 메일 서버의 메시지를 암호화한 수신 메일 서버의 메시지 인증 코드값을 상기 송신 메일 서버로 전송하는 단계; 상기 송신 메일 서버에서 상기 수신 메일 서버의 메시지 인증 코드값이 유효한 지의 여부를 검증하고, 상기 송신 메일 서버에서 수신 메일 서버의 메시지, 상기 제 1 암호키를 이용하여 상기 수신 메일 서버의 메시지를 암호화한 송신 메일 서버의 제 1 메시지 인증 코드값을 상기 수신 단말기에 전송하는 단계; 상기 송신 단말기에서 상기 송신 메일 서버로부터 전송된 상기 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한지의 여부를 판단하고, 제 3 난수를 선택하여 생성된 송신 단말 메시지 및 상기 송신 단말 메시지 및 상기 제 2 난수를 이용하여 생성된 제 2 세션키를 연산하는 단계; 상기 송신 단말기에서 상기 제 2 세션키로 상기 이메일 메시지를 암호화한 암호문, 상기 송신 단말 메시지, 및 상기 제 1 암호키를 이용하여 상기 송신 단말 메시지를 암호화한 송신 단말의 메시지 인증 코드값을 상기 송신 메일 서버로 전송하는 단계; 상기 송신 메일 서버에서 상기 송신 단말기로부터 전송된 송신 단말의 메시지 인증 코드값이 유효한지의 여부를 판단하고, 상기 송신 메일 서버에서 상기 암호문, 상기 송신 단말 메시지 및 상기 제 1 세션키로 상기 송신 단말 메시지를 암호화한 송신 메일 서버의 제 2 메시지 인증 코드값을 상기 수신 메일 서버로 전송하는 단계; 상기 수신 메일 서버에서 상기 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 지의 여부를 판단하고, 상기 수신 메일 서버에서 상기 암호문 및 상기 송신 단말 메시지를 저장하는 단계; 상기 수신 단말기가 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기 및 상기 수신 메일 서버에서 로그인 프로토콜을 수행하여 제 2 암호키를 공유하는 단계; 상기 수신 메일 서버에서 상기 송신 단말기의 아이디, 상기 암호문, 상기 송신 단말 메시지 및 상기 제 2 암호키로 상기 송신 단말 메시지를 암호화한 수신 단말의 메시지 인증 코드값을 상기 수신 단말기에 전송하는 단계; 및 상기 수신 단말기에서 상기 수신 단말의 메시지 인증 코드값이 유효한지의 여부를 판단하고, 상기 제 2 난수를 이용하여 상기 제 2 세션키를 추출하고, 상기 제 2 세션키를 이용하여 상기 암호문으로부터 상기 이메일 메시지를 추출하는 단계를 포함하는 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 제공한다.

<25> 한편, 상기 수신 메일 서버의 메시지 인증 코드값이 유효한 지의 여부는 상기 제 1 세션키 k_{SS}를 이용하여 상기 수신 메일 서버의 메시지 인증 코드값 τ_1이 유효한지의 여부를 $Check\ Mac\ V_{k_{SS}}(\tau_1)$에 의해 검

증하며, 검증값이 '1'이 출력되면 수신 메일 서버의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어, 수신된 수신 메일 서버의 메시지 인증 코드값을 버리는 것을 특징으로 한다.

<26> 그리고, 상기 송신 메일 서버로부터 전송된 상기 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한지의 여부는 상기 제 1 암호키 K_A를 이용하여 상기 송신 메일 서버의 제 1 메시지 인증 코드값 τ_2이 유효한지의 여부를 $Check\ Mac\ V_{K_A}(\tau_2)$에 의해 검증하며, 검증값이 '1'이 출력되면 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어 수신된 송신 메일 서버의 제 1 메시지 인증 코드값을 버리는 것을 특징으로 한다.

<27> 또한, 상기 송신 단말의 메시지 인증 코드값이 유효한지의 여부는 상기 제 1 암호키 K_A를 이용하여 상기 송신 단말의 메시지 인증 코드값 τ_3가 유효한지의 여부를 $Check\ Mac\ V_{K_A}(\tau_3)$에 의해 검증하며, 검증값이 '1'이 출력되면 상기 송신 단말의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어 수신된 상기 송신 단말의 메시지 인증 코드값을 버리는 것을 특징으로 한다.

<28> 여기서, 상기 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 지의 여부는 상기 제 1 세션키 k_{SS}를 이용하여 상기 송신 메일 서버의 제 2 메시지 인증 코드값 τ_4가 유효한지의 여부를 $Check\ Mac\ V_{k_{SS}}(\tau_4)$에 의해 검증하며, 검증값이 '1'이 출력되면 상기 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어, 수신된 상기 송신 메일 서버의 제 2 메시지 인증 코드값을 버리는 것을 특징으로 한다.

<29> 아울러, 상기 수신 단말의 메시지 인증 코드값이 유효한지의 여부는 상기 제 2 비밀키 K_B를 이용하여 상기 수신 단말의 메시지 인증 코드값 τ_5가 유효한지의 여부를 $Check\ Mac\ V_{K_B}(\tau_5)$에 의해 검증하며, 검증값이 '1'이 출력되면 상기 수신 단말의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 유효하지 않은 것으로 판단되어, 수신된 상기 수신 단말의 메시지 인증 코드값을 버리는 것을 특징으로 한다.

<30> 상기 두 번째 과제를 해결하기 위하여 본 발명은 상기 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 기록매체를 제공하는 것이다.

효 과

<31> 본 발명에 의하면, 사용자의 패스워드 또는 메일 서버의 비밀키가 노출된 경우에도 공개키 인증서의 필요 없이 이메일 계정의 패스워드만을 이용하여 이메일 메시지의 기밀성과 전방향 안전성을 제공하는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<32> 이하, 본 발명의 바람직한 실시예를 첨부도면에 의거하여 상세히 설명하기로 한다.

<33> 그러나, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형할 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다. 본 발명의 실시예는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공된다.

<34> 본 발명의 설명에서 A는 송신 메일 서버 S_A에 아이디 ID_A(이하, 'A'라고 함.) 및 패스워드 pw_A로 이루어진 메일 계정 $(ID_A=A, pw_A)$을 등록한 송신 단말기이고, B는 수신 메일 서버 S_B에 아이디 ID_B(이하, 'B'라고 함.)및 패스워드 pw_B로 이루어진 메일 계정 $(ID_B=B, pw_B)$를 등록한 수신 단말기이

다. 송신 메일 서버 S_A와 수신 메일 서버 S_B는 서로 다른 메일 서버이다.

<35> 본 발명은 사용자의 송신 단말기 A를 통한 로그인 단계(Login phase of A), 송신 단말기 A의 암호화된 메시지 발송단계(Sending phase of A), 그리고 수신 단말기 B의 수신단계(Receiving phase of B)로 구성된다. 본 발명에서 사용되는 수식의 표기는 다음과 같다.

표 1

기 호	내 용
G	order가 q인 유한 순환군
g_1, g_2	유한 순환군 G의 서로 다른 두 개의 생성자
$Mac = (Mac.K, Mac.G, Mac.V)$	메시지 인증 코드(Message Authentication Code : MAC)에 따른 MAC 키 생성 방법으로, $Mac.K$는 맥 키인 k_{mac}를 생성하고, $Mac.G$는 맥 키 k_{mac}을 이용하여 메시지 M의 메시지 MAC 값인 τ를 생성하며, $Mac.V$는 맥 키 k_{mac}을 이용하여 메시지에 대한 MAC 값이 유효한지의 여부를 검증한다. 만약, MAC 값이 유효하면 1을 출력하고, 그렇지 않을 경우 0을 출력한다.
$SE = (K, E, D)$	대칭키 암호 생성 방법으로, K는 암호키 K_{enc}를 생성한다. E는 암호키 K_{enc}를 이용하여 메시지 M을 암호화 하여 암호문 Z를 생성한다. D는 암호문 Z를 암호키 K_{enc}를 이용하여 복호한다.
$PE = (PK, PE, PD)$	공개키 암호 생성 방법으로 PK는 공개키와 개인키 쌍 (y, x)를 생성한다. PE는 y를 이용하여 메시지 M을 암호화하여 암호문 Z를 생성한다. PD는 암호문 Z를 x를 이용하여 복호한다.
$H()$	해쉬 함수, $H: \{0,1\}^* \rightarrow \{0,1\}^l$
$F_{K'}$	암호키 K를 이용한 의사 난수 함수

<36>

<37> 도 1은 본 발명의 제1 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에 대한 흐름도이다.

<38> 도 1을 참조하면 우선, 이메일 메시지를 전송하고자 하는 송신 단말기에서 수신 메일 서버와 제 1 세션키를 미리 공유한 송신 메일 서버에 로그인하면, 상기 송신 단말기에서 선택된 제 1 난수와 상기 송신 메일 서버에서 선택된 제 2 난수를 이용하여 상기 송신 단말기와 상기 송신 메일 서버간에 공유되는 제 1 암호키를 각각 생성하고 상기 제 1 암호키를 공유한다(S110).

<39> 그 다음, 상기 송신 단말기에서 제 3 난수를 선택하고, 상기 선택된 제 3 난수에 따라 생성된 제 2 세션키를 이용하여 상기 송신 단말기에서 전송하고자 하는 이메일 메시지를 암호화한 제 1 암호문 및 상기 제 1 암호키를 이용하여 상기 제 2 세션키를 암호화한 제 2 암호문을 상기 송신 메일 서버에 전송한다(S120).

<40> 그 다음, 상기 송신 메일 서버에서 상기 제 1 암호키를 이용하여 상기 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 제 1 세션키를 이용하여 상기 제 2 세션키를 암호화하여 변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 변형 제 2 암호문을 수신 메일 서버에 전송한다(S130).

<41> 그 다음, 상기 수신 메일 서버에서 상기 제 1 세션키를 이용하여 상기 변형 제 2 암호문으로부터 상기 제 2 세션키를 복호한다(S140).

<42> 그 다음, 수신 단말기가 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기와 상기 수신 메일 서버 간의 제 2 암호키를 각각 생성하고, 상기 수신 단말기와 상기 수신 메일 서버에서 상기 제 2 암호키를 공유한다(S150).

<43> 그 다음, 상기 수신 메일 서버에서 상기 제 2 암호키를 이용하여 상기 제 2 세션키를 암호화하여 재변형 제 2 암호문을 생성하고, 상기 제 1 암호문 및 상기 재변형 제 2 암호문을 상기 수신 단말기에 전송한다(S160).

<44> 마지막으로, 상기 수신 단말기에서 상기 제 2 암호키를 이용하여 상기 재변형 제 2 암호문으로부터 상기 제 2 세션키를 복호하고, 상기 복호된 상기 제 2 세션키를 이용하여 상기 제 1 암호문으로부터 상기 이메일 메시지를 복호한다(S170).

<45> 도 2은 도 1의 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에서의 데이터 흐름을 도시한 것이다.

<46> 이하, 도 1 및 도 2를 참조하여 본 발명의 제1 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 더욱 상세히 설명하기로 한다.

<47> 송신 단말기 A의 로그인 단계(Login phase of A)에서 송신 단말기 A가 송신 메일 서버 S_A에 로그인하기 위해서 송신 단말기 A와 송신 메일 서버 S_A는 다음 프로토콜을 수행한다.

<48> 우선, 송신 단말기 A는 임의의 제 1 난수 x_A를 선택한다. 송신 단말기 A는 상기 선택된 임의의 제 1 난수 x_A를 이용하여 하기의 수학식 1에 의해 송신 단말 메시지 X_A를 송신 메일 서버 S_A로 전송한다.

수학식 1

<49> $$X_A = g_1^{x_A} g_2^{H(A||S_A||pw_A)} \bmod p$$

<50> 여기서, g_1, g_2는 오더가 q인 유한 순환군의 서로 다른 두 개의 생성자이고, x_A는 송신 단말기 A에서 선택된 제 1 난수이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, pw_A는 송신 단말기 A의 패스워드이고, $H()$는 해쉬 함수이며, p는 상기 $2q+1=p$를 만족하는 소수이다.

<51> 한편, 송신 메일 서버 S_A는 수신된 송신 단말 메시지 X_A를 저장하고, 마찬가지로 송신 메일 서버 S_A에서 선택된 임의의 제 2 난수 y_A를 이용하여 하기의 수학식 2에 의해 연산되는 송신 메일 서버 메시지 X_{S_A}를 송신 단말기 A에게 전송한다.

수학식 2

<52> $$X_{S_A} = g_1^{y_A} g_2^{H(A||S_A||pw_A)} \bmod p$$

<53> 여기서, g_1, g_2는 오더가 q인 유한 순환군의 서로 다른 두 개의 생성자이고, y_A는 송신 메일 서버에서 생성된 제 2 난수이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, pw_A는 송신 단말기 A의 패스워드이고, $H()$는 해쉬 함수이며, p는 $2q+1=p$를 만족하는 소수이다.

<54> 한편, 송신 단말기 A는 송신 메일 서버 메시지 X_{S_A}를 수신한 후, 수신한 송신 메일 서버 메시지 X_{S_A}를 이용하여 하기의 수학식 3에 의해 연산되는 송신 단말기 A와 송신 메일 서버 S_A가 공유하는 제 1 공유 메시지 인증 코드(MAC) 키 k_A를 연산한다.

수학식 3

<55> $$k_A = \left(X_{S_A} / g_2^{H(A||S_A||pw_A)}\right)^{x_A} = g_1^{x_A y_A}$$

<56> 여기서, X_{S_A}는 상기 수학식 2에 의해 얻어진 송신 메일 서버 메시지이고, g_1, g_2는 오더가 q인 유한 순

환군의 생성자이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, pw_A는 송신 단말기 A의 패스워드이고, $H()$는 해쉬 함수이다.

<57> 이와 같이, 송신 단말기 A는 상기 수학식 3에 따라 연산된 제 1 공유 메시지 인증 코드(MAC) 키 k_A를 이용하여 하기의 수학식 4에 의해 송신 단말기의 메시지 인증 코드값 τ_A를 송신 메일 서버 S_A에게 전송한다.

수학식 4

<58> $$\tau_A=Mac.G_{k_A}(A||S_A||X_A||X_{S_A})$$

<59> 이와 같이, $Mac.G$는 상기 연산된 제 1 공유 메시지 인증 코드키 k_A를 사용하여 송신 단말기의 메시지 인증 코드값 τ_A를 생성하는데, 상기 수학식 4에서 A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, X_A는 수학식 1에 의해 얻어진 송신 단말 메시지이고, X_{S_A}는 수학식 2에 의해 얻어진 송신 메일 서버 메시지이다.

<60> 그리고, 송신 메일 서버 S_A도 마찬가지 방법으로 하기의 수학식 5에 의해 연산되는 제 1 공유 메시지 인증 코드키인 k_A를 계산한 후 하기의 수학식 6에 의해 연산되는 송신 메일 서버의 메시지 인증 코드값인 τ_{S_A}를 송신 단말기 A에게 전송한다.

수학식 5

<61> $$k_A=g_1^{x_A y_A}$$

<62> 여기서, g_1은 오더가 q인 유한 순환군의 생성자이고, x_A는 A에 의해 선택된 제 1 난수이고, y_A는 송신 메일 서버 S_A에 의해 선택된 제 2 난수이다.

수학식 6

<63> $$\tau_{S_A}=Mac.G_{k_A}(S_A||A||X_A||X_{S_A})$$

<64> 여기서, $Mac.G$는 제 1 공유 메시지 인증 코드키 k_A를 사용하여 송신 메일 서버의 메시지 인증 코드값 τ_{S_A}를 생성하고, S_A는 송신 메일 서버이고, A는 송신 단말기의 아이디이고, X_A는 수학식 1에 의해 얻어진 송신 단말 메시지이고, X_{S_A}는 수학식 2에 의해 얻어진 송신 메일 서버 메시지이다.

<65> 한편, 송신 단말기 A는 송신 메일 서버로부터 전송된 송신 메일 서버 메시지 X_{S_A}가 유효한 메시지 인증 코드값인지를 검증한다.

<66> 여기서, 송신 메일 서버로부터 전송된 송신 메일 서버 메시지 X_{S_A}가 유효한지의 검증은 상기 제 1 공유 메시

지 인증 코드키 k_A를 이용하여 전송된 송신 메일 서버의 메시지 인증 코드값 τ_{S_A}이 $Check\ Mac.V_{k_A}(\tau_{S_A}) = 1$ 인지의 여부를 검증하는데, 여기서 '1'이 출력되면, 송신 메일 서버로부터 전송된 송신 메일 서버 메시지 X_{S_A}가 유효한 메시지 인증 코드값으로 판단하여 중간 과정에서 메시지의 수정이나 변경이 없었음을 의미한다.

<67> 그러나, '0'의 값이 출력되면, 송신 메일 서버로부터 전송된 송신 메일 서버 메시지 X_{S_A}가 중간 과정에서 수정이나 변경이 있었음을 의미하므로 유효하지 않으므로, 전송된 송신 메일 서버 메시지 X_{S_A}를 버리게 된다.

<68> 상기와 같은 과정으로, τ_{S_A}가 유효하면 송신 단말기 A는 하기의 수학식 7에 의해 연산되는 제 1 암호키 K_A를 계산한다.

수학식 7

<69> $$K_A = F_{k_A}(A||S_A||X_A||X_{S_A})$$

<70> 상기 수학식 7에서의 A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, X_A는 수학식 1에 의해 얻어진 송신 단말 메시지이고, X_{S_A}는 수학식 2에 의해 얻어진 송신 메일 서버 메시지이다.

<71> 상기 수학식 7에서 제 1 공유 메시지 인증 코드키 k_A를 의사 난수 함수 F에 적용하여 제 1 암호키 K_A를 생성한다.

<72> 만약 τ_{S_A}가 유효하지 않으면 송신 단말기 A는 프로토콜 수행을 멈춘다.

<73> 한편, 송신 메일 서버 S_A도 송신 메일 서버의 메시지 인증 코드값인 τ_{S_A}가 유효한 메시지 인증 코드값인지를 검증 후에 제 1 암호키 $K_A = F_{k_A}(A||S_A||X_A||X_{S_A})$를 연산하고, 송신 단말기 A와 송신 메일 서버 S_A는 동일한 제 1 암호키를 상호 저장한다.

<74> 상기와 같은 과정에 의해 송신 단말기의 송신 메일 서버로의 로그인 과정이 종료된다.

<75> 그 다음은, 송신 단말기 A의 암호화된 메시지를 발송하는 과정으로, 송신 단말기 A가 이메일 메시지 M을 수신 단말기 B에게 안전하게 전송하기를 원할 경우, 송신 단말기 A, 송신 메일 서버 S_A 그리고 수신 메일 서버 S_B는 다음 프로토콜을 수행한다.

<76> 여기서 송신 메일 서버 S_A와 수신 메일 서버 S_B는 이미 하나의 제 1 세션키 k_{SS}를 안전한 키 교환 프로토콜을 사용하여 교환했다고 가정한다.

<77> 우선, 송신 단말기 A는 임의의 제 3 난수 sk를 선택하고 하기의 수학식 8에 의해 제 2 세션키 SK를 계산한다.

수학식 8

<78> $$SK=H(A||S_A||sid||sk)$$

<79> 여기서, $H()$는 해쉬 함수이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, sid는 세션 아이디이며 $sid=X_A||X_{S_A}||\tau_A||\tau_{S_A}$에 의해 연산되고, sk는 제 3 난수이다.

<80> 한편, 송신 단말기 A는 하기의 수학식 9에 의해 연산되는 Z_1, Z_2를 송신 메일 서버 S_A에게 전송한다.

수학식 9

<81> $$(Z_1=E_{SK}(A||B||M), Z_2=E_{K_A}(A||B||SK))$$

<82> 여기서, E는 대칭키 암호 방법으로 제 2 세션키 SK를 이용하여 제 1 암호문 Z_1을 생성하고, 제 1 암호키 K_A를 이용하여 제 2 암호문 Z_2를 생성하며, 여기서 A는 송신 단말기이고, B는 수신 단말기이고, SK는 세션키이며, M은 이메일 메시지이다.

<83> 그러면, 송신 메일 서버 S_A는 상기 수학식 9에 의해 생성된 Z_1, Z_2를 수신하고, 상기 로그인 과정에서 생성한 제 1 암호키 K_A를 이용하여 Z_2로부터 제 2 세션키 SK를 복호한 후, 하기의 수학식 10에 의해 연산되는 제 1 암호문 Z_1 및 변형 제 2 암호문 Z_2'를 수신 메일 서버 S_B에게 전송한다.

<84> 제 2 암호문 Z_2'를 생성하는 이유는, 상기 제 2 세션키 SK를 미리 저장된 제 1 세션키 k_{SS}를 이용하여 암호화하여 수신 메일 서버로 전송하기 위함이다.

수학식 10

<85> $$(Z_1, Z_2'=E_{k_{SS}}(A||B||SK))$$

<86> 여기서, E는 대칭키 암호화 함수로 제 1 세션키 k_{SS}를 이용하여 제 2 세션키 SK를 암호화하고, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이다.

<87> 그러면, 수신 메일 서버 S_B는 상기의 수학식 10에 의해 연산되는 제 1 암호문 Z_1 및 변형 제 2 암호문 Z_2'를 수신하고, 제 1 세션키 k_{SS}를 사용하여 Z_2'로부터 제 2 세션키 SK를 복호한 후, (A, B, Z_1, SK)를 저장한다.

<88> 한편, 수신 단말기 B의 로그인 단계에서 수신 단말기 B가 수신 메일 서버 S_B에 로그인하기 위해 수신 단말기 B와 수신 메일 서버 S_B는 송신 단말기 A의 로그인 단계와 동일한 프로토콜을 수행한다.

<89> 수신 단말기 B가 성공적으로 수신 메일 서버 S_B에 로그인하면 수신 단말기 B와 수신 메일 서버 S_B는

하기의 수학식 11에 의해 연산되는 제 2 암호키 K_B를 공유하게 된다.

수학식 11

<90> $$K_B = F_{k_B}(B||S_B||X_B||X_{S_B})$$

<91> 여기서, F는 의사 난수 함수이고, 수신 단말기 B와 수신 메일 서버 S_B가 공유하는 제 2 공유 메시지 인증 코드키 k_B를 이용하여 제 2 암호키 K_B를 생성하며, B는 수신 단말기의 아이디이고, S_B는 수신 메일 서버이고, X_B는 수학식 1과 동일한 방법에 의해 얻어진 수신 단말 메시지이고, X_{S_B}는 수학식 2와 동일한 방법에 의해 얻어진 수신 메일 서버 메시지이다.

<92> 한편, 수신 메일 서버 S_B는 하기의 수학식 12에 의해 연산되는 제 1 암호문 Z_1 및 재변형 제 2 암호문 Z_2''를 수신 단말기 B에게 전송한다.

수학식 12

<93> $$(Z_1, Z_2'' = E_{K_B}(A||B||SK))$$

<94> 여기서, E는 대칭키 암호화 함수로 제 2 암호키 K_B를 이용하여 제 2 세션키 SK를 암호화함으로써 재변형 제 2 암호문 Z_2''를 생성하며, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이다.

<95> 그러면, 최종적으로 수신 단말기 B는 제 2 암호키 K_B를 사용하여 재변형 제 2 암호문 Z_2''로부터 SK를 복호한 후, SK를 이용하여 Z_1으로부터 이메일 메시지 M을 복호한다.

<96> 상기의 과정은 이메일 메시지 M은 제 2 세션키 SK로 암호화되어 전송되기 때문에 이메일 메시지 M의 기밀성은 SK의 키 기밀성 (key secrecy)에 기반한다. SK의 키 기밀성은 다시 송신 단말기 A와 송신 메일 서버 S_A (송신 단말기 B와 메일 서버 S_B)가 교환한 암호키 K_A (K_B)와 송신 메일 서버와 수신 메일 서버가 교환한 제 1 세션키 k_{SS}의 키 기밀성에 기반한다. 만약 DDH (Decisional Diffie-Hellman) 문제가 다항식 시간 안에 풀기 어려운 문제이고, F가 안전한 의사 난수 함수라면 K_A (K_B)를 임의의 난수와 구별하는 것은 다항식 시간 내에 풀기 어려운 문제이다. 즉, K_A (K_B)는 키 기밀성을 제공한다. k_{SS}는 두 서버간에 안전한 키 교환 프로토콜에 의해 교환된 세션키 값이므로, k_{SS}는 키 기밀성을 제공한다. 따라서 SK는 임의의 난수와 다항식 시간 안에 구별 불가능한 값이다.

<97> 사용자들의 패스워드 pw_A, pw_B가 노출된 경우, 본 발명은 Diffie-Hellman 키 교환 기법으로 K_A (K_B)가 생성되기 때문에 pw_A, pw_B값들이 노출되기 이전에 생성된 K_A (K_B)의 값을 계산할 수 없다. 따라서 K_A (K_B)를 이용하여 SK가 암호화 되어 전송되므로 SK의 값을 알 수 없고, SK로 암호화되어 전송된 이메일 메시지 M을 복호할 수 없기 때문에 본 발명은 전방향 안전성을 제공한다. 메일 서버들의 암호

키가 노출된 경우에도 본 발명이 전방향 안전성을 제공하려면 제 1 세션키 k_{SS}를 교환하기 위하여 두 메일 서버는 Diffie-Hellman 키 교환 기법의 키교환 프로토콜을 사용하여야 한다.

<98> 도 3은 본 발명의 제 2 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법의 흐름도를 도시한 것이다.

<99> 도 3을 참조하면 우선, 송신 단말기에서 송신 단말 일회용 공개키와 송신 단말 비밀키로 이루어진 송신 단말 데이터 쌍을 저장하고, 송신 메일 서버에서 송신 단말 아이디 및 상기 송신 단말 일회용 공개키로 이루어진 송신 메일 서버 데이터 쌍을 메일 서버 리스트에 저장하며, 수신 단말기에서 수신 단말 일회용 공개키와 수신 단말 비밀키로 이루어진 수신 단말 데이터 쌍을 저장하고, 수신 메일 서버에서 수신 단말기의 아이디 및 수신 단말 일회용 공개키로 이루어진 수신 메일 서버 데이터 쌍을 메일 서버 리스트에 미리 저장한다(S310).

<100> 그 다음, 이메일 메시지를 전송하고자 하는 상기 송신 단말기에서 상기 수신 메일 서버와 제 1 세션키를 미리 공유한 상기 송신 메일 서버에 로그인하면, 상기 송신 단말기에서 선택된 제 1 난수와 상기 송신 메일 서버에서 선택된 제 2 난수를 이용하여 상기 송신 단말기와 상기 송신 메일 서버간에 공유되는 제 1 암호키를 각각 생성하고 상기 제 1 암호키를 공유한다(S320).

<101> 그 다음, 상기 수신 메일 서버에서 상기 송신 메일 서버와 미리 공유한 제 1 세션키 및 상기 수신 메일 서버 리스트에 저장된 수신 단말 일회용 공개키를 이용하여 수신 서버 암호문을 생성하여 상기 송신 메일 서버에 전송한다(S330).

<102> 그 다음, 상기 송신 메일 서버에서 상기 수신 서버 암호문으로부터 상기 수신 단말 일회용 공개키를 복호하고, 상기 복호된 수신 단말 일회용 공개키 및 상기 제 1 암호키를 이용하여 송신 서버 암호문을 생성하여 상기 송신 단말기에 전송한다(S340).

<103> 그 다음, 상기 송신 단말기에서 상기 제 1 암호키를 이용하여 제 1 암호문을 생성하여 상기 송신 메일 서버로 상기 제 1 암호문을 전송한다(S350).

<104> 그 다음, 상기 송신 메일 서버에서 상기 제 1 암호키를 이용하여 상기 제 1 암호문으로부터 상기 송신 단말 암호문을 복호한 후, 복호된 상기 송신 단말 암호문에 상기 제 1 세션키를 이용하여 제 2 암호문을 생성하여 상기 수신 메일 서버에 전송한다(S360).

<105> 그 다음, 상기 수신 메일 서버에서 상기 제 1 세션키를 이용하여 상기 제 2 암호문으로부터 상기 송신 단말 암호문을 복호한다(S370).

<106> 그 다음, 상기 수신 단말기에서 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기와 상기 수신 메일 서버에서 제 2 암호키를 생성하여 상기 수신 단말기 및 상기 수신 메일 서버에서 공유한다(S380).

<107> 그 다음, 상기 수신 메일 서버에서 상기 제 2 암호키를 이용하여 상기 송신 단말 암호문을 암호화하여 제 3 암호문을 생성하여 상기 수신 단말기에 전송한다(S390).

<108> 마지막으로, 상기 수신 단말기에서 상기 제 2 암호키를 이용하여 상기 제 3 암호문으로부터 상기 송신 단말 암호문을 복호하고, 복호된 상기 송신 단말 암호문으로부터 상기 수신 단말 비밀키를 이용하여 상기 이메일 메시지를 복호한다(S391).

<109> 도 4는 도 3의 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에서의 데이터 흐름을 도시한 것이다.

<110> 이하, 도 3 및 도 4를 참조하여 본 발명의 제1 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 더욱 상세히 설명하기로 한다.

<111> 송신 단말기 A는 송신 단말 일회용 공개키와 송신 단말 비밀키 쌍 (y_A, x_A)을 저장하고 있다. 그리고 송신 메일 서버 S_A는 송신 단말기 A와 이전에 프로토콜을 수행한 결과로 송신 단말기의 아이디 및 송신 단말 일회용 공개키의 데이터 쌍인 (A, y_A)를 메일 서버 리스트에 저장하고 있다.

<112> 수신 단말기 B도 수신 단말 일회용 공개키와 수신 단말 비밀키 쌍 (y_B, x_B)을 저장하고 있다. 수신 메일 서

버 S_B는 수신 단말기 B와 이전에 프로토콜을 수행한 결과로 수신 단말기의 아이디 및 수신 단말 일회용 공개키의 데이터 쌍인 (B, y_B)를 수신 메일 서버 리스트에 저장하고 있다.

<113> 송신 단말기 A의 로그인 단계에서 송신 단말기 A가 송신 메일 서버 S_A에 로그인하기 위해서 송신 단말기 A와 송신 메일 서버 S_A는 상기 실시예 1에서와 동일한 로그인 프로토콜을 수행하여 상기 수학식 7에 의해 연산되는 제 1 비밀키 K_A를 교환한다.

<114> 여기서, 본 발명의 제 2 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에 있어서, 로그인 과정(Login phase)은 상기 실시예 1에서 기술된 바와 동일하므로 중복된 설명은 발명의 명확화를 위하여 과감히 생략하기로 한다.

<115> 한편, 로그인 과정이 수행된 후, 송신 단말기 A의 암호화된 메시지를 발송하는 단계(Sending phase of A)에서 송신 단말기 A가 이메일 메시지 M을 수신 단말기 B에게 안전하게 전송하기를 원할 경우, 송신 단말기 A, 송신 메일 서버 S_A 그리고 수신 메일 서버 S_B는 다음 프로토콜을 수행한다.

<116> 여기서, 송신 메일 서버 S_A와 수신 메일 서버 S_B는 이미 하나의 제 1 세션키 k_{SS}를 안전한 키 교환 프로토콜을 사용하여 교환했다고 가정한다.

<117> 수신 메일 서버 S_B는 수신 메일 서버 리스트로부터 수신 단말기의 아이디 및 수신 단말 일회용 공개키의 데이터 쌍인 (B, y_B)를 가져온다.

<118> 그리고, 수신 메일 서버 S_B는 하기의 수학식 13에 의해 연산되는 수신 서버 암호문 Y_B를 송신 메일 서버 S_A에게 전송한다.

수학식 13

<119> $$Y_B = E_{k_{SS}}(S_B || S_A || B || y_B)$$

<120> 여기서, E는 대칭키 암호화 함수로 제 1 세션키 k_{SS}를 이용하여 수신 단말 일회용 공개키 y_B를 암호화하여 수신 서버 암호문 Y_B를 생성하며, S_B는 수신 메일 서버의 아이디이고, S_A는 송신 메일 서버의 아이디이고, B는 수신 단말기의 아이디이다.

<121> 한편, 송신 메일 서버 S_A는 상기 수신 서버 암호문으로부터 수신 단말 일회용 공개키를 복호하고, 하기의 수학식 14에 의해 연산되는 송신 서버 암호문 Y_A를 송신 단말기 A에게 전송한다.

수학식 14

<122> $$Y_A = E_{K_A}(S_A || A || B || y_B)$$

<123> 상기 수학식 14에서, E는 대칭키 암호화 함수로 제 1 암호키 K_A를 이용하여 수신 단말 일회용 공개키 y_B를 암호화하여 송신 서버 암호문 Y_A를 생성하는데, S_A는 송신 메일 서버의 아이디이고, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이다.

<124> 그 다음, 송신 단말기 A는 제 1 암호키 K_A를 이용하여 송신 서버 암호문 Y_A로부터 수신 단말 일회용 공개키 y_B를 복호화한 후, 하기의 수학식 15에 의해 송신 단말 암호문 Z를 연산한다.

수학식 15

$$Z=PE_{y_B}(A||B||y_B||M)$$

<125>

<126> 여기서, PE는 공개키 암호화 함수로 수신 단말 일회용 공개키 y_B를 이용하여 이메일 메시지 M을 암호화하는데, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이다.

<127> 이와 같이, 송신 단말기 A는 하기의 수학식 16과 같이, 메일 메시지 M을 암호화한 송신 단말 암호문 Z에 제 1 암호키 K_A를 이용하여 제 1 암호문 Z_1을 생성하고, 생성된 제 1 암호문 Z_1을 송신 메일 서버 S_A에게 전송한다.

수학식 16

$$Z_1=E_{K_A}(A||B||Z)$$

<128>

<129> 여기서, E는 대칭키 암호화 함수이고, K_A는 제 1 암호키이며, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이고, Z는 수학식 15에 의해 연산된 송신 단말 암호문이다.

<130> 이와 같이, 송신 메일 서버 S_A는 제 1 암호키 K_A를 이용하여 제 1 암호문 Z_1으로부터 송신 단말 암호문 Z를 복호한 후, 하기의 수학식 17에 따라 복호화된 송신 단말 암호문 Z에 제 1 세션키 k_{SS}를 이용하여 제 2 암호문 Z_2를 생성하고, 생성된 제 2 암호문 Z_2를 수신 메일 서버 S_B에게 전송한다.

수학식 17

$$Z_2=E_{k_{ss}}(S_A||S_B||Z)$$

<131>

<132> 여기서, E는 대칭키 암호화 함수로 제 1 세션키 k_{SS}를 이용하여 송신 단말 암호문 Z를 암호화하고, S_A는 송신 메일 서버의 아이디이고, S_B는 수신 메일 서버의 아이디이다.

<133> 그러면, 수신 메일 서버 S_B는 제 1 세션키 k_{SS}를 사용하여 제 2 암호문 Z_2로부터 송신 단말 암호문 Z를 복호화 한다.

<134> 한편, 수신 단말기 B의 로그인 단계에서 수신 단말기 B가 수신 메일 서버 S_B에 로그인하기 위하여 수신 단말기 B와 수신 메일 서버 S_B는 송신 단말기 A의 로그인 단계와 동일한 프로토콜을 수행한다.

<135> 수신 단말기 B가 성공적으로 수신 메일 서버 S_B에 로그인하면 수신 단말기 B와 수신 메일 서버 S_B는 하기의 수학식 18에 의해 연산되는 제 2 암호키 K_B를 공유하게 된다.

수학식 18

<136> $$K_B=F_{k_B}(B||S_B||X_B||X_{S_B})$$

<137> 여기서 F는 의사 난수 함수이고, B는 수신 단말기의 아이디이고, S_B는 수신 메일 서버의 아이디이고, X_B는 수학식 1과 동일한 방법에 의해 얻어진 수신 단말 메시지이고, X_{S_B}는 수학식 2와 동일한 방법에 의해 얻어진 수신 메일 서버 메시지이다.

<138> 즉, 수신 단말기 B와 수신 메일 서버 S_B는 상호 공유하는 제 2 공유 메시지 인증 코드키 k_B를 이용하여 제 2 암호키 K_B를 생성하는 것이다.

<139> 그러면, 수신 메일 서버 S_B는 상기 전송된 송신 단말 암호문 Z를 상기 생성된 제 2 암호키 K_B를 대칭키 암호화 함수 E를 이용하여 $E_{k_B}(Z)$에 따라 암호화하여 제 3 암호문 Z_3를 생성한 후, (A, B, Z_3)를 저장한다.

<140> 그 다음, 이메일 메시지의 수신 단계에서 수신 메일 서버 S_B는 상기 제 3 암호문 Z_3를 수신 단말기 B에게 전송한다.

<141> 수신 단말기 B는 저장되어 있는 제 2 암호키 K_B를 이용하여 상기 제 3 암호문 Z_3로부터 송신 단말 암호문 Z를 복호화하고, 복호화된 송신 단말 암호문 Z로부터 수신 단말 비밀키 x_B를 사용하여 이메일 메시지 M을 복호한다.

<142> 그리고, 마지막으로 수신 단말기 B는 새로운 일회용 공개키와 비밀 키 쌍 (y_B', x_B')을 선택한 후, 기존의 (y_B, x_B) 값을 (y_B', x_B')로 대체한다.

<143> 이메일 메시지 M은 수신 단말기 B의 수신 단말 일회용 공개키 y_B로 암호화되어 전송되기 때문에 이메일 메시지 M의 기밀성은 y_B의 키 기밀성 (key secrecy)에 기반한다. y_B의 키 기밀성은 다시 송신 단말기 A와 송신 메일 서버 S_A (수신 단말기 B와 수신 메일 서버 S_B)가 교환한 비밀 키 K_A (K_B)와 두 서버가 교환한 제 1 세션키 k_{SS}의 키 기밀성에 기반한다. 만약 DDH (Decisional Diffie-Hellman) 문제가 다항식 시간 안에 풀기 어려운 문제이고, F가 안전한 의사 난수 함수라면 K_A (K_B)를 임의의 난수와 구별하는 것은

다항식 시간 내에 풀기 어려운 문제이다. 즉, K_A (K_B)는 키 기밀성을 제공한다. k_{SS}는 두 서버간에 안전한 키 교환 프로토콜에 의해 교환된 세션키 값이므로, k_{SS}는 키 기밀성을 제공한다. 따라서 y_B는 임의의 난수와 다항식 시간 안에 구별 불가능한 값이다.

<144> 한편, 사용자들의 비밀키 (pw_A, pw_B)가 노출된 경우, 본 발명은 Diffie-Hellman 키 교환 기법으로 K_A (K_B)가 생성되기 때문에 (pw_A, pw_B)값들이 노출되기 이전에 생성된 K_A (K_B)의 값을 계산할 수 없다. 따라서 K_A (K_B)로 암호화되어 전송되는 수신 단말기 B의 일회용 공개키 y_B를 계산할 수 없고, y_B로 암호화되는 이메일 메시지 M을 복호할 수 없기 때문에 본 발명은 전방향 안전성을 제공한다. 메일 서버들의 비밀키가 노출된 경우에도 본 발명이 제 1 세션키 k_{SS}를 교환하기 위하여 두 메일 서버가 Diffie-Hellman 키 교환 기법의 키교환 프로토콜을 사용하지 않더라도 전방향 안전성을 제공한다.

<145> 왜냐하면, 메일 서버들의 비밀키로부터 제 1 세션키 k_{SS}를 얻은 후 수신 단말기 B의 일회용 공개키 y_B를 얻을 수 있더라도 y_B에 대응되는 수신 단말 비밀키 x_B를 알 수 없기 때문에 $Z=PE_{y_B}(A||B||y_B||M)$를 복호할 수 없다.

<146> 도 5는 본 발명의 제 3 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법의 흐름도를 도시한 것이다.

<147> 도 5를 참조하면 우선, 송신 단말기에서 제 1 난수를 생성하고, 송신 메일 서버에서 상기 송신 단말기의 아이디 및 상기 송신 메일 서버에서 생성한 생성자에 상기 제 1 난수를 지수승한 송신 메일 서버의 메시지로 이루어진 데이터 쌍을 송신 메일 서버 리스트에 저장하고, 수신 단말기에서 제 2 난수를 생성하고, 수신 메일 서버에서 상기 수신 단말기의 아이디 및 상기 수신 메일 서버에서 생성한 생성자에 상기 제 2 난수를 지수승한 수신 메일 서버의 메시지로 이루어진 데이터 쌍을 수신 메일 서버 리스트에 저장한다(S510).

<148> 그 다음, 이메일 메시지를 전송하고자 하는 상기 송신 단말기에서 상기 송신 메일 서버와 로그인 프로토콜을 수행하여 생성된 제 1 암호키를 상호 공유한다(S520).

<149> 그 다음, 상기 송신 메일 서버에서 수신 메일 서버와 키 교환 프로토콜을 수행하여 제 1 세션키를 상호 공유하고, 상기 수신 메일 서버에서 상기 수신 메일 서버의 메시지 및 상기 제 1 세션키를 이용하여 상기 수신 메일 서버의 메시지를 암호화한 수신 메일 서버의 메시지 인증 코드값을 상기 송신 메일 서버로 전송한다(S530).

<150> 그 다음, 상기 송신 메일 서버에서 상기 수신 메일 서버의 메시지 인증 코드값이 유효한 지의 여부를 검증하고, 상기 송신 메일 서버에서 수신 메일 서버의 메시지, 상기 제 1 암호키를 이용하여 상기 수신 메일 서버의 메시지를 암호화한 송신 메일 서버의 제 1 메시지 인증 코드값을 상기 수신 단말기에 전송한다(S540).

<151> 그 다음, 상기 송신 단말기에서 상기 송신 메일 서버로부터 전송된 상기 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한지의 여부를 판단하고, 제 3 난수를 선택하여 생성된 송신 단말 메시지 및 상기 송신 단말 메시지 및 상기 제 2 난수를 이용하여 생성된 제 2 세션키를 연산한다(S550).

<152> 그 다음, 상기 송신 단말기에서 상기 제 2 세션키로 상기 이메일 메시지를 암호화한 암호문, 상기 송신 단말 메시지, 및 상기 제 1 암호키를 이용하여 상기 송신 단말 메시지를 암호화한 송신 단말의 메시지 인증 코드값을 상기 송신 메일 서버로 전송한다(S560).

<153> 그 다음, 상기 송신 메일 서버에서 상기 송신 단말기로부터 전송된 송신 단말의 메시지 인증 코드값이 유효한지의 여부를 판단하고, 상기 송신 메일 서버에서 상기 암호문, 상기 송신 단말 메시지 및 상기 제 1 세션키로 상기 송신 단말 메시지를 암호화한 송신 메일 서버의 제 2 메시지 인증 코드값을 상기 수신 메일 서버로 전송한다(S570).

<154> 그 다음, 상기 수신 메일 서버에서 상기 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 지의 여부를 판단

하고, 상기 수신 메일 서버에서 상기 암호문 및 상기 송신 단말 메시지를 저장한다(S580).

<155> 그 다음, 상기 수신 단말기가 상기 수신 메일 서버에 로그인하면, 상기 수신 단말기 및 상기 수신 메일 서버에서 로그인 프로토콜을 수행하여 제 2 암호키를 공유한다(S590).

<156> 그 다음, 상기 수신 메일 서버에서 상기 송신 단말기의 아이디, 상기 암호문, 상기 송신 단말 메시지 및 상기 제 2 암호키로 상기 송신 단말 메시지를 암호화한 수신 단말의 메시지 인증 코드값을 상기 수신 단말기에 전송한다(S591).

<157> 마지막으로, 상기 수신 단말기에서 상기 수신 단말의 메시지 인증 코드값이 유효한지의 여부를 판단하고, 상기 제 2 난수를 이용하여 상기 제 2 세션키를 추출하고, 상기 제 2 세션키를 이용하여 상기 암호문으로부터 상기 이메일 메시지를 추출한다(S592).

<158> 도 6은 도 5의 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에서의 데이터 흐름을 도시한 것이다.

<159> 이하, 도 5 및 도 6을 참조하여 본 발명의 제1 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법을 더욱 상세히 설명하기로 한다.

<160> 송신 단말기 A는 임의의 제 1 난수 r_A를 저장하고 있다. 그리고 송신 메일 서버 S_A는 송신 단말기 A와 이전에 프로토콜을 수행한 결과로 송신 단말기의 아이디 및 유한 순환군 G로 부터 생성된 생성자 g_2에 상기 제 1 난수 지수승한 $g_2^{r_A}$의 데이터 쌍인 $(A, g_2^{r_A})$를 송신 메일 서버 리스트에 저장하고 있다.

<161> 수신 단말기 B도 자신의 모바일 기기에 임의의 제 2 난수 r_B를 저장하고 있다. 수신 메일 서버 S_B는 마찬가지로 $(B, g_2^{r_B})$를 수신 메일 서버 리스트에 저장하고 있다.

<162> 송신 단말기 A의 로그인 단계에서 송신 단말기 A가 송신 메일 서버 S_A에 로그인하기 위해서 송신 단말기 A와 송신 메일 서버 S_A는 상기 실시예 1에서의 로그인 프로토콜과 동일한 과정을 수행하여 상기 수학식 7에 의해 연산되는 제 1 비밀키 $K_A=F_{k_A}(A\|S_A\|X_A\|X_{S_A})$를 교환한다.

<163> 이는 전술한 바와 동일하므로 중복된 상세한 설명은 발명의 명확화를 위하여 과감히 생략하기로 한다.

<164> 그 다음, 송신 단말기 A의 암호화된 이메일 메시지를 발송하는 단계에서 송신 단말기 A가 이메일 메시지 M을 수신 단말기 B에게 안전하게 전송하기를 원할 경우 송신 단말기 A, 송신 메일 서버 S_A 그리고 수신 메일 서버 S_B는 다음 프로토콜을 수행한다. 여기서 송신 메일 서버 S_A와 수신 메일 서버 S_B는 이미 하나의 제 1 세션키 k_{SS}를 안전한 키 교환 프로토콜을 사용하여 교환했다고 가정한다.

<165> 한편, 수신 메일 서버 S_B는 수신 메일 서버 리스트로부터 $(B, g_2^{r_B})$를 가져온다. 그리고 수신 메일 서버 S_B는 하기의 수학식 19에 의해 연산되는 수신 메일 서버의 메시지 Y_B, 수신 메일 서버의 메시지 인증 코드값 τ_1을 송신 메일 서버 S_A에게 전송한다.

수학식 19

<166> $$Y_B=g_2^{r_B}, \tau_1=Mac.G_{k_{SS}}(B\|A\|S_A\|S_B\|Y_B)$$

<167> 여기서, g_2는 오더가 q인 유한 순환군 G의 생성자이고, $Mac.G$는 제 1 세션키 k_{SS}를 사용하여 수신 메일 서버의 메시지 인증 코드값 τ_1을 생성하고, B는 수신 단말기의 아이디이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, S_B는 수신 메일 서버의 아이디이다.

<168> 한편, 송신 메일 서버 S_A는 수신 메일 서버 S_B로부터 전송된 수신 메일 서버의 메시지 인증 코드값 τ_1이 유효한지의 여부를 하기의 수학식 20에 따라 판단한다.

수학식 20

<169> $$Check\ \mathbf{Mac}\ V_{k_{SS}}(\tau_1) = 1$$

<170> 즉, 수학식 20을 참조하면, 제 1 세션키를 이용하여 상기 수신 메일 서버의 메시지 인증 코드값 τ_1이 유효한지의 여부를 검증하며, 검증값이 '1'이 출력되면 수신 메일 서버의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 중간에 수정 또는 변경이 발생한 것으로 판단되어, 수신된 수신 메일 서버의 메시지 인증 코드값을 버리게 된다.

<171> 이와 같이, 수신 메일 서버의 메시지 인증 코드값 τ_1이 유효하면, 송신 메일 서버 S_A는 하기의 수학식 21에 의해 연산되는 수신 메일 서버의 메시지 Y_B 및 송신 메일 서버의 제 1 메시지 인증 코드값 τ_2를 송신 단말기 A에게 전송한다.

수학식 21

<172> $$(Y_B, \tau_2 = Mac.G_{K_A}(A||B||S_A||S_B||Y_B))$$

<173> 여기서, $Mac.G$는 제 1 암호키 K_A를 사용하여 송신 메일 서버의 제 1 메시지 인증 코드값 τ_2를 생성하고, B는 수신 단말기의 아이디이고, A는 송신 단말기의 아이디이고, S_A는 송신 메일 서버의 아이디이고, S_B는 수신 메일 서버의 아이디이고, Y_B는 수학식 19에 의해 연산되는 수신 메일 서버의 메시지이다.

<174> 그러면, 송신 단말기 A는 송신 메일 서버 S_A로부터 전송된 송신 메일 서버의 제 1 메시지 인증 코드값 τ_2가 유효한지의 여부를 하기의 수학식 22에 의해 판단한다.

수학식 22

<175> $$Check\ \mathbf{Mac}\ V_{K_A}(\tau_2) = 1$$

<176> 즉, 수학식 22를 참조하면, 제 1 암호키 K_A를 이용하여 상기 송신 메일 서버의 제 1 메시지 인증 코드값 τ_2가 유효한지의 여부를 검증하며, 검증값이 '1'이 출력되면 송신 메일 서버의 제 1 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 중간에 수정 또는 변경이 발생한 것으로 판단되어, 수신된 송신 메일 서버의 제 1 메시지 인증 코드값 τ_2을 버리게 된다.

<177> 만약 τ_2가 유효하면 송신 단말기 A는 임의의 제 3 난수 r_A'를 선택한 후 하기의 수학식 23에 의해 연산되는 송신 단말 메시지 Y_A와 하기의 수학식 24에 의해 연산되는 제 2 세션키 SK를 연산한다.

수학식 23

<178> $$Y_A = g_2^{r_A'}$$

<179> 여기서, g_2는 오더가 q인 유한 순환군 G의 생성자이다.

수학식 24

<180> $$sk = H(A \| B \| Y_A \| Y_B \| g_2^{r_A r_B})$$

<181> 여기서, $H()$는 해쉬 함수이고, A는 송신 단말기의 아이디이고, B는 수신 단말기이고, Y_A는 수학식 23에 의해 연산된 송신 단말 메시지이고, Y_B는 수학식 21에 의해 수신 메일 서버의 메시지이고, g_2는 오더가 q인 유한 순환군 G의 생성자이다.

<182> 한편, 송신 단말기 A는 하기의 수학식 25에 의해 연산되는 암호문 Z, 송신 단말 메시지 Y_A, 송신 단말의 메시지 인증 코드값 τ_3를 송신 메일 서버 S_A에게 전송한다.

수학식 25

<183> $$(Z=E_{sk}(A \| B \| M), Y_A, \tau_3 = Mac.G_{K_A}(A \| B \| S_A \| Z \| Y_A))$$

<184> 여기서, E는 대칭키 암호화 함수로 제 2 세션키 SK를 이용하여 메시지 M를 암호화하고, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이고, M은 메시지이고, $Mac.G$는 제 1 암호키 K_A를 사용하여 송신 단말의 메시지 인증 코드값 τ_3를 생성하고, S_A는 송신 메일 서버의 아이디이고, Y_A는 수학식 23에 의해 생성된 송신 단말 메시지이다.

<185> 여기서, 송신 메일 서버 S_A는 송신 단말기 A로부터 전송된 송신 단말의 메시지 인증 코드값 τ_3가 유효한지의 여부를 하기의 수학식 26에 따라 판단한다.

수학식 26

<186> $$Check\ Mac\ V_{K_A}(\tau_3) = 1$$

<187> 즉, 수학식 26를 참조하면, 제 1 암호키 K_A를 이용하여 상기 송신 단말의 메시지 인증 코드값 τ_3가 유효한지의 여부를 검증하며, 검증값이 '1'이 출력되면 송신 단말의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 중간에 수정 또는 변경이 발생한 것으로 판단되어, 수신된 송신 단말의 메시지 인증 코드값 τ_3

를 버리게 된다.

<188> 만약 τ_3가 유효하면, 송신 메일 서버 S_A는 하기의 수학식 27에 의해 연산되는 암호문 Z, 송신 단말 메시지 Y_A, 송신 메일 서버의 제 2 메시지 인증 코드값 τ_4를 수신 메일 서버 S_B에게 전송한다.

수학식 27

<189> $$(Z, Y_A, \tau_4 = Mac.G_{k_{SS}}(S_A||S_B||A||B||Z||Y_A))$$

<190> 여기서, $Mac.G$는 제 1 세션키 k_{SS}를 사용하여 송신 메일 서버의 제 2 메시지 인증 코드값 τ_4를 생성하고, S_A는 송신 메일 서버의 아이디이고, S_B는 수신 메일 서버의 아이디이고, A는 송신 단말기이고, B는 수신 단말기이고, Z는 수학식 25에 의해 연산되는 암호문이고, Y_A는 수학식 23에 의해 얻어진 송신 단말 메시지이다.

<191> 그러면, 수신 메일 서버 S_B는 전송된 송신 메일 서버의 제 2 메시지 인증 코드값 τ_4가 유효한 지의 여부를 하기의 수학식 28에 따라 검증한다.

수학식 28

<192> $$Check\ Mac\ V_{k_{SS}}(\tau_4) = 1$$

<193> 즉, 수학식 28를 참조하면, 제 1 세션키 k_{SS}를 이용하여 상기 송신 메일 서버의 제 2 메시지 인증 코드값 τ_4가 유효한지의 여부를 검증하며, 검증값이 '1'이 출력되면 송신 메일 서버의 제 2 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 중간에 수정 또는 변경이 발생한 것으로 판단되어, 수신된 송신 메일 서버의 제 2 메시지 인증 코드값 τ_4를 버리게 된다.

<194> 여기서, τ_4가 유효한 것으로 판단되면, 수신 메일 서버 S_B는 (A, B, Z, Y_A)를 저장한다.

<195> 그런 다음, 수신 단말기 B의 로그인 단계에서 수신 단말기 B가 수신 메일 서버 S_B에 로그인하기 위해 수신 단말기 B와 수신 메일 서버 S_B는 송신 단말기 A의 로그인 단계에서와 같이 프로토콜을 수행한다. 수신 단말기 B가 성공적으로 수신 메일 서버 S_B에 로그인하면 수신 단말기 B와 수신 메일 서버 S_B는 수학식 11에 의해 연산되는 제 2 암호키 $K_B = F_{k_B}(B||S_B||X_B||X_{S_B})$를 공유하게 된다.

<196> 수신 단말기 B의 메시지 수신 단계에서 수신 메일 서버 S_B는 하기의 수학식 29에 의해 연산되는 수신 단말기의 아이디 A, 암호문 Z, 송신 단말 메시지 Y_A, 수신 단말의 메시지 인증 코드값 τ_5를 수신 단말기 B에게 전송한다.

수학식 29

$$(A,Z,Y_A,\tau_5=Mac.G_{K_B}(S_B||A||B||Z||Y_A))$$

<197>

<198> 여기서, $Mac.G$는 제 2 암호키 K_B를 사용하여 수신 단말의 메시지 인증 코드값 τ_5를 생성하고, S_B는 수신 메일 서버이고, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이고, Z는 수학식 25에 의해 연산되는 암호문이고, Y_A는 수학식 23에 의해 연산되는 송신 단말 메시지이다.

<199> 그런 다음, 수신 단말기 B는 수신 메일 서버 S_B로부터 전송된 수신 단말의 메시지 인증 코드값 τ_5가 유효한지의 여부를 하기의 수학식 30에 따라 판단한다.

수학식 30

$$Check\ Mac\ V_{K_B}(\tau_5)=1$$

<200>

<201> 즉, 수학식 26를 참조하면, 제 2 비밀키 K_B를 이용하여 상기 수신 단말의 메시지 인증 코드값 τ_5가 유효한지의 여부를 검증하며, 검증값이 '1'이 출력되면 수신 단말의 메시지 인증 코드값이 유효한 것으로 판단하고, '0'이 출력되면 중간에 수정 또는 변경이 발생한 것으로 판단되어, 수신된 수신 단말의 메시지 인증 코드값 τ_5를 버리게 된다.

<202> 만약 τ_5가 유효하면, 수신 단말기 B는 저장되어 있는 제 2 난수 r_B를 사용하여 하기의 수학식 31에 의해 제 2 세션키 SK를 추출해낸다.

수학식 31

$$sk=H(A\,||\,B\,||\,Y_A\,||\,Y_B\,||\,g_2^{r_A r_B})$$

<203>

<204> 여기서, A는 송신 단말기의 아이디이고, B는 수신 단말기의 아이디이고, Y_A는 수학식 23에 의해 얻어진 송신 단말 메시지이고, Y_B는 수학식 21에 의해 얻어진 수신 메일 서버의 메시지이고, g_2는 오더가 q인 유한 순환군 G의 생성자이다.

<205> 그 다음, 수신 단말기 B는 상기 수학식 31에서 생성된 제 2 세션키 SK를 이용하여 하기의 수학식 32에 의해 암호문 Z로부터 이메일 메시지 M을 복호한다.

<206> 이메일 메시지 M은 세션키 제 2 세션키SK로 암호화되어 전송되기 때문에 이메일 메시지 M의 기밀성은 SK의 키 기밀성 (key secrecy)에 기반한다. SK의 키 기밀성은 다시 메일 송신 단말기 A와 송신 메일 서버 S_A (수신 단말기 B와 메일 서버 S_B)가 교환한 비밀 키 K_A (K_B)와 두 서버가 교환한 제 1 세션

키 k_{SS}의 키 기밀성에 기반한다. 만약 DDH (Decisional Diffie-Hellman) 문제가 다항식 시간 안에 풀기 어려운 문제이고, F가 안전한 의사 난수 함수라면 K_A (K_B)를 임의의 난수와 구별하는 것은 다항식 시간 내에 풀기 어려운 문제이다.

<207> 즉, K_A (K_B)는 키 기밀성을 제공한다. k_{SS}는 두 서버간에 안전한 키 교환 프로토콜에 의해 교환된 제 1 세션키 이므로, k_{SS}는 키 기밀성을 제공한다.

<208> 만약, 사용자들의 패스워드 (pw_A, pw_B)가 노출된 경우, 본 발명은 Diffie-Hellman 키 교환 기법으로 K_A (K_B)가 생성되기 때문에 (pw_A, pw_B) 값들이 노출되기 이전에 생성된 K_A (K_B)의 값을 계산할 수 없다.

<209> 이메일 메시지 M을 암호화하는데 사용하는 제 2 세션키 SK는 K_A (K_B)로부터 Diffie-Hellman 값들 $g_2^{r_A'}$, $g_2^{r_B}$을 인증하는데 (메시지 인증 코드키 값으로) 사용하기 때문에 $g_2^{r_A'}$, $g_2^{r_B}$로부터 SK를 연산하는 것은 Diffie-Hellman문제에 기반한다.

<210> 따라서 전송된 이메일 메시지 M을 복호할 수 없기 때문에 본 발명은 전방향 안전성을 제공한다. 메일 서버들의 비밀키가 노출된 경우에도 본 발명이 세션키 k_{SS}를 교환하기 위하여 두 메일 서버가 Diffie-Hellman 키 교환 기법의 키교환 프로토콜을 사용하지 않더라도 전방향 안전성을 제공한다.

<211> 왜냐하면, 서버들로부터의 제 1 세션키인 k_{SS}를 얻은 후 ($g_1^{r_A'}$, $g_1^{r_B}$)를 얻을 수 있더라도 제 2 세션키 SK 자체가 Diffie-Hellman 키 교환 기법으로 생성된 값이므로 SK를 알 수 없고, 암호문 Z를 복호할 수 없다.

<212> 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터(정보 처리 기능을 갖는 장치를 모두 포함한다)가 읽을 수 있는 코드로서 구현하는 것이 가능하다.

<213> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 테이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등이 있다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<214> 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사항에 의해 정해져야 할 것이다.

도면의 간단한 설명

<215> 도 1은 본 발명의 제1 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에 대한 흐름도이다.

<216> 도 2는 도 1의 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에서의 데이터 흐름을 도시한 것이다.

<217> 도 3은 본 발명의 제2 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에 대한 흐름도이다.

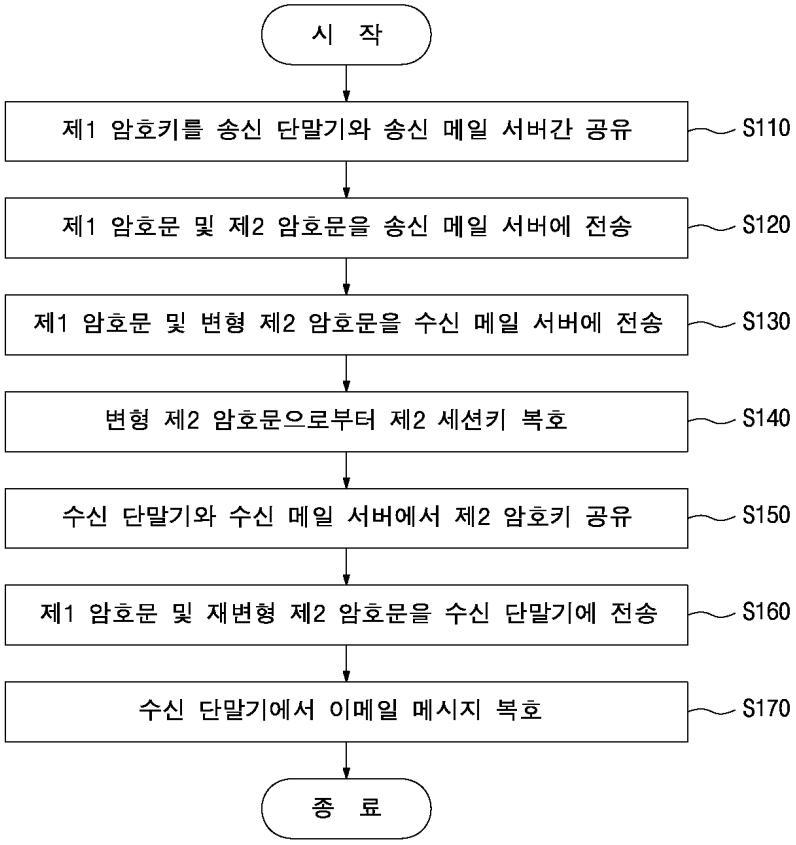
<218> 도 4는 도 3의 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에서의 데이터 흐름을 도시한 것이다.

<219> 도 5는 본 발명의 제3 실시예에 따른 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에 대한 흐름도이다.

<220> 도 6은 도 5의 기밀성과 전방향 안전성을 제공하는 이메일 전송 방법에서의 데이터 흐름을 도시한 것이다.

도면

도면1



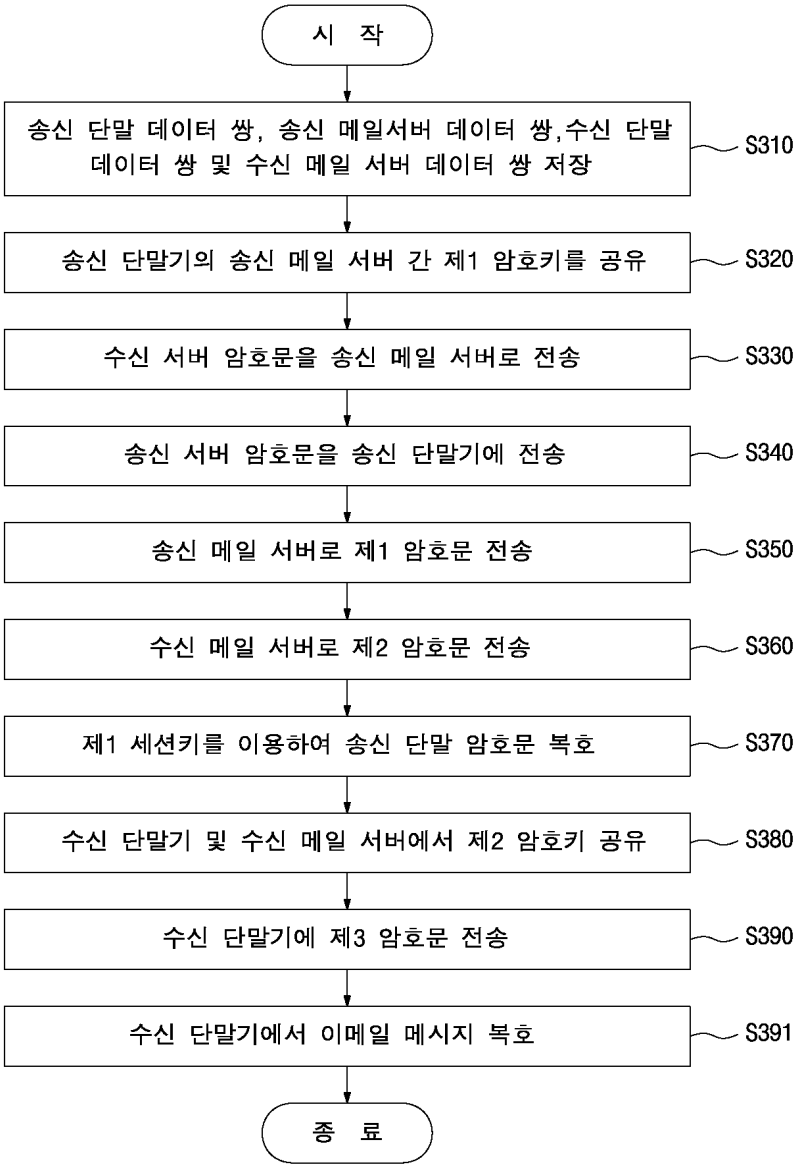
도면2

$\langle Login\ phase\ of\ A \rangle$	$A\ (pw_A)$	$S_A\ (pw_A)$
	$x_A \in_R \mathbb{Z}_q^*$	$y_A \in_R \mathbb{Z}_q^*$
	$A,\ X_A = g_1^{x_A} \cdot g_2^{H(A\|\|S_A\|\|pw_A)} \mod p \longrightarrow$	$\longleftarrow S_A,\ X_{S_A} = g_1^{y_A} \cdot g_2^{H(A\|\|S_A\|\|pw_A)} \mod p$
	$k_A = g_1^{x_A y_A} \mod p$	$k_A = g_1^{x_A y_A} \mod p$
	$B,\ \tau_A = \mathsf{Mac.G}_{k_A}(A\|\|S_A\|\|X_A\|\|X_{S_A}) \longrightarrow$	$\longleftarrow \tau_{S_A} = \mathsf{Mac.G}_{k_A}(S_A\|\|A\|\|X_A\|\|X_{S_A})$
	Check $\mathsf{Mac.V}_{k_A}(\tau_{S_A}) \stackrel{?}{=} 1$	Check $\mathsf{Mac.V}_{k_A}(\tau_A) \stackrel{?}{=} 1$
	$K_A = \mathcal{F}_{k_A}(A\|\|S_A\|\|X_A\|\|X_{S_A})$	$K_A = \mathcal{F}_{k_A}(A\|\|S_A\|\|X_A\|\|X_{S_A})$

$\langle Sending\ phase\ of\ A \rangle$	$A\ (K_A)$	$S_A\ (K_A, k_{SS})$	$S_B\ (k_{SS})$
	$sk \in \{0,1\}^\ell$		
	$SK = H(A\|\|S_A\|\|\mathsf{sid}\|\|sk),$		
	$\mathsf{sid} = X_A\|\|X_{S_A}\|\|\tau_A\|\|\tau_{S_A}$		
	$Z_1 = E_{SK}(A\|\|B\|\|M), Z_2 = \mathsf{E}_{K_A}(A\|\|B\|\|SK) \longrightarrow$		
		$Z_1, Z_2' = \mathsf{E}_{k_{SS}}(A\|\|B\|\|SK) \longrightarrow$	
			Keep (A, B, Z_1, SK)

$\langle Receiving\ phase\ of\ B \rangle$	$S_B\ (K_B)$	$B\ (K_B)$
	$Z_1, Z_2'' = \mathsf{E}_{K_B}(A\|\|B\|\|SK) \longrightarrow$	
		Compute SK by $\mathsf{D}_{K_B}(Z_2'')$ and recover M by $\mathsf{D}_{SK}(Z_1)$

도면3

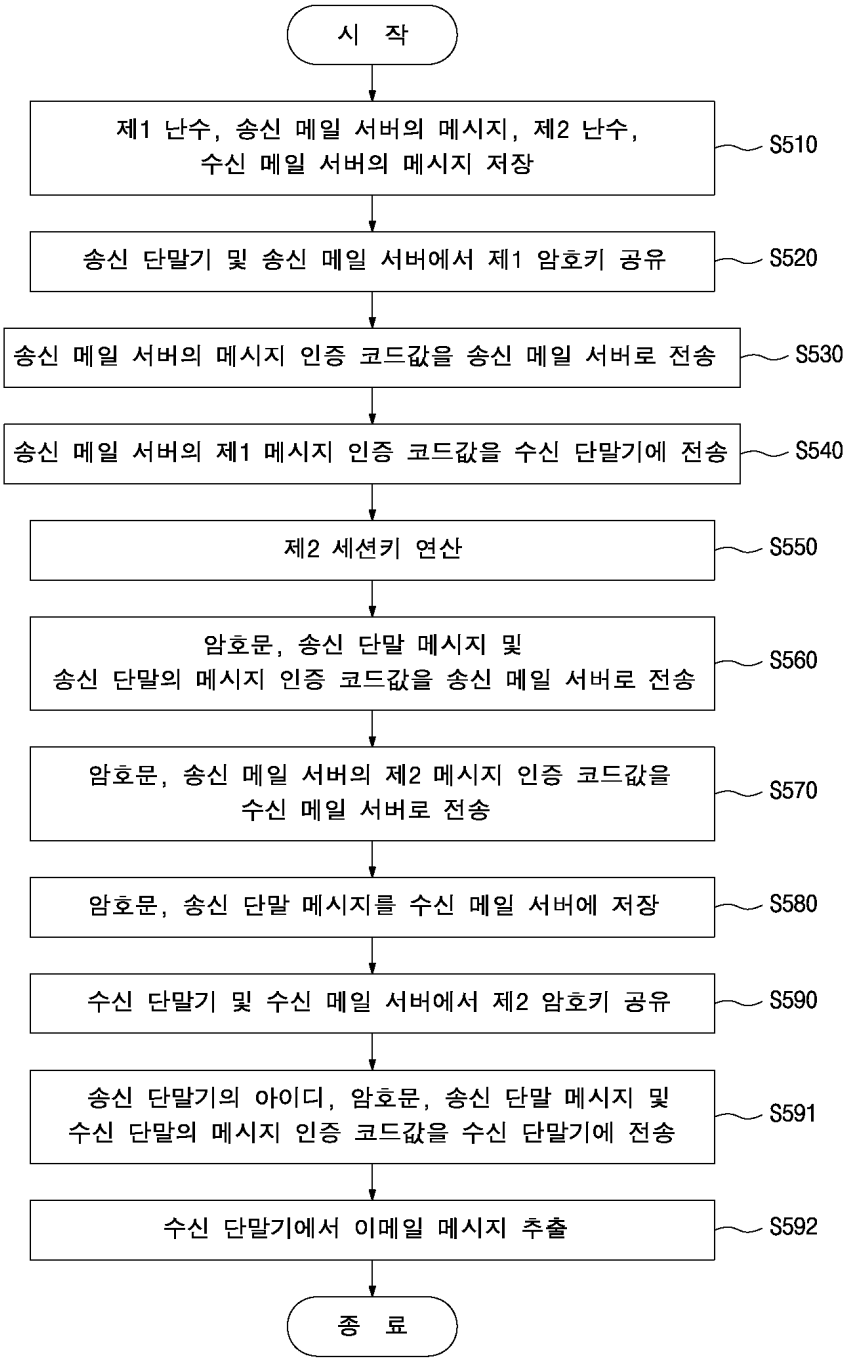


도면4

$\langle$*Sending phase of A*$\rangle$	$A\ (K_A)$	$S_A\ (K_A, k_{SS})$	$S_B\ (k_{SS})$
			Recover (B, y_B)
			$\longleftarrow Y_B = \mathsf{E}_{k_{SS}}(S_B \| S_A \| B \| y_B)$
		$\longleftarrow Y_A = \mathsf{E}_{K_A}(S_A \| A \| B \| y_B)$	
	$Z = \mathsf{PE}_{y_B}(A \| B \| y_B \| M)$		
	$Z_1 = \mathsf{E}_{K_A}(A \| B \| Z) \longrightarrow$		
		$Z_2 = \mathsf{E}_{k_{SS}}(S_A \| S_B \| Z)$	$\longrightarrow$ Compute $Z_3 = \mathsf{E}_{K_B}(Z)$
			Keep (A, B, Z_3)

$\langle$*Receiving phase of B*$\rangle$	$S_B\ (K_B)$	$B\ (K_B, x_B)$
	$Z_3 \longrightarrow$	
		Recover M by $\mathsf{PD}_{x_B}(Z)$
		Choose (y'_B, x'_B) and replace it for (y_B, x_B) in its mobile device

도면5


시 작
제1 난수, 송신 메일 서버의 메시지, 제2 난수,
수신 메일 서버의 메시지 저장
S510
송신 단말기 및 송신 메일 서버에서 제1 암호키 공유
S520
송신 메일 서버의 메시지 인증 코드값을 송신 메일 서버로 전송
S530
송신 메일 서버의 제1 메시지 인증 코드값을 수신 단말기에 전송
S540
제2 세션키 연산
S550
암호문, 송신 단말 메시지 및
송신 단말의 메시지 인증 코드값을 송신 메일 서버로 전송
S560
암호문, 송신 메일 서버의 제2 메시지 인증 코드값을
수신 메일 서버로 전송
S570
암호문, 송신 단말 메시지를 수신 메일 서버에 저장
S580
수신 단말기 및 수신 메일 서버에서 제2 암호키 공유
S590
송신 단말기의 아이디, 암호문, 송신 단말 메시지 및
수신 단말의 메시지 인증 코드값을 수신 단말기에 전송
S591
수신 단말기에서 이메일 메시지 추출
S592
종 료

도면6

$\langle$*Sending phase of A*$\rangle$ $A\ (K_A)$		$S_A\ (K_A, k_{SS})$		$S_B\ (k_{SS})$
				Recover $(B, g_2^{r_B})$
			$\longleftarrow$	$Y_B = g_2^{r_B}$,
				$\tau_1 = \mathsf{Mac.G}_{k_{SS}}(B\|\|A\|\|S_A\|\|S_B\|\|Y_B)$
		Check $\mathsf{Mac.V}_{k_{SS}}(\tau_1) \stackrel{?}{=} 1$		
	$\longleftarrow$	$Y_B, \tau_2 = \mathsf{Mac.G}_{K_A}(A\|\|B\|\|S_A\|\|S_B\|\|Y_B)$		
Check $\mathsf{Mac.V}_{K_A}(\tau_2) \stackrel{?}{=} 1$				
$r'_A \in \mathbb{Z}_q^*, Y_A = g_2^{r'_A}$,				
$sk = H(A\|\|B\|\|Y_A\|\|Y_B\|\|g_2^{r'_A r_B})$				
$Z = \mathsf{E}_{sk}(A\|\|B\|\|M), Y_A$,	$\longrightarrow$			
$\tau_3 = \mathsf{Mac.G}_{K_A}(A\|\|B\|\|S_A\|\|Z\|\|Y_A)$				
		Check $\mathsf{Mac.V}_{K_A}(\tau_3) \stackrel{?}{=} 1$		
		Z, Y_A,	$\longrightarrow$	
		$\tau_4 = \mathsf{Mac.G}_{k_{SS}}(S_A\|\|S_B\|\|A\|\|B\|\|Z\|\|Y_A)$		
				Check $\mathsf{Mac.V}_{k_{SS}}(\tau_4) \stackrel{?}{=} 1$
				Keep (A, B, Z, Y_A)

$\langle$*Receiving phase of B*$\rangle$ $S_B\ (K_B)$		$B\ (K_B, x_B)$
$A, Z, Y_A, \tau_5 = \mathsf{Mac.G}_{K_B}(S_B\|\|A\|\|B\|\|Z\|\|Y_A)$	$\longrightarrow$	
		Check $\mathsf{Mac.V}_{K_B}(\tau_5) \stackrel{?}{=} 1$
		Recover (B, r_B)
		Compute $sk = H(A\|\|B\|\|Y_A\|\|Y_B\|\|g_2^{r'_A r_B})$
		Choose (r'_B) and replace it for (r_B) in its mobile device