



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0096073
(43) 공개일자 2007년10월02일

(51) Int. Cl.

H04L 9/30 (2006.01) H04L 9/32 (2006.01)

G06F 17/00 (2006.01)

(21) 출원번호 10-2005-0116708

(22) 출원일자 2005년12월02일

심사청구일자 2005년12월02일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

이동훈

경기 고양시 일산구 일산3동 후곡마을 동신아파트
808동 804호

구재형

서울 강남구 삼성동 진흥아파트 1동 904호

김범한

서울 송파구 방이1동 130-16 201호

(74) 대리인

현중철

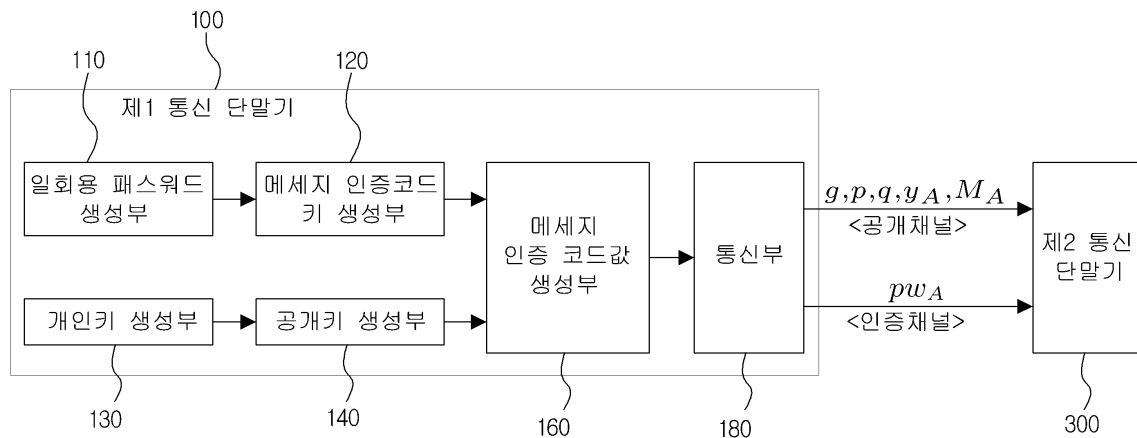
전체 청구항 수 : 총 12 항

(54) 제 3의 신뢰기관의 도움 없이 공개키에 대한 상호 인증 및 키 교환 방법 및 그 장치

(57) 요약

본 발명은 공개키에 대한 상호 인증 및 키 교환 장치 및 방법에 관한 것으로서, 본 발명의 공개키에 대한 상호 인증 및 키 교환 방법은, 임의의 일회용 패스워드를 생성하는 단계, 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하는 단계, 생성한 메시지 인증 코드 키를 기초로 공개키에 대한 메시지 인증 코드 값을 생성하는 단계, 생성한 메시지 인증 코드 값 및 공개키를 비롯한 전송 대상 정보를 공개 채널을 통해 수신측에 전송하는 단계, 및 인증 채널을 통해 일회용 패스워드를 수신측에 제공하는 단계를 포함하며, 인증 서버를 통한 인증이 불가능한 경우 중간에 조작되는 정보들이 조작되는 위험 없이 상호 간에 안전하게 상호 인증 및 키 교환을 수행할 수 있다.

대표도 - 도2



특허청구의 범위

청구항 1

공개키에 대한 상호 인증 및 키 교환 방법에 있어서,

임시로 사용할 일회용 패스워드를 생성하는 단계;

소정 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하는 단계;

상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키에 대한 메시지 인증 코드 값을 생성하는 단계;

상기 생성한 메시지 인증 코드 값 및 상기 공개키를, 공개 채널을 통해 수신측에 전송하는 단계;

인증 채널을 통해 상기 수신측에 상기 일회용 패스워드를 제공하는 단계; 및

상기 일회용 패스워드를 통해 상기 메시지 인증 코드 키를 복원하고 메시지 인증 코드 값에 대한 정당성 검증 결과에 따라 상기 수신측에서 생성한 메시지 인증 코드 값 및 공개키를 수신하여 상기 공개키를 상호 인증 및 공유하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 2

제 1항에 있어서,

상기 메시지 인증 코드 키를 생성하는 단계에서는 해시 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 상기 메시지 인증 코드 키를 생성하는 것을 특징으로 하는 방법.

청구항 3

제 1항에 있어서,

상기 일회용 패스워드 생성 단계 후,

상기 공개키를 생성하기 위한 제너레이터를 선택하는 단계;

개인키를 생성하는 단계; 및

상기 제너레이터를 이용하여 상기 개인키에 대한 공개키를 생성하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 4

제 1항에 있어서,

상기 수신측에 전송할 전송대상정보를 선택하는 단계를 더 포함하며,

이에 따라, 상기 메시지 인증 코드 값 생성 단계에서는 상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키 및 상기 전송대상정보에 대한 메시지 인증 코드 값을 생성하는 것을 특징으로 하는 방법.

청구항 5

제 3항에 있어서,

상기 수신측에서 메시지 인증 코드 값 및 공개키를 생성하는 과정은,

임시로 사용할 일회용 패스워드를 생성하는 단계;

개인키를 생성하는 단계;

상기 제너레이터를 이용하여 상기 개인키에 대한 공개키를 생성하는 단계;

해시 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하는 단계; 및

상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키에 대한 메시지 인증 코드 값을 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 6

공개키에 대한 상호 인증 및 키 교환 장치에 있어서,

임시로 사용할 일회용 패스워드를 생성하는 일회용 패스워드 생성부;

소정 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하는 메시지 인증 코드 키 생성부;

상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키에 대한 메시지 인증 코드 값을 생성하는 메시지 인증 코드 값 생성부; 및

상기 생성한 메시지 인증 코드 값 및 상기 공개키를 공개 채널을 통해 수신측에 전송하고, 인증 채널을 통해 상기 수신측에 상기 일회용 패스워드를 제공하며, 상기 일회용 패스워드를 통해 상기 메시지 인증 코드 키를 복원하고 메시지 인증 코드 값에 대한 정당성 검증 결과에 따라 상기 수신측에서 생성한 메시지 인증 코드 값 및 공개키를 수신하여 상기 공개키를 상호 인증 및 공유하는 통신부를 포함하는 것을 특징으로 하는 장치.

청구항 7

제 6항에 있어서,

상기 메시지 인증 코드 키 생성부는 해시 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 상기 메시지 인증 코드 키를 생성하는 것을 특징으로 하는 장치.

청구항 8

제 6항에 있어서,

개인키를 생성하는 개인키 생성부; 및

상기 공개키를 생성하기 위해 기 선택된 제너레이터를 이용하여 상기 개인키에 대한 상기 공개키를 생성하는 공개키 생성부를 더 포함하는 것을 특징으로 하는 장치.

청구항 9

제 6항에 있어서,

상기 메시지 인증 코드 값 생성부는 상기 생성한 메시지 인증 코드 키를 상기 공개키를 포함하여, 상기 수신측에 전송하기 위해 기 선택된 전송대상정보에 대한 상기 메시지 인증 코드 값을 생성하는 것을 특징으로 하는 장치.

청구항 10

제 8항에 있어서,

상기 공개키 생성부는 공개키 생성을 위해 기 선택된 제너레이터(g)를 이용하여 개인키(a)에 대한 모듈라 역승 연산($g^a \bmod p$)을 통해 상기 공개키(y_A)를 생성하는 것을 특징으로 하는 장치.

청구항 11

제 10항에 있어서,

상기 메시지 인증 코드 키 생성부는 해시 함수 $h(\text{Alice}, \text{Bob}, pw_A)$ 를 통해 상기 생성한 일회용 패스워드(pw_A)에 대한 상기 메시지 인증 코드 키(K)를 생성하는 것을 특징으로 하는 장치.

청구항 12

제 11항에 있어서,

상기 메시지 인증 코드 값 생성부는 상기 생성한 메시지 인증 코드 키(K_A)를 기초로 상기 공개키(y_A)에 대한 메시지 인증 코드 값(M)을 $MAC_{K_A}(\text{Alice}, \text{Bob}, g, p, q, y_A)$ 를 통해 생성하는 것을 특징으로 하는 장치.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <9> 본 발명은 컴퓨터 및 네트워크 환경에서 인증 및 키 교환 방법에 관한 것으로서, 보다 상세하게는, 인증서에 포함되어 있는 공개키에 대한 인증 여부를 처리하는 인증 서버를 통한 인증이 불가능한 경우 공개키에 대한 상호 인증 및 키 교환 방법에 관한 것이다.
- <10> 최근 정보통신 분야의 급속한 성장과 함께 통신망을 이용한 정보의 전달이 일반화되고 있는 현실이다. 그러나, 이와 같이 통신망을 이용하여 정보를 전달하고자 할 경우, 전화망의 '도청' 또는 인터넷상의 '해킹' 등으로 인해 그 정보의 보안 유지가 사실상 어렵다는 단점이 있다.
- <11> 따라서, 이러한 '도청'이나 '해킹'으로부터 정보를 안전하게 보호하기 위해, 정보를 전달하는 측에서 정보에 대한 암호화를 수행하고, 그 정보를 수신하는 측에서 암호화된 해당 정보를 해독하는 과정을 거침으로써, 해당 정보의 유출을 방지하고자하는 기술이 발달하고 있다. 이러한 기술을 일반적으로 암호 알고리즘이라 한다.
- <12> 도 1은 일반적인 암호 알고리즘에 대한 절차를 간략하게 도시한 흐름도이다.
- <13> 도시된 바와 같이, 서버/클라이언트 구조에서 임의의 클라이언트(10)는 서버(20)로부터 원하는 서비스를 제공받기 위해, 자신의 신상정보 등과 같이 보안이 요구되는 정보를 서버(20)로 전송할 필요가 있다.
- <14> 이러한 서비스를 수행하기 위해, 먼저 클라이언트(10)는 서버(20)로 전송할 정보를 생성한다(S12). 이때 클라이언트(10)는 생성된 정보에 대해 소정 방식에 따라 암호화를 수행한다(S14). 이에 따라, 클라이언트(10)는 암호화된 정보를 서버(20)로 전송한다(S16).
- <15> 이에 따라, 서버(20)는 클라이언트(10)로부터 전송된 암호화된 정보를 수신하여 소정 방식에 따라 복호화를 수행하여 클라이언트(10)로부터 수신한 해당 내용을 해독한다(S18).
- <16> 이러한 암호 알고리즘은 해당 정보를 암호화하고 복호화하는 키의 종류에 따라 비밀키 암호 알고리즘과 공개키 암호 알고리즘으로 구분된다. 비밀키 암호 알고리즘은 암호화 및 복호화 시 동일키를 사용하는 것이고, 공개키 암호 알고리즘은 암호화 및 복호화 시 서로 다른 키를 사용하는 것이다.
- <17> 본 발명은 이들 중 '공개키 암호 알고리즘'에 관한 것으로서, '공개키 암호 알고리즘'은 암호화 및 복호화 시 서로 다른 키를 사용한다는 특징으로 인해 비대칭키 암호 알고리즘이라고도 한다. 이러한 '공개키 암호 알고리즘'은 키 생성 알고리즘을 통해 두 개의 키를 생성하여 그 중 하나를 전화번호부에 전화번호를 공개하듯이 공개하고, 나머지 하나를 개인키로 자신이 보관하여 사용한다.
- <18> 예를 들어, 'A'가 'B'로 문서를 송신하고자 할 경우, 'A'는 공개된 'B'의 공개키를 이용하여 해당 문서를 암호화하고, 'B'는 수신된 암호문을 자신의 개인키로 풀게 되는 것이다. 따라서, 공개키 암호 알고리즘의 사용자는 상호 정보를 교환하고자 하는 사람들의 수가 증가하더라도 사용자의 동일한 공개키로 암호화된 정보를 수신하기 때문에, 정보 제공자의 수와 관계없이 자신의 개인키만을 관리하면 된다.
- <19> 현재 암호학적인 기술로 널리 사용되고 있는 공개키 암호 알고리즘, 즉 공개키 기반 기술(Public Key Infrastructure: PKI)을 사용하기 위해서는 공개키에 대한 인증과정이 필수적이다. 일반적으로, 공개키에 대한 인증을 위해 전자서명과 인증서를 사용하고 있다. 즉, 공인 인증기관(Certification Authority: CA)에서 발급한 인증서에 대한 유효성을 확인한 후, 해당 인증서에 포함되어 있는 사용자의 공개키에 대한 인증기관의 서명을 확인하여 사용자의 공개키를 인증하게 된다.
- <20> 그런데, 인증기관의 서버가 다운되거나 테러나 재앙 등에 의해 인증기관 건물이 붕괴되는 등의 이유로 서버의 인증 기능을 정상적으로 수행하지 못할 경우, 종래의 공개키 인증 알고리즘으로는 사용자들의 공개키들을 인증할 수 없는 문제점이 있다.
- <21> 예를 들어, 사용자 A와 사용자 B가 중요 업무나 기타 중요한 문서에 대한 정보를 교환한다고 가정하자. 사용자 A와 사용자 B는 빈번하게 공개키를 암호화 알고리즘으로 상대방을 인증하면서, 중요한 자료들을 암호화하여 주

고받는다. 이때 공개키에 대한 인증을 처리하는 공인 인증기관의 서버가 다운되었을 경우, 상대방으로부터 받은 공개키가 올바른 것인지 또는 상대방의 공개키가 갱신된 것인지에 대해 명확히 확인할 수 없는 문제점이 있다.

- <22> 일반적으로, 기존에 제공되고 있는 공개키 암호 알고리즘은 전자서명을 사용하도록 되어 있기 때문에, 실제 인증기관이 이에 대한 인증을 처리하는 기능을 정상적으로 수행하지 못할 경우 전혀 사용이 불가능하다.
- <23> 이러한 문제점을 해결하기 위해서, 패스워드 기반의 인증 기법이 제안되었다. 이러한 예로, 대한민국 특허 공개번호 2001-0027902(2001년 4월 6일)에 개시된 "사용자가 기억할 수 있는 패스워드를 이용한 안전한 사용자인증과 키 일치 방법"이 있다.
- <24> 이러한 패스워드 기반 인증 방법은, 사용자가 기억할 수 있는 짧은 문자열, 즉 패스워드만을 통해서 안전한 사용자 인증과 암호키 일치를 이루도록 한다. 이러한 종래의 패스워드 기반 인증 방법은 패스워드가 안전하게 관리되어야 하는 전제 조건이 따르게 된다.
- <25> 그런데 종래의 패스워드 기반 인증 방법은 공개키라는 공개된 정보를 미리 지정되어 있는 패스워드를 사용하여 인증하게 되면, 패스워드가 외부로 유출될 확률이 매우 높은 문제점이 있다.
- <26> 한편, 국제표준화 작업문서, IETF RFC-3280에서는 공개키 기반 구조에 대한 전반적인 규약과 함께 인증기관 없이 공개키를 인증할 수 있는 방법을 제시하고 있다. 그러나 여기서 제시하는 방법은 미리 긴 길이의 난수 값을 A 및 B 서로가 공유하고 있어야 한다는 단점이 있다.
- <27> 인증기관의 인증 서버가 공개키에 대한 인증 능력을 상실했을 경우, 공개키를 인증하기 위한 방법은 아직 제시되고 있지 못한 실정이다. 아래에는 패스워드 기반 인증 알고리즘과 관련하여 제안된 논문들을 나열한 것이다.
- <28> 1. S.Bellovin 와 M.Meritt, "Encrypted key exchange : password based protocols secure against dictionary attacks", Symposium on Security and Privacy, pp.72-84, IEEE, 1992.
- <29> 2. D.Jablon, "Strong password only authenticated key exchange", ACM Computer communication Review, Vol.26, No.5, 1996
- <30> 3. T.wu, "Secure remote password protocol", Internet Society Symp. on Network and Distributed Sys. Security, 1998.
- <31> 4. M.Bellare, D.Pointcheval 및 P.Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attack", LNCS Vol.1807, pp.139-155, 2000
- <32> 상기한 바와 같이, 인증기관 서버의 인증 처리가 정상적으로 동작하지 않을 경우, 기존에 제안되어 있는 패스워드 기반 기법이 하나의 해결책으로 사용될 수 있으나, 상기에서 언급한 바와 같이 미리 공유되어 안전하게 관리되는 패스워드가 있어야한다는 단점이 있다. 또한 위의 논문들에서 제안하는 패스워드를 사용한 인증 및 키 공유 기법은, 공개키 인증용으로 사용했을 경우에 모든 사용자들이 각각 자신이 통신하기 위한 모든 사용자들과 미리 패스워드를 공유하고 있어야하기 때문에 공개키 인증용으로는 적합하지 않은 문제점이 있다.

발명이 이루고자 하는 기술적 과제

- <33> 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 공개키에 대한 인증기관의 정상적인 인증 처리가 불가능한 경우 공개키에 대한 상호 인증 및 키 교환 장치 및 방법을 제공하는 데 있다.
- <34> 본 발명의 다른 목적은, 인증기관의 서버를 통한 인증이 불가능한 경우 별도의 채널을 통해 공개키에 대한 상호 인증 및 키 교환이 가능한 장치 및 방법을 제공하는 데 있다.
- <35> 본 발명의 또 다른 목적은, 패스워드에 대한 안전성 문제를 해결하면서 공개키에 대한 상호 인증 및 키 교환 장치 및 방법을 제공하는 데 있다.

발명의 구성 및 작용

- <36> 상기와 같은 목적은 본 발명의 실시예에 따라, 공개키에 대한 상호 인증 및 키 교환 방법에 있어서, 임시로 사용할 임의의 일회용 패스워드를 생성하는 단계; 소정 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하는 단계; 상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키에 대한 메시지 인

증 코드 값을 생성하는 단계; 상기 생성한 메시지 인증 코드 값 및 상기 공개키를, 공개 채널을 통해 수신측에 전송하는 단계; 인증 채널을 통해 상기 수신측에 상기 일회용 패스워드를 제공하는 단계; 및 상기 일회용 패스워드를 통해 상기 메시지 인증 코드 키를 복원하고 메시지 인증 코드 값에 대한 정당성 검증 결과에 따라 상기 수신측에서 생성한 메시지 인증 코드 값 및 공개키를 수신하여 상기 공개키를 상호 인증 및 공유하는 단계를 포함하는 방법에 의해 달성된다.

- <37> 바람직하게는, 상기 메시지 인증 코드 키를 생성하는 단계에서는 해시 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 상기 메시지 인증 코드 키를 생성한다.
- <38> 본 실시예의 공개키에 대한 상호 인증 및 키 교환 방법은, 상기 일회용 패스워드 생성 단계 후, 상기 공개키를 생성하기 위한 제너레이터를 선택하는 단계; 개인키를 생성하는 단계; 및 상기 제너레이터를 이용하여 상기 개인키에 대한 공개키를 생성하는 단계를 더 포함한다.
- <39> 본 실시예의 공개키에 대한 상호 인증 및 키 교환 방법은, 상기 수신측에 전송할 전송대상정보를 선택하는 단계를 더 포함한다. 이에 따라, 상기 메시지 인증 코드 값 생성 단계에서는 상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키 및 상기 전송대상정보에 대한 메시지 인증 코드 값을 생성한다.
- <40> 상기 수신측에서 메시지 인증 코드 값 및 공개키를 생성하는 과정은, 임의로 사용할 임의의 일회용 패스워드를 생성하는 단계; 개인키를 생성하는 단계; 상기 제너레이터를 이용하여 상기 개인키에 대한 공개키를 생성하는 단계; 해시 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하는 단계; 및 상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키에 대한 메시지 인증 코드 값을 생성하는 단계를 포함한다.
- <41> 한편, 상기와 같은 목적은 본 발명의 실시예에 따라, 공개키에 대한 상호 인증 및 키 교환 장치에 있어서, 임의로 사용할 임의의 일회용 패스워드를 생성하는 일회용 패스워드 생성부; 소정 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하는 메시지 인증 코드 키 생성부; 상기 생성한 메시지 인증 코드 키를 기초로 상기 공개키에 대한 메시지 인증 코드 값을 생성하는 메시지 인증 코드 값 생성부; 및 상기 생성한 메시지 인증 코드 값 및 상기 공개키를 공개 채널을 통해 수신측에 전송하고, 인증 채널을 통해 상기 수신측에 상기 일회용 패스워드를 제공하며, 상기 일회용 패스워드를 통해 상기 메시지 인증 코드 키를 복원하고 메시지 인증 코드 값에 대한 정당성 검증 결과에 따라 상기 수신측에서 생성한 메시지 인증 코드 값 및 공개키를 수신하여 상기 공개키를 상호 인증 및 공유하는 통신부를 포함하는 장치에 의해 달성된다.
- <42> 바람직하게는, 상기 메시지 인증 코드 키 생성부는 해시 함수를 이용하여 상기 생성한 일회용 패스워드에 대한 상기 메시지 인증 코드 키를 생성한다.
- <43> 또한 본 실시예의 공개키에 대한 상호 인증 및 키 교환 장치는, 개인키를 생성하는 개인키 생성부; 및 상기 공개키를 생성하기 위해 기 선택된 제너레이터를 이용하여 상기 개인키에 대한 상기 공개키를 생성하는 공개키 생성부를 더 포함한다.
- <44> 상기 메시지 인증 코드 값 생성부는 상기 생성한 메시지 인증 코드 키를 상기 공개키를 포함하여, 상기 수신측에 전송하기 위해 기 선택된 전송대상정보에 대한 상기 메시지 인증 코드 값을 생성한다.
- <45> 상기 공개키 생성부는 공개키 생성을 위해 기 선택된 제너레이터(g)를 이용하여 개인키(a)에 대한 모듈라 역승 연산($g^a \bmod p$)을 통해 상기 공개키(y_A)를 생성한다.
- <46> 상기 메시지 인증 코드 키 생성부는 해시 함수 $h(\text{Alice}, \text{Bob}, pw_A)$ 를 통해 상기 생성한 일회용 패스워드(pw_A)에 대한 상기 메시지 인증 코드 키(K)를 생성한다.
- <47> 상기 메시지 인증 코드 값 생성부는 상기 생성한 메시지 인증 코드 키(K_A)를 기초로 상기 공개키(y_A)에 대한 메시지 인증 코드 값(M)을 $MAC_{KA}(\text{Alice}, \text{Bob}, g, p, q, y_A)$ 를 통해 생성한다.
- <48> 본 발명에 따르면, 일회용 패스워드를 생성하고 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하고 생성한 메시지 인증 코드 키를 기초로 공개키에 대한 메시지 인증 코드 값을 생성하여 공개키를 비롯한 전송대상 정보와 함께 공개 채널을 통해 수신측에 전송하고 인증 채널을 통해 일회용 패스워드를 수신측에 제공함으로써, 인증 서버를 통한 인증이 불가능한 경우 중간에 조작되는 정보들이 조작되는 위험 없이 상호 간에 안전하게 상호 인증 및 키 교환을 수행할 수 있다.

- <49> 이하, 본 발명의 바람직한 실시예들을 첨부한 도면을 참조하여 상세히 설명한다. 도면들 중 동일한 구성요소들은 가능한 한 어느 곳에서든지 동일한 부호들로 나타내고 있음에 유의해야 한다. 또한 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.
- <50> 도 2는 본 발명의 바람직한 실시예에 따른 인증기관의 인증 처리 없이 공개키에 대한 상호 인증 및 키 교환을 위한 통신 장치를 도시한 블록도이다.
- <51> 본 발명에 적용되는 통신 장치는 소정의 통신 방식을 통해 외부와 통신 및 데이터 송수신이 가능하고, 인증 서버를 통해 해당 공개키가 포함된 인증서에 대한 인증을 수행할 수 있는 일반적인 통신 단말기를 말한다.
- <52> 본 발명은 인증기관의 인증 서버가 다운되거나 바이러스에 감염 또는 외부 침입자에 의해 해킹 등의 이유로 공개키에 대한 상호 인증 및 키 교환의 기능을 정상적으로 수행하지 못하는 경우에, 사용자들 간에 상호 공개키를 인증 및 키 교환할 수 있도록 하는 방법을 제시한다. 이를 위하여 본 발명은 일회용 패스워드를 사용하여 공개키에 대한 메시지 인증 코드(Message Authentication Code: MAC)를 생성하여 공개키와 함께 교환한 후 패스워드를 추후에 공유하도록 함으로써, 패스워드를 사용하는 것으로 인해 발생하는 안전성 문제를 해결하면서 공개키에 대한 인증을 제공할 수 있다. 본 실시예에서 공개키를 인증하기 위해 사용되는 메시지 인증 코드(MAC) 알고리즘은 현재 많은 시스템에서 일반적으로 사용하는 것으로서 구현이 쉬우며 어떠한 플랫폼에서도 동작하기 때문에 환경의 상관없이 적용될 수 있다.
- <53> 이하에서는 상기와 같은 특징을 갖는 본 발명의 상세한 구성 및 그 특징에 대해 설명한다.
- <54> 도시된 바와 같이, 통신 단말기(100)는 일회용 패스워드 생성부(110), 메시지 인증코드 생성부(120), 개인키 생성부(130), 공개키 생성부(140), 메시지 인증 코드값 생성부(160), 및 통신부(180)를 갖는다.
- <55> 일회용 패스워드 생성부(110)는 입력되는 명령에 따라 임의로 사용하기 위한 임의의 일회용 패스워드(pw_A)를 선택한다. 여기서 일회용 패스워드 생성부(110)는 입력되는 명령에 따라 일회용 패스워드를 선택(pick)하는 것이나, 실제로는 패스워드를 새롭게 생성하는 것이므로 선택이라는 용어 대신에 '생성한다'라는 용어로 기술한다. 이러한 일회용 패스워드는 숫자 및 영문이 단독 또는 혼합된 형태를 갖는다.
- <56> 메시지 인증코드 생성부(120)는 일회용 패스워드 생성부(110)에서 생성한 일회용 패스워드에 대한 메시지 인증코드(MAC) 키(K_A)를 비밀키로서 생성한다. 바람직하게는, 메시지 인증코드 생성부(120)는 메시지 인증코드 키(K_A)를 생성할 때, 아래 수학식 1과 같이 암호학적으로 안전한 해시 함수(hashing function)($h()$)를 이용한다.

$$K_A \sim = \sim h(Alice, \sim Bob, \sim pw_A)$$

- <58> 해시 함수($h()$)를 이용하여 메시지 인증코드 키(K_A)를 생성할 경우, 메시지 인증코드 생성부(120)는 입력되는 일회용 패스워드(pw_A)에 대해 메시지 인증코드 알고리즘에 사용될 메시지 인증코드 키에 맞는 형태로 난수 값을 생성한 후 출력한다. 이와 같이, 본 실시예에서는 메시지 인증코드 키를 생성하기 위해 암호학적으로 안전한 해시 함수를 사용하기 때문에, 서로 다른 입력값들에 대해 같은 출력값을 생성할 확률이 매우 낮다.
- <59> 개인키 생성부(130)는 임의의 개인키(a)를 생성한다. 공개키 생성부(140)는 기 선택된 제너레이터(g)를 이용하여 아래 수학식 2와 같은 모듈러(modular)몫승 연산을 통해 공개키(y)를 생성한다.

$$y_A \sim = \sim g^a \sim mod \sim p \sim$$

- <61> 메시지 인증코드 키 생성부(120)에서 메시지 인증 코드키(K_A)가 생성되고 공개키 생성부(140)에서 공개키(y_A)가 생성되면, 메시지 인증 코드값 생성부(160)는 아래 수학식 3과 같이 공개키를 포함하여 전송하고자 하는 정보에 대한 메시지 인증코드 값(M)을 생성한다.

$$M_A = \sim MAC_{K_A}(Alice, \sim Bob, \sim g, \sim p, \sim q, \sim y_A) \sim$$

- <63> 본 실시예에서 메시지 인증 코드값 생성부(160)에서 이용되는 메시지 인증코드(MAC) 값 생성을 위한 알고리즘은 입력 값이 1비트만 차이가 나도 서로 상이한 결과를 출력하며, 정확한 메시지 인증코드(MAC) 키(K_A)를 알고 있는 경우에만 수신측에서 동일한 메시지 인증코드 값을 생성할 수 있다.
- <64> 이에 따라, 통신부(180)는 메시지 인증 코드값 생성부(160)에서 생성한 메시지 인증코드값(M_A) 및 공개키(y_A)가 포함된 전송하기 위해 선택된 정보들(g, p, q)을 공개 채널(Public Channel)을 통해 수신자의 통신 장치인 제2 통신 단말기(300)에 전송한다.
- <65> 즉, 본 실시예에서는 일회용 패스워드를 만들어서 이에 대한 메시지 인증 코드 키를 생성한 후 공유할 정보(공개키를 포함함)에 대한 메시지 인증 코드값을 생성하여 공개 채널을 통해 전송함으로써, 상호 공유하고자 하는 정보를 안전하게 전송할 수 있다.
- <66> 도 3은 도 2의 제1통신 단말기가 공개 채널을 통해 공유하고자 하는 정보에 대한 메시지 인증 코드값을 생성하기 위한 처리 과정에서 생성되는 값들의 예를 도시한 도면이다.
- <67> 도시된 바와 같이, 본 실시예에 따라 일회용 패스워드(pw_A), 제너레이터(g), 개인키(a)가 선택되고, 모듈러 역승연산을 통해 공개키(y_A)가 얻어지며, 해시 함수($h()$)를 통해 메시지 인증 코드 키(K_A)가 생성되고 최종적으로 메시지 인증 코드 알고리즘을 통해 전송하고자 하는 정보에 대한 메시지 인증 코드값(M_A)이 생성됨을 알 수 있다.
- <68> 이에 따라, 공개 채널을 통해 메시지 인증코드값(M_A) 및 공개키(y_A)를 포함하여 전송하고자 하는 정보들(g, p, q)이 수신자의 통신 단말기로 전송된다.
- <69> 한편, 도 1에서 제2통신 단말기(300)는 제1통신 단말기(100)로부터 전송된 메시지 인증코드값(M_A) 및 공개키(y_A)를 포함하는 전송 대상 정보들(g, p, q)을 수신한다.
- <70> 제2통신 단말기(300)는 제1통신 단말기(100)로부터 전송된 정보들을 수신하면, 수신한 해당 정보가 올바른 정보인지를 확인하는 과정을 수행한다. 즉, 제2통신 단말기(300)의 사용자인 수신자는 인증 채널을 통해 일회용 패스워드(pw_A)를 제1통신 단말기(100)의 사용자인 발신자로부터 제공받는다. 여기서 인증 채널은 전화 또는 인터넷 채팅 등 다양한 개인 대 개인(personal to personal: P2P) 통신이 가능한 채널이 될 수 있다.
- <71> 본 발명에 따른 제2통신 단말기(300)는 인증 채널을 사용하여 전송된 정보들에 대한 인증을 수행하는 데 필요한 메시지 인증 코드 키(K_B)를 생성한다. 인증 채널은 여러 가지 형태로 구성할 수 있다. 예를 들어, 상대방이 누구인지 아는 경우라면, 상대방의 목소리로 파악할 수 있으며, 또는 채팅 등을 통해 미리 정해 놓은 간단한 정보를 확인하는 절차를 통해 인증할 수도 있다. 회의실과 같이 같은 공간 내에 있는 경우라면, 무선 인터넷을 통해 값을 주고 받은 후, 직접 일회용 패스워드를 알려주거나 종이에 적어서 줄 수도 있다.
- <72> 도 4는 도 2의 제2통신 단말기가 인증 채널을 통해 일회용 패스워드를 수신 및 메시지 인증 코드값에 대한 검증을 위한 처리 과정에서 생성되는 값들의 예를 도시한 도면이다.
- <73> 도시된 바와 같이, 본 실시예에 따라 제2통신 단말기(300)는 인증 채널을 통해 수신한 일회용 패스워드(pw_A)를 이용하여 메시지 인증 코드 키(K'_A)를 복원하고 복원된 메시지 인증 코드 키(K'_A)를 이용하여 메시지 인증 코드값(M'_A)을 복원한다. 이에 따라, 메시지 제2통신 단말기(300)는 복원한 메시지 인증 코드값(M'_A)과 수신한 메시지 인증 코드값(M_A)을 체크하여 정확성 여부를 판별한다.
- <74> 이러한 판별 과정을 통해 제2통신 단말기(300)는 제1통신 단말기(100)로부터 수신한 정보가 사실인 것으로 판단되면, 제1통신 단말기(100)와 마찬가지로 일회용 패스워드(pw_B), 개인키(b)가 선택하고 모듈러 역승연산을 통해 공개키(y_B)를 얻으며, 해시 함수($h()$)를 통해 메시지 인증 코드 키(K_B)를 생성하고 최종적으로 메시지 인증 코드 알고리즘을 통해 제1통신 단말기(100)에 전송하여 공유하고자 하는 정보에 대한 메시지 인증 코드값(M_B)을 생성

하는 일련의 과정을 처리함을 알 수 있다.

- <75> 이에 따라, 제2통신 단말기(300)는 생성한 메시지 인증 코드값(M_B) 및 공개키(y_B)를 포함하여 전송하고자 하는 정보(g, p, q)를 제1통신 단말기(100)에 전송하여 제1통신 단말기(100)와 각 공개키를 비롯한 공유하고자 하는 정보를 상호 공유한다.
- <76> 이후 제1통신 단말기(100)는 제2통신 단말기(300)로부터 수신한 정보들에 대해 제2통신 단말기(300)가 수행하는 동일한 체크 과정을 통해 수신한 정보들을 정당성 여부를 검증하고 공개키를 비롯한 정보들을 상호 공유한다.
- <77> 본 발명에서 제안하는 공개키의 인증 및 키 교환을 위한 기술의 안전성은 기본적으로 해시함수와 메시지 인증 코드 알고리즘의 안전성에 기반으로 한다. 암호학적으로 안전한 해시함수와 메시지 인증 코드 알고리즘은 충돌 방지 성질을 제공하기 때문에, 임의의 다른 두 값이 같은 출력 값을 생성할 확률은 매우 낮다. 즉, 사용자 A가 정보를 전송하면서 메시지 인증 코드 값(M_A)을 같이 보내게 되는데, 임의의 공격자가 사용된 일회용 패스워드(pw_A)를 모르는 상태에서 사용자 A가 생성한 메시지 인증 코드 값과 같은 값을 출력하도록 정보들을 조작할 수 없다. 예를 들어, 사용자 A가 사용자 B에게 패스워드 'pw1'을 사용하여 메시지 인증 코드 키 $K_A(=h(A, B, pw1))$ 를 생성한 후, 정보 m 과 m 에 대한 메시지 인증 코드 값인 $MAC_{KA}(m)$ 을 생성하여 전송하는 경우에, 임의의 공격자 S가 m 대신 자신이 만든 임의의 정보인 q 를 사용자 B가 받도록 하고자 한다면, 자신이 선택한 임의의 메시지 인증 코드 키 t 를 사용하여 생성한 메시지 인증 코드 값, 즉, $MAC_{tS}(q)$ 가 $MAC_{KA}(m)$ 과 같게 설정해야 한다. 즉, $MAC_{tS}(q)$ 가 $MAC_{KA}(m)$ 과 같은 경우에만, 사용자 B는 아무런 의심 없이 q 를 받아들이고 사용하게 된다. 그러나, 서로 다른 입력 값들을 갖는 두 메시지 인증 코드 값($MAC_{tS}(q), MAC_{KA}(m)$)이 같아질 확률은 매우 낮기 때문에, 공격자 S의 이러한 공격은 성공할 가능성이 희박하다. 따라서, 본 발명에 따라 공개키 인증 및 키 공유 방법을 이용할 경우, 중간에 정보들이 조작되는 위험 없이 안전하게 사용될 수 있다.
- <78> 도 5는 본 발명의 바람직한 실시예에 따른 인증기관의 인증 처리 없이 공개키에 대한 상호 인증 및 키 교환을 위한 방법을 도시한 블록도이다.
- <79> 본 실시예는 본 발명의 장치가 도시된 도 2가 적용된다.
- <80> 먼저, 제1통신 단말기(100)는 일회용 패스워드(pw_A)를 생성하여 이를 기초로 메시지 인증 코드키(K_A) 및 공개키(y_A)에 대한 메시지 인증 코드 값(M)을 생성한다(S100).
- <81> 이에 따라, 제1통신 단말기(100)는 생성한 메시지 인증 코드 값(M_A) 및 전송 대상 정보들을 공개 채널을 통해 수신자(본 실시예에서는 제2통신단말기(300))에게 전송한다(S200).
- <82> 한편, 제2통신 단말기(300)는 공개 채널을 통해 제1통신 단말기(100)로부터 전송된 메시지 인증 코드 값(M_A) 및 전송 대상 정보를 수신한다(S310).
- <83> 제2통신 단말기(300)는 인증 채널을 통해 제1통신 단말기(100)와 통화 연결하고 연결된 인증 채널을 통해 제1통신 단말기(100)에서 생성된 일회용 패스워드(pw)를 제공 받는다(S330).
- <84> 이에 따라, 제2통신 단말기(300)는 제공 받은 일회용 패스워드(pw_A)를 이용하여 메시지 인증 코드 값(M_A)에 대한 검증 과정을 수행한다(S350).
- <85> 메시지 인증 코드 값(M_A)에 대한 검증을 통해 메시지 인증 코드 값(M_A)이 정당한 값인 것으로 판별되면, 제2통신 단말기(300)는 일회용 패스워드(pw_B)를 생성하고 생성한 일회용 패스워드(pw_B)를 통해 메시지 인증 코드키(K_B) 및 공개키(y_B)에 대한 메시지 인증 코드 값(M)을 생성한다(S370).
- <86> 이에 따라, 제2통신 단말기(300)는 공개 채널을 통해 메시지 인증 코드 값(M_B) 및 공유하고자 하는 정보들인 전송 대상 정보를 제1통신 단말기(100)에 전송한다(S390).
- <87> 따라서, 공개 채널을 통해 공유하고자 하는 정보들을 전송하고 인증 채널을 통해 일회용 패스워드를 전송함으로써, 인증 서버가 비정상적인 상태에서 상호 간에 안전한 방법으로 상호 인증 및 키 교환을 수행할 수 있다.

- <88> 도 6은 도 5에서 제1통신단말기(100)의 메시지 인증 코드 값(M_A) 생성 단계(S100)를 보다 상세히 도시한 흐름도이다.
- <89> 먼저, 제1통신 단말기(100)는 일회용 패스워드 생성부(110)를 통해 임의의 일회용 패스워드(pw_A)를 생성(선택)한다(S110). 제1통신 단말기(100)는 공개키 생성을 위한 제너레이터, 즉 생성기(g)를 선택한다(S120). 제1통신 단말기(100)는 개인키 생성부(130)를 통해 개인키(a)를 생성(선택)한다(S130). 또한 제1통신 단말기(100)는 공개키 생성부(140)를 통해 S120 단계에서 선택한 생성기(g)를 이용하여 개인키(a)에 대한 공개키(y_A)를 생성한다(S140).
- <90> 이에 따라, 제1통신 단말기(100)는 입력되는 명령에 따라 수신측에 전송하여 함께 공유할 전송대상정보를 선택한다(S150). 제1통신 단말기(100)는 메시지 인증 코드 키 생성부(120)를 통해 일회용 패스워드에 대한 메시지 인증 코드 키(K_A)를 생성한다(S160). 제1통신 단말기(100)는 메시지 인증 코드값 생성부(160)를 통해 메시지 인증 코드 키(K_A)를 통한 공개키(y_A)를 비롯한 전송할 정보들에 대한 메시지 인증 코드 값(M_A)을 생성한다(S170).
- <91> 도 7은 도 5의 메시지 인증 코드 값(M)에 대한 검증 단계(S350)를 보다 상세히 나타낸 흐름도이다.
- <92> 먼저, 제2통신 단말기(300)는 인증 채널을 통해 제1통신 단말기(100)로부터 수신한 일회용 패스워드(pw_A)를 이용하여 메시지 인증 코드 키(K_A)를 복원한다(S352). 제2통신 단말기(300)는 복원한 메시지 인증 코드 키(K'_A)를 이용하여 메시지 인증 코드 값(M)을 복원한다(S354).
- <93> 이때 제2통신 단말기(300)는 복원한 메시지 인증 코드 값(M'_A)과 수신한 메시지 인증 코드 값(M_A)을 비교하여 메시지 인증 코드 값(M_A)에 대한 인증을 처리한다(S356). 이에 따라, 제2통신 단말기(300)는 복원한 메시지 인증 코드 값(M'_A)이 수신한 메시지 인증 코드 값(M)과 같은 지를 판별한다(S358).
- <94> 복원한 메시지 인증 코드 값(M'_A)이 수신한 메시지 인증 코드 값(M_A)과 같은 것으로 판단되면, 제2통신 단말기(300)는 도 5의 S370 단계를 수행한다. 제2통신 단말기(300)는 복원한 메시지 인증 코드 값(M'_A)이 수신한 메시지 인증 코드 값(M_A)과 같지 않은 것으로 판단되면, 상호 인증 및 키 공유를 위한 프로세스를 과정을 종료한다.
- <95> 도 8은 도 5에서 제2통신 단말기(300)의 메시지 인증 코드 값(M_B) 생성 단계(S370)를 보다 상세히 도시한 흐름도이다.
- <96> 먼저, 제2통신 단말기(300)는 일회용 패스워드(pw_B)를 생성(선택)한다(S371). 제2통신 단말기(300)는 개인키(b)를 생성(선택)한다(S372). 또한 제2통신 단말기(300)는 제1통신 단말기(100)에서 수신한 생성기(g)를 이용하여 개인키(b)에 대한 공개키(y_B)를 생성한다(S373).
- <97> 이에 따라, 제2통신 단말기(300)는 입력되는 명령에 따라 제1통신 단말기(100)에 전송하여 함께 공유할 전송대상정보를 선택한다(S375). 제2통신 단말기(300)는 일회용 패스워드(pw_B)에 대한 메시지 인증 코드 키(K_B)를 생성한다(S376). 제2통신 단말기(300)는 메시지 인증 코드 키(K_B)를 통한 공개키(y_B)를 비롯한 전송할 정보들에 대한 메시지 인증 코드 값(M)을 생성한다(S377).
- <98> 이상에서는 본 발명에서 특정의 바람직한 실시예에 대하여 도시하고 또한 설명하였다. 그러나, 본 발명은 상술한 실시예에 한정되지 아니하며, 특허 청구의 범위에서 첨부하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능할 것이다.

발명의 효과

- <99> 본 발명에 따르면, 일회용 패스워드를 생성하고 생성한 일회용 패스워드에 대한 메시지 인증 코드 키를 생성하고 생성한 메시지 인증 코드 키를 기초로 공개키에 대한 메시지 인증 코드 값을 생성하여 공개키를 비롯한 전송대상 정보와 함께 공개 채널을 통해 수신측에 전송하고 인증 채널을 통해 일회용 패스워드를 수신측에 제공함으로써, 인증 서버를 통한 인증이 불가능한 경우 중간에 조작되는 정보들이 조작되는 위험 없이 상호 간에 안전한

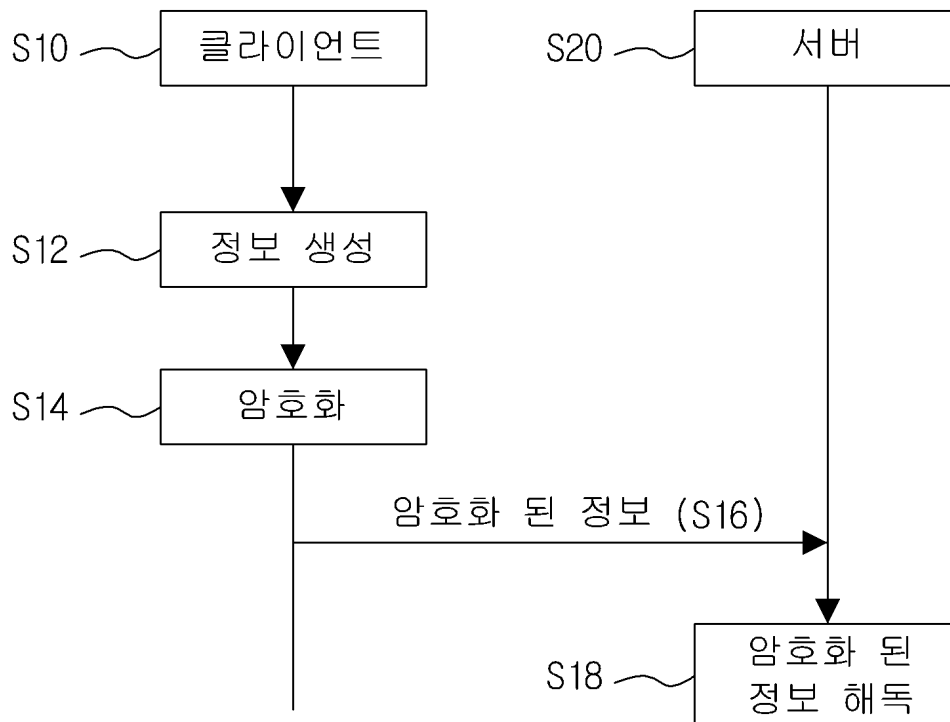
게 상호 인증 및 키 교환을 수행할 수 있다.

도면의 간단한 설명

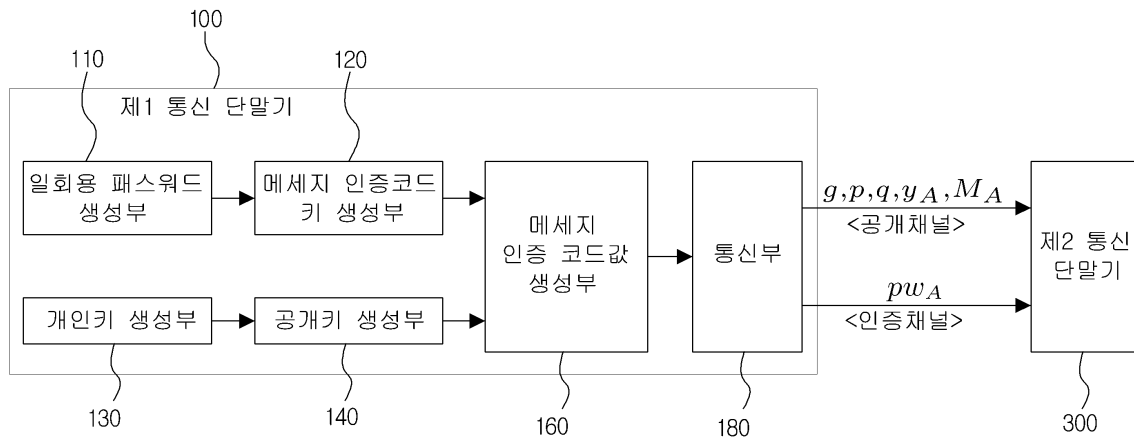
- <1> 도 1은 일반적인 암호 알고리즘에 대한 절차를 간략하게 도시한 흐름도,
- <2> 도 2는 본 발명의 바람직한 실시예에 따른 인증기관의 인증 처리 없이 공개키에 대한 상호 인증 및 키 교환을 위한 통신 장치를 도시한 블록도,
- <3> 도 3은 도 2의 제1통신 단말기가 공개 채널을 통해 공유하고자 하는 정보에 대한 메시지 인증 코드값을 생성하기 위한 처리 과정에서 생성되는 값들의 예를 도시한 도면,
- <4> 도 4는 도 2의 제2통신 단말기가 인증 채널을 통해 일회용 패스워드를 수신 및 메시지 인증 코드값에 대한 검증을 위한 처리 과정에서 생성되는 값들의 예를 도시한 도면,
- <5> 도 5는 본 발명의 바람직한 실시예에 따른 인증기관의 인증 처리 없이 공개키에 대한 상호 인증 및 키 교환을 위한 방법을 도시한 블록도,
- <6> 도 6은 도 5에서 제1통신단말기의 메시지 인증 코드 값(M) 생성 단계를 보다 상세히 도시한 흐름도,
- <7> 도 7은 도 5의 메시지 인증 코드 값(M)에 대한 검증 단계를 보다 상세히 나타낸 흐름도, 그리고
- <8> 도 8은 도 5에서 제2통신 단말기의 메시지 인증 코드 값(M) 생성 단계를 보다 상세히 도시한 흐름도이다.

도면

도면1



도면2



도면3

Public Channel

$$pw_A \leftarrow_R \mathcal{D}$$

$$g \leftarrow_R \mathcal{G}$$

$$a \leftarrow_R Z_q^*$$

$$y_A = g^a \bmod p$$

$$K_A = h(\text{Alice}, \text{Bob}, pw_A)$$

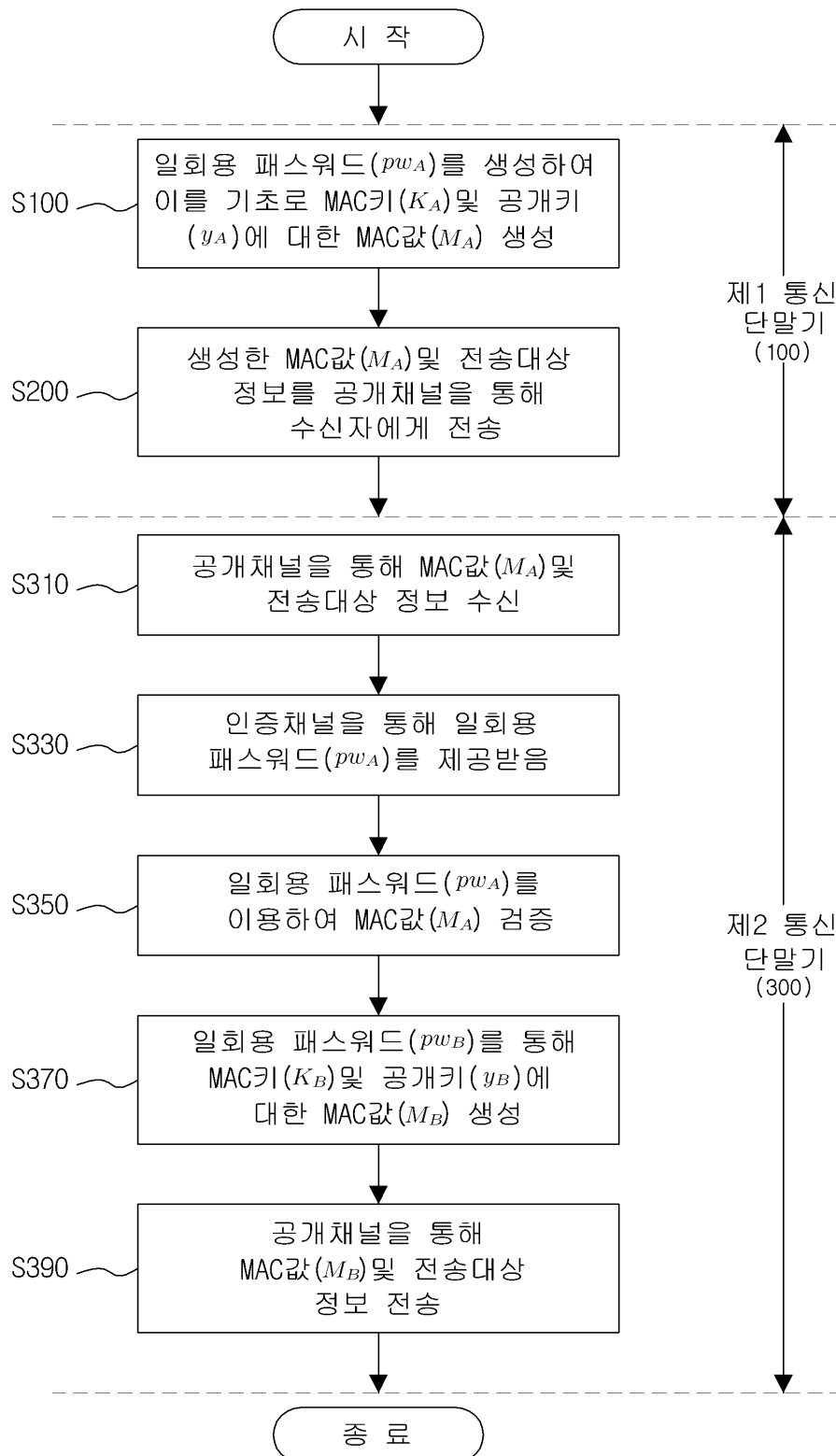
$$M_A = MAC_{K_A}(\text{Alice}, \text{Bob}, g, p, q, y_A) \xrightarrow{g, p, q, y_A, M_A}$$

도면4

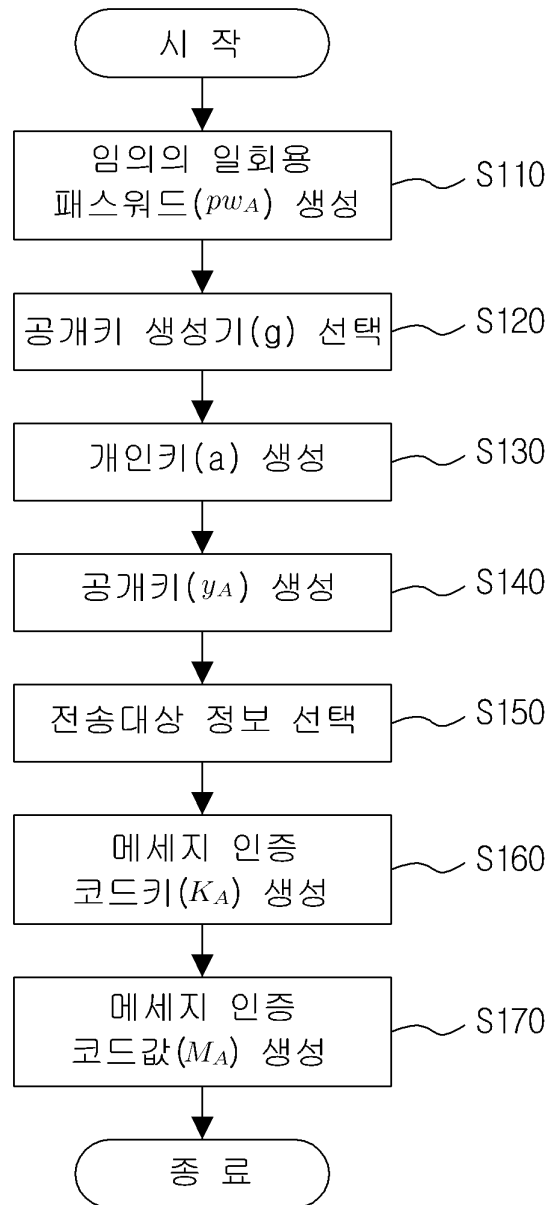
Authenticated Channel

$\xrightarrow{pw_A} K'_A = h(\text{Alice}, \text{Bob}, pw_A)$
 $M'_A = MAC_{K'_A}(\text{Alice}, \text{Bob}, g, p, q, y_A)$
 check $M'_A = M_A$
 if TRUE
 $pw_B \leftarrow_R \mathcal{D}$
 $b \leftarrow_R Z_q^*$
 $y_B = g^b \bmod p$
 $K_B = h(\text{Alice}, \text{Bob}, pw_B)$
 $M_B = MAC_{K_B}(\text{Alice}, \text{Bob}, g, p, q, y_B)$
 else
 terminate

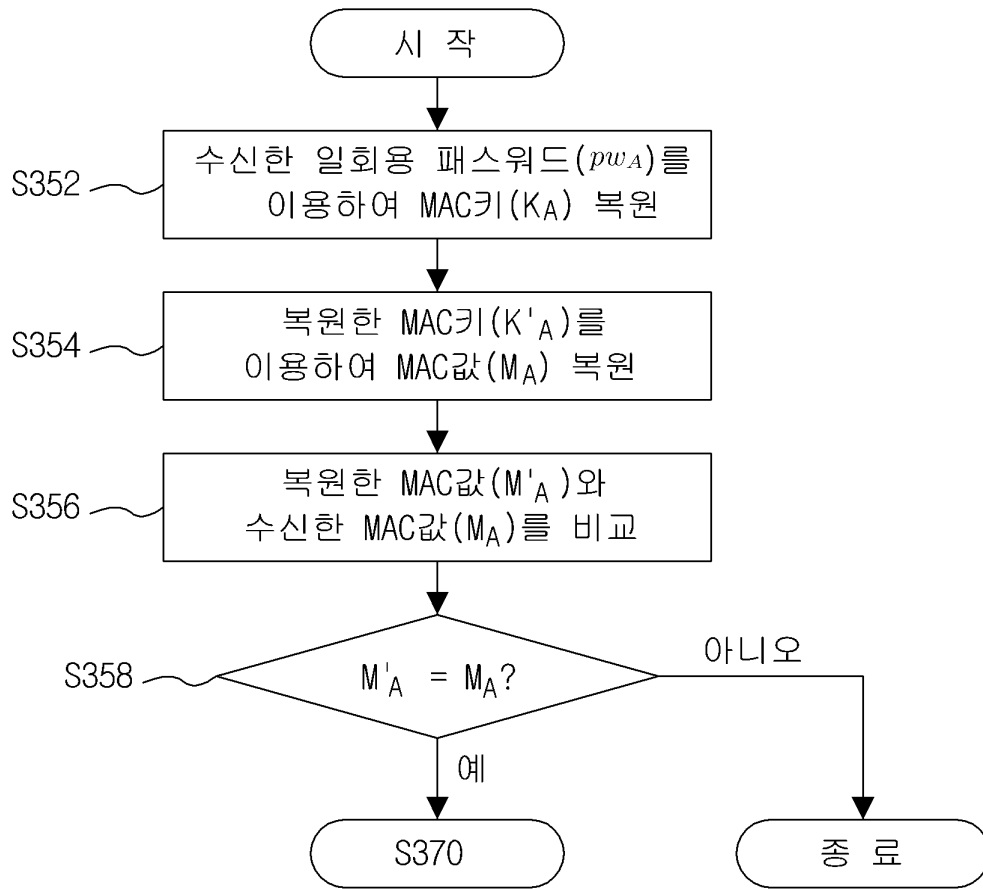
도면5



도면6



도면7



도면8

