(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년07월26일
(11) 등록번호 10-1169100
(24) 등록일자 2012년07월20일

(51) 국제특허분류(Int. Cl.)
G06F 15/00 (2006.01)
(21) 출원번호 10-2006-0012469
(22) 출원일자 2006년02월09일
심사청구일자 2011년01월28일
(65) 공개번호 10-2006-0097583
(43) 공개일자 2006년09월14일
(30) 우선권주장
11/074,885 2005년03월07일 미국(US)
(56) 선행기술조사문헌
EP1478121 A2
JP2005500740 A
JP2004336794 A

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
보츠, 앤드류
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
난다, 아룬 케이.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
(뒷면에 계속)
(74) 대리인
제일특허법인

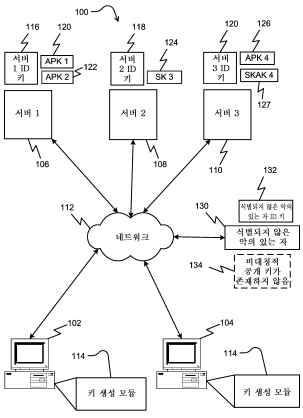
전체 청구항 수 : 총 18 항 심사관 : 박태식

(54) 발명의 명칭 **비대칭 키 보안을 위한 시스템 및 방법**

(57) 요 약

본원에 게시된 예시적인 실시예는, 웹사이트로부터 신원 키를 수신하는 단계, 마스터 키를 생성하는 단계, 신원 키 및 마스터 키의 암호화 함수를 이용함으로써 쌍-단위 대칭 키 또는 비대칭 키 쌍을 생성하는 단계, 및 클라이언트 및 웹사이트에 쌍-단위 공개 또는 비대칭 키를 저장하는 단계를 포함하는, 쌍-단위 보안 키를 생성하는 시스템 및 방법을 포함할 수 있다.

대 표 도 - 도1



(72) 발명자

시몬, 다니엘 알.

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

쇼우척, 존 피.

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

베날로, 조쉬 디.

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

카메론, 킴

미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

특허청구의 범위

청구항 1

복수의 서버 각각과의 이전의 인터렉션(previous interaction)을 인증하기 위해 비대칭 보안 키들을 생성하는 방법으로서,

상기 복수의 서버 중 제1 서버에 관련된 제1 ID 키(first identity key)를 수신하는 단계;

상기 제1 서버에 대응하는 제1 마스터 키(first master key)를 생성하는 단계;

상기 제1 ID 키 및 상기 제1 마스터 키의 암호화 함수를 이용함으로써 하나 이상의 시드(seed)를 생성하는 단계;

상기 하나 이상의 시드를 이용하여 상기 제1 서버에 대응하는 비대칭 공개 키 및 비대칭 개인 키 쌍을 생성하는 단계;

상기 제1 서버에 상기 비대칭 공개 키를 저장하라고 요청하는 단계;

클라이언트에서 상기 비대칭 개인 키를 저장하는 단계; 및

상기 제1 서버와의 이전의 인터렉션을 인증하는 단계를 포함하고,

상기 제1 서버와의 이전의 인터렉션을 인증하는 단계는,

상기 비대칭 공개 키를 알고 있음(knowledge of)에 대한 증명(proof)이 상기 제1 서버에 의해 요청된다면, 상기 비대칭 공개 키를 알고 있음에 대한 증명을 상기 제1 서버에 제시하고 상기 비대칭 개인 키를 송신하지 않고 상기 제1 서버를 액세스하는 단계; 및

상기 비대칭 공개 키를 알고 있음에 대한 증명에 추가하여 상기 비대칭 개인 키를 가지고 있음(possession of)에 대한 증명이 상기 제1 서버에 의해 요청된다면, 상기 비대칭 개인 키를 가지고 있음에 대한 증명을 상기 제1 서버에 제시하고 상기 제1 서버를 액세스하는 단계를 포함하는 방법.

청구항 2

제1항에 있어서,

상기 하나 이상의 시드를 생성하는 단계는 하나 이상의 상수들을 이용하는 단계를 더 포함하는 방법.

청구항 3

제1항에 있어서,

상기 비대칭 공개 키를 이용하여 상기 클라이언트가 이전에 상기 제1 서버를 액세스하였는지 여부를 판정하는 단계를 더 포함하는 방법.

청구항 4

제1항에 있어서,

상기 클라이언트가 이전에 상기 제1 서버를 액세스하였다는 판정에 응답하여, 상기 제1 서버를 액세스하는 단계를 더 포함하는 방법.

청구항 5

제1항에 있어서,

상기 비대칭 공개 키를 이용하여 상기 제1 서버를 인증하는 단계를 더 포함하는 방법.

청구항 6

제1항에 있어서,

상기 제1 마스터 키를 생성하는 단계는 난수(random number)를 생성하는 단계를 포함하는 방법.

청구항 7

제1항에 있어서,

상기 하나 이상의 시드를 생성하는 단계는 상기 제1 ID 키, 상기 제1 마스터 키, 및 상수의 해쉬 함수를 이용하는 단계를 포함하는 방법.

청구항 8

제1항에 있어서,

상기 제1 서버는 웹 서버를 포함하는 방법.

청구항 9

제1항에 있어서,

상기 비대칭 키 쌍을 시드로서 이용하여 대칭 키를 생성하는 단계를 더 포함하는 방법.

청구항 10

제1항에 있어서,

상기 비대칭 공개 키는 상기 제1 ID 키에 적어도 일부 기초하는 방법.

청구항 11

제1항에 있어서,

상기 제1 ID 키를 수신하는 단계는 웹사이트와 관련된 인증서(certificate)를 수신하는 단계를 포함하는 방법.

청구항 12

비대칭 키 쌍을 이용하여 하나 이상의 서버와의 이전의 인터렉션을 인증하기 위한 시스템으로서,

프로세서;

상기 프로세서에 접속된 통신 채널; 및

상기 프로세서와 연결되며 상기 프로세서에 의해 판독가능한 메모리를 포함하고,

상기 메모리는, 상기 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

제1 서버에 관련된 제1 ID 키를 수신하고,

제1 마스터 키를 생성하고,

상기 제1 ID 키 및 상기 제1 마스터 키의 암호화 함수를 이용함으로써 시드를 생성하고,

상기 시드를 이용하여 비대칭 개인 키 및 비대칭 공개 키 쌍을 생성하고,

상기 제1 서버에 상기 비대칭 공개 키를 저장하라고 요청하고,

클라이언트에서 상기 비대칭 개인 키를 저장하고,

상기 제1 서버와의 이전의 인터렉션을 인증하게 하는 일련의 명령어를 포함하고,

상기 제1 서버와의 이전의 인터렉션을 인증하는 것은,

상기 제1 서버로부터 상기 비대칭 공개 키를 알고 있음에 대한 증명을 요청하는 것과,

상기 비대칭 공개 키를 알고 있음에 대한 증명을 수신하면, 상기 제1 서버를 액세스하는 것을 포함하는 시스템.

청구항 13

제12항에 있어서,

상기 제1 마스터 키를 생성하는 것은 난수를 생성하는 것을 포함하는 시스템.

청구항 14

제12항에 있어서,

상기 시드를 생성하는 것은 상기 제1 ID 키, 상기 제1 마스터 키, 및 하나 이상의 상수의 해쉬 함수를 이용하는 것을 포함하는 시스템.

청구항 15

제12항에 있어서,

상기 명령어는

상기 비대칭 공개 키에 적어도 일부 기초하여 상기 제1 서버로부터 인증에 대한 요청을 수신하게 하는 명령어를 더 포함하는 시스템.

청구항 16

하나 이상의 서버와의 이전의 인터렉션을 인증하기 위한 컴퓨터 구현 방법을 실행시키기 위한 명령어들의 컴퓨터 프로그램을 인코딩하는 컴퓨터 판독가능 기억 매체로서,

상기 방법은

제1 서버에 관련된 제1 ID 키를 수신하는 단계;

제1 마스터 키를 생성하는 단계;

상기 제1 ID 키, 상기 제1 마스터 키 및 하나 이상의 상수의 암호화 함수를 이용함으로써 하나 이상의 시드를 생성하는 단계;

상기 하나 이상의 시드를 이용하여 비대칭 개인 키 및 비대칭 공개 키 쌍을 생성하는 단계;

상기 제1 서버에 상기 비대칭 공개 키를 저장하라고 요청하는 단계;

클라이언트에서 상기 비대칭 개인 키를 저장하는 단계; 및

상기 제1 서버와의 이전의 인터렉션을 인증하는 단계를 포함하고,

상기 제1 서버와의 이전의 인터렉션을 인증하는 단계는,

상기 비대칭 공개 키를 알고 있음에 대한 증명을 상기 제1 서버에 제시하는 단계;

상기 제1 서버로부터 상기 비대칭 개인 키를 가지고 있음에 대한 증명의 요청을 수신하는 단계;

상기 비대칭 개인 키를 가지고 있음에 대한 증명을 상기 제1 서버에 제시하는 단계;

상기 제1 서버로부터 상기 클라이언트가 인증되었으며 액세스가 허용된다는 표시자(indication)를 수신하는 단계를 포함하는 컴퓨터 판독가능 기억 매체.

청구항 17

제16항에 있어서,

상기 비대칭 키는 대칭 키로서 작용하는 컴퓨터 판독가능 기억 매체.

청구항 18

제16항에 있어서,

상기 암호화 함수는 상기 제1 ID 키, 상기 제1 마스터 키, 및 하나 이상의 상수의 해쉬 함수인 컴퓨터 판독가능 기억 매체.

청구항 19

삭제

청구항 20

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0018] 본 발명은 일반적으로 컴퓨터 및 네트워크 보안과 같은 전자 보안 분야에 관한 것이며, 보다 상세히는 컴퓨터 시스템 및 사용자의 신원 인증에 관한 것이다.

[0019] 통상적인 전자 보안은 공개 키/개인 키 시스템을 이용하여 인터넷과 같은 네트워크를 통하여 자원들을 액세스하는 자들을 인증할 수 있다. 이들 공개 키/개인 키 시스템은 일정하며 웹사이트와 같은 다수의 서로 다른 자원들에 대하여 이용되는 하나의 공개 키, 및 자원들을 액세스하는 클라이언트 컴퓨터와 같은 발신자만이 액세스할 수 있는 하나의 개인 키를 가지고 동작한다. 이 전자 보안 키 시스템은 발신자를 식별하는 고정 키가 다수의 다른 웹사이트들이 발신자에 대한 많은 정보 및 이들의 습관, 참조 등을 얻는 데에 이용될 수 있다는 점을 포함하는 중대한 단점을 가진다. 이러한 시스템은 공개 키와 일치하고 이 일치되는 공개 키에 대응하는 정보를 교환하는 다양한 웹사이트 운영자들에 의해 수행될 수 있다. 또한, 웹사이트들의 운영자들은 일단 공개 키들이 일치되면 진행 기반(ongoing basis)으로 자유롭게 발신자에 대한 정보를 교환하여 사용자의 습관에 관한 정보 등을 더 획득할 수 있다.

발명이 이루고자 하는 기술적 과제

[0020] 본원에 게시된 예시적인 실시예는 상술한 단점 및 다른 단점들을 완화하는 시스템 및 방법을 포함할 수 있다. 본원에 게시된 예시적인 실시예들은 마스터 키를 생성하는 단계, 서버로부터 신원 키를 수신하는 단계, 신원 키, 마스터 키, 및 상수(들)의 해쉬(hash) 또는 암호화 함수를 이용함으로써 시드(seed)를 생성하는 단계, 및 이 시드를 키 또는 키 쌍을 생성하는 프로세스로의 입력으로서 이용하는 단계를 포함하는, 비대칭 키 쌍(들)을 생성하는 시스템 및 방법을 포함한다. 본원에 기술된 예시적인 실시예에서, 이 시드는 비대칭 키 쌍을 생성하는 데에 이용되며, 결과인 공개 비대칭 키는 서버에 저장된다.

[0021] 다른 실시예들은, 클라이언트 컴퓨터에서 공개 비대칭 키를 산출하는 단계, 이 공개 비대칭 키가 서버에서 이용가능한 대응하는 비대칭 키와 일치하는지 여부를 판정하는 단계, 및 비대칭 키가 일치하면 서버 및/또는 클라이언트를 인증하는 단계를 포함하는, 웹사이트 및/또는 서버나 사용자 시스템을 인증하는 시스템 및 방법을 포함한다.

[0022] 또 다른 실시예들은 마스터 키를 생성하는 단계, 서버로부터 신원 키를 수신하는 단계, 신원 키, 마스터 키, 및 상수(들)의 암호화 함수를 이용함으로써 시드를 생성하는 단계, 및 이 시드를 안전한 대칭 키를 생성하는 프로세스로의 입력으로서 이용하는 단계, 및 서버와 클라이언트 간의 대칭 인증 프로세스를 게시함으로써 이 대칭 키가 서버에서 이용가능한 대응하는 대칭 키와 일치하는지 여부를 판정하는 단계를 포함하는, 웹사이트 및/또는 서버나 사용자 시스템을 인증하는 시스템 및 방법을 포함한다.

[0023] 본원에 게시된 예시적인 실시예는 컴퓨터 프로세스, 컴퓨팅 시스템, 또는 컴퓨터 프로그램 제품과 같은 제조품으로서 구현될 수 있다. 컴퓨터 프로그램 제품은 컴퓨터 시스템에 의해 판독가능하고 컴퓨터 프로세스를 실행하는 명령어들로 된 컴퓨터 프로그램이 인코딩되어 있는 컴퓨터 저장 매체일 수 있다. 컴퓨터 프로그램 제품은 또한 컴퓨팅 시스템에 의해 판독가능하고 컴퓨터 프로세스를 실행하는 명령어들로 된 컴퓨터 프로그램이 인코딩되어 있는 반송파에 의해 전파되는 신호일 수 있다.

[0024] 본 게시물의 보다 완전한 평가 및 그 이점은 이하 간단히 요약된 첨부된 도면, 바로 다음의 본 발명의 바람직한 실시예의 상세한 설명, 및 특허 청구 범위로의 참조에 의해 얻을 수 있다.

발명의 구성 및 작용

[0025] 도 1은, 일반적으로 참조번호(100)로, 예시적인 실시예에 따라서 비대칭적 키 쌍(들)을 생성하고 ID(identification)를 인증하는 데에 이용될 수 있는 시스템의 블럭도이다. 이러한 실시예에서, 시스템(100)은 클라이언트들(102, 104)을 가진다. 클라이언트들(102, 104)은 네트워크(112)에 접속되고, 이 네트워크는 서버 1(106), 서버 2(108), 및 서버 3(110)에 접속된다. 네트워크(112)는 클라이언트들(102 및 104)과 서버들(106, 108, 110) 간에 통신하는 데에 이용될 수 있는 인터넷, 또는 다른 통신 채널일 수 있다. 본 기술 분야에서 숙련된 기술을 가진 자라면 시스템(100)은 단지 예시적인, 클라이언트들 및 서버들과의 통신 시스템이며, 다양한 대안적이고 다른 구성이 이용될 수 있음을 인식할 것이다.

[0026] 이러한 실시예에서, 클라이언트들(102 및 104)은 각각 키 생성 모듈들(114 및 115)을 가진다. 키 생성 모듈들(114 및 115)은 대칭적 키(들) 및/또는 비대칭적 키 쌍(들)을 생성할 수 있다.

[0027] 비대칭적 키들을 포함하는 예시적인 실시예에서, 비대칭적 키 쌍(들)은 이들의 값이, 동일한 함수를 동일한 입력 값들을 가지고 반복함으로써, 다시 산출될 수 있도록 알려진 입력들에 기초하여 계산된 고유한 값들이다. 그 다음 서버들의 고정된 ID 키들 및/또는 클라이언트 상의 키 생성 모듈에 의해 생성된 공개 키들이 상호 인증에 이용된다. 즉, 클라이언트는 서버를 검사할 수 있고 서버 또한 클라이언트를 검사할 수 있다.

[0028] 클라이언트들(102 및 104)은 서버들(106, 108, 110)에 정보를 요청하고 송신한다. 마찬가지로, 서버들(106, 108, 110)은 정보에 대한 요청을 수신하고 응답하기를 시도한다. 또한, 서버들은 클라이언트들로부터 직접 정보를 요청할 수 있다. 때때로, 민감한 정보가 서버에 송신된다. 서버 및 클라이언트들을 보호하기 위하여, 시스템(100)은 대칭적 또는 비대칭적 키 보안을 포함한다. 이들 보안 특징들을 이용하면, 클라이언트 시스템들은 정보를 훔치려 하는 부적절한 서버 기술로부터 어느 정도 보호될 수 있다.

[0029] 클라이언트(102)는 서버 1(106)과 관련된 ID 키(116)를 요청할 수 있다. 그 다음 클라이언트(102)는 마스터 키를 생성하고 신원 키(116), 마스터 키, 및 상수(들)를 이용하여 키 생성 모듈(114)로 비대칭 공개 키(APK) 1(120)을 포함하는 비대칭적 키 쌍을 생성할 수 있다. 그 다음 비대칭적 공개 키 1(120)은 서버 1(106)에 저장될 수 있고, 대응하는 개인 비대칭 키가 클라이언트(102)에 저장될 수 있어서, 클라이언트(102)가 서버 1(106)을 다시 방문하고/거나, 클라이언트(102)의 사용자가 서버 1(106)을 다시 방문할 때, 이 클라이언트가 이전에 서버 1(106)을 액세스하였는지 여부를 판정할 수 있도록 비대칭적 공개 키(120)를 알고 있음에 대한 확인을 요청할 수 있도록 한다. 이러한 실시예는 또한 비대칭적 공개 키 1(120)을 통하여 서버 1(106) 및/또는 관련된 웹사이트의 신뢰성을 판정하는 데에 이용될 수 있다. 또한, 클라이언트(102)는 개인 비대칭 키를 버리고 그 후에 비대칭 키 쌍을 다시 생성하고 서버를 다시 액세스할 때 비대칭 공개 키를 진행중인 디지털 관계가 존재하는 서버에게 제시하여 확인할 수 있다.

[0030] 클라이언트(102)는 서버 1(106)을 다시 액세스할 때 다시 생성된 비대칭적 공개 키를 서버 1(106)에게 제시하여 클라이언트(102)를 검사할 수 있다. 클라이언트(102) 및 서버 1(106)은 모두 서로가 신원을 검사하는 것에 대하여 더 확실할 것을 요구할 수 있다. 이들 더 확실할 것이란 이 쌍으로부터의 공개 또는 개인 키 중 하나의 홀더(holder)만이 복호화하고, 이해할 수 있고/거나 응답할 수 있도록 하는 형태일 수 있다.

[0031] 비대칭 키 메카니즘들을 이용할 때, 클라이언트(102)가 각 서버(106, 108 및 110) 마다 서로 다른 키 쌍을 생성하고, 암호화된 채널을 이용하여 공개 키를 전달하기 때문에, 신원을 검사하기 위해서 비대칭적 공개 키를 알고 있음에 대한 확인을 제시하기만 하는 것이 충분할 수 있다. 이는 비대칭 공개 키가 편할 경우 대칭 키로서 작용할 수 있음을 의미한다. 다른 경우 서버는 관련된 개인 키의 소유 여부에 대한 확인을 요구하도록 구성될 수 있다.

[0032] 마찬가지로, 다른 클라이언트(104)도 서버 1(106) 및 요청 서버 1 ID 키(116)를 액세스할 수 있다. 서버 1 ID 키(116)는 또한 제3자로부터 인증서, 또는 보안 인증서를 요청하고 이 인증서를 파싱(parse)하여 신원 키, 또는 다른 신원 정보를 획득함으로써 획득될 수 있다. 신원 키 및/또는 보안 인증서를 획득하는 다른 방법 및 시스템이 본원에 게시된 개념을 벗어나지 않고 이용될 수 있다고 인식될 것이다. 마찬가지로, 클라이언트(104)도 ID 키(116), 다른 마스터 키 및 선택적으로 상수(들)를 이용하여 비대칭 공개 키 (APK) 2(122)를 생성할 수 있다. 그 다음 클라이언트 2(104)는 비대칭 공개 키 2(122)를 서버 1(106)과 관련시킬 수 있다. 그 다음 클라이언트(104)는 대응하는 개인 비대칭 키를 저장하거나, 버리고 다음에 서버를 액세스할 때 키 쌍을 다시 생성할 수 있다.

[0033] 비대칭적 공개 키 2(122)는 클라이언트(104)와 관련된 키 생성 모듈(114)에 의해 생성될 수 있다. 상술한 방법과 마찬가지로, 클라이언트(104)가 다음에 서버 1(106)을 액세스할 때, 클라이언트는 이전에 서버 1(106)을 액

세스하였고/거나 서버 1(106)에 소정의 신원 정보를 제공하였는지 여부를 판정할 수 있도록 비대칭 공개 키 2(122)를 알고 있음에 대한 확인을 요청할 수 있다. 마찬가지로, 클라이언트(104)는 비대칭적 공개 키 2(122)를 알고 있음에 대한 확인을 생성하고 서버 1(106)에 진술하여 클라이언트(104)의 신원을 인증할 수 있거나, 관련된 개인 키의 소유 여부에 대한 확인을 요구할 수 있다.

[0034] 또한, 클라이언트 1(102)은 서버 2(108) 및 요청 서버 2 ID 키(118)를 액세스할 수 있다. 클라이언트(102)는 ID 키(118)를 수신한 이후에 ID 키(118) 및 다르거나 동일한 마스터 키, 및 상수(들)를 이용하여 대칭 키 3(SK)(124)을 생성할 수 있다(이 경우 시드는 비대칭 키에서보다는 대칭 키를 생성하는 모듈에 제공된다). 그 다음 대칭 키는 암호화된 채널을 이용하여 서버 2(108)에게 전달된다.

[0035] 그 다음 클라이언트(102)는 서버 2(108)를 다시 액세스할 때 대칭 키 3(124)를 알고 있음에 대한 확인을 요청할 수 있다. 마찬가지로, 서버는 클라이언트에 의해 키를 알고 있음에 대한 확인을 요구할 수 있다. 오직 이 사용자만이 대칭 키를 생성하는 데에 이용되는 마스터 키 등을 가질 것이다. 클라이언트(102)는 각각 및 모든 방문된 웹사이트 및/또는 서버마다 서로 다른 대칭 키들을 저장할 수 있고, 서버가 이전에 액세스되었는지를 판정하도록 이들 키를 알고 있음에 대한 확인을 요청할 수 있다. 또한, 서버에 대칭 키를 저장하였던 특정 클라이언트 또는 사용자만이 요구되는 상호 인증을 전달할 수 있을 것이기 때문에 대칭적 키가 서버, 클라이언트, 및/또는 웹사이트들을 인증하는 데에 이용될 수 있다.

[0036] 마찬가지로, 클라이언트(104)는 서버 3(110)을 액세스하고 서버 3 ID 키(120)를 요청할 수 있다. 그 다음 클라이언트(104)는 키 생성 모듈(114)을 이용하여 서버 3 ID 키(120) 및 선택적으로 상수와 함께, 이용될 무작위 마스터 키를 생성하여 다음에 서버 3(110)에 저장되거나 이 서버와 관련될 수 있는 비대칭 공개 키(APK) 4(126)를 생성할 수 있다. 그 다음 클라이언트(104)도 마스터 키, 서버 3 ID 키 및 몇몇의 상수로부터 유도된 키와 같은 대칭 키 아래에 비대칭 키 쌍을 암호화하여 비대칭 키 쌍을 비대칭 공개 키 APK 4(126)와 관련된 서버 3에서의 시드(SKAK)(127) 및 이 서버의 관련된 신원으로서 이용하도록 만들어진 이러한 대칭 키를 저장할 수 있다. 비대칭 키(127)를 이용하는 대칭 키가 암호화되기 때문에, 클라이언트(104)만이 이를 복호화할 수 있거나 이 정보를 이용하여 비대칭 키 쌍을 검색할 것이다. 그러므로, 비대칭 키(127)를 이용하는 대칭 키는 클라이언트(104)가 자신이 이전에 서버 3(110)를 액세스하였는지 여부를 판정하는 데에 이용될 수 있다. 또한, 이전에 방문된 서버만이 특정 클라이언트로부터 비대칭 키를 이용하는 관련된 대칭키를 가질 것이므로 이러한 구성은 웹사이트 및/또는 서버를 인증하는 데에 이용될 수 있다. 또한, 서버를 방문할 때 비대칭 키를 이용하는 대칭 키를 복호화할 수 있는 클라이언트는 비대칭 공개 키를 이용하여 서버로의 자신의 고유의 신원을 인증할 수 있다.

[0037] 상술한 바와 같이, 믿을만하지 못한 사람들은 클라이언트 및/또는 클라이언트의 사용자를 속여 개인적인 정보를 제공하게 하려는 시도를 할 수 있다. 식별되지 않은 악의 있는 자(130)는 클라이언트들(102, 104)로부터 신원 및/또는 다른 정보를 획득하기 위하여 적법한 서버 및/또는 웹사이트를 복사하거나 적법한 서버 및/또는 웹사이트처럼 보이려고 할 수 있다. 본원에 게시된 예시적인 실시예에서는, 클라이언트가 신원 키를 요청할 때, 식별되지 않은 악의 있는 자 ID 키(132)가 클라이언트에게 제공될 것이고, 그러므로, 클라이언트는 이 서버가 이전에 방문되었던 서버가 아니라고 이해할 수 있다. 또한, 클라이언트가 비대칭 공개 키를 요청할 때, 클라이언트 및/또는 사용자가 이전에 식별되지 않은 악의 있는 자의 웹사이트를 액세스하지 않았기 때문에 식별되지 않는 악의 있는 자는 비대칭적 공개 키(들)(APK)(134)를 가지고 있지 않을 것이다. 이들 시나리오들 중 하나가 클라이언트(102, 104)의 사용자에게 이 웹사이트 및/또는 서버가 신뢰될 수 없다고 경고할 것이고, 사용자는 신원 또는 다른 정보를 노출하는 것에 대하여 신중해야 한다.

[0038] 마찬가지로, 식별되지 않은 악의 있는 자(130)가 클라이언트의 신원 정보를 얻기 위하여 임의의 서버들을 액세스하고자 한다면, 식별되지 않은 악의 있는 자(130)는 클라이언트 또는 서버인 것처럼 행동하기 위하여 요구되는 대칭 또는 비대칭 키를 알고 있음을 진술할 수 없을 것이다.

[0039] 이러한 예시적인 실시예에서, 서버, 사용자 및/또는 클라이언트는 식별되지 않은 악의 있는 자들이 웹사이트를 속임으로써 개인 정보를 획득하는 것을 저지할 수 있는 다른 수준 또는 2개의 보안을 가질 수 있다. 또한, 이는 정보의 "중간에 위치한 자(man in the middle)" 방해를 저지하여 보다 안전성을 제공할 수 있다.

[0040] 사이트-특정 비대칭적 공개 키 또는 대칭 키가 서버들 및/또는 웹사이트들에 저장되기 때문에, 사용자는 이들의 마스터 키를 다수의 다른 클라이언트들에게 제공하여 웹사이트를 액세스할 수 있으며, 이들이 인증 웹사이트를 다루고 있다는 점에서 여전히 어느 정도 안전하다. 또한, 이들은 서버 ID 키, 이들의 마스터 키(들), 및 상수(들)를 이용하여 사이트의 대칭 또는 공개 비대칭 키들을 알고 있음에 대한 확인을 요청할 수 있다; 또는 이들은 웹사이트에 저장되거나 이 웹사이트와 관련된 투명한 키 블럽(blob)을 요청하고 복호화하여 이들이 이전에

서버 및/또는 웹사이트를 방문하였는지 여부를 판정할 수 있다. 이는 또한 이들이 웹사이트를 다루는 데에 훨씬 더 편리해질 수 있다는 점에서 가정, 직장, 도서관 등에서 복수의 기기를 이용하는 사용자에게 매력적일 수 있다. 마스터 키가 한 경우에 새로운 장치, 또는 컴퓨터로 송신되기만 하면 된다는 것은 이러한 시스템의 뛰어나고 핵심적인 특징이다. 이로부터, 모든 사이트-특정 키 및 진행중인 디지털 관계의 확인들을 줄일 수 있다. 이는 진행중인 비동기화를 다시 진행할 필요성을 없앤다.

[0041] 이는 속임수를 우려하는 웹사이트의 운영자들 또는 서버들에 매력적일 수 있다. 이는 식별되지 않은 사용자가 기밀 정보를 획득하지 못하게 할 수 있는 여분의 수준의 사용자가 생성한 보안을 제공할 수 있다.

[0042] 도 2는 본 발명의 실시예들이 구현될 수 있는 적절한 컴퓨팅 시스템 환경의 일례를 도시한다. 시스템(200)은 상술한 바와 같이 클라이언트 및/또는 서버로서 작용하는 데에 이용될 수 있는 것을 나타낸다. 가장 기본적인 구성으로, 시스템(200)은 통상적으로 적어도 하나의 프로세싱 유닛(202) 및 메모리(204)를 포함한다. 컴퓨팅 장치의 정확한 구성 및 유형에 따라서, 메모리(204)는 (RAM과 같은) 휘발성, (ROM, 플래쉬 메모리 등과 같은) 비휘발성, 또는 이 둘의 몇몇의 조합일 수 있다. 이 가장 기본적인 구성은 도 2에서 점선(206)으로 도시된다. 또한, 시스템(200)은 추가적인 특징/기능도 가질 수 있다. 예를 들면, 장치(200)는 자기 또는 광 디스크나 테이프를 포함하지만 이에 한정되지 않는 (분리형 및/또는 비분리형인) 추가적인 저장 장치 또한 포함할 수 있다. 이러한 추가적인 저장 장치는 도 2에서 분리형 저장 장치(208) 및 비분리형 저장 장치(210)로 도시된다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈들 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 포함한다. 메모리(204), 분리형 저장 장치(208) 및 비분리형 저장 장치(210)는 모두 컴퓨터 저장 매체의 예이다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래쉬 메모리, 또는 기타 메모리 기술, CD-ROM, DVD, 또는 광 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 시스템(200)에 의해 액세스될 수 있고 원하는 정보를 저장하는 데 사용될 수 있는 임의의 기타 매체를 포함하지만 이에 한정되지 않는다. 이러한 임의의 컴퓨터 저장 매체는 시스템(200)의 일부일 수 있다.

[0043] 시스템(200)은 또한 시스템이 다른 장치와 통신할 수 있게 하는 통신 접속(들)(212)을 포함할 수 있다. 통신 접속(들)(212)은 통신 매체의 일례이다. 통신 매체는 통상적으로 반송파 또는 기타 전송 메카니즘 등의 변조된 데이터 신호에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 다른 데이터를 구현하며, 임의의 정보 전달 매체를 포함한다. "변조된 데이터 신호"라는 용어는 신호 내의 정보를 인코딩하도록 하나 또는 그 이상의 특성을 설정 또는 변경시킨 신호를 의미한다. 예로서, 통신 매체는 유선 네트워크 또는 직접 유선 접속 등의 유선 매체와, 음향, RF, 적외선 및 기타 무선 매체 등의 무선 매체를 포함하지만, 이에 한정되지 않는다. 본원에서 사용된 컴퓨터 판독가능 매체라는 용어는 저장 매체 및 통신 매체를 모두 포함한다.

[0044] 시스템(200)은 키보드, 마우스, 펜, 음성 입력 장치, 접촉 입력 장치 등과 같은 입력 장치(들)(214)를 가질 수 있다. 디스플레이, 스피커, 프린터 등과 같은 출력 장치(들)(216)도 포함될 수 있다. 모든 이들 장치는 본 기술 분야에서 잘 알려져 있어 장황하게 기술될 필요가 없다.

[0045] 시스템(200)과 같은 컴퓨팅 장치는 통상적으로 컴퓨터 판독가능 매체의 적어도 몇몇의 형태를 포함한다. 컴퓨터 판독가능 매체는 시스템(200)에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있다. 예로서, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함할 수 있지만 이에 한정되지 않는다.

[0046] 도 3은, 일반적으로 참조번호(300)로, 개념적인 수준에서, 예시적인 실시예에 따른 비대칭적 보안 키 교환을 위한 시스템을 도시한다. 이러한 예는 네트워크(314) 또는 다른 채널을 통하여 접속된 클라이언트(301) 및 서버(306)를 포함하는 시스템(300)을 도시한다. 대부분의 장치는 클라이언트(301) 및 서버(306) 모두로서 여러 번 작용할 수 있음이 명백해질 것이다. 그러나, 간단히 하기 위하여, 본원에서는 이들 기능을 구별하여 도시한다. 또한, 네트워크(314)는 대부분, 인터넷을 포함하는 임의의 유형의 네트워크일 수 있거나 클라이언트(301)와 서버(306) 간의 통신을 구축하는 데에 적절한 몇 가지 다른 유형의 채널일 수 있다.

[0047] 클라이언트(301)는 인터넷을 통하여 웹사이트, 또는 서버(306)를 액세스하는 퍼스널 컴퓨터와 같은 클라이언트일 수 있다. 그러나, 본원에 기술된 개념으로부터 벗어나지 않고 다른 장치 및 구성이 이용될 수 있다고 인식될 것이다. 마찬가지로, 서버(306)는 웹사이트, 장치, 또는 다른 시스템을 위한 호스트, 또는 다른 구성일 수 있다.

[0048] 서버(306)는 관련된 신원 키(307)를 가진다. 신원 키(307)는 다른 정보 중에서도 서버에 대한 정보를 포함한다. 일 실시예에서, 정보는 URL의 컴포넌트, 시스템을 소유하고 운영하는 주체(principal)의 이름, 및/

또는 다른 "신원" 정보에 관련된다. 서버(306)를 액세스할 때, 클라이언트(301)는 신원 키(307)를 요청할 수 있고/거나 신원 키(307)는 서버 또는 다른 엔티티에 의해 클라이언트(301)에 제공될 수 있다. 신원 키(307)는 본원에서 서버(306)에 상주하거나 서버(306)로부터 발행된 것으로 도시되지만, 신원 키(307)는 다른 것들 중에서도 검사 엔티티를 포함하지만 이에 한정되지 않는 다른 소스에 상주하거나 이러한 소스로부터 발행될 수 있다는 것을 인식해야 한다.

[0049] 다른 예시적인 실시예에서, 클라이언트(301)는 서버(306)에 대한 정보를 포함하는 인증서를 수신한다. 인증서 내에 포함되는 정보는 신원 키(307), 또는 다른 신원 정보를 포함한다. 클라이언트(301)는 신원 키(307)를 액세스하기 위하여 인증서를 파싱한다. 상술한 바와 같이 인증서는 서버, 검사 엔티티, 및/또는 다른 엔티티로부터 발행될 수 있다.

[0050] 그 다음 클라이언트는 신원 정보를 이용하여 서버에 저장된 고유한 비대칭 공개 키(또는 대칭 키)(309)를 생성한다. 키(309)는 서버의 신원 정보, 클라이언트에 의해 생성된 마스터 키, 및 선택적으로는 상수(들)의 함수이다. 이 함수는 이 함수를 생성하는 데에 이용되는 컴포넌트들이 최후 산출물(즉, 암호화된)과 구별될 수 없도록 하는 함수일 수 있다.

[0051] 클라이언트(301)는 이전에 마스터 키(302)를 생성하였을 수 있다. 마스터 키(302)는 무작위로 생성된 숫자 및/또는 타임 스탬프(time stamp), 신원 정보 등을 포함하지만 이에 한정되지 않는 다양한 서로 다른 유형의 정보 또는 다른 정보나 이들의 조합일 수 있다. 그 다음 클라이언트(301)는 마스터 키(302)와 신원 키(307)의 조합, 및 상수(들)의 암호화 함수를 이용하여 개인 키(308), 및 공개 키(309)를 포함하는 비대칭 키 쌍을 생성하는 데에 이용되는 하나 이상의 시드를 생성할 수 있다. 그러므로 비대칭 키들(308 및 309)은 방문된 웹사이트 및/또는 서버(306) 각각에 대하여 생성될 수 있다. 대안으로, 시드 및 시드들은 참조번호(309)로 다시 도시된 암호화된 채널을 통하여 전달될 수 있는 대칭 키를 생성하는 데에 이용될 수 있다.

[0052] 그 다음 키(309)는 서버(306)에 저장될 수 있다. 비대칭 경우에서, 비대칭 개인 키는 클라이언트(301)에 저장되거나, 버려지고 다음에 서버를 액세스할 때 이 키들을 다시 생성할 수 있다. 클라이언트(301)가 서버(306)를 다시 액세스할 때, 클라이언트(301)는 서버(306)에 의한 키(309)를 알고 있음에 대한 확인을 요청하고/거나 수신하고 이 키를 자신의 시스템에서 다시 생성된 키와 비교하여 클라이언트(301)가 이전에 서버(306)를 액세스했는지 여부를 판정할 수 있다. 서버(306)는 또한 이러한 방법을 이용하여 클라이언트(301)가 이전에 서버(306)를 방문했는지 여부를 판정할 수 있거나, 비대칭 경우에서는 클라이언트가 개인 키(308)를 알고 있음에 대한 확인을 보여주기를 요구할 수 있다.

[0053] 이러한 정보는 또한, 클라이언트(301) 및 클라이언트(301)를 이용하는 주체가 서버(306) 및/또는 관련된 웹사이트가 신뢰성 있고/거나 적법한 것을 보다 더 확신할 수 있도록 서버(306)의 신뢰성을 판정하는 데에 이용될 수 있다. 이는 속임수를 줄이고 사용자가 신원 정보 또는 다른 정보를 서버(306)에게 노출하기 전에 사용자 신뢰를 향상시키는 것 및 많은 다른 이점을 가진다.

[0054] 정보의 확인은 검사될 수 있고 기밀을 알고/거나 시드(들) 및 키를 가지는 엔티티에 의해 이해될 수 있는 기밀을 채용하는 몇몇의 정보 상의 디지털 시그니처(signature)를 제출하는 단계를 포함할 수 있다. 이전에 서버에 저장된 키를 알고 있음에 대한 확인을 요청함으로써, 사용자는 서버/웹사이트를 식별하고, 그 다음 서버에 정보를 노출시킬 때에는 보다 특정될 수 있다. 예시적인 실시예는 식별되지 않은 시스템(312)이 이전에 액세스된 서버(306)인 것처럼 행동함으로써 클라이언트(301)로부터 신원 정보를 얻으려 할 가능성을 줄일 수 있다. 또한, 서버(306)는 비대칭 개인 키(308)를 이용하여 서버(306)를 액세스하려 하고/거나 특정 클라이언트에 대한 정보를 변경하거나 획득하는 클라이언트(301)의 신뢰성을 판정할 수도 있다.

[0055] 일단 생성되면, 비대칭 공개 키 또는 대칭 키는 웹 서버에 또는 이 생성되었던 키에 대한 웹사이트와 관련되어 저장된다. 결과적으로, 사용자는 그 사이트를 다시 방문하고 키를 알고 있음에 대하여 진술하기 위하여 사이트의 챌린지(challenge)를 통하여 사이트를 빠르게 증명/인식할 수 있다. 또한, 방문된 각 시스템에 고유한 쌍-단위의 키가 부여될 수 있기 때문에 서로 다른 시스템의 운영자들은 키들을 비교하지 않고도 클라이언트 또는 사용자에 대한 정보를 공유하고 상호 동작시킬 수 있다.

[0056] 알고 있음에 대한 확인에 이용되는 암호화는, 상황에 따라서 AES 256 함수일 수 있거나 RSA와 같은 공개 키 알고리즘에 기초할 수 있다. 그러나, 다른 암호화 알고리즘, 함수, 및 구성이 본원에 게시된 개념으로부터 벗어나지 않고 이용될 수 있다고 인식될 것이다.

[0057] 이러한 함수는 또한 클라이언트(301) 및 클라이언트(301)의 사용자가 서버(306) 및/또는 관련된 웹사이트와 시

스템이 신뢰성 있고/거나 적법한 것을 더 확신할 수 있도록 서버(306)의 신뢰성을 판정하는 데에 이용될 수 있다. 이는, 다른 이점들 중에서도, 속임수를 줄이고, 사용자가 신원 정보 또는 다른 민감한 정보를 서버(306)에게 노출하기 전에 사용자 신뢰를 향상시킬 수 있다. 이러한 인증은 진행중인 디지털 관계의 일관된 인식을 제공할 수 있다.

[0058] 클라이언트(301)가 키(309)의 소유 여부에 대하여 예상되는 확인과 다른 임의의 것을 수신한다면, 이는 클라이언트(301)가 이 서버(306)를 이전에 액세스하지 않았음을 나타낼 수 있다. 이는 다른 시나리오들 중에서도, 적법한 사이트가 모방되고 있음, 또는 서버(306)가 키를 상실했음을 나타낼 수도 있다. 이는 클라이언트(301)의 사용자에게 서버(306)는 믿을만하지 않으며, 사용자는 서버(306)로부터 접속을 종료하거나 주의를 하며 진행하고/거나 임의의 민감한 정보, 기밀 정보, 및/또는 신원 정보를 누설하지 않아야 함을 나타낼 수 있다.

[0059] 도 3에 도시된 실시예의 다른 이점은 사용자가 본래의 마스터 키를 가지고 다수의 서로 다른 클라이언트로부터 웹사이트 및/또는 서버(306)를 액세스할 수 있으면서, 웹사이트가 적법하다는 것에 대한 어느 수준의 확신을 가진다는 것이다.

[0060] 도 4는 예시적인 실시예에 따라서 쌍-단위 보안 키를 생성하는 방법의 예시적인 실시예를, 일반적으로 참조번호(400)로 도시하는 흐름도이다. 방법(400)은 수신 동작(402)을 포함한다. 수신 동작(402)은 서버 또는 다른 엔티티로부터 신원 키를 수신하는 단계를 포함한다. 신원 키는 고유한 URL, 시스템을 소유하는 주체, 및/또는 다른 ID 정보를 포함하지만 이에 한정되지 않는, 서버에 대한 신원 정보를 포함할 수 있다. 또한, 신원 키는 보안 인증서, 또는 다른 인증서와 같은, 서버와 관련된 인증서의 일부일 수 있다. 신원 키는 이 인증서로부터 파싱될 수 있다. 그 다음 제어는 생성 동작(404)으로 넘어간다.

[0061] 생성 동작(404)은 마스터 키를 생성하는 단계를 포함할 수 있다. 마스터 키는 난수, 신원 정보, 또는 다른 고유한 정보 및/또는 이들의 조합일 수 있다. 마스터 키는 또한 미리 생성되었고 서로 다른 애플리케이션에 대하여 다시 이용될 수 있다. 마스터 키는 권한이 없는 사용자 또는 엔티티가 정보를 손상시키고 보고/거나 훔칠 수 없게 하는 매우 안전한 위치에 저장되어야 함을 인식할 것이다. 그 다음 제어는 획득 단계(406)로 넘어간다.

[0062] 획득 단계(406)는 상수(들)를 획득하는 단계를 포함한다. 상수(들)는 무작위로 생성된 숫자, 또는 다른 정보 및/또는 이들의 조합일 수 있다. 상수(들)는 추후에 필요하다면 다시 산출될 수 있도록, 이 상수를 생성한 사용자에게만 알려질 수 있다. 그 다음 제어는 생성 동작(408)으로 넘어간다.

[0063] 생성 동작(408)은 신원 키, 마스터 키, 및 상수(들)의 함수로서 시드를 생성하는 단계를 포함할 수 있다. 본원에 게시된 개념을 벗어나지 않고 다른 정보 및/또는 정보의 조합이 이용될 수 있음을 인식할 것이다. 이 함수는, 본래의 정보가 결과적 시드로부터 결정될 수 없도록 하는, 상기 정보의 단방향 암호화일 수 있다. 이 함수는 AES 암호화 함수 또는 다른 암호화 함수나 알고리즘 및/또는 이들의 조합일 수 있다. 소정의 범위의 시드들이 산출될 필요가 있다면, 제어는 획득 동작(406)으로 다시 돌아가서 다른 상수를 이용하는 다른 시드를 생성하는 데에 이용될 다른 상수를 획득할 수 있다. 그 다음 시드(들)는 비대칭 키 쌍 생성기가 비대칭 키 쌍(들)을 생성하거나, 대칭 키 생성 또는 검사 함수가 대칭 키를 생성하는 데에 이용될 수 있다.

[0064] 도 5는 예시적인 실시예에 따라서 비대칭 키 쌍(들)을 생성하는 단계 및 진행중인 디지털 관계를 인식하는 단계에 포함되는 다른 동작적인 특징을, 일반적으로 참조번호(500)로 도시하는 흐름도이다.

[0065] 방법(500)은 참조번호(502)에서 수신 동작을 포함한다. 수신 동작(502)은 이전에 생성된 시드(들)를 수신하는 단계를 포함한다. 상술한 바와 같이 시드(들)가 생성된다. 그 다음 시드는 생성 동작(504)으로 넘어간다.

[0066] 생성 동작(504)은 수신된 시드(들)를 이용하여 비대칭 키 쌍을 생성하는 단계를 포함한다. 하나 이상의 시드(들)가 비대칭 키 쌍의 생성에 이용될 수 있다. 이용되는 시드(들)의 수는 이용되는 비대칭 키 쌍 생성기의 특정 타입에 따라 다를 수 있다. 그 다음 제어는 저장 동작(506)으로 넘어간다.

[0067] 저장 동작(506)은 서버에 비대칭 공개 키를 저장하는 단계 및/또는 비대칭 공개 키를 서버 또는 웹사이트와 관련시키는 단계를 포함할 수 있다. 비대칭 공개 키는 클라이언트가 서버를 다시 액세스할 때 클라이언트로부터 액세스될 수 있도록 서버와 관련된다. 또한, 이 키는, 사용자가 서로 다른 장치 또는 시스템으로부터 시스템 또는 웹사이트를 인증하거나 인식할 수 있도록 다른 시스템으로부터 사용자에 의해 액세스될 수 있다. 클라이언트는 또한 비대칭 공개 키를 다시 생성하고 다음에 서버를 다시 액세스할 때 이 키를 제시하여 클라이언트의 ID를 검사할 수 있다. 마찬가지로, 클라이언트는 서버가 이전에 액세스되었는지 여부를 판정할 수 있다.

또한, 이 정보는 서버 및/또는 클라이언트의 적법성 및/또는 신뢰성을 판정하는 데에 이용될 수 있다.

[0068] 도 6은 예시적인 실시예에 따라 서버, 클라이언트, 시스템 또는 웹사이트의 신뢰성을 판정하는 방법을, 일반적으로 참조번호(600)로 도시하는 흐름도이다. 방법(600)의 양태에 따르면, 프로세싱은 산출 동작(602)으로 시작된다. 산출 동작(602)은 사용자/클라이언트가 사용자/클라이언트의 신원을 검사하기 위하여 서버에 비대칭 공개 키를 알고 있음에 대한 확인을 산출하는 단계를 포함할 수 있다. 클라이언트 및/또는 서버에 의한 비대칭 공개 키를 알고 있음에 대한 확인의 산출은 진행중인 관계의 검증을 구성할 수 있다. 이는 클라이언트 및 서버가 이전에 정보를 교환했을 수 있다는 것이다. 클라이언트는 또한 대응하는 개인 비대칭 키를 이용하여 이전 방문을 표시하고/거나 서버와 정보를 교환할 수 있다. 또한, 클라이언트는 키 쌍을 저장했거나 비대칭 키를 초기에 생성하는 데에 이용되었던 정보를 이용하여 비대칭 키 쌍을 다시 생성함으로써 비대칭 공개 키를 알고 있음을 진술할 수 있다. 그 다음 제어는 질의 동작(600)으로 넘어간다.

[0069] 질의 동작(604)은 산출된 비대칭 공개 키가 저장되고/거나 다시 생성되고/거나 복호화되고/거나 이전에 클라이언트에 의해 저장된 비대칭 공개 키와 일치하는지 여부를 판정하는 단계를 포함한다. 클라이언트가 대응하는 비대칭 공개 키를 저장하였을 수 있기 때문에, 비대칭 공개 키가 비교되어 서버가 이전에 액세스되었는지 여부를 판정할 수 있다. 또한, 클라이언트는, 다른 정보 중에서도, 신원 키 및 본래의 마스터 키를 이용하여 비대칭 공개 키를 재생성하여 서버가 이전에 액세스되었는지 여부를 판정할 수 있다.

[0070] 비대칭 공개 키들이 일치한다면, 제어는 인증된 시스템(606)으로 넘어간다. 이는 클라이언트가 이전에 서버를 액세스하였고 비대칭 공개키를 저장하고/거나 서버와 관련시켰음을 나타낸다. 인증된 시스템은 서버 및/또는 클라이언트일 수 있다. 클라이언트 및/또는 서버는 선택적으로 서로의 신원을 인증하기 전에 서로의 신원을 더 확신시키기를 요청할 수 있다. 이는 식별되지 않는 악의 있는 자가 은밀히 키를 얻었는지 여부를 판정하는 것일 수 있다. 이러한 더 확신시키기는 다른 정보 중에서도, 오직 이전에 노출된 대응하는 키 또는 정보를 이용하여 복호화되고/거나 응답될 수 있는, 메세지 또는 챌린지를 서로에게 송신하는 단계를 포함할 수 있다.

[0071] 비대칭 공개 키가 일치하지 않거나, 비대칭 공개 키가 산출되지 않는다면, 사용자는 인증되지 않은 것이다(608). 사용자가 인증되지 않았다고 판정된(608) 이후에, 제어는 요청 동작(610)으로 넘어간다. 요청 동작(610)은 서버로부터 신원 키를 요청하는 단계, 또는 서버에 의해 클라이언트로부터 정보를 더 요청하는 단계를 포함할 수 있다. 클라이언트가 이전에 서버, 또는 웹사이트를 액세스하였고, 이 동작이 게시되면, 사용자 및/또는 서버는 웹사이트가 신뢰되지 않으며 이 클라이언트는 의도한 클라이언트가 아니라는 몇몇의 표시자를 가질 수 있다 이는 또한 사용자 또는 서버에게 다른 엔티티가 주체로부터 신원 정보를 얻기를 시도한다고 나타낼 수 있다. 이는 또한 서버 또는 클라이언트가 비대칭 공개 또는 개인 키를 상실했거나, 서버 또는 클라이언트가 부당하게 변경되었음을 나타낼 수 있다. 임의의 이들 시나리오에서, 클라이언트 또는 서버의 사용자는 이 시스템은 신뢰되지 않으며 임의의 정보를 다른 자에게 노출시킬 때 주의를 기울여야 한다는 표시자를 가질 수 있다.

[0072] 예시적인 실시예들의 다양한 실시예의 논리적 동작들은 (1) 컴퓨팅 시스템에서 실행되는 프로그램 모듈 또는 컴퓨터가 구현한 행위의 시퀀스 및/또는 (2)컴퓨팅 시스템 내의 상호접속된 기기 논리 회로들 또는 회로 모듈들로서 구현될 수 있다. 이 구현은 본 발명을 구현하는 컴퓨팅 시스템의 수행 요구사항들에 따라 선택될 수 있는 사항이다. 따라서, 본원에 기술된 예시적인 실시예들의, 이 실시예들을 구축하는 논리적 동작들은 동작, 구조적 장치, 행위 또는 모듈이라 다양하게 칭한다. 본 기술 분야에서 숙련된 기술을 가진 자들은 특허 청구 범위에 인용된 본 게시물의 사상 및 범위로부터 벗어나지 않고 이들 동작, 구조적 장치, 행위 및 모듈이 소프트웨어, 펌웨어, 특수 목적 디지털 로직, 및/또는 이들의 임의의 조합으로 구현될 수 있음을 인식할 것이다.

[0073] 예시적인 실시예가 컴퓨터 구조적 특징, 방법논리적 행위에, 및 컴퓨터 판독가능 매체에 의한 특정된 언어로 기술되었지만, 특허 청구 범위에 정의된 예시적인 실시예들은 기술된 특정 구조, 행위 또는 매체에 반드시 제한될 필요는 없다. 예로서, XML과는 다른 포맷이 ID 정보를 인코딩하는 데에 이용될 수 있다. 그러므로, 특정 구조적 특징, 행위 및 매체는 청구된 발명을 구현하는 예시적인 실시예로서 게시된다.

[0074] 상술한 다양한 실시예는 단지 예로서 제공되며 본 게시물을 한정한다고 해석되어서는 안된다. 본 기술 분야에서 숙련된 기술을 가진 자라면 이하의 특허 청구 범위에 설명된 본 게시물의 진정한 사상 및 범위로부터 벗어나지 않으면서 본원에 기술되고 도시된 예시적인 실시예 및 적용을 따르지 않고, 본 게시물에 이루어질 수 있는 다양한 수정 및 변경을 쉽게 인정할 것이다.

발명의 효과

[0075] 본원에 게시된 예시적인 실시예는 상술한 단점 및 다른 단점들을 완화하는 시스템 및 방법을 포함할 수 있다. 본원에 게시된 예시적인 실시예들은 마스터 키를 생성하는 단계, 서버로부터 신원 키를 수신하는 단계, 신원 키, 마스터 키, 및 상수(들)의 해쉬(hash) 또는 암호화 함수를 이용함으로써 시드(seed)를 생성하는 단계, 및 이 시드를 키 또는 키 쌍을 생성하는 프로세스로의 입력으로서 이용하는 단계를 포함하는 비대칭 키 쌍(들)을 생성하는 시스템 및 방법을 포함한다. 본원에 기술된 예시적인 실시예에서, 이 시드는 비대칭 키 쌍을 생성하는 데에 이용되며, 결과인 공개 비대칭 키는 서버에 저장된다.

도면의 간단한 설명

[0001] 도 1은 예시적인 실시예에 따라서 비대칭적 키 쌍(들)을 생성하고, 진행중인 디지털 관계를 인식하는 시스템의 블럭도.

[0002] 도 2는 예시적인 실시예들이 구현될 수 있는 적절한 컴퓨팅 시스템 환경의 예를 도시하는 도면.

[0003] 도 3은 예시적인 실시예에 따라서 비대칭적 키 쌍(들)을 생성하고 시스템을 인증하는 시스템의 블럭도.

[0004] 도 4는 예시적인 실시예에 따라서 비대칭적 키 쌍(들)을 생성하는 단계 및 진행중인 디지털 관계를 인식하는 단계에 포함되는 동작적 특징들을 도시하는 흐름도.

[0005] 도 5는 예시적인 실시예에 따라서 비대칭적 키 쌍(들)을 생성하는 단계 및 진행중인 디지털 관계를 인식하는 단계에 포함되는 다른 동작적 특징들을 도시하는 흐름도.

[0006] 도 6은 예시적인 실시예에 따라서 시스템을 인증하는 단계에 포함되는 동작적인 특징들을 도시하는 흐름도.

[0007] <도면의 주요 부분에 대한 부호의 설명>

[0008] 106 서버 1

[0009] 112 네트워크

[0010] 114: 키 생성 모듈

[0011] 116: 서버 1 ID 키

[0012] 212: 통신 접속(들)

[0013] 301: 클라이언트

[0014] 302: 마스터 키

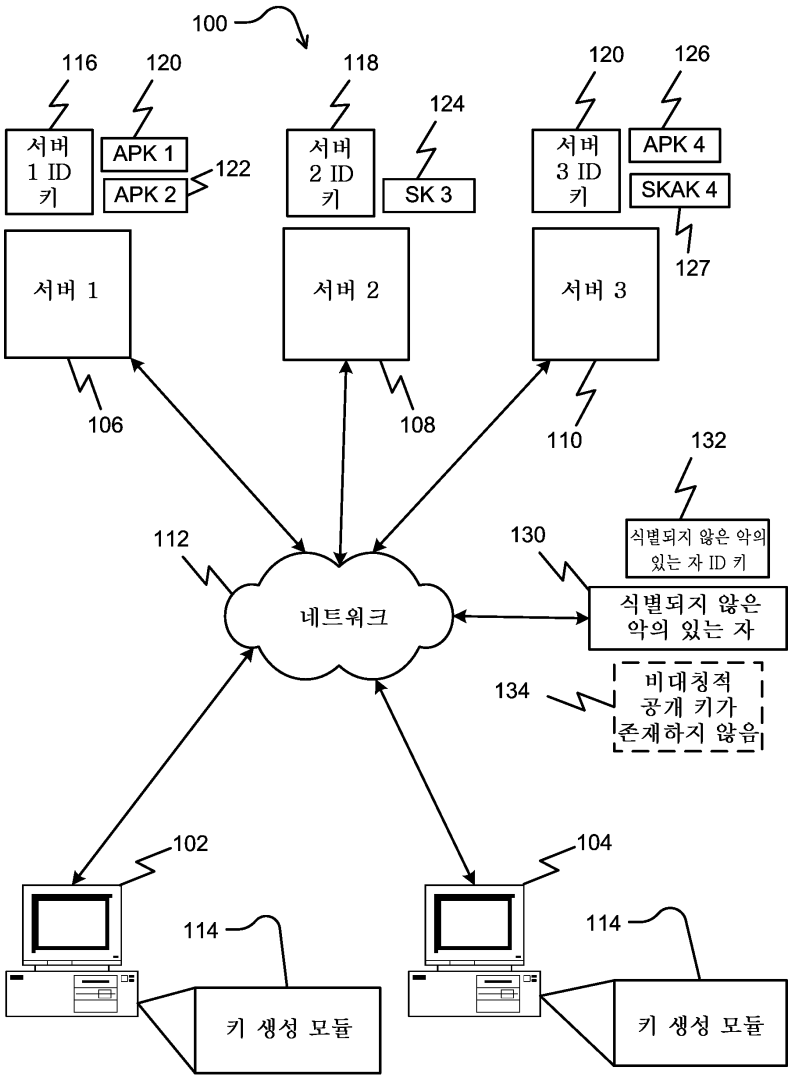
[0015] 308: 비대칭 개인 키

[0016] 307: 신원 키

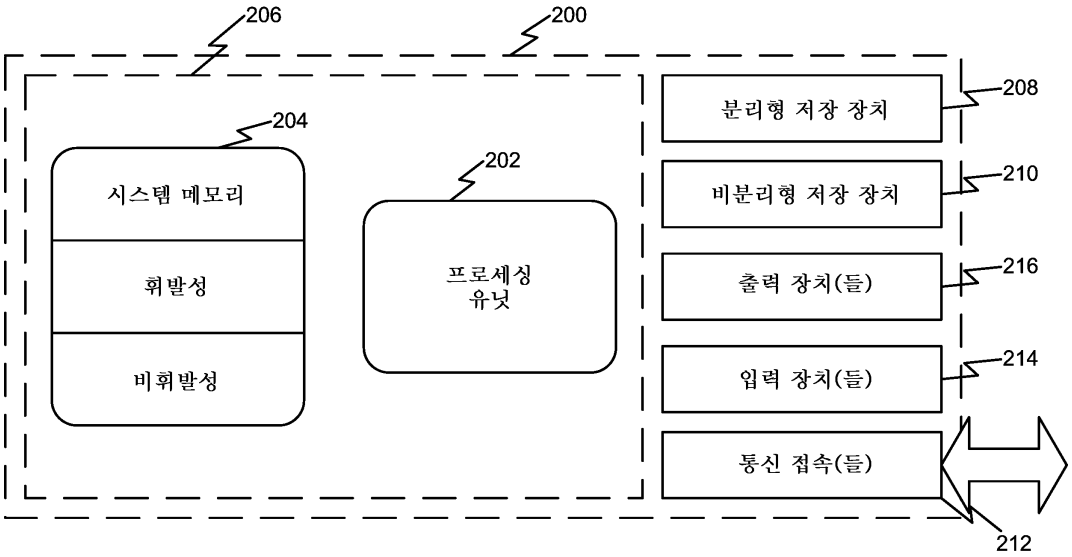
[0017] 309: 비대칭 공개 키

도면

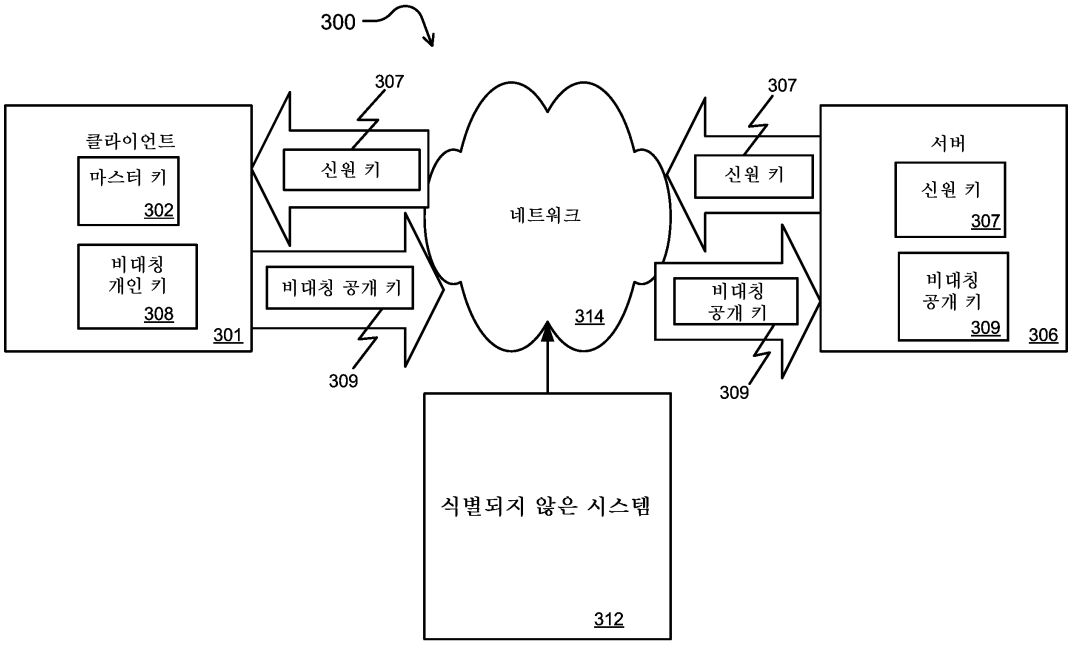
도면1


100
116
120
118
124
120
126
서버 1 ID 키
APK 1
APK 2
122
서버 2 ID 키
SK 3
서버 3 ID 키
APK 4
SKAK 4
127
서버 1
서버 2
서버 3
106
108
110
132
112
130
식별되지 않은 악의 있는 자 ID 키
네트워크
식별되지 않은 악의 있는 자
134
비대칭적 공개 키가 존재하지 않음
102
104
114
114
키 생성 모듈
키 생성 모듈

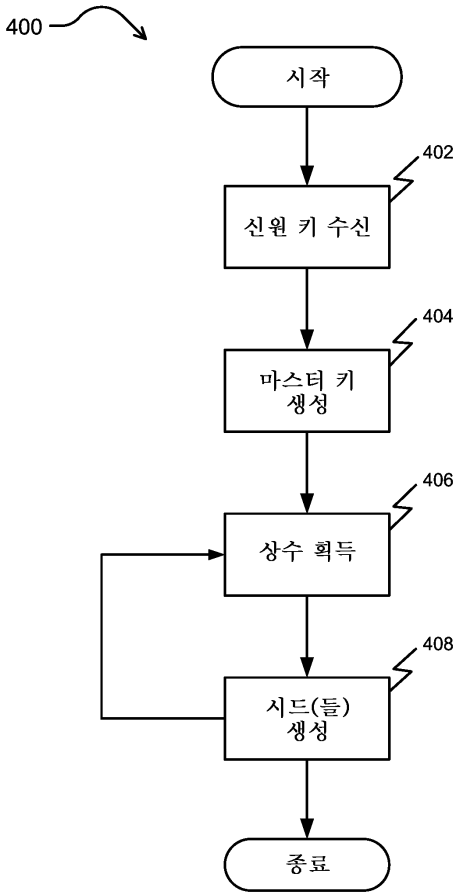
도면2


206
200
204
시스템 메모리
휘발성
비휘발성
202
프로세싱 유닛
분리형 저장 장치
208
비분리형 저장 장치
210
출력 장치(들)
216
입력 장치(들)
214
통신 접속(들)
212

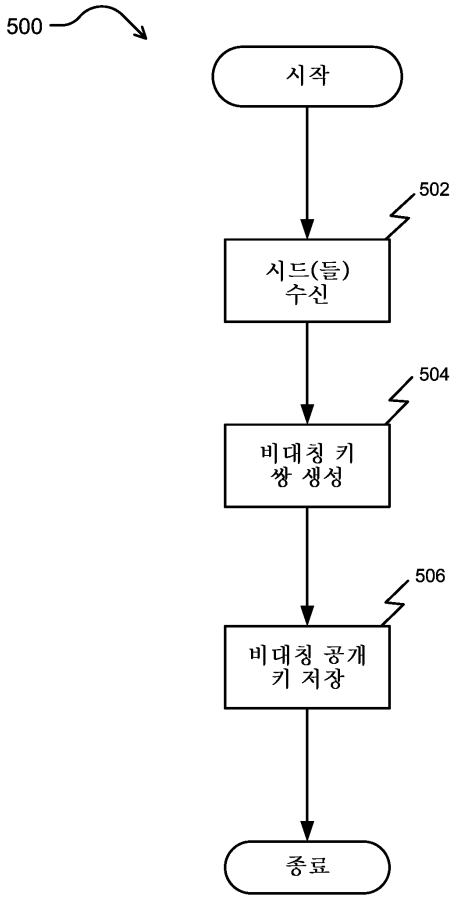
도면3


300
307
307
클라이언트
마스터 키
302
비대칭 개인 키
308
301
신원 키
비대칭 공개 키
309
네트워크
314
신원 키
비대칭 공개 키
309
서버
신원 키
307
비대칭 공개 키
309
306
식별되지 않은 시스템
312

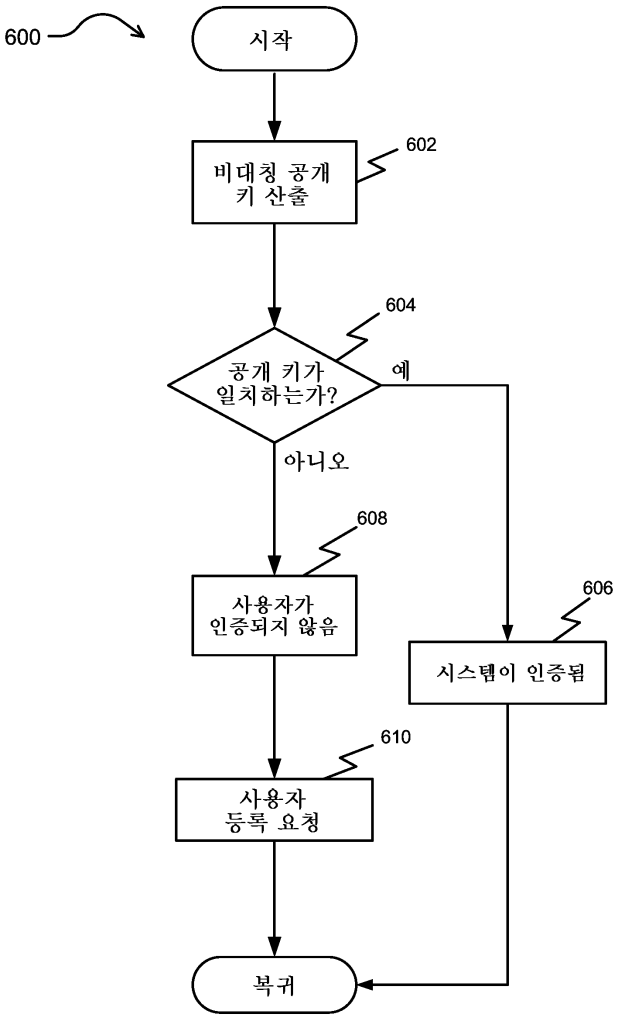
도면4



도면5



도면6


600
시작
602
비대칭 공개 키 산출
604
공개 키가 일치하는가?
예
아니오
606
시스템이 인증됨
608
사용자가 인증되지 않음
610
사용자 등록 요청
복귀