(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0022906
(43) 공개일자 2013년03월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/28* (2006.01)
(21) 출원번호 10-2011-0085927
(22) 출원일자 2011년08월26일
심사청구일자 2011년08월26일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 경희궁의아침3단지 아파트 1404호 (내수동)
구우권
서울특별시 서초구 잠원동 동아아파트 108동 1201호
김기탁
경기도 용인시 기흥구 고매동 동성아파트 102동 1407호
(74) 대리인
특허법인충현

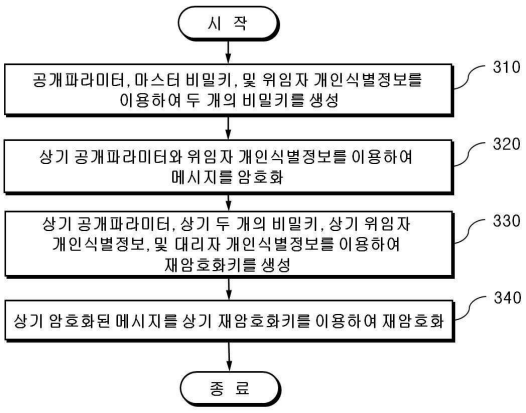
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 **두 개의 비밀키를 이용하는 프락시 재암호화 방법 및 프락시 재암호화 메시지 복호화방법**

(57) 요 약

본 발명은 프락시 재암호화 방법에 관한 것으로서 공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하는 단계, 상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하는 단계, 상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하는 단계, 및 상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화하는 단계를 포함하는 것을 특징으로 하며, 두 개의 비밀키를 이용함으로써 프락시와 대리자의 공모공격에 안전하다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업

과제고유번호	KI002113201103100110013918KI002113201103
부처명	한국산업기술평가관리원
연구사업명	산업원천기술개발사업
연구과제명	Car-헬스케어 보안 기술개발
주관기관	고려대학교 산학협력단
연구기간	2011.03.01 ~ 2012.02.29

특허청구의 범위

청구항 1

공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하는 단계;

상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하는 단계;

상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하는 단계; 및

상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화하는 단계를 포함하는 프락시 재암호화 방법.

청구항 2

제 1 항에 있어서,

상기 재암호화키를 생성하는 단계는,

제 1 해시함수를 이용하여 상기 대리자 개인식별정보로부터 제 1 해시값을 산출하는 단계;

겹선형 함수를 이용하여 상기 제 1 해시값과 상기 각 비밀키로부터 각각의 연산값을 산출하는 단계; 및

소정의 난수와 상기 두 개의 비밀키의 비율로부터 상기 재암호화키를 생성하는 단계를 포함하고,

상기 두 개의 비밀키의 비율은 상기 연산값과 상기 두 개의 비밀키로부터 산출되는 것을 특징으로 하는 프락시 재암호화 방법.

청구항 3

제 1 항에 있어서,

상기 두 개의 비밀키는,

제 1 해시함수를 이용하여 상기 위임자의 개인식별정보로부터 제 2 해시값을 산출하고, 상기 제 2 해시값을 두 개의 마스터 비밀키로 지수승함으로써 생성된 것을 특징으로 하는 프락시 재암호화 방법.

청구항 4

제 1 항에 있어서,

상기 재암호화하는 단계는,

제 2 해시함수를 이용하여 상기 위임자의 개인식별정보 및 암호화된 메시지로부터 제 3 해시값을 산출하는 단계;

상기 제 3 해시값을 이용하여 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는지 판단하는 단계; 및

상기 판단결과, 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는 경우, 상기 암호화된 메시지를 상기 공개파라미터와 상기 재암호화키를 이용하여 재암호화하는 단계를 포함하는 프락시 재암호화 방법.

청구항 5

재암호화된 메시지를 수신하는 단계; 및

공개 파라미터와 대리자 비밀키를 이용하여 상기 재암호화된 메시지를 복호화하는 단계를 포함하고,

상기 재암호화된 메시지는, 상기 공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하고, 상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하고, 상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하며, 상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화함으로써 생성된 것을 특징으로 하는 프락시 재암호화 메시지 복호화방법.

청구항 6

제 5 항에 있어서,

상기 재암호화키는,

제 1 해시함수를 이용하여 상기 대리자 개인식별정보로부터 제 1 해시값을 산출하고, 겹선형 함수를 이용하여 상기 제 1 해시값과 상기 각 비밀키로부터 각각의 연산값을 산출하여, 소정의 난수와 상기 두 개의 비밀키의 비율로부터 생성되며,

상기 두 개의 비밀키의 비율은 상기 연산값과 상기 두 개의 비밀키로부터 산출되는 것을 특징으로 하는 프락시 재암호화 메시지 복호화방법.

청구항 7

제 5 항에 있어서,

상기 두 개의 비밀키는,

제 1 해시함수를 이용하여 상기 위임자의 개인식별정보로부터 제 2 해시값을 산출하고, 상기 제 2 해시값을 두 개의 마스터 비밀키로 지수승함으로써 생성된 것을 특징으로 하는 프락시 재암호화 메시지 복호화방법.

청구항 8

제 5 항에 있어서,

상기 재암호화된 메시지는,

제 2 해시함수를 이용하여 상기 위임자의 개인식별정보 및 암호화된 메시지로부터 제 3 해시값을 산출하고, 상기 제 3 해시값을 이용하여 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는지 판단하며, 상기 판단결과, 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는 경우, 상기 암호화된 메시지를 상기 공개파라미터와 상기 재암호화키를 이용하여 재암호화함으로써 생성된 것을 특징으로 하는 프락시 재암호화 메시지 복호화방법.

청구항 9

제 1 항 내지 제 8 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 프락시 재암호화 방법 및 프락시 재암호화 메시지 복호화방법에 관한 것으로서, 더욱 상세하게는 두 개의 비밀키를 이용함으로써 공모공격에 안전한 ID기반 프락시 재암호화 방법 및 상기 방법에 의해 암호화된 메시지를 복호화하는 프락시 재암호화 메시지 복호화방법, 및 기록매체에 관한 것이다.

배 경 기 술

[0002] ID기반 프락시 재암호화 기법(ID-based proxy re-encryption scheme)은 프락시(proxy server)를 통해서 위임자(delegator)의 공개 아이디(Identity)로 암호화된 암호문을 대리자(delegatee)의 비밀키로 복호화 할 수 있도록 암호문을 변환시키는 기법이다. ID기반 재암호화 시스템에서 위임자는 자신의 비밀키를 노출시키지 않고 일시적으로 자신의 암호문에 대한 복호화 권리를 프락시를 통하여 대리자에게 분산시킬 수 있다. 이처럼 재암호화 기법은 DRM(Digital Rights Management), 이메일 전달 시스템, 분산 데이터 저장에서의 접근 제어 등 여러 응용분야에 원천 기술로 사용될 수 있다. 한 예로, 여러 응용분야 중에 분산된 네트워크 저장소에 대한 접근 제어(access control) 시스템을 고려할 수 있다. 이러한 접근 제어 시스템에서 위임자 는 컨텐츠 제공자로서 자신의 공개 아이디로 컨텐츠를 암호화하여 네트워크 저장소에 저장하고 프락시는 시스템에 대한 접근 제어자로서 가 대리자의 자신의 컨텐츠로의 접근을 허용할 때, 저장된 의 암호문을 의 비밀키로 복호화할 수 있는 암호문으로 변환시키는 역할을 수행한다.

[0003] 상기 프락시 재암호화 기법은 선행문헌 국내등록특허(KR 10-2010-0008711)에서 의료데이터의 정보 공유시 재암호화키에 의한 암호문의 재암호화 방식 및 멀티 프록시에 의한 다중 분산 방식으로 제공하여 기밀성을 유지할 수 있도록 하는 멀티 프록시 재암호화 기반 의료데이터 공유 방법 및 장치에 이용하고 있으며, 미국공개특허(US 2008-0059787)에서는 공개키와 비밀키를 포함하는 키쌍을 생성하고 암호화를 바꾸는 재암호화키를 생성하여 메시지를 암호화하는 방법에 이용하고 있다. 또한, 국내등록특허(KR 10-2005-0044242, KR 10-2003-0045217) 등 다양한 선행문헌에서 프락시 재암호화 기법을 이용하고 있다.

[0004] 기본적으로, 프락시가 암호문을 변환하는 재암호화 과정을 수행할 때 프락시는 위임자와 대리자의 비밀키를 알 수 없어야 하고 단독으로는 암호문에 대한 평문의 정보를 알 수 없어야 한다.

[0005] 추가적으로 프락시와 위임자 또는 프락시와 대리자의 사이의 공모를 통하여 시스템의 보안 취약점이 드러나지 않아야 한다. ID기반 재암호화 기법의 구조상, 프락시와 대리자의 사이의 공모는 위임자의 아이디로 암호화된 암호문 (또는 암호문 중 일부)을 (주어진 특정한 조건 내에서) 항상 복호화 할 수 있다. 하지만 프락시와 대리자의 공모를 통해 위임자의 비밀키에 대한 유용한 정보가 노출된다면 이는 심각한 보안 위협이 된다. 사용자의 비밀키는 다양한 형태로 중요하고 사용자-민감한(user-sensitive) 보안 업무들을 수행하는 데 이용되기 때문이다.

[0006] 그러나 선행 연구들이 프락시와 대리자의 공모공격을 통하여 위임자의 비밀키가 노출되는 취약한 구조를 지니고 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하고자 하는 첫 번째 과제는 두 개의 비밀키를 이용하여 공모공격에 안전한 프락시 재암호화 방법을 제공하는 것이다.

[0008] 본 발명이 해결하고자 하는 두 번째 과제는 두 개의 비밀키를 이용하여 공모공격에 안전한 프락시 재암호화 방법에 의해 암호화된 메시지를 복호화하는 프락시 재암호화 메시지 복호화방법을 제공하는 것이다.

[0009] 또한, 상기된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공하는데 있다.

과제의 해결 수단

[0010] 본 발명은 상기 첫 번째 과제를 달성하기 위하여, 공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하는 단계, 상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하는 단계, 상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하는 단계, 및 상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화하는 단계를 포함하는 프락시 재암호화 방법을 제공한다.

[0011] 본 발명의 일 실시예에 의하면, 상기 재암호화키를 생성하는 단계는, 제 1 해시함수를 이용하여 상기 대리자 개인식별정보로부터 제 1 해시값을 산출하는 단계, 겹선형 함수를 이용하여 상기 제 1 해시값과 상기 각 비밀키로부터 각각의 연산값을 산출하는 단계, 및 소정의 난수와 상기 두 개의 비밀키의 비율로부터 상기 재암호화키를 생성하는 단계를 포함하고, 상기 두 개의 비밀키의 비율은 상기 연산값과 상기 두 개의 비밀키로부터 산출되는 것을 특징으로 하는 프락시 재암호화 방법일 수 있다.

[0012] 본 발명은 상기 두 번째 과제를 달성하기 위하여, 재암호화된 메시지를 수신하는 단계, 및 공개 파라미터와 대리자 비밀키를 이용하여 상기 재암호화된 메시지를 복호화하는 단계를 포함하고, 상기 재암호화된 메시지는, 상기 공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하고, 상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하고, 상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하며, 상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화함으로써 생성된 것을 특징으로 하는 프락시 재암호화 메시지 복호화방법을 제공한다.

[0013] 상기 다른 기술적 과제를 해결하기 위하여, 본 발명은 상기된 프락시 재암호화 방법과 프락시 재암호화 메시지 복호화방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

발명의 효과

[0014] 본 발명에 따르면, 두 개의 비밀키를 이용함으로써 프락시와 대리자의 공모공격에 안전하다. 또한, 위임자의 비밀키가 노출되지 않는다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일 실시예에 따른 프락시 재암호화 장치를 도시한 블록도이다.

도 2는 본 발명의 다른 실시예에 따른 프락시 재암호화 방법으로 메시지를 재암호화하는 동안 이용되는 파라미터와 키들을 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 프락시 재암호화 방법의 흐름도이다.

도 4는 본 발명의 다른 실시예에 따른 재암호화키를 생성하는 방법의 흐름도이다.

도 5는 본 발명의 다른 실시예에 따른 암호화된 메시지를 재암호화 하는 방법의 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 프락시 재암호화 메시지 복호화방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 혹은 기술적 사상의 핵심을 우선 제시한다.

[0017] 본 발명의 일 실시예에 따른 프락시 재암호화 방법은 공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하는 단계, 상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하는 단계, 상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하는 단계, 및 상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화하는 단계를 포함한다.

[0018] 이하 첨부된 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 본 발명을 용이하게 실시할 수 있는 실시 예를 상세히 설명한다. 그러나 이들 실시예는 본 발명을 보다 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 의하여 제한되지 않는다는 것은 당업계의 통상의 지식을 가진 자에게 자명할 것이다.

[0019] 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명의 바람직한 실시 예에 대한 동작 원리를 상세하게 설명함에 있어 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0020] 도 1은 본 발명의 일 실시예에 따른 프락시 재암호화 장치를 도시한 블록도이다.

[0021] 위임자(Delegator, 110)는 자신의 비밀키로 메시지를 암호화한 메시지를 프락시 재암호화 장치(120)를 이용하여 대리자(Delegatee, 130)에게 분산한다.

[0022] 프락시 재암호화 장치(120)는 암호화된 메시지를 재암호화키를 이용하여 재암호화한다. 상기 재암호화키는 공개파라미터, 두 개의 비밀키, 상기 위임자(110)로부터 입력받은 위임자 개인식별정보, 및 상기 대리자(130)으로부터 입력받은 대리자 개인식별정보를 이용하여 생성된다. 상기 재암호화키는 해시함수를 이용하여 상기 대리자 개인식별정보로부터 해시값을 산출하고, 겹선형 함수를 이용하여 상기 해시값과 상기 각 비밀키로부터 각각의 연산값을 산출함으로써, 소정의 난수와 상기 두 개의 비밀키의 비율로부터 생성되고, 상기 두 개의 비밀키의 비율은 상기 연산값과 상기 두 개의 비밀키로부터 산출된다. 본 장치에 대한 상세한 설명은 도 2에 대한 상세한 설명에 대응하는바, 도 2 에 대한 상세한 설명에서 자세히 살펴보도록 한다.

[0023] 대리자(Delegatee, 130)는 프락시 재암호화 장치(120)가 재암호화된 메시지를 자신의 비밀키로 복호화하여 메시지를 확인한다. 대리자(130)는 위임자(110)의 상기 재암호화된 메시지에 대한 접근을 허용하는 경우에만 재암호화된 메시지를 복호화할 수 있다.

[0024] 도 2는 본 발명의 다른 실시예에 따른 프락시 재암호화 방법으로 메시지를 재암호화하는 동안 이용되는 파라미터와 키들을 도시한 도면이다.

[0025] 마스터 비밀키(210), 공개파라미터(220), 및 위임자 개인식별정보(230)을 이용하여 비밀키(250)를 생성한다. 공개파라미터(220)와 위임자 개인식별정보(230)을 이용하여 메시지(270)를 암호화하여 암호화된 메시지(280)를 생성한다. 공개파라미터(220), 위임자 개인식별정보(230), 대리자 개인식별정보(240), 및 비밀키(250)을 이용하여 재암호화키(260)를 생성한다. 재암호화키(260)을 이용하여 암호화된 메시지(280)를 재암호화하여 재암호화된 메시지(290)를 생성한다.

[0026] 본 발명의 실시예에 따른 상기 파라미터와 키들을 이용하는 프록시 재암호화 방법은 두 개의 비밀키의 비율을 이용하여 재암호화키를 생성하므로, 상기 비밀키의 비율은 노출될 수 있어도 비밀키 각각이 노출되지 않는바 악의적인 프락시와 대리자의 공모공격에 안전하다. 본 발명의 실시예에 따른 상기 파라미터와 키들을 이용하는 프록시 재암호화 방법을 전체적으로 살펴보면 다음과 같다.

[0027] 첫 번째, 공개파라미터와 마스터 비밀키를 설정한다.(Setup(1^k) 단계)

[0028] 보다 구체적으로, 겸선형 함수와 관련된 순환군(cyclic group)들 (G_1, G_2, e)를 생성한다. 상기 G1과 G2는 소수 q를 위수로 갖으며, e: $G_1 \times G_1 \rightarrow G_2$는 어드미서블 겹선형 함수(admissible bilinear map)이다. 겹선형 함수는 $e(P^a,Q^b)=e(P,Q)^{ab}$를 만족하는 겹선형성 $e(P,Q)\neq 1$을 만족하는 $P,Q\in G_x$의 존재성, 및 모든 $P,Q\in G_x$에 대한 e(P,Q)계산의 효율성을 만족하는 함수이다. G_1에서 임의의 생성원 g와 암호학적인 해시 함수들 H_i: $\{0,1\}^* \rightarrow G_1^*$ (i=1,2,3), H_4: $G_2^* \times \{0,1\}^n \rightarrow Z_q^*$, H_5: $G_2 \rightarrow \{0,1\}^n$을 선택한다. 임의의 난수 $\alpha, \beta \in Z_q^*$를 선택하고, $w = g^{\alpha-\beta}$를 계산한다. 그리고 공개파라미터(Public Parameter, PP)와 마스터 비밀키(Master Key, MK)를 다음 수학식 1과 같이 설정한다.

[0029] [수학식 1]

[0030] $PP= (G_1,G_2,e,q,g,w = g^{\alpha-\beta},H_1,H_2,H_3,H_4,H_5)$

[0031] $MK = \alpha, \beta$

[0032] 두 번째, 위임자의 두 개의 비밀키를 생성한다.(Extract(MK, PP, ID) 단계)

[0033] 보다 구체적으로, 마스터 비밀키(MK), 공개파라미터(PP), 및 개인식별정보 $ID\in\{0,1\}^*$을 입력받는다. 상기 개인식별정보를 이용하여 두 개의 비밀키(SK_{ID})를 다음 수학식 2와 같이 생성한다.

[0034] [수학식 2]

[0035] $SK_{ID} = (H_1(ID)^{\alpha},H_2(ID)^{\beta})$

[0036] 세 번째, 메시지를 암호화한다.(Encryption(M,PP,ID) 단계)

[0037] 보다 구체적으로, 메시지(M), 공개파라미터(PP), 및 위임자의 개인식별정보(ID)를 입력받는다. 임의의 $\sigma\in G_2$를 선택하고 $r = H_4(\sigma, M)$을 산출한다. 다음, 암호문 $c' = (A,B,C) = (g^r, \sigma \cdot e(w,H_1(ID)^r), M \oplus H_5(\sigma))$을 산출한다. 상기 암호문 c'을 이용하여 $h = H_3(ID \| c') \in G_1$를 생성하고 $S = h^r$을 산출한다. 상기 S와 암호문 c'를 이용하여 메시지(M)를 암호화한 암호문 C_{ID}를 다음 수학식 3과 같이 생성한다.

[0038] [수학식 3]

[0039] $C_{ID} = (S,A,B,C)$

[0040] 네 번째, 재암호화 키를 생성한다.(RKGen(PP,SK_{ID1},ID_1,ID_2) 단계)

[0041] 보다 구체적으로, 공개파라미터(PP), 위임자 개인식별정보(ID_1), 대리자 개인식별정보(ID_2), 비밀키(SK_{ID1})를 입

력받는다. 임의의 난수 $N \in \{0,1^n\}$ 를 선택하고 $K_1 = e(H_1(ID_1)^{\alpha}, H_1(ID_2))$, $K_2 = e(H_1(ID_1)^{\beta}, H_1(ID_2))$을 산출한다. 상기 난수, 비밀키, K_1, K_2 를 이용하여 재암호화키 $RK_{ID1 \to ID2}$를 다음 수학식 4와 같이 생성한다.

[0042] [수학식 4]

[0043]
$$RK_{ID_1 \to ID_2} = \left\langle N, \frac{H_2(K_1 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\beta}}{H_2(K_2 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\alpha}} \right\rangle$$

[0044] 다섯 번째, 암호화된 메시지를 재암호화한다.(Re-Encryption(PP,C_{ID1},$RK_{ID1 \to ID2}$)단계)

[0045] 보다 구체적으로, 공개파라미터(PP), 암호화된 메시지(C_{ID1} = (S,A,B,C)), 재암호화키 ($RK_{ID_1 \to ID_2} = \left\langle N, \frac{H_2(K_1 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\beta}}{H_2(K_2 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\alpha}} \right\rangle$)를 입력받는다. 우선, 상기 암호화된 메시지가 상기 암호화방법에 의해 암호화된 메시지인지 겹선형 함수를 이용하여 검증한다. h= H_2(ID∥(A,B,C))를 생성하고 e(g,S)=e(h,A)인지 검증한다. 상기 검증결과, 상기 식을 만족하는 경우에만 재암호화과정을 수행한다. 임의의 $t \in Z_q^*$를 선택하고 $B' = B \cdot e(g^t, S) \cdot e(A, RK_{ID1 \to ID2} \cdot h^t)^{-1}$를 산출하고, 암호화된 메시지를 재암호화한 암호문 C_{ID2} 를 다음 수학식 5와 같이 생성한다.

[0046] [수학식 5]

[0047] C_{ID2} = (A,B',C,ID_1,N)

[0048] 마지막으로 대리자는 상기 암호화된 메시지를 복호화한다.(Decryption (PP,C_{ID},SK_{ID}) 단계)

[0049] 보다 구체적으로, 공개파라미터(PP), 암호문(C_{ID}), 및 비밀키(SK_{ID})를 입력받는다. 암호문이 암호화 되었는지, 재암호화 되었는지에 따라 다음 두가지 방법으로 복호화한다.

[0050] 상기 Encryption(M,PP,ID) 단계에 의해 암호화된 암호문 C_{ID} = (S,A,B,C)을 복호화하는 과정(레벨1(Level-1))은 우선, h= H_2(ID∥(A,B,C))를 산출한다. 다음, 임의의 $t \in Z_q^*$를 선택하고 $\sigma' = B \cdot e(A, H_1(ID)^{\alpha} \cdot H_1(ID)^{-\beta} h^t) \cdot e(g^t, S)^{-1}$를 산출한다. 상기 σ'를 이용하여 $M' = C \oplus H_5(\sigma')$을 산출하여 메시지를 복호화하고, $r' = H_4(\sigma', M')$을 생성한다. $S = h^{r'}$와 $A = g^{r'}$의 등호가 성립하는지 확인하여, 등호가 성립하는 경우에만 M'를 반환한다.

[0051] 상기 Re-Encryption(PP,C_{ID1},$RK_{ID1 \to ID2}$)단계에 의해 재암호화된 암호문 C_{ID} = (A,B,C,ID_{src},N)을 복호화하는 과정(레벨2(Level-2))은 우선, $K = e(H_1(ID_{src}), SK_{ID})$를 산출하고, $\sigma' = B \cdot e(A, H_2(K \| ID_{src} \| ID \| N)$를 산출한다. $M' = C \oplus H_5(\sigma')$을 산출하여 메시지를 복호화하고, $r' = H_4(\sigma', M')$을 생성한다. $A = g^{r'}$의 등호가 성립하는지 확인하여, 등호가 성립하는 경우에만 M'를 반환한다.

[0052] 상기 6단계로 설명한 바와 같이 두 개의 비밀키를 이용하여 메시지를 재암호화하면 프락시와 대리자의 공모공격에 안전할 수 있다. 악의적인 프락시와 공모자는 재암호화키($RK_{ID1 \to ID2}$)와 대리자의 비밀키 $(H_1(ID_2)^{\alpha}, H_2(ID_2)^{\beta})$를 이용하여 $K_1 = e(H_1(ID_1), H_1(ID_2)^{\alpha}) = e(H_1(ID_1)^{\alpha}, H_1(ID_2))$를 산출할 수 있고, $K_2 = e(H_1(ID_1), H_1(ID_2)^{\beta}) = e(H_1(ID_1)^{\beta}, H_1(ID_2))$을 산출할 수 있다. ID_1, ID_2, N이 모두 공개된 정보인바, $P_1 = H_2(K_1 \| ID_1 \| ID_2 \| N)$, $P_2 = H_2(K_2 \| ID_1 \| ID_2 \| N)$를 산출할 수 있다. 상기 산출된 값들을 이용하여 다음 수학식 6과 같이 위임자의 비밀키에 대해 알 수 있다.

[0053] [수학식 6]

[0054]
$$\frac{H(ID_1)^{\beta}}{H(ID_1)^{\alpha}} = \frac{H_2(K_1 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\beta}}{H_2(K_2 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\alpha}} \cdot \frac{P_2}{P_1}$$

[0055] 상기와 같이 $H_1(ID_1)^{\alpha}/H_1(ID_1)^{\beta}$로부터 $H_1(ID_1)^{\alpha}$과 $H_1(ID_1)^{\beta}$의 비율만을 알 수 있고, $H_1(ID_1)^{\alpha}$,$H_1(ID_1)^{\beta}$ 각각을 알 수 없으므로 위임자의 비밀키가 노출되지 않는다.

[0056] 이에 반해, 두 개의 비밀키를 이용하지 않고 한 개의 비밀키를 이용하여 재암호화하는 경우에는 위임자의 비밀키가 노출될 수 있다. 두 개의 비밀키를 이용하지 않는 경우, 공개파라미터(PP)와 마스터 비밀키(MK)는 다음 수학식 7과 같이 상기 수학식 1과 다르다.

[0057] [수학식 7]

[0058] $PP = (G_1,G_2,e,q,g,g^s,H_1,H_2,H_3,H_4,H_5)$

[0059] $MK = s$

[0060] 또한, 비밀키(SK_{ID})는 다음 수학식 8과 같이 수학식 2와 다르다.

[0061] [수학식 8]

[0062] $SK_{ID} = H_1(ID)^{\alpha}$

[0063] 상기와 같이 비밀키(SK_{ID}) 하나만 이용하므로, 재암호화키가 두 개의 비밀키를 이용하는 경우와 다르다. 즉, 재암호화키는 다음 수학식 9와 같이 수학식 4와 다르다.

[0064] [수학식 9]

[0065] $$RK_{ID_1 \rightarrow ID_2} = \langle N, H_2(K \| ID_1 \| ID_2 \| N) \cdot SK_{ID_1} \rangle$$

[0066] 상기 비밀키(SK_{ID}) 하나를 이용하여 재암호화하는 방법은 악의적인 프락시와 대리자의 공모공격에 의해 위임자의 비밀키가 노출될 수 있다. 프락시는 재암호화키 $RK_{ID_1 \rightarrow ID_2} = \langle N, H_2(K \| ID_1 \| ID_2 \| N) \cdot SK_{ID_1} \rangle$를 알 수 있으며, 상기 N은 $\{0,1\}^{n(k)}$에서 임의로 선택한 수이고 $SK_{ID1}=H_1(ID_1)^{\alpha}$, $K=e(H_1(ID_1),H_1(ID_2))^{\alpha}$이다. 프락시와 대리자는 우선 SK_{ID2}를 이용하여 $K=e(H_1(ID_1),SK_{ID2})=e(H_1(ID_1),H_1(ID_2))^{\alpha}$를 산출할 수 있다. 등록된 재암호화키 $RK_{ID1 \rightarrow ID2}$와 상기 산출한 K를 이용하여 다음 수학식 10과 같이 위임자의 비밀키(SK_{ID1})를 산출할 수 있다.

[0067] [수학식 10]

[0068] $$SK_{ID_1} = (H_2(K \| ID_1 \| ID_2 \| N) \cdot SK_{ID_1}) \cdot H_2(K \| ID_1 \| ID_2 \| N)^{-1}$$

[0069] 도 3은 본 발명의 일 실시예에 따른 프락시 재암호화 방법의 흐름도이다.

[0070] 310단계는 공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하는 단계이다.

[0071] 보다 구체적으로, 암호화와 재암호화에 이용되는 공개파라미터, 비밀키를 생성하는데 필요한 마스터 비밀키, 및 위임자의 개인식별정보를 이용하여 두 개의 비밀키를 생성한다. 악의적인 프락시와 대리자의 공모공격으로부터 안전하기 위해 두 개의 비밀키를 생성한다. 본 단계에 대한 상세한 설명은 상기 Extract(MK, PP, ID) 단계에 대응하는바, 상기 Extract(MK, PP, ID) 단계에 대한 상세한 설명으로 대신한다. 상기 공개파라미터와 마스터 비밀키의 설정에 대한 상세한 설명은 Setup(1^k) 단계에 대응한다.

[0072] 상기 두 개의 비밀키는, 제 1 해시함수를 이용하여 상기 위임자의 개인식별정보로부터 제 2 해시값을 산출하고, 상기 제 2 해시값을 두 개의 마스터 비밀키로 지수승함으로써 생성한다.

[0073] 보다 구체적으로, 제 1해시함수 H_i: $\{0,1\}^* \rightarrow G_1^*$ (i=1,2,3)를 이용하여 위임자의 개인식별정보로부터 제 2 해시값 $H_1(ID_1)$을 산출한다. 상기 제 2 해시값 $H_1(ID_1)$을 두 개의 마스터 비밀키 $MK = \alpha, \beta$로 지수승함으로써 두 개의 비밀키 $SK_{ID} = (H_1(ID)^{\alpha},H_2(ID)^{\beta})$를 생성한다.

[0074] 320단계는 상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하는 단계이다.

[0075] 보다 구체적으로, 위임자의 개인식별부호를 이용하여 메시지를 암호화한다. 메시지를 암호화할 때 Setup(1^k) 단계에서 설정한 공개파라미터를 이용한다. 본 단계에 대한 상세한 설명은 상기 Encryption(M,PP,ID) 단계에 대응하는바, 상기 Encryption(M,PP,ID) 단계에 대한 상세한 설명으로 대신한다.

[0076] 330단계는 상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하는 단계이다.

[0077] 보다 구체적으로, 공개파라미터, 위임자 개인식별정보, 대리자 개인식별정보, 및 310단계에서 생성한 두 개의 비밀키를 이용하여 재암호화키를 생성하는 단계이다. 본 단계에 대해 도 4에서 자세히 살펴보도록 한다.

[0078] 340단계는 상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화하는 단계이다.

[0079] 보다 구체적으로, 320단계에서 암호화된 메시지를 330단계에서 생성한 재암호화키를 이용하여 재암호화하는 단계이다. 본 단계에 대한 상세한 설명은 상기 Re-Encryption (PP, C_{ID1}, $RK_{ID1\rightarrow ID2}$)단계에 대응하는바, 상기 Re-Encryption (PP, C_{ID1}, $RK_{ID1\rightarrow ID2}$)단계에 대한 상세한 설명으로 대신한다.

[0080] 상기 본 발명의 일 실시예에 따른 프락시 재암호화 방법은 일련의 연산을 처리할 수 있는 처리기(processor) 및 이러한 연산에 필요한 기억공간(memory)을 통해 구현될 수 있으며, 필요에 따라서는 처리기와 기억공간 간의 데이터 처리를 적절하게 제어할 수 있는 제어기(controller)가 활용될 수도 있다. 이러한 처리기, 기억공간 및 제어기는 본 발명이 속하는 기술분야의 활용 환경이나 동작 환경을 고려하여 통상의 지식을 가진 기술자에 의해 적절하게 선택될 수 있다. 나아가, 이러한 제어 과정에는 이상에서 예시된 하드웨어들을 제어하기 위한 부가적인 소프트웨어 코드(code)도 활용될 수 있다.

[0081] 도 4는 본 발명의 다른 실시예에 따른 재암호화키를 생성하는 방법의 흐름도이다.

[0082] 410단계는 제 1 해시함수를 이용하여 상기 대리자 개인식별정보로부터 제 1 해시값을 산출하는 단계이다.

[0083] 보다 구체적으로, 제 1 해시함수에 대리자 개인식별정보를 입력하여 제 1 해시값을 산출한다. 상기 제 1 해시함수는 H_i: $\{0,1\}^* \rightarrow G_1^*$ (i=1,2,3)일 수 있다. 상기 제 1 해시함수를 이용하여 해시값 $H_1(ID_2)$을 산출한다.

[0084] 420단계는 겹선형 함수를 이용하여 상기 제 1 해시값과 상기 각 비밀키로부터 각각의 연산값을 산출하는 단계이다.

[0085] 보다 구체적으로, 410단계에서 산출한 제 1 해시값과 310단계에서 생성한 각 비밀키로부터 각각의 연산값을 산출한다. 상기 각 비밀키는 $(H_1(ID)^{\alpha}, H_2(ID)^{\beta})$로써 $H_1(ID)^{\alpha}$에 대한 연산값 $K_1 = e(H_1(ID_1)^{\alpha}, H_1(ID_2))$과 $H_2(ID)^{\beta}$에 대한 연산값 $K_2 = e(H_1(ID_1)^{\beta}, H_1(ID_2))$을 산출한다.

[0086] 430단계는 소정의 난수와 상기 두 개의 비밀키의 비율로부터 상기 재암호화키를 생성하는 단계이다.

[0087] 보다 구체적으로, 특정 하나의 난수와 310단계에서 생성한 두 개의 비밀키의 비율로부터 상기 재암호화키를 생성한다. 상기 두 개의 비밀키의 비율은 420단계에서 산출한 연산값과 상기 두 개의 비밀키로부터 산출한다. 상기 난수는 $N \in \{0,1^n\}$ 일 수 있다. 상기 난수, 상기 연산값 K_1과 K_2, 두 개의 비밀키를 이용하여 재암호화키

$$RK_{ID_1\rightarrow ID_2} = \left\langle N, \frac{H_2(K_1 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\beta}}{H_2(K_2 \| ID_1 \| ID_2 \| N) \cdot H(ID_1)^{\alpha}} \right\rangle$$

를 생성한다.

[0088] 도 5는 본 발명의 다른 실시예에 따른 암호화된 메시지를 재암호화 하는 방법의 흐름도이다.

[0089] 510단계는 제 2 해시함수를 이용하여 상기 위임자의 개인식별정보 및 암호화된 메시지로부터제 3 해시값을 산출하는 단계이다.

[0090] 보다 구체적으로, 제 2 해시함수에 위임자의 개인식별정보와 암호화된 메시지를 입력하여 제 3 해시값을 산출한다. 제 2 해시함수 H_i: $\{0,1\}^* \rightarrow G_1^*$ (i=1,2,3)를 이용하여 암호화된 메시지 c' = (A,B,C) = (g^r, σ ·

$e(w,H_1(ID)^r)$, $M \oplus H_5(\sigma))$와 위임자 개인식별정보로부터 $h= H_2(ID \| (A,B,C))$를 산출한다.

[0091] 520단계는 상기 제 3 해시값을 이용하여 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는지 판단하는 단계이다.

[0092] 보다 구체적으로, 510단계에서 산출한 제 3 해시값을 이용하여 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는지 판단한다. 상기 제 3 해시값 $h= H_2(ID \| (A,B,C))$를 이용하여 겹선형 함수 $e(g,S)=e(h,A)$인지 판단한다.

[0093] 530단계는 상기 판단결과, 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는 경우, 상기 암호화된 메시지를 상기 공개파라미터와 재암호화키를 이용하여 재암호화하는 단계이다.

[0094] 보다 구체적으로, 520단계의 판단결과, 겹선형 함수의 정의를 만족하는 경우, 공개파라미터, 320단계에서 암호화된 메시지, 330단계에서 생성한 재암호화키를 이용하여 암호화된 메시지를 재암호화하는 단계이다. $e(g,S)=e(h,A)$인지 검증하여, 상기 식을 만족하는 경우에만 재암호화과정을 수행한다. 임의의 $t \in Z_q^*$를 선택하고 $B'= B \cdot e(g^t,S) \cdot e(A,RK_{ID1 \rightarrow ID2} \cdot h^t)^{-1}$를 산출하고, 암호화된 메시지를 재암호화한 암호문 $C_{ID2} = (A,B',C,ID_1,N)$를 생성한다.

[0095] 도 6은 본 발명의 일 실시예에 따른 프락시 재암호화 메시지 복호화방법의 흐름도이다.

[0096] 610단계는 재암호화된 메시지를 수신하는 단계이다.

[0097] 보다 구체적으로, 프락시 재암호화된 메시지를 수신한다. 상기 재암호화된 메시지는 상기 공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성하고, 상기 공개파라미터와 상기 위임자 개인식별정보를 이용하여 메시지를 암호화하고, 상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성하며, 상기 재암호화키를 이용하여 상기 암호화된 메시지를 재암호화함으로써 생성된 메시지이다. 상기 재암호화된 메시지는 도 3 내지 도 5의 방법에 의해 생성된 것일 수 있다. 재암호화된 메시지에 대한 상세한 설명은 도 3 내지 도 5에 대한 상세한 설명에 대응하는바, 도 3 내지 도 5에 대한 상세한 설명으로 대신한다.

[0098] 620단계는 공개 파라미터와 대리자 비밀키를 이용하여 상기 재암호화된 메시지를 복호화하는 단계이다.

[0099] 보다 구체적으로, 공개파라미터와 대리자 개인식별정보를 이용하여 생성된 비밀키를 이용하여 상기 재암호화된 메시지를 복호화하는 단계이다. 본 단계에 대한 상세한 설명은 상기 Decryption (PP,C_{ID},SK_{ID}) 단계에 대응하는 바, 상기 Decryption (PP,C_{ID},SK_{ID}) 단계에 대한 상세한 설명으로 대신한다.

[0100] 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0101] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0102] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0103] 110: 위임자

120: 프락시 재암호화 장치

210: 마스터 비밀키

220: 공개파라미터

230: 위임자 개인식별정보

240: 대리자 개인식별정보

250: 비밀키

260: 재암호화키

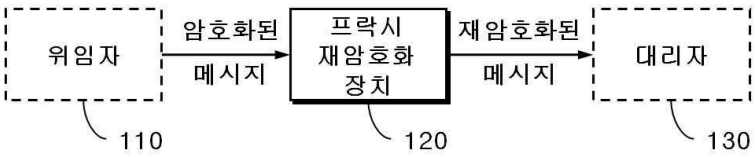
270: 메시지

280: 암호화된 메시지

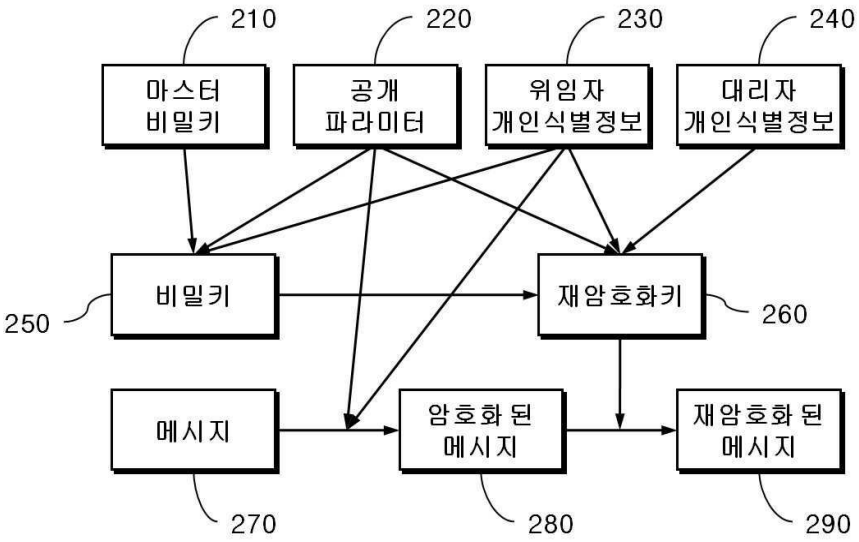
290: 재암호화된 메시지

도면

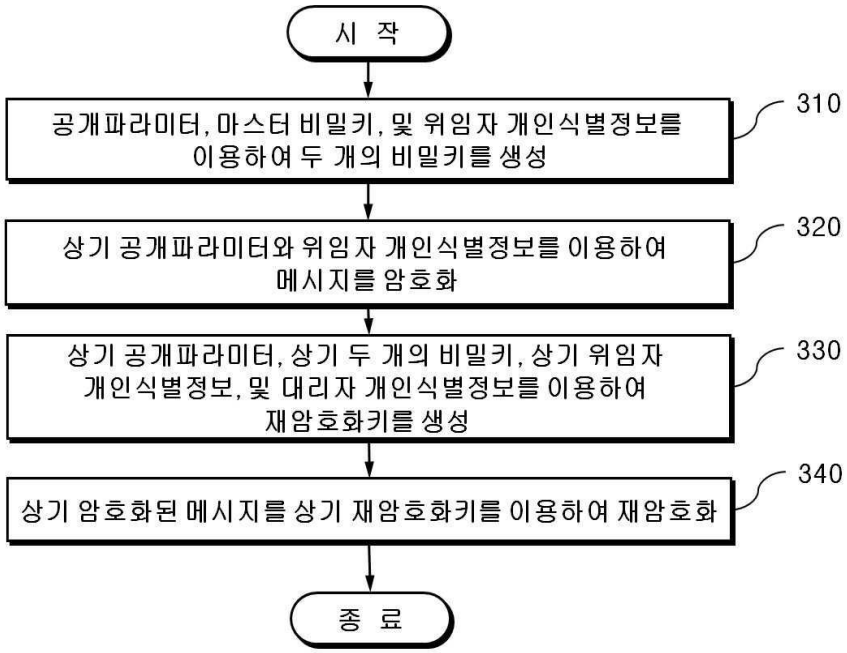
도면1



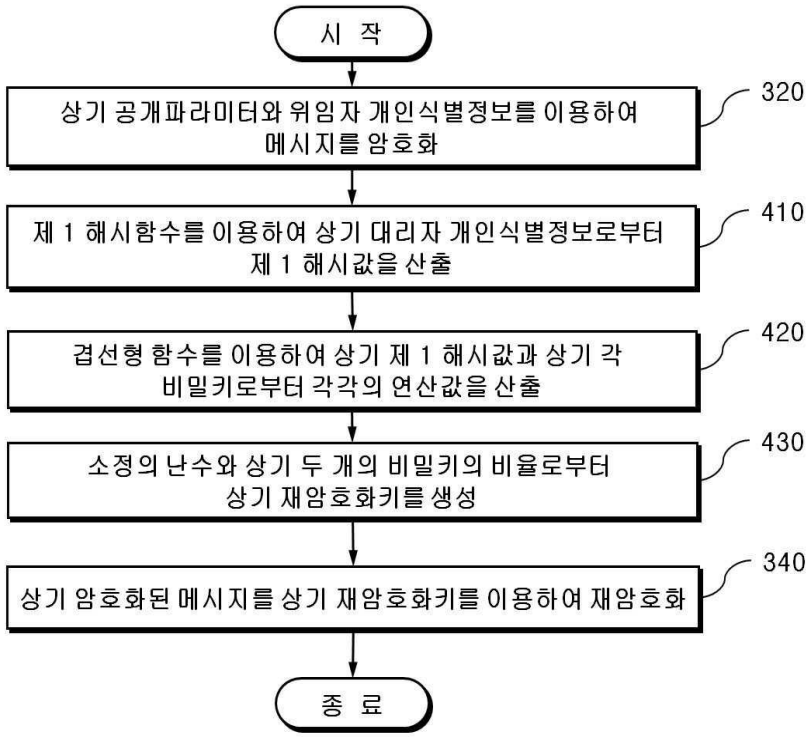
도면2



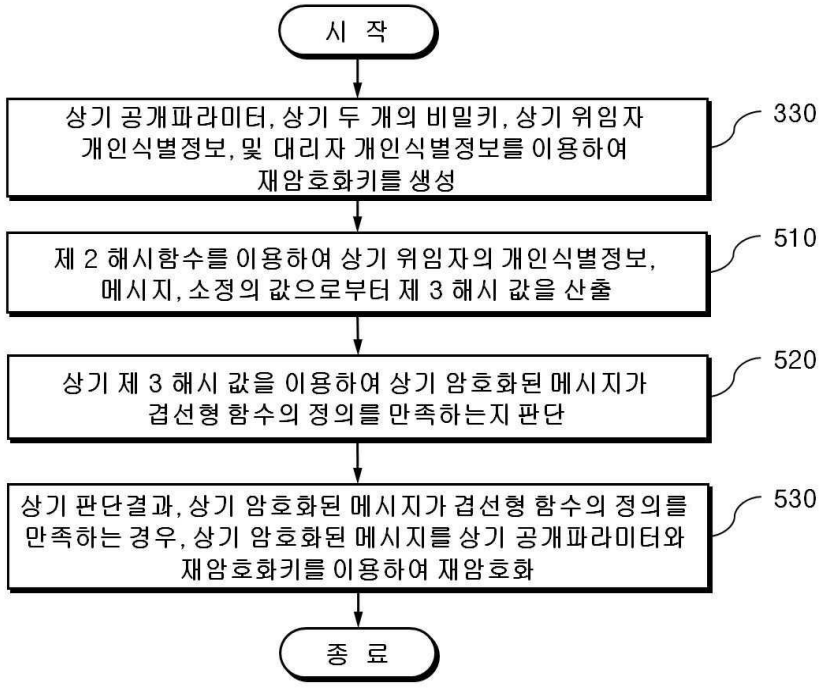
도면3


시 작
공개파라미터, 마스터 비밀키, 및 위임자 개인식별정보를 이용하여 두 개의 비밀키를 생성
310
상기 공개파라미터와 위임자 개인식별정보를 이용하여 메시지를 암호화
320
상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성
330
상기 암호화된 메시지를 상기 재암호화키를 이용하여 재암호화
340
종 료

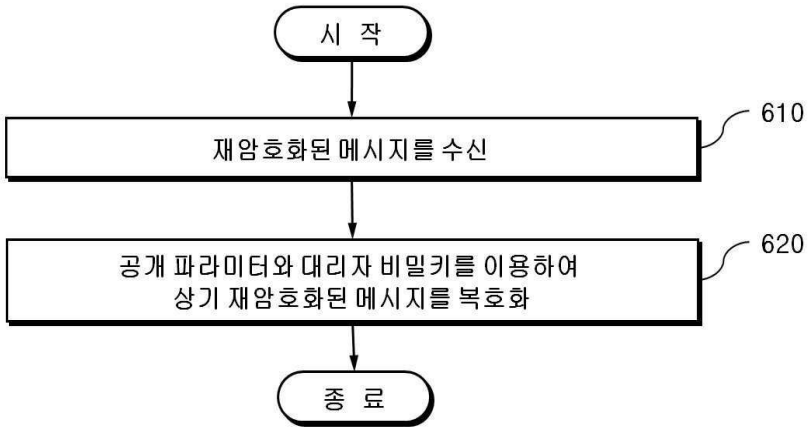
도면4


시 작
상기 공개파라미터와 위임자 개인식별정보를 이용하여 메시지를 암호화
320
제 1 해시함수를 이용하여 상기 대리자 개인식별정보로부터 제 1 해시값을 산출
410
겹선형 함수를 이용하여 상기 제 1 해시값과 상기 각 비밀키로부터 각각의 연산값을 산출
420
소정의 난수와 상기 두 개의 비밀키의 비율로부터 상기 재암호화키를 생성
430
상기 암호화된 메시지를 상기 재암호화키를 이용하여 재암호화
340
종 료

도면5


시 작
상기 공개파라미터, 상기 두 개의 비밀키, 상기 위임자 개인식별정보, 및 대리자 개인식별정보를 이용하여 재암호화키를 생성
330
제 2 해시함수를 이용하여 상기 위임자의 개인식별정보, 메시지, 소정의 값으로부터 제 3 해시 값을 산출
510
상기 제 3 해시 값을 이용하여 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는지 판단
520
상기 판단결과, 상기 암호화된 메시지가 겹선형 함수의 정의를 만족하는 경우, 상기 암호화된 메시지를 상기 공개파라미터와 재암호화키를 이용하여 재암호화
530
종 료

도면6


시 작
재암호화된 메시지를 수신
610
공개 파라미터와 대리자 비밀키를 이용하여 상기 재암호화된 메시지를 복호화
620
종 료