(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0069387
(43) 공개일자 2012년06월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/20 (2006.01) *H04L 9/14* (2006.01)
G06F 17/30 (2006.01)
(21) 출원번호 10-2010-0130917
(22) 출원일자 2010년12월20일
심사청구일자 2010년12월20일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 경희궁의아침 3단지 아파트 1404호 (내수동)
이현숙
서울 노원구 공릉동 81 태강아파트 1018동 301호
엄지은
서울특별시 서대문구 가재울로 45, 현대아파트 102동 102호 (남가좌동)
(74) 대리인
특허법인충현

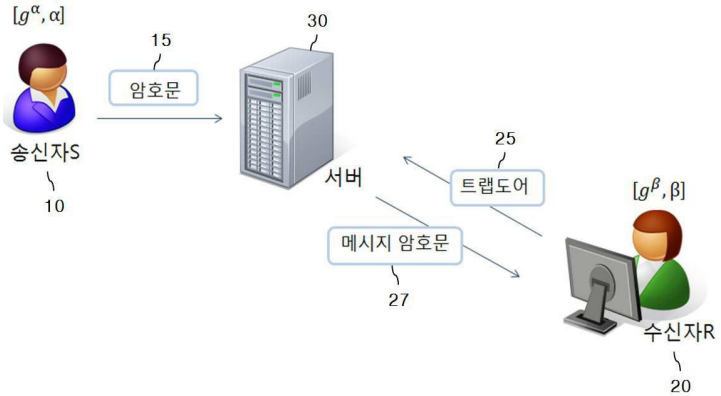
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **공개키 기반의 키워드 검색 방법**

(57) 요 약

본 발명은 공개키 기반의 키워드 검색 방법에 관한 것으로서, 본 발명에 따른 키워드 검색 방법은 송신자가 수신자의 공개키를 사용하여 메시지를 암호화하고, 송신자가 수신자의 공개키 및 송신자의 비밀키를 사용하여 키워드를 암호화하며, 암호화된 메시지 및 암호화된 키워드를 서버에 전송하되, 서버는 키워드, 수신자의 비밀키 및 송신자의 공개키를 이용하여 생성된 트랩도어를 수신자로부터 수신하고, 테스트 함수를 이용하여 암호화된 키워드와 트랩도어의 일치 여부를 검사함으로써, 키워드에 대응하는 암호화된 메시지를 수신자에게 선택적으로 출력한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	ITAA1100090100480001000100100
부처명	정보통신연구진흥원
연구사업명	IT산업원천기술개발사업
연구과제명	Car-헬스케어 보안 기술개발
주관기관	고려대학교 산학협력단
연구기간	2010.03.01 ~ 2011.02.28

특허청구의 범위

청구항 1

공개키 기반의 키워드 검색 방법에 있어서,

송신자가 수신자의 공개키를 이용하여 메시지를 암호화하는 단계;

상기 송신자가 상기 수신자의 공개키 및 상기 송신자의 비밀키를 이용하여 상기 메시지에 대응하는 키워드를 암호화하는 단계;

상기 암호화된 메시지 및 상기 암호화된 키워드로부터 암호문을 생성하는 단계; 및

상기 생성된 암호문을 서버에 전송하는 단계를 포함하는 방법.

청구항 2

제 1 항에 있어서,

상기 키워드를 암호화하는 단계는,

상기 송신자로부터 상기 메시지에 대응하는 적어도 하나 이상의 키워드를 입력받는 단계;

제 1 해시 함수를 이용하여 상기 입력된 키워드로부터 제 1 해시값을 산출하는 단계;

겹선형(bilinear) 함수를 이용하여 상기 산출된 제 1 해시값, 상기 수신자의 공개키 및 상기 송신자의 비밀키로부터 연산값을 산출하고, 제 2 해시 함수를 이용하여 상기 산출된 연산값으로부터 제 2 해시값을 산출하는 단계; 및

상기 송신자의 비밀키 및 상기 산출된 제 2 해시값으로부터 암호화된 키워드를 생성하는 단계를 포함하는 방법.

청구항 3

제 1 항에 있어서,

상기 암호문은 상기 암호화된 메시지와 상기된 적어도 하나 이상의 암호화된 키워드를 결합함으로써 생성되는 것을 특징으로 하는 방법.

청구항 4

제 1 항에 있어서,

상기 키워드는 상기 메시지를 검색하기 위해 수신자가 생성하는 트랩도어(trapdoor)에 대응하여 입력된 것을 특징으로 하는 방법.

청구항 5

제 1 항 내지 제 4 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 6

공개키 기반의 키워드 검색 방법에 있어서,

서버가 암호화된 메시지와 이에 대응하는 암호화된 키워드를 포함하는 암호문을 송신자로부터 수신하여 저장하는 단계;

서버가 수신자의 비밀키, 상기 송신자의 공개키 및 상기 메시지를 검색하기 위한 키워드를 이용하여 생성된 트랩도어를 상기 수신자로부터 수신하는 단계;

테스트 함수를 이용하여 상기 저장된 암호문에 포함된 암호화된 키워드와 상기 수신된 트랩도어의 일치 여부

를 검사하는 단계; 및

상기 검사 결과에 따라 상기 암호화된 키워드에 대응하는 상기 암호화된 메시지를 상기 수신자에게 선택적으로 출력하는 단계를 포함하는 방법.

청구항 7

제 6 항에 있어서,

상기 트랩도어는 제 1 해시 함수를 이용하여 상기 메시지를 검색하기 위한 키워드로부터 제 1 해시값을 산출하고, 상기 산출된 제 1 해시값과 상기 송신자의 공개키를 승산하며, 상기 승산 결과를 상기 수신자의 비밀키로 지수승함으로써 생성된 것을 특징으로 하는 방법.

청구항 8

제 7 항에 있어서,

상기 제 1 해시 함수는 상기 송신자가 상기 키워드를 암호화하기 위해 사용한 함수와 동일한 함수인 것을 특징으로 하는 방법.

청구항 9

제 6 항에 있어서,

상기 테스트 함수는 상기 암호화된 키워드로부터 상기 송신자의 공개키 성분 및 상기 송신자의 해시값을 추출하고, 겹선형 함수를 이용하여 상기 추출된 송신자의 공개키 성분 및 상기 수신된 트랩도어로부터 연산값을 산출하고, 제 2 해시 함수를 이용하여 상기 산출된 연산값으로부터 제 2 해시값을 산출하며, 상기 추출된 송신자의 해시값과 상기 산출된 제 2 해시값을 비교함으로써 상기 암호화된 키워드와 상기 수신된 트랩도어의 일치 여부를 검사하는 것을 특징으로 하는 방법.

청구항 10

제 9 항에 있어서,

상기 제 2 해시 함수는 상기 송신자가 겹선형 함수의 연산값을 암호화하기 위해 사용한 함수와 동일한 함수인 것을 특징으로 하는 방법.

청구항 11

제 6 항에 있어서,

상기 암호화된 메시지를 선택적으로 출력하는 단계는,

상기 암호화된 키워드와 상기 수신된 트랩도어가 일치하는 경우 참(true)의 응답 신호 및 상기 저장된 암호화된 메시지를 상기 수신자에게 출력하고,

상기 암호화된 키워드와 상기 수신된 트랩도어가 일치하지 않는 경우 거짓(false)의 응답 신호를 상기 수신자에게 출력하는 것을 특징으로 하는 방법.

청구항 12

제 6 항에 있어서,

상기 암호문을 저장하는 단계는 상기 서버가 상기 송신자를 기준으로 상기 수신된 암호문을 분류하여 저장하고,

상기 트랩도어를 상기 수신자로부터 수신하는 단계는 상기 서버가 상기 송신자에 대한 제한 정보가 부가된 트랩도어를 상기 수신자로부터 수신하며,

상기 암호화된 키워드와 상기 수신된 트랩도어의 일치 여부를 검사하는 단계는 상기 서버가 상기 부가된 제한 정보에 따라 상기 분류되어 저장된 암호문을 검색하는 것을 특징으로 하는 방법.

청구항 13

제 6 항 내지 제 12 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 공개키 기반의 키워드 검색 방법에 관한 것으로, 특히 공개키 암호를 기반으로 암호화된 시스템에서 키워드를 통해 암호화된 데이터를 검색할 수 있는 장치, 방법 및 그 방법을 기록한 기록매체에 관한 것이다.

배 경 기 술

[0002] 웹 서버(web server) 또는 이메일 서버(e-mail server) 등과 같은 외부 서버에 저장되는 디지털 정보들이 해킹과 바이러스로 인해 유출되는 위험을 방지하기 위한 전통적인 방법으로 데이터를 암호화하여 저장하는 방법이 있다. 그러나 이러한 방법은 사용자가 희망하는 데이터를 검색하기 위해 암호문을 모두 복호화한 후 내용을 각각 확인해야 하기 때문에 효율성이 떨어지고, 안전하지 않은 서버의 경우 기밀성과 프라이버시를 보장하기 어렵다는 문제점이 지적되어 왔다.

[0003] 이러한 문제점을 해결하기 위해 최근 암호화된 데이터 상에서 키워드를 검색할 수 있는 시스템이 제안되었다. 이러한 시스템에서 송신자는 미리 키워드를 설정한 후 메시지와 키워드를 각각 암호화하여 함께 서버로 전송하고, 수신자는 검색하고자 하는 키워드에 대해 검색 요청 데이터를 생성하여 서버에 전송한다. 이 때, 서버는 검색 요청 데이터와 암호화된 키워드를 비교하고 검색할 수는 있지만, 키워드 그 자체에 대한 정보는 얻지 못한다.

[0004] 이상과 같은 공개키 기반의 키워드 검색 시스템(public key encryption with keyword search, PEKS)은 웹 디스크나 블로그와 같이 공개된 데이터베이스에 적용 가능한 공개키 암호 시스템을 기반으로 한 기법이다. 이러한 기법은 메시지와 이에 대응하는 키워드를 각각 수신자의 공개키로 암호화하고 암호화된 메시지와 키워드를 함께 서버로 전송하여 수신자로 하여금 자신의 비밀키를 사용하여 키워드를 검색할 수 있는 환경을 제공한다.

[0005] 그러면, 수신자는 검색하고자 하는 키워드와 자신의 비밀키를 이용하여 검색 요청 데이터인 트랩도어(trapdoor)을 생성하여 서버에 전송하고, 서버는 트랩도어와 키워드 암호문을 테스트 함수를 통해 검사함으로써 양자가 동일한 키워드로부터 비롯된 데이터인지 여부를 판단한다. 만약, 검사 결과 동일한 키워드를 포함하고 있다면 암호화된 메시지를 수신자에게 전송하고, 반대의 경우에는 검색 결과가 없음을 알리는 메시지를 출력할 수 있다. 이상과 같은 과정을 통해 서버는 저장된 암호화 데이터 전부에 대한 복호화 과정 없이도 수신자가 희망하는 키워드를 통해 암호화된 데이터를 검색할 수 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 해결하고자 하는 기술적 과제는 공개키 기반의 키워드 검색 시스템이 공격자의 키워드 추측 공격에 취약한 한계를 극복하고, 특히 공격자에 의해 정당한 트랩도어가 획득된 경우 안전성을 담보하지 못하는 문제점을 극복하며, 수신자의 트랩도어에 의한 키워드 질의시 서버에 저장된 모든 암호문에 대한 검색을 수행하는 불편함을 해소하고자 한다.

과제의 해결 수단

[0007] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 공개키 기반의 키워드 검색 방법은 송신자가 수신자의 공개키를 이용하여 메시지를 암호화하는 단계; 상기 송신자가 상기 수신자의 공개키 및 상기 송신자의 비밀키를 이용하여 상기 메시지에 대응하는 키워드를 암호화하는 단계; 상기 암호화된 메시지 및 상기 암호화된 키워드로부터 암호문을 생성하는 단계; 및 상기 생성된 암호문을 서버에 전송하는 단계를 포함한다.

[0008] 또한, 상기된 공개키 기반의 키워드 검색 방법에서 키워드를 암호화하는 단계는, 상기 송신자로부터 상기 메시지에 대응하는 적어도 하나 이상의 키워드를 입력받는 단계; 제 1 해시 함수를 이용하여 상기 입력된 키워드로부터 제 1 해시값을 산출하는 단계; 겹선형(bilinear) 함수를 이용하여 상기 산출된 제 1 해시값, 상기 수신자의 공개키 및 상기 송신자의 비밀키로부터 연산값을 산출하고, 제 2 해시 함수를 이용하여 상기 산출된

연산값으로부터 제 2 해시값을 산출하는 단계; 및 상기 송신자의 비밀키 및 상기 산출된 제 2 해시값으로부터 암호화된 키워드를 생성하는 단계를 포함한다.

[0009] 상기 기술적 과제를 해결하기 위하여, 본 발명에 따른 공개키 기반의 키워드 검색 방법은 서버가 암호화된 메시지와 이에 대응하는 암호화된 키워드를 포함하는 암호문을 송신자로부터 수신하여 저장하는 단계; 서버가 수신자의 비밀키, 상기 송신자의 공개키 및 상기 메시지를 검색하기 위한 키워드를 이용하여 생성된 트랩도어를 상기 수신자로부터 수신하는 단계; 테스트 함수를 이용하여 상기 저장된 암호문에 포함된 암호화된 키워드와 상기 수신된 트랩도어의 일치 여부를 검사하는 단계; 및 상기 검사 결과에 따라 상기 암호화된 키워드에 대응하는 상기 암호화된 메시지를 상기 수신자에게 선택적으로 출력하는 단계를 포함한다.

[0010] 또한, 상기된 공개키 기반의 키워드 검색 방법에서 상기 트랩도어는 제 1 해시 함수를 이용하여 상기 메시지를 검색하기 위한 키워드로부터 제 1 해시값을 산출하고, 상기 산출된 제 1 해시값과 상기 송신자의 공개키를 승산하며, 상기 승산 결과를 상기 수신자의 비밀키로 지수승함으로써 생성된 것이 바람직하다.

[0011] 나아가, 상기된 공개키 기반의 키워드 검색 방법에서 상기 테스트 함수는 상기 암호화된 키워드로부터 상기 송신자의 공개키 성분 및 상기 송신자의 해시값을 추출하고, 겹선형 함수를 이용하여 상기 추출된 송신자의 공개키 성분 및 상기 수신된 트랩도어로부터 연산값을 산출하고, 제 2 해시 함수를 이용하여 상기 산출된 연산값으로부터 제 2 해시값을 산출하며, 상기 추출된 송신자의 해시값과 상기 산출된 제 2 해시값을 비교함으로써 상기 암호화된 키워드와 상기 수신된 트랩도어의 일치 여부를 검사하는 것이 바람직하다.

[0012] 한편, 상기 다른 기술적 과제를 해결하기 위하여, 상기된 공개키 기반의 키워드 검색 방법에서 상기 암호문을 저장하는 단계는 상기 서버가 상기 송신자를 기준으로 상기 수신된 암호문을 분류하여 저장하고, 상기 트랩도어를 상기 수신자로부터 수신하는 단계는 상기 서버가 상기 송신자에 대한 제한 정보가 부가된 트랩도어를 상기 수신자로부터 수신하며, 상기 암호화된 키워드와 상기 수신된 트랩도어의 일치 여부를 검사하는 단계는 상기 서버가 상기 부가된 제한 정보에 따라 상기 분류되어 저장된 암호문을 검색하는 것이 바람직하다.

[0013] 또한, 이하에서는 상기 기재된 공개키 기반의 키워드 검색 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

발명의 효과

[0014] 본 발명은 키워드를 암호화함에 있어서 송신자의 비밀키를 이용함으로써 공개키 기반의 키워드 검색 시스템에서 공격자의 키워드 추측 공격을 원천적으로 차단하고, 비록 공격자가 불법적으로 정당한 트랩도어를 획득하더라도 이에 대응하는 키워드 암호문을 생성할 수 없으므로 안전성을 보장할 수 있으며, 송신자를 기준으로 암호문을 분류하여 검색함으로써 수신자의 키워드 질의시 검색 범위 및 연산량을 감소시킬 수 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법의 기본 아이디어와 전체적인 동작 방법을 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법을 송신자를 중심으로 도시한 흐름도이다.

도 3은 도 2의 공개키 기반의 키워드 검색 방법에서 키워드를 암호화하는 방법을 보다 구체적으로 도시한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법에서 송신자 및 서버의 수행 동작을 데이터를 중심으로 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법을 서버를 중심으로 도시한 흐름도이다.

도 6은 도 5의 공개키 기반의 키워드 검색 방법에서 트랩도어를 생성하는 방법을 보다 구체적으로 도시한 흐름도이다.

도 7은 도 5의 공개키 기반의 키워드 검색 방법에서 암호화된 키워드와 트랩도어의 일치 여부를 검사하는 방법을 보다 구체적으로 도시한 흐름도이다.

도 8은 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법에서 수신자와 서버의 수행 동작을 데이

터를 중심으로 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0016] 본 발명의 실시예들을 설명하기에 앞서 본 발명의 실시예들이 구현되는 환경 및 배경 기술들에 대해 개괄적으로 소개하고자 한다.

[0017] 앞서 소개한 공개키 기반의 키워드 검색 기법은 오프라인 상에서 공격자에 의한 키워드 추측 공격(keyword guessing attack)이 가능하다. 여기서, 키워드 추측 공격이란 수신자가 검색하고자 했던 키워드가 무엇인지 추측하여 알아내는 공격을 말한다. 즉, 공격자가 트랩도어를 얻게 되었을 때 공격자는 수신자가 어떤 키워드를 검색했을지를 추측함으로써 해당 키워드를 암호화하고 트랩도어와 키워드 암호문을 테스트 함수를 사용하여 동일성을 확인할 수 있다. 이 경우, 만약 수신자가 해당 트랩도어를 이용하여 검색에 성공했다는 사실이 공격자에게 알려진다면, 공격자는 최초의 송신자가 생성한 키워드를 추측함으로써 해당 키워드에 대한 암호문이 서버에 존재하는지 여부를 확인할 수 있게 되는 문제점이 발생한다.

[0018] 이상과 같은 키워드 추측 공격이 가능한 이유는 암호문에 대한 키워드가 누구나 추측할 수 있는 단어로 구성되는 것이 일반적이고, 나아가 누구나 손쉽게 수신자의 공개키로부터 키워드 암호문을 생성하는 것이 가능하기 때문이다. 즉, 공격자는 언제든지 테스트 함수를 이용하여 트랩도어에 사용된 키워드와 추측한 키워드가 동일한지 확인할 수 있으며, 그 결과 공개키 기반의 키워드 검색 기법은 상술한 바와 같은 키워드 추측 공격에 대한 안전성을 제공하지 못한다는 문제점이 발견되었다.

[0019] 상기된 문제점에 대한 인식에 기초하여 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명한다.

[0020] 도 1은 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법의 기본 아이디어와 전체적인 동작 방법을 설명하기 위한 도면으로, 해당 시스템은 크게 송신자(10), 수신자(20) 및 서버(30)로 구성된다.

[0021] 본 발명의 실시예들은 무엇보다도 키워드 추측 공격이 수신자의 공개키로부터 누구나 키워드 암호문을 생성할 수 있다는 점에서 비롯되었음에 주목하였다. 따라서, 본 발명의 실시예들은 트랩도어(trapdoor)에 대응하는 키워드 암호문을 생성할 수 있는 능력을 제한함으로써 키워드 추측 공격에 대한 안전성을 제공하고자 한다. 이를 위해, 본 발명의 실시예들에서는 트랩도어에 대응하는 암호문을 생성할 수 있는 능력을 제한하기 위해 키워드 암호문을 생성하는 과정에서 송신자의 비밀정보를 사용하는 방법을 제안한다. 즉, 키워드를 암호화함에 있어서 송신자의 비밀키를 사용하고자 한다.

[0022] 공개키 암호화 시스템에서 송신자의 비밀키는 송신자만이 알 수 있으므로, 결국 키워드에 대한 암호화는 오직 송신자만이 가능하다는 결론을 얻을 수 있다. 이를 통해 공격자가 아무리 정확한 키워드를 추측할 수 있더라도 송신자의 비밀키를 알 수 없으므로 트랩도어에 대응하는 키워드 암호문을 생성할 수 없다. 그 결과 공격자에 의한 키워드 추측 공격은 그 수행 자체가 불가능해진다. 이 경우, 물론 테스트 함수를 통한 연산을 위해 트랩도어 생성 과정에서 송신자의 공개키가 활용되어야 함은 당연하다.

[0023] 이에, 본 발명의 도면들을 통해 공통적으로 사용할 기호들을 소개하도록 한다. pk는 공개키(public key)를 나타내고, sk는 비밀키(secret key)를 나타내고, 영문자 S는 송신자(sender)를 나타내고, 영문자 R은 수신자(receiver)를 나타내고, 영문자 W는 키워드를 나타내며, 영문자 T_W는 트랩도어를 나타낸다. 공개키 기반의 키워드 검색 시스템을 구현하기 위해 위수가 소수 p인 순환군(cyclic group) G_1과 G_2를 설정하고, G_1의 생성원(generator) g와 겹선형 함수 $e:G_1\times G_1\rightarrow G_2$를 설정한다. 그리고, 2 개의 암호학적 해시 함수(hash function)를 각각 $H_1:\{0,1\}^*\rightarrow G_1$과 $H_2:G_2\rightarrow\{0,1\}^{\log p}$와 같이 정의한다.

[0024] 도 1에서 우선 키를 발급하는 기관(key generation center)에서 송신자의 공개키 및 비밀키를 생성하는 알고리즘 $KeyGen_S(1^\lambda)$에 따라 임의의 랜덤(random)값 $\alpha\in Z_p^*$를 선택하여 송신자의 비밀키로 설정하고, 이로부터 송신자의 공개키를 산출한다. 산출된 송신자의 공개키 및 비밀키는 다음의 수학식 1과 같이 표현된다.

수학식 1

[0025] $$[pk_S = g^{\alpha}, sk_S = \alpha]$$

[0026] 이제 수학식 1과 같이 생성된 송신자의 공개키 및 비밀키는 송신자에게 제공되고, 그 중 송신자의 공개키는 대중에게 공개된다.

[0027] 마찬가지로 키 발급 기관에서 수신자의 공개키 및 비밀키를 생성하는 알고리즘 $KeyGen_R(1^{\lambda})$에 따라 임의의 랜덤값 $\beta \in Z_p^*$를 선택하여 수신자의 비밀키로 설정하고, 이로부터 수신자의 공개키를 산출한다. 산출된 수신자의 공개키 및 비밀키는 다음의 수학식 2와 같이 표현된다.

수학식 2

[0028] $$[pk_R = g^{\beta}, sk_R = \beta]$$

[0029] 이제 수학식 2와 같이 생성된 수신자의 공개키 및 비밀키는 수신자에게 제공되고, 그 중 수신자의 공개키는 대중에게 공개된다.

[0030] 도 1에서 송신자 S(10)는 수신자의 공개키를 이용하여 메시지를 암호화하고, 수신자의 공개키 외에 송신자의 비밀키를 이용하여 이러한 메시지에 대응하는 키워드를 암호화함으로써 암호문(15)을 생성한다. 이렇게 생성된 암호문(15)은 서버(30)에 전송된다. 전송된 암호문(15)은 서버(30)에 저장되어 수신자 R(20)로부터의 검색에 활용된다.

[0031] 한편, 수신자 R(20)은 키워드, 수신자의 비밀키 외에 송신자의 공개키를 이용하여 트랩도어(25)를 생성하고, 서버(30)에 질의한다. 그러면, 서버(30)는 수신된 트랩도어(25) 및 저장된 암호문(15) 내에 포함된 암호화된 키워드를 이용하여 테스트 함수(미도시)를 통해 검사를 수행한다. 검사 결과 트랩도어(25) 및 암호화된 키워드가 동일하다고 판단되면, 서버는 이에 대한 응답으로서 메시지 암호문(27)을 수신자(20)에게 출력한다.

[0032] 이상과 같은 아이디어에 기초하여 이하에서는 각각의 구성 요소들이 수행하는 동작을 보다 구체적으로 검토한다.

[0033] 도 2는 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법을 송신자를 중심으로 도시한 흐름도로서, 다음과 같은 단계들을 포함한다.

[0034] 210 단계에서 송신자는 수신자의 공개키를 이용하여 메시지를 암호화한다. 이 과정은 통상적인 공개키 암호화 시스템에서 메시지를 암호화하는 방법과 동일하므로 여기서는 구체적인 설명을 생략한다.

[0035] 220 단계에서 송신자는 수신자의 공개키 및 송신자의 비밀키를 이용하여 메시지에 대응하는 키워드를 암호화한다. 통상적인 키워드 암호화와는 달리 본 실시예에서는 암호화 과정 중에 송신자의 비밀키가 활용된다. 이러한 송신자의 비밀키는 송신자만이 알 수 있는 것으로 공격자에 의한 키워드 추측 공격을 원천적으로 차단하기 위한 기술적 수단으로서 사용되었다. 보다 구체적인 암호화 과정은 이후에 도 3을 통해 다시 설명한다.

[0036] 230 단계에서는 210 단계를 통해 암호화된 메시지 및 220 단계를 통해 암호화된 키워드로부터 암호문을 생성한다. 이러한 암호문은 210 단계를 통해 암호화된 메시지와 220 단계를 통해 생성된 적어도 하나 이상의 암호화 키워드를 결합함으로써 생성될 수 있다. 즉, 하나의 메시지에 대하여 복수 개의 키워드가 설정될 수 있으며, 이러한 키워드의 내용 및 개수는 검색을 용이하게 하기 위해 송신자의 판단에 따라 적절히 선택될 수 있다.

[0037] 240 단계에서 서버는 230 단계를 통해 생성된 암호문을 서버에 전송한다. 이렇게 전송된 암호문은 서버에 저장되어 수신자의 검색에 의해 제공될 수 있다.

[0038] 도 3은 도 2의 공개키 기반의 키워드 검색 방법에서 키워드를 암호화하는 방법을 보다 구체적으로 도시한 흐름도로서, 다음과 같은 단계들을 포함한다.

[0039] 221 단계에서 서버는 송신자로부터 송신자가 생성한 메시지에 대응하는 적어도 하나 이상의 키워드를 입력받는다. 특히, 이러한 키워드는 메시지를 검색하기 위해 수신자가 생성하는 트랩도어(trapdoor)에 대응하여 입력된 것으로, 메시지의 특징을 명확하게 나타내는 단어가 선택되는 것이 바람직하다.

[0040] 222 단계에서는 제 1 해시 함수를 이용하여 221 단계를 통해 입력된 키워드로부터 제 1 해시값을 산출한다. 이어서, 223 단계에서는 겹선형(bilinear) 함수를 이용하여 222 단계를 통해 산출된 제 1 해시값, 수신자의 공개키 및 송신자의 비밀키로부터 연산값을 산출한다. 제 1 해시 함수와 겹선형 함수는 앞서 도 1을 통해 정의된 바와 같으며, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 이상에서 정의된 함수들의 기본 원리가 동일 또는 유사하게 유지되는 한도 내에서 해당 함수들이 다양하게 정의되어 활용될 수 있음을 알 수 있다.

[0041] 공개키 암호 시스템에서 암호문에는 랜덤값이 포함되어야 하므로 송신자의 공개키 g^{α} 와 랜덤값 $\gamma \in Z_p^*$ 를 선택하여 키워드 암호문의 첫 번째 요소인 $C_1=(g^{\alpha})^{\gamma}$ 를 산출하고, 또한 이로부터 다음의 수학식 3을 연산한다.

수학식 3

[0042] $$t=e(g^{\alpha}\cdot H_1(W),(g^{\beta})^{\alpha})^{\gamma}$$

[0043] 여기서, e는 $e(g^x,g^y)=e(g,g)^{xy}$ 를 만족하는 겹선형 함수이고, H_1 및 H_2는 각각 암호학적 제 1 해시 함수 및 제 2 해시 함수를 나타낸다.

[0044] 224 단계에서는 제 2 해시 함수를 이용하여 223 단계를 통해 산출된 연산값으로부터 제 2 해시값을 산출한다. 즉, 수학식 3을 통해 키워드 암호문의 두 번째 요소인 $C_2=H_2(t)$ 를 산출한다.

[0045] 다음으로, 225 단계에서는 송신자의 비밀키 및 224 단계를 통해 산출된 제 2 해시값으로부터 암호화된 키워드를 생성한다. 따라서, 암호문은 첫 번째 요소인 송신자의 공개키 성분(보다 구체적으로는 송신자의 공개키를 랜덤값 γ 로써 지수승한 것을 의미한다.) 및 두 번째 요소인 제 2 해시값으로 구성된다. 생성된 암호문은 다음의 수학식 4와 같다.

수학식 4

[0046] $$C=[C_1,C_2]=[(g^{\alpha})^{\gamma},H_2(t)]$$

[0047] 도 4는 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법에서 송신자 및 서버의 수행 동작을 데이터를 중심으로 설명하기 위한 도면이다.

[0048] 송신자 S(10)는 암호문(15)을 생성하여 서버(30)에 전송한다. 암호문(15)은 도 4에 도시된 바와 같이 암호화된 메시지 $Enc_{pk_R}(msg)$ 과 W_1 부터 W_n 까지 n 개의 키워드에 대해 암호화된 값 $PEKS\text{-}RT(pk_R,sk_S,W)$ 을 결합한 형태를 예시하고 있다.

[0049] 한편, 도 4의 서버(30)에는 다양한 암호문(35)이 저장되어 있는 것을 볼 수 있다. 각각의 암호문(35)은 암호화된 메시지와 이에 대응하는 암호화된 키워드들의 집합으로 각각 사상되어 저장되며, 수신자에 의해 검색될 경우 암호화된 키워드들을 활용하여 해당하는 암호화된 메시지를 발견한 후, 이를 수신자에게 제공하게 된다.

[0050] 이하에서는 서버에서 암호문을 검색하는 방법을 설명하도록 한다.

[0051] 도 5는 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법을 서버를 중심으로 도시한 흐름도로서, 다음과 같은 단계들을 포함한다.

[0052] 510 단계에서 서버는 암호화된 메시지와 이에 대응하는 암호화된 키워드를 포함하는 암호문을 송신자로부터 수신하여 저장한다. 이 경우 암호문이 하나의 암호화된 메시지를 포함하고, 적어도 하나 이상의 암호화된 키워드를 포함하는 것은 당연하다. 또한, 서버에 저장되는 암호문은 메시지 및 키워드가 각각 암호화된 형태로 저장되며, 검색을 위해 복호화되지 않는다.

[0053] 520 단계에서 서버는 수신자의 비밀키, 송신자의 공개키 및 메시지를 검색하기 위한 키워드를 이용하여 생성된 트랩도어를 수신자로부터 수신한다. 이러한 키워드는 앞서 송신자가 설정한 키워드에 해당하는 것으로 트랩도어는 암호화된 키워드를 복호화 없이 검색하기 위해 마련된 기술적 수단이다. 이러한 트랩도어는 통상적인 공개키 기반의 암호화 시스템과는 달리 송신자의 공개키를 사용한다는 점에서 차별화된다. 이러한 공개키는 암호화된 키워드가 송신자의 비밀키로서 암호화되어 있으므로 테스트 함수를 통한 연산을 위해 필요한 구성 요소이다. 트랩도어에 관한 보다 구체적인 설명은 이후에 도 6을 통해 다시 설명하도록 한다.

[0054] 530 단계에서는 테스트 함수를 이용하여 510 단계를 통해 저장된 암호문에 포함된 암호화된 키워드와 520 단계를 통해 수신된 트랩도어의 일치 여부를 검사한다. 앞서 설명한 바와 같이 저장된 암호문은 송신자의 비밀키 및 수신자의 공개키를 사용하여 암호화되어 있고, 수신된 트랩도어는 송신자의 공개키 및 수신자의 비밀키를 사용하여 암호화되어 있다. 따라서, 테스트 함수를 통해 서버는 양자를 통해 연산 결과가 일치하는지 여부를 검사할 수 있다. 테스트 함수에 관한 보다 구체적인 설명은 이후에 도 7을 통해 다시 설명하도록 한다.

[0055] 540 단계에서 서버는 530 단계의 검사 결과에 따라 암호화된 키워드에 대응하는 암호화된 메시지를 수신자에게 선택적으로 출력한다. 보다 구체적으로, 암호화된 메시지를 선택적으로 출력하는 단계는 암호화된 키워드와 수신된 트랩도어가 일치하는 경우 참(true)의 응답 신호 및 상기 저장된 암호화된 메시지를 수신자에게 출력한다. 이에 반해, 암호화된 키워드와 수신된 트랩도어가 일치하지 않는 경우 거짓(false)의 응답 신호를 수신자에게 출력할 것이다.

[0056] 도 6은 도 5의 공개키 기반의 키워드 검색 방법에서 트랩도어를 생성하는 방법을 보다 구체적으로 도시한 흐름도로서, 다음과 같은 단계들을 포함한다.

[0057] 521 단계에서 수신자는 제 1 해시 함수를 이용하여 메시지를 검색하기 위한 키워드로부터 제 1 해시값을 산출한다. 특히, 제 1 해시 함수는 앞서 설명한 송신자가 키워드를 암호화하기 위해 사용한 함수와 동일한 함수이다.

[0058] 522 단계에서는 521 단계를 통해 산출된 제 1 해시값과 송신자의 공개키를 승산한다. 이어서, 523 단계에서는 522 단계를 통한 승산 결과를 수신자의 비밀키로 지수승함으로써 트랩도어를 생성한다. 이상의 일련의 과정에 따라 트랩도어 생성 함수 $Trapdoor(pk_S, sk_R, W)$ 는 송신자의 공개키 $pk_S = g^{\alpha}$, 수신자의 비밀키 $sk_R = \beta$ 및 키워드 W를 입력받은 후, 다음의 수학식 5와 같은 트랩도어를 산출한다.

수학식 5

[0059] $$T_W = (g^{\alpha} \cdot H_1(W))^{\beta}$$

[0060] 도 7은 도 5의 공개키 기반의 키워드 검색 방법에서 암호화된 키워드와 트랩도어의 일치 여부를 검사하는 방법을 보다 구체적으로 도시한 흐름도로서, 테스트 함수 $Test(C, T_W)$ 는 입력 파라메터로서 암호문

$C=[C_1, C_2]$와 트랩도어 T_W를 입력받는다. 이 경우, 테스트 함수는 $C_2=H_2(e(T_W, C_1))$의 등호가 성립할 경우 '참'의 결과값을 출력하고, 등호가 성립하지 않을 경우 '거짓'의 결과값을 출력한다.

[0061] 531 단계에서 서버는 암호화된 키워드로부터 송신자의 공개키 성분(앞서 도 3을 통해 설명한 암호문의 첫 번째 요소를 의미한다.) 및 상기 송신자의 해시값(앞서 도 3을 통해 설명한 암호문의 두 번째 요소로서 제 2 해시값을 의미한다.)을 추출한다.

[0062] 532 단계에서 서버는 겹선형 함수를 이용하여 531 단계를 통해 추출된 송신자의 공개키 성분 및 상기 수신된 트랩도어로부터 연산값을 산출한다. 다음으로, 533 단계에서 서버는 제 2 해시 함수를 이용하여 532 단계를 통해 산출된 연산값으로부터 제 2 해시값을 산출한다. 특히, 제 2 해시 함수는 송신자가 겹선형 함수의 연산값을 암호화하기 위해 사용한 함수와 동일한 함수이다. 이렇게 산출된 제 2 해시값은 다음의 수학식 6과 같다.

수학식 6

[0063] $$H_2(e(T_W, C_1))$$

[0064] 534 단계에서 서버는 531 단계를 통해 추출된 송신자의 해시값과 533 단계를 통해 산출된 제 2 해시값을 비교함으로써 암호화된 키워드와 수신된 트랩도어의 일치 여부를 검사한다. 키워드 암호문의 두 번째 성분 C_2는 $C_2=H_2(t)$이므로 상기 산출된 제 2 해시값과 C_2이 일치한다면 제 2 해시 함수의 입력값인 $e(T_W, C_1)$와 t가 서로 일치한다는 것을 의미하므로, 결국 트랩도어의 키워드의 암호문의 키워드가 동일함을 의미한다.

[0065] 저장된 키워드 암호문 $C=[C_1, C_2]$와 수신자로부터 요청된 트랩도어 $T_W=(g^{\alpha}\cdot H_1(W))^{\beta}$에 대한 검증은 다음과 같은 수학식 7을 통해 확인할 수 있다.

수학식 7

[0066] $$t=e(g^{\alpha}\cdot H_1(W),(g^{\beta})^{\alpha})^{\gamma}=e(g^{\alpha}\cdot H_1(W),g^{\alpha})^{\gamma\beta}=e((g^{\alpha}\cdot H_1(W))^{\beta},(g^{\alpha})^{\gamma})=e(T_W, C_1)$$

[0067] 도 8은 본 발명의 일 실시예에 따른 공개키 기반의 키워드 검색 방법에서 수신자와 서버의 수행 동작을 데이터를 중심으로 설명하기 위한 도면이다.

[0068] 우선, 서버(30)는 송신자(미도시)로부터 암호문(35)을 수신하여 저장한다. 이 때, 암호문은 암호화된 메시지와 이에 대응하는 적어도 하나 이상의 암호화된 키워드를 포함한다. 각각의 암호화된 메시지와 암호화된 키워드는 검색을 용이하도록 하기 위해 연관된 데이터별로 사상되어 저장된다.

[0069] 이제 수신자 R(20)은 트랩도어(25)를 생성하여 서버(30)에게 전송한다. 트랩도어(25)는 키워드, 송신자의 비밀키 및 수신자의 공개키를 이용하여 생성되므로 저장된 암호문(35)과 테스트 함수(37)를 통해 일치 여부를 비교할 수 있다. 만약 테스트 함수(37)를 통해 '참'의 결과가 산출되었다면 서버(30)는 수신자(20)에게 검색된 키워드에 대응하는 암호화된 메시지 $Enc_{pk_R}(msg)$ (27)를 출력한다. 이 때도 역시 메시지는 암호화된 채로 수신자(20)에게 제공된다. 그러면, 수신자(20)는 자신의 비밀키를 이용하여 해당 메시지를 복호화

함으로써 최종적인 평문을 얻을 수 있다.

[0070] 상기된 본 발명의 실시예들에 따르면 키워드를 암호화함에 있어서 송신자의 비밀키를 이용함으로써 공개키 기반의 키워드 검색 시스템에서 공격자의 키워드 추측 공격을 원천적으로 차단하고, 비록 공격자가 불법적으로 정당한 트랩도어를 획득하더라도 이에 대응하는 키워드 암호문을 생성할 수 없으므로 안전성을 보장할 수 있다. 따라서, 공격자가 키워드를 통해 테스트를 할 수 있는 능력이 제한됨으로써 서버를 지정하지 않아도 키워드 추측 공격에 강인한 암호 시스템을 제공할 수 있다.

[0071] 한편, 본 발명의 다른 실시예에서 서버는 암호문을 저장함에 있어서 송신자를 기준으로 수신된 암호문을 분류하여 저장할 수 있다. 이 경우, 수신자는 송신자에 대한 제한 정보가 부가된 트랩도어를 생성하여 서버에 질의함으로써 검색 대상을 한정할 수 있다. 그 결과, 서버는 부가된 제한 정보에 따라 분류되어 저장된 암호문을 검색할 수 있다. 즉, 검색의 측면에서 볼 때, 트랩도어를 생성할 때 송신자의 공개키를 사용하기 때문에 수신자는 특정 송신자를 지정하여 검색할 수 있다. 만일, 송신자의 정보가 알려져 있거나 송신자별로 메시지가 분류되어 있다면, 수신자가 트랩도어를 생성할 경우 검색하고자 하는 송신자의 범위를 제한하여 서버에 전송함으로써 서버의 검색 범위를 좁힐 수 있고, 이를 통해 수신자는 키워드 질의에 관한 테스트 단계에서의 연산량을 감소시킬 수 있다.

[0072] 나아가, 본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0073] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0074] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0075] 10 : 송신자 15 : 암호문

20 : 수신자

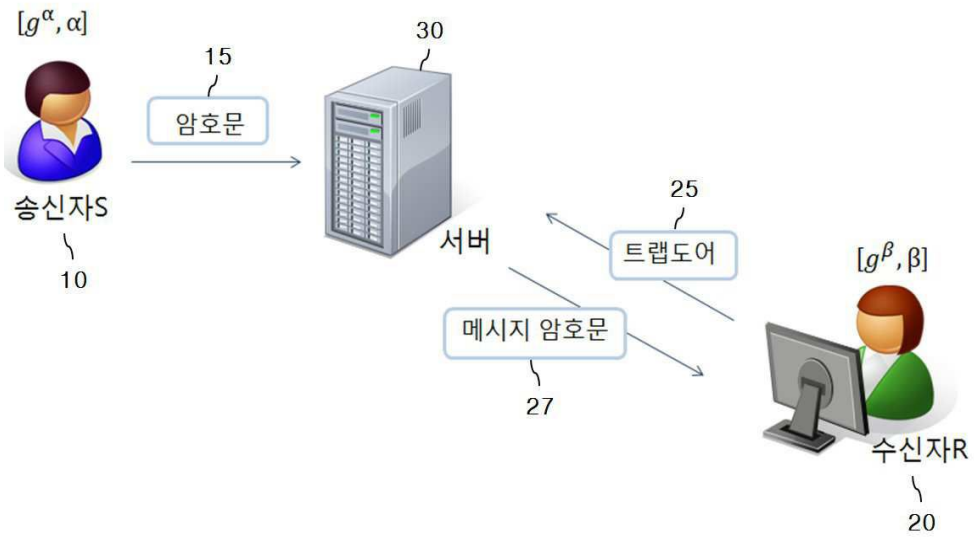
25 : 트랩도어 27 : 메시지 암호문

30 : 서버

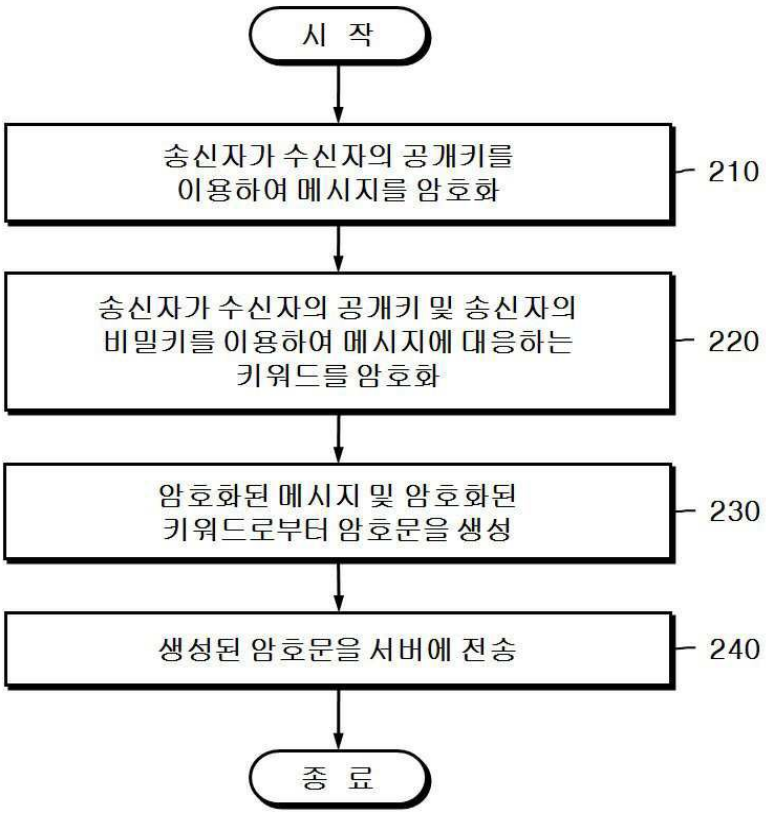
35 : 저장된 암호문 37 : 테스트 함수

도면

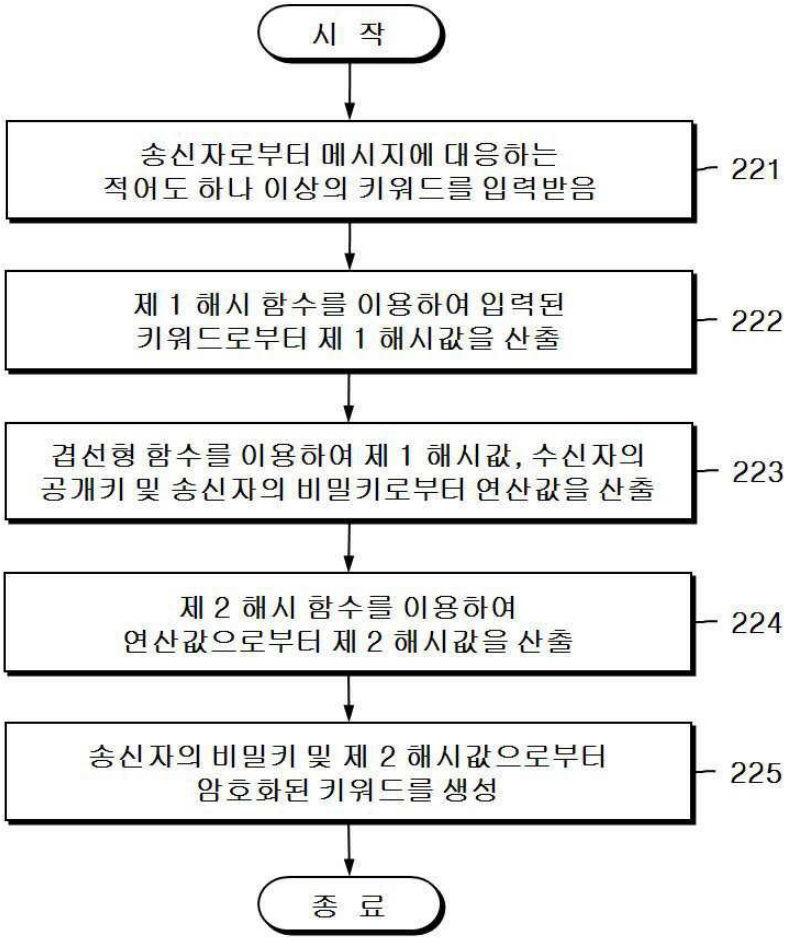
도면1


$[g^{\alpha}, \alpha]$
15
암호문
30
송신자S
10
서버
25
트랩도어
$[g^{\beta}, \beta]$
메시지 암호문
27
수신자R
20

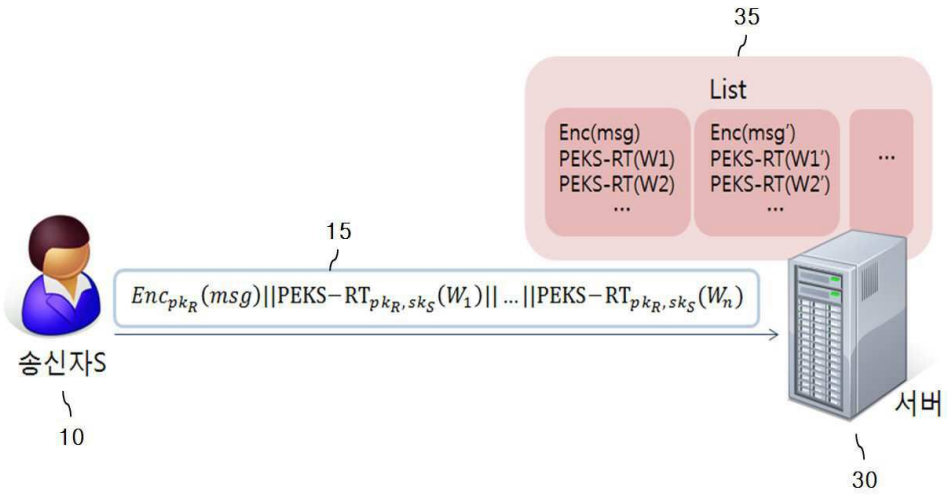
도면2


시 작
송신자가 수신자의 공개키를 이용하여 메시지를 암호화
210
송신자가 수신자의 공개키 및 송신자의 비밀키를 이용하여 메시지에 대응하는 키워드를 암호화
220
암호화된 메시지 및 암호화된 키워드로부터 암호문을 생성
230
생성된 암호문을 서버에 전송
240
종 료

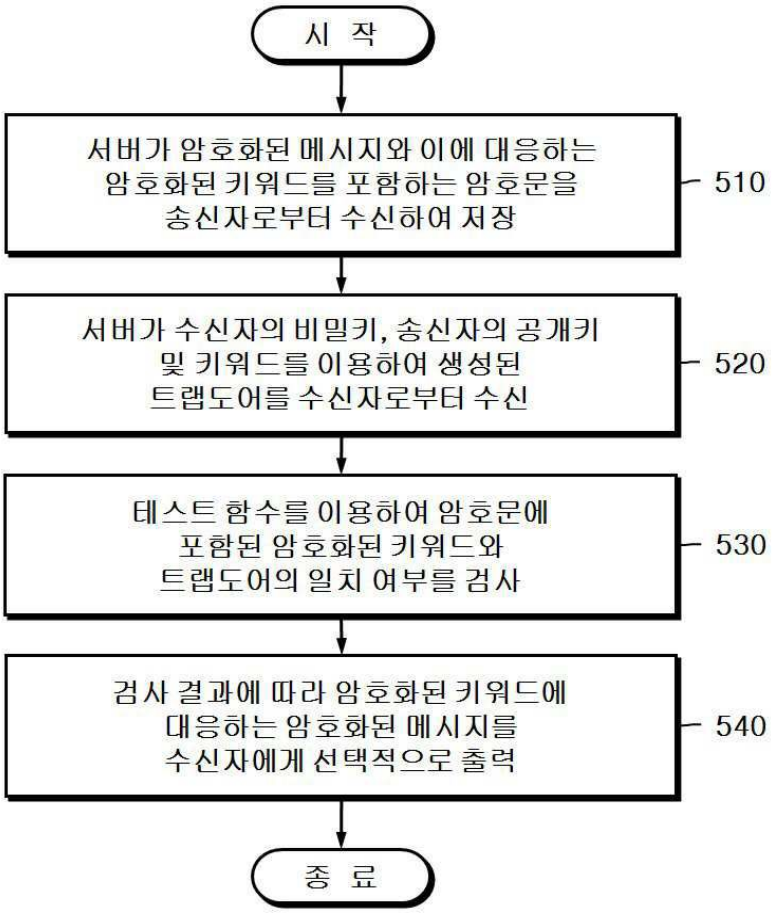
도면3


시 작
송신자로부터 메시지에 대응하는
적어도 하나 이상의 키워드를 입력받음
221
제 1 해시 함수를 이용하여 입력된
키워드로부터 제 1 해시값을 산출
222
겹선형 함수를 이용하여 제 1 해시값, 수신자의
공개키 및 송신자의 비밀키로부터 연산값을 산출
223
제 2 해시 함수를 이용하여
연산값으로부터 제 2 해시값을 산출
224
송신자의 비밀키 및 제 2 해시값으로부터
암호화된 키워드를 생성
225
종 료

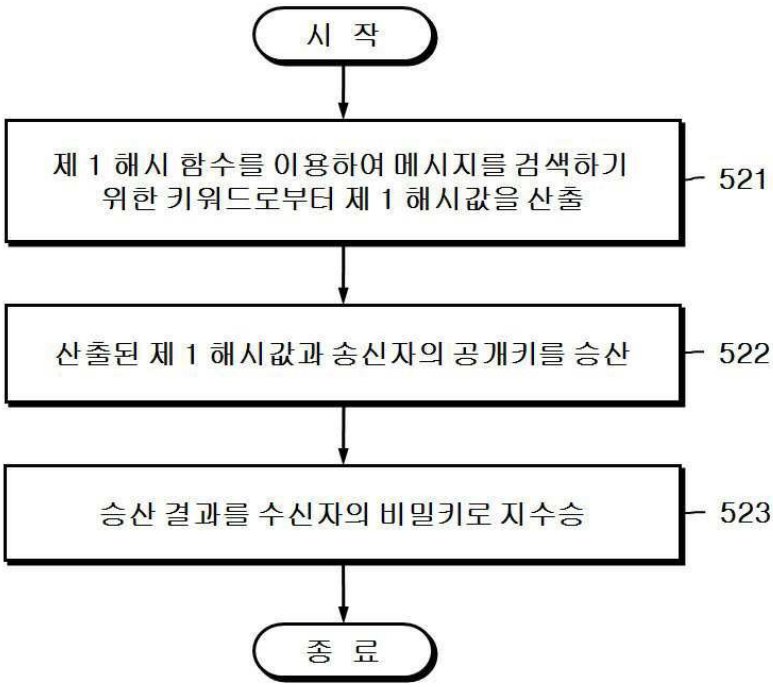
도면4


35
List
Enc(msg)
PEKS-RT(W1)
PEKS-RT(W2)
...
Enc(msg')
PEKS-RT(W1')
PEKS-RT(W2')
...
...
15
$Enc_{pk_R}(msg)||\text{PEKS}-\text{RT}_{pk_R,sk_S}(W_1)||\ldots||\text{PEKS}-\text{RT}_{pk_R,sk_S}(W_n)$
송신자S
10
서버
30

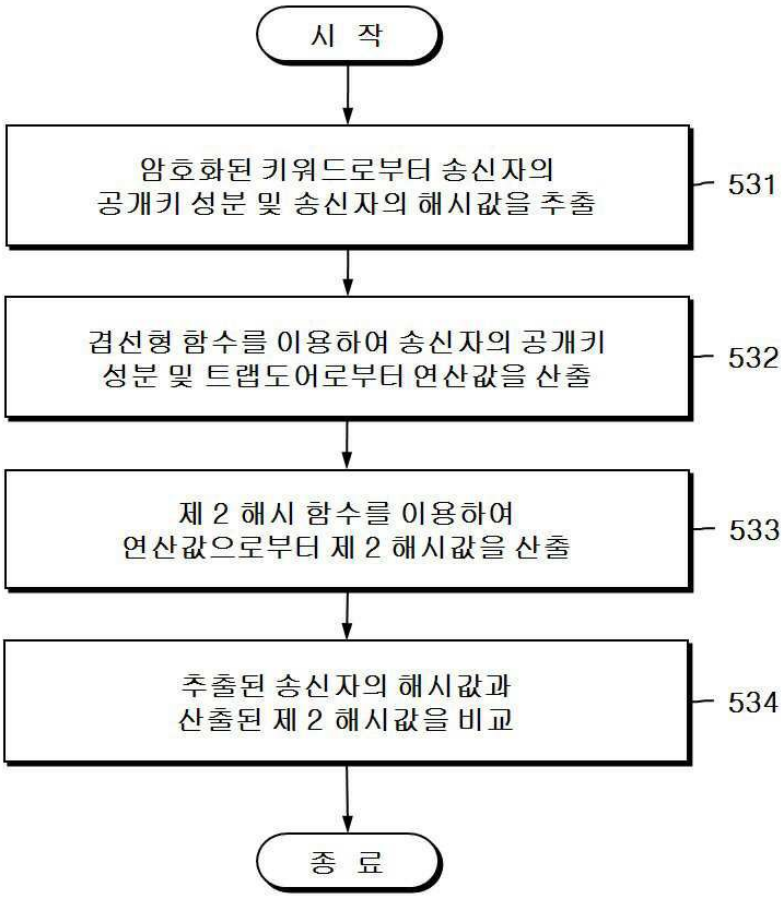
도면5


시 작
서버가 암호화된 메시지와 이에 대응하는 암호화된 키워드를 포함하는 암호문을 송신자로부터 수신하여 저장
510
서버가 수신자의 비밀키, 송신자의 공개키 및 키워드를 이용하여 생성된 트랩도어를 수신자로부터 수신
520
테스트 함수를 이용하여 암호문에 포함된 암호화된 키워드와 트랩도어의 일치 여부를 검사
530
검사 결과에 따라 암호화된 키워드에 대응하는 암호화된 메시지를 수신자에게 선택적으로 출력
540
종 료

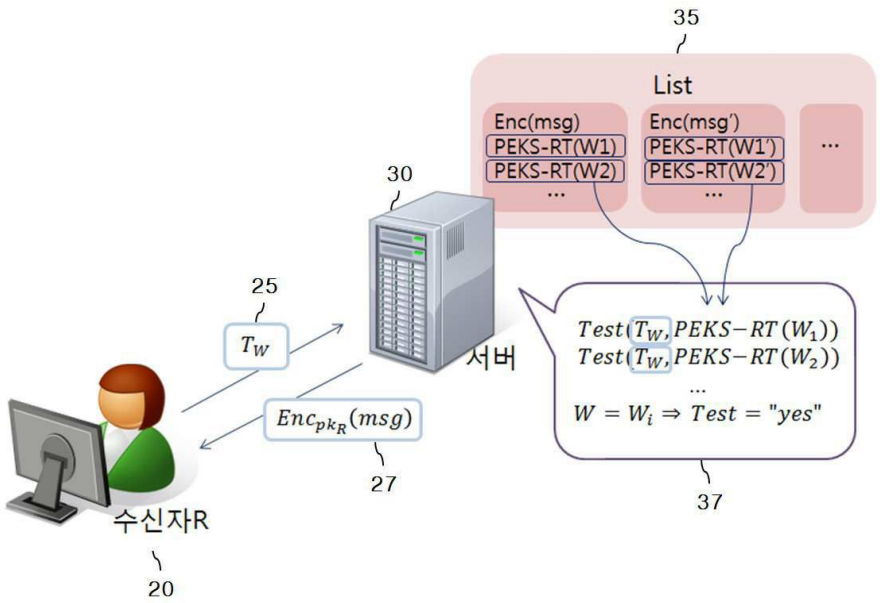
도면6


시 작
제 1 해시 함수를 이용하여 메시지를 검색하기 위한 키워드로부터 제 1 해시값을 산출
521
산출된 제 1 해시값과 송신자의 공개키를 승산
522
승산 결과를 수신자의 비밀키로 지수승
523
종 료

도면7


시 작
암호화된 키워드로부터 송신자의 공개키 성분 및 송신자의 해시값을 추출
531
겹선형 함수를 이용하여 송신자의 공개키 성분 및 트랩도어로부터 연산값을 산출
532
제 2 해시 함수를 이용하여 연산값으로부터 제 2 해시값을 산출
533
추출된 송신자의 해시값과 산출된 제 2 해시값을 비교
534
종 료

도면8


35
List
Enc(msg)
PEKS-RT(W1)
PEKS-RT(W2)
Enc(msg')
PEKS-RT(W1')
PEKS-RT(W2')
30
서버
25
T_W
$Enc_{pk_R}(msg)$
27
$Test(T_W, PEKS-RT(W_1))$
$Test(T_W, PEKS-RT(W_2))$
$W = W_i \Rightarrow Test = "yes"$
37
수신자R
20