(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년11월11일
(11) 등록번호 10-1460541
(24) 등록일자 2014년11월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01)
(21) 출원번호 10-2013-0082745
(22) 출원일자 2013년07월15일
심사청구일자 2013년07월15일
(56) 선행기술조사문헌
JP2011237475 A*
JP2009141674 A
JP2010113181 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)
박종환
서울특별시 성북구 정릉로 292 (정릉동,현대홈타운아파트) 106동 801호
구우권
서울 서초구 신반포로33길 15, 108동 1201호 (잠원동, 동아아파트)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 9 항 심사관 : 홍기완

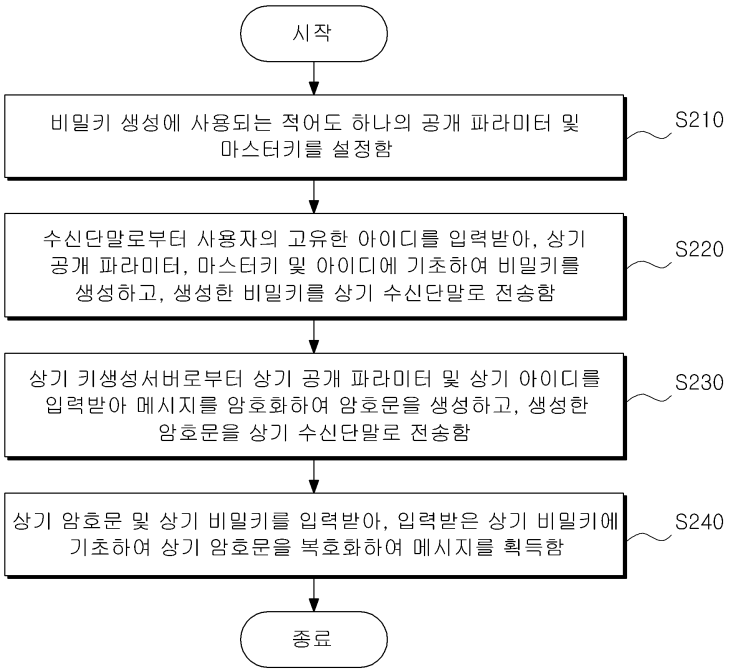
(54) 발명의 명칭 **사용자 아이디 기반 공개키 암호화 방법**

(57) 요 약

본 발명은 사용자 아이디 기반 공개키 암호화 방법에 관한 것으로, 보다 구체적으로는 키생성서버가 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정하는 단계; 상기 키생성서버가 수신단말로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생

(뒷면에 계속)

대 표 도 - 도2



성한 비밀키를 상기 수신단말로 전송하는 단계; 송신단말이 상기 키생성서버로부터 상기 공개 파라미터 및 상기 아이디를 입력받아 메시지를 암호화하여 암호문을 생성하고, 생성한 암호문을 상기 수신단말로 전송하는 단계; 및 상기 수신단말이 상기 암호문 및 상기 비밀키를 입력받아, 입력받은 상기 비밀키에 기초하여 상기 암호문을 복호화하여 메시지를 획득하는 단계;를 포함한다.

이러한 구성에 의해, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 사용자의 고유한 아이디를 공개키로 사용하여, 제3의 신뢰기관을 통한 공개키를 인증하는 절차가 생략됨으로써, 통신을 효율적으로 수행할 수 있도록 하는 효과가 있다.

이 발명을 지원한 국가연구개발사업

과제고유번호	20120008697
부처명	교육과학기술부
연구관리전문기관	한국연구재단
연구사업명	중견연구자지원_도약연구(전략)
연구과제명	속성 기반 공개키 시스템에 관한 연구
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2012.09.01 ~ 2015.08.31

특허청구의 범위

청구항 1

키생성서버가 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정하는 단계;

상기 키생성서버가 수신단말로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계;

송신단말이 상기 키생성서버로부터 상기 공개 파라미터 및 상기 아이디를 입력받아 메시지를 암호화하여 암호문을 생성하고, 생성한 암호문을 상기 수신단말로 전송하는 단계; 및

상기 수신단말이 상기 암호문 및 상기 비밀키를 입력받아, 입력받은 상기 비밀키에 기초하여 상기 암호문을 복호화하여 메시지를 획득하는 단계;

를 포함하되,

상기 키생성서버가 공개 파라미터 및 마스터키를 설정하는 단계는

외부로부터 보안상수를 입력받아, 상기 보안상수를 입력값으로 하는 타원 곡선군에 속하는 생성원 중 임의의 제1 생성원 및 제2 생성원을 선택하고, 상기 타원 곡선군에 속하는 원소 중 임의의 원소를 선택하는 과정;

임의의 난수를 선택하여 마스터키로 설정하는 과정;

상기 제1 생성원, 제2 생성원 및 상기 마스터키를 겹선형 함수에 적용하여 함수값을 연산하는 과정; 및

상기 제1 생성원, 제2 생성원, 상기 임의의 원소 및 상기 겹선형 함수의 함수값 중 적어도 하나를 포함하는 공개 파라미터를 설정하는 과정;

을 포함하는 것을 특징으로 하는 사용자 아이디 기반 공개키 암호화 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 키생성서버가 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계는

임의의 제1 난수를 선택하는 과정;

상기 제2 생성원, 마스터키, 임의의 원소 및 제1 난수에 기초하여 제1 비밀키를 생성하는 과정;

상기 제1 생성원 및 제1 난수에 기초하여 제2 비밀키를 생성하는 과정;

상기 제1 비밀키 및 제2 비밀키를 해쉬연산하여 제1 태그값을 생성하는 과정;

상기 아이디를 해쉬연산한 값, 임의의 원소, 제1 태그값 및 제1 난수에 기초하여 제3 비밀키를 생성하는 과정; 및

상기 제1 비밀키, 제2 비밀키 및 제3 비밀키를 포함하는 비밀키를 생성하여 상기 수신단말로 전송하는 과정;

을 포함하는 것을 특징으로 하는 사용자 아이디 기반 공개키 암호화 방법.

청구항 4

제3항에 있어서,

상기 송신단말이 메시지를 암호화하여 암호문을 생성하는 단계는

임의의 제2 난수를 선택하는 과정;

상기 겹선형 함수의 함수값, 제2 난수 및 메시지에 기초하여 제1 암호문을 생성하는 과정;

상기 제1 생성원 및 상기 제2 난수에 기초하여 제2 암호문을 생성하는 과정;

상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 생성하는 과정;

상기 아이디를 해쉬한 값, 임의의 원소, 제2 태그값 및 제2 난수에 기초하여 제3 암호문을 생성하는 과정; 및

상기 제1 암호문, 제2 암호문 및 제3 암호문을 포함하는 암호문을 생성하여 상기 수신단말로 전송하는 과정;

을 포함하는 것을 특징으로 하는 사용자 아이디 기반 공개키 암호화 방법.

청구항 5

제4항에 있어서,

상기 수신단말이 암호문을 복호화하여 메시지를 획득하는 단계는

상기 키생성서버로부터 수신한 비밀키 중 상기 제1 비밀키 및 제2 비밀키를 해쉬연산하여 제1 태그값을 연산하는 과정;

상기 송신단말로부터 수신한 암호문 중 상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 연산하는 과정;

상기 제1 태그값과 제2 태그값이 동일한지 여부를 판단하는 과정;

상기 제2 암호문과 아이디를 해쉬한 값, 상기 임의의 원소, 앞서 연산한 제2 태그값을 겹선형 함수에 적용한 함수값이 상기 제1 생성원과 상기 제3 암호문 겹선형 함수에 적용한 함수값과 서로 동일한지 여부를 판단하는 과정;

상기 제2 암호문과 제1 비밀키를 겹선형 함수에 적용한 함수값과, 제2 암호문과 제3 비밀키를 겹선형 함수에 적용한 함수값, 제2 비밀키와 제3 암호문을 겹선형 함수에 적용한 함수값, 제1 태그값 및 제2 태그값에 기초하여 복호화 변수를 연산하는 과정; 및

상기 제1 암호문을 상기 복호화 변수로 나누어 메시지를 획득하는 과정;

을 포함하는 것을 사용자 아이디 기반 공개키 암호화 방법.

청구항 6

키생성서버가 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정하는 단계;

상기 키생성서버가 수신단말로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계;

송신단말이 상기 공개 파라미터에 기초하여 세션키를 생성하고, 생성된 세션키에 기초하여 메시지를 암호화한 후, 암호문을 생성하는 단계; 및

수신단말이 생성된 암호문을 입력받고, 세션키를 연산한 후, 생성한 세션키에 기초하여 상기 암호문을 복호화하여 메시지를 획득하는 단계;

를 포함하되,

상기 키생성서버가 공개 파라미터 및 마스터키를 설정하는 단계는

외부로부터 보안상수를 입력받아, 상기 보안상수를 입력값으로 하는 타원 곡선군에 속하는 생성원 중 임의의 제1 생성원 및 제2 생성원을 선택하고, 상기 타원 곡선군에 속하는 원소 중 임의의 원소를 선택하는 과정;

임의의 난수를 선택하여 마스터키로 설정하는 과정;

상기 제1 생성원, 제2 생성원 및 상기 마스터키를 겹선형 함수에 적용하여 함수값을 연산하는 과정; 및

상기 제1 생성원, 제2 생성원, 상기 임의의 원소 및 상기 겹선형 함수의 함수값 중 적어도 하나를 포함하는 공개 파라미터를 설정하는 과정;

을 포함하는 것을 특징으로 하는 사용자 아이디 기반 공개키 암호화 방법.

청구항 7

삭제

청구항 8

제6항에 있어서,

상기 키생성서버가 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계는

임의의 제1 난수를 선택하는 과정;

상기 제2 생성원, 마스터키, 임의의 원소 및 제1 난수에 기초하여 제1 비밀키를 생성하는 과정;

상기 제1 생성원 및 제1 난수에 기초하여 제2 비밀키를 생성하는 과정;

상기 제1 비밀키 및 제2 비밀키를 해쉬하여 제1 태그값을 생성하는 과정;

상기 아이디를 해쉬한 값, 임의의 원소, 제1 태그값 및 제1 난수에 기초하여 제3 비밀키를 생성하는 과정; 및

상기 제1 비밀키, 제2 비밀키 및 제3 비밀키를 포함하는 비밀키를 생성하여 상기 수신단말로 전송하는 과정;

을 포함하는 것을 특징으로 하는 사용자 아이디 기반 공개키 암호화 방법.

청구항 9

제8항에 있어서,

상기 송신단말이 세션키에 기초하여 암호문을 생성하는 단계는

임의의 제2 난수를 선택하는 과정;

상기 겹선형 함수의 함수값 및 제2 난수에 기초하여 세션키를 생성하는 과정;

상기 세션키 및 메시지를 대칭키 알고리즘에 적용하여 제 4 암호문을 생성하는 과정;

상기 제 4 암호문, 제1 생성원 및 제2 난수에 기초하여 제2 태그값을 생성하는 과정; 및

상기 제1 생성원, 상기 제2 난수와, 상기 아이디를 해쉬연산한 값, 상기 임의의 원소, 제2 태그값에 기초하여 암호문을 생성하는 과정;

을 포함하는 것을 특징으로 하는 사용자 아이디 기반 공개키 암호화 방법.

청구항 10

제9항에 있어서,

상기 수신단말이 상기 세션키에 기초하여 암호문을 복호화하여 메시지를 획득하는 단계는

상기 키생성서버로부터 수신한 비밀키 중 상기 제1 비밀키 및 제2 비밀키를 해쉬연산하여 제1 태그값을 연산하는 과정;

상기 송신단말이 수신한 암호문 중 상기 제4 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 연산하는

과정;

상기 제1 태그값과 제2 태그값이 동일한지 여부를 판단하는 과정;

상기 제2 암호문과 제1 비밀키를 겹선형 함수에 적용한 함수값과, 제2 암호문과 제3 비밀키를 겹선형 함수에 적용한 함수값, 제2 비밀키와 제3 암호문을 겹선형 함수에 적용한 함수값, 제1 태그값 및 제2 태그값에 기초하여 복호화 변수를 연산하는 과정;

상기 복호화 변수를 대칭키 암호알고리즘에 적용하여 세션키를 획득하는 과정; 및

상기 세션키 및 제4 암호문을 대칭키 알고리즘에 적용하여 메시지를 획득하는 과정;

을 포함하는 것을 사용자 아이디 기반 공개키 암호화 방법.

청구항 11

제1항 및 제3항 내지 제6항 및 제8항 내지 제10항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 사용자 아이디 기반 공개키 암호화 방법에 관한 것으로, 특히 사용자의 고유한 아이디를 이용하여 내용 확인이 가능한 공개키를 사용하여 용이하게 통신을 수행하도록 하는 사용자 아이디 기반 공개키 암호화 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 사용되는 공개키 시스템 기술은 비밀통신을 수행하고자 하는 각각의 사용자 단말이 자신의 비밀키와 공개키를 쌍으로 생성하고, 비밀통신을 수행하고자 하는 상대방 단말은 정당한 공개키를 획득해야만 통신이 이루어지도록 구성된다. 이때, 통신을 수행하고자 하는 상대방 단말의 공개키를 획득한 사용자는 자신이 획득한 공개키가 정당한지 여부를 입증하기 위해, 제3의 신뢰기관으로 획득한 공개키에 대한 서명을 받아 이를 공개키의 인증서로 사용한다.

[0003] 이러한 공개키 인증서는 공개키와 그 소유자의 신원에 대한 정당성을 연결해주므로, 사용자 단말은 이러한 공개키 인증서를 통해 상대방 단말로부터 획득한 공개키에 대한 신뢰를 하게 되어, 상대방 단말과의 통신을 원활히 수행한다.

[0004] 하지만 이와 같은 인증서 기반의 공개키 시스템은 공개키 인증서의 폐기 시, 인증서 폐기 목록을 일정 기간 동안 유지하거나, 지속적으로 관리해야 함에 따라, 관리에 따른 비용 및 시간 소모가 발생하는 문제점이 발생했다.

발명의 내용

해결하려는 과제

[0005] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 사용자의 고유한 아이디를 이용하여 공개키를 암호화하여, 제3의 신뢰기관을 통한 별도의 공개키 인증절차를 수행하지 않고도 사용자단말간 비밀통신을 용이하게 수행할 수 있는 사용자 아이디 기반 공개키 암호화 방법을 제공하고자 한다.

과제의 해결 수단

[0006] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법은 키생성서버가 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정하는 단계; 상기 키생성서버가 수신단말로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계; 송신단말이 상기 공개 파라미터 및 상기 아이디를 입력받아 메시지를 암호화하여 암호문을 생성하고, 생성한 암호문을 상기 수신단말로 전송하는 단계; 및 상기 수신단말이 상기 암호문 및 상기 비밀키를 입력받아, 입력받은 상기 비밀키에 기초하여 상기 암호문을 복호화하여 메시지를 획득하는 단계; 를 포함한다.

[0007] 보다 바람직하게는 외부로부터 보안상수를 입력받아, 상기 보안상수를 입력값으로 하는 타원 곡선군에 속하는 생성원 중 임의의 제1 생성원 및 제2 생성원을 선택하고, 상기 타원 곡선군에 속하는 원소 중 임의의 원소를 선택하는 과정; 임의의 난수를 선택하여 마스터키로 설정하는 과정; 상기 제1 생성원, 제2 생성원 및 상기 마스터키를 겹선형 함수에 적용하여 함수값을 연산하는 과정; 및 상기 제1 생성원, 제2 생성원, 상기 임의의 원소 및 상기 겹선형 함수의 함수값 중 적어도 하나를 포함하는 공개 파라미터를 설정하는 과정; 을 포함하는 키생성서버가 공개 파라미터 및 마스터키를 설정하는 단계를 포함할 수 있다.

[0008] 보다 바람직하게는 임의의 제1 난수를 선택하는 과정; 상기 제2 생성원, 마스터키, 임의의 원소 및 제1 난수에 기초하여 제1 비밀키를 생성하는 과정; 상기 제1 생성원 및 제1 난수에 기초하여 제2 비밀키를 생성하는 과정; 상기 제1 비밀키 및 제2 비밀키를 해쉬하여 제1 태그값을 생성하는 과정; 상기 아이디를 해쉬한 값, 임의의 원소, 제1 태그값 및 제1 난수에 기초하여 제3 비밀키를 생성하는 과정; 및 상기 제1 비밀키, 제2 비밀키 및 제3 비밀키를 포함하는 비밀키를 생성하여 상기 수신단말로 전송하는 과정;을 포함하는 키생성서버가 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계를 포함할 수 있다.

[0009] 보다 바람직하게는 임의의 제2 난수를 선택하는 과정; 상기 겹선형 함수의 함수값, 제2 난수, 메시지에 기초하여 제1 암호문을 생성하는 과정; 상기 제1 생성원 및 상기 제2 난수에 기초하여 제2 암호문을 생성하는 과정; 상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 생성하는 과정; 상기 아이디를 해쉬한 값, 임의의 원소, 제2 태그값 및 제2 난수에 기초하여 제3 암호문을 생성하는 과정; 및 상기 제1 암호문, 제2 암호문 및 제3 암호문을 포함하는 암호문을 생성하여 상기 수신단말로 전송하는 과정;을 포함하는 송신단말이 메시지를 암호화하여 암호문을 생성하는 단계를 포함할 수 있다.

[0010] 보다 바람직하게는 상기 키생성서버로부터 수신한 비밀키 중 상기 제1 비밀키 및 제2 비밀키를 해쉬연산하여 제1 태그값을 연산하는 과정; 상기 송신단말로부터 수신한 암호문 중 상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 연산하는 과정; 상기 제1 태그값과 제2 태그값이 동일한지 여부를 판단하는 과정; 상기 제2 암호문과 아이디를 해쉬한 값, 상기 임의의 원소, 앞서 연산한 제2 태그값을 겹선형 함수에 적용한 함수값이 상기 제1 생성원과 상기 제3 암호문 겹선형 함수에 적용한 함수값과 서로 동일한지 여부를 판단하는 과정; 상기 제2 암호문과 제1 비밀키를 겹선형 함수에 적용한 함수값과, 제2 암호문과 제3 비밀키를 겹선형 함수에 적용한 함수값, 제2 비밀키와 제3 암호문을 겹선형 함수에 적용한 함수값, 제1 태그값 및 제2 태그값에 기초하여 복호화 변수를 연산하는 과정; 및 상기 제1 암호문을 상기 복호화 변수로 나누어 메시지를 획득하는 과정; 을 포함하는 수신단말이 암호문을 복호화하여 메시지를 획득하는 단계를 포함할 수 있다.

[0011] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법은 키생성서버가 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정하는 단계; 상기 키생성서버가 수신단말로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계; 상기 송신단말이 상기 공개 파라미터에 기초하여 세션키를 생성하고, 생성된 세션키에 기초하여 메시지를 암호화한 후, 암호문을 생성하는 단계; 및 수신단말이 생성된 암호문을 입력받고, 세션키를 연산한 후, 생성한 세션키에 기초하여 상기 암호문을 복호화하여 메시지를 획득하는 단계;를 포함한다.

[0012] 보다 바람직하게는 외부로부터 보안상수를 입력받아, 상기 보안상수를 입력값으로 하는 타원 곡선군에 속하는 생성원 중 임의의 제1 생성원 및 제2 생성원을 선택하고, 상기 타원 곡선군에 속하는 원소 중 임의의 원소를 선택하는 과정; 임의의 난수를 선택하여 마스터키로 설정하는 과정; 상기 제1 생성원, 제2 생성원 및 상기 마스터키를 겹선형 함수에 적용하여 함수값을 연산하는 과정; 및 상기 제1 생성원, 제2 생성원, 상기 임의의 원소 및 상기 겹선형 함수의 함수값 중 적어도 하나를 포함하는 공개 파라미터를 설정하는 과정; 을 포함하는 키생성서

버가 공개 파라미터 및 마스터키를 설정하는 단계를 포함할 수 있다.

[0013] 보다 바람직하게는 임의의 제1 난수를 선택하는 과정; 상기 제2 생성원, 마스터키, 임의의 원소 및 제1 난수에 기초하여 제1 비밀키를 생성하는 과정; 상기 제1 생성원 및 제1 난수에 기초하여 제2 비밀키를 생성하는 과정; 상기 제1 비밀키 및 제2 비밀키를 해쉬하여 제1 태그값을 생성하는 과정; 상기 아이디를 해쉬한 값, 임의의 원소, 제1 태그값 및 제1 난수에 기초하여 제3 비밀키를 생성하는 과정; 및상기 제1 비밀키, 제2 비밀키 및 제3 비밀키를 포함하는 비밀키를 생성하여 상기 수신단말로 전송하는 과정;을 포함하는 키생성서버가 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송하는 단계를 포함할 수 있다.

[0014] 보다 바람직하게는 임의의 제2 난수를 선택하는 과정; 상기 겹선형 함수의 함수값 및 제2 난수에 기초하여 세션키를 생성하는 과정; 상기 세션키 및 메시지를 대칭키 알고리즘에 적용하여 제 4 암호문을 생성하는 과정; 상기 제 4 암호문, 제1 생성원 및 제2 난수에 기초하여 제2 태그값을 생성하는 과정; 및 상기 제1 생성원, 상기 제2 난수와, 상기 아이디를 해쉬연산한 값, 상기 임의의 원소, 제2 태그값에 기초하여 암호문을 생성하는 과정;을 포함하는 송신단말이 세션키에 기초하여 암호문을 생성하는 단계를 포함할 수 있다.

[0015] 보다 바람직하게는 상기 송신단말이 수신한 암호문 중 상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 연산하는 과정; 상기 제1 태그값과 제2 태그값이 동일한지 여부를 판단하는 과정; 상기 제2 암호문과 제1 비밀키를 겹선형 함수에 적용한 함수값과, 제2 암호문과 제3 비밀키를 겹선형 함수에 적용한 함수값, 제2 비밀키와 제3 암호문을 겹선형 함수에 적용한 함수값, 제1 태그값 및 제2 태그값에 기초하여 복호화 변수를 연산하는 과정; 상기 복호화 변수를 대칭키 암호알고리즘에 적용하여 세션키를 획득하는 과정; 및 상기 세션키 및 제 4 암호문을 대칭키 알고리즘에 적용하여 메시지를 획득하는 과정; 을 포함하는 수신단말이 상기 세션키에 기초하여 암호문을 복호화하여 메시지를 획득하는 단계를 포함할 수 있다.

발명의 효과

[0016] 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 사용자의 고유한 아이디를 공개키로 사용하여, 제3의 신뢰기관을 통한 공개키를 인증하는 절차가 생략됨으로써, 통신을 효율적으로 수행할 수 있도록 하는 효과가 있다.

[0017] 또한, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 제3의 신뢰기관을 통한 공개키에 대한 인증서를 사용하지 않으므로, 인증서 폐기 목록을 지속적으로 유지하거나, 관리하는 비용 및 시간을 감소시킬 수 있는 효과가 있다.

[0018] 더불어, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 사용자의 아이디를 공개키로 사용하므로, 공개키 확인을 통해 통신을 수행하고자 하는 사용자의 신원을 용이하게 파악할 수 있는 효과가 있다.

[0019] 이와 더불어, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 복잡한 형태의 공개키 기반 구조 (PKI, Public Key Infrastructure)를 구축할 필요가 없어, 공개키 구조를 구축하는데 소요되는 시간 및 비용을 감소시킬 수 있는 효과가 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 일 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법을 구현하는 시스템의 블록도이다.

도 2는 본 발명의 다른 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법의 순서도이다.

도 3은 도 2의 공개 파라미터 및 마스터키를 설정하는 단계의 세부과정을 나타낸 순서도이다.

도 4는 도 2의 비밀키 생성단계의 세부 과정을 나타낸 순서도이다.

도 5는 도 2의 메시지에 대한 암호문 생성단계의 세부과정을 나타낸 순서도이다.

도 6은 도 2의 암호문을 복호화하는 단계의 세부과정을 나타낸 순서도이다.

도 7은 본 발명의 또 다른 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법의 순서도이다.

도 8은 도 7의 세션키를 이용하여 메시지를 암호화하는 단계의 세부과정을 나타낸 순서도이다.

도 9는 도 7의 세션키를 이용하여 암호문을 복호화하는 단계의 세부과정을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

[0022] 도 1은 본 발명의 일 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법을 구현하는 시스템의 블록도이다.

[0023] 도 1에 도시된 바와 같이, 본 발명의 사용자 아이디 기반 공개키 암호화 방법을 구현하는 시스템(100)은 키생성서버(120), 송신단말(140) 및 수신단말(160)을 포함한다.

[0024] 키생성서버(120)는 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정하는데, 보다 구체적으로는 외부로부터 보안상수를 입력받아, 상기 보안상수를 입력값으로 하는 타원 곡선군에 속하는 생성원 중 임의의 제1 생성원 및 제2 생성원을 선택하고, 상기 타원 곡선군에 속하는 원소 중 임의의 원소를 선택하며, 임의의 난수를 선택하여 마스터키로 설정하여, 상기 제1 생성원, 제2 생성원 및 상기 마스터키를 겹선형 함수에 적용하여 함수값을 연산하고, 상기 제1 생성원, 제2 생성원, 상기 임의의 원소 및 상기 겹선형 함수의 함수값 중 적어도 하나를 포함하는 공개 파라미터를 설정한다.

[0025] 또한, 상기 키생성서버(120)는 수신단말(160)로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말(160)로 전송한다. 즉, 상기 키생성서버(120)는 임의의 제1 난수를 선택하고, 상기 제2 생성원, 마스터키, 임의의 원소 및 제1 난수에 기초하여 제1 비밀키를 생성하며, 상기 제1 생성원 및 제1 난수에 기초하여 제2 비밀키를 생성하고, 상기 제1 비밀키 및 제2 비밀키를 해쉬하여 제1 태그값을 생성하며, 상기 아이디를 해쉬한 값, 임의의 원소, 제1 태그값 및 제1 난수에 기초하여 제3 비밀키를 생성하고, 상기 제1 비밀키, 제2 비밀키 및 제3 비밀키를 포함하는 비밀키를 생성하여 상기 수신단말(160)로 전송한다.

[0026] 송신단말(140)은 상기 키생성서버(120)로부터 상기 공개 파라미터 및 상기 아이디를 입력받아 메시지를 암호화하여 암호문을 생성하고, 생성한 암호문을 상기 수신단말로 전송하는데, 보다 구체적으로는 임의의 제2 난수를 선택하고, 상기 겹선형 함수의 함수값, 제2 난수, 메시지에 기초하여 제1 암호문을 생성하며, 상기 제1 생성원 및 상기 제2 난수에 기초하여 제2 암호문을 생성하고, 상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 생성하며, 상기 아이디를 해쉬한 값, 임의의 원소, 제2 태그값 및 제2 난수에 기초하여 제3 암호문을 생성하고, 상기 제1 암호문, 제2 암호문 및 제3 암호문을 포함하는 암호문을 생성하여 상기 수신단말(160)로 전송한다.

[0027] 수신단말(160)은 상기 암호문 및 상기 비밀키를 입력받아, 입력받은 상기 비밀키에 기초하여 상기 암호문을 복호화하여 메시지를 획득하는데, 보다 구체적으로는 상기 키생성서버(120)로부터 수신한 비밀키 중 상기 제1 비밀키 및 제2 비밀키를 해쉬연산하여 제1 태그값을 연산하고, 상기 송신단말(140)로부터 수신한 암호문 중 상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 연산하며, 상기 제1 태그값과 제2 태그값이 동일한지 여부를 판단하고, 상기 제2 암호문과 아이디를 해쉬한 값, 상기 임의의 원소, 앞서 연산한 제2 태그값을 겹선형 함수에 적용한 함수값이 상기 제1 생성원과 상기 제3 암호문 겹선형 함수에 적용한 함수값과 서로 동일한지 여부를 판단하며, 상기 제2 암호문과 제1 비밀키를 겹선형 함수에 적용한 함수값과, 제2 암호문과 제3 비밀키를 겹선형 함수에 적용한 함수값, 제2 비밀키와 제3 암호문을 겹선형 함수에 적용한 함수값, 제1 태그값 및 제2 태그값에 기초하여 복호화 변수를 연산하여, 상기 제1 암호문을 상기 복호화 변수로 나누어 공개키를 획득한다.

[0028] 이하, 도 2를 참조하여, 본 발명에 따른 사용자 아이디 기반 공개키 암호화 방법에 대하여 자세히 살펴보도록 한다.

[0029] 도 2는 본 발명의 다른 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법의 순서도이다.

[0030] 도 2에 도시된 바와 같이, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 먼저, 키생성서버(120)가 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정한다(S210).

[0031] 이후, 상기 키생성서버(120)가 수신단말(160)로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디 에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말(160)로 전송한다(220).

[0032] 이어서, 송신단말(140)이 상기 키생성서버(120)로부터 상기 공개 파라미터 및 상기 아이디를 입력받아 메시지를

암호화하여 암호문을 생성하고, 생성한 암호문을 상기 수신단말(160)로 전송한다(S230).

[0033] 이에 따라, 상기 수신단말(160)이 상기 암호문 및 상기 비밀키를 입력받아, 입력받은 상기 비밀키에 기초하여 상기 암호문을 복호화하여 메시지를 획득한다(S240).

[0034] 이하에서는 도 3 내지 도 6을 참조하여, 상술한 각 단계별 세부과정에 대하여 자세히 설명하도록 한다.

[0035] 도 3은 공개 파라미터 및 마스터키를 설정하는 단계의 세부과정을 나타낸 순서도이다.

[0036] 먼저, 본 발명에서 사용되는 $G, \hat{G}$는 소수 p를 위수로 갖는 순환군을 나타내고, $G, \hat{G}$는 각각의 타원 곡선군에서의 생성원을 나타낸다.

[0037] 도 3에 도시된 바와 같이, 상기 키생성서버(120)가 외부로부터 보안상수 $\lambda \in Z^+$를 입력받아, 상기 보안상수 λ를 입력값으로 하여 위수를 p로 갖는 타원 곡선군 $G, \hat{G}$에 속하는 생성원 중 임의의 제1 생성원 $g \in G$ 및 제2 생성원 $\hat{g} \in \hat{G}$을 선택하고, 상기 타원 곡선군에 속하는 원소 중 임의의 원소 $\hat{u} \in \hat{G}$를 선택한다(S211).

[0038] 뿐만 아니라, 상기 키생성서버(120)는 암호학적 해쉬함수 $H_1 : \{0,1\}^* \rightarrow \hat{G}$, $H_2 : \{0,1\}^* \rightarrow Z_p$를 선택한다.

[0039] 이어서, 상기 키생성서버(120)가 임의의 난수 $\alpha \in Z_p$를 선택하고, 이를 마스터키 $msk = \alpha \in Z_p$로 설정한다(S212).

[0040] 이후, 상기 키생성서버(120)가 앞서 선택한 상기 제1 생성원 g, 제2 생성원 $\hat{g}$, 마스터키 α 및 를 겹선형 함수 $e : G \times \hat{G} \rightarrow G_t$를 하기의 수학식 1에 적용하여 겹선형 함수의 함수값을 연산한다(S213).

[0041] [수학식 1]

$$A = e(g, \hat{g})^{\alpha}$$

[0042]

[0043] 이에 따라, 상기 키생성서버(120)가 앞서 과정 S211에서 선택한 상기 제1 생성원 g, 제2 생성원 $\hat{g}$, 상기 임의의 원소 $\hat{u}$ 와, 상기 과정 S213에서 연산한 상기 겹선형 함수의 함수값 A 중 적어도 하나를 포함하는 공개 파라미터 $params = (g, \hat{g}, \hat{u}, A) \in G \times \hat{G}^2 \times G_t$를 설정한다(S214).

[0044] 도 4는 비밀키 생성단계의 세부 과정을 나타낸 순서도이다.

[0045] 도 4에 도시된 바와 같이, 키생성서버(120)가 상술한 공개 파라미터 및 마스터키를 설정하는 단계를 수행함에

따라, 임의의 제1 난수 $r \in Z_p$ 를 선택한다(S221).

[0046] 이후, 상기 키생성서버(120)가 상기 제2 생성원 $\hat{g}$, 마스터키 α, 임의의 원소 $\hat{u}$ 와, 앞서 과정 S221에서 선택한 제1 난수 r 를 하기의 수학식 2에 적용하여 공개키를 암호화하기 위한 전체 비밀키 중 제1 비밀키 d_0 를 생성한다(S222).

[0047] [수학식 2]

$$d_0 = \hat{g}^{\alpha}\hat{u}^{r}$$

[0048]

[0049] 또한, 상기 키생성서버(120)가 상기 제1 생성원 g 및 제1 난수 r 를 하기의 수학식 3에 적용하여 제2 비밀키 d_1 를 생성한다(S223).

[0050] [수학식 3]

$$d_1 = g^{r}$$

[0051]

[0052] 이어서, 상기 키생성서버(120)가 앞서, 과정 S222에서 생성한 상기 제1 비밀키 d_0 와, 과정 S223에서 제2 비밀키 d_1 를 하기의 수학식 4와 같이 해쉬연산하여 제1 태그값 tag_k 을 생성한다(S224).

[0053] [수학식 4]

$$tag_c = H_2(c_0, c_1) \in Z_p$$

[0054]

[0055] 이러한 상기 키생성서버(120)가 수신단말(160)의 아이디 id 를 해쉬연산한 값, 임의의 원소 $\hat{u}$, 제1 태그값 tag_k 및 제1 난수 r 를 하기의 수학식 5에 적용하여 제3 비밀키 d_2 를 생성한다.

[0056] [수학식 5]

$$d_2 = \left(H_1(id)\hat{u}^{tag_k}\right)^{r}$$

[0057]

[0058] 이에 따라, 상기 키생성서버(120)는 상기 제1 비밀키 d_0, 제2 비밀키 d_1 및 제3 비밀키 d_2 를 포함하는 비밀키 $d_{id} = (d_0, d_1, d_2)$ 를 생성하여 수신단말(160)로 전송한다(S226).

[0059] 도 5는 공개키에 대한 암호문 생성단계의 세부과정을 나타낸 순서도이다.

[0060] 도 5에 도시된 바와 같이, 송신단말(140)이 임의의 제2 난수 $s \in Z_p$ 를 선택한다(S231).

[0061] 이후, 상기 송신단말(140)이 앞서 공개 파라미터 및 마스터키 설정단계에서 연산한 겹선형 함수의 함수값 A, 앞서 과정 S231에서 선택한 제2 난수 s, 메시지 M를 하기의 수학식 6에 적용하여 상기 메시지 M의 전체 암호문 중 제1 암호문 c_0을 생성한다(S232).

[0062] [수학식 6]

[0063] $$c_0 = A^s \cdot M$$

[0064] 또한, 상기 송신단말(140)이 앞서 공개 파라미터 및 마스터키 설정단계에서 선택한 제1 생성원 g 과, 상기 과정 S231에서 선택한 상기 제2 난수 s를 하기의 수학식 7에 적용하여 제2 암호문 c_1을 생성한다(S233).

[0065] [수학식 7]

[0066] $$c_1 = g^s$$

[0067] 이후, 상기 송신단말(140)이 앞서 과정 S232에서 생성한 제1 암호문 c_0 과, 과정 S233에서 생성한 제2 암호문 c_1 을 하기의 수학식 8과 같이 해쉬연산하여 제2 태그값 tag_c 을 생성한다(S234).

[0068] [수학식 8]

[0069] $$tag_c = H_2(c_0, c_1) \in Z_p$$

[0070] 이어서, 상기 송신단말(140)은 수신단말(160)의 아이디 id를 해쉬한 값, 임의의 원소 $\hat{u}$, 제2 태그값 tag_c 및 제2 난수 s를 하기의 수학식 9에 적용하여 제3 암호문 c_2 을 생성한다(S235).

[0071] [수학식 9]

[0072] $$c_2 = \left(H_1(id)\hat{u}^{tag_c}\right)^s$$

[0073] 이후, 상기 송신단말(140)은 앞서 과정 S232에서 생성한 상기 제1 암호문 c_0, 과정 S233에서 생성한 제2 암호문 c_1 및 과정 S232 에서 생성한 제3 암호문 c_2 을 포함하는 메시지 M에 대한 전체 암호문

$c_{id} = (c_0, c_1, c_2) \in G_t \times G \times \hat{G}$ 을 생성하여 상기 수신단말(160)로 전송한다.

[0074] 도 6은 암호문을 복호화하는 단계의 세부과정을 나타낸 순서도이다.

[0075] 도 6에 도시된 바와 같이, 수신단말(160)이 먼저, 상기 키생성서버(120)로부터 수신한 비밀키 $d_{id} = (d_0, d_1, d_2)$ 중 제1 비밀키 d_0 및 제2 비밀키 d_1 를 하기의 수학식 4와 같이, 해쉬연산하여 제1 태그값 tag_k 을 연산한다(S241).

[0076] [수학식 4]

$$tag_k = H_2(d_0, d_1)$$

[0077]

[0078] 또한, 상기 수신단말(160)이 상기 송신단말(140)로부터 수신한 암호문 $c_{id} = (c_0, c_1, c_2)$ 중 상기 제1 암호문 c_0 및 제2 암호문 c_1 을 하기의 수학식 8과 같이 해쉬연산하여 제2 태그값 tag_c을 연산한다(S242).

[0079] [수학식 8]

$$tag_c = H_2(c_0, c_1)$$

[0080]

[0081] 이후, 상기 수신단말(160)이 앞서 과정 S241에서 연산한 제1 태그값 tag_k 과 과정 S242에서 연산한 제2 태그값 tag_c 이 동일한지 여부를 판단한다(S243).

[0082] 만약, 상기 제1 태그값 tag_k 과 제2 태그값 tag_c 이 서로 동일한 경우에는 공개키에 대한 암호문의 복호화에 실패한 것으로 판단한다.

[0083] 하지만 이와 달리, 상기 제1 태그값 tag_k 과 제2 태그값 tag_c 이 서로 상이한 경우에는 상기 수신단말(160)이 하기의 수학식 10과 같이, 상기 제2 암호문 c_1 과 아이디 id 를 해쉬한 값, 상기 임의의 원소 $\hat{u}$, 앞서 연산한 제2 태그값 tag_c 을 겹선형 함수 e 에 적용한 함수값이 상기 제1 생성원 g 과 상기 제3 암호문 c_2 을 겹선형 함수 e 에 적용한 함수값과 서로 동일한지 여부를 판단한다(S244).

[0084] [수학식 10]

$$e(c_1, H_1(id)\hat{u}^{tag_c}) =^{?} e(g, c_2)$$

[0085]

[0086] 이때 만약, 상기 제2 암호문 c_1 과 아이디 id 를 해쉬한 값, 상기 임의의 원소 $\hat{u}$, 앞서 연산한 제2 태그값 tag_c 을 겹선형 함수 e 에 적용한 함수값 이 상기 제1 생성원 g 과 상기 제3 암호문 c_2 을 겹선형 함수 e 에 적용한 함수값이 동일하지 않으면 메시지에 대한 암호문의 복호화에 실패하였다고 판단한다.

[0087] 이후, 상기 수신단말(160)은 상기 제2 암호문 c_1 과 제1 비밀키 d_0 를 겹선형 함수 e 에 적용한 함수값과, 제2 비밀키 d_1 와 제3 암호문 c_2 을 겹선형 함수 e 에 적용한 함수값, 제2 암호문 c_1 과 제3 비밀키 d_2 를 겹선형 함수 e 에 적용한 함수값, 제1 태그값 tag_k 및 제2 태그값 tag_c 을 하기의 수학식 11에 적용하여 복호화 변수 x 를 연산한다.

[0088] [수학식 11]

[0089] $$x = \left(\frac{1}{e(c_1, d_0)} \cdot \left(\frac{e(d_1, c_2,)}{e(c_1, d_2)} \right)^{\frac{1}{tag_c - tag_k}} \right)$$

[0090] 이에 따라, 상기 수신단말(160)이 상기 제1 암호문 c_0 을 상기 복호화변수 x 로 나누어 메시지 M 를 획득한다.

[0091] 또한 이러한 사용자 아이디를 이용하여 공개키를 암호화하는데 있어서, 세션키의 캡슐화 과정을 통해 메시지를 암호화하는 방법에 대하여 자세히 살펴보도록 한다.

[0092] 도 7은 본 발명의 또 다른 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법의 순서도이다.

[0093] 도 7에 도시된 바와 같이, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 먼저, 키생성서버(120)가 비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정한다(S310).

[0094] 이어서, 상기 키생성서버(120)가 수신단말(160)로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말(160)로 전송한다(S320).

[0095] 이후, 상기 송신단말(140)이 상기 공개 파라미터에 기초하여 세션키를 생성하고, 생성된 세션키에 기초하여 메시지를 암호화한 후, 암호문을 생성한다(S330).

[0096] 따라서, 수신단말(160)이 생성된 암호문을 입력받고, 세션키를 연산한 후, 생성한 세션키에 기초하여 상기 암호문을 복호화하여 메시지를 획득한다(S340).

[0097] 이하, 도 8 내지 도 9를 참조하여, 본 발명의 다른 실시 예에 따른 사용자 아이디 기반 공개키 암호화 방법에 대하여 자세히 살펴보도록 한다.

[0098] 특히, 키생성서버(120)가 공개 파라미터 및 마스터키를 설정하는 과정과, 비밀키를 생성하는 과정은 앞서 도 3 내지 도 4를 통해 설명한 내용과 동일하므로, 해당 부분의 구체적인 설명은 생략하기로 한다.

[0099] 도 8은 세션키를 이용하여 메시지를 암호화하는 단계의 세부과정을 나타낸 순서도이다.

[0100] 도 8에 도시된 바와 같이, 송신단말(140)이 임의의 제2 난수 $s \in Z_p$ 를 선택한다(S331).

[0101] 이어서, 상기 송신단말(140)이 앞서 공개 파라미터 및 마스터키를 설정하는 단계에서 연산된 겹선형 함수의 함수값 A 및 앞서 과정 S331에서 선택한 제2 난수 s 를 하기의 수학식 7에 적용하여 세션키 K 를 생성한다(S332).

[0102] [수학식 8]

[0103] $$K = A^s \in G_t$$

[0104] 이후, 상기 송신단말(140)이 앞서 연산한 상기 세션키 K 와, 메시지 M 를 하기의 도 13과 같은 대칭키 알고리즘에 적용하여 제4 암호문을 연산한다(S333).

[0105] [수학식 13]

[0106] $$C_M = SymEnc(K, M)$$

[0107] 이어서, 상기 송신단말(140)은 제4 암호문 C_M , 제1 생성원 g 및 제2 난수 s 를 하기의 수학식 14와 같이 해시연산하여 제2 태그값 tag_c 을 생성한다(S334).

[0108] [수학식 14]

[0109] $$tag_c = H_2(C_M, g^s)$$

[0110] 이에 따라, 상기 송신단말(140)이 상기 제1 생성원 g , 상기 제2 난수 s 와, 상기 아이디 id 를 해쉬연산한 값, 상기 임의의 원소 $\hat{u}$ 및 제2 태그값 tag_c 을 하기의 수학식 15에 적용하여 암호문 c_{id} 을 생성한다(S335).

[0111] [수학식 15]

[0112] $$C_{id} = (C_M, C_1, C_2) = (C_M, g^s, (\mathrm{H}_1(\mathrm{id})\hat{u}^{tag_c})^s)$$

[0113] 도 9는 세션키를 이용하여 암호문을 복호화하는 단계의 세부과정을 나타낸 순서도이다.

[0114] 도 9에 도시된 바와 같이, 수신단말(160)이 상기 키생성서버(120)로부터 수신한 비밀키 $d_{id} = (d_0, d_1, d_2)$ 중 상기 제1 비밀키 d_0 및 제2 비밀키 d_1 를 하기의 수학식 4와 같이 해쉬연산하여 제1 태그값 tag_k 을 연산한다(S341).

[0115] [수학식 4]

[0116] $$tag_k = H_2(d_0, d_1)$$

[0117] 상기 수신단말(160)이 상기 송신단말(140)로부터 수신한 암호문 $C_{id} = (C_M, C_1, C_2)$ 중 상기 제4 암호문 C_M 및 제2 암호문 c_1 을 하기의 수학식 8과 같이 해쉬연산하여 제2 태그값 tag_c을 연산한다(S342).

[0118] [수학식 8]

[0119] $$tag_c = H_2(C_M, C_1)$$

[0120] 상기 수신단말(160)이 상기 제1 태그값 tag_k 과 제2 태그값 tag_c 이 동일한지 여부를 판단한다(S343).

[0121] 이때, 상기 제1 태그값 tag_k 과 제2 태그값 tag_c 이 동일한 경우에는 공개키의 암호문에 대한 복호화에 실패하였다고 판단한다.

[0122] 하지만, 상기 제1 태그값 tag_k 과 제2 태그값 tag_c 이 동일하지 않은 경우에는 상기 수신단말(160)이 상기 제2 암호문 c_1 과 제1 비밀키 d_0 를 겹선형 함수 e 에 적용한 함수값과, 제2 비밀키 d_1 와 제3 암호문 c_2 을 겹선형 함수 e 에 적용한 함수값, 제2 암호문 c_1 과 제3 비밀키 d_2 를 겹선형 함수 e 에 적용한 함수값, 제1 태그값 tag_k 및 제2 태그값 tag_c 을 하기의 수학식 11에 적용하여 복호화 변수 x 를 연산한다(S344).

[0123] [수학식 11]

[0124] $$x = \left(\frac{1}{e(c_1, d_0)} \cdot \left(\frac{e(d_1, c_2,)}{e(c_1, d_2)} \right)^{\frac{1}{tag_c - tag_k}} \right)$$

[0125] 이에 따라, 상기 수신단말(160)이 앞서 연산한 복호화 변수 x 를 대칭키 암호 알고리즘 을 이용하여 세션키 K 를 획득한다(S345).

[0126] 상기 수신단말(160)이 상기 세션키 K 및 제4 암호문 C_M 를 대칭키 알고리즘에 적용하여 메시지 M 를 획득한다(S346).

[0127] 이러한 본 발명의 사용자 아이디 기반 공개키 암호화 방법의 주요 특징을 살펴보면, 태그를 사용하고, 사용자의

아이디를 마스터 비밀키와 결합하지 않는 것을 알 수 있다.

[0128] 특히, 암호문과 비밀키의 구조를 서로 비교하여 살펴보면, 제2 비밀키 $d_1 = \left(H_1(id)\hat{u}^{tag_k}\right)^r$ 와 제3 암호문 $c_2 = \left(H_1(id)\hat{u}^{tag_c}\right)^s$ 의 구조가 동일한 것을 알 수 있다.

[0129] 이에 따라, 본 발명은 공개키의 복호화 단계에서 비밀키와 암호문에서의 아이디가 같더라도, $1/tag_c - tag_k$ 는 상기 제1 태그값 tag_k 과 제2 태그값 tag_c 이 서로 다를 때만 연산이 수행되기 때문에, 비밀키 생성 시 사용되었던 제1 태그값 tag_k 과 암호문 생성 시 사용되었던 제2 태그값 tag_c 이 서로 다른 경우에만 정당한 메시지 M 를 연산할 수 있다.

[0130] 이하, 표 1을 참조하여 본 발명과 종래기술간의 연산량을 살펴보도록 한다.

[0131] 본 발명과 종래기술의 연산량 판단조건을 살펴보기 위해, 타원곡선의 종류와 안정성의 비도에 따라 SS80(비트 안전성 비도를 가지는 supersingular 타원곡선), MNT80(80비트 안전성 비도를 가지는 MNT 타원곡선), MNT128 경우(128비트 안전성 비도를 가지는 MNT 타원곡선)을 고려하였다.

[0132] 연산량은 지수 연산과, 겹선형 함수의 연산 횟수, 타원곡선군을 치역으로 하는 해쉬함수의 연산에 따라 달라지게 되는데, 지수 연산의 경우에는 밑(base)이 항상 고정되어 있는 경우에는 사전 연산을 통하여 일반적인 지수 연산보다 효율적으로 연산이 수행될 수 있다. 또한, 겹선형 함수의 연산은 전체 연산량 중에서 가장 큰 비중을 차지하는데, 겹선형 함수간 나눗셈(ratio of two bilinear map)은 1회 내지 2회의 비교적 적은 연산횟수를 통해 효율적인 연산량이 수행된다.

표 1

[0133]

	원소의 크기 (bits)				계산량								
	Z_n	G	$\hat{G}$	G_t	G		$\hat{G}$			G_t			
					고정된 밑의 지수승	일반적 지수승	고정된 밑의 지수승	일반적 지수승	해쉬	고정된 밑의 지수승	일반적 지수승	페어링	페어링나눗셈
SS / 80	160	512	512	1024	2	10	2	10	10	2	10	100	120
MNT / 80	160	171	1026	1026	0.2	1	8	40	40	2	10	100	120
MNT / 128	256	512	3072	3072	3	15	100	500	500	30	150	1500	1800

[0134] 하기의 표 2는 본 발명과 종래기술들간에 안전성 소신을 고려한 연산의 효율성 비교를 나타낸 표이다.

표 2

[0135]

	커브 / 보안 레벨	오버헤드 (bits)		상대적인 연산량		
		공개키 크기	암호문 크기	비밀키 생성	암호화	복호화
종래기술1(BF)	MNT / 128	1024	768	1000	2006	1503
종래기술2(BB)	MNT / 128	4608	1280	200	39	1833
종래기술3(SK)	MNT / 128	4096	768	100	36	1536
본 발명	SS / 80	2048	1024	28	26	130

[0136] 표 2에 기재된 바와 같이, 비밀키 생성시 연산량을 기준으로 본 발명과 종래기술을 살펴보면, 본 발명이 28회에 연산이 이루어지는 반면, 종래기술들은 100 내지 1000 회의 연산과정이 수행되는 것을 알 수 있어, 본 발명이

적게는 1/5 에서 많게는 1/50 정도의 연산량이 감소하는 것을 확인할 수 있다.

[0137] 이와 같은 본 발명의 연산량 감소의 효과는 비밀키 생성과정에서 뿐만 아니라, 암호화 및 복호화 과정에서도 확인되는 것을 알 수 있다.

[0138] 또한, 이러한 사용자 아이디 기반 공개키 암호화 방법은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0139] 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 사용자의 고유한 아이디를 공개키로 사용하여, 제3의 신뢰기관을 통한 공개키를 인증하는 절차가 생략됨으로써, 통신을 효율적으로 수행할 수 있도록 하는 효과가 있다.

[0140] 또한, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 제3의 신뢰기관을 통한 공개키에 대한 인증서를 사용하지 않으므로, 인증서 폐기 목록을 지속적으로 유지하거나, 관리하는 비용 및 시간을 감소시킬 수 있는 효과가 있다.

[0141] 더불어, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 사용자의 아이디를 공개키로 사용하므로, 공개키 확인을 통해 통신을 수행하고자 하는 사용자의 신원을 용이하게 파악할 수 있는 효과가 있다.

[0142] 이와 더불어, 본 발명의 사용자 아이디 기반 공개키 암호화 방법은 복잡한 형태의 공개키 기반 구조 (PKI, Public Key Infrastructure)를 구축할 필요가 없어, 공개키 구조를 구축하는데 소요되는 시간 및 비용을 감소시킬 수 있는 효과가 있다.

[0143] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

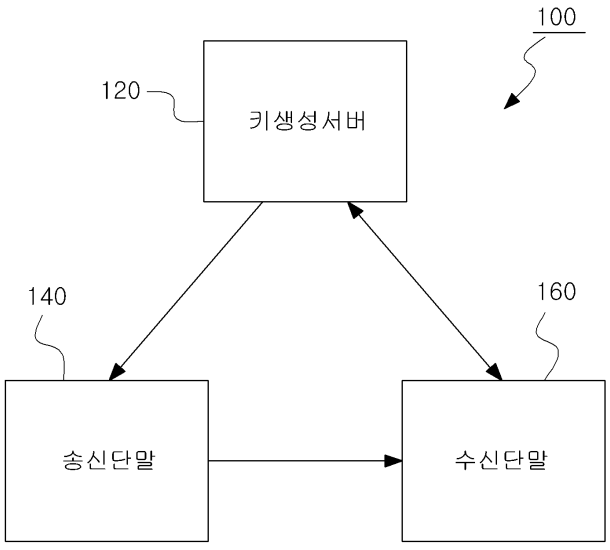
부호의 설명

[0144] 120: 키생성서버 140: 송신단말

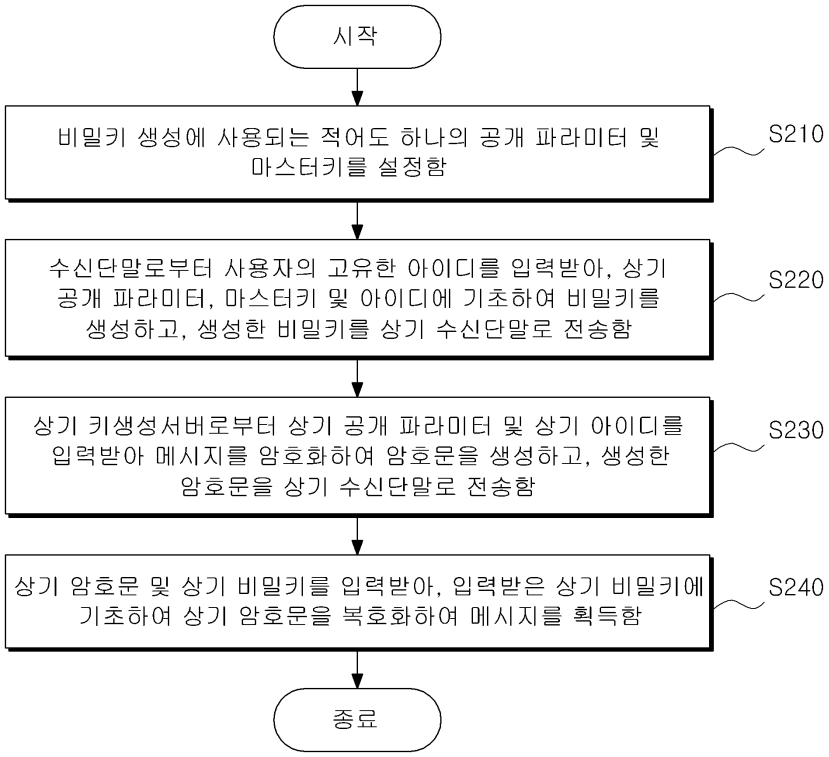
160: 수신단말

도면

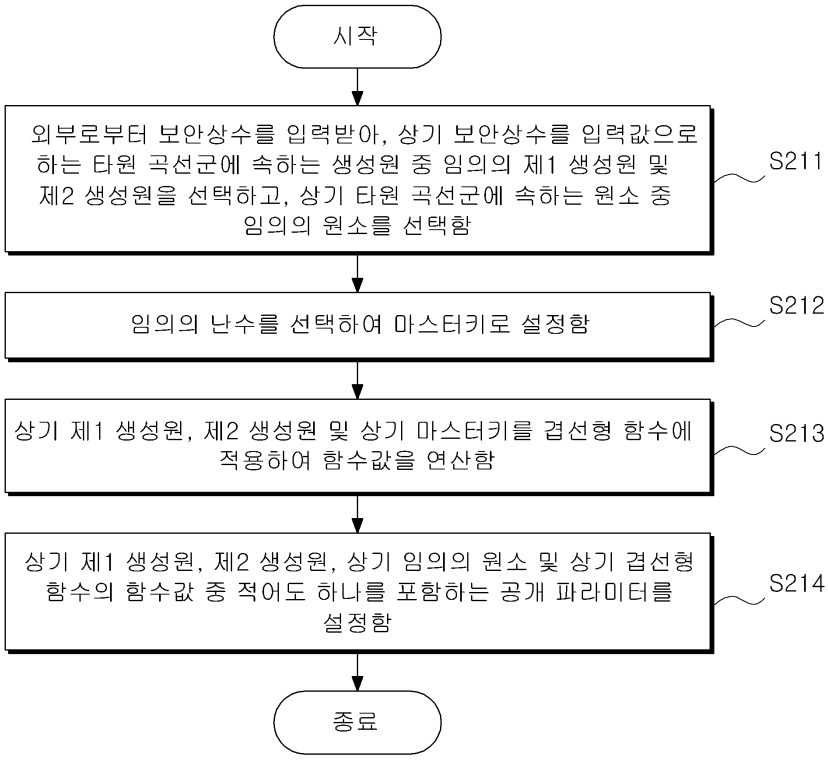
도면1



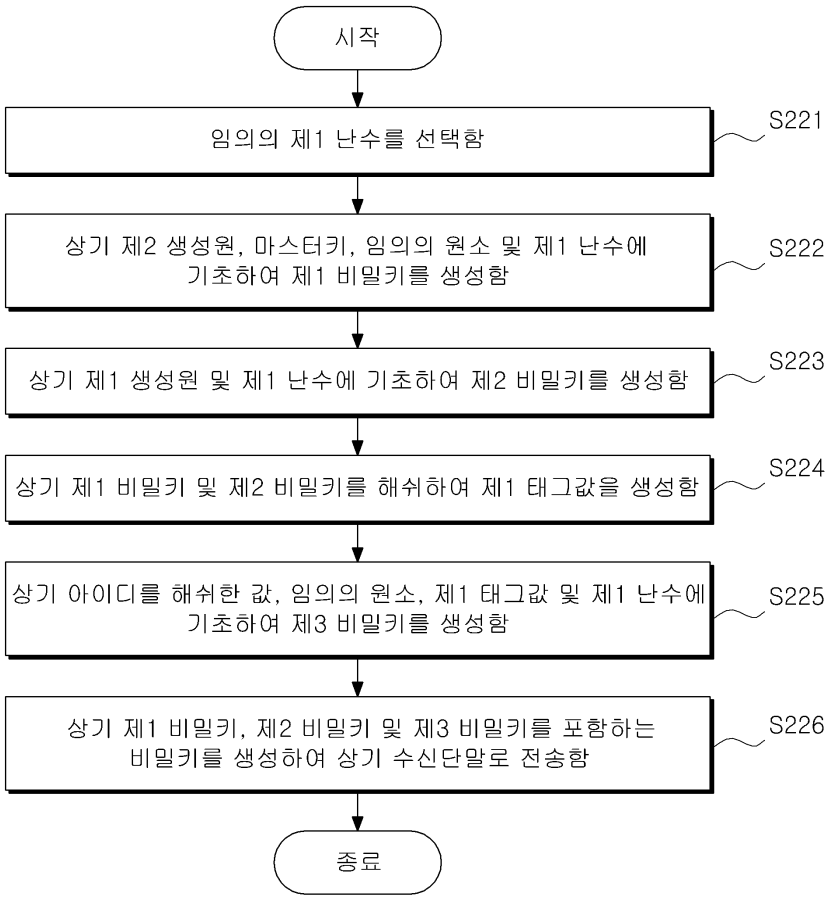
도면2


시작
비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정함
S210
수신단말로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송함
S220
상기 키생성서버로부터 상기 공개 파라미터 및 상기 아이디를 입력받아 메시지를 암호화하여 암호문을 생성하고, 생성한 암호문을 상기 수신단말로 전송함
S230
상기 암호문 및 상기 비밀키를 입력받아, 입력받은 상기 비밀키에 기초하여 상기 암호문을 복호화하여 메시지를 획득함
S240
종료

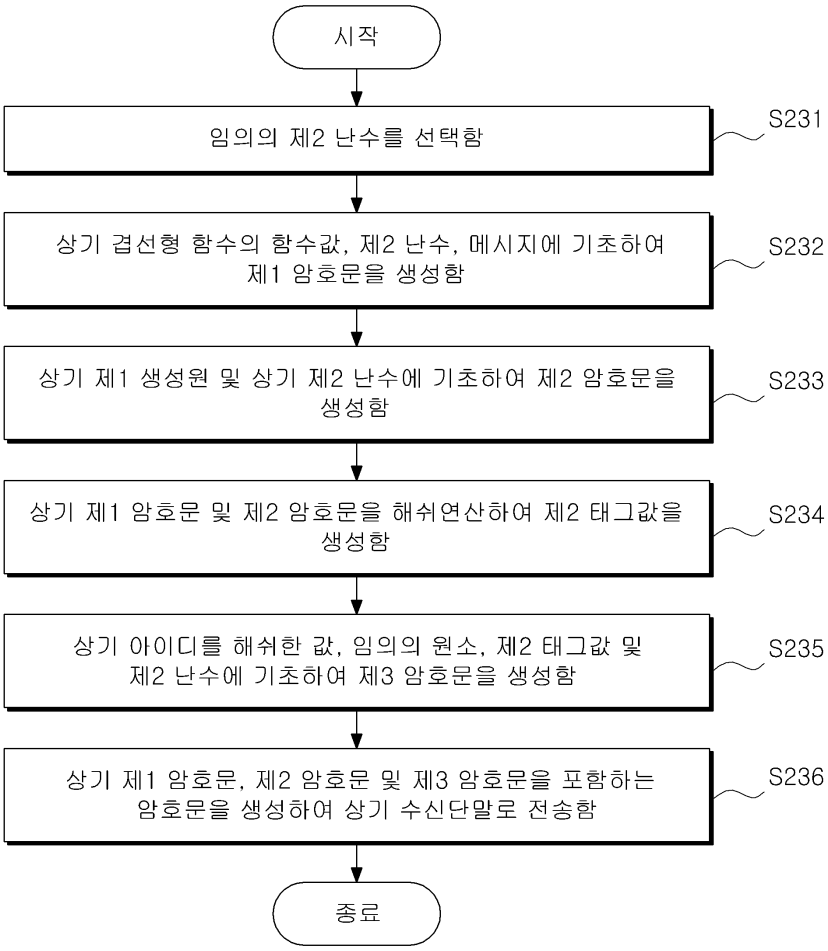
도면3


시작
외부로부터 보안상수를 입력받아, 상기 보안상수를 입력값으로 하는 타원 곡선군에 속하는 생성원 중 임의의 제1 생성원 및 제2 생성원을 선택하고, 상기 타원 곡선군에 속하는 원소 중 임의의 원소를 선택함
S211
임의의 난수를 선택하여 마스터키로 설정함
S212
상기 제1 생성원, 제2 생성원 및 상기 마스터키를 겹선형 함수에 적용하여 함수값을 연산함
S213
상기 제1 생성원, 제2 생성원, 상기 임의의 원소 및 상기 겹선형 함수의 함수값 중 적어도 하나를 포함하는 공개 파라미터를 설정함
S214
종료

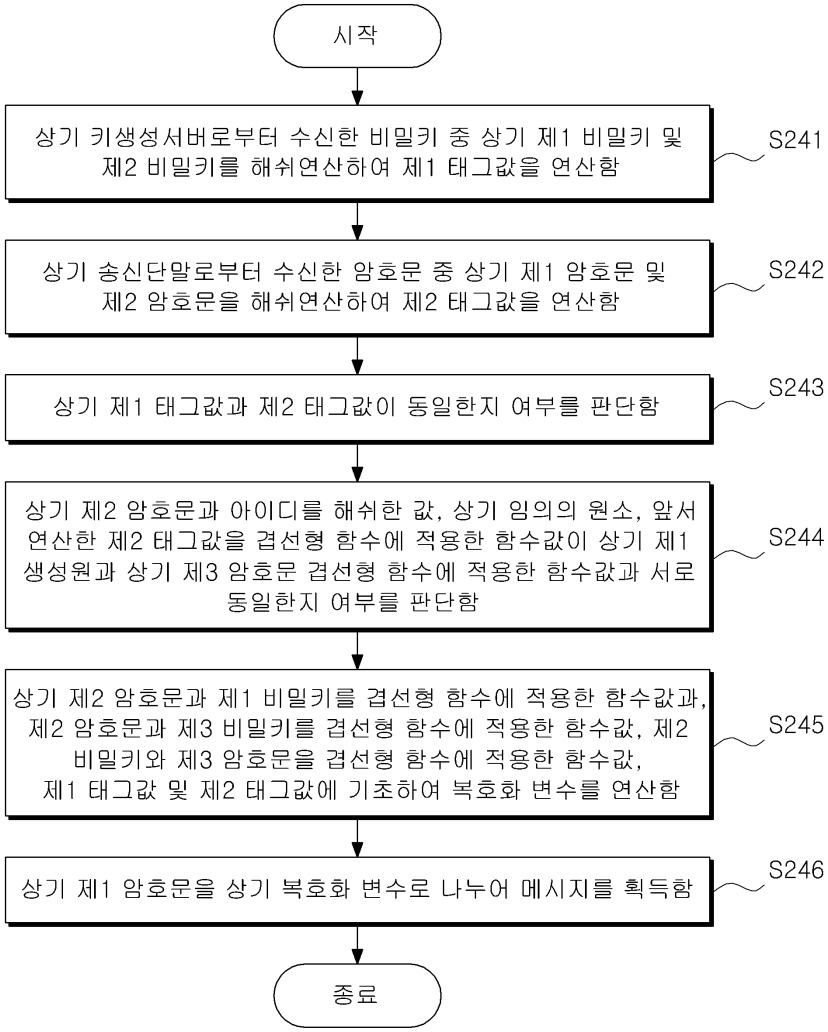
도면4


시작
임의의 제1 난수를 선택함
S221
상기 제2 생성원, 마스터키, 임의의 원소 및 제1 난수에 기초하여 제1 비밀키를 생성함
S222
상기 제1 생성원 및 제1 난수에 기초하여 제2 비밀키를 생성함
S223
상기 제1 비밀키 및 제2 비밀키를 해쉬하여 제1 태그값을 생성함
S224
상기 아이디를 해쉬한 값, 임의의 원소, 제1 태그값 및 제1 난수에 기초하여 제3 비밀키를 생성함
S225
상기 제1 비밀키, 제2 비밀키 및 제3 비밀키를 포함하는 비밀키를 생성하여 상기 수신단말로 전송함
S226
종료

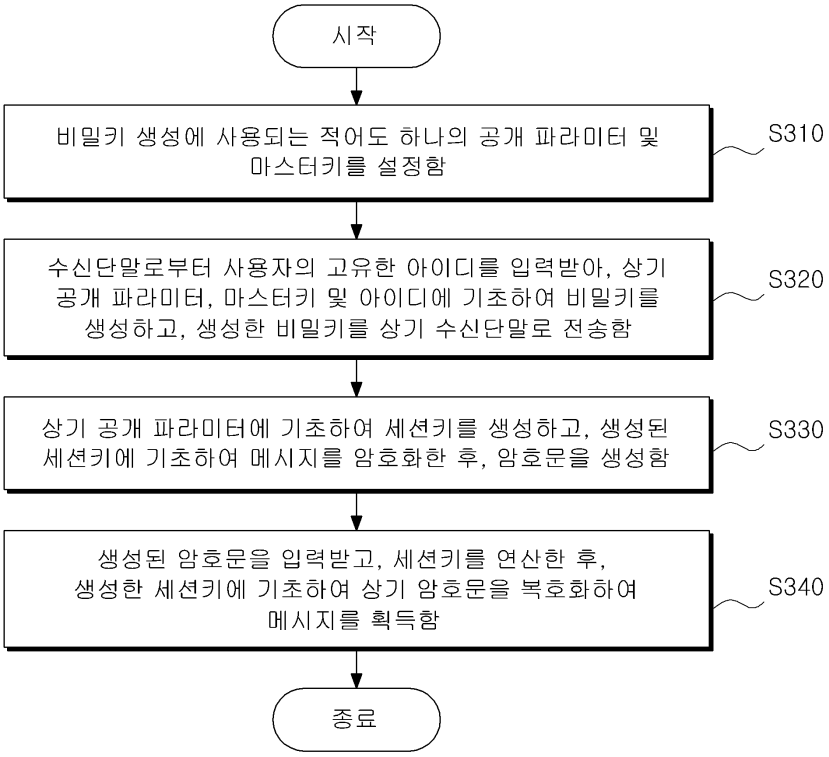
도면5


시작
임의의 제2 난수를 선택함
S231
상기 겹선형 함수의 함수값, 제2 난수, 메시지에 기초하여 제1 암호문을 생성함
S232
상기 제1 생성원 및 상기 제2 난수에 기초하여 제2 암호문을 생성함
S233
상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 생성함
S234
상기 아이디를 해쉬한 값, 임의의 원소, 제2 태그값 및 제2 난수에 기초하여 제3 암호문을 생성함
S235
상기 제1 암호문, 제2 암호문 및 제3 암호문을 포함하는 암호문을 생성하여 상기 수신단말로 전송함
S236
종료

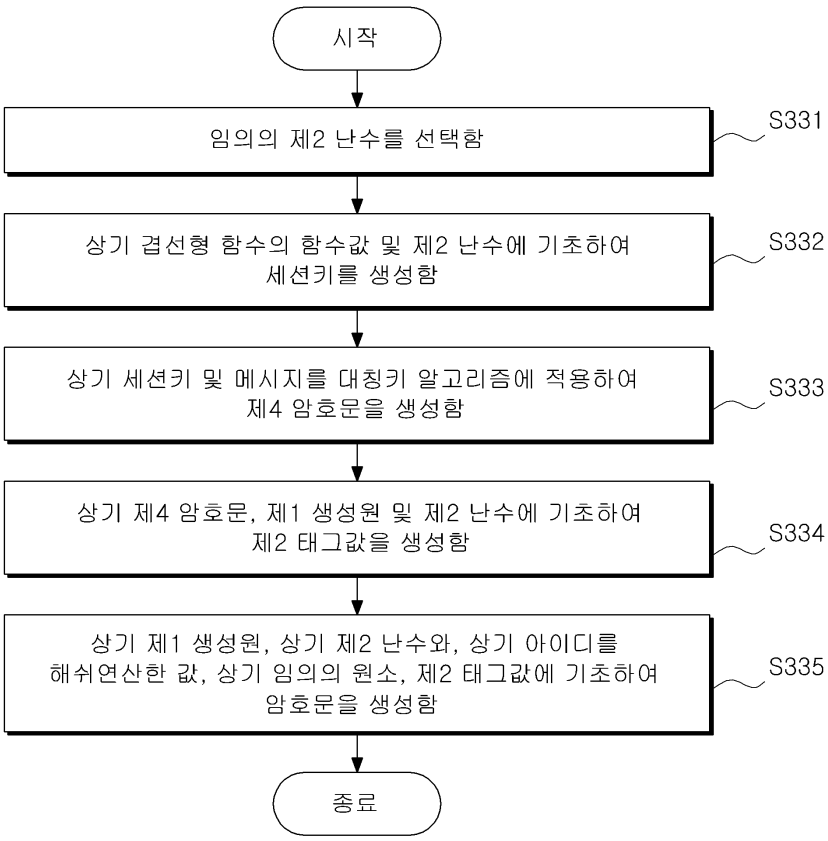
도면6


시작
상기 키생성서버로부터 수신한 비밀키 중 상기 제1 비밀키 및 제2 비밀키를 해쉬연산하여 제1 태그값을 연산함
S241
상기 송신단말로부터 수신한 암호문 중 상기 제1 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 연산함
S242
상기 제1 태그값과 제2 태그값이 동일한지 여부를 판단함
S243
상기 제2 암호문과 아이디를 해쉬한 값, 상기 임의의 원소, 앞서 연산한 제2 태그값을 겹선형 함수에 적용한 함수값이 상기 제1 생성원과 상기 제3 암호문 겹선형 함수에 적용한 함수값과 서로 동일한지 여부를 판단함
S244
상기 제2 암호문과 제1 비밀키를 겹선형 함수에 적용한 함수값과, 제2 암호문과 제3 비밀키를 겹선형 함수에 적용한 함수값, 제2 비밀키와 제3 암호문을 겹선형 함수에 적용한 함수값, 제1 태그값 및 제2 태그값에 기초하여 복호화 변수를 연산함
S245
상기 제1 암호문을 상기 복호화 변수로 나누어 메시지를 획득함
S246
종료

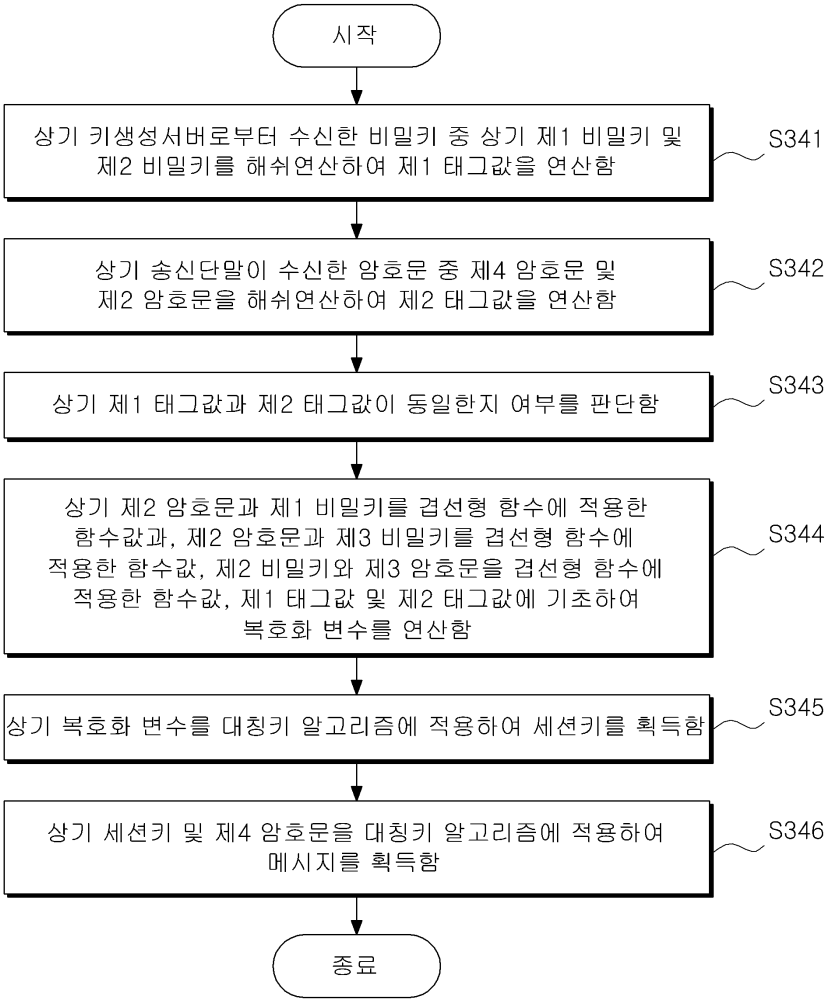
도면7


시작
비밀키 생성에 사용되는 적어도 하나의 공개 파라미터 및 마스터키를 설정함
S310
수신단말로부터 사용자의 고유한 아이디를 입력받아, 상기 공개 파라미터, 마스터키 및 아이디에 기초하여 비밀키를 생성하고, 생성한 비밀키를 상기 수신단말로 전송함
S320
상기 공개 파라미터에 기초하여 세션키를 생성하고, 생성된 세션키에 기초하여 메시지를 암호화한 후, 암호문을 생성함
S330
생성된 암호문을 입력받고, 세션키를 연산한 후, 생성한 세션키에 기초하여 상기 암호문을 복호화하여 메시지를 획득함
S340
종료

도면8


시작
임의의 제2 난수를 선택함
S331
상기 겹선형 함수의 함수값 및 제2 난수에 기초하여 세션키를 생성함
S332
상기 세션키 및 메시지를 대칭키 알고리즘에 적용하여 제4 암호문을 생성함
S333
상기 제4 암호문, 제1 생성원 및 제2 난수에 기초하여 제2 태그값을 생성함
S334
상기 제1 생성원, 상기 제2 난수와, 상기 아이디를 해쉬연산한 값, 상기 임의의 원소, 제2 태그값에 기초하여 암호문을 생성함
S335
종료

도면9


시작
상기 키생성서버로부터 수신한 비밀키 중 상기 제1 비밀키 및 제2 비밀키를 해쉬연산하여 제1 태그값을 연산함
S341
상기 송신단말이 수신한 암호문 중 제4 암호문 및 제2 암호문을 해쉬연산하여 제2 태그값을 연산함
S342
상기 제1 태그값과 제2 태그값이 동일한지 여부를 판단함
S343
상기 제2 암호문과 제1 비밀키를 겹선형 함수에 적용한 함수값과, 제2 암호문과 제3 비밀키를 겹선형 함수에 적용한 함수값, 제2 비밀키와 제3 암호문을 겹선형 함수에 적용한 함수값, 제1 태그값 및 제2 태그값에 기초하여 복호화 변수를 연산함
S344
상기 복호화 변수를 대칭키 알고리즘에 적용하여 세션키를 획득함
S345
상기 세션키 및 제4 암호문을 대칭키 알고리즘에 적용하여 메시지를 획득함
S346
종료