(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년12월28일
(11) 등록번호 10-1580204
(24) 등록일자 2015년12월18일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01)
(21) 출원번호 10-2014-0109746
(22) 출원일자 2014년08월22일
심사청구일자 2014년08월22일
(56) 선행기술조사문헌
US20120296829 A1
KR1020140079544 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
서민혜
서울 양천구 목동중앙남로 21-15, 101동 703호 (목동, 에이스아파트)
박승환
서울특별시 동작구 노량진로 6마길 8
(뒷면에 계속)
(74) 대리인
김등용

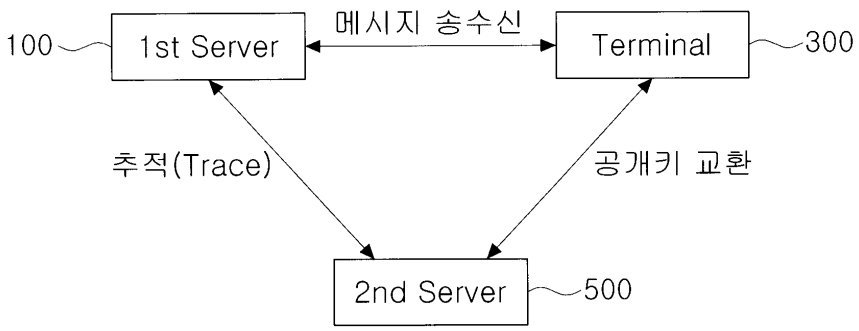
전체 청구항 수 : 총 8 항 심사관 : 문형섭

(54) 발명의 명칭 **추적가능한 불확정 전송 방법 및 메시지를 추적하는 방법**

(57) 요 약

추적가능한 불완전 전송 방법이 개시된다. 상기 추적가능한 불완전 전송 방법은, 서버가 겹선형 그룹의 생성원, 다수의 제1 난수들, 및 제1 비밀값을 선택하는 단계, 상기 서버가 상기 생성원과 상기 제1 비밀값을 이용하여 제1 공개키를 생성하는 단계, 상기 서버가 상기 제1 공개키와 상기 다수의 제1 난수들을 이용하여 다수의 메시지들 각각에 대한 다수의 암호문들을 생성하는 암호화 단계, 상기 서버가 상기 제1 공개키와 상기 다수의 암호문들을 단말기로 송신하는 제1 송신 단계, 상기 서버가 상기 단말기가 전송받고자 하는 메시지와 임의의 제2 난수를 이용하여 계산된 제1 계산값을 상기 단말기로부터 수신하는 제1 수신 단계, 및 상기 서버가 상기 제1 계산값과 상기 제1 비밀값을 이용하여 복호화키를 생성하고, 상기 복호화키를 상기 단말기로 송신하는 제2 송신 단계를 포함한다.

대 표 도 - 도1



10

(72) 발명자

엄지은

서울 서대문구 가재울로 45, 102동 102호 (남가좌동, 현대아파트)

이동훈

서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)

이 발명을 지원한 국가연구개발사업

과제고유번호	2013060756
부처명	미래창조과학부
연구관리전문기관	한국연구재단
연구사업명	중견연구자지원_도약연구(전략)
연구과제명	속성 기반 공개키 시스템에 관한 연구
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2013.09.01 ~ 2014.08.31

명 세 서

청구범위

청구항 1

서버가 겹선형 그룹(G)의 생성원(g), 다수의 제1 난수들($(r_1, \cdots, r_n) \in (Z_q)^{n+1}$), 및 제1 비밀값($x \in (Z_q)^{n+1}$)을 선택하는 단계;

상기 서버가 상기 생성원(g)과 상기 제1 비밀값(x)을 이용하여 제1 공개키를 생성하는 단계;

상기 서버가 상기 제1 공개키와 상기 다수의 제1 난수들을 이용하여 다수의 메시지들($M_1, \cdots, M_n$) 각각에 대한 다수의 암호문들($C_i=(A_i, B_i)$, $1 \leq i \leq n$)을 생성하는 암호화 단계;

상기 서버가 상기 제1 공개키와 상기 다수의 암호문들을 단말기로 송신하는 제1 송신 단계;

상기 서버가 상기 단말기가 전송받고자 하는 메시지(C_{σ_i})와 임의의 제2 난수($v \in Z_q$)를 이용하여 계산된 제1 계산값($V_{i,1}$)을 상기 단말기로부터 수신하는 제1 수신 단계; 및

상기 서버가 상기 제1 계산값($V_{i,1}$)과 상기 제1 비밀값을 이용하여 복호화키를 생성하고, 상기 복호화키를 상기 단말기로 송신하는 제2 송신 단계를 포함하는, 추적가능한 불확정 전송 방법.

청구항 2

제1항에 있어서,

상기 추적가능한 불확정 전송 방법은,

상기 제1 수신 단계 이전에, 상기 서버가, 영지식 증명(Zero Knowledge Proof of Knowledge)을 통하여 상기 단말기를 대상으로 상기 서버가 상기 제1 비밀값(x)을 알고 있음을 증명하는 단계; 및

상기 제2 송신 단계 이전에, 상기 서버가, 증거 구분불가능 증명(Witness Indistinguishability Proof of Knowledge)을 통하여 상기 다수의 암호문들(C_i)에 포함된 값들 중 어느 하나를 이용하여 상기 제1 계산값($V_{i,1}$)이 계산되었음을 검증하는 단계를 더 포함하는, 추적가능한 불확정 전송 방법.

청구항 3

제1항에 있어서,

상기 단말기는 PC(personal computer), 태블릿(tablet) PC, 또는 스마트폰(smart phone)인, 추적가능한 불확정 전송 방법.

청구항 4

제1항에 있어서,

상기 제1 수신단계와 상기 제2 송신단계는 상기 단말기가 수신하려는 메시지의 갯수에 해당하는 횟수만큼 반복 수행되는, 추적가능한 불확정 전송 방법.

청구항 5

제1항에 있어서,

상기 제1 수신 단계는, 상기 단말기에 의해 계산된 제2 계산값($V_{i,2} \leftarrow A_{\sigma_i} g^{av}$)과 제3 계산값($V_{i,3} \leftarrow g^{v}$)을 수신하는 단계를 포함하고,

상기 g^a는 상기 단말기가 제2 서버로부터 수신한 제2 공개키이고,

상기 a는 상기 제2 서버에 의해 선택된 임의의 난수이고,

상기 추적가능한 불확정 전송 방법은,

상기 서버가 상기 제1 계산값 내지 상기 제3 계산값을 상기 제2 서버로 송신하는 제3 송신 단계를 더 포함하는, 추적가능한 불확정 전송 방법.

청구항 6

제5항에 있어서,

상기 제1 수신 단계는, 상기 단말기에 의해 계산된 제4 계산값($V_{i,4} \leftarrow (g^a)^{H(g^v)v}$)과 제5 계산값($V_{i,5} \leftarrow (A_{\sigma_i})^{H(g^{av})vs}$)을 수신하는 단계를 포함하고,

상기 $H()$는 해시 함수이고,

상기 제3 송신 단계는, 상기 제4 계산값과 상기 제5 계산값을 상기 제2 서버로 송신하는 단계를 포함하는, 추적가능한 불확정 전송 방법.

청구항 7

제5항에 기재된 추적가능한 불확정 전송 방법에 의하여 상기 단말기가 전송받은 메시지를 추적하는 방법에 있어서,

상기 제2 서버가 상기 제2 계산값($V_{i,2}$)과 상기 제3 계산값($V_{i,3}$)을 이용하여 제6 계산값($A'_{\sigma_i} = V_{i,2}/(V_{i,3})^a$)을 계산하는 단계; 및

상기 제6 계산값이 상기 단말기가 전송받은 메시지인지 여부를 결정하는 단계를 포함하는, 메시지를 추적하는 방법.

청구항 8

제6항에 기재된 추적가능한 불확정 전송 방법에 의하여 상기 단말기가 전송받은 메시지를 추적하는 방법에 있어서,

상기 제2 서버가 상기 제2 계산값($V_{i,2}$)과 상기 제3 계산값($V_{i,3}$)을 이용하여 제6 계산값($A'_{\sigma_i} = V_{i,2}/(V_{i,3})^a$)을 계산하는 단계;

상기 제2 서버가 수학식 1과 수학식 2를 통하여 상기 제6 계산값(A'_{σ_i})을 검증하는 단계; 및

상기 제2 서버가, 상기 수학식 1과 상기 수학식 2가 만족되는 경우 상기 제6 계산값(A'_{σ_i})을 상기 단말기가 전송받은 메시지로 결정하는 단계를 포함하고,

상기 수학식 1은 $e(A'_{\sigma_i}, V_{i,4}) = ?e(V_{i,1}, g^{H(V_{i,3})a})$ 이고,

상기 수학식 2는 $e(V_{i,5}, g) = ?e(pk_R, (V_{i,1})^{H((V_{i,3})^{\alpha})})$ 인, 메시지를 추적하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 추적가능한 불확정 전송 방법에 관한 것으로, 특히 불확정 전송 기법을 통하여 단말기가 수신한 메시지를 추적할 수 있는 추적가능한 불확정 전송 방법 및 메시지를 추적하는 방법에 관한 것이다.

배 경 기 술

[0002] 불확정 전송(Oblivious Transfer; OT) 기법은 송신자와 수신자 간 통신에 사용되는 프로토콜이다. 불확정 전송의 개념은 1981년 Rabin에 의해 처음 제안되었으며, 기본적으로 다음의 두 가지 요구사항을 만족해야 한다. 첫 번째로, 송신자는 수신자가 어떤 메시지를 원하는지 알 수 없어야 한다. 두 번째로, 수신자는 자신이 원하는 메시지 이외에 다른 메시지에 대해서 어떠한 정보도 얻을 수 없어야 한다. 불확정 전송 기법은 암호학적 프리미티브로써, 여러 암호학적 기법의 구성요소로 사용하기 위해 기능성과 효율성을 높이는 방향으로 연구가 진행되고 있다. 초기에는 두 개의 메시지 중 한 개의 메시지를 수신자가 얻을 수 있는 1-out-of-2 OT(OT_1^2)가 제안되었고, 1999년 Naor와 Pinkas에 의해 확장된 개념인 k-out-of-N OT(OT_k^N)가 제안되었다.

[0003] 상기와 같은 불확정 전송 기법은 안전한 양자간 연산으로, 신뢰 기관을 두지 않기 때문에 프로토콜 수행 후 문제가 발생했을 때, 수신자가 어떤 메시지를 전송 받았는지 추적할 수 없다. 따라서 불확정 전송 기법을 이용하여 송신자와 수신자가 프로토콜을 수행하고, 이후에 문제가 발생했을 때, 수신자가 송신자로부터 받은 메시지를 추적할 수 있는 기법이 필요하다.

선행기술문헌

비특허문헌

[0004] (비특허문헌 0001) Kurosawa, K., Nojima, R.: Simple Adaptive Oblivious Transfer without Random Oracle. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 334-346. Springer, Heidelberg (2009)

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 기술적인 과제는, 불확정 전송 기법을 통하여 수신자가 전송받은 메시지를 추적할 수 있는, 추적가능한 불확정 전송 방법 및 메시지를 추적하는 방법을 제공하는 것이다.

과제의 해결 수단

[0006] 본 발명의 실시 예에 따른 추적 가능한 불확정 전송 방법은, 서버가 겹선형 그룹의 생성원, 다수의 제1 난수들, 및 제1 비밀값을 선택하는 단계, 상기 서버가 상기 생성원과 상기 제1 비밀값을 이용하여 제1 공개키를 생성하

는 단계, 상기 서버가 상기 제1 공개키와 상기 다수의 제1 난수들을 이용하여 다수의 메시지들 각각에 대한 다수의 암호문들을 생성하는 암호화 단계, 상기 서버가 상기 제1 공개키와 상기 다수의 암호문들을 단말기로 송신하는 제1 송신 단계, 상기 서버가 상기 단말기가 전송받고자 하는 메시지와 임의의 제2 난수를 이용하여 계산된 제1 계산값을 상기 단말기로부터 수신하는 제1 수신 단계, 및 상기 서버가 상기 제1 계산값과 상기 제1 비밀값을 이용하여 복호화키를 생성하고, 상기 복호화키를 상기 단말기로 송신하는 제2 송신 단계를 포함한다.

발명의 효과

[0007] 본 발명의 실시 예에 따른 추적가능한 불확정 전송 방법은 제3의 주체인 개봉자(Opener)를 통하여 수신자가 송신자로부터 전송받은 메시지를 추적할 수 있는 효과가 있다.

[0008] 또한, 상기 추적가능한 불확정 전송 방법에 따를 경우, 송신자와 개봉자가 공모하여 수신자가 요청하지 않은 메시지를 전송받았다는 공격을 방지할 수 있으며, 수신자와 개봉자가 공모하여 수신자가 송신자에게 요청하지 않은 메시지에 대한 정보를 얻을 수 없게 된다.

도면의 간단한 설명

[0009] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 불확정 전송 시스템을 도시한다.

도 2는 도 1에 도시된 불확정 전송 시스템을 이용한 불확정 전송 방법 중 초기 설정 단계를 설명하기 위한 흐름도이다.

도 3은 도 1에 도시된 불확정 전송 시스템을 이용한 불확정 전송 방법 중 전송 단계를 설명하기 위한 흐름도이다.

도 4는 도 1에 도시된 불확정 전송 시스템을 이용한 불확정 전송 방법 중 추적 단계를 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0010] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0011] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0012] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0013] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0014] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야

한다.

[0015] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0016] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0017] 도 1은 본 발명의 일 실시 예에 따른 불확정 전송 시스템을 도시한다.

[0018] 도 1을 참조하면, 불확정 전송 시스템(10)은 제1 서버(100), 단말기(300), 및 제2 서버(500)를 포함하고, 제1 서버(100)와 단말기(300), 단말기(300)와 제2 서버(500), 및 제1 서버(100)와 제2 서버(500) 각각은 유무선 통신망을 통하여 통신할 수 있다.

[0019] 불확정 전송 시스템(10) 내에서 제1 서버(100), 즉 송신자(Sender)와 단말기(300), 즉 수신자(Receiver)는 초기 설정 단계(Initializaion Phase)와 전송 단계(Transfer Phase)를 통하여 불확정 전송 프로토콜을 수행한다. 또한, 단말기(300)가 전송받은 메시지를 추적할 필요가 있는 경우, 제1 서버(100)와 제2 서버(500), 즉 개봉자(Opener)는 추적 단계(Trace Phase)를 통하여 단말기(300)가 전송받은 메시지를 추적할 수 있다.

[0020] 단말기(300)는 PC(personal computer), 태블릿 PC, 노트북(notebook), 넷-북(net-book), e-리더(e-reader), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 또는 MP4 플레이어와 같은 데이터 처리 장치로 구현될 수 있다. 실시 예에 따라, 단말기(300)는 모바일폰(mobile phone) 또는 스마트폰(smart phone)과 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.

[0021] 이하에서는 본 발명에 이용되는 불확정 전송 기법으로서, 2009년 Kurosawa와 Nojima가 제안한 기법에 대해 설명한다. 상기 불확정 전송 기법에서 송신자(100)가 지닌 n 개의 메시지들은 $M_1, \cdots, M_n$ 으로, 수신자(300)가 전송받고자 하는 k 개의 메시지들의 인덱스는 $\sigma_1, \cdots, \sigma_k$로 표현된다. 상기 불확정 전송 기법은 초기 설정 단계와 전송 단계로 구성된다.

[0022] 초기 설정 단계에서, 송신자(100)는 겹선형 군 G를 선택하고 G의 원소 g와 $(Z_q)^{n+1}$의 원소 $(r_1, \cdots, r_n, x)$를 랜덤하게 선택한 후 $h=g^x$를 계산한다. 또한, 송신자(100)는 n 개의 메시지들($M_1, \cdots, M_n$) 각각에 대한 암호문($C_i = (A_i, B_i) = (g^{r_i}, M_i h^{r_i})$, $1 \le i \le n$)을 생성한 후, 수신자(300)에게 $(G, h, C_1, \cdots, C_n)$을 송신한다. 또한, 송신자(100)는 영지식 증명(Zero Knowledge Proof of Knowledge; ZK-PoK)을 통하여 송신자(100)가 x를 알고 있음을 증명하고, 수신자(300)는 이를 검증한다. 검증에 실패하는 경우 불확정 전송 프로토콜의 수행은 중단될 수 있다.

[0023] 전송 단계 중 $i(1 \le i \le k)$ 번째 전송 단계에서, 수신자(300)는 Z_q에서 임의의 값 v를 선택하고, $V = (A_{\sigma_j})^v$를 계산한 후 송신자(100)에게 V를 전송한다. 이 때, 증거 구분불가능 증명(Witness Indistinguishability Proof of Knowledge; WI-PoK)을 통하여, 수신자(300)는 송신자(100)로부터 전송받은 $A_{\sigma_1}, \cdots, A_{\sigma_n}$ 중 하나의 값으로 V를 계산했음을 증명하고, 송신자(100)는 이를 검증할 수 있다. 검증에 실패하는 경우 불확정 전송 프로토콜의 수행은 중단될 수 있다.

[0024] 검증에 통과하면, 송신자(100)는 $U = V^x$를 계산하고, 계산된 U를 수신자(300)에게 송신한다. 또한, 멤버십 형식 증명(Zero Knowledge Proof of Membership; ZK-PoM)을 통하여, 송신자(100)는 (g, h, U, V)가 결정적인 디피-헬만 투플(Dicisional Diffie-Hellman tuple)임을 증명하고, 수신자(300)는 이를 검증한다. 검증

에 실패하는 경우, 불확정 전송 프로토콜의 수행은 중단될 수 있다.

[0025] 검증에 통과하면, 수신자(300)는 $B_{\sigma_i}/U^{\frac{1}{v}}$ 를 계산하여 M_{σ_i}를 얻을 수 있다. 상기와 같은 전송 단계가 k회 반복되면, 수신자는 k 개의 메시지들을 얻을 수 있다.

[0026] 또한, 상기 불확정 전송 기법은 조정(Adaptive) 기능을 제공한다. 조정 기능이란, 수신자가 원하는 k 개의 메시지들을 한 번에 요청하는 것이 아니라 전송 단계를 통해 하나씩 순차적으로 얻을 수 있는 것이다. 이전에 전송받은 메시지를 보고 다음에 얻을 메시지를 선택할 수 있기 때문에, 수신자의 정보 선택 측면에서 효율적이다. 또한, 상기 불확정 전송 기법은 겹선형 함수(bilinear map) 혹은 페어링(pairing)을 사용하지 않기 때문에, 기존에 페어링을 사용한 불확정 전송 기법들에 비해 연산량 측면에서 효율적이다.

[0027] 상기 불확정 전송 기법에 대한 보다 자세한 설명에 관하여는 Kaoru Kurosawa와 Ryo Nomima의 "Simple Adaptive Oblivious Transfer without Random Oracle"가 참조될 수 있다.

[0028] 도 2는 도 1에 도시된 불확정 전송 시스템을 이용한 불확정 전송 방법 중 초기 설정 단계를 설명하기 위한 흐름도이다.

[0029] 도 1과 도 2를 참조하면, 제1 서버(100)는 겹선형 군 G를 선택하고, 겹선형 군 G의 원소, 즉 G의 생성원인 g를 랜덤하게 선택한다. 또한, 제1 서버(100)는, 제1 서버(100)가 가진 n(n은 자연수) 개의 메시지들($M_1, \cdots, M_n$) 각각에 대응하는 n 개의 제1 난수들과 제2 난수(r_1, …, r_n, x)를 랜덤하게 선택한다. n 개의 제1 난수들과 제2 난수(r_1, …, r_n, x)는 $(Z_q)^{n+1}$의 원소이다. n 개의 제1 난수들(r_1, …, r_n) 각각은 n 개의 메시지들($M_1, \cdots, M_n$) 각각을 암호화할 때 이용될 수 있다. 제2 난수(x)는 공개키(pk_S)를 생성할 때 이용되는 제1 서버(100)의 비밀 값이다. 즉, 제1 서버(100)는 선택된 값(g, x)을 이용하여 비밀키(pk_S=(g, $h=g^x$))를 생성한다(S110).

[0030] 제1 서버(100)는 n 개의 메시지들($M_1, \cdots, M_n$) 각각에 대한 암호문 ($C_i = (A_i, B_i) = (g^{r_i}, M_i h^{r_i})$)을 생성한다(1≤i≤n)(S120).

[0031] 영지식 증명(ZK-PoK) 프로토콜이라도 불리는 영지식 증명(ZK-Pok)을 통하여, 제1 서버(100)는 $h=g^x$에 사용된 제2 난수(x)를 제1 서버(100)가 알고 있음을 단말기(300)를 대상으로 증명할 수 있고, 단말기(300)는 제1 서버(100)가 제2 난수(x)를 알고 있음을 검증할 수 있다(S140). 이때, 검증이 실패한 경우, 불확정 전송 프로토콜의 수행은 중단될 수 있다.

[0032] 상기 영지식 증명(ZK-PoK)은 대화형(interactive) 영지식 증명(ZK-PoK) 또는 비대화형(non-interactive) 영지식 증명(ZK-Pok)일 수 있다. 다만, 상기 영지식 증명(ZK-PoK)에는 알려진 여러 방식들이 존재하므로, 이에 대한 자세한 설명은 생략하기로 한다.

[0033] 검증이 성공한 경우, 단말기(300)는 임의의 난수($s \in Z_q$)를 선택한다. 상기 임의의 난수(s)는 단말기(300)의 공개키를 생성하는 과정에서 이용되는 단말기(300)의 비밀값이다. 단말기(300)는 선택된 임의의 난수(s)를 이용하여 공개키($pk_R=g^s$)를 생성한다. 단말기(300)는 생성된 공개키(pk_S)를 제2 서버(500)로 송신할 수 있다(S150).

[0034] 공개키(pk_S)를 수신한 제2 서버(500)는 임의의 난수($a \in Z_q$)를 선택한다. 상기 임의의 난수(a)는 제2 서버(500)의 공개키를 생성하는 과정에서 이용되는 제2 서버(500)의 비밀값이다. 제2 서버(500)는 선택된 임의의 난수(a)를 이용하여 공개키($pk_0=g^a$)를 생성한 후, 생성된 공개키($pk_0=g^a$)를 단말기(300)로 송신한다(S160).

[0035] 도 3은 도 1에 도시된 불확정 전송 시스템을 이용한 불확정 전송 방법 중 전송 단계를 설명하기 위한 흐름도이

다.

[0036] 도 1과 도 3을 참조하면, 도 3은 전송 단계 중 1회의 전송 단계를 도시하고 있으며, 도 3에 도시된 전송 단계가 k회 반복되면, 단말기(300)는 k 개의 메시지들을 얻을 수 있다. 다만, 본 발명이 전송 단계의 반복 횟수에 제한되는 것은 아니며, 실시 예에 따라 단말기(300)는 적어도 하나의 메시지를 얻을 수 있다.

[0037] 수행되는 전송 단계를 i($1 \le i \le k$) 번째 전송 단계라 할 때, i 번째 전송 단계는 다음과 같은 과정을 통하여 수행된다.

[0038] 단말기(300)는 Z_q에 속하는 임의의 값(v)을 선택한 후, 수신받고자 하는 메시지(C_{σ_i})에 대한 값을 다음과 같이 계산한다(S310). 이 때, 해시 함수(H)는 $H: G \rightarrow Z_q$ 와 같이 정의된다.

[0039]
$$V_{i,1} \leftarrow (A_{\sigma_i})^v,\ V_{i,2} \leftarrow A_{\sigma_i} g^{av},\ V_{i,3} \leftarrow g^v,$$
$$V_{i,4} \leftarrow (g^a)^{H(g^v)v},\ V_{i,5} \leftarrow (A_{\sigma_i})^{H(g^{av})vs}$$

[0040] 단말기(300)는 계산된 값들($V_{i,1}, V_{i,2}, V_{i,3}, V_{i,4}, V_{i,5}$)을 제1 서버(100)로 송신한다. 또한, 증거 구분불가능 증명(WI-PoK)을 통하여, 단말기(300)는 제1 서버(100)로부터 수신한 $A_{\sigma_1}, \cdots, A_{\sigma_n}$ 중 하나를 이용하여 $V_{i,1}$ 을 계산하였음을 증명할 수 있고, 제1 서버(100)는 이를 검증할 수 있다(S320). 검증에 실패할 경우, 불확정 전송 프로토콜의 수행은 중단될 수 있다. 상기 증거 구분불가능 증명(WI-PoK)에는 알려진 여러 방식들이 존재하므로, 이에 대한 자세한 설명은 생략하기로 한다.

[0041] 검증에 성공한 경우, 제1 서버(100)는 단말기(300)로부터 수신한 값($V_{i,1}$)과 자신의 비밀 정보(x)를 이용하여 복호화 키($U \leftarrow (V_{i,1})^x$)를 생성한다. 제1 서버(100)는 생성된 복호화 키($U \leftarrow (V_{i,1})^x$)를 단말기(300)로 송신한다(S330). 또한, 멤버십 형식 증명(ZK-PoM)을 통하여, 제1 서버(100)는 (g, h, $V_{i,1}$, U)가 DDH-tuple 임을 증명할 수 있고, 단말기(300)는 이를 검증할 수 있다(S340). 검증에 실패할 경우, 불확정 전송 프로토콜의 수행은 중단될 수 있다. 상기 멤버십 형식 증명(ZK-PoM)에는 알려진 여러 방식들이 존재하므로, 이에 대한 자세한 설명은 생략하기로 한다.

[0042] 검증에 성공한 경우, 단말기(300)는 수신된 복호화 키($U \leftarrow (V_{i,1})^x$)를 이용하여 메시지($M_{\sigma_i} = B_{\sigma_i} / U^{\frac{1}{v}}$)를 얻을 수 있다(S350).

[0043] 도 4는 도 1에 도시된 불확정 전송 시스템을 이용한 불확정 전송 방법 중 추적 단계를 설명하기 위한 흐름도이다. 도 1과 도 4를 참조하여, 추적 단계를 설명하면 다음과 같다.

[0044] 단말기(300)가 수신한 메시지에 대한 추적이 필요한 경우, 제1 서버(100)는 전송 단계에서 단말기(300)로부터 수신한 메시지($V_{i,1}, V_{i,2}, V_{i,3}, V_{i,4}, V_{i,5}$)를 제2 서버(500)로 송신한다(S510).

[0045] 제2 서버(500)는 $V_{i,2}, V_{i,3}$ 을 이용하여, $A'_{\sigma_i} = V_{i,2} / (V_{i,3})^a$ 을 계산한다. 제2 서버(500)는 계산된 값(A'_{σ_i})이 다음의 수학식 1과 수학식 2를 만족하는 경우, A'_{σ_i} 를 단말기(300)가 전송받은 메시지로 결정하고, 추적을 완료할 수 있다(S520).

수학식 1

[0046] $$e(A'_{\sigma_i}, V_{i,4}) = ?e(V_{i,1}, g^{H(V_{i,3})a})$$

수학식 2

[0047] $$e(V_{i,5}, g) = ?e(pk_R, (V_{i,1})^{H((V_{i,3})^a)})$$

[0048] 상기 수학식 1과 상기 수학식 2에서, H()는 해시함수를 의미할 수 있고, 겹선형 함수(Bilinear map)는 $e : G \times G \rightarrow G_T$ 와 같이 정의된다.

[0049] 상기 추적 단계에서, 수학식 1을 통하여 단말기(300)가 동일한 메시지에 대한 값(A_{σ_i})을 사용하여, 복호화 키 생성에 이용되는 $V_{i,1}$ 과 추적 단계에서 쓰이는 $V_{i,2}$ 를 생성하였음을 확인할 수 있다. 즉, 단말기(300)가 메시지를 조작하지 않았음을 확인할 수 있다.

[0050] 또한, 수학식 2를 통하여 단말기(300)로부터 전송받은 메시지를 제1 서버(100)가 위조하지 않았음을 확인할 수 있다. 즉, 제1 서버(100)는 단말기(300)가 전송받지 않은 메시지에 대하여 단말기(300)가 전송받은 것처럼 위조하지 않았음을 확인할 수 있다.

[0051] 또한, 본 발명에 의한 불확정 전송 방법을 이용할 경우, 송신자와 개봉자, 즉 제1 서버(100)와 제2 서버(500)가 공모하더라도 수신자, 즉 단말기(300)의 비밀값(s)에 대한 정보를 얻을 수 없기 때문에 수신자가 전송받지 않은 메시지를 전송받았다고 할 수 없다. 마찬가지로 수신자와 개봉자가 공모하더라도 송신자의 비밀값(x)에 대한 정보를 얻을 수 없기 때문에 수신자가 송신자에게 요청하지 않은 메시지에 대한 정보를 얻을 수 없다.

[0052] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0053] 10 : 불확정 전송 시스템

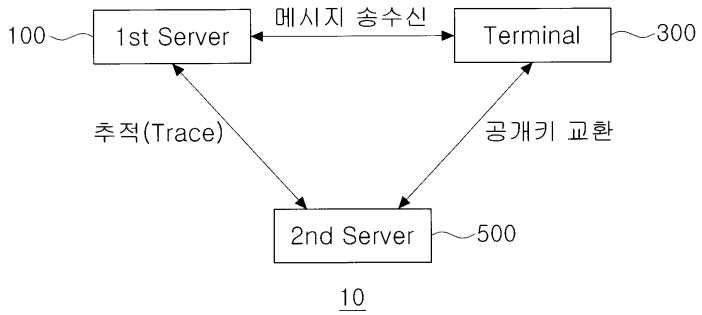
100 : 제1 서버

300 : 단말기

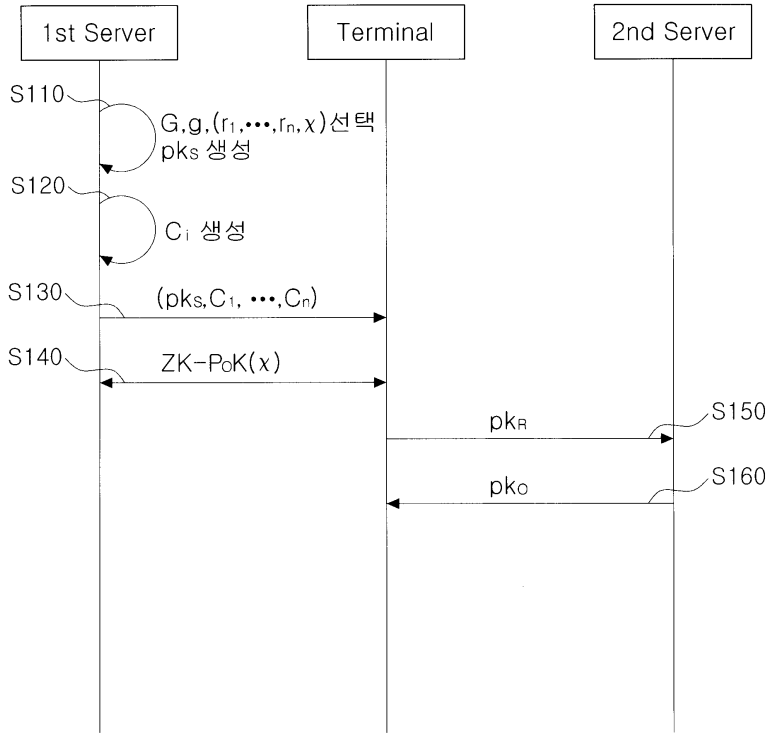
500 : 제2 서버

도면

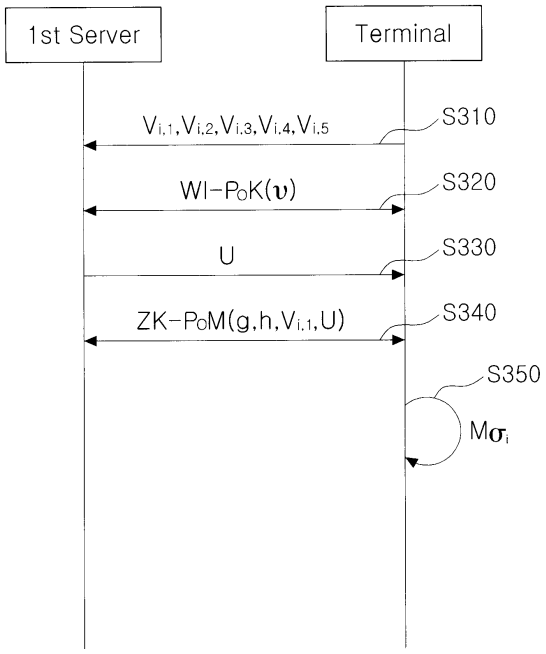
도면1


100
1st Server
메시지 송수신
Terminal
300
추적(Trace)
공개키 교환
2nd Server
500
10

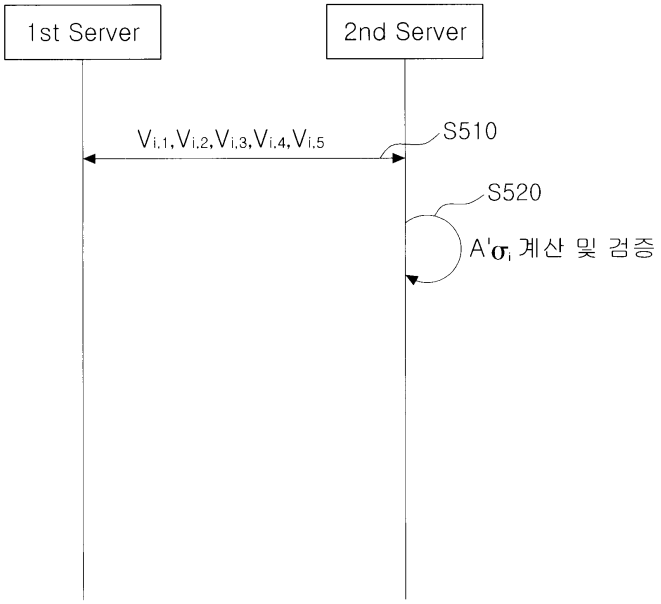
도면2


1st Server
Terminal
2nd Server
S110
G,g,(r1,•••,rn,x)선택
pks 생성
S120
Ci 생성
S130
(pks,C1, •••,Cn)
S140
ZK-PoK(x)
pkR
S150
pko
S160

도면3


1st Server
Terminal
$V_{i,1}, V_{i,2}, V_{i,3}, V_{i,4}, V_{i,5}$
S310
$WI-P_OK(\upsilon)$
S320
U
S330
$ZK-P_OM(g,h,V_{i,1},U)$
S340
S350
$M\sigma_i$

도면4


1st Server
2nd Server
$V_{i,1}, V_{i,2}, V_{i,3}, V_{i,4}, V_{i,5}$
S510
S520
$A'\sigma_i$ 계산 및 검증