(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년08월03일
(11) 등록번호 10-1541165
(24) 등록일자 2015년07월27일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 12/04* (2009.01)
(21) 출원번호 10-2014-0024384
(22) 출원일자 2014년02월28일
심사청구일자 2014년02월28일
(56) 선행기술조사문헌
KR1020090019228 A*
KR1020120108663 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)
백정하
서울 송파구 송파대로32길 15, 105동 802호 (가락동, 가락금호아파트)
(뒷면에 계속)
(74) 대리인
김홍석, 김등용

전체 청구항 수 : 총 11 항 심사관 : 손영태

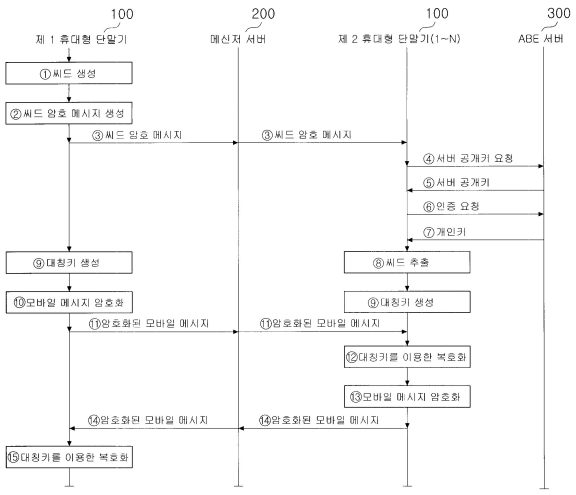
(54) 발명의 명칭 **모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 저장한 다운로드 서버**

(57) 요 약

본 발명은 모바일 메신저를 통해 송수신 되는 모바일 메시지를 속성기반 암호화 기술을 이용하여 암호화하여 지정된 사용자 간에만 모바일 메시지의 판독이 가능하도록 하는, 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버에 관한 것이다.

본 발명을 이용함으로써, 모바일 메시지의 외부 노출을 방지하고 원하는 사용자에게만 암호화된 모바일 메시지의 판독이 가능하도록 한다.

대 표 도 - 도3



(72) 발명자

김순일

서울특별시 동대문구 장한로 14길 81, 105동 1202호(장안동, 레미안장안아파트)

이상혁

서울특별시 마포구 마포대로7길 22, 306동 1302호(공덕동, 삼성래미안공덕3차아파트)

명 세 서

청구범위

청구항 1

(a) ABE(Attribute Based Encryption) 서버로부터 서버 공개키를 제1 휴대형 단말기가 수신하는 단계; 및

(b) 모바일 메신저를 통해 송수신될 모바일 메시지의 암호화에 이용되는 대칭키의 씨드(Seed)를 상기 서버 공개키로 암호화하여 씨드 암호 메시지를 암호화된 모바일 메시지를 수신할 사용자의 속성 정보에 따라 상기 제1 휴대형 단말기가 생성하는 단계;를 포함하고,

상기 씨드 암호 메시지는 모바일 메시지의 암호화에 이용될 대칭키 생성을 위해 상기 모바일 메신저를 통해 제2 휴대형 단말기로 전송되고, 상기 씨드 암호 메시지를 수신한 제2 휴대형 단말기의 사용자의 속성 정보에 따라 상기 씨드 암호 메시지로부터 동일한 씨드가 추출될 수 있는,

모바일 메시지 암호화 방법.

청구항 2

제1항에 있어서,

상기 단계 (b)는 암호화된 상기 모바일 메시지를 복수의 제2 휴대형 단말기에 의해 복호화 가능하게 하는 복수 사용자들의 속성 정보에 따라 상기 씨드 암호 메시지를 생성하고,

상기 모바일 메시지 암호화 방법은,

(c) 상기 씨드 암호 메시지를 상기 모바일 메신저를 통해 상기 복수의 제2 휴대형 단말기로 상기 제1 휴대형 단말기가 전송하는 단계;를 더 포함하는,

모바일 메시지 암호화 방법.

청구항 3

제2항에 있어서,

상기 속성 정보는 상기 복수의 제2 휴대형 단말기의 사용자 각각의 이메일 주소를 포함하는,

모바일 메시지 암호화 방법.

청구항 4

제2항에서 있어서,

상기 씨드 암호 메시지의 수신에 따라 제2 휴대형 단말기에 의해, (f) ABE 서버로부터 수신된 개인키로 상기 제2 휴대형 단말기의 사용자의 속성 정보에 따라 상기 씨드 암호 메시지를 복호화하여 씨드를 추출하는 단계; 및 (g) 추출된 씨드를 이용하여 상기 모바일 메시지의 암호화에 이용될 대칭키를 생성하는 단계;를 더 포함하는,

모바일 메시지 암호화 방법.

청구항 5

제4항에 있어서,

상기 단계 (f) 이전에, 상기 제2 휴대형 단말기에 의해, (d) 상기 ABE 서버로 인증을 요청하는 단계; 및 (e) 상기 인증 요청에 후속하여 상기 제2 휴대형 단말기를 위한 상기 개인키를 수신하는 단계;를 더 포함하는,

모바일 메시지 암호화 방법.

청구항 6

제4항에 있어서,

상기 제2 휴대형 단말기에 의해, (h) 모바일 메시지를 생성된 대칭키로 암호화하는 단계; 및 (i) 암호화된 모바일 메시지를 모바일 메신저를 통해 상기 제1 휴대형 단말기로 전송하는 단계;를 더 포함하는,

모바일 메시지 암호화 방법.

청구항 7

제1항에 있어서,

상기 단계 (a) 및 단계 (b)는 상기 모바일 메신저와 상이한 응용 프로그램에 의해서 수행되고, 상기 응용 프로그램은 URL 스킴(Scheme)에 따라 상기 모바일 메신저로 생성된 상기 씨드 암호 메시지를 전달하는,

모바일 메시지 암호화 방법.

청구항 8

제6항에 있어서,

상기 단계 (h)는 상기 모바일 메신저와 상이한 응용 프로그램에 의해서 수행되고, 상기 응용 프로그램은 암호화된 모바일 메시지를 URL 스킴에 따라 상기 모바일 메신저로 전달하는,

모바일 메시지 암호화 방법.

청구항 9

제5항에 있어서,

상기 단계 (d) 이후에 상기 ABE 서버에 의해, 상기 요청에 포함된 이메일 주소와 패스워드로 사용자를 인증하는 단계; 인증의 결과에 따라 상기 ABE 서버의 마스터키와 이메일 주소를 이용하여 개인키를 생성하는 단계; 및 생성된 개인키를 요청한 제2 휴대형 단말기로 전송하는 단계;를 더 포함하는,

모바일 메시지 암호화 방법.

청구항 10

제1항에 따른 모바일 메시지 암호화 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체.

청구항 11

다운로드 서버로서,

인터넷 망에 연결되기 위한 네트워크 인터페이스; 및

제1항에 따른 모바일 메시지 암호화 방법을 수행하는 프로그램을 저장하는 대용량 저장 매체;를 포함하고,

상기 다운로드 서버는 휴대형 단말기로부터의 상기 인터넷 망을 통한 다운로드 요청에 따라 상기 대용량 저장 매체에 저장된 상기 프로그램을 요청한 휴대형 단말기로 전송하는,

다운로드 서버.

발명의 설명

기 술 분 야

[0001] 본 발명은 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버에 관한 것으로서, 모바일 메신저를 통해 송수신 되는 모바일 메시지를 속성기반 암호화 기술을 이용하여 암호화하여 지정된 사용자 간에만 모바일 메시지의 판독이 가능하도록 하는, 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버에 관한 것이다.

배 경 기 술

[0002] 스마트 폰과 같은 휴대형 단말기를 이용한 모바일 메신저가 일반적으로 활용된다. 이런 모바일 메신저는 1 대 1

대화, N(N은 3 이상)명 간의 그룹 대화가 가능하도록 하고 인터넷 망을 통해서 이루어지며 실시간 대화가 가능하도록 한다.

[0003] 모바일 메신저를 통해서 송수신 되는 모바일 메시지는 필요에 따라 개인적인 중요 정보를 포함할 수 있다. 예를 들어 모바일 메시지는 개인의 주민 번호, 사회 보장 번호, 카드 번호, 계좌 번호 등과 같은 개인의 중요 정보를 포함할 수 있다.

[0004] 인터넷 망을 통한 개인의 중요 정보의 노출은 다양한 문제를 야기할 수 있다. 특히 인터넷 망을 통해 송수신 되는 데이터는 일반적으로 암호화되지 않는 데이터이기에 해킹 될 수 있고 이에 따라 보호될 필요가 있다.

[0005] 인터넷 망을 통한 안전한 메시지 전송을 위해 HTTP(Hyper Text Transfer Protocol) 상에서 수행되는 SSL(Secure Socket layer) 통신을 이용하여 암호화가 추가적으로 이루어질 수 있다. 모바일 메신저와 연동하는 메신저 서버는 대화가 이루어지고 있는 휴대형 단말기들과 각각 SSL 통신 채널을 통해 암호화된 모바일 메시지를 송수신하도록 구성된다.

[0006] 예를 들어, 만일 1 대 1로 휴대형 단말기 간에 대화가 이루어지는 경우에, 메신저 서버는 하나의 휴대형 단말기와 메신저 서버 사이에서 SSL 통신 채널에 이용될 암호화/복호화 키를 생성하고 암/복호화키에 따라 모바일 메시지를 송수신한다. 또한 1 대 1의 상대편인 다른 휴대형 단말기 사이에도 별도의 SSL 통신 채널에 이용될 별도의 암/복호화키에 따라 모바일 메시지를 송수신한다. 이로 인해 메신저 서버는 하나의 SSL 통신 채널을 통해 수신된 모바일 메시지를 복호화하고 다시 다른 SSL 통신 채널을 통해 모바일 메시지를 암호화하여 대화 상대 측의 휴대형 단말기로 전송한다.

[0007] 이런 기존의 SSL 통신을 이용하는 방법은 인터넷 망을 통한 해킹을 방지할 수 있는 반면에 다른 문제점을 노출시킨다. 메신저 서버가 각각의 모바일 메시지를 복호화하고 재차 암호화하기에 메신저 서버가 모바일 메시지 원문(plain text)을 저장하거나 알 수 있는 문제가 발생한다. 이로 인해 휴대형 단말기 사이에서 송수신 되는 개인의 중요 정보가 그대로 메신저 서버에 저장될 수 있고 메신저 서버의 해킹에 따라 또는 메신저 서버의 관리자 등에 의한 모바일 메시지 또는 모바일 메시지의 개인 중요 정보의 유출로 악용될 수 있는 문제가 발생한다.

[0008] 또한 기존의 모바일 메신저는 대화 상대방을 사용자에 의해서 인증할 방법이 존재하지 않고 모바일 메시지를 원치 않는 상대방에게 전송한 경우에 상대방이 이를 확인할 수 있는 문제가 존재한다.

[0009] 이와 같이 기존의 모바일 메신저에서 발생하는 다양한 문제점을 해소할 수 있도록 하는, 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버가 필요하다.

발명의 내용

해결하려는 과제

[0010] 본 발명은, 상술한 문제점을 해결하기 위해서 안출한 것으로서, 모바일 메신저를 이용한 사용자 간 모바일 메시지의 송수신시에 원문이 메신저 서버에 노출되지 않도록 하는 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버를 제공하는 데 그 목적이 있다.

[0011] 또한 본 발명은 모바일 메신저를 이용한 사용자 간 모바일 메시지의 송수신시에 메신저 서버의 관여 없이 모바일 메시지의 암호화에 이용될 대칭키를 생성할 수 있도록 하는 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버를 제공하는 데 그 목적이 있다.

[0012] 또한 본 발명은 지정된 사용자만이 암호화된 모바일 메시지를 복호화할 수 있도록 하는 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버를 제공하는 데 그 목적이 있다.

[0013] 또한 본 발명은 속성기반 암호화 기술을 이용하여 지정된 복수의 사용자에게만 개인키의 발급이 가능하도록 하고 발급된 개인키를 이용하여 모바일 메시지의 복호화가 각 사용자별로 가능하도록 하는 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버를 제공하는 데 그 목적이 있다.

[0014] 또한 본 발명은 복수의 사용자 간의 대화시에 모바일 메시지의 암호화에 이용될 키 교환이 사용자의 수에 상관없이 상수 시간으로 이루어질 수 있도록 하는 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버를 제공하는 데 그 목적이 있다.

[0015] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0016] 상기와 같은 목적을 달성하기 위한, 모바일 메시지 암호화 방법은 (a) ABE(Attribute Based Encryption) 서버로부터 서버 공개키를 수신하는 단계 및 (b) 모바일 메신저를 통해 송수신 될 모바일 메시지의 암호화에 이용되는 대칭키의 씨드(Seed)를 서버 공개키로 암호화하여 씨드 암호 메시지를 생성하는 단계를 포함하고 씨드 암호 메시지는 모바일 메신저를 통해 제2 휴대형 단말기로 전송된다.

[0017] 또한 모바일 메시지 암호화 방법의 단계 (b)는 암호화된 모바일 메시지를 복수의 제2 휴대형 단말기에 의해 복호화 가능하게 하는 속성 정보에 따라 씨드 암호 메시지를 생성하고, 모바일 메시지 암호화 방법은 (c) 씨드 암호 메시지를 모바일 메신저를 통해 복수의 제2 휴대형 단말기로 전송하는 단계를 더 포함한다.

[0018] 또한 속성 정보는 복수의 제2 휴대형 단말기의 사용자 각각의 이메일 주소를 포함한다.

[0019] 또한 모바일 메시지 암호화 방법의 단계 (a) 내지 (c)는 제1 휴대형 단말기에서 수행되고, 모바일 메시지 암호화 방법은 씨드 암호 메시지의 수신에 따라 제2 휴대형 단말기에 의해 (f) ABE 서버로부터 수신된 개인키로 씨드 암호 메시지를 복호화하여 씨드를 추출하는 단계 및 (g) 추출된 씨드를 이용하여 모바일 메시지의 암호화에 이용될 대칭키를 생성하는 단계를 더 포함한다.

[0020] 또한 모바일 메시지 암호화 방법의 단계 (f) 이전에, 모바일 메시지 암호화 방법은 제2 휴대형 단말기에 의해 (d) ABE 서버로 인증을 요청하는 단계 및 (e) 인증 요청에 후속하여 제2 휴대형 단말기를 위한 개인키를 수신하는 단계를 더 포함한다.

[0021] 또한 모바일 메시지 암호화 방법은 제2 휴대형 단말기에 의해 (h) 모바일 메시지를 생성된 대칭키로 암호화하는 단계 및 (i) 암호화된 모바일 메시지를 모바일 메신저를 통해 제1 휴대형 단말기로 전송하는 단계를 더 포함한다.

[0022] 또한 모바일 메시지 암호화 방법의 단계 (a) 및 단계 (b)는 모바일 메신저와 상이한 응용 프로그램에 의해서 수행되고, 응용 프로그램은 URL 스킴(Scheme)에 따라 모바일 메신저로 생성된 씨드 암호 메시지를 전달한다.

[0023] 또한 모바일 메시지 암호화 방법의 단계 (h)는 모바일 메신저와 상이한 응용 프로그램에 의해서 수행되고, 응용 프로그램은 암호화된 모바일 메시지를 URL 스킴에 따라 모바일 메신저로 전달한다.

[0024] 또한 모바일 메시지 암호화 방법은 단계 (d) 이후에 ABE 서버에 의해 요청에 포함된 이메일 주소와 패스워드로 사용자를 인증하는 단계, 인증의 결과에 따라 ABE 서버의 마스터키와 이메일 주소를 이용하여 개인키를 생성하는 단계 및 생성된 개인키를 요청한 제2 휴대형 단말기로 전송하는 단계를 더 포함한다.

[0025] 또한 상기와 같은 목적을 달성하기 위한, 컴퓨터 판독가능 기록매체는 모바일 메시지 암호화 방법을 수행하는 프로그램을 기록하고, 모바일 메시지 암호화 방법은 (a) ABE(Attribute Based Encryption) 서버로부터 서버 공개키를 수신하는 단계 및 (b) 모바일 메신저를 통해 송수신 될 모바일 메시지의 암호화에 이용되는 대칭키의 씨드(Seed)를 서버 공개키로 암호화하여 씨드 암호 메시지를 생성하는 단계를 포함하고 씨드 암호 메시지는 모바일 메신저를 통해 제2 휴대형 단말기로 전송된다.

[0026] 또한 상기와 같은 목적을 달성하기 위한, 다운로드 서버는 모바일 메시지 암호화 방법을 수행하는 프로그램을 저장하고, 모바일 메시지 암호화 방법은 (a) ABE(Attribute Based Encryption) 서버로부터 서버 공개키를 수신하는 단계 및 (b) 모바일 메신저를 통해 송수신 될 모바일 메시지의 암호화에 이용되는 대칭키의 씨드(Seed)를 서버 공개키로 암호화하여 씨드 암호 메시지를 생성하는 단계를 포함하고 씨드 암호 메시지는 모바일 메신저를 통해 제2 휴대형 단말기로 전송된다.

발명의 효과

[0027] 상기와 같은 본 발명에 따른 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버는 모바일 메신저를 이용한 사용자 간 모바일 메시지의 송수신시에 원문이 메신저 서버에 노출되지 않도록 하는 효과가 있다.

[0028] 또한 상기와 같은 본 발명에 따른 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버는 모바일 메신저를 이용한 사용자 간 모바일 메시지의 송수신시에 메신저 서버의 관여 없이 모바일 메시지의 암호화에 이용될 대칭키를 생성할 수 있도록 하는 효과가 있다.

[0029] 또한 상기와 같은 본 발명에 따른 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버는 지정된 사용자만이 암호화된 모바일 메시지를 복호화할 수 있도록 하는 효과가 있다.

[0030] 또한 상기와 같은 본 발명에 따른 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버는 속성기반 암호화 기술을 이용하여 지정된 복수의 사용자에게만 개인키의 발급이 가능하도록 하고 발급된 개인키를 이용하여 모바일 메시지의 복호화가 각 사용자별로 가능하도록 하는 효과가 있다.

[0031] 또한 상기와 같은 본 발명에 따른 모바일 메시지 암호화 방법, 이 방법을 수행하는 프로그램을 기록한 컴퓨터 판독가능 기록매체 및 이 방법을 수행하는 프로그램을 저장한 다운로드 서버는 복수의 사용자 간의 대화시에 모바일 메시지의 암호화에 이용될 키 교환이 사용자의 수에 상관없이 상수 시간으로 이루어질 수 있도록 하는 효과가 있다.

[0032] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0033] 도 1은 모바일 메신저를 통한 암호화된 모바일 메시지를 송수신할 수 있도록 하는 시스템을 도시한 도면이다.

도 2는 ABE 서버와 연동하여 개인키를 획득하기 위한 데이터 흐름을 도시한 도면이다.

도 3은 휴대형 단말기 사이에서 이용될 대칭키 설정과 모바일 메시지의 송수신의 예시적인 데이터 흐름을 도시한 도면이다.

도 4는 휴대형 단말기에 탑재된 프로그램의 구조를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0034] 상술한 목적, 특징 및 장점은 첨부된 도면을 참조하여 상세하게 후술 되어 있는 상세한 설명을 통하여 더욱 명확해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시 예를 상세히 설명하기로 한다.

[0035] 도 1은 모바일 메신저를 통한 암호화된 모바일 메시지를 송수신할 수 있도록 하는 시스템을 도시한 도면이다.

[0036] 도 1에 따르면 본 시스템은 메신저 서버(200), 속성기반 암호화에 기초한 ABE(Attribute Based Encryption) 서버(300), 다운로드 서버(400), 복수의 휴대형 단말기(100) 및 서버(200, 300, 400)와 단말기(100) 사이를 연결하기 위한 인터넷 망(500)을 포함한다.

[0037] 본 시스템의 각 장치들을 간단히 살펴보면, 휴대형 단말기(100)는 사용자 개인이 휴대하는 단말기이다. 휴대형 단말기(100)는 예를 들어 핸드폰, 스마트폰, PDA, 태블릿 PC 등일 수 있다. 휴대형 단말기(100)는 내부에 프로세서와 비휘발성 메모리, 근거리 무선 통신이나 이동 통신망에 접속하기 위한 네트워크 인터페이스, 사용자 입력을 수신하기 위한 입력 인터페이스 및 디스플레이를 적어도 구비한다.

[0038] 또한 휴대형 단말기(100)는 비휘발성 메모리 등에 저장된 각종 프로그램들을 프로세서를 통해 로딩하여 프로그

램을 수행함으로써 사용자가 원하는 기능을 수행할 수 있도록 한다. 이러한 프로그램은 예를 들어 특정 모바일 OS(Operating System) 상에서 수행 될 수 있는 앱(App) 프로그램일 수 있다. 휴대형 단말기(100)는 적어도 모바일 메신저 프로그램(120)(이하 '모바일 메신저'라고도 함.)과 속성 기반 암호화를 위한 대칭키 생성 및 암호화 프로그램(110)을 저장한다. 본 발명과 관련된 프로그램의 구체적인 내용은 도 2 내지 도 4를 통해서 상세히 살펴보도록 한다.

[0039] ABE 서버(300)는 속성기반으로 모바일 메시지의 암호화가 가능하도록 하는 서버이다. ABE 서버(300)는 프로세서와 네트워크 인터페이스와 대용량 저장매체 등을 포함하여 사용자 인증과 각 휴대형 단말기(100)에서 이용될 개인키를 생성하고 전송할 수 있다. 휴대형 단말기(100)로 전송되는 개인키는 모바일 메신저(120)를 통해 송수신되는 모바일 메시지의 암복호화에 이용되는 대칭키 생성에 이용된다. 이 ABE 서버(300)에 관해서는 도 2 및 도 3을 통해서 살펴보도록 한다.

[0040] 다운로드 서버(400)는 휴대형 단말기(100)에서 이용되는 각종 프로그램들을 저장한다. 다운로드 서버(400)는 프로세서, 복수의 프로그램들을 저장하기 위한 하드디스크 등과 같은 대용량 저장 매체 및 인터넷 망(500)에 연결되기 위한 네트워크 인터페이스를 적어도 포함한다.

[0041] 다운로드 서버(400)는 휴대형 단말기(100)와 연동하여 휴대형 단말기(100)로 저장되어 있는 프로그램에 관련된 정보를 인터넷 망(500)을 통해 전송하고 다운로드 요청을 수신할 수 있다. 다운로드 요청의 수신에 따라 다운로드 서버(400)는 요청된 특정 프로그램을 휴대형 단말기(100)로 전송할 수 있다. 다운로드 서버(400)는 적어도 본 발명에 따른 모바일 메시지 암호화 방법(아래의 도 2 및 3 참조)을 수행하기 위한 프로그램을 저장하며 휴대형 단말기(100)로부터의 이 프로그램의 다운로드 요청의 수신에 따라 대용량 저장 매체로부터 로딩하여 요청한 휴대형 단말기(100)로 전송한다.

[0042] 메신저 서버(200)는 휴대형 단말기(100)에 탑재된 모바일 메신저(120)와 연동하여 휴대형 단말기(100) 간 모바일 메시지를 저장하고 전송할 수 있는 서버이다. 메신저 서버(200)는 SSL 통신을 통해 각 휴대형 단말기(100)로(부터)의 모바일 메시지를 암호화하고 복호화할 수 있다.

[0043] 한편 본 발명에 따라 암호화된 모바일 메시지는 메신저 서버(200)와 별도로 암호화될 수 있다. 이에 따라 메신저 서버(200)는 이 모바일 메시지를 복호화할 수 없도록 구성된다. 이로 인해 메신저 서버(200)에 임시로 저장되는 모바일 메시지는 판독 불가능하게 구성되고 개인의 중요 정보의 외부 노출로부터 보호될 수 있다. 본 발명과 관련된 메신저 서버(200)에 대해서는 도 3을 통해서 좀 더 살펴보도록 한다.

[0044] 인터넷 망(500)은 복수의 휴대형 단말기(100), 메신저 서버(200), ABE 서버(300) 및 다운로드 서버(400) 사이의 데이터를 인터넷(IP) 프로토콜에 기반하여 송수신한다. 인터넷 망(500)은 유선 망 및/또는 무선 망으로 구성될 수 있다. 또한 인터넷 망(500)은 특정 이동통신 사업자에 의해서 제공되는 이동통신망을 포함할 수 있다.

[0045] 도 2는 ABE 서버와 연동하여 개인키를 획득하기 위한 데이터 흐름을 도시한 도면이다. 도 2에 따른 데이터 흐름은 휴대형 단말기(100)와 ABE 서버(300) 사이의 요청과 요청에 따른 데이터 전송으로 이루어진다.

[0046] 도 2에 따른 데이터 흐름을 살펴보면, 먼저 ABE 서버(300)는 서버 공개키(Ksub)와 서버 마스터키(Kmaster)를 생성(도 2의 ① 참조)한다. 서버 공개키는 휴대형 단말기(100) 사이에서의 씨드(Seed) 공유에 이용되고 서버 마스키는 암호화된 씨드를 복호화하기 위한 휴대형 단말기(100)의 개인키 생성에 이용된다.

[0047] 이후 휴대형 단말기(100)는 모바일 메신저(120)를 통해 송수신될 모바일 메시지를 암호화 하기 위해 서버 공개키를 요청(도 2의 ② 참조)한다.

[0048] 서버 공개키의 요청을 수신한 ABE 서버(300)는 생성된 서버 공개키를 요청한 휴대형 단말기(100)로 전송(도 2의 ③ 참조)한다. 이와 같이 전송된 서버 공개키는 이후 휴대형 단말기(100)와 ABE 서버(300) 사이의 데이터 통신시에 데이터 암호화에 이용될 수 있다. 또한 서버 공개키는 휴대형 단말기(100) 간 모바일 메신저(120)를 통한 모바일 메시지의 송수신시에 이용될 대칭키의 씨드 암호화에 이용될 수 있다.

[0049] 이후 휴대형 단말기(100)는 ABE 서버(300)로 사용자 인증을 요청(도 2의 ④ 참조)한다. 이 인증 요청은 사용자 ID(Identification), 사용자 속성 및 인증에 이용될 패스워드를 포함하고 인증 요청의 데이터들은 서버 공개키로 암호화된다.

[0050] 여기서 사용자 ID와 사용자 속성은 동일할 수 있고 휴대형 단말기(100)를 이용하는 사용자의 이메일 주소를 나

타낼 수 있고 패스워드는 이메일 주소를 통해 로그인 시 이용되는 패스워드일 수 있다. 사용자 ID와 사용자 속성이 동일한 경우에는 사용자 ID나 사용자 속성 중 하나는 생략될 수 있다.

[0051] 이러한 인증 요청을 수신한 ABE 서버(300)는 인증 요청에 포함된 이메일 주소와 패스워드로 사용자를 인증한다. 이를 위해 ABE 서버(300)는 이메일 서버(도면 미도시)로 이메일 주소와 패스워드를 전달하여 사용자가 이메일 주소에 대한 접근 권한이 있는지를 나타내는 인증 결과를 수신할 수 있다. 또는 ABE 서버(300) 내에 저장되어 있는 복수의 이메일 주소와 대응하는 패스워드를 수신된 이메일 주소와 패스워드와 비교하여 이메일 주소에 대한 접근 권한이 있는 지를 나타내는 인증 결과를 생성한다.

[0052] ABE 서버(300)는 인증 결과에 따라 수신된 사용자 속성(이메일 주소)과 이미 생성된 서버 마스터키를 이용하여 휴대형 단말기(100) 사용자를 위한 개인키(Kpriv)를 생성한다.

[0053] 이후 ABE 서버(300)는 생성된 개인키를 인증 요청한 휴대형 단말기(100)로 전송하고 휴대형 단말기(100)는 이를 수신(도 2의 ⑤ 참조)한다.

[0054] 이와 같은 도 2의 데이터 흐름에 의해서 모바일 메신저(120)를 이용하여 모바일 메시지를 송수신할 휴대형 단말기(100)들은 서버의 공개키와 각 휴대형 단말기(100) 사용자 개인의 개인키를 획득할 수 있다.

[0055] 속성 기반 암호화 알고리즘은 지정된 속성에 따라 암복호화가 가능하도록 하는 알고리즘이다. 속성 기반 암호화 알고리즘은 셋업 과정으로서 서버의 공개키와 서버의 마스터키 생성 과정, 특정 속성에 대응하는 비밀키인 개인키를 생성하는 키 생성 과정, 서버의 공개키로 지정된 속성 정보에 따라 복호화 가능하도록 하는 암호문(메시지)를 생성하는 과정 및 암호문을 개인키를 이용하여 복호화하는 과정으로 이루어진다.

[0056] 본 발명에 따라, ABE 서버(300)는 서버의 공개키와 마스터키를 생성하고 개인키를 생성하며, 휴대형 단말기(100)에 의해서 암호 메시지(특히 씨드를 포함하는 암호 메시지)를 생성하고 또한 이 암호 메시지를 각각의 개인키를 이용하여 복호화하도록 구성된다.

[0057] 도 2에 따른 데이터 흐름은 적어도 휴대형 단말기(100)에 서버의 공개키를 제공할 수 있도록 하고 또한 인증된 사용자만을 위한 개인키를 획득가능하도록 한다. 또한 이 데이터 흐름은 모바일 메시지의 암호화가 필요한 시점(예를 들어 사용자를 통한 암호화 요청)에 발생할 수 있다. 이 도 2의 데이터 흐름의 적용 사례를 아래의 도 3을 통해서 살펴보도록 한다.

[0058] 도 3은 휴대형 단말기 사이에서 이용될 대칭키 설정과 모바일 메시지의 송수신의 예시적인 데이터 흐름을 도시한 도면이다.

[0059] 휴대형 단말기(100)의 사용자는 모바일 메신저(120)를 통해 여러 다른 사용자와 채팅이나 대화를 모바일 메시지의 송수신으로 수행할 수 있다. 필요에 따라 특정 하나의 휴대형 단말기(100)의 사용자는 휴대형 단말기(100)에 구비된 입력 인터페이스를 통해 이후 송수신되는 모바일 메시지를 암호화하도록 요청한다.

[0060] 암호화 요청을 수신한 휴대형 단말기(100)(이하 '제1 휴대형 단말기'라 함.)는 ABE 서버(300)와 연동하여 서버 공개키와 나아가 개인키를 수신(도 2 참조)한다.

[0061] 또한 제1 휴대형 단말기(100)는 기존의 모바일 메신저(120)를 통해 이후 송수신 되고 동적으로 생성된 대칭키를 이용하여 암호화될 모바일 메시지에 대한 한 명 이상의 상대방 선택을 입력 인터페이스를 통해 수신한다. 이러한 상대방 측의 선택은 대화 상대방의 ID를 결정할 수 있다. 대화 상대방의 ID는 예를 들어 이메일 주소일 수 있다.

[0062] 제1 휴대형 단말기(100)는 대칭키 생성에 이용될 씨드를 생성(도 3의 ① 참조)한다. 생성된 씨드는 예를 들어 제1 휴대형 단말기(100)에서 무작위(random)로 선택된 숫자, 문자 또는 숫자와 문자의 조합일 수 있다. 생성된 씨드는 모바일 메신저(120)를 통해 대화 상대방 측과 송수신되는 모바일 메시지의 암호화에 이용되는 대칭키를 생성할 수 있도록 한다.

[0063] 이후 제1 휴대형 단말기(100)는 생성된 씨드를 서버 공개키로 암호화하여 암호 메시지(이하 '씨드 암호 메시지'라 함.)를 생성(도 3의 ② 참조)한다. 이와 같이 생성된 씨드 암호 메시지는 접근 정책에 따른 속성 정보에 따라서 생성된다. 속성 정보는 대화 상대방의 ID를 포함하고 바람직하게는 대화 상대방의 이메일 주소를 포함한다.

[0064] 따라서 제1 휴대형 단말기(100)가 복수의 휴대형 단말기(100)(이하 '제2 휴대형 단말기'라 함)와 대화를 하고자 하는 경우에는 제1 휴대형 단말기(100)는 복수의 제2 휴대형 단말기(100)가 암호화된 모바일 메시지의 복호화가 가능하도록 선택된 상대방의 이메일 주소(속성)에 따른 접근 정책에 따라 씨드 암호 메시지를 생성한다.

[0065] 이후 제1 휴대형 단말기(100)는 씨드 암호 메시지를 메신저 서버(200)로 전송하고 메신저 서버(200)는 다시 지정된 하나 혹은 복수의 제2 휴대형 단말기(100)로 씨드 암호 메시지를 전송(도 3의 ③ 참조)한다. 이 과정에서 SSL 통신이 메신저 서버(200)와 휴대형 단말기(100) 각각 간에 이루어질 수 있다.

[0066] 씨드 암호 메시지를 수신한 제2 휴대형 단말기(100)는 개인키를 획득한다. 예를 들어 제2 휴대형 단말기(100)는 씨드 암호 메시지의 수신에 따라 혹은 씨드 암호 메시지 수신 이전에 제1 휴대형 단말기(100)를 통한 개인키 획득 요청에 따라, ABE 서버(300)로 서버 공개키를 요청(도 3의 ④ 참조)하고 서버 공개키를 수신(도 3의 ⑤ 참조)하고 인증 요청(도 3의 ⑥ 참조)하고 개인키를 수신(도 3의 ⑦ 참조)한다. 이러한 개인키 획득 과정은 도 2의 데이터 흐름과 동일하여 그 상세한 설명을 생략한다.

[0067] 개인키를 획득한 제2 휴대형 단말기(100)는 씨드 암호 메시지를 ABE 서버(300)로부터 수신된 개인키로 복호화하여 씨드를 추출(도 3의 ⑧ 참조)한다. 만일 씨드 암호 메시지가 이 제2 휴대형 단말기(100)에 대해서 복호화 가능하도록 구성(예를 들어 제2 휴대형 단말기(100)의 사용자의 이메일 주소)되었다면 정상적으로 동일한 씨드를 추출할 수 있을 것이다. 만일 동일한 씨드를 추출할 수 없다면 대화 세션(session, 또는 채널)을 끊도록 구성하거나 비록 암호화된 모바일 메시지가 전송된다 하더라도 복호화가 불가능할 것이다.

[0068] 이후 제1 휴대형 단말기(100)와 하나 혹은 복수의 제2 휴대형 단말기(100)는 씨드를 이용하여 동일한 대칭키를 생성(도 3의 ⑨ 참조)한다. 대칭키는 암호화된 대화 세션의 생성시에 동적으로 생성되는 암복호화키일 수 있고 예를 들어 AES 암호화 알고리즘에 이용되는 비밀키일 수 있다.

[0069] 씨드 암호 메시지는 기존의 모바일 메신저(120)를 통해 메신저 서버(200)를 거쳐 하나 또는 복수의 제2 휴대형 단말기(100)로 동시에 전송(도 3의 ③ 참조)될 수 있다.

[0070] 이후 모바일 메시지의 암호화를 시작 요청한 제1 휴대형 단말기(100)와 이를 대칭키 생성을 통해 수락한 복수의 제2 휴대형 단말기(100)는 암호화된 모바일 메시지를 서로서로 송수신할 수 있다.

[0071] 이러한 대칭키 공유는 메신저 서버(200)의 관여 없이 이루어지고 비록 메신저 서버(200)를 통해 모바일 메시지가 송수신 되더라도 메신저 서버(200)에서 평문(plain text)으로 복호화될 수가 없어 중요한 개인 정보를 보호할 수 있다. 또한 대칭키가 암호화된 사용자간 대화 세션 생성시에 동적으로 생성되기에 해킹을 어렵게 한다.

[0072] 예를 들어, 제1 휴대형 단말기(100)는 대화 세션을 통해 연결된 복수의 제2 휴대형 단말기(100)로 전송할 모바일 메시지를 대칭키를 이용하여 암호화(도 3의 ⑩ 참조)한다.

[0073] 이후 제1 휴대형 단말기(100)는 암호화된 모바일 메시지를 메신저 서버(200)를 통해 대화 세션으로 연결된 복수의 제2 휴대형 단말기(100)로 전송(도 3의 ⑪ 참조)한다.

[0074] 암호화된 모바일 메시지를 수신한 제2 휴대형 단말기(100)는 씨드를 통해 생성된 대칭키를 이용하여 복호화(도 3의 ⑫ 참조)하고 제2 휴대형 단말기(100)의 디스플레이에 표시한다.

[0075] 마찬가지로, 제2 휴대형 단말기(100)는 입력 인터페이스를 통해 사용자 입력을 수신하고 모바일 메시지를 생성한다. 또한 모바일 메시지를 대칭키를 이용하여 암호화(도 3의 ⑬ 참조)한다.

[0076] 이후 제2 휴대형 단말기(100)는 암호화된 모바일 메시지를 메신저 서버(200)를 통해 제1 휴대형 단말기(100)로 전송(도 3의 ⑭ 참조)한다.

[0077] 암호화된 모바일 메시지를 수신한 제1 휴대형 단말기(100)는 대칭키를 이용하여 복호화(도 3의 ⑮ 참조)하고 복호화된 모바일 메시지를 디스플레이에 표시한다.

[0078] 제1 휴대형 단말기(100)와 복수의 제2 휴대형 단말기(100)는 동일한 대칭키를 이용하여 서로 모바일 메시지의 암호화와 복호화가 가능하고 서로서로 외부에 노출되기를 원치 않는 대화가 가능하도록 한다.

[0079] 또한 씨드가 하나의 휴대형 단말기(100)에서 생성되고 이를 다른 휴대형 단말기(100)가 공유하기에 메신저 서버(200)나 ABE 서버(300)에 의한 대화 내용의 노출을 불가능하게 할 수 있다.

[0080] 또한 씨드가 대화 상대방의 모든 휴대형 단말기(100)로 동시에 전송되고 휴대형 단말기(100) 측에서 대칭키 생성이 발생하여 인터넷을 통한 별도의 데이터 통신의 발생을 방지할 수 있다.

[0081] 도 2 및 도 3의 데이터 흐름은 프로그램으로 구성될 수 있다. 예를 들어 도 2 및 도 3의 데이터 흐름은 휴대형 단말기(100)에서 이루어지는 흐름을 수행하기 위한 응용 프로그램으로 구성될 수 있다. 이러한 응용 프로그램은 USB 메모리, DVD, CD, SD 카드 등과 같은 컴퓨터 판독가능 기록매체에 기록될 수 있다. 또는 이 응용 프로그램은 다운로드 서버(400)에 저장될 수 있다.

[0082] 도 4는 휴대형 단말기에 탑재된 프로그램의 구조를 도시한 도면이다. 도 4에 따르면 본 발명에 따른 모바일 메시지 암호화 방법을 수행하기 위한 프로그램은 대칭키 생성 및 암호화 프로그램(110)과 모바일 메신저 프로그램(120)을 포함한다. 이러한 프로그램은 스마트폰에서 수행되는 앱 프로그램일 수 있고 비휘발성 메모리 등에 저장될 수 있다.

[0083] 모바일 메신저 프로그램(120)은 메신저 서버(200)와 연동하여 지정된 상대방과 대화가 이루어지도록 모바일 메시지를 송수신할 수 있는 프로그램이다. 이러한 모바일 메신저 프로그램(120)은 인터넷 망(500)을 통해 메신저 서버(200)와 모바일 메시지를 송신하고 수신하며 이를 디스플레이하도록 구성된다.

[0084] 한편, 모바일 메신저 프로그램(120)은 다른 프로그램과 연동하기 위한 프로그램 인터페이스를 제공한다. 이러한 프로그램 인터페이스는 약속된 포맷으로 구성되고 예를 들어 URL(Uniform Resource Locator) 스킴(scheme)을 통해서 이루어질 수 있다. 이에 따라 모바일 메신저 프로그램(120)은 URL 스킴을 통해 다른 응용 프로그램을 구동하거나 다른 응용 프로그램에 특정 정보나 메시지를 전달하고 수신할 수 있다.

[0085] 대칭키 생성 및 암호화 프로그램(110)은 대칭키를 생성하고 모바일 메시지를 암호화할 수 있도록 하는 프로그램이다. 대칭키 생성 및 암호화 프로그램(110)은 URL 스킴을 통해 모바일 메신저(120)를 통해 전송할 암호화된 모바일 메시지를 전송하고 수신할 수 있도록 구성된다.

[0086] 대칭키 생성 및 암호화 프로그램(110)은 서버의 공개키와 개인키를 수신하도록 메신저 서버(200) 경유 없이 직접 ABE 서버(300)와 연동(도 2 참조)할 수 있고, 씨드 생성, 씨드 암호 메시지 생성, 대칭키 생성, 모바일 메시지 암호화, 대칭키를 이용한 복호화 및 디스플레이를 수행(도 3의 ③ ⑪ ⑭를 제외한 데이터 흐름)할 수 있다.

[0087] 따라서 대칭키 생성 및 암호화 프로그램(110)은 모바일 메신저(120)를 통한 모바일 메시지의 송수신을 제외하고 휴대형 단말기(100) 간 암호화와 복호화에 관련된 작업(task)를 수행하며, 휴대형 단말기(100) 간에 인식가능한 URL 스킴에 따른 메시지를 모바일 메신저(120)를 통해 송수신할 수 있다.

[0088] 예를 들어 대칭키 생성 및 암호화 프로그램(110)은 URL 스킴을 이용하여 모바일 메신저(120)로 씨드 암호 메시지를 전달하고 모바일 메신저(120)는 메신저 서버(200)를 거쳐 상대 측 휴대형 단말기(100)로 전송한다. 씨드 암호 메시지를 수신한 휴대형 단말기(100)의 모바일 메신저(120)는 수신된 URL 스킴에 따른 이미지를 디스플레이한다. 이후 이미지의 사용자 선택에 따라 대칭키 생성 및 암호화 프로그램(110)을 호출하여 씨드를 추출할 수 있다.

[0089] 또한 대칭키 생성 및 암호화 프로그램(110)은 사용자 입력에 따른 모바일 메시지를 암호화하고 URL 스킴에 따라 모바일 메신저(120)로 전달하고 모바일 메신저(120)는 메신저 서버(200)를 거쳐 휴대형 단말기(100)로 전송한다. URL 스킴에 따라 암호화된 모바일 메시지를 수신한 휴대형 단말기(100)의 모바일 메신저(120)는 수신된 URL 스킴에 따른 이미지를 디스플레이한다. 이후 이미지의 사용자의 선택에 따라 대칭키 생성 및 암호화 프로그램(110)을 호출하여 암호화된 모바일 메시지를 복호화하고 원래의 모바일 메시지를 디스플레이할 수 있다.

[0090] 도 4에서는 모바일 메신저 프로그램(120)과 대칭키 생성 및 암호화 프로그램(110)이 휴대형 단말기(100)에 별도로 존재하는 것으로 설명하였다. 이에 국한될 필요는 없으며 대칭키 생성 및 암호화 프로그램(110)이 모바일 메신저 프로그램(120) 내에 내장될 수 있다. 이때에는 URL 스킴을 이용하지 않을 수도 있고 직접 모바일 메신저(120)가 복호화 등을 수행하고 이를 디스플레이할 수 있다.

[0091] 모바일 메신저 프로그램(120)과 대칭키 생성 및 암호화 프로그램(110)을 분리함으로써 모바일 메신저에 원문이 노출되지 않아 모바일 메시지의 기밀성을 극대화시킬 수 있다.

[0092] 모바일 메신저 프로그램(120) 내에 대칭키 생성 및 암호화 프로그램(110)이 내장되는 경우에도, 적어도 메신저 서버(200)와 ABE 서버(300)를 분리 구성하는 것이 메신저 서버(200)에 메시지를 노출할 수 없도록 하여 바람직하다.

[0093] 대칭키 생성 및 암호화 프로그램(110)을 통해 송수신 되는 모바일 메시지는 약속된 포맷에 따라 구성될 수

있다. 예를 들어 모바일 메시지는 URL 스킴에 따라 타입(메시지 타입 : 예를 들어 대칭키 생성을 위한 씨드 암호 메시지 타입, 대칭키 생성 후의 암호화된 모바일 메시지 타입), 채팅(또는 대화)방 ID, 모바일 메시지의 송신자 ID(예를 들어 이메일 주소), 데이터 등을 구별하기 위한 각각의 파라미터 이름과, 각 파라미터에 대응하는 데이터나 값들을 포함할 수 있다. 데이터 파라미터에 대응하는 데이터는 예를 들어 타입에 따라 씨드 암호 메시지나 암호화된 모바일 메시지를 포함할 수 있다.

[0094] 이러한 약속된 URL 스킴의 포맷에 따라, 휴대형 단말기(100)는 대칭키 생성을 위한 대화 세션의 대칭키 생성 과정인지 이후 대칭키 생성 후의 과정인지를 식별할 수 있고 이에 따라 대칭키를 생성하거나 대칭키를 이용하여 암호화 및 복호화를 수행할 수 있다.

[0095] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시 예 및 첨부된 도면에 의해 한정되는 것이 아니다.

부호의 설명

[0096] 100 : 휴대형 단말기

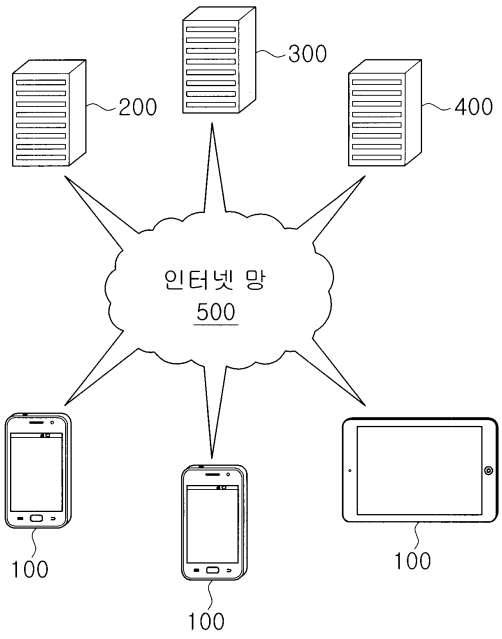
110 : 대칭키 생성 및 암호화 프로그램 120 : 모바일 메신저 프로그램

200 : 메신저 서버 300 : ABE 서버

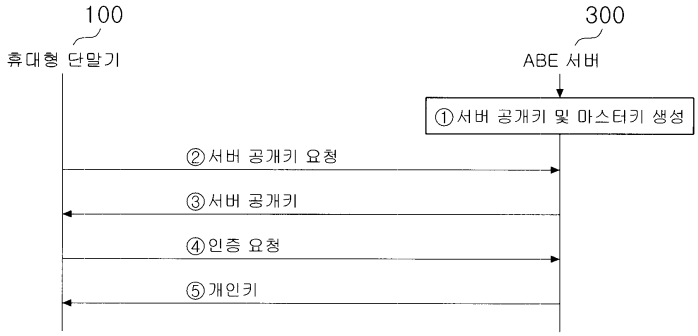
400 : 다운로드 서버 500 : 인터넷 망

도면

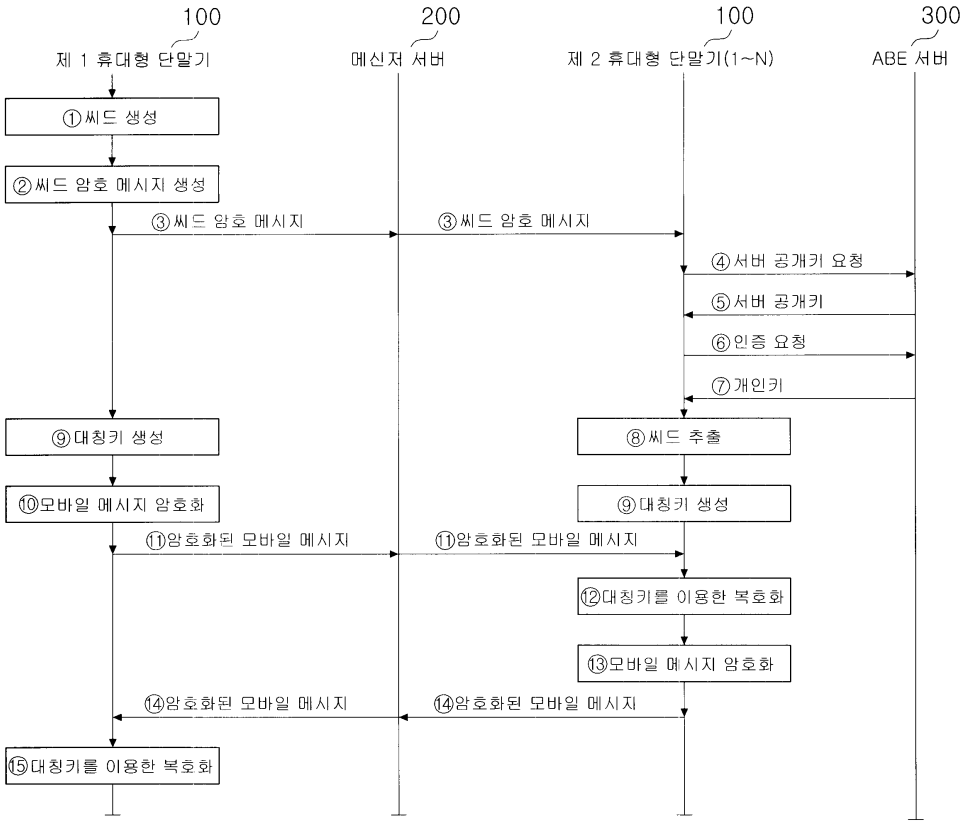
도면1



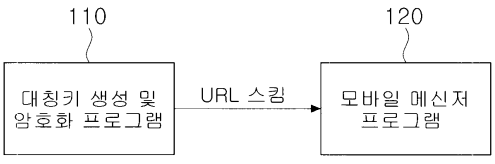
도면2


100
휴대형 단말기
300
ABE 서버
①서버 공개키 및 마스터키 생성
②서버 공개키 요청
③서버 공개키
④인증 요청
⑤개인키

도면3


100
제 1 휴대형 단말기
200
메신저 서버
100
제 2 휴대형 단말기(1~N)
300
ABE 서버
①씨드 생성
②씨드 암호 메시지 생성
③씨드 암호 메시지
③씨드 암호 메시지
④서버 공개키 요청
⑤서버 공개키
⑥인증 요청
⑦개인키
⑨대칭키 생성
⑧씨드 추출
⑩모바일 메시지 암호화
⑨대칭키 생성
⑪암호화된 모바일 메시지
⑪암호화된 모바일 메시지
⑫대칭키를 이용한 복호화
⑬모바일 메시지 암호화
⑭암호화된 모바일 메시지
⑭암호화된 모바일 메시지
⑮대칭키를 이용한 복호화

도면4


110
대칭키 생성 및
암호화 프로그램
URL 스킴
120
모바일 메신저
프로그램