(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0108663
(43) 공개일자 2012년10월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
G06K 9/18 (2006.01) *H04W 4/12* (2009.01)
(21) 출원번호 10-2011-0026836
(22) 출원일자 2011년03월25일
심사청구일자 2011년03월25일

(71) 출원인
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
인천광역시 남구 인하로 100, 인하대학교 하이테크센터 317호 (용현동)
(74) 대리인
특허법인무한

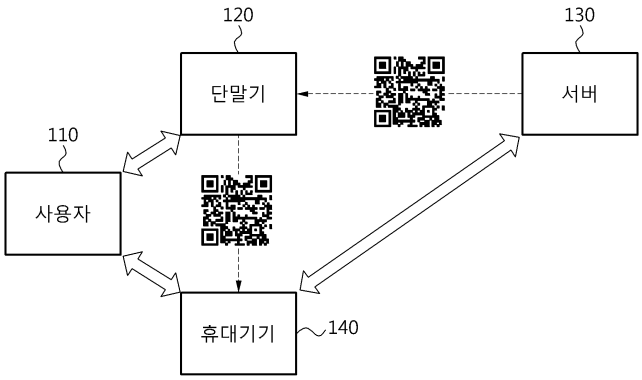
전체 청구항 수 : 총 26 항

(54) 발명의 명칭 **안전한 디지털 정보의 전달을 위한 데이터 전송 시스템, 데이터 전송 방법, 데이터 해독 시스템 및 데이터 해독 방법**

(57) 요 약

안전한 디지털 정보의 전달을 위한 데이터 전송 시스템, 데이터 전송 방법, 데이터 해독 시스템 및 데이터 해독 방법이 개시된다. 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템은 사용자의 공개키를 수신 및 유지하는 공개키 수신부, 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부, 수신된 사용자의 공개키로 메시지를 암호화하는 암호화부, 암호화된 메시지를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부 및 생성된 다차원 코드를 사용자에게 제공하는 다차원 코드 제공부를 포함한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고, 다차원 코드는 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 다차원 코드에서 암호화된 메시지가 추출되고, 사용자의 비밀키를 통해 암호화된 메시지가 복호화되어 메시지가 추출된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서,

상기 사용자의 공개키를 수신 및 유지하는 공개키 수신부;

상기 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부;

상기 수신된 사용자의 공개키로 상기 메시지를 암호화하는 암호화부;

상기 암호화된 메시지를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 다차원 코드 제공부

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 암호화된 메시지가 추출되고, 상기 사용자의 비밀키를 통해 상기 암호화된 메시지가 복호화되어 상기 메시지가 추출되는, 메시지 전송 시스템.

청구항 2

제1항에 있어서,

상기 사용자에게 제공하기 위한 메시지의 크기가 기선정된 크기 이상이 경우,

상기 암호화부는,

임의의 대칭키로 상기 메시지를, 상기 사용자의 공개키로 상기 대칭키를 각각 암호화하고,

상기 다차원 코드 생성부는,

상기 대칭키로 암호화된 메시지와 상기 사용자의 공개키로 암호화된 대칭키를 포함하는 다차원 코드를 생성하는, 메시지 전송 시스템.

청구항 3

제2항에 있어서,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 대칭키로 암호화된 메시지 및 상기 사용자의 공개키로 암호화된 대칭키가 추출되고,

상기 사용자의 비밀키를 통해 상기 사용자의 공개키로 암호화된 대칭키가 복호화되어 상기 대칭키가 추출되며, 상기 추출된 대칭키를 통해 상기 대칭키로 암호화된 메시지가 복호화되어 상기 메시지가 추출되는, 메시지 전송 시스템.

청구항 4

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서,

공개키 및 비밀키를 생성하는 키 생성부;

상기 생성된 공개키를 사용자에게 제공하는 공개키 제공부;

상기 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부;

상기 생성된 비밀키로 상기 메시지를 서명하여 서명된 메시지를 생성하는 메시지 서명부;

상기 서명된 메시지를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 다차원 코드 제공부

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 서명된 메시지가 추출되고, 상기 사용자에게 제공된 공개키를 통해 상기 서명된 메시지가 서명검증되는, 메시지 전송 시스템.

청구항 5

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서,

공개키 및 비밀키를 생성하는 키 생성부;

상기 생성된 공개키를 사용자에게 제공하는 공개키 제공부;

상기 사용자의 공개키를 수신하는 공개키 수신부;

상기 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부;

상기 생성된 비밀키로 상기 메시지를 서명하여 서명된 메시지를 생성하는 메시지 서명부;

상기 사용자의 공개키로 상기 서명된 메시지를 암호화하는 암호화부;

상기 암호화된 메시지를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 다차원 코드 제공부

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 암호화된 메시지가 추출되고, 상기 사용자의 비밀키를 통해 상기 암호화된 메시지가 복호화되어 상기 서명된 메시지가 추출되고, 상기 사용자에게 제공된 공개키를 통해 상기 서명된 메시지가 서명검증되는, 메시지 전송 시스템.

청구항 6

제5항에 있어서,

상기 서명된 메시지의 크기가 기선정된 크기 이상이 경우,

상기 암호화부는,

임의의 대칭키로 상기 서명된 메시지를, 상기 사용자의 공개키로 상기 대칭키를 각각 암호화하고,

상기 다차원 코드 생성부는,

상기 대칭키로 암호화된 서명된 메시지 및 상기 사용자의 공개키로 암호화된 대칭키를 포함하는 다차원 코드를 생성하는, 메시지 전송 시스템.

청구항 7

제6항에 있어서,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 대칭키로 암호화된 서명된 메시지 및 상기 사용자의 공개키로 암호화된 대칭키가 추출되고,

상기 사용자의 비밀키를 통해 상기 사용자의 공개키로 암호화된 대칭키가 복호화되어 상기 대칭키가 추출되며, 상기 추출된 대칭키를 통해 상기 대칭키로 암호화된 서명된 메시지가 복호화되어 서명된 메시지가 추출되고, 상

기 사용자에게 제공된 공개키를 통해 상기 서명된 메시지가 서명검증되는, 메시지 전송 시스템.

청구항 8

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서,

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부;

상기 다차원 코드에서 사용자의 공개키로 암호화된 메시지를 추출하는 메시지 추출부; 및

상기 사용자의 공개키로 암호화된 메시지를 상기 사용자의 비밀키로 복호화하여 상기 메시지를 추출하는 복호화부

를 포함하고,

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버에서 상기 메시지가 상기 사용자의 공개키로 암호화되고, 상기 암호화된 메시지를 포함하는 상기 다차원 코드가 생성되는, 메시지 해독 시스템.

청구항 9

제8항에 있어서,

상기 사용자에게 제공하기 위한 메시지의 크기가 기선정된 크기 이상이 경우,

상기 서버에서 임의의 대칭키로 상기 메시지가, 상기 사용자의 공개키로 상기 대칭키가 각각 암호화되고, 상기 대칭키로 암호화된 메시지와 상기 사용자의 공개키로 암호화된 대칭키를 포함하는 다차원 코드가 생성되는, 메시지 해독 시스템.

청구항 10

제9항에 있어서,

상기 메시지 추출부는,

상기 다차원 코드에서 상기 대칭키로 암호화된 메시지와 상기 사용자의 공개키로 암호화된 대칭키를 추출하고,

상기 복호화부는,

상기 사용자의 공개키로 암호화된 대칭키를 상기 사용자의 비밀키로 복호화하여 대칭키를 추출하고, 상기 대칭키로 암호화된 메시지를 상기 대칭키로 복호화하여 상기 메시지를 추출하는, 메시지 해독 시스템.

청구항 11

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서,

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 상기 서버의 공개키를 수신하는 공개키 수신부;

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부;

상기 다차원 코드에서 상기 서버의 비밀키로 서명된 메시지를 추출하는 메시지 추출부; 및

상기 서버의 공개키로 상기 서명된 메시지를 서명검증하는 서명검증부

를 포함하고,

상기 서버에서 상기 메시지가 상기 서버의 비밀키로 서명되고, 상기 서명된 비밀키를 포함하는 상기 다차원 코드가 생성되는, 메시지 해독 시스템.

청구항 12

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서,

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 상기 서버의 공개키를 수신하는 공개키 수신부;

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부;

상기 다차원 코드에서 상기 서버의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지를 추출하는 메시지 추출부; 및

상기 추출된 메시지를 상기 사용자의 비밀키로 복호화하여 서명된 메시지를 추출하고, 상기 서명된 메시지를 상기 서버의 공개키로 서명검증하는 인증부

를 포함하고,

상기 서버에서 상기 서버의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지를 포함하는 상기 다차원 코드가 생성되는, 메시지 해독 시스템.

청구항 13

제12항에 있어서,

상기 서명된 메시지의 크기가 기선정된 크기 이상이 경우, 상기 서버에서 임의의 대칭키로 상기 서명된 메시지가, 상기 사용자의 공개키로 상기 대칭키가 각각 암호화되고, 상기 대칭키로 암호화된 서명된 메시지와 상기 사용자의 공개키로 암호화된 대칭키를 포함하는 다차원 코드가 생성되는, 메시지 해독 시스템.

청구항 14

제13항에 있어서,

상기 메시지 추출부는,

상기 다차원 코드에서 상기 대칭키로 암호화된 서명된 메시지와 상기 사용자의 공개키로 암호화된 대칭키를 추출하고,

상기 복호화부는,

상기 사용자의 공개키로 암호화된 대칭키를 상기 사용자의 비밀키로 복호화하여 대칭키를 추출하고, 상기 대칭키로 암호화된 서명된 메시지를 상기 대칭키로 복호화하여 상기 서명된 메시지를 추출하고, 상기 서버의 공개키로 상기 서명된 메시지를 서명검증하는, 메시지 해독 시스템.

청구항 15

제8항, 제11항 또는 제12항 중 어느 한 항에 있어서,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 수신되어 상기 단말기의 디스플레이를 통해 표시되는, 메시지 해독 시스템.

청구항 16

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서,

상기 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부;

휴대기기와 미리 공유된 암호용 대칭키로 상기 메시지를 암호화하여 암호화된 메시지를 생성하거나 상기 휴대기기와 미리 공유된 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드를 생성하거나 또는 상기 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드를 생성한 후 상기 메시지 인증 코드를 상기 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드를 생성하는 암호화부;

상기 암호화된 메시지, 상기 메시지 인증 코드 또는 상기 암호화된 메시지 인증 코드를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 다차원 코드 제공부

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케

이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 다차원 코드에서 상기 암호화된 메시지, 상기 메시지 인증 코드 또는 상기 암호화된 메시지 인증 코드가 추출되고, 상기 암호용 대칭키로 상기 암호화된 메시지가 복호화되거나 상기 인증용 대칭키로 상기 메시지 인증 코드가 검증되거나 또는 상기 암호용 대칭키로 상기 암호화된 메시지 인증 코드가 복호화된 후 상기 인증용 대칭키로 상기 메시지 인증 코드가 검증되는, 메시지 전송 시스템.

청구항 17

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서,

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부;

상기 다차원 코드에서 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드를 추출하는 메시지 추출부; 및

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버와 미리 공유된 암호용 대칭키로 상기 암호화된 메시지를 복호화하거나 상기 서버와 미리 공유된 인증용 대칭키로 상기 메시지 인증 코드를 검증하거나 또는 상기 암호용 대칭키로 상기 암호화된 메시지 인증 코드를 복호화한 후 상기 인증용 대칭키로 상기 복호화된 메시지 인증 코드를 검증하는 메시지 처리부

를 포함하고,

상기 서버에서 상기 암호용 대칭키로 상기 메시지가 암호화되어 상기 암호화된 메시지가 생성되거나 상기 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드가 생성되거나 또는 상기 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드가 생성된 후 상기 메시지 인증 코드를 상기 암호용 대칭키로 암호화하여 상기 암호화된 메시지 인증 코드가 생성되는, 메시지 해독 시스템.

청구항 18

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 방법에 있어서,

상기 사용자의 공개키를 수신 및 유지하는 단계;

상기 사용자에게 제공하기 위한 메시지를 수신하는 단계;

상기 수신된 사용자의 공개키로 상기 메시지를 암호화하는 단계;

상기 암호화된 메시지를 포함하는 다차원 코드를 생성하는 단계; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 단계

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 암호화된 메시지가 추출되고, 상기 사용자의 비밀키를 통해 상기 암호화된 메시지가 복호화되어 상기 메시지가 추출되는, 메시지 전송 방법.

청구항 19

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 방법에 있어서,

공개키 및 비밀키를 생성하는 단계;

상기 생성된 공개키를 사용자에게 제공하는 단계;

상기 사용자에게 제공하기 위한 메시지를 수신하는 단계;

상기 생성된 비밀키로 상기 메시지를 서명하여 서명된 메시지를 생성하는 단계;

상기 서명된 메시지를 포함하는 다차원 코드를 생성하는 단계; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 단계

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 서명된 메시지가 추출되고, 상기 사용자에게 제공된 공개키를 통해 상기 서명된 메시지가 서명검증되는, 메시지 전송 방법.

청구항 20

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 방법에 있어서,

공개키 및 비밀키를 생성하는 단계;

상기 생성된 공개키를 사용자에게 제공하는 단계;

상기 사용자의 공개키를 수신하는 단계;

상기 사용자에게 제공하기 위한 메시지를 수신하는 단계;

상기 생성된 비밀키로 상기 메시지를 서명하여 서명된 메시지를 생성하는 단계;

상기 사용자의 공개키로 상기 서명된 메시지를 암호화하는 단계;

상기 암호화된 메시지를 포함하는 다차원 코드를 생성하는 단계; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 단계

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 상기 암호화된 메시지가 추출되고, 상기 사용자의 비밀키를 통해 상기 암호화된 메시지가 복호화되어 상기 서명된 메시지가 추출되고, 상기 사용자에게 제공된 공개키를 통해 상기 서명된 메시지가 서명검증되는, 메시지 전송 방법.

청구항 21

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 방법에 있어서,

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계;

상기 다차원 코드에서 사용자의 공개키로 암호화된 메시지를 추출하는 단계; 및

상기 사용자의 공개키로 암호화된 메시지를 상기 사용자의 비밀키로 복호화하여 상기 메시지를 추출하는 단계

를 포함하고,

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버에서 상기 메시지가 상기 사용자의 공개키로 암호화되고, 상기 암호화된 메시지를 포함하는 상기 다차원 코드가 생성되는, 메시지 해독 방법.

청구항 22

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 방법에 있어서,

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 상기 서버의 공개키를 수신하는 단계;

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계;

상기 다차원 코드에서 상기 서버의 비밀키로 서명된 메시지를 추출하는 단계; 및

상기 서버의 공개키로 상기 서명된 메시지를 서명검증하는 단계

를 포함하고,

상기 서버에서 상기 메시지가 상기 서버의 비밀키로 서명되고, 상기 서명된 비밀키를 포함하는 상기 다차원 코드가 생성되는, 메시지 해독 방법.

청구항 23

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 방법에 있어서,

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 상기 서버의 공개키를 수신하는 단계;

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계;

상기 다차원 코드에서 상기 서버의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지를 추출하는 단계;

상기 추출된 메시지를 상기 사용자의 비밀키로 복호화하여 서명된 메시지를 추출하고, 상기 서명된 메시지를 상기 서버의 공개키로 서명검증하는 단계

를 포함하고,

상기 서버에서 상기 서버의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지를 포함하는 상기 다차원 코드가 생성되는, 메시지 해독 방법.

청구항 24

전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 방법에 있어서,

상기 사용자에게 제공하기 위한 메시지를 수신하는 단계;

휴대기기와 미리 공유된 암호용 대칭키로 상기 메시지를 암호화하거나 상기 휴대기기와 미리 공유된 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드를 생성하거나 또는 상기 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드를 생성한 후 상기 메시지 인증 코드를 상기 암호용 대칭키로 암호화하여 암호화된 메시지를 생성하는 단계;

상기 암호화된 메시지를 포함하는 다차원 코드를 생성하는 단계; 및

상기 생성된 다차원 코드를 상기 사용자에게 제공하는 단계

를 포함하고,

상기 생성된 다차원 코드는 상기 사용자의 전자메일 계정 또는 상기 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 상기 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고,

상기 다차원 코드는 상기 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 상기 다차원 코드에서 다차원 코드에서 상기 암호화된 메시지가 추출되고, 상기 암호용 대칭키로 상기 암호화된 메시지가 복호화되거나 상기 인증용 대칭키로 상기 메시지 인증 코드가 검증되거나 또는 상기 암호용 대칭키로 상기 암호화된 메시지가 복호화된 후 상기 인증용 대칭키로 상기 메시지 인증 코드가 검증되는, 메시지 전송 방법.

청구항 25

전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 방법에 있어서,

카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 단계;

상기 다차원 코드에서 사용자의 공개키로 암호화된 메시지를 추출하는 단계; 및

상기 전자메일 또는 상기 인스턴트 메시징에 대한 서비스를 제공하는 서버와 미리 공유된 암호용 대칭키로 상기 암호화된 메시지를 복호화하거나 상기 서버와 미리 공유된 인증용 대칭키로 상기 메시지 인증 코드를 검증하거나 또는 상기 암호용 대칭키로 상기 암호화된 메시지 인증 코드를 복호화한 후 상기 인증용 대칭키로 상기 복호

화된 메시지 인증 코드를 검증하는 단계

를 포함하고,

상기 서버에서 상기 암호용 대칭키로 상기 메시지가 암호화되어 상기 암호화된 메시지가 생성되거나 상기 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드가 생성되거나 또는 상기 인증용 대칭키로 상기 메시지에 대한 메시지 인증 코드가 생성된 후 상기 메시지 인증 코드를 상기 암호용 대칭키로 암호화하여 상기 암호화된 메시지 인증 코드가 생성되는, 메시지 해독 방법.

청구항 26

제18항 내지 제25항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

명 세 서

기 술 분 야

[0001] 본 발명의 실시예들은 안전한 디지털 정보의 전달을 위한 데이터 전송 시스템, 데이터 전송 방법, 데이터 해독 시스템 및 데이터 해독 방법에 관한 것이다.

배 경 기 술

[0002] 전자메일은 컴퓨터 통신망을 이용하여 컴퓨터 사용자 간에 편지나 여러 정보를 주고받는 개인 통신방법을 의미하고, 인스턴트 메시징은 사용자가 메신저 서버에 접속되어 있을 때, 착신 메시지를 사용 중인 개인용 컴퓨터(PC) 화면에 표시해서 이것을 받은 사용자는 곧 반송할 수 있는 서비스를 의미한다. 이러한 전자메일과 인스턴트 메시징은 통신망을 통해 다른 사용자와 전화고 싶은 내용이나 자료 등의 디지털 정보를 편리하게 주고 받을 수 있는 서비스이다.

[0003] 본 명세서에서는 안전하게 디지털 정보를 전달할 수 있는 시스템 및 방법이 제공된다.

발명의 내용

해결하려는 과제

[0004] 전자메일 또는 인스턴트 메시징을 위한 메시지를 QR 코드와 같은 다차원 코드를 이용하여 휴대기기로 전송할 수 있는 시스템 및 방법이 제공된다.

[0005] 사용자의 공개키와 비밀키 또는 사용자의 휴대기기와 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버간에 미리 공유된 암호용/인증용 대칭키, 그리고 다차원 코드를 이용하여 전자메일 또는 인스턴트 메시징을 위한 메시지를 안전하게 전달할 수 있는 시스템 및 방법이 제공된다.

과제의 해결 수단

[0006] 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서, 사용자의 공개키를 수신 및 유지하는 공개키 수신부, 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부, 수신된 사용자의 공개키로 메시지를 암호화하는 암호화부, 암호화된 메시지를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부 및 생성된 다차원 코드를 사용자에게 제공하는 다차원 코드 제공부를 포함하고, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고, 다차원 코드는 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 다차원 코드에서 암호화된 메시지가 추출되고, 사용자의 비밀키를 통해 암호화된 메시지가 복호화되어 메시지가 추출되는, 메시지 전송 시스템이 제공된다.

[0007] 일측에 따르면, 사용자에게 제공하기 위한 메시지의 크기가 기선정된 크기 이상이 경우, 암호화부는 임의의 대칭키로 메시지를, 사용자의 공개키로 대칭키를 각각 암호화할 수 있고, 다차원 코드 생성부는 대칭키로 암호화된 메시지와 사용자의 공개키로 암호화된 대칭키를 포함하는 다차원 코드를 생성할 수 있다. 이 경우, 다차원 코드는 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 다차원 코드에서 대칭키로 암호화된 메시지 및 사용자의 공개키로 암호화된 대칭키가 추출될 수 있고, 사용자의 비밀키를 통해 사용자의 공개키로 암호화된 대칭키가 복호화되어 대칭키가 추출되며, 추출된 대칭키를 통해 대칭키로 암호화된 메시지가 복호화되어

메시지가 추출될 수 있다.

[0008] 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서, 공개키 및 비밀키를 생성하는 키 생성부, 생성된 공개키를 사용자에게 제공하는 공개키 제공부, 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부, 생성된 비밀키로 메시지를 서명하여 서명된 메시지를 생성하는 메시지 서명부, 서명된 메시지를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부 및 생성된 다차원 코드를 사용자에게 제공하는 다차원 코드 제공부를 포함하고, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고, 다차원 코드는 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 다차원 코드에서 서명된 메시지가 추출되고, 사용자에게 제공된 공개키를 통해 서명된 메시지가 서명검증되는, 메시지 전송 시스템이 제공된다.

[0009] 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서, 공개키 및 비밀키를 생성하는 키 생성부, 생성된 공개키를 사용자에게 제공하는 공개키 제공부, 사용자의 공개키를 수신하는 공개키 수신부, 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부, 생성된 비밀키로 메시지를 서명하여 서명된 메시지를 생성하는 메시지 서명부, 사용자의 공개키로 서명된 메시지를 암호화하는 암호화부, 암호화된 메시지를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부 및 생성된 다차원 코드를 사용자에게 제공하는 다차원 코드 제공부를 포함하고, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고, 다차원 코드는 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 다차원 코드에서 암호화된 메시지가 추출되고, 사용자의 비밀키를 통해 암호화된 메시지가 복호화되어 서명된 메시지가 추출되고, 사용자에게 제공된 공개키를 통해 서명된 메시지가 서명검증되는, 메시지 전송 시스템이 제공된다.

[0010] 전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서, 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부, 다차원 코드에서 사용자의 공개키로 암호화된 메시지를 추출하는 메시지 추출부 및 사용자의 공개키로 암호화된 메시지를 사용자의 비밀키로 복호화하여 메시지를 추출하는 복호화부를 포함하고, 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버에서 메시지가 사용자의 공개키로 암호화되고, 암호화된 메시지를 포함하는 다차원 코드가 생성되는, 메시지 해독 시스템이 제공된다.

[0011] 전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서, 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 서버의 공개키를 수신하는 공개키 수신부, 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부, 다차원 코드에서 서버의 비밀키로 서명된 메시지를 추출하는 메시지 추출부 및 서버의 공개키로 서명된 메시지를 서명검증하는 서명검증부를 포함하고, 서버에서 메시지가 서버의 비밀키로 서명되고, 서명된 비밀키를 포함하는 다차원 코드가 생성되는, 메시지 해독 시스템이 제공된다.

[0012] 전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서, 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 서버의 공개키를 수신하는 공개키 수신부, 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부, 다차원 코드에서 서버의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지를 추출하는 메시지 추출부 및 추출된 메시지를 사용자의 비밀키로 복호화하여 서명된 메시지를 추출하고, 서명된 메시지를 서버의 공개키로 서명검증하는 인증부를 포함하고, 서버에서 서버의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지를 포함하는 다차원 코드가 생성되는, 메시지 해독 시스템이 제공된다.

[0013] 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템에 있어서, 사용자에게 제공하기 위한 메시지를 수신하는 메시지 수신부, 휴대기기와 미리 공유된 암호용 대칭키로 메시지를 암호화하여 암호화된 메시지를 생성하거나 휴대기기와 미리 공유된 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성하거나 또는 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성한 후 메시지 인증 코드를 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드를 생성하는 암호화부, 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드를 포함하는 다차원 코드를 생성하는 다차원 코드 생성부 및 생성된 다차원 코드를 사용자에게 제공하는 다차원 코드 제공부를 포함하고, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공되어 디스플레이를 통해 표시되고, 다차원 코드는 사용자의 휴대기기에 포함된 카메라를 통해 입력 및 인식되어, 다차원 코드에서 다차원 코드에서 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드가 추출되고, 암호용 대칭키로 암호화

된 메시지가 복호화되거나 인증용 대칭키로 메시지 인증 코드가 검증되거나 또는 암호용 대칭키로 암호화된 메시지 인증 코드가 복호화된 후 인증용 대칭키로 메시지 인증 코드가 검증되는, 메시지 전송 시스템이 제공된다.

[0014] 전자메일 또는 인스턴트 메시징을 위한 메시지를 해독하는 메시지 해독 시스템에 있어서, 카메라를 통해 입력된 이미지에서 다차원 코드를 인식하는 다차원 코드 인식부, 다차원 코드에서 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드를 추출하는 메시지 추출부 및 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버와 미리 공유된 암호용 대칭키로 암호화된 메시지를 복호화하거나 서버와 미리 공유된 인증용 대칭키로 메시지 인증 코드를 검증하거나 또는 암호용 대칭키로 암호화된 메시지 인증 코드를 복호화한 후 인증용 대칭키로 복호화된 메시지 인증 코드를 검증하는 메시지 처리부를 포함하고, 서버에서 암호용 대칭키로 메시지가 암호화되어 암호화된 메시지가 생성되거나 인증용 대칭키로 메시지에 대한 메시지 인증 코드가 생성되거나 또는 인증용 대칭키로 메시지에 대한 메시지 인증 코드가 생성된 후 메시지 인증 코드를 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드가 생성되는, 메시지 해독 시스템이 제공된다.

발명의 효과

[0015] 전자메일 또는 인스턴트 메시징을 위한 메시지를 QR 코드와 같은 다차원 코드를 이용하여 휴대기기로 전송할 수 있다.

[0016] 사용자의 공개키와 비밀키 또는 사용자의 휴대기기와 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버간에 미리 공유된 암호용/인증용 대칭키, 그리고 다차원 코드를 이용하여 전자메일 또는 인스턴트 메시징을 위한 메시지를 안전하게 전달할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시예들에 있어서, 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하기 위한 전체적인 시스템 구조를 나타낸 도면이다.

도 2 내지 도 5는 본 발명의 실시예들에 있어서, 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템 및 메시지를 해독하는 메시지 해독 시스템의 내부 구성을 각각 설명하기 위한 블록도들이다.

도 6 내지 도 11은 본 발명의 실시예들에 있어서, 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 방법 및 메시지를 해독하는 메시지 해독 방법을 도시한 흐름도들이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0019] 도 1은 본 발명의 실시예들에 있어서, 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하기 위한 전체적인 시스템 구조를 나타낸 도면이다. 도 1은 사용자(110), 단말기(120), 서버(130) 및 휴대기기(140)를 나타내고 있다. 여기서, 단말기(120)는 PC나 노트북과 같이 사용자(110)가 서버(130)에서 전자메일 계정을 통해 제공하거나 또는 인스턴트 메시징을 위한 어플리케이션을 통해 제공된 메시지를 수신하여 사용자(110)에게 제공하는 시스템을 의미할 수 있고, 서버(130)는 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 전자메일 시스템이나 인스턴트 메시징 시스템을 의미할 수 있다. 또한, 서버(130)는 전자메일 또는 인스턴트 메시징에 따른 메시지를 사용자(110)에게 제공하기 위한 주체일 수도 있다. 예를 들어, 서버(130)는 이메일 청구서와 같은 메시지를 제 3자에게 노출되지 않도록 사용자(110)의 전자메일 계정을 통해 전달하고자 하는 시스템일 수 있다. 이때, 어플리케이션은 단말기(120)에 설치되어 동작될 수 있다. 또한, 휴대기기(140)는 카메라를 포함하는 휴대용 장치를 의미할 수 있다.

[0020] 이때, 사용자(110)에 의해 단말기(120) 또는 휴대기기(140)에서 생성된 공개키/비밀키 쌍을 <pku, pru>라 하자. 이때, 공개키는 다른 사람에게 알려지는 키이다.

[0021] 이때, 서버(130)에서 전자메일이나 또는 인스턴트 메시징을 위한 메시지가 사용자(110)에게 전송될 수 있다. 이 경우, 서버(130)는 사용자(110)에게 전달하기 위한 메시지가 제 3자에게 노출되지 않도록 하기 위해 또는 메시지의 무결성을 보장하기 위해, 메시지를 암호화하거나 또는 메시지에 대한 메시지 인증 코드를 생성하여 사용자(110)에게 제공할 수 있다. 이때, 암호화된 메시지나 메시지 인증 코드의 전달에 QR 코드와 같은 다차원 코드가 이용될 수 있다.

[0022] 일실시예로, 서버(130)는 사용자(110)의 공개키를 이용하여 사용자(110)에게 전송하고자 하는 메시지 'M'을 암호화할 수 있다. 즉, 사용자(110)에 의해 단말기(120) 또는 휴대기기(140)에서 공개키/비밀키 쌍인 <pku, pru>가 생성되면, 단말기(120) 또는 휴대기기(140)에서 생성된 공개키 "pku"가 서버(130)로 전송될 수 있다. 서버(130)는 메시지 'M'을 공개키 "pku"로 암호화하여 암호화된 메시지 "$Enc_{pku}(M)$"를 생성할 수 있다. 또한, 서버(130)는 암호화된 메시지 "$Enc_{pku}(M)$"를 포함하는 다차원 코드를 생성하여 사용자(110)에게 제공할 수 있다. 예를 들어, 서버(130)는 사용자(110)의 전자메일 계정으로 다차원 코드가 포함된 메일을 발송하거나 또는 단말기(120)에 설치된 어플리케이션을 통해 단말기(120)로 다차원 코드를 전송할 수 있다.

[0023] 이 경우, 사용자(110)는 단말기(120)를 통해 전자메일 계정으로 발송된 다차원 코드를 획득하거나 어플리케이션을 통해 다차원 코드를 획득할 수 있게 된다. 단말기(120)로 다차원 코드가 수신되면, 단말기(120)는 단말기(120)의 디스플레이를 통해 다차원 코드를 표시할 수 있다. 사용자(110)는 휴대기기(140)의 카메라를 이용하여 다차원 코드가 표시된 디스플레이에서 다차원 코드를 포함하는 이미지를 촬영함으로써, 다차원 코드가 포함된 이미지가 휴대기기로 입력되도록 할 수 있다. 이때, 휴대기기(140)는 입력된 이미지에서 다차원 코드를 추출하고, 다차원 코드를 인식하여 다차원 코드에서 암호화된 메시지 "$Enc_{pku}(M)$"를 추출할 수 있다. 또한, 휴대기기(140)는 사용자(110)의 비밀키 'pru'를 이용하여 암호화된 메시지 "$Enc_{pku}(M)$"를 복호화함으로써, 메시지 'M'을 얻을 수 있다. 이때, 휴대기기(140)는 복호화된 메시지 'M'을 휴대기기(140)의 디스플레이를 통해 표시하여 사용자(110)에게 제공할 수 있고, 사용자(110)는 표시된 메시지 'M'을 확인할 수 있게 된다.

[0024] 만약, 메시지 'M'의 크기가 기선정된 크기 이상인 경우, 서버(130)는 임의의 대칭키 'k'를 통해 메시지 'M'을 암호화하여 암호화된 메시지 '$Enc_k(M)$'를 생성할 수 있다. 여기서, 기선정된 크기는 일례로 다차원 코드에 포함될 수 있는 데이터의 크기를 포함할 수 있다. 또한, 서버(130)는 대칭키 'k'를 사용자의 공개키 "pku"로 암호화하여 암호화된 대칭키 '$Enc_{pku}(k)$'를 생성할 수 있다. 이때, 서버(130)는 암호화된 메시지 '$Enc_k(M)$'와 암호화된 대칭키 '$Enc_{pku}(k)$'를 모두 포함하는 다차원 코드를 생성하여 사용자(110)에게 제공할 수 있다. 예를 들어, 서버(130)는 사용자(110)의 전자메일 계정으로 다차원 코드가 포함된 메일을 발송하거나 또는 단말기(120)에 설치된 어플리케이션을 통해 단말기(120)로 다차원 코드를 전송할 수 있다.

[0025] 이 경우, 사용자(110)는 단말기(120)를 통해 전자메일 계정으로 발송된 다차원 코드를 획득하거나 어플리케이션을 통해 다차원 코드를 획득할 수 있게 된다. 단말기(120)에 다차원 코드가 수신되면, 다차원 코드는 단말기(120)의 디스플레이를 통해 표시될 수 있다. 사용자(110)는 휴대기기(140)의 카메라를 이용하여 다차원 코드를 포함하는 이미지가 휴대기기로 입력되도록 할 수 있고, 휴대기기(140)는 입력된 이미지에서 다차원 코드를 추출하고, 다차원 코드를 인식하여 다차원 코드에서 대칭키로 암호화된 메시지 '$Enc_k(M)$'와 암호화된 대칭키 '$Enc_{pku}(k)$'를 추출할 수 있다. 이때, 휴대기기(140)는 사용자(110)의 비밀키 'pru'를 이용하여 암호화된 대칭키 '$Enc_{pku}(k)$'를 복호화함으로써, 대칭키 'k'를 얻을 수 있고, 암호화된 메시지 '$Enc_k(M)$'를 대칭키 'k'로 복호화함으로써, 메시지 'M'을 얻을 수 있다.

[0026] 다른 실시예에서는 서버(130)의 공개키/비밀키 쌍인 <pks, prs>가 이용될 수 있다. 우선, 서버(130)는 서버(130)의 비밀키 'prs'를 이용하여 메시지 'M'을 서명하여 서명된 메시지 '$Sign_{prs}(M)$'를 생성할 수 있다. 이러한 서명된 메시지 '$Sign_{prs}(M)$'는 메시지 인증 코드로서 이용될 수 있다. 또한, 서버(130)는 서명된 메시지 '$Sign_{prs}(M)$'를 포함하는 다차원 코드를 생성하여 사용자에게 제공할 수 있다. 예를 들어, 서버(130)는 사용자(110)의 전자메일 계정으로 다차원 코드가 포함된 메일을 발송하거나 또는 단말기(120)에 설치된 어플리케이션을 통해 단말기(120)로 다차원 코드를 전송할 수 있다.

[0027] 이 경우, 사용자(110)는 단말기(120)를 통해 전자메일 계정으로 발송된 다차원 코드를 획득하거나 어플리케이션을 통해 다차원 코드를 획득할 수 있게 된다. 단말기(120)에 다차원 코드가 수신되면, 다차원 코드는 단말기(120)의 디스플레이를 통해 표시될 수 있다. 사용자(110)는 휴대기기(140)의 카메라를 이용하여 다차원 코드를 포함하는 이미지가 휴대기기로 입력되도록 할 수 있고, 휴대기기(140)는 입력된 이미지에서 다차원 코드를 추출하고, 다차원 코드를 인식하여 다차원 코드에서 서명된 메시지 '$Sign_{prs}(M)$'를 추출할 수 있다. 이때, 휴대기기(140)는 서버(130)의 공개키 'pks'를 이용하여 서명된 메시지 '$Sign_{prs}(M)$'를 서명검증함으로써, 메시지 'M'의 무결성을 확보할 수 있다.

[0028] 또 다른 실시예에서는 사용자(110)의 공개키/비밀키 쌍인 <pku, pru>와 서버(130)의 공개키/비밀키 쌍인 <pks, prs>가 모두 이용될 수 있다. 우선, 서버(130)는 서버(130)의 비밀키 'prs'를 이용하여 메시지 'M'을 서명하여 서명된 메시지 '$Sign_{prs}(M)$'를 생성할 수 있다. 이러한 서명된 메시지 이때, 서버(130)는 사용자의 공개키 'pku'를 이용하여 서명된 메시지 '$Sign_{prs}(M)$'를 암호화하여 암호화된 메시지 '$Enc_{pku}(M||S)$'를 생성할 수 있다. 여기서, 'S'는 서명된 메시지 '$Sign_{prs}(M)$'를 의미할 수 있다. 이 경우, 서버(130)는 암호화된 메시지 '$Enc_{pku}(M||S)$'를 포함하는 다차원 코드를 생성하여 사용자(110)에게 제공할 수 있다. 예를 들어, 서버(130)는 사용자(110)의 전자메일 계정으로 다차원 코드가 포함된 메일을 발송하거나 또는 단말기(120)에 설치된 어플리케이션을 통해 단말기(120)로 다차원 코드를 전송할 수 있다.

[0029] 사용자(110)는 단말기(120)를 통해 전자메일 계정으로 발송된 다차원 코드를 획득하거나 어플리케이션을 통해 다차원 코드를 획득할 수 있게 된다. 단말기(120)에 다차원 코드가 수신되면, 다차원 코드는 단말기(120)의 디스플레이를 통해 표시될 수 있다. 사용자(110)는 휴대기기(140)의 카메라를 이용하여 다차원 코드를 포함하는 이미지가 휴대기기로 입력되도록 할 수 있고, 휴대기기(140)는 입력된 이미지에서 다차원 코드를 추출하고, 다차원 코드를 인식하여 다차원 코드에서 암호화된 메시지 '$Enc_{pku}(M||S)$'를 추출할 수 있다. 이때, 휴대기기(140)는 사용자(110)의 공개키 'pku'를 이용하여 암호화된 메시지 '$Enc_{pku}(M||S)$'를 복호화함으로써, 서명된 메시지 '$Sign_{prs}(M)$'를 추출할 수 있고, 서버(130)의 공개키 'pks'를 이용하여 서명된 메시지 '$Sign_{prs}(M)$'를 서명검증함으로써, 메시지 'M'의 무결성을 확보할 수 있다.

[0030] 만약, 서명된 메시지 '$Sign_{prs}(M)$'의 크기가 기선정된 크기 이상인 경우, 서버(130)는 임의의 대칭키 'k'를 통해 서명된 메시지 '$Sign_{prs}(M)$'을 암호화하여 암호화된 메시지 '$Enc_k(M||S)$'를 생성할 수 있다. 또한, 서버(130)는 대칭키 'k'를 사용자의 공개키 "pku"로 암호화하여 암호화된 대칭키 '$Enc_{pku}(k)$'를 생성할 수 있다. 이때, 서버(130)는 암호화된 메시지 '$Enc_k(M||S)$'와 암호화된 대칭키 '$Enc_{pku}(k)$'를 모두 포함하는 다차원 코드를 생성하여 사용자에게 제공할 수 있다. 예를 들어, 서버(130)는 사용자(110)의 전자메일 계정으로 다차원 코드가 포함된 메일을 발송하거나 또는 단말기(120)에 설치된 어플리케이션을 통해 단말기(120)로 다차원 코드를 전송할 수 있다.

[0031] 이 경우, 사용자(110)는 단말기(120)를 통해 전자메일 계정으로 발송된 다차원 코드를 획득하거나 어플리케이션을 통해 다차원 코드를 획득할 수 있게 된다. 단말기(120)에 다차원 코드가 수신되면, 다차원 코드는 단말기(120)의 디스플레이를 통해 표시될 수 있다. 사용자(110)는 휴대기기(140)의 카메라를 이용하여 다차원 코드를 포함하는 이미지가 휴대기기로 입력되도록 할 수 있고, 휴대기기(140)는 입력된 이미지에서 다차원 코드를 추출하고, 다차원 코드를 인식하여 다차원 코드에서 대칭키로 암호화된 메시지 '$Enc_k(M||S)$'와 암호화된 대칭키 '$Enc_{pku}(k)$'를 추출할 수 있다. 이때, 휴대기기(140)는 사용자(110)의 비밀키 'pru'를 이용하여 암호화된 대칭키 '$Enc_{pku}(k)$'를 복호화함으로써, 대칭키 'k'를 얻을 수 있고, 암호화된 메시지 '$Enc_k(M||S)$'를 대칭키 'k'로 복호화함으로써, 서명된 메시지 '$Sign_{prs}(M)$'를 얻을 수 있다. 또한, 휴대기기(140)는 서버(130)의 공개키 'pks'를 이용하여 서명된 메시지 '$Sign_{prs}(M)$'를 서명검증함으로써, 메시지 'M'의 무결성을 확보할 수 있다.

[0032] 또 다른 실시예에서는, 서버(130)와 휴대기기(140)간에 사전에 공유된 암호용/인증용 대칭키 <ke, km>가 이용될 수 있다. 우선, 서버(130)는 사용자에게 전송하고자 하는 메시지 'M'을 암호용 대칭키 'ke'로 암호화하여 암호화된 메시지 '$Enc_{ke}(M)$'을 생성하거나 인증용 대칭키 'km'으로 계산한 데이터 인증 코드 '$MAC_{km}(M)$'를 생성하거나 또는 인증용 대칭키 'km'으로 계산한 데이터 인증 코드 '$MAC_{km}(M)$'를 다시 암호용 대칭키 'ke'로 암호화하여 암호화된 데이터 인증 코드 '$Enc_{ke}(M||S)$'를 생성할 수 있다. 여기서, 'M||S'는 데이터 인증 코드 '$MAC_{km}(M)$'를 의미할 수 있다. 이때, 서버(130)는 암호화된 메시지 '$Enc_{ke}(M)$'나 데이터 인증 코드 '$MAC_{km}(M)$' 또는 암호화된 데이터 인증 코드 '$Enc_{ke}(M||S)$'를 포함하는 다차원 코드를 생성하여 사용자(110)에게 제공할 수 있다. 예를 들어, 서버(130)는 사용자(110)의 전자메일 계정으로 다차원 코드가 포함된 메일을 발송하거나 또는 단말기(120)에 설치된 어플리케이션을 통해 단말기(120)로 다차원 코드를 전송할 수 있다.

[0033] 사용자(110)는 단말기(120)를 통해 전자메일 계정으로 발송된 다차원 코드를 획득하거나 어플리케이션을 통해 다차원 코드를 획득할 수 있게 된다. 단말기(120)에 다차원 코드가 수신되면, 다차원 코드는 단말기(120)의 디

스플레이를 통해 표시될 수 있다. 사용자(110)는 휴대기기(140)의 카메라를 이용하여 다차원 코드를 포함하는 이미지가 휴대기기로 입력되도록 할 수 있고, 휴대기기(140)는 입력된 이미지에서 다차원 코드를 추출하고, 다차원 코드를 인식하여 다차원 코드에서 암호화된 메시지 '$Enc_{ke}(M)$'나 데이터 인증 코드 '$MAC_{km}(M)$' 또는 암호화된 데이터 인증 코드 '$Enc_{ke}(M||S)$'를 추출할 수 있다.

[0034] 이때, 다차원 코드에서 암호화된 메시지 '$Enc_{ke}(M)$'가 추출된 경우, 휴대기기(140)는 암호화된 메시지 '$Enc_{ke}(M)$'를 암호용 대칭키 'ke'로 복호화하여 메시지 'M'을 획득할 수 있다.

[0035] 또한, 다차원 코드에서 데이터 인증 코드 '$MAC_{km}(M)$'가 추출된 경우, 휴대기기(140)는 인증용 대칭키 'km'을 이용하여 데이터 인증 코드 '$MAC_{km}(M)$'를 검증함으로써, 메시지 'M'의 무결성을 확보할 수 있다.

[0036] 뿐만 아니라, 다차원 코드에서 암호화된 데이터 인증 코드 '$Enc_{ke}(M||S)$'가 추출된 경우, 휴대기기(140)는 암호용 대칭키 'ke'로 암호화된 데이터 인증 코드 '$Enc_{ke}(M||S)$'를 복호화하여 데이터 인증 코드 '$MAC_{km}(M)$'를 추출할 수 있고, 다시 인증용 대칭키 'km'을 이용하여 데이터 인증 코드 '$MAC_{km}(M)$'를 검증함으로써, 메시지 'M'의 무결성을 확보할 수 있다.

[0037] 다차원 코드를 생성하는 방법은 아래 수학식 1과 같이 표현될 수 있다.

수학식 1

[0038] $$QR\,code = encode(M_{QR})$$

[0039] 여기서, 'QR code'는 상술한 다차원 코드를, 'encode(x)'는 'x'를 이용하여 'x'를 포함하는 다차원 코드를 생성하기 위한 함수를 각각 의미할 수 있다. 또한, 'M_{QR}'는 상술한 첫 번째 실시예에서는 암호화된 메시지 "Encpku(M)"나 암호화된 메시지 'Enck(M)' 및 암호화된 대칭키 'Encpku(k)'를, 두 번째 실시예에서는 서명된 메시지 'Signprs(M)', 세 번째 실시예에서는 암호화된 메시지 'Encpku(M||S)'나 암호화된 메시지 'Enck(M||S)' 및 암호화된 대칭키 'Encpku(k)'를 각각 의미할 수 있다. 네 번째 실시예에서, 'M_{QR}'는 암호화된 메시지 '$Enc_{ke}(M)$'나 데이터 인증 코드 '$MAC_{km}(M)$' 또는 암호화된 데이터 인증 코드 '$Enc_{ke}(M||S)$'를 의미할 수 있다.

[0040] 휴대기기(140)는 메시지 'M'을 획득하는 경우, 메시지 'M'을 디스플레이를 통해 표시할 수 있고, 메시지 'M'의 무결성을 확보하는 경우, 메시지 'M'의 검증에 대한 성공 여부에 대한 정보를 디스플레이를 통해 표시할 수 있다.

[0041] 도 2 내지 도 5는 본 발명의 실시예들에 있어서, 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 시스템 및 메시지를 해독하는 메시지 해독 시스템의 내부 구성을 각각 설명하기 위한 블록도들이다.

[0042] 우선, 도 2는 도 1의 첫 번째 실시예를 통해 설명한 서버(130)에 대응하는 메시지 전송 시스템(210)과 역시 첫 번째 실시예를 통해 설명한 휴대기기(140)에 대응하는 메시지 해독 시스템(220)을 나타내고 있다. 여기서, 메시지 전송 시스템(210)은 공개키 수신부(211), 메시지 수신부(212), 암호화부(213), 다차원 코드 생성부(214) 및 다차원 코드 제공부(215)를 포함하고, 메시지 해독 시스템(220)은 다차원 코드 인식부(221), 메시지 추출부(222) 및 복호화부(223)를 포함한다.

[0043] 공개키 수신부(211)는 사용자의 공개키를 수신 및 유지한다. 예를 들어, 메시지 전송 시스템(210)은 사용자가 전자메일 서비스나 인스턴트 메시징을 위한 서비스에 가입할 때, 혹은 관련 어플리케이션을 사용자의 단말기에 설치할 때, 공개키 수신부(211)를 통해 미리 사용자의 공개키를 수신하고, 사용자의 식별자와 연관하여 저장함으로써 유지할 수 있다.

[0044] 메시지 수신부(212)는 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(210)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 메시지 수신부(212)를 통해 수

신할 수 있다.

[0045] 암호화부(213)는 수신된 사용자의 공개키로 메시지를 암호화한다. 예를 들어, 암호화부(213)는 공개키 수신부(211)에서 유지하는 공개키 중 메시지를 전송하고자 하는 사용자의 공개키를 확인하고, 확인된 공개키로 메시지를 암호화할 수 있다.

[0046] 다차원 코드 생성부(214)는 암호화된 메시지를 포함하는 다차원 코드를 생성한다. 다차원 코드를 생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0047] 다차원 코드 제공부(215)는 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 다차원 코드 제공부(215)는 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는 메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0048] 사용자의 단말기에 다차원 코드가 수신되면 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(220)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0049] 다차원 코드 인식부(221)는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0050] 메시지 추출부(222)는 다차원 코드에서 사용자의 공개키로 암호화된 메시지를 추출한다. 이때, 사용자의 공개키로 암호화된 메시지는 상술한 메시지 전송 시스템(210)의 암호화부(213)에서 암호화된 메시지를 의미할 수 있다.

[0051] 복호화부(223)는 사용자의 공개키로 암호화된 메시지를 사용자의 비밀키로 복호화하여 상기 메시지를 추출한다. 따라서, 메시지 해독 시스템(220)은 다차원 코드를 이용하여 안전하게 메시지를 얻을 수 있고, 필요에 따라 해당 메시지를 디스플레이를 통해 표시할 수 있다.

[0052] 도 3은 도 1의 두 번째 실시예를 통해 설명한 서버(130)에 대응하는 메시지 전송 시스템(310)과 역시 두 번째 실시예를 통해 설명한 휴대기기(140)에 대응하는 메시지 해독 시스템(320)을 나타내고 있다. 여기서, 메시지 전송 시스템(310)은 키 생성부(311), 공개키 제공부(312), 메시지 수신부(313), 메시지 서명부(314), 다차원 코드 생성부(315) 및 다차원 코드 제공부(316)를 포함하고, 메시지 해독 시스템(320)은 공개키 수신부(321), 다차원 코드 인식부(322), 메시지 추출부(323) 및 서명검증부(324)를 포함한다.

[0053] 키 생성부(311)는 공개키 및 비밀키를 생성한다. 즉, 메시지 전송 시스템(310)의 공개키와 비밀키가 키 생성부(311)를 통해 생성될 수 있다.

[0054] 공개키 제공부(312)는 생성된 공개키를 사용자에게 제공한다. 이후, 사용자에게 제공된 공개키는 비밀키를 통해 서명된 메시지를 서명검증하기 위해 이용될 수 있다.

[0055] 메시지 수신부(313)는 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(310)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 메시지 수신부(313)를 통해 수신할 수 있다.

[0056] 메시지 서명부(314)는 생성된 비밀키로 메시지를 서명하여 서명된 메시지를 생성한다. 서명된 메시지는 메시지의 무결성을 확보하는데 이용될 수 있다.

[0057] 다차원 코드 생성부(315)는 서명된 메시지를 포함하는 다차원 코드를 생성한다. 다차원 코드를 생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0058] 다차원 코드 제공부(316)는 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 다차원 코드 제공부(316)는 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는 메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0059] 사용자의 단말기에 다차원 코드가 수신되면 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(320)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0060] 공개키 수신부(321)는 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버 즉, 도 3에서는 메시지

전송 시스템(310)으로부터 메시지 전송 시스템(310)의 공개키를 수신한다. 이러한 메시지 전송 시스템(310)의 공개키는 메시지 전송 시스템(310)의 공개키 제공부(312)가 사용자에게 제공한 공개키에 대응할 수 있다.

[0061] 다차원 코드 인식부(322)는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0062] 메시지 추출부(323)는 다차원 코드에서 메시지 전송 시스템(310)의 비밀키로 서명된 메시지를 추출한다. 이때, 메시지 전송 시스템(310)의 비밀키로 서명된 메시지는 상술한 메시지 전송 시스템(310)의 메시지 서명부(314)에서 서명된 메시지를 의미할 수 있다.

[0063] 서명검증부(324)는 메시지 전송 시스템(310)의 공개키로 상기 서명된 메시지를 서명검증한다. 즉, 메시지 해독 시스템(320)은 상술한 서명검증의 결과에 따라 메시지의 무결성을 확보할 수 있다. 필요에 따라 메시지 해독 시스템(320)은 서명 검증의 성공 여부를 디스플레이를 통해 표시할 수 있다.

[0064] 도 4는 도 1의 세 번째 실시예를 통해 설명한 서버(130)에 대응하는 메시지 전송 시스템(410)과 역시 세 번째 실시예를 통해 설명한 휴대기기(140)에 대응하는 메시지 해독 시스템(420)을 나타내고 있다. 여기서, 메시지 전송 시스템(410)은 키 생성부(411), 공개키 제공부(412), 공개키 수신부(413), 메시지 수신부(414), 메시지 서명부(415), 암호화부(416), 다차원 코드 생성부(417) 및 다차원 코드 제공부(418)를 포함하고, 메시지 해독 시스템(420)은 공개키 수신부(421), 다차원 코드 인식부(422), 메시지 추출부(423) 및 인증부(424)를 포함한다.

[0065] 키 생성부(411)는 공개키 및 비밀키를 생성한다. 즉, 메시지 전송 시스템(410)의 공개키와 비밀키가 키 생성부(411)를 통해 생성될 수 있다.

[0066] 공개키 제공부(412)는 생성된 공개키를 사용자에게 제공한다. 이후, 사용자에게 제공된 공개키는 비밀키를 통해 서명된 메시지를 서명검증하기 위해 이용될 수 있다.

[0067] 공개키 수신부(413)는 사용자의 공개키를 수신한다. 예를 들어, 메시지 전송 시스템(410)은 사용자가 전자메일 서비스나 인스턴트 메시징을 위한 서비스에 가입할 때, 혹은 관련 어플리케이션을 사용자의 단말기에 설치할 때, 공개키 수신부(413)를 통해 미리 사용자의 공개키를 수신하고, 사용자의 식별자와 연관하여 저장함으로써 유지할 수 있다.

[0068] 메시지 수신부(414)는 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(410)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 메시지 수신부(414)를 통해 수신할 수 있다.

[0069] 메시지 서명부(415)는 생성된 비밀키로 메시지를 서명하여 서명된 메시지를 생성한다. 서명된 메시지는 메시지의 무결성을 확보하는데 이용될 수 있다.

[0070] 암호화부(416)는 사용자의 공개키로 서명된 메시지를 암호화한다. 즉, 암호화부(416)는 공개키 수신부(413)에서 수신된 공개키로 서명된 메시지를 암호화할 수 있다.

[0071] 다차원 코드 생성부(417)는 암호화된 메시지를 포함하는 다차원 코드를 생성한다. 다차원 코드를 생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0072] 다차원 코드 제공부(418)는 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 다차원 코드 제공부(418)는 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는 메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0073] 사용자의 단말기에 다차원 코드가 수신되면 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(420)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0074] 공개키 수신부(421)는 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버 즉, 도 4에서는 메시지 전송 시스템(410)으로부터 메시지 전송 시스템(410)의 공개키를 수신한다. 이러한 메시지 전송 시스템(410)의 공개키는 메시지 전송 시스템(410)의 공개키 제공부(412)가 사용자에게 제공한 공개키에 대응할 수 있다.

[0075] 다차원 코드 인식부(422)는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0076] 메시지 추출부(423)는 다차원 코드에서 메시지 전송 시스템(410)의 비밀키로 서명되고, 사용자의 공개키로 암호화된 메시지를 추출한다. 이때, 메시지 전송 시스템(410)의 비밀키로 서명되고, 사용자의 공개키로 암호화된 메시지는 상술한 메시지 전송 시스템(410)의 메시지 서명부(415) 및 암호화부(416)에서 서명되고 암호화된 메시지를 의미할 수 있다.

[0077] 인증부(424)는 추출된 메시지를 사용자의 비밀키로 복호화하여 서명된 메시지를 추출하고, 서명된 메시지를 메시지 전송 시스템(410)의 공개키로 서명검증한다. 즉, 메시지 해독 시스템(420)은 상술한 서명검증의 결과에 따라 메시지의 무결성을 확보할 수 있다. 필요에 따라 메시지 해독 시스템(420)은 서명 검증의 성공 여부를 디스플레이를 통해 표시할 수 있다.

[0078] 도 5는 도 1의 네 번째 실시예를 통해 설명한 서버(130)에 대응하는 메시지 전송 시스템(510)과 역시 네 번째 실시예를 통해 설명한 휴대기기(140)에 대응하는 메시지 해독 시스템(520)을 나타내고 있다. 여기서, 메시지 전송 시스템(510)은 메시지 수신부(511), 암호화부(512), 다차원 코드 생성부(513) 및 다차원 코드 제공부(514)를 포함하고, 메시지 해독 시스템(520)은 다차원 코드 인식부(521), 메시지 추출부(522) 및 메시지 처리부(523)를 포함한다.

[0079] 메시지 수신부(511)는 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(510)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 메시지 수신부(511)를 통해 수신할 수 있다.

[0080] 암호화부(512)는 (1) 휴대기기와 미리 공유된 암호용 대칭키로 메시지를 암호화하여 암호화된 메시지를 생성하거나 (2) 휴대기기와 미리 공유된 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성하거나 또는 (3) 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성한 후 메시지 인증 코드를 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드를 생성한다.

[0081] 다차원 코드 생성부(513)는 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드를 포함하는 다차원 코드를 생성한다. 다차원 코드를 생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0082] 다차원 코드 제공부(514)는 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 다차원 코드 제공부(514)는 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는 메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0083] 사용자의 단말기로 다차원 코드가 전송되면, 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(520)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0084] 다차원 코드 인식부(521)는 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0085] 메시지 추출부(522)는 다차원 코드에서 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드를 추출한다. 이때, 메시지 전송 시스템(510)에서 암호용 대칭키로 메시지가 암호화되어 암호화된 메시지가 생성되거나 인증용 대칭키로 메시지에 대한 메시지 인증 코드가 생성되거나 또는 인증용 대칭키로 메시지에 대한 메시지 인증 코드가 생성된 후 메시지 인증 코드를 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드가 생성된다.

[0086] 메시지 처리부(523)는 (1) 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버와 미리 공유된 암호용 대칭키로 암호화된 메시지를 복호화하거나 (2) 서버와 미리 공유된 인증용 대칭키로 메시지 인증 코드를 검증하거나 또는 (3) 암호용 대칭키로 암호화된 메시지 인증 코드를 복호화한 후 인증용 대칭키로 복호화된 메시지 인증 코드를 검증한다. 즉, 메시지 해독 시스템(520)은 상술한 검증의 결과에 따라 메시지의 무결성을 확보할 수 있다. 필요에 따라 메시지 해독 시스템(520)은 검증의 성공 여부를 디스플레이를 통해 표시할 수 있다.

[0087] 도 6 내지 도 11은 본 발명의 실시예들에 있어서, 전자메일 또는 인스턴트 메시징을 위한 메시지를 사용자에게 전송하는 메시지 전송 방법 및 메시지를 해독하는 메시지 해독 방법을 도시한 흐름도들이다.

[0088] 도 6에 나타난 단계(611) 내지 단계(615)는 도 2를 통해 설명한 메시지 전송 시스템(210)을 통해 수행되는 메시지 전송 방법을, 단계(621) 내지 단계(623)는 도 2를 통해 설명한 메시지 해독 시스템(220)을 통해 수행되는 메

시지 해독 방법을 각각 나타낼 수 있다.

[0089] 단계(611)에서 메시지 전송 시스템(210)은 사용자의 공개키를 수신 및 유지한다. 예를 들어, 메시지 전송 시스템(210)은 사용자가 전자메일 서비스나 인스턴트 메시징을 위한 서비스에 가입할 때, 혹은 관련 어플리케이션을 사용자의 단말기에 설치할 때, 단계(611)를 통해 미리 사용자의 공개키를 수신하고, 사용자의 식별자와 연관하여 저장함으로써 유지할 수 있다.

[0090] 단계(612)에서 메시지 전송 시스템(210)은 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(210)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 단계(612)를 통해 수신할 수 있다.

[0091] 단계(613)에서 메시지 전송 시스템(210)은 수신된 사용자의 공개키로 메시지를 암호화한다. 예를 들어, 메시지 전송 시스템(210)은 단계(611)에서 수신 및 유지되는 공개키 중 메시지를 전송하고자 하는 사용자의 공개키를 확인하고, 확인된 공개키로 메시지를 암호화할 수 있다.

[0092] 단계(614)에서 메시지 전송 시스템(210)은 암호화된 메시지를 포함하는 다차원 코드를 생성한다. 다차원 코드를 생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0093] 단계(615)에서 메시지 전송 시스템(210)은 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 메시지 전송 시스템(210)은 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는 메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0094] 사용자의 단말기에 다차원 코드가 수신되면 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(220)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0095] 단계(621)에서 메시지 해독 시스템(220)은 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0096] 단계(622)에서 메시지 해독 시스템(220)은 다차원 코드에서 사용자의 공개키로 암호화된 메시지를 추출한다. 이때, 사용자의 공개키로 암호화된 메시지는 상술한 메시지 전송 시스템(210)에서 암호화된 메시지를 의미할 수 있다.

[0097] 단계(623)에서 메시지 해독 시스템(220)은 사용자의 공개키로 암호화된 메시지를 사용자의 비밀키로 복호화하여 상기 메시지를 추출한다. 따라서, 메시지 해독 시스템(220)은 다차원 코드를 이용하여 안전하게 메시지를 얻을 수 있고, 필요에 따라 해당 메시지를 디스플레이를 통해 표시할 수 있다.

[0098] 도 7에 나타난 단계(711) 내지 단계(716)는 도 3을 통해 설명한 메시지 전송 시스템(310)을 통해 수행되는 메시지 전송 방법을, 단계(721) 내지 단계(724)는 도 3를 통해 설명한 메시지 해독 시스템(320)을 통해 수행되는 메시지 해독 방법을 각각 나타낼 수 있다.

[0099] 단계(711)에서 메시지 전송 시스템(310)은 공개키 및 비밀키를 생성한다. 즉, 메시지 전송 시스템(310)의 공개키와 비밀키가 단계(711)를 통해 생성될 수 있다.

[0100] 단계(712)에서 메시지 전송 시스템(310)은 생성된 공개키를 사용자에게 제공한다. 이후, 사용자에게 제공된 공개키는 비밀키를 통해 서명된 메시지를 서명검증하기 위해 이용될 수 있다.

[0101] 단계(713)에서 메시지 전송 시스템(310)은 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(310)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 단계(713)를 통해 수신할 수 있다.

[0102] 단계(714)에서 메시지 전송 시스템(310)은 생성된 비밀키로 메시지를 서명하여 서명된 메시지를 생성한다. 서명된 메시지는 메시지의 무결성을 확보하는데 이용될 수 있다.

[0103] 단계(715)에서 메시지 전송 시스템(310)은 서명된 메시지를 포함하는 다차원 코드를 생성한다. 다차원 코드를

생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0104] 단계(716)에서 메시지 전송 시스템(310)은 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 메시지 전송 시스템(310)은 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는 메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0105] 사용자의 단말기에 다차원 코드가 수신되면 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(320)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0106] 단계(721)에서 메시지 해독 시스템(320)은 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버 즉, 메시지 전송 시스템(310)으로부터 메시지 전송 시스템(310)의 공개키를 수신한다. 이러한 메시지 전송 시스템(310)의 공개키는 메시지 전송 시스템(310)이 단계(712)에서 사용자에게 제공한 공개키에 대응할 수 있다.

[0107] 단계(722)에서 메시지 해독 시스템(320)은 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0108] 단계(723)에서 메시지 해독 시스템(320)은 다차원 코드에서 메시지 전송 시스템(310)의 비밀키로 서명된 메시지를 추출한다. 이때, 메시지 전송 시스템(310)의 비밀키로 서명된 메시지는 단계(714)에서 상술한 메시지 전송 시스템(310)에 의해 서명된 메시지를 의미할 수 있다.

[0109] 단계(724)에서 메시지 해독 시스템(320)은 메시지 전송 시스템(310)의 공개키로 상기 서명된 메시지를 서명검증한다. 즉, 메시지 해독 시스템(320)은 상술한 서명검증의 결과에 따라 메시지의 무결성을 확보할 수 있다. 필요에 따라 메시지 해독 시스템(320)은 서명 검증의 성공 여부를 디스플레이를 통해 표시할 수 있다.

[0110] 도 8의 메시지 전송 방법은 도 4를 통해 설명한 메시지 전송 시스템(410)을 통해 수행될 수 있고, 도 9의 메시지 해독 방법은 도 4를 통해 설명한 메시지 해독 시스템(420)을 통해 수행될 수 있다.

[0111] 우선, 도 8의 메시지 전송 방법은 도 8에 도시된 바와 같이 단계(810) 내지 단계(880)를 포함한다.

[0112] 단계(810)에서 메시지 전송 시스템(410)은 공개키 및 비밀키를 생성한다. 즉, 메시지 전송 시스템(410)의 공개키와 비밀키가 단계(810)를 통해 생성될 수 있다.

[0113] 단계(820)에서 메시지 전송 시스템(410)은 생성된 공개키를 사용자에게 제공한다. 이후, 사용자에게 제공된 공개키는 비밀키를 통해 서명된 메시지를 서명검증하기 위해 이용될 수 있다.

[0114] 단계(830)에서 메시지 전송 시스템(410)은 사용자의 공개키를 수신한다. 예를 들어, 메시지 전송 시스템(410)은 사용자가 전자메일 서비스나 인스턴트 메시징을 위한 서비스에 가입할 때, 혹은 관련 어플리케이션을 사용자의 단말기에 설치할 때, 단계(830)를 통해 미리 사용자의 공개키를 수신하고, 사용자의 식별자와 연관하여 저장함으로써 유지할 수 있다.

[0115] 단계(840)에서 메시지 전송 시스템(410)은 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(410)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 단계(840)를 통해 수신할 수 있다.

[0116] 단계(850)에서 메시지 전송 시스템(410)은 생성된 비밀키로 메시지를 서명하여 서명된 메시지를 생성한다. 서명된 메시지는 메시지의 무결성을 확보하는데 이용될 수 있다.

[0117] 단계(860)에서 메시지 전송 시스템(410)은 사용자의 공개키로 서명된 메시지를 암호화한다. 즉, 메시지 전송 시스템(410)는 단계(830)에서 수신된 사용자의 공개키로 서명된 메시지를 암호화할 수 있다.

[0118] 단계(870)에서 메시지 전송 시스템(410)은 암호화된 메시지를 포함하는 다차원 코드를 생성한다. 다차원 코드를 생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0119] 단계(880)에서 메시지 전송 시스템(410)은 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 메시지 전송 시스템(410)은 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는

메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0120] 사용자의 단말기에 다차원 코드가 수신되면 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(420)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0121] 도 9의 메시지 해독 방법은 도 9에 도시된 바와 같이 단계(910) 내지 단계(940)를 포함한다.

[0122] 단계(910)에서 메시지 해독 시스템(420)은 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버 즉, 도 4에 도시된 메시지 전송 시스템(410)으로부터 메시지 전송 시스템(410)의 공개키를 수신한다. 이러한 메시지 전송 시스템(410)의 공개키는 메시지 전송 시스템(410)이 단계(820)에서 사용자에게 제공한 공개키에 대응할 수 있다.

[0123] 단계(920)에서 메시지 해독 시스템(420)은 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명은 생략한다.

[0124] 단계(930)에서 메시지 해독 시스템(420)은 다차원 코드에서 메시지 전송 시스템(410)의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지를 추출한다. 이때, 메시지 전송 시스템(410)의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지는 상술한 메시지 전송 시스템(410)에 의해 단계(850) 및 단계(860)에서 서명되고 암호화된 메시지를 의미할 수 있다.

[0125] 단계(940)에서 메시지 해독 시스템(420)은 추출된 메시지를 사용자의 비밀키로 복호화하여 서명된 메시지를 추출하고, 서명된 메시지를 메시지 전송 시스템(410)의 공개키로 서명검증한다. 즉, 메시지 해독 시스템(420)은 상술한 서명검증의 결과에 따라 메시지의 무결성을 확보할 수 있다. 필요에 따라 메시지 해독 시스템(420)은 서명 검증의 성공 여부를 디스플레이를 통해 표시할 수 있다.

[0126] 도 10의 메시지 전송 방법은 도 5를 통해 설명한 메시지 전송 시스템(510)을 통해 수행될 수 있고, 도 11의 메시지 해독 방법은 도 5를 통해 설명한 메시지 해독 시스템(520)을 통해 수행될 수 있다.

[0127] 우선, 도 10의 메시지 전송 방법은 도 10에 도시된 바와 같이 단계(1010) 내지 단계(1040)를 포함한다.

[0128] 단계(1010)에서 메시지 전송 시스템(510)은 사용자에게 제공하기 위한 메시지를 수신한다. 예를 들어, 메시지 전송 시스템(510)은 사용자 자신 또는 다른 사용자가 사용자에게 메일과 같은 메시지를 전송하거나 또는 인스턴트 메시징을 위한 메시지를 전송할 때, 상기 사용자 자신 또는 다른 사용자에 의해 생성된 메시지를 단계(1010)에서 수신할 수 있다.

[0129] 단계(1020)에서 메시지 전송 시스템(510)은 (1) 휴대기기와 미리 공유된 암호용 대칭키로 메시지를 암호화하여 암호화된 메시지를 생성하거나 (2) 휴대기기와 미리 공유된 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성하거나 또는 (3) 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성한 후 메시지 인증 코드를 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드를 생성한다.

[0130] 단계(1030)에서 메시지 전송 시스템(510)은 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드를 포함하는 다차원 코드를 생성한다. 다차원 코드를 생성하는 방법에 대해서는 상술한 수학식 1을 참조할 수 있다.

[0131] 단계(1040)에서 메시지 전송 시스템(510)은 생성된 다차원 코드를 사용자에게 제공한다. 이때, 생성된 다차원 코드는 사용자의 전자메일 계정 또는 사용자의 인스턴트 메시징을 위한 어플리케이션을 통해 사용자의 단말기로 제공될 수 있다. 즉, 메시지 전송 시스템(510)은 일례로, 사용자의 전자메일 계정으로 다차원 코드를 포함하는 메일을 발송하거나 또는 사용자의 단말기에 설치된 어플리케이션을 통해 사용자의 단말기로 다차원 코드를 전송할 수 있다.

[0132] 사용자의 단말기로 다차원 코드가 전송되면, 단말기는 디스플레이를 통해 다차원 코드를 표시할 수 있고, 사용자는 메시지 해독 시스템(520)이 포함하는 카메라를 통해 다차원 코드를 포함하는 이미지를 촬영할 수 있다.

[0133] 도 11의 메시지 해독 방법은 도 11에 도시된 바와 같이 단계(1110) 내지 단계(1130)를 포함한다.

[0134] 단계(1110)에서 메시지 해독 시스템(520)은 카메라를 통해 입력된 이미지에서 다차원 코드를 인식한다. 다차원 코드를 포함하는 이미지에서 다차원 코드를 인식하는 방법에 대해서는 이미 잘 알려져 있기 때문에 자세한 설명

은 생략한다.

[0135] 단계(1120)에서 메시지 해독 시스템(520)은 다차원 코드에서 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드를 추출한다. 이때, 메시지 전송 시스템(510)에서 암호용 대칭키로 메시지가 암호화되어 암호화된 메시지가 생성되거나 인증용 대칭키로 메시지에 대한 메시지 인증 코드가 생성되거나 또는 인증용 대칭키로 메시지에 대한 메시지 인증 코드가 생성된 후 메시지 인증 코드를 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드가 생성된다.

[0136] 단계(1130)에서 메시지 해독 시스템(520)은 (1) 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버와 미리 공유된 암호용 대칭키로 암호화된 메시지를 복호화하거나 (2) 서버와 미리 공유된 인증용 대칭키로 메시지 인증 코드를 검증하거나 또는 (3) 암호용 대칭키로 암호화된 메시지 인증 코드를 복호화한 후 인증용 대칭키로 복호화된 메시지 인증 코드를 검증한다. 즉, 메시지 해독 시스템(520)은 상술한 검증의 결과에 따라 메시지의 무결성을 확보할 수 있다. 필요에 따라 메시지 해독 시스템(520)은 검증의 성공 여부를 디스플레이를 통해 표시할 수 있다.

[0137] 이와 같이, 본 발명의 실시예들에 따른 시스템 및 방법을 이용하면, 전자메일 또는 인스턴트 메시징을 위한 메시지를 QR 코드와 같은 다차원 코드를 이용하여 휴대기기로 전송할 수 있다. 또한, 사용자의 공개키와 비밀키 또는 사용자의 휴대기기와 전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버간에 미리 공유된 암호용/인증용 대칭키, 그리고 다차원 코드를 이용하여 전자메일 또는 인스턴트 메시징을 위한 메시지를 안전하게 전달할 수 있다.

[0138] 본 발명의 실시예에 따른 방법들은 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. 또한, 상술한 파일 시스템은 컴퓨터 판독이 가능한 기록 매체에 기록될 수 있다.

[0139] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0140] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0141] 110: 사용자

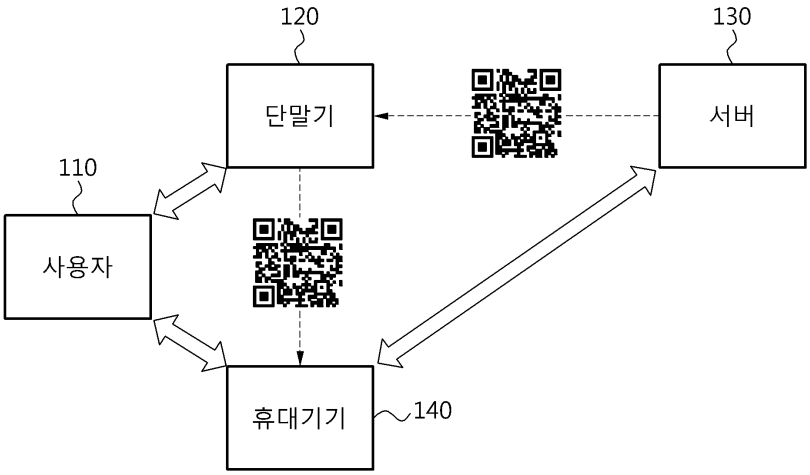
120: 단말기

130: 서버

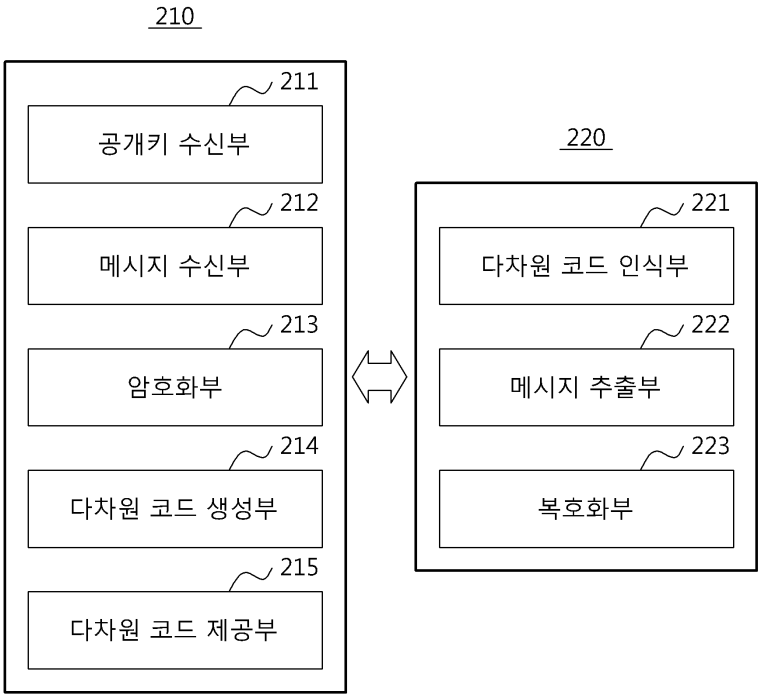
140: 휴대기기

도면

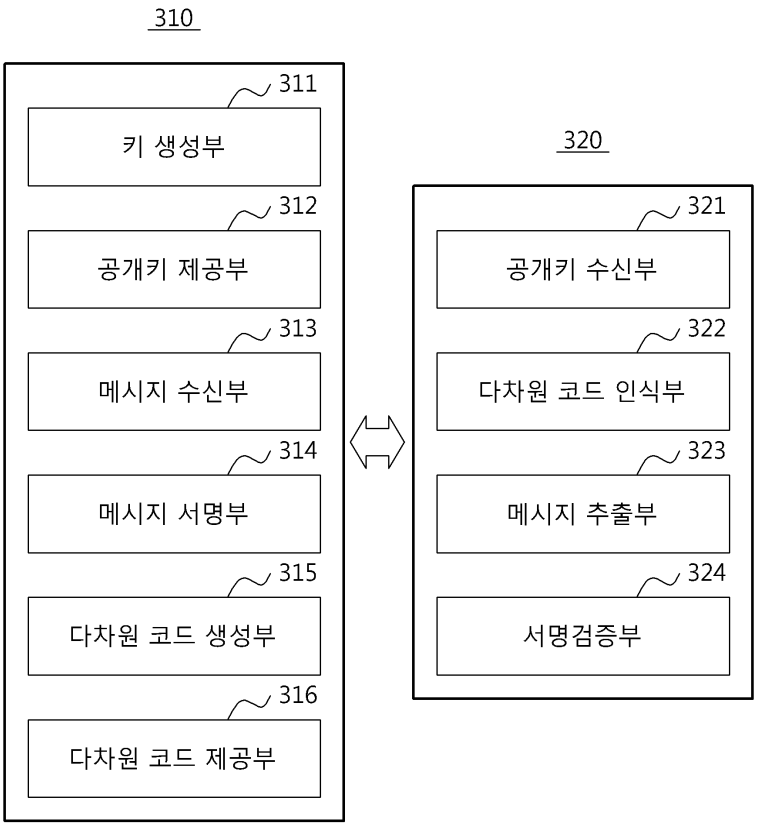
도면1


120
130
단말기
서버
110
사용자
휴대기기
140

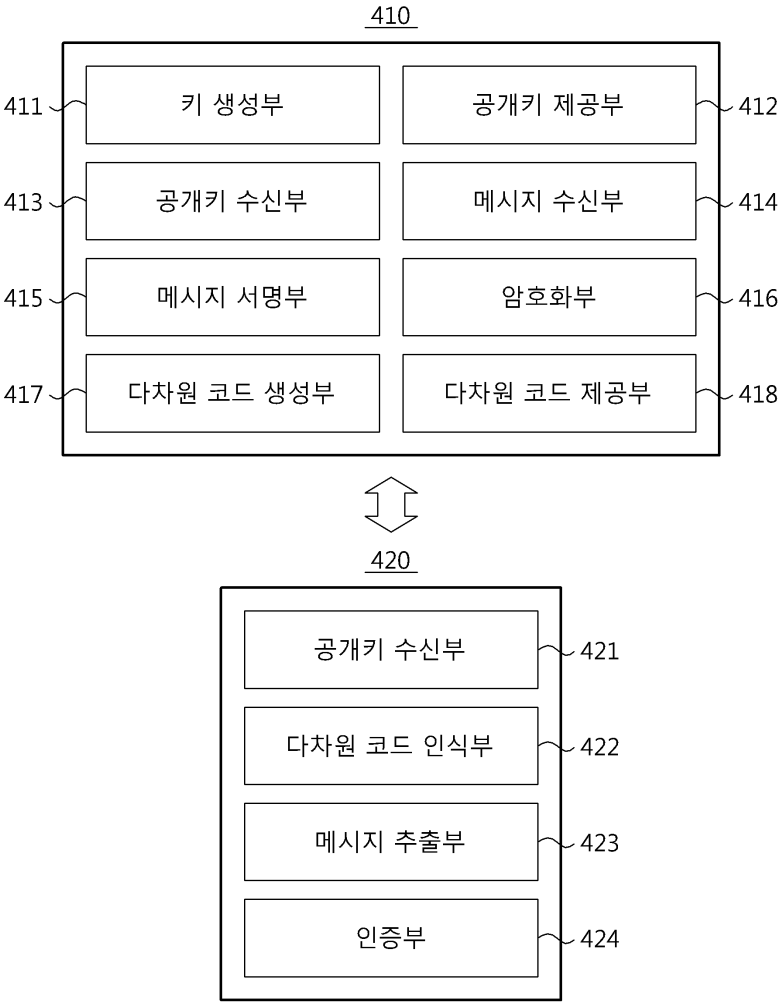
도면2


210
211
공개키 수신부
212
메시지 수신부
213
암호화부
214
다차원 코드 생성부
215
다차원 코드 제공부
220
221
다차원 코드 인식부
222
메시지 추출부
223
복호화부

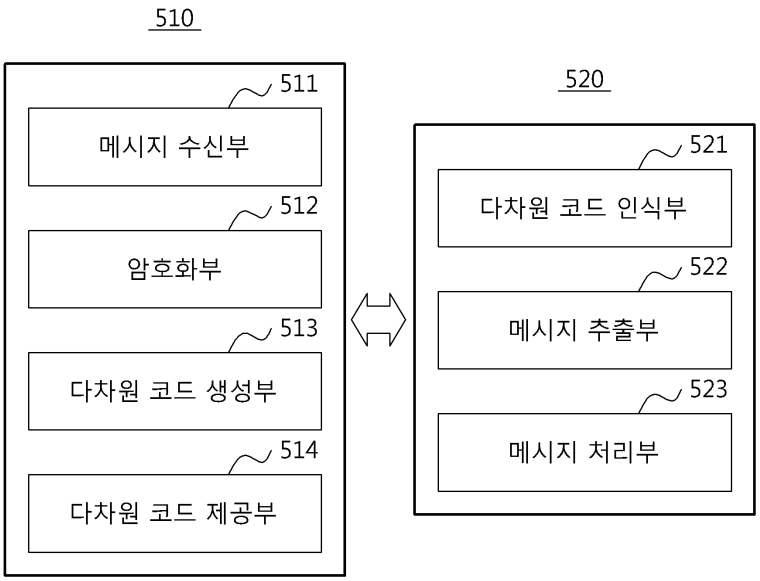
도면3


310
311
키 생성부
312
공개키 제공부
313
메시지 수신부
314
메시지 서명부
315
다차원 코드 생성부
316
다차원 코드 제공부
320
321
공개키 수신부
322
다차원 코드 인식부
323
메시지 추출부
324
서명검증부

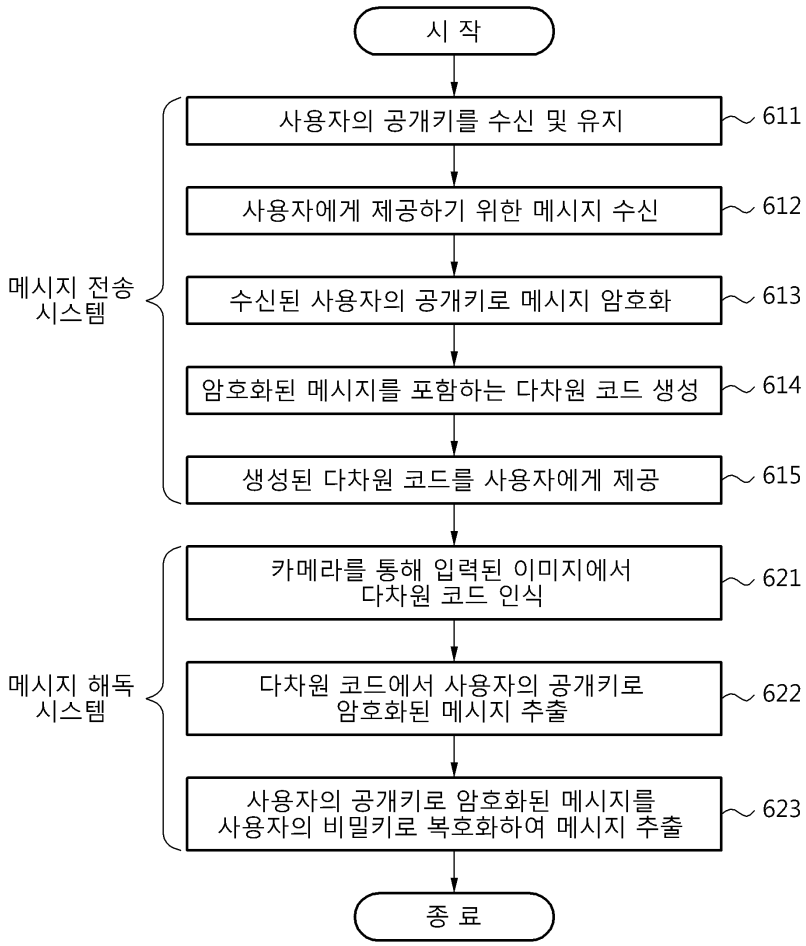
도면4


410
411
키 생성부
412
공개키 제공부
413
공개키 수신부
414
메시지 수신부
415
메시지 서명부
416
암호화부
417
다차원 코드 생성부
418
다차원 코드 제공부
420
421
공개키 수신부
422
다차원 코드 인식부
423
메시지 추출부
424
인증부

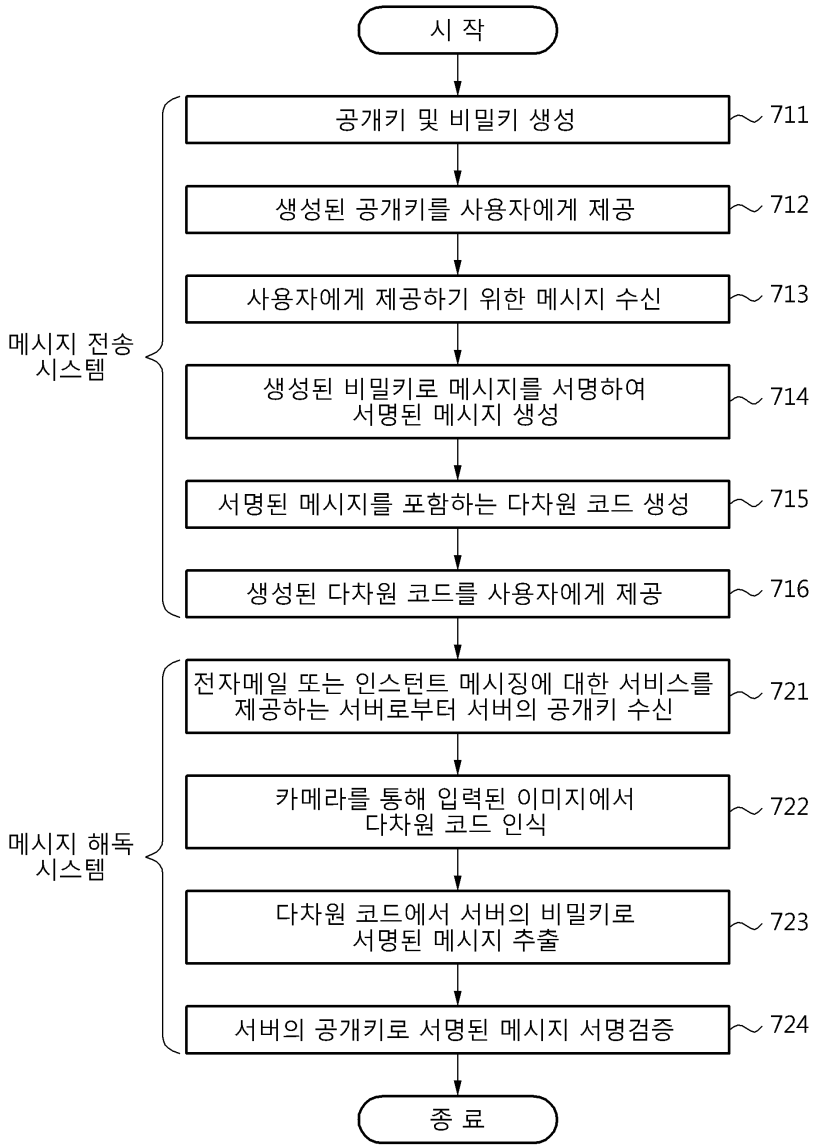
도면5


510
511
메시지 수신부
512
암호화부
513
다차원 코드 생성부
514
다차원 코드 제공부
520
521
다차원 코드 인식부
522
메시지 추출부
523
메시지 처리부

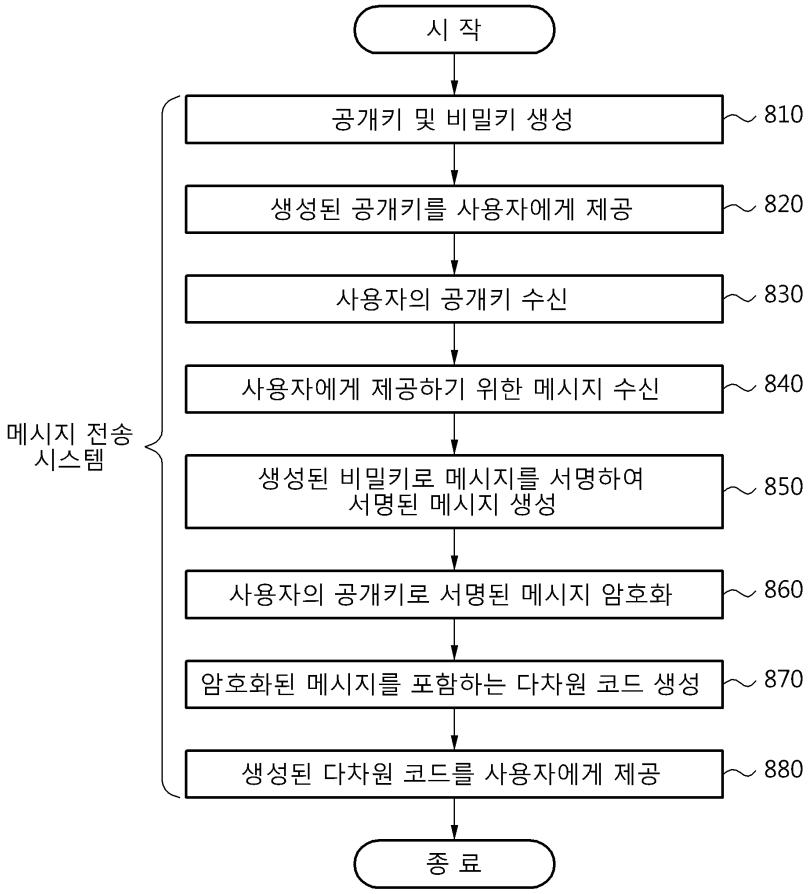
도면6


시 작
사용자의 공개키를 수신 및 유지
611
사용자에게 제공하기 위한 메시지 수신
612
수신된 사용자의 공개키로 메시지 암호화
613
암호화된 메시지를 포함하는 다차원 코드 생성
614
생성된 다차원 코드를 사용자에게 제공
615
메시지 전송 시스템
카메라를 통해 입력된 이미지에서 다차원 코드 인식
621
다차원 코드에서 사용자의 공개키로 암호화된 메시지 추출
622
사용자의 공개키로 암호화된 메시지를 사용자의 비밀키로 복호화하여 메시지 추출
623
메시지 해독 시스템
종 료

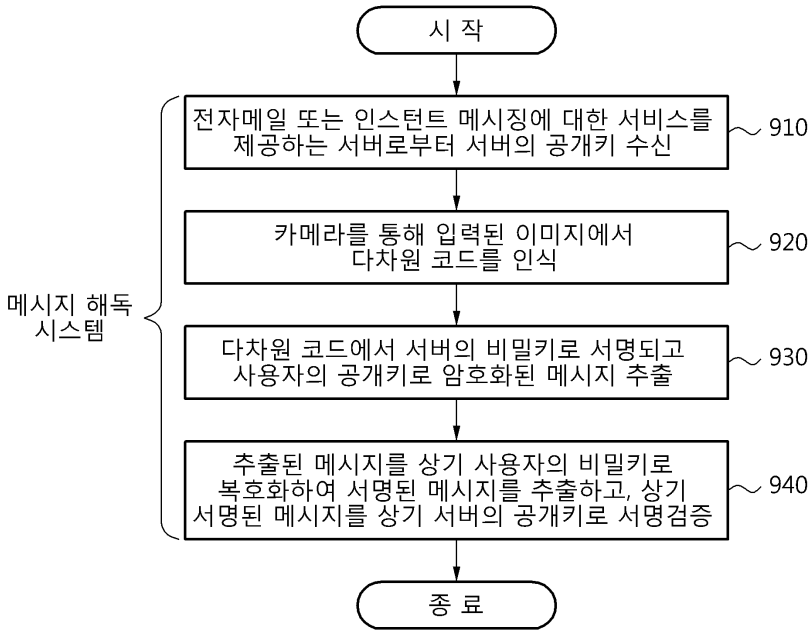
도면7


시 작
공개키 및 비밀키 생성
711
생성된 공개키를 사용자에게 제공
712
사용자에게 제공하기 위한 메시지 수신
713
메시지 전송 시스템
생성된 비밀키로 메시지를 서명하여 서명된 메시지 생성
714
서명된 메시지를 포함하는 다차원 코드 생성
715
생성된 다차원 코드를 사용자에게 제공
716
전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 서버의 공개키 수신
721
카메라를 통해 입력된 이미지에서 다차원 코드 인식
722
메시지 해독 시스템
다차원 코드에서 서버의 비밀키로 서명된 메시지 추출
723
서버의 공개키로 서명된 메시지 서명검증
724
종 료

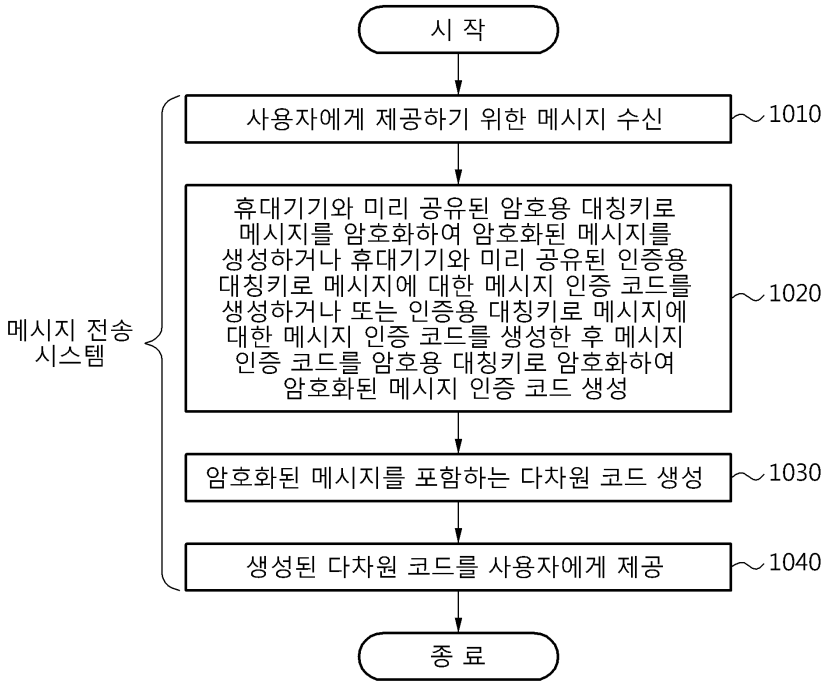
도면8


시 작
공개키 및 비밀키 생성
810
생성된 공개키를 사용자에게 제공
820
사용자의 공개키 수신
830
사용자에게 제공하기 위한 메시지 수신
840
생성된 비밀키로 메시지를 서명하여 서명된 메시지 생성
850
사용자의 공개키로 서명된 메시지 암호화
860
암호화된 메시지를 포함하는 다차원 코드 생성
870
생성된 다차원 코드를 사용자에게 제공
880
종 료
메시지 전송 시스템

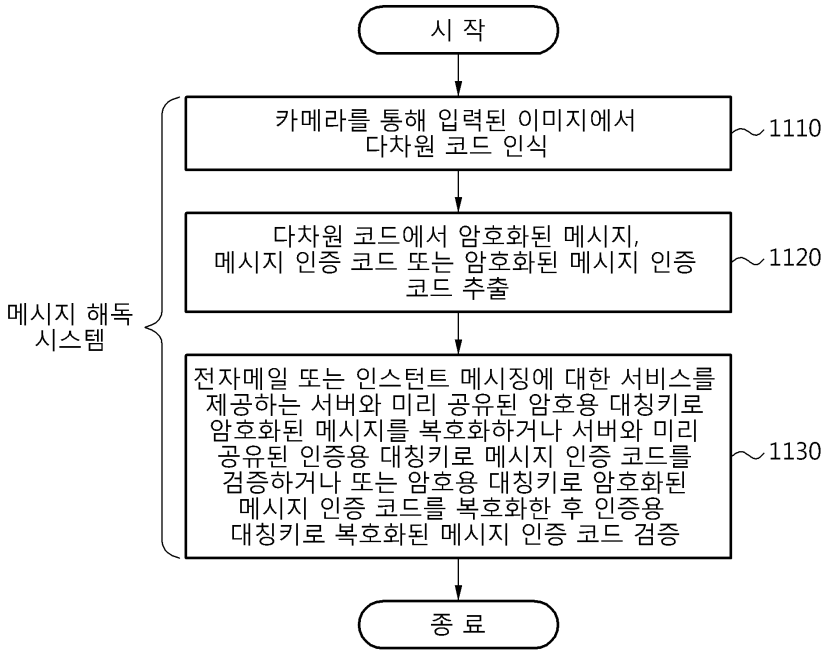
도면9


시 작
전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버로부터 서버의 공개키 수신
910
카메라를 통해 입력된 이미지에서 다차원 코드를 인식
920
다차원 코드에서 서버의 비밀키로 서명되고 사용자의 공개키로 암호화된 메시지 추출
930
추출된 메시지를 상기 사용자의 비밀키로 복호화하여 서명된 메시지를 추출하고, 상기 서명된 메시지를 상기 서버의 공개키로 서명검증
940
종 료
메시지 해독 시스템

도면10


시 작
사용자에게 제공하기 위한 메시지 수신
1010
휴대기기와 미리 공유된 암호용 대칭키로 메시지를 암호화하여 암호화된 메시지를 생성하거나 휴대기기와 미리 공유된 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성하거나 또는 인증용 대칭키로 메시지에 대한 메시지 인증 코드를 생성한 후 메시지 인증 코드를 암호용 대칭키로 암호화하여 암호화된 메시지 인증 코드 생성
1020
메시지 전송 시스템
암호화된 메시지를 포함하는 다차원 코드 생성
1030
생성된 다차원 코드를 사용자에게 제공
1040
종 료

도면11


시 작
카메라를 통해 입력된 이미지에서 다차원 코드 인식
1110
다차원 코드에서 암호화된 메시지, 메시지 인증 코드 또는 암호화된 메시지 인증 코드 추출
1120
메시지 해독 시스템
전자메일 또는 인스턴트 메시징에 대한 서비스를 제공하는 서버와 미리 공유된 암호용 대칭키로 암호화된 메시지를 복호화하거나 서버와 미리 공유된 인증용 대칭키로 메시지 인증 코드를 검증하거나 또는 암호용 대칭키로 암호화된 메시지 인증 코드를 복호화한 후 인증용 대칭키로 복호화된 메시지 인증 코드 검증
1130
종 료