(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년02월06일
(11) 등록번호 10-1489862
(24) 등록일자 2015년01월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2013-0144315
(22) 출원일자 2013년11월26일
심사청구일자 2013년11월26일
(56) 선행기술조사문헌
KR1020050111533 A*
KR1020110016813 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국과학기술정보연구원
대전광역시 유성구 대학로 245 (어은동)
(72) 발명자
박상배
인천 연수구 비류대로278번길 18-14, 다동 301호 (청학동, 청학파크맨션)
(74) 대리인
지관영, 김용인

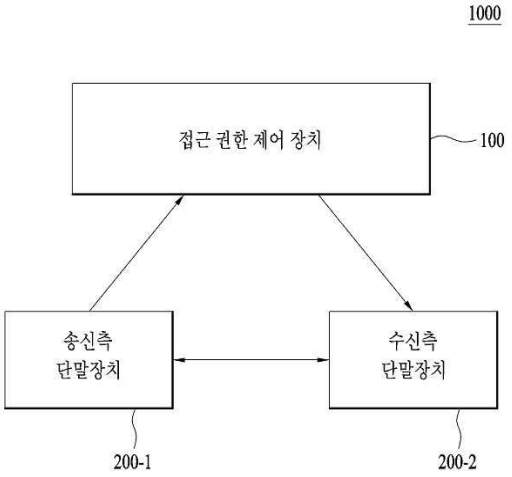
전체 청구항 수 : 총 9 항 심사관 : 하정훈

(54) 발명의 명칭 **접근 권한 제어 장치, 단말 장치를 포함하는 접근 권한 제어 시스템 및 암호화 및 복호화 방법, 접근 권한 제어 방법**

(57) 요 약

접근 권한 제어 방법이 개시된다. 접근 권한 제어 방법은 이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하는 단계, 생성된 환경 변수를 출력하는 단계, 단말 장치로부터 이벤트 정보를 수신하는 단계 및 수신된 이벤트 정보로부터 이벤트 발생 조건을 판단하고, 이벤트가 발생하면 복호를 위한 이벤트에 대응하는 개인 키를 생성하는 단계를 포함한다. 이에 따라, 접근 권한 제어 방법은 메시지에 대한 접근을 세부적으로 통제할 수 있어 보안성을 향상시킬 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하는 단계;

상기 생성된 환경 변수를 출력하는 단계;

단말 장치로부터 이벤트 정보를 수신하는 단계; 및

상기 수신된 이벤트 정보로부터 이벤트 발생 조건을 판단하고, 이벤트가 발생하면 복호화를 위한 상기 이벤트에 대응하는 개인 키를 생성하는 단계;를 포함하고

상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 정보 중 적어도 하나를 포함하는 것을 특징으로 하며,

상기 복호화는 상기 기 설정된 시점, 상기 기 설정된 기간 및 상기 기 설정된 단계에서만 복호화하는 것을 특징으로 하는 접근 권한 제어 방법.

청구항 2

암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화하는 단계;

상기 암호화된 메시지를 수신측 단말 장치로 전송하는 단계; 및

상기 이벤트 정보를 상기 접근 권한 제어 장치로 전송하는 단계;를 포함하고

상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 송신측 단말 장치의 암호화 방법.

청구항 3

제2항에 있어서,

상기 암호화 키는,

수신측 단말 장치의 공개 키 또는 상기 송신측 단말 장치의 개인 키이고,

상기 메시지를 암호화하는 단계는,

상기 수신측 단말 장치의 공개 키 및 상기 이벤트 정보를 공개 키로 이용하여 상기 메시지를 암호화하거나, 상기 송신측 단말 장치의 개인 키로 전자 서명하고 상기 이벤트 정보를 공개 키로 이용하여 상기 메시지를 암호화하는 것을 특징으로 하는 송신측 단말 장치의 암호화 방법.

청구항 4

암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 암호화된 메시지를 송신측 단말 장치로부터 수신하는 단계;

이벤트 발생 여부를 판단하는 단계;

이벤트가 발생하면 접근 권한 제어 장치에서 생성된 상기 이벤트에 대응하는 개인 키를 수신하는 단계; 및

복호화 키 및 상기 수신된 이벤트에 대응하는 개인 키를 이용하여 상기 암호화된 메시지를 복호화하는 단계;를 포함하고

상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 수신측 단말 장치의 복호화 방법.

청구항 5

제4항에 있어서,

상기 복호화 키는,

상기 수신측 단말 장치의 개인 키 또는 송신측 단말 장치의 공개 키이고,

상기 메시지를 복호화하는 단계는,

상기 수신측 단말 장치의 개인 키 및 상기 이벤트에 대응하는 개인 키를 이용하여 상기 메시지를 복호화하거나, 상기 송신측 단말 장치의 공개 키와 상기 이벤트에 대응하는 개인 키를 이용하여 메시지를 확인하는 것을 특징으로 하는 수신측 단말 장치의 복호화 방법.

청구항 6

이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하는 제어부;

상기 생성된 환경 변수를 출력하는 출력부; 및

단말 장치로부터 이벤트 정보를 수신하는 통신부;를 포함하며,

상기 제어부는,

상기 수신된 이벤트 정보로부터 이벤트 발생 조건을 판단하고, 이벤트가 발생하면 복호화를 위한 상기 이벤트에 대응하는 개인 키를 생성하며,

상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 정보 중 적어도 하나를 포함하는 접근 권한 제어 장치.

청구항 7

암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화하는 제어부;

상기 암호화된 메시지를 수신측 단말 장치로 전송하고, 상기 이벤트 정보를 상기 접근 권한 제어 장치로 전송하는 통신부;를 포함하고

상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 송신측 단말 장치.

청구항 8

암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 암호화된 메시지를 송신측 단말 장치로부터 수신하는 통신부; 및

이벤트 발생 여부를 판단하는 제어부;를 포함하며,

이벤트가 발생하면, 상기 통신부는,

접근 권한 제어 장치에서 생성된 상기 이벤트에 대응하는 개인 키를 수신하고,

상기 제어부는,

복호화 키 및 상기 수신된 이벤트에 대응하는 개인 키를 이용하여 상기 암호화된 메시지를 복호화하고,

상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 수신측 단말 장치.

청구항 9

이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하여 출력하는 접근 권한 제어 장치;

암호화 키 및 상기 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화하고, 상기 암호화된 메시지 및 상기 이벤트 정보를 전송하는 송신측 단말 장치; 및

상기 암호화된 메시지를 수신하는 수신측 단말 장치;를 포함하며,

상기 접근 권한 제어 장치는,

상기 이벤트 정보를 수신하여 이벤트 발생 조건을 판단하고, 이벤트가 발생하면 복호화를 위한 상기 이벤트에 대응하는 개인 키를 생성하여 전송하고,

상기 수신측 단말 장치는,

이벤트가 발생하면, 상기 접근 권한 제어 장치에서 생성된 상기 이벤트에 대응하는 개인 키를 수신하고, 복호화 키 및 상기 수신된 이벤트에 대응하는 개인 키를 이용하여 상기 암호화된 메시지를 복호화하고

상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 정보 중 적어도 하나를 포함하는 것을 특징으로 하는 접근 권한 제어 시스템.

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 접근 권한 제어 장치, 단말 장치를 포함하는 접근 권한 제어 시스템 및 암호화 및 복호화 방법, 접근 권한 제어 방법에 관한 것으로, 더욱 상세하게는 일정한 조건을 이용하여 접근 권한을 제어하는 접근 권한 제어 장치, 단말 장치를 포함하는 접근 권한 제어 시스템 및 암호화 및 복호화 방법, 접근 권한 제어 방법에 관한 것이다.

배 경 기 술

[0002] 정보 통신의 발전에 따라 사용자들은 다양한 유/무선 통신 방식을 이용하여 메시지를 주고 받는다. 메시지 중에는 공개를 위한 것도 있지만, 특정 사용자에게만 알리기 위한 것도 있고, 특정 조건을 만족한 경우에만 알리기 위한 것도 있다.

[0003] 일반적으로 특정 사용자에게만 알리기 위한 메시지는 암호화 및 복호화 과정을 거치게 된다. 즉, 송신측 사용자는 수신측 사용자의 공개 키를 이용하여 메시지를 암호화하여 전송한다. 수신측 사용자는 암호화된 메시지를 수신하여 자신의 개인 키를 이용하여 메시지를 복호화한다. 특정 공개 키로 암호화된 메시지는 대응되는 특정 개인 키를 이용해야 복호화할 수 있다. 그리고, 특정 개인 키는 특정 개인만이 소유하고 있으므로 메시지의 비밀이 유지될 수 있다.

[0004] 그러나, 위와 같은 방법은 메시지를 수신하는 순간 메시지를 복호화할 수 있으므로 특정 조건을 만족한 경우에 메시지를 확인할 수 있도록 하는 것이 불가능하다. 예를 들어, 기사의 엠바고(news embargo)와 같이, 사용자가 미리 언론사에 기사를 배포하지만 특정 시점까지는 비밀을 유지해야 하는 경우가 있다. 그리고, 공모, 입찰 등과 같이, 응모자가 미리 서류를 접수시키지만 접수 마감까지 서류에 대한 접근을 막을 필요가 있는 경우가 있다.

[0005] 따라서, 특정 조건을 만족한 경우 메시지를 확인할 수 있는 접근 제한 기술에 대한 필요성이 대두되고 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명은 상술한 필요성에 따라 안출된 것으로, 본 발명의 목적은 특정 조건을 이용하여 메시지를 암호화하고 복호화하는 접근 권한 제어 장치, 단말 장치를 포함하는 접근 권한 제어 시스템 및 암호화 및 복호화 방법, 접

근 권한 제어 방법을 제공함에 있다.

과제의 해결 수단

[0007] 본 발명의 상술한 목적을 달성하기 위한 일 실시 예에 따르면, 접근 권한 제어 방법은 이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하는 단계, 상기 생성된 환경 변수를 출력하는 단계, 단말 장치로부터 이벤트 정보를 수신하는 단계 및 상기 수신된 이벤트 정보로부터 이벤트 발생 조건을 판단하고, 이벤트가 발생하면 복호를 위한 상기 이벤트에 대응하는 개인 키를 생성하는 단계를 포함한다.

[0008] 그리고, 상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 조건 중 적어도 하나를 포함할 수 있다.

[0009] 본 발명의 상술한 목적을 달성하기 위한 일 실시 예에 따르면, 송신측 단말 장치의 암호화 방법은 암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화하는 단계, 상기 암호화된 메시지를 수신측 단말 장치로 전송하는 단계 및 상기 이벤트 정보를 상기 접근 권한 제어 장치로 전송하는 단계를 포함한다.

[0010] 그리고, 상기 암호화 키는 수신측 단말 장치의 공개 키 또는 상기 송신측 단말 장치의 개인 키이고, 상기 메시지를 암호화하는 단계는 상기 수신측 단말 장치의 공개 키 및 상기 이벤트 정보를 공개 키로 이용하여 상기 메시지를 암호화하거나, 상기 송신측 단말 장치의 개인 키로 전자 서명하고 상기 이벤트 정보를 공개 키로 이용하여 상기 메시지를 암호화할 수 있다.

[0011] 또한, 상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 조건 중 적어도 하나를 포함할 수 있다.

[0012] 본 발명의 상술한 목적을 달성하기 위한 일 실시 예에 따르면, 수신측 단말 장치의 복호화 방법은 암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 암호화된 메시지를 송신측 단말 장치로부터 수신하는 단계, 이벤트 발생 여부를 판단하는 단계, 이벤트가 발생하면 접근 권한 제어 장치에서 생성된 상기 이벤트에 대응하는 개인 키를 수신하는 단계 및 복호화 키 및 상기 수신된 이벤트에 대응하는 개인 키를 이용하여 상기 암호화된 메시지를 복호화하는 단계를 포함한다.

[0013] 그리고, 상기 복호화 키는 상기 수신측 단말 장치의 개인 키 또는 송신측 단말 장치의 공개 키이고, 상기 메시지를 복호화하는 단계는 상기 수신측 단말 장치의 개인 키 및 상기 이벤트에 대응하는 개인 키를 이용하여 상기 메시지를 복호화하거나, 상기 송신측 단말 장치의 공개 키와 상기 이벤트에 대응하는 개인 키를 이용하여 메시지를 확인할 수 있다.

[0014] 또한, 상기 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 조건 중 적어도 하나를 포함할 수 있다.

[0015] 본 발명의 상술한 목적을 달성하기 위한 일 실시 예에 따르면, 접근 권한 제어 장치는 이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하는 제어부, 상기 생성된 환경 변수를 출력하는 출력부 및 단말 장치로부터 이벤트 정보를 수신하는 통신부를 포함하며, 상기 제어부는 상기 수신된 이벤트 정보로부터 이벤트 발생 조건을 판단하고, 이벤트가 발생하면 복호를 위한 상기 이벤트에 대응하는 개인 키를 생성한다.

[0016] 본 발명의 상술한 목적을 달성하기 위한 일 실시 예에 따르면, 송신측 단말 장치는 암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화하는 제어부, 상기 암호화된 메시지를 수신측 단말 장치로 전송하고, 상기 이벤트 정보를 상기 접근 권한 제어 장치로 전송하는 통신부를 포함한다.

[0017] 본 발명의 상술한 목적을 달성하기 위한 일 실시 예에 따르면, 수신측 단말 장치는 암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 암호화된 메시지를 송신측 단말 장치로부터 수신하는 통신부 및 이벤트 발생 여부를 판단하는 제어부를 포함하며, 이벤트가 발생하면, 상기 통신부는 접근 권한 제어 장치에서 생성된 상기 이벤트에 대응하는 개인 키를 수신하고, 상기 제어부는 복호화 키 및 상기 수신된 이벤트에 대응하는 개인 키를 이용하여 상기 암호화된 메시지를 복호화한다.

[0018] 본 발명의 상술한 목적을 달성하기 위한 일 실시 예에 따르면, 접근 권한 제어 시스템은 이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하여 출력하는 접근 권한 제어 장치, 암호화 키 및 상기 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화하고, 상기 암호화된 메시지 및 상기 이벤트 정보를 전송하

는 송신측 단말 장치 및 상기 암호화된 메시지를 수신하는 수신측 단말 장치를 포함하며, 상기 접근 권한 제어 장치는 상기 이벤트 정보를 수신하여 이벤트 발생 조건을 판단하고, 이벤트가 발생하면 복호를 위한 상기 이벤트에 대응하는 개인 키를 생성하여 전송하고, 상기 수신측 단말 장치는 이벤트가 발생하면, 상기 접근 권한 제어 장치에서 생성된 상기 이벤트에 대응하는 개인 키를 수신하고, 복호화 키 및 상기 수신된 이벤트에 대응하는 개인 키를 이용하여 상기 암호화된 메시지를 복호화한다.

발명의 효과

[0019] 상술한 다양한 실시 예에 따르면, 접근 권한 제어 장치, 단말 장치를 포함하는 접근 권한 제어 시스템 및 암호화 및 복호화 방법, 접근 권한 제어 방법은 메시지에 대한 접근을 세부적으로 통제할 수 있어 보안성을 향상시킬 수 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 일 실시 예에 따른 접근 권한 제어 시스템을 설명하는 도면.

도 2는 본 발명의 일 실시 예에 따른 접근 권한 제어 장치의 블록도.

도 3은 본 발명의 일 실시 예에 따른 단말 장치의 블록도.

도 4는 본 발명의 일 실시 예에 따른 이벤트 기반 암호 메시지를 설명하는 도면.

도 5는 본 발명의 다른 실시 예에 따른 이벤트 기반 암호 메시지를 설명하는 도면.

도 6은 본 발명의 일 실시 예에 따른 접근 권한 제어 방법의 흐름도.

도 7은 본 발명의 일 실시 예에 따른 암호화 방법의 흐름도.

도 8은 본 발명의 일 실시 예에 따른 복호화 방법의 흐름도.

발명을 실시하기 위한 구체적인 내용

[0021] 이하 상기의 목적을 구체적으로 실현할 수 있는 본 발명의 바람직한 실시 예를 첨부한 도면을 참조하여 설명한다. 이때 도면에 도시되고 또 이것에 의해서 설명되는 본 발명의 구성과 작용은 적어도 하나의 실시 예로서 설명되는 것이며, 이것에 의해서 본 발명의 기술적 사상과 그 핵심 구성 및 작용이 제한되지는 않는다.

[0022] 본 발명에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어를 선택하였으나, 이는 당해 기술 분야에 종사하는 기술자의 의도 또는 관례 또는 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 발명에서 사용되는 용어는 단순한 용어의 명칭이 아닌 그 용어가 가지는 의미와 본 발명의 전반에 걸친 내용을 토대로 정의되어야 함을 밝혀두고자 한다.

[0023] 도 1은 본 발명의 일 실시 예에 따른 접근 권한 제어 시스템을 설명하는 도면이다.

[0024] 도 1을 참조하면, 접근 권한 제어 시스템(1000)은 접근 권한 제어 장치(100), 송신측 단말 장치(200-1), 수신측 단말 장치(200-2)를 포함한다. 접근 권한 제어 장치(100)는 이벤트 기반 암호를 사용하기 위한 환경 변수를 생성하여 출력한다. 환경 변수는 기존과 같은 기본적인 암호 구조를 기초로 일정 조건을 입력하여 조건을 포함하는 암호 메시지를 생성할 수 있는 구조를 의미한다. 예를 들어, 송신측 사용자는 환경 변수를 포함하는 공개 키를 이용하여 2013년 11월 25일 18시라는 이벤트 정보를 함께 입력하여 메시지를 암호화할 수 있다. 수신측 사용자는 공개 키에 대응하는 개인 키만으로 메시지를 복호화할 수 없고, 이벤트 정보인 2013년 11월 24일 18시라는 시간 조건을 만족할 때 메시지를 복호화할 수 있다.

[0025] 송신측 단말 장치(200-1)는 암호화 키 및 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화하고, 암호화된 메시지를 수신측 단말 장치(200-2)로 전송한다. 암호화 키는 수신측 단말 장치(200-2)의 공개 키 또는 송신측 단말 장치(200-1)의 개인 키일 수 있다. 즉, 송신측 단말 장치(200-1)는 수신측 단말 장치(200-2)의 공개 키와 환경 변수를 이용하여 이벤트 정보를 공캐 키로 이용하여 메시지를 암호화할 수 있다. 또는, 송신측 단말 장치(200-1)는 송신측 단말 장치(200-1)의 개인 키로 전자 서명하고 환경 변수를 이용하여 이벤트 정보를 공개 키로 이용하여 메시지를 암호화할 수 있다.

[0026] 그리고, 송신측 단말 장치(200-1)는 이벤트 정보를 접근 권한 제어 장치(100)로 전송할 수 있다. 일 실시 예로

서, 이벤트 정보를 접근 권한 제어 장치(100)로 전송하는 경우, 접근 권한 제어 장치(100)는 이벤트가 발생할 때 세션 키로 암호화한 개인 키를 수신측 단말 장치(200-2)로 전송할 수 있다. 다른 실시 예로서, 이벤트 정보를 접근 권한 제어 장치(100)로 전송하지 않는 경우, 접근 권한 제어 장치(100)는 임의의 시간에 세션 키로 암호화한 개인 키를 수신측 단말 장치(200-2)로 전송할 수 있다. 이때, 수신측 단말 장치(200-2)는 환경 변수를 이용하여 이벤트 정보를 포함하여 암호화된 메시지를 이벤트가 발생할 때 수신한 개인 키를 이용하여 복호화할 수 있다.

[0027] 일 실시 예로서, 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 조건 중 적어도 하나일 수 있다. 예를 들어, 기 설정된 시점 정보는 2013년 11월 25일 18시와 같은 한 시점에 대한 정보일 수 있다. 즉, 암호화된 메시지는 2013년 11월 25일 18시가 되어야 복호화될 수 있다. 기 설정된 기간 정보는 2013년 11월 25일 0시부터 11월 28일 24시까지와 같은 특정 기간 또는 2013년 11월 25일 0시부터 일주일간과 같은 특정 기간에 대한 정보일 수 있다. 즉, 암호화된 메시지는 특정 기간 동안만 복호화될 수 있고, 특정 기간 전 또는 후에는 복호화될 수 없다. 기 설정된 단계 조건은 1단계 또는 입력 단계와 같은 단계 정보일 수 있다. 즉, 1단계 또는 입력 단계에 대한 접근 권한을 가지고 있는 수신자만이 해당 메시지를 복호화할 수 있다.

[0028] 수신측 단말 장치(200-2)는 암호화된 메시지를 수신한다. 수신측 단말 장치(200-2)는 접근 권한 제어 장치(100)로부터 세션 키로 암호화된 개인 키를 수신한다. 수신측 단말 장치(200-2)는 이벤트가 발생하면 수신한 개인 키 및 복호화 키를 이용하여 암호화된 메시지를 복호화한다. 복호화 키는 수신측 단말 장치(200-2)의 개인 키 또는 송신측 단말 장치(200-1)의 공개 키일 수 있다. 즉, 메시지가 수신측 단말 장치(200-2)의 공개 키와 환경 변수를 기초로 이벤트 정보를 공개 키로 이용하여 암호화된 경우, 수신측 단말 장치(200-2)는 수신측 단말 장치(200-2)의 개인 키 및 이벤트에 대응하여 수신한 개인 키를 이용하여 메시지를 복호화할 수 있다. 또는, 메시지가 송신측 단말 장치(200-1)의 개인 키로 전자 서명하고 환경 정보를 기초로 이벤트 정보를 공개 키로 이용하여 암호화된 경우, 수신측 단말 장치(200-2)는 송신측 단말 장치(200-1)의 공개 키 및 이벤트에 대응하여 수신한 개인 키를 이용하여 메시지를 복화화할 수 있다.

[0029] 아래에서는 접근 권한 제어 장치(100), 단말 장치(200-1, 200-2)의 블록도에 대해 설명하기로 한다.

[0030] 도 2는 본 발명의 일 실시 예에 따른 접근 권한 제어 장치의 블록도이다.

[0031] 도 2를 참조하면, 접근 권한 제어 장치(100)는 제어부(110), 출력부(120) 및 통신부(130)를 포함한다.

[0032] 제어부(110)는 이벤트 기반 암호를 사용하기 위한 환경 변수를 생성한다. 그리고, 제어부(11)는 단말 장치로부터 이벤트 정보를 수신하면, 수신된 이벤트 정보로부터 이벤트 발생 조건을 판단한다. 제어부(110)는 이벤트가 발생하면 복호를 위한 이벤트에 대응되는 개인 키를 생성한다.

[0033] 출력부(120)는 생성된 환경 변수를 출력한다. 일 실시 예로서, 출력부(120)는 통신부(130)로 구현될 수 있으며, 이 경우, 환경 변수는 다양한 유/무선 통신 방식을 이용하여 출력될 수 있다. 통신부(130)는 단말 장치로부터 이벤트 정보를 수신한다. 또한, 통신부(130)는 생성된 이벤트에 대응되는 개인 키를 수신측 단말 장치로 전송할 수 있다.

[0034] 도 3은 본 발명의 일 실시 예에 따른 단말 장치의 블록도이다.

[0035] 도 3을 참조하면, 단말 장치(300)는 제어부(310) 및 통신부(320)를 포함한다. 단말 장치(300)는 송신측 또는 수신측으로 동작할 수 있다. 일 실시 예로서, 단말 장치(300)가 송신측으로 동작하는 경우에 대해 설명한다.

[0036] 제어부(310)는 암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화한다. 암호화 키는 수신측의 공개 키 또는 송신측의 개인 키일 수 있다. 제어부(310)는 수신측의 공개 키 및 이벤트 정보를 공개 키로 이용하여 메시지를 암호화할 수 있다. 또는, 제어부(310)는 송신측의 개인 키로 전자 서명하고 이벤트 정보를 공개 키로 이용하여 메시지를 암호화할 수 있다.

[0037] 제어부(310)는 접근 권한 제어 장치로부터 출력된 환경 변수 및 이벤트 정보를 기초로 공개 키로 이용할 수 있다. 즉, 환경 변수는 접근 권한 제어 장치의 기본적인 공개 키에 이벤트 정보를 더 포함할 수 있는 구조를 의미한다. 개념적으로 송신측이 접근 권한 제어 장치의 공개 키에 이벤트 정보를 추가하여 공개 키로 이용하는 것을 의미한다. 이와 같이, 제어부(310)는 환경 변수와 이벤트 정보를 이용한 접근 권한 제어 장치의 공개 키 및 암호화 키를 이용하여 메시지를 암호화한다.

[0038] 통신부(320)는 암호화된 메시지를 수신측으로 전송하고, 이벤트 정보를 접근 권한 제어 장치로 전송한다.

[0039] 다음으로, 단말 장치(300)가 수신측으로 동작하는 경우에 대해 설명한다.

[0040] 통신부(320)는 암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 암호화된 메시지를 송신측으로부터 수신한다. 그리고, 통신부(320)는 이벤트가 발생하면, 접근 권한 제어 장치에서 생성된 이벤트에 대응하는 개인 키를 수신한다. 접근 권한 제어 장치는 수신측과 상호 인증을 통해 세션 키를 생성하고, 개인 키를 암호화하여 전송한다. 암호화된 개인 키는 수신측에서 복호화된다.

[0041] 제어부(310)는 이벤트 발생 여부를 판단한다. 그리고, 제어부(310)는 복호화 키 및 수신된 이벤트에 대응하는 개인 키를 이용하여 암호화된 메시지를 복호화한다. 복호화 키는 수신측의 개인 키 또는 송신측의 공개 키일 수 있다. 제어부(310)는 수신측의 개인 키 및 이벤트에 대응하는 개인 키를 이용하여 메시지를 복호화할 수 있다. 또는, 제어부(310)는 송신측의 공개 키 및 이벤트에 대응하는 개인 키를 이용하여 메시지를 복호화하여 확인할 수 있다.

[0042] 이벤트 정보는 기 설정된 시점 정보, 기 설정된 기간 정보 및 기 설정된 단계 조건 중 적어도 하나를 포함할 수 있다. 일 실시 예로서, 거대 과학 실험의 경우, 데이터는 여러 단계로 나누어 가공된 후, 전세계에 분포되어 있는 분산 컴퓨팅을 활용하여 처리될 수 있다. 이 경우, 데이터는 각 단계를 이벤트 정보로 해서 암호화되고 저장될 수 있다. 접근 권한 제어 장치는 가공 단계에 따라 각 단계에 해당하는 개인 키를 생성하여 전송할 수 있다. 수신측은 메시지의 단계에 해당하는 이벤트 정보를 확인하고, 대응되는 개인 키를 수신하여 메시지의 복호에 이용할 수 있다.

[0043] 다른 실시 예로서, 송신측은 특정 기간을 이벤트 정보로 하여 메시지를 암호화하여 수신측으로 전송할 수 있다. 수신측은 해당 기간 동안만 접근 권한 제어 장치로 부터 이벤트에 대응하는 개인 키를 수신하여 메시지의 복호에 이용할 수 있다. 해당 기간이 지나면, 수신측은 이벤트에 대응하는 개인 키를 수신할 수 없으므로 메시지 복호를 할 수 없다.

[0044] 또 다른 실시 예로서, 송신측은 수신측으로 비상용 메시지를 비상 경보 이벤트를 공개 키로 하여 암호화하고 전송할 수 있다. 접근 권한 제어 장치는 이벤트에 해당하는 비상 경보의 발생을 판단하면, 대응하는 개인 키를 생성하여 수신측에 전송한다. 수신측은 비상 경보 이벤트에 대응하는 개인 키를 수신하여 비상용 메시지를 복호화할 수 있다.

[0045] 도 4 및 도 5는 본 발명의 일 실시 예에 따른 이벤트 기반 암호 메시지를 설명하는 도면이다.

[0046] 도 4를 참조하면, 수신측 공개 키로 암호화된 이벤트 기반 암호 메시지 구조(10)가 도시되어 있다. Enc(Pub, Message)(11)는 수신측 공개 키(Pub)로 암호화된 메시지(Message)를 의미한다. Enc(KS, End(Pub, Message))(12)는 세션 키(KS)로 다시 암호화를 한 암호화된 메시지(11)를 의미한다. 세션 키(KS)는 특정 시간(time)과 같은 이벤트 정보를 이용하여 암호화된다(13). 따라서, 특정 시점과 같은 이벤트가 발생되면, 세션 키가 생성되어 복호화되고, 순차적으로 메시지의 복호 과정이 수행될 수 있다.

[0047] 도 5를 참조하면, 송신측 개인 키로 암호화된 이벤트 기반 암호 메시지 구조(20)가 도시되어 있다. Sig(Prv, Message)(21)는 송신측 개인 키(Prv)로 메시지(Message)를 암호화한 전자 서명을 의미한다. Enc(KS, Sig(Prv, Message))(22)는 세션 키(KS)로 다시 암호화를 한 암호화된 전자 서명(21)을 의미한다. 세션 키(KS)는 특정 시간(time)과 같은 이벤트 정보를 이용하여 암호화된다(23). 따라서, 특정 시점과 같은 이벤트가 발생되면, 세션 키가 생성되어 복호화되고, 순차적으로 메시지의 복호 과정이 수행될 수 있다.

[0048] 지금까지 접근 권한 제어 장치, 단말 장치의 구성 및 암호 메시지의 구조에 대해 설명하였다. 아래에서는 접근 권한 제어 방법, 암호화 방법 및 복호화 방법의 흐름도에 대해 설명한다.

[0049] 도 6은 본 발명의 일 실시 예에 따른 접근 권한 제어 방법의 흐름도이다.

[0050] 도 6을 참조하면, 접근 권한 제어 장치는 환경 변수를 생성한다(S610). 환경 변수는 이벤트 기반 암호를 사용하기 위한 것이다. 접근 권한 제어 장치는 특정 이벤트가 발생되면 수신측 단말 장치와 통신을 할 수 있는 세션 키를 생성한다. 접근 권한 제어 장치는 환경 변수를 출력한다(S620). 따라서, 송신측 단말 장치는 별도로 접근 권한 제어 장치에 접속하지 않더라도 메시지를 암호화하여 수신측 단말 장치로 전송할 수 있다. 접근 권한 제어 장치는 송신측 단말 장치로부터 이벤트 정보를 수신할 수 있다.

[0051] 접근 권한 제어 장치는 이벤트의 발생 여부를 판단한다(S630). 접근 권한 제어 장치는 이벤트가 발생하지 않으면, 연속적으로 이벤트 발생 여부를 확인한다. 그리고, 접근 권한 제어 장치는 이벤트가 발생하면 이벤트에 대응하는 개인 키를 생성한다(S640). 접근 권한 제어 장치는 수신측 단말 장치와 상호 인증 과정을 수행하고, 세

션 키로 암호화된 이벤트에 대응하는 개인 키를 생성하여 수신측 단말 장치로 전송할 수 있다.

[0052] 이벤트 정보는 특정 시간이 되면 발생하는 기 설정된 시점 정보, 특정 기간 동안 발생하는 기 설정된 기간 정보, 특정 단계에 대해서만 유효한 기 설정된 단계 조건 등이 될 수 있다.

[0053] 도 7은 본 발명의 일 실시 예에 따른 암호화 방법의 흐름도이다.

[0054] 도 7을 참조하면, 송신측 단말 장치는 암호화 키 및 접근 권한 제어 장치로부터 출력된 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메시지를 암호화한다(S710). 암호화 키는 수신측 단말 장치의 공개 키 또는 송신측 단말 장치의 개인 키일 수 있다.

[0055] 송신측 단말 장치는 암호화된 메시지를 수신측 단말 장치로 전송한다(S720). 송신측 단말 장치는 이벤트 정보를 접근 권한 제어 장치로 전송한다(S730). 경우에 따라, 송신측 단말 장치는 이벤트 정보를 접근 권한 제어 장치로 전송하지 않을 수 있다. 예를 들어, 이벤트 정보가 시간 정보인 경우, 수신측 단말 장치는 시간 정보를 확인하고 이벤트의 발생 시간이 되면, 접근 권한 제어 장치로 시간 정보에 대응하는 개인 키 전송을 요청할 수도 있다.

[0056] 도 8은 본 발명의 일 실시 예에 따른 복호화 방법의 흐름도이다.

[0057] 도 8을 참조하면, 수신측 단말 장치는 암호화 키 및 환경 변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 암호화된 메시지를 수신한다(S810). 수신측 단말 장치는 이벤트 발생 여부를 판단한다(S820).

[0058] 이벤트가 발생하지 않으면 이벤트 발생 여부를 계속 판단하고, 이벤트가 발생하면 접근 권한 제어 장치에서 생성된 이벤트에 대응하는 개인 키를 수신한다(S830). 예를 들어, 이벤트가 발생하면, 수신측 단말 장치가 접근 권한 제어 장치로 해당 이벤트에 대응하는 개인 키의 전송을 요청할 수 있다. 수신측 단말 장치는 접근 권한 제어 장치와 상호 인증 과정을 거쳐 세션 키로 암호화된 개인 키를 수신할 수 있다. 또는, 이벤트가 발생하면, 접근 권한 제어 장치가 해당 이벤트에 대응하는 개인 키의 전송을 위해 수신측 단말 장치로 상호 인증 과정을 요청할 수도 있다.

[0059] 수신측 단말 장치는 복호화 키 및 수신된 이벤트에 대응하는 개인 키를 이용하여 암호화된 메시지를 복호화한다(S840). 복호화 키는 수신측 단말 장치의 개인 키 또는 송신측 단말 장치의 공개 키일 수 있다.

[0060] 구체적인 과정은 상술하였으므로 설명을 생략하기로 한다.

[0061] 본 발명에 따른 접근 권한 제어 장치, 단말 장치를 포함하는 접근 권한 제어 시스템 및 암호화 및 복호화 방법, 접근 권한 제어 방법은 상술한 실시 예들의 구성과 방법으로 한정되어 적용되는 것이 아니라, 각 실시 예들의 전부 또는 일부가 선택적으로 조합되어 다양한 변형이 이루어질 수 있다.

[0062] 한편, 본 발명의 접근 권한 제어 방법은 접근 권한 제어 장치에 구비된 프로세서가 읽을 수 있는 저장 매체에 프로세서가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 또한 본 발명의 암호화 방법 및 복호화 방법은 단말 장치에 구비된 프로세서가 읽을 수 있는 저장 매체에 프로세사가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 프로세서가 읽을 수 있는 저장 매체는 프로세서에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 저장 장치를 포함한다. 프로세서가 읽을 수 있는 저장 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한, 인터넷을 통한 전송 등과 같은 캐리어 웨이브의 형태로 구현되는 것도 포함한다. 또한, 프로세서가 읽을 수 있는 저장 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 프로세서가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0063] 또한, 이상에서는 본 발명의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해돼서는 안 될 것이다.

부호의 설명

[0064] 1000 : 접근 권한 제어 시스템

100 : 접근 권한 제어 장치 110 : 제어부

120 : 출력부 130 : 통신부

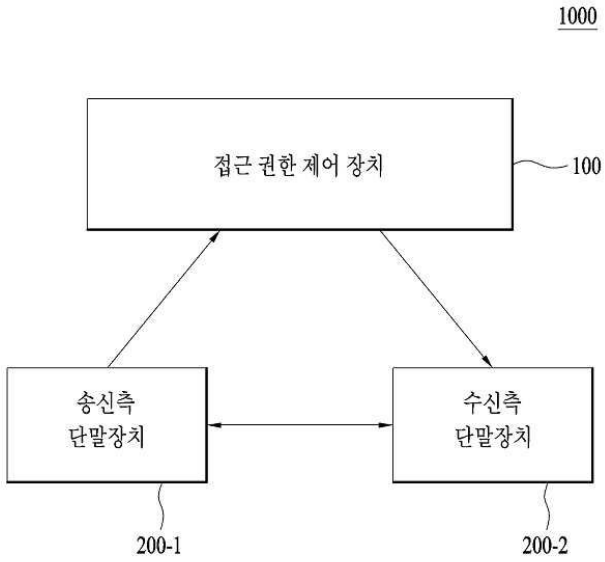
200-1 : 송신측 단말 장치　　200-2 : 수신측 단말 장치

300 : 단말 장치

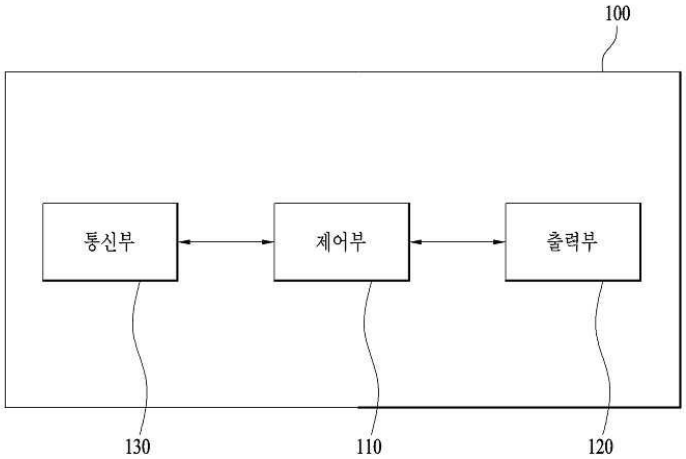
310 : 제어부　　320 : 통신부

도면

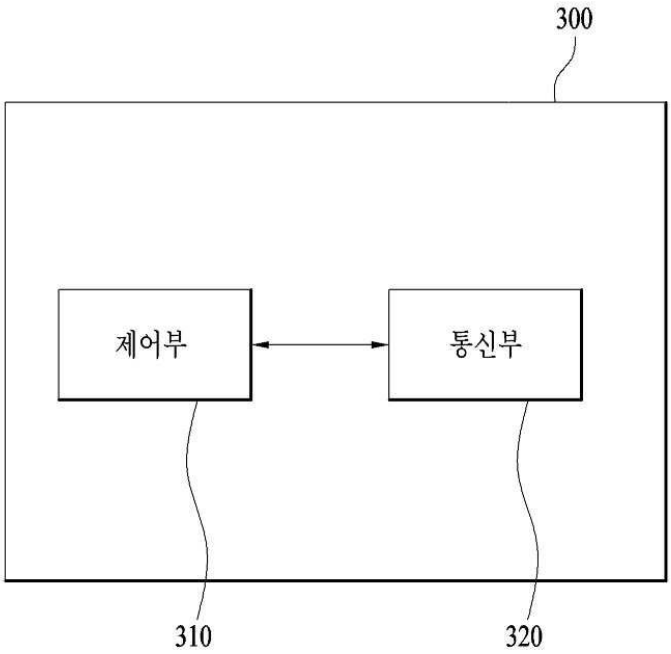
도면1



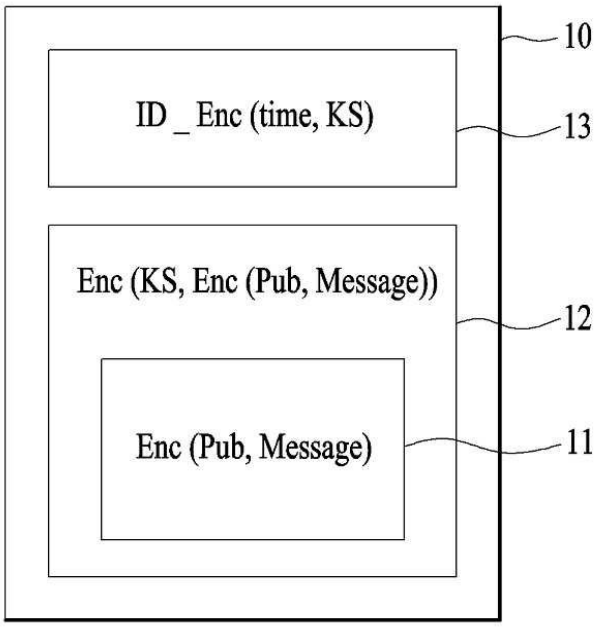
도면2



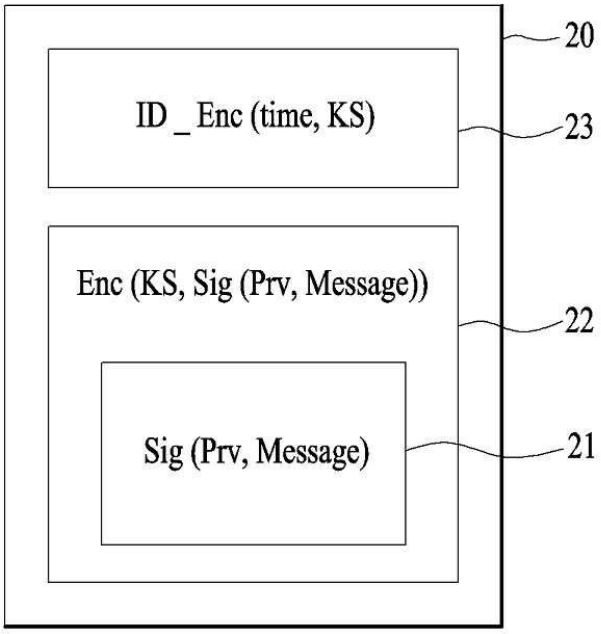
도면3


300
제어부
통신부
310
320

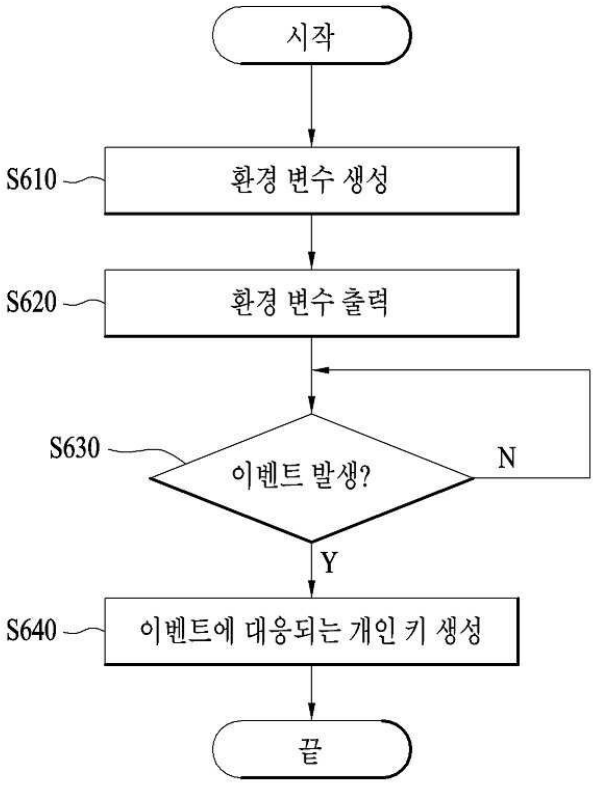
도면4


10
ID _ Enc (time, KS)
13
Enc (KS, Enc (Pub, Message))
12
Enc (Pub, Message)
11

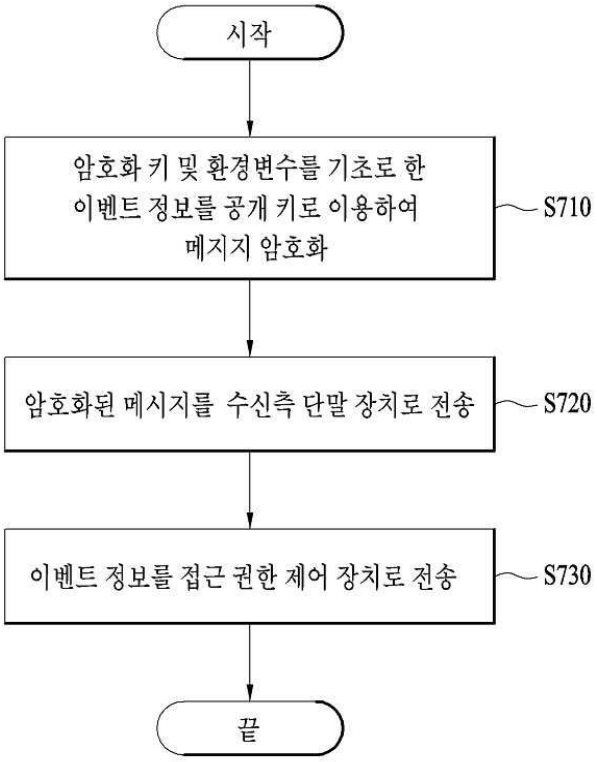
도면5


20
ID _ Enc (time, KS)
23
Enc (KS, Sig (Prv, Message))
22
Sig (Prv, Message)
21

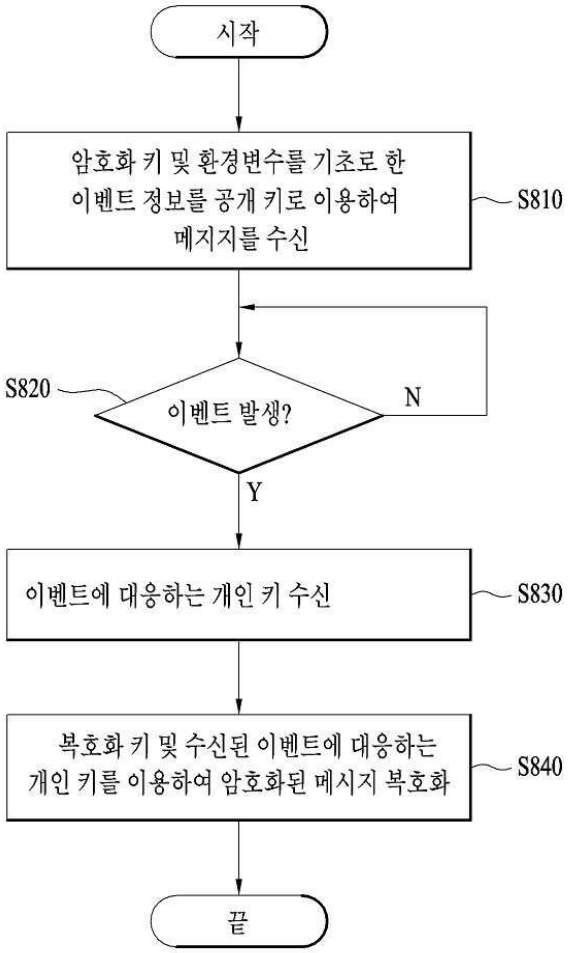
도면6


시작
S610
환경 변수 생성
S620
환경 변수 출력
S630
이벤트 발생?
N
Y
S640
이벤트에 대응되는 개인 키 생성
끝

도면7


시작
암호화 키 및 환경변수를 기초로 한 이벤트 정보를 공개 키로 이용하여 메지지 암호화
S710
암호화된 메시지를 수신측 단말 장치로 전송
S720
이벤트 정보를 접근 권한 제어 장치로 전송
S730
끝

도면8


시작
암호화 키 및 환경변수를 기초로 한
이벤트 정보를 공개 키로 이용하여
메지지를 수신
S810
S820
이벤트 발생?
N
Y
이벤트에 대응하는 개인 키 수신
S830
복호화 키 및 수신된 이벤트에 대응하는
개인 키를 이용하여 암호화된 메시지 복호화
S840
끝