(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년12월28일
(11) 등록번호 10-1004886
(24) 등록일자 2010년12월22일

(51) Int. Cl.
H04N 7/167 (2006.01) *H04L 9/08* (2006.01)
(21) 출원번호 10-2009-0015586
(22) 출원일자 2009년02월25일
심사청구일자 2009년02월25일
(65) 공개번호 10-2010-0096618
(43) 공개일자 2010년09월02일
(56) 선행기술조사문헌
KR1020090012013 A
KR1020060079491 A
KR1020090048682 A

(73) 특허권자
성균관대학교산학협력단
경기 수원시 장안구 천천동 300 성균관대학교내
(72) 발명자
최형기
서울특별시 서초구 반포본동 반포아파트 53동 106호
김정윤
경기도 수원시 장안구 천천동 300 성균관대학교 제2공학관 27313호 인터넷보안연구실
(뒷면에 계속)
(74) 대리인
특허법인이상

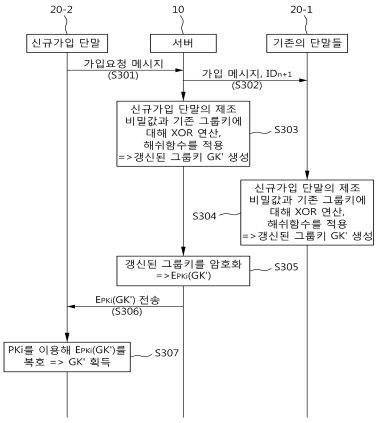
전체 청구항 수 : 총 16 항 심사관 : 조남신

(54) 그룹 키 분배 방법 및 이를 이용한 수신 제한 시스템

(57) 요 약

본 발명, 그룹 키 분배 방법 및 이를 이용한 수신 제한 시스템은, 수신제한 서버 및 적어도 하나의 단말을 포함하는 수신제한 시스템에서 그룹 키를 분배하는 방법에 관한 것으로, 적어도 하나의 단말 각각이, 자신을 제외한 모든 단말 전체에 대한 제조 비밀값을 저장하고, 특정 단말의 그룹 가입 또는 그룹 탈퇴시, 수신제한 서버는 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신함으로써, 전방향 안전성 및 후방향 안전성을 보장함과 동시에 저비용으로 매우 빠른 그룹 키 분배를 실현할 수 있도록 한다.

대 표 도 - 도3



(72) 발명자

김인환

경기도 수원시 장안구 율전동 280-40 403호

김동진

경기도 안양시 동안구 비산 2동 미륭아파트 7동 1007호

특허청구의 범위

청구항 1

수신제한 서버 및 적어도 하나의 단말을 포함하는 수신제한 시스템에서 그룹 키를 분배하는 방법에 있어서,

상기 적어도 하나의 단말 각각이, 자신을 제외한 모든 단말 전체에 대한 제조 비밀값을 저장하는 단계; 와

특정 단말의 그룹 가입 또는 그룹 탈퇴시, 기존에 사용하던 그룹 키 및 상기 특정 단말의 제조 비밀값에 대해 XOR 연산을 수행하고, 상기 연산의 결과에 대해 해쉬함수를 적용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는 단계를 포함하는, 그룹 키 분배 방법.

청구항 2

청구항 1에 있어서,

상기 모든 단말 전체는,

기존에 존재하는 적어도 하나의 단말 및 향후 제조가 될 것으로 예상되는 모든 단말을 포함하는, 그룹 키 분배 방법.

청구항 3

청구항 1에 있어서,

특정 단말의 그룹 가입 또는 그룹 탈퇴시,

상기 특정 단말을 제외한 상기 수신제한 시스템에 포함된 나머지 모든 단말이, 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는 단계를 더 포함하는, 그룹 키 분배 방법.

청구항 4

청구항 1 또는 청구항 3에 있어서,

상기 특정 단말을 제외한 상기 수신제한 시스템에 포함된 나머지 모든 단말이 생성하는 새로운 그룹 키는,

상기 특정 단말의 제조 비밀값과 기존에 사용하던 그룹키에 대해 XOR 연산을 수행하고, 상기 연산 결과에 대해 해쉬함수를 적용하여 생성되는 것을 특징으로 하는, 그룹 키 분배 방법.

청구항 5

청구항 1에 있어서,

상기 수신제한 서버의 그룹키 갱신 단계에서 상기 특정 단말이 그룹에 새로이 가입하고자 하는 경우, 상기 그룹 키 갱신 단계는,

상기 수신제한 서버가 상기 새로운 그룹 키를 암호화하는 단계; 와

상기 수신제한 서버가 상기 암호화된 새로운 그룹키를 상기 특정 단말로 전송하는 단계를 포함하는, 그룹 키 분배 방법.

청구항 6

청구항 5에 있어서,

상기 새로운 그룹 키에 대한 암호화는,

상기 특정 단말과 상기 수신제한 서버 사이에만 공유되는 사전 공유키를 이용해 수행되는 것을 특징으로 하는, 그룹 키 분배 방법.

청구항 7

청구항 6에 있어서,

암호화된 상기 새로운 그룹 키를 수신한 상기 특정 단말이, 상기 사전 공유키를 이용해 상기 새로운 그룹 키를 복호하는 단계를 더 포함하는, 그룹 키 분배 방법.

청구항 8

적어도 하나의 단말에 대해 수신제한 서비스를 제공하는 수신제한 서버에 있어서,

상기 적어도 하나의 단말 각각과 서로 다른 사전 공유키를 공유하고,

상기 수신제한 서버와 연관 가능한 모든 단말에 대한 제조 비밀값을 저장하고,

특정 단말로부터 그룹 가입 또는 그룹 탈퇴 요청이 있는 경우, 기존에 사용하던 그룹키 및 상기 특정 단말의 제조 비밀값에 대해 XOR 연산을 수행하고, 상기 연산 결과에 대해 해쉬함수를 적용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는 수신제한 서버.

청구항 9

삭제

청구항 10

청구항 8에 있어서,

상기 수신제한 서버와 연관 가능한 모든 단말은,

기존에 존재하는 적어도 하나의 단말 및 향후 제조가 될 것으로 예상되는 모든 단말을 포함하는, 수신제한 서버.

청구항 11

청구항 8에 있어서,

상기 특정 단말이 그룹에 새로이 가입하고자 요청하는 경우,

상기 새로운 그룹 키를 암호화하고, 상기 암호화된 새로운 그룹키를 상기 특정 단말로 전송하는 것을 특징으로 하는, 수신제한 서버.

청구항 12

청구항 11에 있어서,

상기 새로운 그룹 키에 대한 암호화는,

상기 특정 단말과 상기 수신제한 서버 사이에만 공유되는 사전 공유키를 이용해 수행되는 것을 특징으로 하는, 수신제한 서버.

청구항 13

수신제한 서버와 사전 공유키를 공유하여 저장하고, 자신을 제외한 다른 모든 단말에 대한 제조 비밀값을 저장하고 있다가,

상기 수신제한 서버로부터 특정 단말의 그룹 가입 메시지 또는 그룹 탈퇴 메시지를 수신하는 경우, 기존에 사용하던 그룹키 및 상기 특정 단말의 제조 비밀값에 대해 XOR 연산을 수행하고, 상기 연산 결과에 대해 해쉬함수를 적용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는, 수신제한 단말.

청구항 14

삭제

청구항 15

청구항 13에 있어서,

상기 자신을 제외한 다른 모든 단말은,

기존에 존재하는 적어도 하나의 단말 및 향후 제조가 될 것으로 예상되는 모든 단말을 포함하는, 수신제한 단말.

청구항 16

적어도 하나의 단말 각각과 서로 다른 사전 공유키를 공유하고, 연관 가능한 모든 단말에 대한 제조 비밀값을 저장하고, 특정 단말로부터 그룹 가입 또는 그룹 탈퇴 요청이 있는 경우, 특정 단말로부터 그룹 가입 또는 그룹 탈퇴 요청이 있는 경우, 기존에 사용하던 그룹키 및 상기 특정 단말의 제조 비밀값에 대해 XOR 연산을 수행하고, 상기 연산 결과에 대해 해쉬함수를 적용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는, 수신제한 서버; 와

수신제한 서버와 사전 공유키를 공유하여 저장하고, 자신을 제외한 다른 모든 단말에 대한 제조 비밀값을 저장하고 있다가, 상기 수신제한 서버로부터 특정 단말의 그룹 가입 메시지 또는 그룹 탈퇴 메시지를 수신하는 경우, 기존에 사용하던 그룹키 및 상기 특정 단말의 제조 비밀값에 대해 XOR 연산을 수행하고, 상기 연산 결과에 대해 해쉬함수를 적용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는, 수신제한 단말을 포함하는 수신제한 시스템.

청구항 17

삭제

청구항 18

청구항 16에 있어서,

상기 적어도 하나의 수신제한 단말 중 특정 단말이 그룹에 새로이 가입하고자 하는 경우, 상기 수신제한 서버는,

상기 특정 단말과 공유하는 사전 공유키를 이용하여 상기 새로운 그룹 키를 암호화하고, 상기 암호화된 새로운 그룹키를 상기 특정 단말로 전송하는, 수신제한 시스템.

청구항 19

청구항 18에 있어서,

상기 암호화된 새로운 그룹키를 수신한 상기 특정 단말은,

상기 사전 공유키를 이용해 상기 암호화된 새로운 그룹키를 복호하여 새로운 그룹키를 획득하는, 수신제한 시스템.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 그룹 키 분배 방법 및 이를 이용한 수신 제한 시스템에 관한 것으로, 더욱 상세하게는 다자간 통화, 모바일TV, IP-TV 등의 서비스를 제공함에 있어 저장 공간을 소비하는 대신 연산 효율 및 통신 효율을 극대화 시킴으로써 낮은 비용으로 매우 빠른 그룹 키 분배를 실현하는 그룹 키 분배 방법 및 이를 이용한 수신 제한 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 각종 방송 매체가 기존의 아날로그 형태에서 디지털로 바뀌고 있는 것이 세계적인 추세이다. 기존의 아날로그 방송과 비교하였을 때 디지털 방송은 TV 방송에 필요한 비디오, 오디오 이외에도 각종 컴퓨터 파일, 문서 등을 디지털 데이터로 보낼 수 있다는 장점이 있다.

[0003] 이러한 디지털 방송에서 가장 문제가 되는 것이 송신 측과 수신 측 사이의 보안성인데, 상호 보안성이 확립되지 않을 경우 방송의 상업적 구조가 무너지게 되어 현실성을 잃게 된다. 보안성을 위해 개발된 것이 디지털 방송의

핵심 기술인 제한 수신 시스템(Conditional Access System)이다.

[0004] 제한 수신은 최종 사용자에게 어느 특정한 방송 프로그램에 대한 수신 가능 여부를 각각의 디지털 수신기가 결정하도록 하는 일련의 과정을 의미한다. 제한 수신 기술은, 상용 서비스를 인증받지 못한 수신으로부터 보호하기 위한 스크램블링 키(Scrambling Key, SK) 키, 특정 수신기만 해독할 수 있는 키인 인증 키(Authorization Key, AK), 마스터 키(Master Private Key, MPK)로 구성된 3 단계 키 체계를 사용한다.

[0005] 스크램블링 키는 CAS 서버가 미디어 컨텐츠를 스크램블링할 때 사용되는데, 스크램블링이란 데이터를 뒤섞는 것을 말한다. 이때, 일정한 규칙으로 뒤섞기 위해 CW를 사용하는데, CW는 의사 난수 생성기(Pseudo Random Number Generator, PRNG)로 연산한 결과값이다. CW는 일반적으로 5 내지 20초 정도의 간격으로 CA 서버에 의해 갱신되는데, 이는 공격자에 의한 기지 평문 공격(known-plaintext attack)의 위험을 줄이기 위한 것이다. 또한, AK는 CW를 암호화하여 그룹(각 방송채널)에게 전송할 때 사용하는 그룹 키이고, MPK는 AK를 암호화하여 각 단말에게 전송할 때 사용되는 키로서, 각 단말마다 다른 MPK가 존재한다. 일반적인 mobile-TV, IP-TV 보안 시스템에서는 AK로 암호화된 CW를 전송할 때, CW에 대한 서버의 전자서명을 함께 전송함으로써, CW의 변조를 막는 것은 물론이 CW가 정상적인 서버로부터 생성되었음을 보장한다.

[0006] 한편, IP 기반의 Pay-TV 시스템에서의 그룹키 분배 시 요구되는 보안성을 만족하기 위해서는 다음과 같은 요구사항이 만족되어야 한다.

[0007] 첫째는 후방향 안전성으로, 그룹을 탈퇴한 단말이 과거의 그룹키를 이용하여 현재의 암호문 및 미래의 암호문을 복호화할 수 없는 것을 의미한다. IP기반의 Pay-TV 시스템에서의 후방향 안전성은, 임의의 가입자가 특정 채널에서 탈퇴한 이후에 과거의 그룹키 AK를 이용하여 해당 채널의 암호화된 컨텐츠를 복호화할 수 없는 것을 의미한다.

[0008] 둘째는 전방향 안전성으로, 그룹에 가입한 단말이 현재의 그룹 키 및 미래의 그룹 키를 이용하여 과거의 암호문을 복호화할 수 없는 것을 의미한다. IP 기반의 Pay-TV 시스템에서의 전방향 안전성은, 임의의 가입자가 특정 채널에 가입한 이후에 현재의 그룹 키 및 미래의 그룹 키 AK를 이용하여 과거에 전송되었던 컨텐츠를 복호화할 수 없는 것을 의미한다.

[0009] 셋째, 내부/외부 공격 방지(prevention of insider/outsider attacks)는 IP 기반의 Pay-TV 시스템은 외부 공격자로부터 안전하게 보호되어야 하며, 나아가서 내부 공격자에 의한 공격도 차단할 수 있어야 한다. 즉, 특정 채널에 가입하지 않은 사용자가 불법으로 미디어 컨텐츠를 시청하기 위해 그룹 키 획득을 시도할 수 있다. 또한, 임의의 가입자가 해당 채널에서 탈퇴한 이후에도 지속적으로 미디어 컨텐츠를 시청하기 위해 다른 가입자의 가입 정보 수집을 시도할 수 있다. 이러한 공격자들의 다양한 시도가 발생하더라도, CAS는 모든 가입자들이 어떠한 피해도 받지 않도록 안전하게 시스템을 보호해야 한다.

[0010] 도 1은 일반적인 제한 수신 시스템의 키 구조 및 키 전달 과정을 나타낸 블록도이다.

[0011] 자격제어메시지(Entitlement Control Message, ECM)는 각 방송 채널마다 존재하는 값으로서, 여기에는 해당 채널에 대한 정보와 AK로 암호화된 CW가 포함되어 있다. CAS 서버(10)는 ECM을 서명한 후, 미디어 컨텐츠와 함께 멀티캐스트를 통해 가입자들에게 전송한다. 자격관리메시지(Entitlement Management Message, ECM)는 각 가입자마다 존재하는 값으로, 여기에는 각 가입자에 대한 정보와 MPK로 암호화된 AK가 포함되어 있다. CAS 서버(10)는 EMM을 서명한 후, 각 가입자에게 유니캐스트를 통해 전송한다.

[0012] 이러한 시스템을 기반으로 하여, 임의의 단말이 그룹에 가입했을 때, CAS 서버(10)가 그룹 키를 분배하는 일반적인 과정을 알아보자면 다음과 같다.

[0013] 현재 그룹에 n개의 단말이 가입한 상태에서 (n+1) 번째 단말인 C_{n+1}이 가입할 경우, 서버는 AK를 MPKi ($1 \leq i \leq n+1$)로 암호화하여 각 단말에 전송한다. 마찬가지로, Cj 가 탈퇴할 경우, 서버는 AK를 MPKi ($1 \leq i \leq n$, $i \neq j$)로 암호화하여 Cj 를 제외한 모든 단말에 전송하게 된다. 이러한 시스템은, IP-TV와 같이 그룹 멤버쉽의 변화가 빈번한 대규모 그룹 통신에 적용될 경우, 심각한 지연 시간을 유발할 수 있다. 실시간 방송 서비스에서 지연 시간은 매우 민감한 요소이고 서비스의 품질과 직결되기 때문에, 효율적인 그룹 키 분배에 관한 연구는 매우 중요하다. 특히, 모바일 환경에서의 방송 서비스는 단말의 한정된 배터리 수명 및 제한된 성능으로 인해 연산 오버헤드를 최소화시키는 것이 필수적이다.

[0014] 살펴본 바와 같은 문제점들을 해결하기 위해 연산 효율 및 통신 효율이 뛰어난 많은 그룹 키 분배 기법들이 제안되어 왔다. 그러나 이들이 제안한 그룹 키 분배 기법은 전방향 안전성을 제공하지 않기 때문에, 그룹 가입자는 추가적인 과금없이 과거의 정보를 모두 열람할 수 있다. 또한, 선행 기법들의 주장과 달리 후방향 안전성조차 만족하지 못하기 때문에, 그룹 가입자는 최소한의 과금만으로 불법적인 서비스 수신이 가능하다는 문제가 있음이 지적되고 있다.

발명의 내용

해결 하고자하는 과제

[0015] 따라서 본 발명은 상술한 문제점을 감안한 것으로, 제조되는 모든 단말에 대한 제조 비밀값을 이용하여 간단한 연산만으로 그룹 키를 갱신하는 그룹 키 분배 방법 및 이를 이용한 수신 제한 시스템을 제공하는 데 그 목적이 있다.

과제 해결수단

[0016] 상술한 본 발명의 목적을 달성하기 위한 본 발명의 일 측면에 따른 그룹 키 분배 방법은, 수신제한 서버 및 적어도 하나의 단말을 포함하는 수신제한 시스템에서 그룹 키를 분배하는 방법에 관한 것으로, 상기 적어도 하나의 단말 각각이, 자신을 제외한 모든 단말 전체에 대한 제조 비밀값을 저장하는 단계와 특정 단말의 그룹 가입 또는 그룹 탈퇴시, 상기 수신제한 서버는 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는 단계를 포함한다.

[0017] 상기 모든 단말 전체는, 기존에 존재하는 적어도 하나의 단말 및 향후 제조가 될 것으로 예상되는 모든 단말을 포함한다.

[0018] 상기 그룹 키 분배 방법은, 특정 단말의 그룹 가입 또는 그룹 탈퇴시, 상기 특정 단말을 제외한 상기 수신제한 시스템에 포함된 나머지 모든 단말이, 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는 단계를 더 포함한다.

[0019] 상기 수신제한 서버가 생성하는 새로운 그룹 키, 및 상기 특정 단말을 제외한 상기 수신제한 시스템에 포함된 나머지 모든 단말이 생성하는 새로운 그룹 키 중 적어도 하나는, 상기 특정 단말의 제조 비밀값과 기존의 그룹 키에 대해 XOR 연산을 수행하고, 상기 연산 결과에 대해 해쉬함수를 적용하여 생성되는 것을 특징으로 한다.

[0020] 상기 수신제한 서버의 그룹키 갱신 단계에서 상기 특정 단말이 그룹에 새로이 가입하고자 하는 경우, 상기 그룹 키 갱신 단계는, 상기 수신제한 서버가 상기 새로운 그룹 키를 암호화하는 단계와 상기 수신제한 서버가 상기 암호화된 새로운 그룹키를 상기 특정 단말로 전송하는 단계를 포함할 수 있다.

[0021] 상기 새로운 그룹 키에 대한 암호화는, 상기 특정 단말과 상기 수신제한 서버 사이에만 공유되는 사전 공유키를 이용해 수행된다.

[0022] 상기 그룹 키 분배 방법은, 암호화된 상기 새로운 그룹 키를 수신한 상기 특정 단말이 상기 사전 공유키를 이용해 상기 새로운 그룹 키를 복호하는 단계를 더 포함한다.

[0023] 본 발명의 다른 측면에 따른 수신제한 서버는, 적어도 하나의 단말에 대해 수신제한 서비스를 제공하며, 상기 적어도 하나의 단말 각각과 서로 다른 사전 공유키를 공유하고, 상기 수신제한 서버와 연관 가능한 모든 단말에 대한 제조 비밀값을 저장하고, 특정 단말로부터 그룹 가입 또는 그룹 탈퇴 요청이 있는 경우, 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신한다.

[0024] 본 발명의 또 다른 측면에 따른 수신제한 단말은, 수신제한 서버와 사전 공유키를 공유하여 저장하고, 자신을 제외한 다른 모든 단말에 대한 제조 비밀값을 저장하고 있다가, 상기 수신제한 서버로부터 특정 단말의 그룹 가입 메시지 또는 그룹 탈퇴 메시지를 수신하는 경우, 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신한다.

[0025] 본 발명의 또 다른 측면에 따른 수신제한 시스템은, 적어도 하나의 단말 각각과 서로 다른 사전 공유키를 공유하고, 연관 가능한 모든 단말에 대한 제조 비밀값을 저장하고, 특정 단말로부터 그룹 가입 또는 그룹 탈퇴 요청이 있는 경우, 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는, 수신제한 서버와 상기 수신제한 서버와 사전 공유키를 공유하여 저장하고, 자신을 제외한 다른 모든 단말에 대한 제조 비밀값을 저장하고 있다가, 상기 수신제한 서버로부터 특정 단말의 그룹 가입 메시지 또는 그룹 탈퇴 메시지를 수신하는 경우, 기존의 그룹 키 및 상기 특정 단말의 제조 비밀값을 이용해 새로운 그룹 키를 생성하여 그룹 키를 갱신하는 적어도 하나의 수신제한 단말을 포함한다.

효 과

[0026] 본 발명, 그룹 키 분배 방법 및 이를 이용한 수신 제한 시스템에 따르면, 저장 공간을 소비하는 대신 연산 효율 및 통신 효율을 극대화 시킴으로써 낮은 비용으로 매우 빠른 그룹 키 분배가 가능하고, 가입자의 그룹 가입 또는 탈퇴시에 가입자의 수에 관계없이 서버 및 각 단말이 동일한 횟수의 연산 및 동일한 개수의 메시지 송수신만으로 그룹키 갱신이 가능하다는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0027] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0028] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는 데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0029] 본 명세서에서 사용되는 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0030] 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 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0031] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 이하, 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0032] 도 2는 본 발명의 그룹 키 분배 방법의 일 실시예에 따르는 경우, 단말 출하 시의 단말과 서버의 동작을 설명하기 위한 도면이다.

[0033] 본 발명에서는 수신제한 서버(10)와 각 단말(20) 사이에 둘만이 공유하고 있는 사전 공유 키(pre-shared key)가 존재한다고 가정한다. 즉, 서버와 i번째 단말 C_i는 사전 공유키 PK_i를 공유한다(S101). 따라서, 각 단말이 서버와 공유하는 사전 공유키는 서로 다르게 설정되고, 서버와 각각의 단말 사이에서만 공유되어 다른 단말 또는 외부에 대해 비밀이 유지된다. 실제로 IP-TV를 비롯한 여러 그룹 서비스에서 이러한 사전 공유키를 활용한다.

[0034] 또한, 본 발명에 따른 각 단말 C_i는 일반 사용자에게 판매되기 이전에 (즉, 공장 출하 시) 자신을 제외한 다른 모든 단말에 대한 제조 비밀값, 즉, R_1, R_2, ... , R_{i-1}, R_{i+1}, R_{i+2}, ..., R_z (여기서, z는 전체 단말의 수, 전체

단말이라 함은 기존에 존재하는 적어도 하나의 단말 및 향후 제조될 것으로 예상되는 모든 단말을 포함)를 저장한다(S103). 예를 들어, 임의의 IP-TV 서비스 제공업체가 총 z 개의 단말을 보급할 계획으로 z 개의 단말을 생산하였다면, 각 단말에는 (z-1) 개의 제조 비밀값이 저장된다. 그리고 서버는 z 개의 제조 비밀값 R_1, R_2, ..., R_z을 모두 저장한다(S102).

[0035] 이 제조 비밀값들 각각은 그룹 키와 동일한 크기로 이루어지며, 일반적으로 128 비트의 크기로 가정할 수 있다. 만약 IP-TV 서비스 제공업체가 총 1억 (100,000,000) 대의 단말을 생산하였다면, 각 단말에는 약 1.5 GB(GigaByte)의 제조 비밀값이 저장된다. 최근 공급되는 하드디스크의 용량 및 비용을 고려해볼 때, 1.5GB는 매우 낮은 비용으로 장착이 가능하다. 각 단말은 공장 출하시 위와 같은 사전 비밀키 및 제조 비밀값을 저장하게 되고, 이후 사용자에게 판매된다.

[0036] 이후 수신제한 서버(10)는 α 비트의 크기를 갖는 임의의 랜덤값을 생성하여 이를 최초의 그룹 키 GK로 사용한다(S104). 제조 비밀값 R_i ($1 \leq i \leq z$) 또한, 각각 α 비트로 이루어진다.

[0037] 도 3은 본 발명의 그룹 키 분배 방법에 따른 새로운 단말의 그룹 가입 시, 단말 및 서버의 동작 흐름의 일 실시예를 나타낸다.

[0038] 만약 새로운 단말 C_{n+1} (20-2) (여기서, n은 현재 그룹에 존재하는 가입자의 수)이 그룹에 가입하고자 가입 요청 메시지(JOIN request)를 수신제한 서버(10)로 전송하는 경우(S301), 이를 수신한 서버(10)는 새로운 단말이 가입했다는 사실을 알리는 메시지(JOIN message)에, 가입한 단말 C_{n+1}의 ID인 ID_{n+1}을 실어 기존의 모든 단말(20-1)로 브로드캐스트한다(S302). 한편, 서버(100)는 신규가입 단말의 제조 비밀값 R_{n+1}과 기존의 그룹키 GK에 대해 XOR 연산을 수행한 결과에 해쉬함수를 적용하여 새로운 그룹키 GK'를 생성함으로써 그룹키를 갱신한다(S303). 좀더 구체적으로는, 아래 수학식 1을 이용해 그룹 키 GK를 갱신한다.

[0039] [수학식 1]

[0040] $$GK' = H(GK \otimes R_{n+1})$$

[0041] 여기서, H( )는 해쉬함수를, $\otimes$는 XOR 연산을 의미한다. 또한, R_{n+1}은 신규가입 단말의 제조 비밀값, GK는 갱신 전의 그룹 키이다.

[0042] 서버(10)뿐 아니라 새로운 단말이 가입했음을 통지받은 기존의 모든 다른 단말들(20-1)도 상술한 서버(10)가 사용한 방법과 동일한 방법을 통해 그룹 키 GK를 갱신한다. 즉, 신규가입 단말의 제조 비밀값 R_{n+1}과 기존의 그룹 키 GK에 대해 XOR 연산을 수행한 결과에 해쉬함수를 적용하여 새로운 그룹키 GK'를 생성한다(S304). 단말 C_{n+1}을 제외한 기존의 모든 가입 단말은 과거의 그룹 키 GK와 제조 비밀값 R_{n+1}을 이미 알고 있기 때문에, 수학식 식 1과 같은 방법으로 새로운 그룹 키 GK′ 를 획득할 수 있다.

[0043] 또한, 서버(10)는 신규로 가입한 단말 C_{n+1}과 사전에 공유하고 있는 사전 공유키 PK_{n+1}를 이용하여 갱신된 그룹키 GK′ 를 암호화하여 $E_{PKi}(GK')$를 생성하고 (S305), 이를 단말 C_{n+1} (20-2)로 전송한다(S306). 서버(10)로부터 $E_{PKi}(GK')$를 수신한 단말(20-2)은 PKi를 이용해 $E_{PKi}(GK')$를 복호하고 GK'를 획득한다(S307).

[0044] 단말 C_{n+1}은 해쉬함수의 단방향성(one-wayness) 때문에 GK′ 로부터 $GK \otimes R_{n+1}$를 계산할 수 없다. 또한, 이를 계산해낸다고 하더라도, 단말 C_{n+1}은 제조 비밀값 R_{n+1}를 모르기 때문에 과거의 그룹 키인 GK를 획득할 수 없다. 따라서 본 발명은 전방향 안전성(forward secrecy)을 보장한다. 전방향 안전성이란, 임의의 단말이 현재 혹은 미래의 그룹 키를 이용하여 과거의 그룹 키를 획득하거나 과거의 암호문을 복호화 할 수 없는 것을 의미함을 이미 살펴본 바 있다. 전방향 안전성이 보장되지 않으면, 임의의 단말은 과거의 정보를 과금없이 모두 수신할 수 있게 되므로, 이는 서비스 제공자의 입장에서 매우 중요한 보안요소이다.

[0045] 도 4는 본 발명의 그룹키 분배 방법에 따르는 임의의 단말이 그룹을 탈퇴할 경우 나머지 단말들과 서버의 동작 흐름을 나타낸다.

[0046] 그룹 가입자 중 단말 C_i(20-3)가 그룹으로부터 탈퇴하고자 하는 경우, 단말 C_i(20-3)는 탈퇴요청 메시지를 수신한 서버(10)로 전송한다(S401). 서버(10)는 기존 단말들 중 C_i가 탈퇴했다는 사실을 알리는 메시지(LEAVE message)에 탈퇴하는 단말 C_i의 ID인 ID_i을 실어 다른 모든 단말(20-4)에게 브로드캐스트한다(S402). 이를 수신한 나머지 각 단말과 서버는 기존의 그룹 키 GK를 아래 수학식 2와 같이 갱신한다(S403). 즉, 탈퇴 단말의 제조 비밀값 R_i 와 기존의 그룹키 GK에 대해 XOR 연산을 수행한 결과에 해쉬함수를 적용하여 새로운 그룹키 GK″ 를 생성한다.

[0047] [수학식 2]

[0048] $$GK'' = H(GK \otimes R_i)$$

[0049] 여기서, H( )는 해쉬함수를, $\otimes$는 XOR 연산을 의미한다. 또한, R_i 는 탈퇴하고자 하는 단말의 제조 비밀값, GK는 갱신 전의 그룹 키, GK″ 는 갱신된 그룹 키이다.

[0050] 단말 C_i를 제외한 모든 가입되어 있던 단말은 과거의 그룹 키 GK와 제조 비밀값 R_i를 알기 때문에, 수학식 2를 이용해 새로운 그룹 키 GK″ 를 획득할 수 있다.

[0051] 그러나, 단말 C_i (20-3)는 제조 비밀값 R_i를 모르기 때문에, 과거의 그룹 키인 GK를 알더라도 새로운 그룹 키인 GK″ 를 획득할 수 없다. 따라서 본 발명은 후방향 안전성을 보장한다.

[0052] 후방향 안전성이란, 임의의 단말이 과거 혹은 현재의 그룹 키를 이용하여 미래의 그룹 키를 획득하거나 미래의 암호문을 복호화 할 수 없는 것을 의미한다. 후방향 안전성이 보장되지 않으면, 임의의 단말은 그룹으로부터 탈퇴한 이후에도 과금없이 서비스를 수신할 수 있게 되므로, 이는 서비스 제공자의 입장에서 매우 중요한 보안요소이다.

[0053] 살펴본 바와 같이, 본 발명은 HASH 및 XOR만을 사용하여 매우 빠른 연산이 가능하며, 단말의 가입이나 탈퇴에 따른 그룹 키 갱신 시, 서버와 단말이 송수신하는 메시지가 하나뿐이다. 특히, 단말과 서버 모두 그룹 내 가입자의 수와 관계 없이 XOR 연산 1회와 HASH 연산 1회만으로 그룹 키의 갱신이 가능하다.

[0054] 이렇듯 본 발명은 저장 공간을 소비하는 대신 그룹 키 갱신에 소요되는 연산 횟수 및 메시지 개수를 크게 줄임으로써, 궁극적으로 매우 빠르고 효율적인 그룹 키의 갱신을 가능하게 한다. 최근 저장 장치의 경우, 용량은 점점 증가하는 반면 가격은 점점 하락하는 추세이다. 따라서 본 발명에서 소모하는 저장 공간은 매우 현실적인 비용으로 확보 가능하다. 본 발명은 Mobile-TV, IP-TV, 다자간 회의 등 각종 응용에서 필수적으로 요구되는 보안요구사항인 후방향 안전성 및 전방향 안전성을 모두 만족한다. 즉, 본 발명은 안전하면서도 매우 빠르고 효율적인 그룹 키 분배를 가능하게 한다.

[0055] 이상 실시예를 참조하여 설명하였지만, 해당 기술분야의 숙련된 당업자는 하기의 특허청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면의 간단한 설명

[0056] 도 1은 일반적인 제한 수신 시스템의 키 구조 및 키 전달 과정을 나타낸 블록도.

[0057] 도 2는 본 발명의 그룹 키 분배 방법의 일 실시예에 따르는 경우, 단말 출하 시의 단말과 서버의 동작을 설명하기 위한 도면.

[0058] 도 3은 본 발명의 그룹 키 분배 방법에 따른 새로운 단말의 그룹 가입 시, 단말 및 서버의 동작 흐름의 일 실시예를 나타낸 도면.

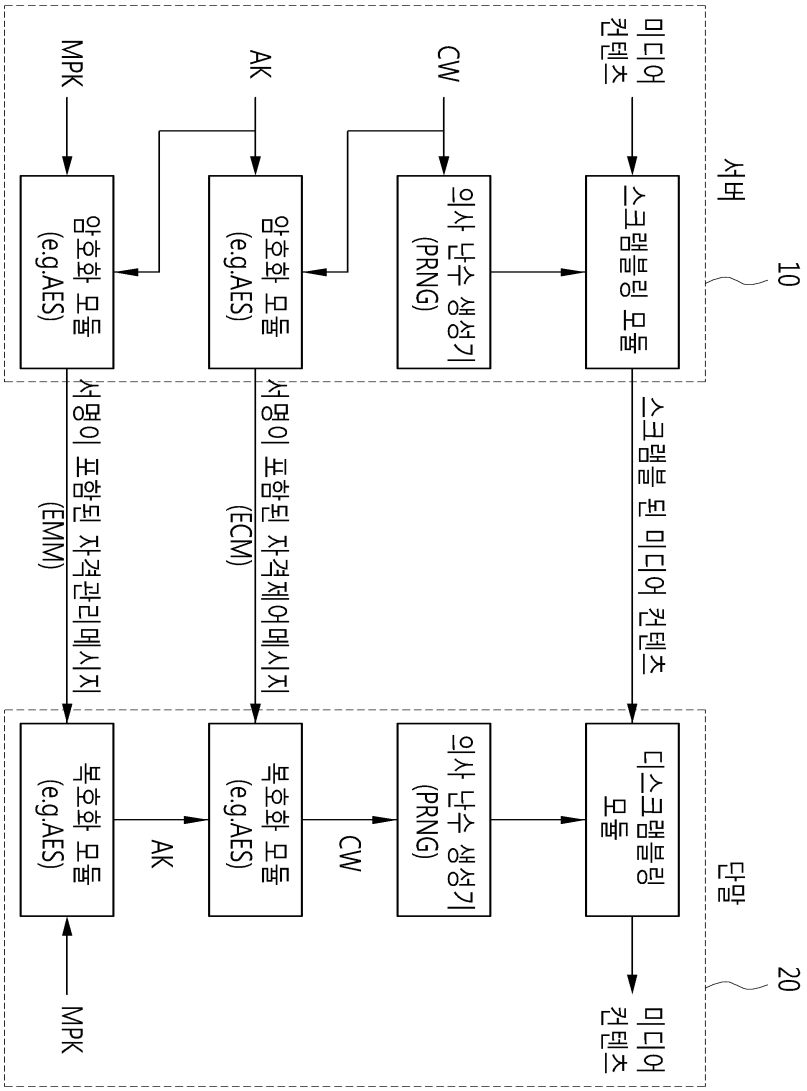
[0059] 도 4는 본 발명의 그룹키 분배 방법에 따르는 임의의 단말이 그룹을 탈퇴할 경우 나머지 단말들과 서버의 동작 흐름을 나타낸 도면.

[0060] * 도면의 주요부분에 대한 부호의 설명 *

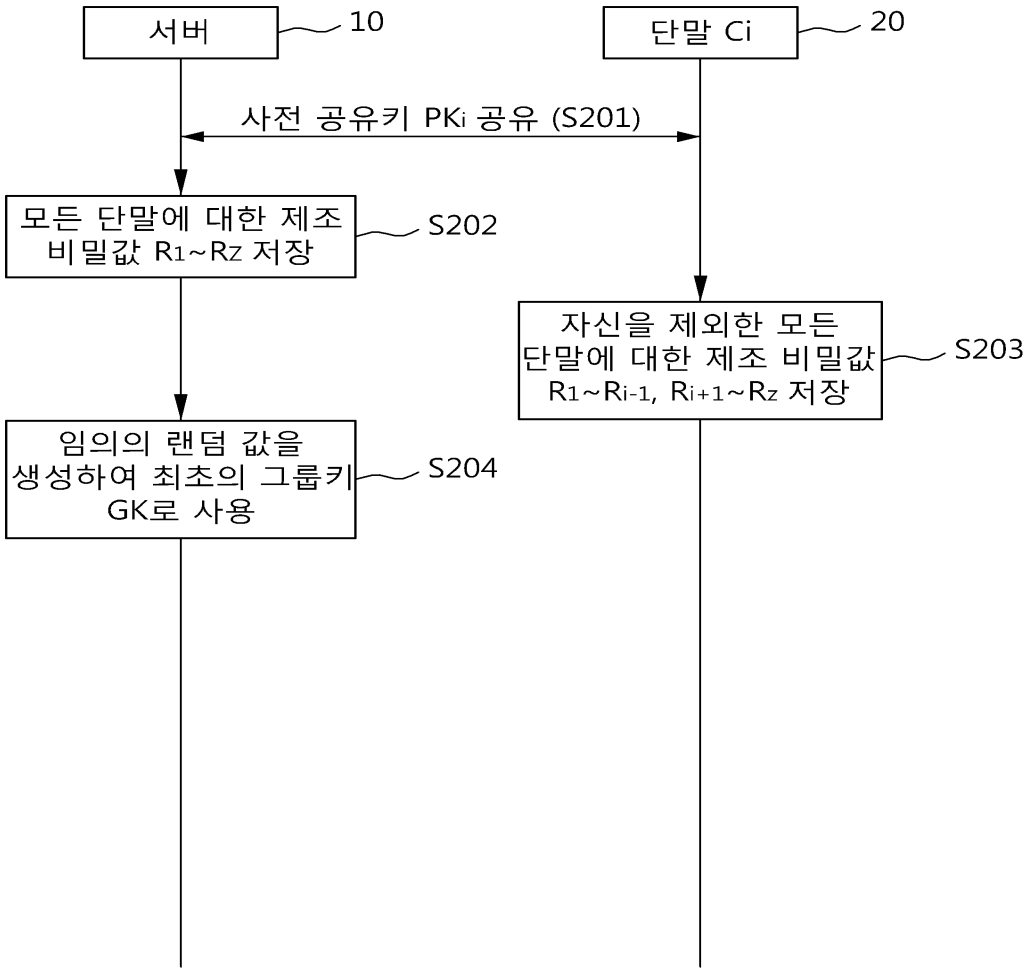
[0061] 10 : 수신제한 서버 20 : 단말

도면

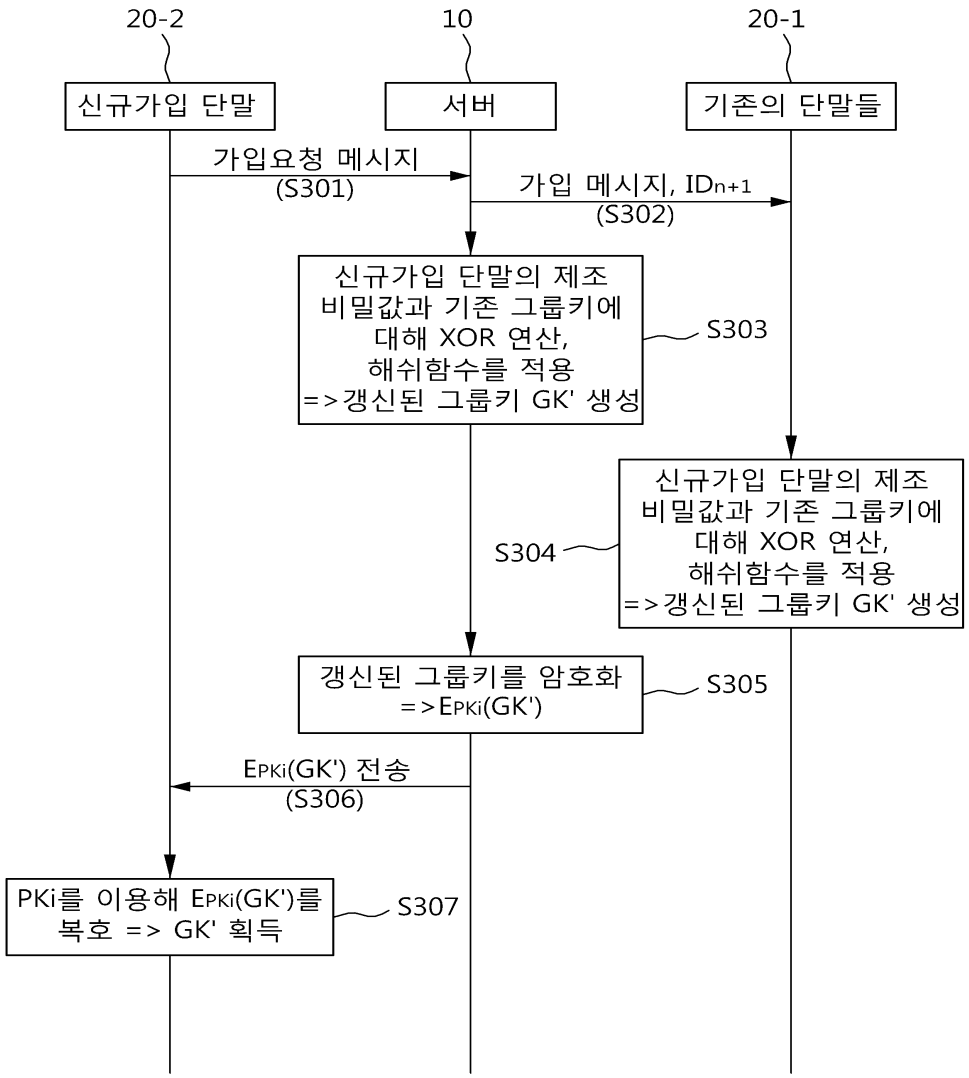
도면1



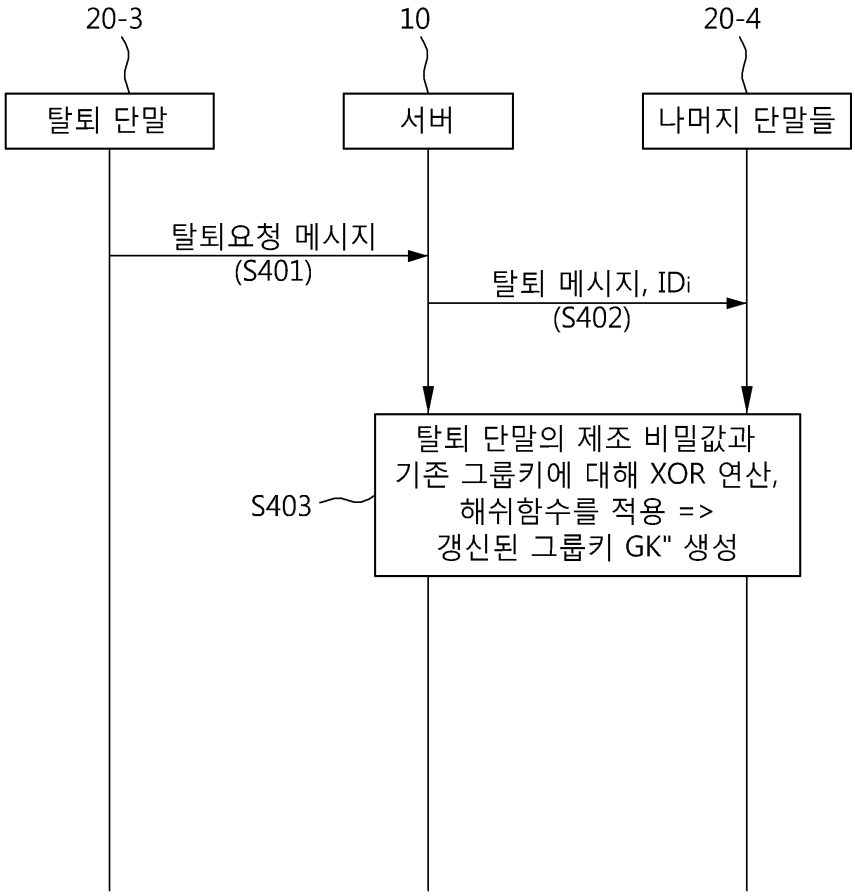
도면2


서버
10
단말 Ci
20
사전 공유키 PKi 공유 (S201)
모든 단말에 대한 제조 비밀값 R1~Rz 저장
S202
자신을 제외한 모든 단말에 대한 제조 비밀값 R1~Ri-1, Ri+1~Rz 저장
S203
임의의 랜덤 값을 생성하여 최초의 그룹키 GK로 사용
S204

도면3


20-2
10
20-1
신규가입 단말
서버
기존의 단말들
가입요청 메시지
(S301)
가입 메시지, IDn+1
(S302)
신규가입 단말의 제조 비밀값과 기존 그룹키에 대해 XOR 연산, 해쉬함수를 적용 =>갱신된 그룹키 GK' 생성
S303
S304
신규가입 단말의 제조 비밀값과 기존 그룹키에 대해 XOR 연산, 해쉬함수를 적용 =>갱신된 그룹키 GK' 생성
갱신된 그룹키를 암호화 =>EPKi(GK')
S305
EPKi(GK') 전송
(S306)
PKi를 이용해 EPKi(GK')를 복호 => GK' 획득
S307

도면4


20-3
10
20-4
탈퇴 단말
서버
나머지 단말들
탈퇴요청 메시지
(S401)
탈퇴 메시지, IDi
(S402)
S403
탈퇴 단말의 제조 비밀값과
기존 그룹키에 대해 XOR 연산,
해쉬함수를 적용 =>
갱신된 그룹키 GK" 생성