(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/32 (2006.01)
H04L 12/16 (2006.01)
H04L 9/30 (2006.01)
H04L 9/08 (2006.01)

(45) 공고일자 2007년02월02일
(11) 등록번호 10-0677152
(24) 등록일자 2007년01월26일

(21) 출원번호 10-2004-0099434
(22) 출원일자 2004년11월30일
심사청구일자 2004년11월30일

(65) 공개번호 10-2006-0055263
(43) 공개일자 2006년05월23일

(30) 우선권주장 60/628,386 2004년11월17일 미국(US)

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 김명선
경기 의왕시 삼동 대우아파트 105동 104호

한성휴
서울특별시 송파구 문정2동 훼미리1단지아파트 102동 1006호

유용국
서울 성동구 금호동3가 두산아파트 115동 206호

윤영선
경기 수원시 권선구 권선동 5단지 상록아파트 511동 704호

김봉선
경기 성남시 분당구 금곡동 청솔마을 주공9단지아파트 903동 411호

이재흥
경기 수원시 영통구 원천동 260-14 현대빌 204호

(74) 대리인 리앤목특허법인
이해영

(56) 선행기술조사문헌
JP2004336619 A
KR1020040089274 A
KR1020040003629 A
KR1020050052978 A
* 심사관에 의하여 인용된 문헌

심사관 : 이준석

전체 청구항 수 : 총 18 항

(54) 사용자 바인딩을 이용한 홈 네트워크에서의 콘텐츠 전송방법

(57) 요약

홈 네트워크에 있어서 콘텐츠 전송 방법이 개시된다. 본 발명은, 홈 네트워크에서 홈 서버로부터 사용자 기기로 콘텐츠를 전송하는 방법에 있어서, a)상기 홈 서버가 속한 사용자의 사용자 공개키 및 사용자 개인키를 할당받는 단계; b)임의의 세션 공개키 및 세션 개인키를 생성하고, 상기 사용자 기기의 공개키인 기기 공개키를 이용하여 상기 세션 개인키를 암호화함으로써 암호화한 세션 개인키를 생성한 후 사용자 기기로 전송하는 단계; c)상기 사용자 기기에게 소정의 콘텐츠 키를 이용하여 암호화한 콘텐츠 및 상기 세션 개인키를 이용하여 암호화한 콘텐츠 키를 전송하는 단계를 포함한다. 본 발명에 의하면, 홈 네트워크내에서 콘텐츠를 사용자 기기마다 바인딩하는 것이 아니라, 사용자마다 바인딩함으로써, 콘텐츠를 사용자마다 바인딩함으로써 콘텐츠를 안전하면서도 편리하게 공유할 수 있는 콘텐츠 전송 방법이 제공된다.

대표도

도 3

특허청구의 범위

청구항 1.

홈 네트워크에서 홈 서버로부터 사용자 기기로 콘텐츠를 전송하는 방법에 있어서,

상기 사용자 기기에게 소정의 콘텐츠 키를 이용하여 암호화한 상기 콘텐츠 및 소정의 세션 공개키 및 세션 개인키 쌍를 이용하여 암호화한 상기 콘텐츠 키를 전송하는 단계를 포함하고,

상기 콘텐츠는, 상기 홈 서버가 속한 사용자의 사용자 공개키 및 사용자 개인키를 이용하여 상기 사용자에게 바인딩되는 것을 특징으로 하는 방법.

청구항 2.

제 1 항에 있어서,

a)상기 홈 서버가 속한 사용자의 사용자 공개키 및 사용자 개인키를 할당받는 단계;

b)임의의 세션 공개키 및 세션 개인키를 생성하고, 상기 사용자 기기의 공개키인 기기 공개키를 이용하여 상기 세션 개인키를 암호화함으로써 암호화한 세션 개인키를 생성한 후 사용자 기기로 전송하는 단계; 및

c)상기 사용자 기기에게 소정의 콘텐츠 키를 이용하여 암호화한 콘텐츠 및 상기 세션 개인키를 이용하여 암호화한 콘텐츠 키를 전송하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 3.

제 2 항에 있어서, 상기 세션 공개키 및 상기 세션 개인키는 상기 사용자 기기의 가입 또는 변경시 마다 갱신되는 것을 특징으로 하는 방법.

청구항 4.

제 2 항에 있어서, 상기 사용자 기기는 기기 개인키를 이용하여 상기 암호화한 세션 개인키를 복호화함으로써 세션 개인키를 획득하고, 상기 세션 개인키를 이용하여 상기 암호화한 콘텐츠 키를 복호화함으로써 상기 콘텐츠 키를 획득하는 것을 특징으로 하는 방법.

청구항 5.

홈 네트워크에 있어서, 제 2 사용자 기기로부터 제 1 사용자 기기로 콘텐츠를 전송하는 방법에 있어서,

상기 제 1 사용자 기기 및 제 2 사용자 기기의 사용자 공개키 및 사용자 개인키 쌍에 기초하여 상기 사용자 기기의 사용자가 동일한지를 검사하고, 상기 사용자가 동일하다고 판단된 경우에만, 소정의 콘텐츠 키를 이용하여 암호화한 상기 콘텐츠 및 소정의 세션 공개키를 이용하여 암호화한 상기 콘텐츠 키를 상기 제 1 사용자 기기로 전송하는 단계를 포함하고,

상기 콘텐츠는, 상기 사용자 기기가 속한 사용자의 사용자 공개키 및 사용자 개인키를 이용하여 상기 사용자에게 바인딩되는 것을 특징으로 하는 방법.

청구항 6.

제 5 항에 있어서,

a)제 2 사용자 기기로부터 제 2 사용자 기기가 속한 제 2 사용자의 사용자 공개키를 수신하는 단계;

b)소정의 기기 값 및 상기 제 2 사용자 공개키을 이용하여 기기 인증값 CA를 생성한 후, 제 1 사용자 기기의 홈 서버로 전송하는 단계;

c)상기 기기 인증값 및 상기 제 1 사용자 기기가 속한 제 1 사용자의 사용자 개인키를 이용하여 상기 홈 서버에 의해 생성된 서버 인증값 및 상기 기기값에 기초하여 상기 제 1 사용자와 상기 제 2 사용자가 동일한지 검사하는 단계; 및

d)상기 사용자가 동일하다고 판단된 경우, 상기 제 2 사용자 기기로부터 소정의 콘텐츠 키를 이용하여 암호화한 콘텐츠 및 소정의 세션 공개키를 이용하여 암호화한 콘텐츠 키를 수신하는 단계를 포함하고,

상기 세션 공개키에 대응하는 세션 개인키는 상기 사용자 기기의 공개키 및 개인키 쌍을 이용하여 상기 사용자 기기의 변경시마다 상기 사용자 기기로 전송되는 것을 특징으로 하는 방법.

청구항 7.

제 6 항에 있어서, 상기 기기 인증값은 이하 수학식에 의해 생성되고,

$$CA = m^{Kpub\text{-}u1'}$$

여기서 CA 는 기기 인증값, m 는 기기값, Kpub_u1' 는 상기 제 2 기기로부터 전송된 사용자 공개키인 것을 특징으로 하는 방법.

청구항 8.

제 7 항에 있어서, 상기 서버 인증값은 이하 수학식에 의해 생성되고,

$$CA' = CA^{Kpri\text{-}u1}$$

여기서 CA' 는 서버 인증값, Kpri_u1 는 제 1 사용자의 사용자 개인키인 것을 특징으로 하는 방법.

청구항 9.

제 8 항에 있어서, 상기 c)단계는, 상기 서버 인증값 CA' 와 기기값 m 이 동일한지 검사함으로써 수행되는 것을 특징으로 하는 방법.

청구항 10.

제 6 항에 있어서, 상기 기기 인증값은 이하 수학식에 의해 생성되고,

$$CA = m * r^{Kpub\text{-}u1'}$$

여기서 CA 는 기기 인증값, m 는 기기값, Kpub_u1' 는 상기 제 2 기기로부터 전송된 사용자 공개키, r 는 임의의 난수인 것을 특징으로 하는 방법.

청구항 11.

제 10 항에 있어서, 상기 서버 인증값은 이하 수학식에 의해 생성되고,

$$CA' = CA^{Kpri\text{-}u1}$$

여기서 CA' 는 서버 인증값, Kpri_u1 는 제 1 사용자의 사용자 개인키인 것을 특징으로 하는 방법.

청구항 12.

제 11 항에 있어서, 상기 c)단계는, 상기 서버 인증값 CA'을 상기 임의의 난수 r 로 나눈값이 기기값 m 이 동일한지 검사함으로써 수행되는 것을 특징으로 하는 방법.

청구항 13.

제 6 항에 있어서, e)상기 사용자가 동일하지 않다고 판단된 경우, 상기 제 2 사용자 기기로부터 상기 콘텐츠를 전송받을 수 없다고 판단하고 절차를 종료하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 14.

제 6 항에 있어서, 상기 c) 단계와 d)단계 사이에, f)상기 사용자가 동일하다고 판단된 경우, 전자 서명을 이용하여 상기 제 1 사용자 기기의 세션 개인키와 상기 제 2 사용자 기기의 세션 개인키가 동일한 지 여부를 검사하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 15.

제 14 항에 있어서, 상기 f)단계는,

f1)제 1 사용자 기기가 상기 제 1 사용자 기기의 세션 개인 키를 이용하여 임의의 제 1 난수를 암호화함으로써 전자서명한 제 1 전자 서명값을 생성하는 단계;

f2)상기 제 1 사용자 기기가 상기 제 1 전자서명값 및 제 1 난수를 제 2 사용자 기기로 전송하는 단계;

f3)상기 제 2 사용자 기기가 상기 제 2 사용자 기기의 세션 공개 키를 이용하여 상기 제 1 서명값을 복호화함으로써 생성된 결과값 V(Kpub_s, S_A) 이 상기 제 1 난수와 동일한 지를 검사하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 16.

제 15 항에 있어서, 상기 f)단계는,

f4)제 2 사용자 기기가 상기 제 2 사용자 기기의 세션 개인 키를 이용하여 임의의 제 2 난수를 암호화함으로써 전자서명한 제 2 전자 서명값을 생성하는 단계;

f5)상기 제 2 사용자 기기가 상기 제 2 전자서명값 및 제 2 난수를 제 1 사용자 기기로 전송하는 단계;

f6)상기 제 1 사용자 기기가 상기 제 1 사용자 기기의 세션 공개 키를 이용하여 상기 제 2 서명값을 복호화함으로써 생성된 결과값이 상기 제 2 난수와 동일한 지를 검사하는 단계를 더 포함하는 것을 특징으로 하는 방법.

청구항 17.

제 16 항에 있어서, 상기 제 1 난수 및 상기 제 2 난수는 서로 연관된 수인 것을 특징으로 하는 방법.

청구항 18.

제 6 항에 기재된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 콘텐츠 전송 방법에 관한 것으로서, 보다 상세하게는 홈 네트워크에 있어서 사용자 기기들 사이에 보다 편리하면서도 안전하게 콘텐츠를 공유할 수 있게 하는 콘텐츠 전송 방법에 관한 것이다.

디지털 콘텐츠는 콘텐츠 제공자로부터 사용자에게 전송된다. 사용자는 콘텐츠에 대한 비용 지불 등을 통해 정당한 권한을 획득하여야만 디지털 콘텐츠를 사용할 수 있고, 또한 정당한 권한을 획득하지 않은 사용자는 디지털 콘텐츠를 사용할 수 없도록, 콘텐츠는 보호되어야 한다.

정당한 권한 없는 사용자로하여금 콘텐츠를 획득하는 것을 방지하기 위해, 콘텐츠는 콘텐츠 키로 암호화되고, 콘텐츠 키는 정당한 권한 있는 사용자에게만 배포된다.

한편, 최근 홈 네트워크 기술의 발달에 따라 하나의 사용자가 하나이상의 사용자 기기를 소유하게 되었고, 또한 이들간에 콘텐츠의 이동이 가능하게 되었다. 사용자는 한번의 비용결제로 자신이 소유한 모든 기기에 대하여 콘텐츠를 사용할 수 있기를 바란다. 하지만 콘텐츠가 기기사이에서 재생할 수 있는 형태로 자유스럽게 이동가능하면, 권한 없는 사용자가 콘텐츠

를 획득하고 사용할 수 있게 된다. 따라서 홈 네트워크 기술에서는 권한 있는 사용자의 홈 네트워크내의 사용자 기기간에는 콘텐츠의 이동을 허용하면서, 권한 없는 사용자는 콘텐츠를 획득할 수 없거나 획득한다 하더라도 콘텐츠를 사용할 수 없게 하는 기술이 필요하다.

특히 미연방 통신 위원회(FCC, Federal Communications Commission)은 2005년 7월부터 미국내의 디지털 방송으로 방송되는 고화질 HD 급 콘텐츠에 대하여 1비트의 브로드캐스트 플래그(broadcast flag, BF)를 첨가하고, 해당 콘텐츠의 브로드캐스트 플래그가 1 인 경우에는, 콘텐츠 보호가 이루어지도록 즉 권한 없는 사용자의 사용이 방지되도록 하는 기술을 디지털 방송 구현 기술 표준에서 요구하고 있기 때문에, 홈 서버와 사용자 기기사이의 디지털 방송 콘텐츠의 안전한 사용에 대한 요구는 더욱 절실하다.

도 1 는 홈 네트워트의 구조를 나타내는 도면이다.

콘텐츠 제공자 CP 는 전송 채널(10)을 통하여 홈 서버 HS 로 콘텐츠를 전송한다.

홈 서버 HS 는 사용자 기기 DA,DB,DC 와 연결되어 있으며, 정당한 사용자 기기의 가입 및 탈퇴를 관리하며, 정당한 권한이 있는 사용자 기기 즉 현재 가입된 기기에게만 콘텐츠를 전송한다.

여기서 도메인은 하나의 홈 서버에 연결된 사용자 기기의 집합을 의미한다. 사용자 기기의 홈 네트워크로의 가입 및 탈퇴로 인하여 도메인은 항상 변한다. 즉 도메인에 연결된 사용자 기기는 항상 변한다. 따라서 탈퇴한 사용자 기기는 더 이상 콘텐츠를 획득할 수 없도록 하는 과정이 필요하다.

콘텐츠는 콘텐츠 키를 이용하여 암호화되고, 콘텐츠 키는 공통 키를 이용하여 암호화된후, 사용자 기기 DA,DB,DC 로 각각 전송된다. 공통 키는 현재 홈 네트워크에 가입된 사용자 기기 만이 획득가능하다.

도 2 는 종래의 콘텐츠 전송 방법을 나타내는 도면이다.

단계 210에서, 홈 서버 HS 는 콘텐츠 C 를 전송 채널 10 로부터 수신하고, 콘텐츠 키 Kc를 이용하여 콘텐츠 C를 암호화함으로써 암호화된 콘텐츠 E(Kc,C)를 생성한다. 전송 채널 10 은 인터넷, 지상파 또는 위성 방송 등 여러 가지가 가능하다.

단계 220에서, 사용자 기기 DA 는 자신의 고유 정보 Xa'를 홈 서버 HS 로 전송한다.

단계 230에서, 홈 서버 HS 는 고유 정보 Xa'를 이용하여 공통 키 Ks를 생성한후 사용자 기기 DA 로 전송한다.

단계 240에서, 홈 서버 HS 는 암호화된 콘텐츠 E(Kc,C), 암호화된 콘텐츠 키 E(Ks,Kc) 및 라이센스 L_A를 사용자 기기 DA 로 전송한다. 라이센스 L_A 는 콘텐츠 C 에 대한 사용 규칙 UR 및 사용자 기기 DA 의 고유 정보 Xa' 가 포함되어 있다.

단계 250에서, 사용자 기기 DA 는 단계 240에서 수신한 라이센스 L_A 로부터 고유 정보 Xa'를 추출한 후 이를 자신이 가진 고유 정보 Xa 와 비교한다.

단계 260에서, 사용자 기기 DA 는 만약 Xa'=Xa 이고, 단계 230에서 수신한 공통키 Ks를 이용하여 단계 240에서 수신한 암호화된 콘텐츠 키 E(Ks,Kc)를 복호화함으로써 콘텐츠 키 Kc를 생성가능한지를 판단한다. 만약 이 두가지가 만족된다면, 단계 220에서의 사용자 기기 DA 와 단계 240에서의 사용자 기기 DA는 동일한 기기이므로, 사용자 기기 DA 는 콘텐츠 C를 재생가능하다.

그러나, 이러한 종래의 방법에 의하면, 다음과 같은 단점이 존재한다.

첫째, 콘텐츠 C 는 사용자 기기에 바인딩(binding)되기 때문에 하나의 사용자에 속한 둘 이상의 사용자 기기사이에 콘텐츠의 공유가 불편하다. 이러한 즉 하나의 사용자에 속한 사용자 기기라도 모든 기기는 자신의 고유 정보를 이용하여 라이센스를 새로 발급받아야한다. 예를 들면 기기 DB 가 기기 DA에서 수신하였던 콘텐츠를 재생할려고 하는경우에, 기기 DB 의 고유 정보 Xb' 의 전송, 콘텐츠 Kc' 의 생성, 공통키 Ks' 의 생성 및 기기 DB를 위한 라이센스 L_B 의 생성의 단계를 모두 다시 수행하여야 한다.

둘째, 사용자 기기의 고유 정보가 외부 기기에 노출된다. 사용자 기기의 고유 정보 Xa',Xb',... 등은 홈 네트워크의 보안의 관점에서 중요한 정보로서 역할하는 것이 대부분이므로, 이러한 정보의 외부 유출은 되도록 피하는 것이 바람직하다.

셋째, 사용자 기기사이의 콘텐츠의 공유가 반드시 홈 서버 HS를 통하여 수행되어야 한다.

일반적으로, 콘텐츠 C 에 대한 정당한 권한의 유무는 사용자의 비용결제 유무에 의존하는 것이 대부분이고, 하나의 사용자는 자신의 도메인에 속하는 둘 이상의 사용자 기기에 콘텐츠를 자유롭게 사용하길 원하기 때문에, 위의 불편함은 현재수요가 증가하고 있는 홈 네트워크의 발전에 있어서 더욱 심한 장애 요소가 된다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명은 전술한 과제를 해결하기 위해 안출된 것으로서, 홈 네트워크내에서 콘텐츠를 사용자 기기마다 바인딩하는 것이 아니라, 사용자마다 바인딩함으로써 콘텐츠를 안전하면서도 편리하게 공유할 수 있는 콘텐츠 전송 방법을 제공하고자 한다.

발명의 구성

전술한 과제를 해결하기 위한 본 발명은, 홈 네트워크에서 홈 서버로부터 사용자 기기로 콘텐츠를 전송하는 방법에 있어서, a)상기 홈 서버가 속한 사용자의 사용자 공개키 및 사용자 개인키를 할당받는 단계; b)임의의 세션 공개키 및 세션 개인키를 생성하고, 상기 사용자 기기의 공개키인 기기 공개키를 이용하여 상기 세션 개인키를 암호화함으로써 암호화한 세션 개인키를 생성한 후 사용자 기기로 전송하는 단계; c)상기 사용자 기기에게 소정의 콘텐츠 키를 이용하여 암호화한 콘텐츠 및 상기 세션 개인키를 이용하여 암호화한 콘텐츠 키를 전송하는 단계를 포함하는 것을 특징으로 한다.

여기서, 상기 세션 공개키 및 상기 세션 개인키는 상기 사용자 기기의 가입 또는 변경시 마다 갱신된다.

또한 본 발명은, 홈 네트워크에 있어서, 제 2 사용자 기기로부터 제 1 사용자 기기로 콘텐츠를 전송하는 방법에 있어서, a)제 2 사용자 기기로부터 제 2 사용자 기기가 속한 제 2 사용자의 사용자 공개키를 수신하는 단계; b)소정의 기기 값 및 상기 제 2 사용자 공개키을 이용하여 기기 인증값 CA를 생성한 후, 제 1 사용자 기기의 홈 서버로 전송하는 단계; c)상기 기기 인증값 및 상기 제 1 사용자 기기가 속한 제 1 사용자의 사용자 개인키를 이용하여 상기 홈 서버에 의해 생성된 서버 인증값 및 상기 기기값에 기초하여 상기 제 1 사용자와 상기 제 2 사용자가 동일한지 검사하는 단계; 및 d)상기 사용자가 동일하다고 판단된 경우, 상기 제 2 사용자 기기로부터 소정의 콘텐츠 키를 이용하여 암호화한 콘텐츠 및 소정의 세션 공개키를 이용하여 암호화한 콘텐츠 키를 수신하는 단계를 포함하고, 상기 세션 공개키에 대응하는 세션 개인키는 상기 사용자 기기의 공개키 및 개인키 쌍을 이용하여 상기 사용자 기기의 변경시마다 상기 사용자 기기로 전송된다.

제 1 실시예에서, 상기 기기 인증값은 이하 수학식에 의해 생성되고,

$$CA = m^{Kpub\text{-}u1'}$$

여기서 CA 는 기기 인증값, m 는 기기값, Kpub_u1' 는 상기 제 2 기기로부터 전송된 사용자 공개키이다.

또한 여기서, 상기 서버 인증값은 이하 수학식에 의해 생성되고,

$$CA' = CA^{Kpri\text{-}u1}$$

여기서 CA' 는 서버 인증값, Kpri_u1 는 제 1 사용자의 사용자 개인키이다.

또한 여기서, 상기 c)단계는, 상기 서버 인증값 CA' 와 기기값 m 이 동일한지 검사함으로써 수행된다.

제 2 실시예에서, 상기 기기 인증값은 이하 수학식에 의해 생성되고,

$$CA = m * r^{Kpub\text{-}u1'}$$

여기서 CA 는 기기 인증값, m 는 기기값, Kpub_u1' 는 상기 제 2 기기로부터 전송된 사용자 공개키, r 는 임의의 난수이다.

여기서, 서버 인증값은 이하 수학식에 의해 생성되고,

$$CA' = CA^{Kpri\text{-}u1}$$

여기서 CA' 는 서버 인증값, Kpri_u1 는 제 1 사용자의 사용자 개인키이다.

또한 여기서, 상기 c)단계는, 상기 서버 인증값 CA'을 상기 임의의 난수 r 로 나눈값이 기기값 m 이 동일한지 검사함으로써 수행된다.

또한 본 발명은, 상기 c) 단계와 d)단계 사이에, f)상기 사용자가 동일하다고 판단된 경우, 전자 서명을 이용하여 상기 제 1 사용자 기기의 세션 개인키와 상기 제 2 사용자 기기의 세션 개인키가 동일한 지 여부를 검사하는 단계를 더 포함한다.

여기서, 상기 f)단계는, f1)제 1 사용자 기기가 상기 제 1 사용자 기기의 세션 개인 키를 이용하여 임의의 제 1 난수를 암호화함으로써 전자서명한 제 1 전자 서명값을 생성하는 단계; f2)상기 제 1 사용자 기기가 상기 제 1 전자서명값 및 제 1 난수를 제 2 사용자 기기로 전송하는 단계; 및 f3)상기 제 2 사용자 기기가 상기 제 2 사용자 기기의 세션 공개 키를 이용하여 상기 제 1 서명값을 복호화함으로써 생성된 결과값 V(Kpub_s, S_A) 이 상기 제 1 난수와 동일한 지를 검사하는 단계를 포함한다.

또한 여기서, 상기 f)단계는, f4)제 2 사용자 기기가 상기 제 2 사용자 기기의 세션 개인 키를 이용하여 임의의 제 2 난수를 암호화함으로써 전자서명한 제 2 전자 서명값을 생성하는 단계; f5)상기 제 2 사용자 기기가 상기 제 2 전자서명값 및 제 2 난수를 제 1 사용자 기기로 전송하는 단계; f6)상기 제 1 사용자 기기가 상기 제 1 사용자 기기의 세션 공개 키를 이용하여 상기 제 2 서명값을 복호화함으로써 생성된 결과값이 상기 제 2 난수와 동일한 지를 검사하는 단계를 더 포함한다.

이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일 실시예를 상세히 설명한다.

도 3 은 본 발명에 따른 홈 서버로부터 사용자 기기로의 콘텐츠 전송 방법을 나타내는 도면이다.

현재 홈 서버 HS 에 사용자 기기 DA,DB,DC 가 연결되어 있고, 홈 서버 HS, 사용자 기기 DA,DB,DC 으로 구성된 홈 네트워크 HN 는 사용자 u 에 의해 소유된 상태라고 가정한다.

단계 310에서, 홈 서버 HS 는 홈 서버 HS 가 속한 사용자 U 의 사용자 공개키 Kpub_u 및 사용자 개인키 Kpri_u를 할당받는다. 공개키 구조의 특징에 따라, 사용자 공개키 Kpub_u 는 공개되고, 사용자 개인키 Kpri_u 는 홈 서버 HS 만이 소유한다.

단계 312에서, 홈 서버 HS 는 임의의 세션키 쌍 (Kpub_s, Kpri_s) 즉 세션 공개키 Kpub_s 및 세션 개인키 Kpri_s를 생성한다. 마찬가지로 공개키 구조의 특징에 따라, 공개키 Kpub_s 는 공개되고, 개인키 Kpri_s는 현재 홈 서버에 연결된 사용자 기기 즉 홈 서버 HS 의 도메인에 속한 사용자 기기만이 획득가능하다.

단계 320에서, 홈 서버 HS 는 기기 공개키 Kpub_DA, Kpub_DB, Kpub_DC를 이용하여 세션 개인키 Kpri_s를 암호화함으로써 암호화한 세션 개인키 E(Kpub_DA, Kpri_s), E(Kpub_DB, Kpri_s),E(Kpub_DC, Kpri_s)를 생성한 후 각각 사용자 기기 DA,DB,DC 에게 전송한다.

단계 330에서, 홈 서버 HS 는, 사용자 기기 DA,DB,DC 의 요청에 대응하여, 사용자 기기 DA,DB,DC에게 암호화한 콘텐츠 E(Kc,C) 및 암호화한 콘텐츠 키 E(Kpri_s, Kc)를 전송한다. 여기서 Kc 는 콘텐츠 키이다.

단계 340에서, 사용자 기기의 변경이 발생한다. 예를 들면, 사용자 기기 DA 가 홈 네트워크 HN 으로부터 탈퇴한다고 가정한다. 이러한 사용자 기기의 변경의 예는, 사용자 기기를 다른 사용자에게 파는 경우를 들수 있다.

단계 350에서, 홈 서버 HS 는 새로운 세션키 쌍 (Kpub_s', Kpri_s')을 생성한 후, 변경후 홈 네트워크 HN 에 속한 사용자 기기 즉 사용자 기기 DB, DC 에게 새로운 세션 개인키 Kpri_s'를 암호화한 상태로 전송한다.

즉 홈 서버 HS 는 기기 공개키 Kpub_DB, Kpub_DC를 이용하여 새로운 세션 개인키 Kpri_s' 를 암호화함으로써 암호화한 세션 개인키 E(Kpub_DB, Kpri_s'), E(Kpub_DC, Kpri_s')를 생성한 후 각각 사용자 기기 DB,DC 에게 전송한다.

단계 360에서, 홈 서버 HS 는, 사용자 기기 DB,DC 의 요청에 대응하여, 사용자 기기 DB,DC에게 암호화한 콘텐츠 E(Kc',C) 및 암호화한 콘텐츠 키 E(Kpri_s', Kc')를 전송한다. 여기서, Kc' 는 새로운 콘텐츠 키이다.

도 3 의 방법에 의하면, 사용자 u 에 속한 사용자 기기 DA,DB,DC 는, 사용자 DA 가 탈퇴하기 전에, 모두 세션 개인키 Kpri_s를 획득가능하므로, 콘텐츠 C를 재생할 수 있다. 따라서 사용자 기기가 별도로 라이센스를 취득하여야 하는 불편을 감소시킬 수 있다. 또한 사용자 기기는 고유 정보를 홈 서버로 전송할 필요가 없기 때문에 고유 정보의 불필요한 외부 유출을 막을 수 있다.

도 4 는 본 발명에 의한 홈 네트워크의 예를 나타내는 도면이다.

도 4에서, 현재 홈 서버 HS1 에 사용자 기기 DA,DB,DC 가 연결되어 있고, 홈 서버 HS1, 사용자 기기 DA,DB,DC 으로 구성된 홈 네트워크 HN 는 사용자 u 에 의해 소유된 상태라고 가정한다. 이 때 사용자 기기 DA 가 탈퇴하고자 한다.

도 3 의 콘텐츠 전송 방법에 따르면, 사용자 기기 DA 가 탈퇴한 후에는 세션키 쌍(Kpub_s, Kpri_s)이 새로운 세션 키 쌍(Kpub_s', Kpri_s')으로 갱신되기 때문에, 탈퇴한 사용자 기기 DA 는 사용자 기기 DA 의 탈퇴후에 사용자 기기로 전송되는 콘텐츠는 재생할 수 없다. 그렇지만, 사용자 기기 DA 는 여전히 세션 개인키 Kpri_s를 가지고 있기 때문에, 사용자 기기 DB 로부터 암호화된 콘텐츠 E(Kc,C) 및 암호화된 콘텐츠 키 E(Kpri_s, Kc)를 전송 받는다면, 탈퇴이전의 콘텐츠인 콘텐츠 C를 획득 및 재생할 수 있다.

디지털 콘텐츠에 대한 정책상의 이유로, 만약 사용자 기기 DA로하여금 사용자 기기 DB 로부터 탈퇴이전의 콘텐츠를 전송받아 재생하는 것을 방지하여야 하는 경우가 있다. 예를 들면 사용자 기기 DA 가 다른 사용자 u2 의 홈 네트워크 HN2 에 가입하게 된 경우이다. 이 경우에는, 사용자 u2 가 사용자 u 의 콘텐츠 C 를 사용하게 되는 불합리가 발생하기 때문에 바람직하지 않다. 도 5 의 사용자 기기 사이의 콘텐츠 전송 방법은 이러한 경우에 대한 대응책을 제시한다.

도 5 는 본 발명의 일 실시예에 따른 사용자 기기 사이의 콘텐츠 전송 방법을 나타내는 도면이다.

현재, 사용자 u1 의 홈 네트워크 HN1 에 홈 서버 HS1, 사용자 기기 DA,DB,DC 가 속해있고, 사용자 u2 의 홈 네트워크 HN2 에 홈 서버 HS2, 사용자 기기 DD,DE 가 속해 있다고 가정한다.

단계 510에서, 사용자 기기 DA 가 사용자 기기 DB 에게 콘텐츠 C를 요청한다.

단계 520에서, 사용자 기기 DB 는 사용자 기기 DB 가 속한 사용자의 사용자 공개키 Kpub_u1'을 사용자 기기 DA 로 전송한다.

단계 530 및 535에서, 사용자 기기 DA 는 소정의 기기 값 m 및 단계 520에서 수신한 사용자 공개키 Kpub_u1'을 이용하여 기기 인증값 CA를 생성한 후, 사용자 기기 DA 가 속한 홈 서버 HS1 에게 전송한다. 기기 인증값 CA 는 예를 들면 다음과 같이 생성된다.

[수학식1]

$$CA = m^{Kpub\text{-}u1'}$$

단계 540 및 545에서, 홈 서버 HS1은 단계 535에서 수신한 기기 인증값 C_A 및 홈 서버 HS1 이 속한 사용자인 사용자 u1 의 사용자 개인키 Kpri_u1을 이용하여 서버 인증값 CA'를 생성한 후, 사용자 기기 DA 로 전송한다. 서버 인증값 CA' 는 예를 들면 다음과 같이 생성된다.

[수학식 2]

$$CA' = CA^{Kpri\text{-}u1}$$

단계 550에서, 사용자 기기 DA 는 기기 인증값 CA 및 기기값 m 에 기초하여 사용자 기기 DA 의 사용자 u1 이 사용자 기기 DB 의 사용자와 동일한 지를 검사한다. 동일한 경우 단계 560으로 진행하고, 그렇지 않은 경우 단계 580으로 진행한다.

수학식 1 및 수학식 2 와 같이 기기 인증값 및 서버 인증값이 정의되는 경우에, 만약 사용자 기기 DB 의 사용자가 u1 이라면, 즉 단계 520에서 전송되는, 사용자 기기 DB 가 속한 사용자(미확인)의 사용자 공개키 Kpub_u1' 가 사용자 u1 의 사용자 공개키 Kpub_u1 라면, 서버 인증값 CA' 와 기기값 m 는 동일하다. 이는 이하 수학식 3 에 의해 증명된다.

[수학식 3]

$$CA' = CA^{Kpri\text{-}u1}$$
$$=(m^{Kpub\text{-}u1'})^{Kpri\text{-}u1}$$
$$=m^{Kpub\text{-}u1'*Kpri\text{-}u1}$$
$$=m^{Kpub\text{-}u1*Kpri\text{-}u1}$$
$$=m$$

단계 560에서, 사용자 기기 DA 는 성공 메시지 success를 사용자 기기 DB 로 전송한다.

단계 570에서, 사용자 기기 DB 는 성공 메시지 success 를 수신하면, 암호화된 콘텐츠 키 E(Kpub_s, Kc) 및 암호화된 콘텐츠 E(Kc,C)를 사용자 기기 DA 로 전송한다.

단계 580에서, 사용자 기기 DA 는 자신의 사용자와 사용자 기기 DB 의 사용자가 동일하지 않기 때문에, 콘텐츠 C를 전송받을 수 없다고 판단하고, 절차를 종료한다.

위의 실시예에서, 사용자 기기 DA 는 홈 서버 HS1 로부터 사용자에 관한 정보를 포함하는 서버 인증값 CA'를 수신하기 때문에, 사용자 기기 DA 는 자신이 속한 사용자 u1을 다른 사용자로 속일 수 없다. 즉 사용자 기기 DA 가 다른 사용자 u2 의 홈 네트워크에 속하게 된 경우에는 사용자 기기 DA 는 홈 서버 HS2로부터 서버 인증값을 수신할 것이므로, 수학식 3 과 같은 결과가 발생할 수 없다.

따라서 결국 사용자 기기 DA 는 사용자 기기 DB 의 사용자가 사용자 기기 DA 의 사용자와 동일한 경우에만 성공 메시지 success를 사용자 기기 DB에게 전송할 수 있다. 즉 사용자 기기 DA 는 자신의 사용자가 사용자 기기 DB 의 사용자가 동일함을 사용자 기기 DB 에게 입증한 경우에만 콘텐츠를 사용자 기기 DB 로부터 전송받을 수 있다.

도 6 는 본 발명의 다른 실시예에 따른 사용자 기기 사이의 콘텐츠 전송 방법을 나타내는 도면이다.

도 5와 마찬가지로, 사용자 u1 의 홈 네트워크 HN1 에 홈 서버 HS1, 사용자 기기 DA,DB,DC 가 속해있고, 사용자 u2 의 홈 네트워크 HN2 에 홈 서버 HS2, 사용자 기기 DD,DE 가 속해 있다고 가정한다.

단계 610에서, 사용자 기기 DA 가 사용자 기기 DB 에게 콘텐츠 C를 요청한다.

단계 620에서, 사용자 기기 DB 는 사용자 기기 DB 가 속한 사용자의 사용자 공개키 Kpub_u1'을 사용자 기기 DA 로 전송한다.

단계 630 및 635에서, 사용자 기기 DA 는 임의의 난수 r, 소정의 기기 값 m 및 단계 620에서 수신한 사용자 공개키 Kpub_u1'을 이용하여 기기 인증값 CA를 생성한 후, 사용자 기기 DA 가 속한 홈 서버 HS1 에게 전송한다. 기기 인증값 CA 는 예를 들면 다음과 같이 생성된다.

[수학식4]

$$CA = m * r^{Kpub\text{-}u1'}$$

단계 640 및 645에서, 홈 서버 HS1은 단계 635에서 수신한 기기 인증값 CA 및 홈 서버 HS1 이 속한 사용자인 사용자 u1 의 사용자 개인키 Kpri_u1을 이용하여 서버 인증값 CA'를 생성한 후, 사용자 기기 DA 로 전송한다. 서버 인증값 CA' 는 예를 들면 다음과 같이 생성된다.

[수학식 5]

$$CA' = CA^{Kpri\text{-}u1}$$

단계 650에서, 사용자 기기 DA 는 단계 630에서 사용되었던 임의의 난수 r, 기기 인증값 CA 및 기기값 m 에 기초하여 사용자 기기 DA 의 사용자 u1 이 사용자 기기 DB 의 사용자와 동일한 지를 검사한다. 동일한 경우 단계 660으로 진행하고, 그렇지 않은 경우 단계 680으로 진행한다.

수학식 4 및 수학식 5 와 같이 기기 인증값 및 서버 인증값이 정의되는 경우에, 만약 사용자 기기 DB 의 사용자가 u1 이라면, 즉 단계 620에서 전송되는, 사용자 기기 DB 가 속한 사용자(미확인)의 사용자 공개키 Kpub_u1' 가 사용자 u1 의 사용자 공개키 Kpub_u1 라면, 서버 인증값 CA'을 난수 r 로 나눈값 CA' r^{-1}와 기기값 m 는 동일하다. 이는 이하 수학식 6 에 의해 증명된다.

[수학식 6]

$$\begin{aligned} CA'*r^{-1} &= CA^{Kpri\text{-}u1}*r^{-1} \\ &= (m*r^{Kpub\text{-}u1'})^{Kpri\text{-}u1}*r^{-1} \\ &= m^{Kpri\text{-}u1}*r^{Kpub\text{-}u1'*Kpri\text{-}u1}*r^{-1} \\ &= m^{Kpri\text{-}u1}*r^{Kpub\text{-}u1*Kpri\text{-}u1}*r^{-1} \\ &= m*r*r^{-1} \\ &= m \end{aligned}$$

단계 660에서, 사용자 기기 DA 는 성공 메시지 success를 사용자 기기 DB 로 전송한다.

단계 670에서, 사용자 기기 DB 는 성공 메시지 success 를 수신하면, 암호화된 콘텐츠 키 E(Kpub_s, Kc) 및 암호화된 콘텐츠 E(Kc,C)를 사용자 기기 DA 로 전송한다.

단계 680에서, 사용자 기기 DA 는 자신의 사용자와 사용자 기기 DB 의 사용자가 동일하지 않기 때문에, 콘텐츠 C를 전송받을 수 없다고 판단하고, 절차를 종료한다.

도 5 와 마찬가지로, 사용자 기기 DA 는 홈 서버 HS1 로부터 사용자에 관한 정보를 포함하는 서버 인증값 CA'를 수신하기 때문에, 사용자 기기 DA 는 자신이 속한 사용자 u1을 다른 사용자로 속일 수 없다. 즉 사용자 기기 DA 가 다른 사용자 u2 의 홈 네트워크에 속하게 된 경우에는 사용자 기기 DA 는 홈 서버 HS2로부터 서버 인증값을 수신할 것이므로, 수학식 6 과 같은 결과가 발생할 수 없다. 따라서 결국 사용자 기기 DA 는 사용자 기기 DB 의 사용자가 사용자 기기 DA 의 사용자와 동일한 경우에만 성공 메시지 success를 사용자 기기 DB에게 전송할 수 있다. 즉 사용자 기기 DA 는 자신의 사용자가 사용자 기기 DB 의 사용자가 동일함을 사용자 기기 DB 에게 입증한 경우에만 콘텐츠를 사용자 기기 DB 로부터 전송받을 수 있다.

도 5 및 6 의 실시예에서, 기기값 m 는 사용자 기기 DA 의 고유 정보인 Xa를 해쉬한 값 m = h(Xa) 으로 정의되는 것도 가능하다. 고유 정보 Xa 는 해쉬된 후 홈 서버 HS1 으로 전송되기 때문에 고유 정보 Xa 는 외부에 공개되지 않는다.

도 7 은 도 5 의 콘텐츠 전송 방법에 있어서, 세션 키가 갱신되는 경우에 세션 키가 동일한지 검사하는 과정을 나타내는 도면이다.

사용자 기기 DA 와 DB 가 동일한 사용자 u1에 속하는 경우이더라도, 사용자 기기 DA 가 홈 네트워크 HN1 에 가입한 시기와 사용자 기기 DB 가 홈 네트워크 HN1 에 가입한 시기가 상이한 경우에는, 사용자 기기 DB가 가진 세션 키 Kpri_s 와 사용자 기기 DA 가 가진 세션 키 Kpri_s' 는 상이하다. 예를 들면 시간 t1 이전에 사용자 기기 DB 및 DC 가 홈 네트워크 HN1 에 존재하였는데 시간 t1에 사용자 기기 DA가 홈 네트워크 HN1 가입하였고, 그 결과 시간 t1 이후에 홈 네트워크 HN1 에 사용자 기기 DA,DB,DC 가 존재하는 경우이다.

홈 네트워크의 구성원의 변경이 있을 때에는 콘텐츠 키를 암호화하는데 사용되는 세션 키는 갱신되므로, 사용자 기기 DA 가 사용자 기기 DB로부터 암호화된 콘텐츠 키 E(Kpub_s,Kc)를 전송받더라도, 새로 가입한 사용자 기기 DA 는 가입 이전의 세션 키인 Kpri_s를 가지고 있지 않기 때문에 콘텐츠 키 Kc를 획득할 수 없다. 결국 사용자 기기 DA 와 DB 사이에 콘텐츠를 전송하는 경우에 세션 키의 버전이 동일한지를 검사하는 과정이 추가적으로 필요하다.

이하에서는 표 1 과 같은 상황을 전제로 세션 키의 버전을 검사하는 과정을 설명한다. 사용자 기기 DA 는 사용자 기기 DB 로부터 콘텐츠 C를 전송받고자 한다.

[표 1]

	t1이전	t1이후
HN1의 사용자 기기	DB,DC	DA,DB,DC
세션키 쌍	Kpri_s, Kpub_s	Kpri_s', Kpub_s'
암호화된 콘텐츠 키	E(Kpub_s, Kc)	E(Kpub_s', Kc)

단계 710에서, 사용자 기기 DA 는 임의의 난수인 제 1 난수 r 및 세션 개인 키 Kpri_s' 를 전자 서명 함수 S()를 이용하여 전자서명한다. 즉 사용자 기기 DA 는 자신이 가진 세션 개인 키 Kpri_s'를 이용하여 제 1 난수 r을 암호화함으로써 전자서명값 S_A = S(Kpri_s',r)을 생성한다.

단계 720에서, 사용자 기기 DA 는 단계 710에서 생성된 전자서명값 S_A 및 제 1 난수 r을 사용자 기기 DB 로 전송한다.

단계 730에서, 사용자 기기 DB는 단계 720에서 전송된 전자 서명값 S_A를 검증 함수 V()를 이용하여 검증한다. 즉 사용자 기기 DB 는 자신이 가진 세션 공개 키 Kpub_s를 이용하여 단계 720에서 전송된 전자 서명값 S_A를 복호화함으로써 생성된 결과값 V(Kpub_s, S_A) 이 단계720에서 전송된 제 1 난수 r과 동일한 지를 검사한다.

만약 사용자 기기 DA 가 전자 서명에 사용한 세션 개인키 Kpri_s' 가 사용자 기기 DB 가 가진 세션 공개키 Kpub_s 의 쌍인 세션 개인키 Kpri_s 와 동일하다면, 결과값 V(Kpub_s, S_A) 와 제 1 난수 r은 동일할 것이다. 이는 사용자 기기 DA 가 가진 세션 키 쌍의 버전이 사용자 기기 DB 가 가진 세션 키 쌍과 동일함을 의미한다.

단계 740에서, 사용자 기기 DB 는 단계 730에서의 제 1 난수 r 과 연관된 수인 제 2 난수(예를 들면 r+ 1) 및 세션 개인 키 Kpri_s 를 전자 서명 함수 S()를 이용하여 전자서명한다. 즉 사용자 기기 DB 는 자신이 가진 세션 개인 키 Kpri_s를 이용하여 전술한 연관된 난수 r+ 1 을 암호화함으로써 전자서명값 S_B = S(Kpri_s,r+ 1)을 생성한다.

단계 750에서, 사용자 기기 DB 는 단계 740에서 생성된 전자서명값 S_B 및 연관된 난수 r+ 1 을 사용자 기기 DA 로 전송한다.

단계 760에서, 사용자 기기 DA는 단계 750에서 전송된 전자 서명값 S_B를 검증 함수 V()를 이용하여 검증한다. 즉 사용자 기기 DA 는 자신이 가진 세션 공개 키 Kpub_s'를 이용하여 단계 750에서 전송된 전자 서명값 S_B를 복호화함으로써 생성된 결과값 V(Kpub_s', S_B) 이 단계 710에서의 제 1 난수에 + 1 한 값인 제 2 난수 r+ 1 과 동일한 지를 검사한다.

단계 710 내지 730과 마찬가지로, 만약 사용자 기기 DB 가 전자 서명에 사용한 세션 개인키 Kpri_s가 사용자 기기 DA 가 가진 세션 공개키 Kpub_s' 의 쌍인 세션 개인키 Kpri_s' 와 동일하다면, 결과값 V(Kpub_s', S_B) 와 제 2 난수 r+ 1은 동일할 것이다. 이는 사용자 기기 DB 가 가진 세션 키 쌍의 버전이 사용자 기기 DA 가 가진 세션 키 쌍과 동일함을 의미한다.

전술한 단계 710 내지 760 의 세션 키 버전 검사 과정은 도 5 의 단계 660 과 단계 670 사이에 추가된다. 즉 사용자 기기 DA 와 사용자 기기 DB 가 동일한 사용자에 속한 기기인지 확인하는 과정이후에 사요자 기기 DA 와 사용자 기기 DB 가 가진 세션키 쌍이 동일한 버전인지 확인하는 과정이 추가된다.

한편, 본 발명에 따른 콘텐츠 전송 방법은 컴퓨터 프로그램으로 작성 가능하다. 상기 프로그램을 구성하는 코드들 및 코드 세그먼트들은 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 상기 프로그램은 컴퓨터가 읽을 수 있는 정보저장매체(computer readable media)에 저장되고, 컴퓨터에 의하여 읽혀지고 실행됨으로써 콘텐츠 전송 방법을 구현한다. 상기 정보저장매체는 자기 기록매체, 광 기록매체, 및 캐리어 웨이브 매체를 포함한다.

이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

발명의 효과

전술한 바와 같이 본 발명에 따르면, 홈 네트워크내에서 콘텐츠를 사용자 기기마다 바인딩하는 것이 아니라, 공개키 구조를 이용하여 사용자마다 바인딩함으로써 콘텐츠를 안전하면서도 편리하게 공유할 수 있는 콘텐츠 전송 방법이 제공된다.

도면의 간단한 설명

도 1 는 홈 네트워트의 구조를 나타내는 도면.

도 2 는 종래의 콘텐츠 전송 방법을 나타내는 도면.

도 3 은 본 발명에 따른 홈 서버로부터 사용자 기기로의 콘텐츠 전송 방법을 나타내는 도면.

도 4 는 본 발명에 의한 홈 네트워크의 예를 나타내는 도면.

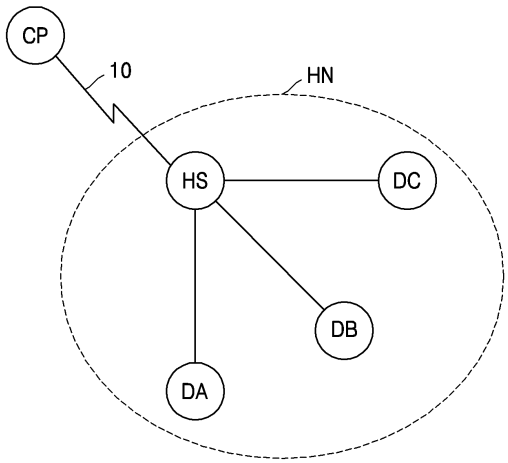
도 5 는 본 발명의 일 실시예에 따른 사용자 기기 사이의 콘텐츠 전송 방법을 나타내는 도면.

도 6 는 본 발명의 다른 실시예에 따른 사용자 기기 사이의 콘텐츠 전송 방법을 나타내는 도면.

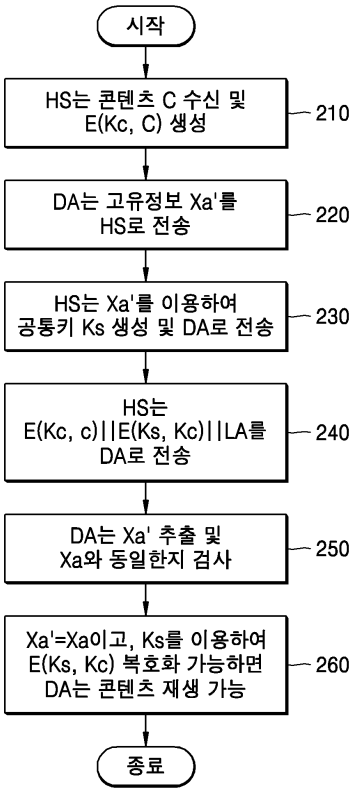
도 7 은 도 5 의 콘텐츠 전송 방법에 있어서, 세션 키가 갱신되는 경우에 세션 키가 동일한지 검사하는 과정을 나타내는 도면이다.

도면

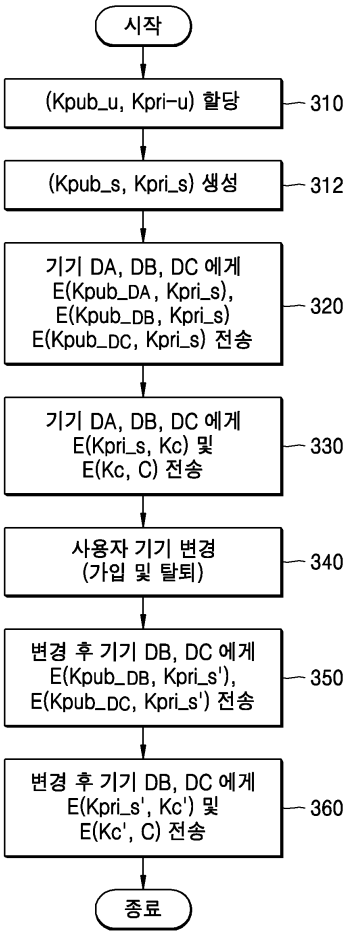
도면1



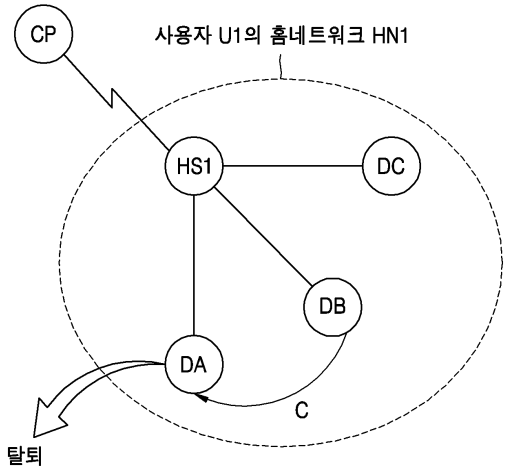
도면2


시작
HS는 콘텐츠 C 수신 및 E(Kc, C) 생성
210
DA는 고유정보 Xa'를 HS로 전송
220
HS는 Xa'를 이용하여 공통키 Ks 생성 및 DA로 전송
230
HS는 E(Kc, c)||E(Ks, Kc)||LA를 DA로 전송
240
DA는 Xa' 추출 및 Xa와 동일한지 검사
250
Xa'=Xa이고, Ks를 이용하여 E(Ks, Kc) 복호화 가능하면 DA는 콘텐츠 재생 가능
260
종료

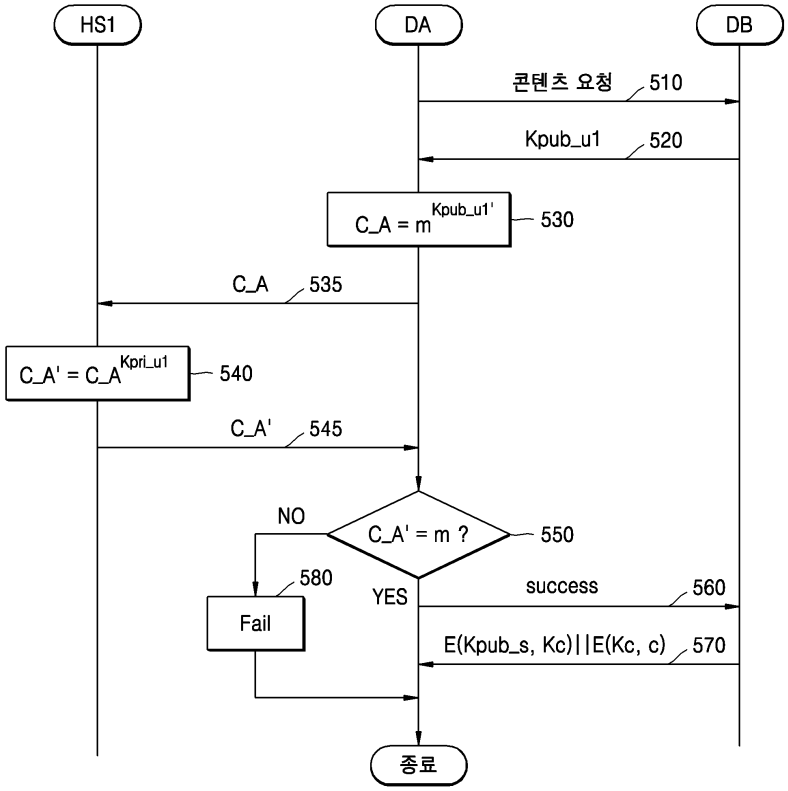
도면3


시작
(Kpub_u, Kpri-u) 할당
310
(Kpub_s, Kpri_s) 생성
312
기기 DA, DB, DC 에게 E(Kpub_DA, Kpri_s), E(Kpub_DB, Kpri_s) E(Kpub_DC, Kpri_s) 전송
320
기기 DA, DB, DC 에게 E(Kpri_s, Kc) 및 E(Kc, C) 전송
330
사용자 기기 변경 (가입 및 탈퇴)
340
변경 후 기기 DB, DC 에게 E(Kpub_DB, Kpri_s'), E(Kpub_DC, Kpri_s') 전송
350
변경 후 기기 DB, DC 에게 E(Kpri_s', Kc') 및 E(Kc', C) 전송
360
종료

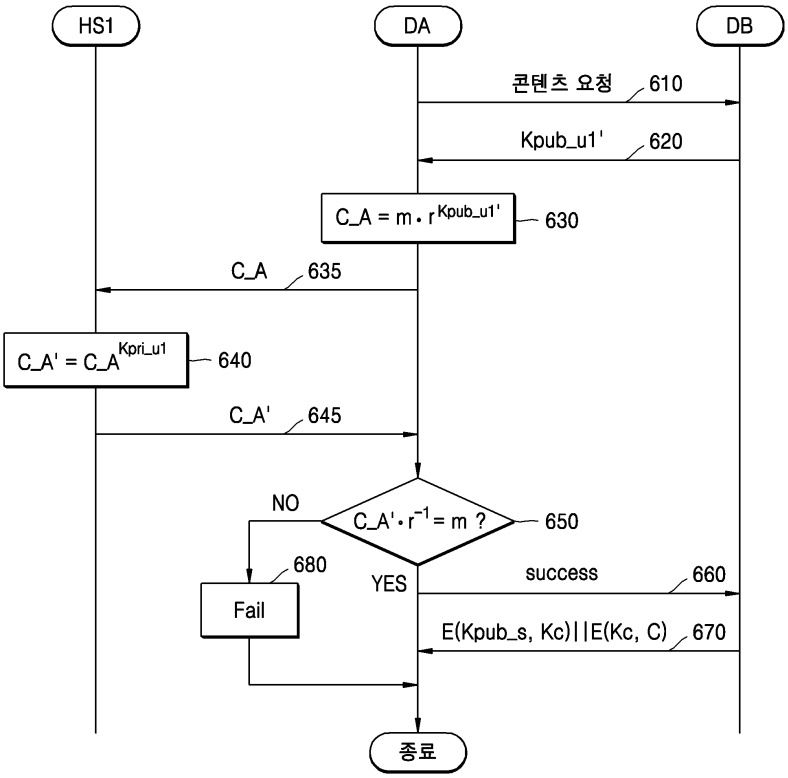
도면4


CP
사용자 U1의 홈네트워크 HN1
HS1
DC
DB
DA
C
탈퇴

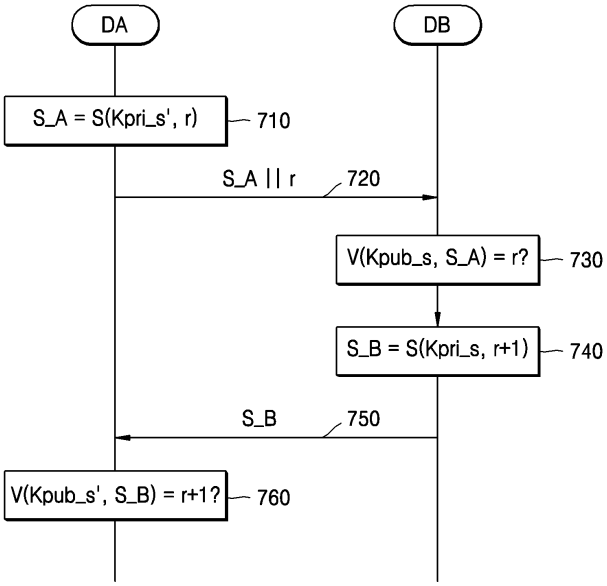
도면5


HS1
DA
DB
콘텐츠 요청
510
Kpub_u1
520
C_A = m^Kpub_u1'
530
C_A
535
C_A' = C_A^Kpri_u1
540
C_A'
545
NO
C_A' = m ?
550
580
YES
success
560
Fail
E(Kpub_s, Kc)||E(Kc, c)
570
종료

도면6


HS1
DA
DB
콘텐츠 요청
610
Kpub_u1'
620
C_A = m • r^Kpub_u1'
630
C_A
635
C_A' = C_A^Kpri_u1
640
C_A'
645
NO
C_A' • r^-1 = m ?
650
680
Fail
YES
success
660
E(Kpub_s, Kc)||E(Kc, C)
670
종료

도면7


DA
DB
S_A = S(Kpri_s', r)
710
S_A || r
720
V(Kpub_s, S_A) = r?
730
S_B = S(Kpri_s, r+1)
740
S_B
750
V(Kpub_s', S_B) = r+1?
760