



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월01일
(11) 등록번호 10-1423955
(24) 등록일자 2014년07월22일

(51) 국제특허분류(Int. Cl.)

H04N 21/6334 (2011.01) H04N 21/2347

(2011.01)

H04N 21/4623 (2011.01)

(21) 출원번호 10-2013-0075344

(22) 출원일자 2013년06월28일

심사청구일자 2013년06월28일

(56) 선행기술조사문헌

KR1020130022906 A

KR1020120035069 A

KR1020110070765 A

KR1020090089948 A

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

이동훈

서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)

김효승

서울 성북구 안암로 145, 정보보호대학원 (안암동5가, 고려대학교)

(뒷면에 계속)

(74) 대리인

특허법인충현

전체 청구항 수 : 총 6 항

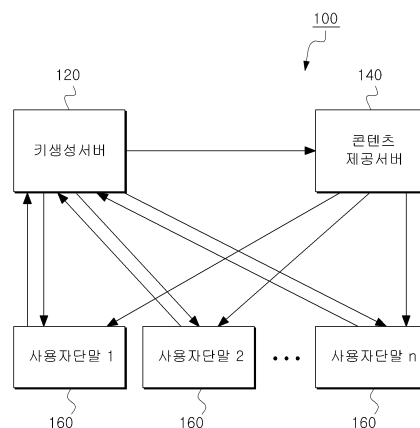
심사관 : 박부식

(54) 발명의 명칭 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템

(57) 요약

본 발명은 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템에 관한 것으로, 보다 구체적으로는 키생성서버가 접속형 그룹에 속하는 생성원 및 임의의 원소를 생성하고, 생성한 생성원 및 원소를 접속형 함수에 적용하여 공개 파라미터를 생성하는 단계; 상기 키생성서버가 사용자단말로부터 콘텐츠에 접근하고자 하는 접근구조 집합을 수신하고, 상기 접근구조 집합에 기초하여 상기 콘텐츠에 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 단계; 콘텐츠 제공서버가 상기 키생성서버로부터 상기 공개 파라미터를 수신하고, 수신한 공개 파라미터에 기초하여 상기 콘텐츠를 암호화하여 콘텐츠 암호문을 생성한 후, 생성된 콘텐츠 암호문을 사용자단말로 전송하는 단계; 및 상기 사용자단말이 상기 키생성서버로부터 접근권리 비밀키를 수신하고, 수신한 접근권리 비밀키에 기초하여 상기 콘텐츠 제공서버로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠에 접근하는 단계;를 포함한다. 이러한 구성에 의해, 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 콘텐츠의 접근 가능 여부를 나타내는 접근권리 비밀키를 콘텐츠와 함께 암호화하여 사용자단말이 콘텐츠에 대한 접근 가능 여부 및 콘텐츠 수신을 보다 효율적으로 수신할 수 있는 효과가 있다.

대표도 - 도1



(72) 발명자

박승환

서울 성북구 안암로 145, 정보보호대학원 (안암동 5가, 고려대학교)

박중환

서울특별시 성북구 정릉로 292 (정릉동, 현대홈타운아파트) 106동 801호

이 발명을 지원한 국가연구개발사업

과제고유번호 20120008697

부처명 한국연구재단

연구사업명 중견연구자지원_도약연구(전략)

연구과제명 속성 기반 공개키 시스템에 관한 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2012.09.01 ~ 2013.08.31

특허청구의 범위

청구항 1

키생성서버가 겹선형 그룹에 속하는 생성원 및 임의의 원소를 생성하고, 생성한 생성원 및 원소를 겹선형 함수에 적용하여 공개 파라미터를 생성하는 단계;

상기 키생성서버가 사용자단말로부터 콘텐츠에 접근하고자 하는 접근구조 집합을 수신하고, 상기 접근구조 집합에 기초하여 상기 콘텐츠에 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 단계;

콘텐츠 제공서버가 상기 키생성서버로부터 상기 공개 파라미터를 수신하고, 수신한 공개 파라미터에 기초하여 상기 콘텐츠를 암호화하여 콘텐츠 암호문을 생성한 후, 생성된 콘텐츠 암호문을 사용자단말로 전송하는 단계; 및

상기 사용자단말이 상기 키생성서버로부터 접근권리 비밀키를 수신하고, 수신한 접근권리 비밀키에 기초하여 상기 콘텐츠 제공서버로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠에 접근하는 단계;

를 포함하되,

상기 키생성서버가 공개 파라미터를 생성하는 단계는

제1 겹선형 그룹에 속하는 생성원 및 복수 개의 임의의 원소를 생성하고, 상기 복수 개의 임의의 원소들에 대한 집합을 설정하는 과정;

상기 제1 겹선형 그룹에 속하는 임의의 제1 원소 및 제2 원소를 생성하고, 제2 겹선형 그룹에 속하는 임의의 제3 원소 및 제4 원소를 생성하는 과정;

상기 생성원 및 제1 원소에 기초하여 제1 변수를 생성하고, 상기 생성원 및 제2 원소에 기초하여 제2 변수를 생성하는 과정;

상기 제3 원소와 제1 변수 및 상기 제4 원소와 제2 변수를 각각 겹선형 함수에 적용하여 겹선형 함수값을 생성하는 과정;

상기 생성원, 제1 변수, 제2 변수, 상기 복수 개의 임의의 원소들의 집합 및 겹선형 함수값을 포함하는 공개 파라미터를 생성하는 과정; 및

상기 공개 파라미터를 상기 콘텐츠 제공서버로 전송하는 과정;

을 포함하는 것을 특징으로 하는 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 키생성서버가 접근권리 비밀키를 생성하는 단계는

상기 콘텐츠에 대한 복수 개의 접근구조를 나타내는 접근구조의 집합을 획득하는 과정;

제1 겹선형 그룹에 속하는 임의의 제5 원소 및 제6 원소를 생성하는 과정;

상기 제5 원소와 제1 원소를 곱한값을 상기 제6 원소와 제2 원소를 곱한 값을 합산하여 제3 변수를 생성하는 과정;

상기 제3 변수 및 공개 파라미터에 기초하여 상기 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 과정; 및

상기 접근권리 비밀키를 상기 사용자단말로 전송하는 과정;
을 포함하는 것을 특징으로 하는 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법.

청구항 4

제1항 및 제3항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록 매체.

청구항 5

공개 파라미터를 생성하고, 콘텐츠에 접근하고자 하는 사용자단말에 대하여 콘텐츠에 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 키생성서버;

상기 키생성서버로부터 상기 공개 파라미터를 수신하고, 수신한 공개 파라미터에 기초하여 콘텐츠를 암호화한 후 콘텐츠 암호문을 생성하고, 생성된 콘텐츠 암호문을 상기 사용자단말로 분배하는 콘텐츠 제공서버; 및

상기 콘텐츠에 접근하고자 하는 접근구조를 상기 키생성서버에 전송하고, 상기 키생성서버로부터 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 수신하며, 수신한 접근권리 비밀키에 기초하여 상기 콘텐츠 제공서버로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠에 접근하는 사용자단말;

을 포함하되,

상기 키생성서버는

제1 곱선형 그룹에 속하는 생성원 및 복수 개의 임의의 원소를 생성하고, 상기 복수 개의 임의의 원소들에 대한 집합을 설정하고, 상기 제1 곱선형 그룹에 속하는 임의의 제1 원소 및 제2 원소를 생성하며, 제2 곱선형 그룹에 속하는 임의의 제3 원소 및 제4 원소를 생성하고, 상기 생성원 및 제1 원소에 기초하여 제1 변수를 생성하며, 상기 생성원 및 제2 원소에 기초하여 제2 변수를 생성하는 변수생성모듈;

상기 제3 원소와 제1 변수 및 상기 제4 원소와 제2 변수를 각각 곱선형 함수에 적용하여 곱선형 함수값을 생성하는 곱선형함수연산모듈;

상기 생성원, 제1 변수, 제2 변수, 상기 복수 개의 임의의 원소들의 집합 및 곱선형 함수값을 포함하는 공개 파라미터를 생성하는 공개 파라미터 생성모듈; 및

상기 공개 파라미터를 상기 콘텐츠 제공서버로 전송하는 전송모듈;

을 포함하는 것을 특징으로 하는 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 시스템.

청구항 6

삭제

청구항 7

제5항에 있어서,

상기 키생성서버는

상기 콘텐츠에 대한 복수 개의 접근구조를 나타내는 접근구조 집합을 상기 사용자단말로부터 수신하는 접근구조 집합 수신모듈;

제1 곱선형 그룹에 속하는 임의의 제5 원소 및 제6 원소를 생성하는 원소생성모듈; 및

상기 제5 원소와 제1 원소를 곱한 값을 상기 제6 원소와 제2 원소를 곱한 값을 합산하여 제3 변수를 생성한 후, 상기 제3 변수 및 공개 파라미터에 기초하여 상기 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 접근권리 비밀키 생성모듈;

을 포함하는 것을 특징으로 하는 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 시스템.

청구항 8

제7항에 있어서,

상기 전송모듈은

상기 접근권리 비밀키를 상기 사용자단말로 전송하는 것을 더 포함하는 것을 특징으로 하는 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 시스템.

명세서

기술 분야

[0001] 본 발명은 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템에 관한 것으로, 특히 콘텐츠에 접근하고자 하는 사용자단말의 접근 구조를 분배하고자 하는 콘텐츠와 함께 암호화하여 복수 개의 각 사용자단말로 분배하여 사용자단말이 콘텐츠의 접근 제어를 통해 허용된 콘텐츠에 용이하게 접근할 수 있는 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템에 관한 것이다.

배경 기술

[0002] IT 기술이 급격히 발달에 따라, 다양한 정보 제공이 가능한 IPTV가 등장하였다. 이러한 IPTV란, Internet Protocol Television의 약자로서, 초고속 인터넷을 이용하여 정보 서비스, 동영상 콘텐츠 및 방송 등을 텔레비전 수상기로 제공하는 서비스를 말한다. 이러한 IPTV를 이용하기 위해서는, 텔레비전 수상기, 셋탑박스 및 인터넷 회선이 상호 연결되어, 텔레비전에 셋탑박스(set top box) 또는 전용 모뎀을 연결하고, 텔레비전을 켜듯이 전원만 제공하면 이용할 수 있다. 따라서, 컴퓨터의 사용에 익숙하지 않은 사람이라도 리모컨을 사용하여 간단한 인터넷 검색 뿐만 아니라, 영화감상, 홈쇼핑, 홈뱅킹, 온라인 게임, MP3 재생 등과 같이 인터넷이 제공하는 다양한 콘텐츠 및 부가 서비스를 제공받을 수 있다.

[0003] 특히, 이러한 IPTV는 비디오를 비롯한 방송 콘텐츠를 제공한다는 점에서 일반 케이블 방송이나 위성방송과 큰 차이점이 없지만, 양방향성이 추가된다는 점이 큰 특징이며, 일반적인 공중파 방송이나 케이블방송 또는 위성방송과는 달리, 시청자가 자신이 원하는 시간에 보고 싶은 프로그램만 볼 수 있다.

[0004] 이와 같이, IPTV에서 보여지는 콘텐츠에 대해서는 특히, DRM이 사용되고 있다. 상기 DRM(Digital Right Management)이란, 정당하게 구매한 사용자만이 해당 콘텐츠의 사용권한을 제공받고, 구매하지 않은 사용자가 해당 콘텐츠에 불법적으로 접근하는 것을 차단하는 솔루션을 말한다. 즉, 상기 DRM이란, 디지털 콘텐츠의 불법유통과 복제를 방지하고, 적법한 사용자만이 콘텐츠를 이용하도록 하며, 과금 서비스를 통해 디지털 콘텐츠 저작권을 관리하는 기술을 나타낸다. 이때, 보호되는 콘텐츠(contents)란, 지적자산의 가치가 있는 정보단위를 나타내며, 허가되지 않은 사용자의 접근으로부터 보호해야 하는 대상이다.

[0005] 즉, 사용자단말은 부여된 사용권한 및 사용조건에 따라 콘텐츠를 이용하는 주체이며, 이러한 콘텐츠의 이용권리는 콘텐츠별 정해진 사용권한에 의해 결정된다. 특히, 콘텐츠의 사용조건은 사용권한이 수행되기 위한 요구조건 및 제한 요소를 포함하고 있다.

[0006] 이러한 DRM은 각각의 사용자단말로 각 콘텐츠에 대한 접근 권리를 생성하여 전송하기 때문에 사용자의 단말 수 및 제공하는 콘텐츠의 수 만큼 콘텐츠에 대한 접근 권리를 나타내는 접근권리키(REK, Right Encryption Key)를 복수 개 생성해야함에 따라, 사용자로 하여금 번거로움을 야기시키는 문제점이 발생했다.

[0007] 상술한 바와 같이, 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템을 살펴보면 다음과 같다.

[0008] 선행기술 1은 한국등록특허 제10-0753829호(2007.08.24)로서, 콘텐츠 보호 기능을 갖는 모바일 리더 및 콘텐츠 서버와 그 방법에 관한 것이다. 이러한 선행기술 1은 (a) 전자태그에 저장된 콘텐츠 정보를 리드하는 단계; (b) 상기 콘텐츠 정보의 콘텐츠 등급이 사용자가 이용할 수 있는 콘텐츠 등급인지를 판단하는 단계; (c) 상기 (b)

단계에서 사용자가 이용이 가능한 콘텐츠 등급으로 판단되면 콘텐츠 서버에 접속하여 콘텐츠를 요구하는 단계; (d) 상기 콘텐츠 서버로부터 사용자 인증 및 과금 상태를 확인하여 사용자 인증이 완료되면 암호화된 콘텐츠의 암호키(CK) 주소와 콘텐츠를 수신하는 단계; 및 (e) 복호한 CK 주소로 CK 매트릭스를 조회하여 얻은 값을 이용하여 암호화된 상기 콘텐츠를 복호화하는 단계;를 포함하여, 태그가 부착된 스마트 포스터에서 통신 서비스 사업자와 콘텐츠 서비스 사업자간의 공유 정보를 최소화하면서 콘텐츠 보호를 가능하게 하는 한편, 태그 식별자 이외에 콘텐츠 등급을 부가적으로 스마트 포스터에 기록하고 암호키의 전달이 아닌 키 주소만을 통신 경로상에 전달함으로써 콘텐츠 보호 시스템의 효율을 높이는 효과가 있다.

[0009]

또한, 선행기술 2는 한국등록특허 제10-0778951호(2007.11.16)로서, 사생활 보호를 위한 이동통신 단말기 및 수신된 콘텐츠 확인 방법에 관한 것이다. 이러한 선행기술 2는 미리 지정해 놓은 상대방으로부터 발신된 콘텐츠를 보관하는 비밀 콘텐츠 보관함; 상기 비밀 콘텐츠 보관함을 관리할 수 있는 비밀 콘텐츠 보관함 메뉴 정보를 저장하는 메모리; 복수개의 선택 키들을 구비하고, 사용자에게 의해 선택된 선택 키에 해당하는 키 값을 발생시키는 키 입력부; 및 상기 비밀 콘텐츠 보관함의 접근 제한을 위해 미리 설정해 놓은 암호 값이 상기 키 입력부를 통해 입력되는 경우, 상기 메모리에 저장되어 있는 비밀 콘텐츠 보관함 메뉴 정보가 표시부에 표시되도록 하는 제어부;를 포함하여, 타인에 대해 비밀 유지가 필요한 콘텐츠를 주고 받을 상대방 정보를 저장부에 등록하고, 상기 등록한 상대방으로부터 발신되는 콘텐츠를 저장부의 비밀 콘텐츠 보관함에 보관하며, 상기 비밀 콘텐츠 보관함에 접근하기 위한 암호 값을 설정함으로써, 이동통신 단말기에 있어서 사생활 보호 기능을 강화할 수 있다.

발명의 내용

해결하려는 과제

[0010]

상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 사용자단말로 콘텐츠에 대한 접근권리를 나타내는 접근권리 키와 콘텐츠 암호문을 함께 포함하여 생성함으로써, 사용자단말이 비교적 적은 복호화 과정을 통해 콘텐츠에 대한 접근 제어 및 접근이 허용된 콘텐츠를 용이하게 이용할 수 있는 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템을 제공하고자 한다.

과제의 해결 수단

[0011]

위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법은 키생성서버가 곁선형 그룹에 속하는 생성원 및 임의의 원소를 생성하고, 생성한 생성원 및 원소를 곁선형 함수에 적용하여 공개 파라미터를 생성하는 단계; 상기 키생성서버가 사용자단말로부터 콘텐츠에 접근하고자 하는 접근구조 집합을 수신하고, 상기 접근구조 집합에 기초하여 상기 콘텐츠에 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 단계; 콘텐츠 제공서버가 상기 키생성서버로부터 상기 공개 파라미터를 수신하고, 수신한 공개 파라미터에 기초하여 상기 콘텐츠를 암호화하여 콘텐츠 암호문을 생성한 후, 생성된 콘텐츠 암호문을 사용자단말로 전송하는 단계; 및 상기 사용자단말이 상기 키생성서버로부터 접근권리 비밀키를 수신하고, 수신한 접근권리 비밀키에 기초하여 상기 콘텐츠 제공서버로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠에 접근하는 단계;를 포함한다.

[0012]

보다 바람직하게는 제1 곁선형 그룹에 속하는 생성원 및 복수 개의 임의의 원소를 생성하고, 상기 복수 개의 임의의 원소들에 대한 집합을 설정하는 과정; 상기 제1 곁선형 그룹에 속하는 임의의 제1 원소 및 제2 원소를 생성하고, 제2 곁선형 그룹에 속하는 임의의 제3 원소 및 제4 원소를 생성하는 과정; 상기 생성원 및 제1 원소에 기초하여 제1 변수를 생성하고, 상기 생성원 및 제2 원소에 기초하여 제2 변수를 생성하는 과정; 상기 제3 원소와 제1 변수 및 상기 제4 원소와 제2 변수를 각각 곁선형 함수에 적용하여 곁선형 함수값을 생성하는 과정; 상기 생성원, 제1 변수, 제2 변수, 상기 복수 개의 임의의 원소들의 집합 및 곁선형 함수값을 포함하는 공개 파라미터를 생성하는 과정; 및 상기 공개 파라미터를 상기 콘텐츠 제공서버로 전송하는 과정;을 포함하는 키생성서버가 공개 파라미터를 생성하는 단계를 포함할 수 있다.

[0013]

보다 바람직하게는 상기 콘텐츠에 대한 복수 개의 접근구조를 나타내는 접근구조의 집합을 획득하는 과정; 제1 곁선형 그룹에 속하는 임의의 제5 원소 및 제6 원소를 생성하는 과정; 상기 제5 원소와 제1 원소를 곱한값을 상기 제6 원소와 제2 원소를 곱한 값을 합산하여 제3 변수를 생성하는 과정; 상기 제3 변수 및 공개 파라미터에 기초하여 상기 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 과정; 및 상기 접근권리

비밀키를 상기 사용자단말로 전송하는 과정;을 포함하는 키생성서버가 접근구조 비밀키를 생성하는 단계를 포함할 수 있다.

[0014] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 시스템은 공개 파라미터를 생성하고, 콘텐츠에 접근하고자 하는 사용자단말에 대하여 콘텐츠에 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 키생성서버; 상기 키생성서버로부터 상기 공개 파라미터를 수신하고, 수신한 공개 파라미터에 기초하여 콘텐츠를 암호화한 후 콘텐츠 암호문을 생성하고, 생성된 콘텐츠 암호문을 상기 사용자단말로 분배하는 콘텐츠 제공서버; 및 상기 콘텐츠에 접근하고자 하는 접근구조를 상기 키생성서버에 전송하고, 상기 키생성서버로부터 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 수신하며, 수신한 접근권리 비밀키에 기초하여 상기 콘텐츠 제공서버로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠에 접근하는 사용자단말;을 포함한다.

[0015] 보다 바람직하게는 제1 곱선형 그룹에 속하는 생성원 및 복수 개의 임의의 원소를 생성하고, 상기 복수 개의 임의의 원소들에 대한 집합을 설정하고, 상기 제1 곱선형 그룹에 속하는 임의의 제1 원소 및 제2 원소를 생성하며, 제2 곱선형 그룹에 속하는 임의의 제3 원소 및 제4 원소를 생성하고, 상기 생성원 및 제1 원소에 기초하여 제1 변수를 생성하며, 상기 생성원 및 제2 원소에 기초하여 제2 변수를 생성하는 변수생성모듈; 상기 제3 원소와 제1 변수 및 상기 제4 원소와 제2 변수를 각각 곱선형 함수에 적용하여 곱선형 함수값을 생성하는 곱선형함수연산모듈; 상기 생성원, 제1 변수, 제2 변수, 상기 복수 개의 임의의 원소들의 집합 및 곱선형 함수값을 포함하는 공개 파라미터를 생성하는 공개 파라미터 생성모듈; 및 상기 공개 파라미터를 상기 콘텐츠 제공서버로 전송하는 전송모듈;을 포함하는 키생성서버를 포함할 수 있다.

[0016] 보다 바람직하게는 상기 콘텐츠에 대한 복수 개의 접근구조를 나타내는 접근구조 집합을 상기 사용자단말로부터 수신하는 접근구조 집합 수신모듈; 제1 곱선형 그룹에 속하는 임의의 제5 원소 및 제6 원소를 생성하는 원소생성모듈; 및 상기 제5 원소와 제1 원소를 곱한 값을 상기 제6 원소와 제2 원소를 곱한 값을 합산하여 제3 변수를 생성한 후, 상기 제3 변수 및 공개 파라미터에 기초하여 상기 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 생성하는 접근권리 비밀키 생성모듈;을 포함하는 키생성서버를 포함할 수 있다.

[0017] 특히, 상기 접근권리 비밀키를 상기 사용자단말로 전송하는 전송모듈을 포함할 수 있다.

발명의 효과

[0018] 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 콘텐츠의 접근 가능 여부를 나타내는 접근권리 비밀키를 콘텐츠와 함께 암호화하여 사용자단말이 콘텐츠에 대한 접근 가능 여부 및 콘텐츠 수신을 보다 효율적으로 수신할 수 있는 효과가 있다.

[0019] 또한, 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 콘텐츠 암호문의 복호화 시, 사용자단말이 페어링 연산을 0 또는 1 번만 수행하기 때문에 콘텐츠 암호문의 복호화 시간이 감소하는 효과가 있다.

[0020] 더불어, 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 콘텐츠에 접근하고자 하는 사용자단말로 콘텐츠의 접근구조에 대한 AND, OR, threshold, wildcard 등의 기능을 제공함으로써, 콘텐츠에 대하여 다양한 접근 제어를 수행할 수 있는 효과가 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시 예에 따른 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 시스템의 블록도이다.

도 2는 본 발명의 다른 실시 예에 따른 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법의 순서도이다.

도 3은 키생성서버가 공개 파라미터를 생성하는 단계의 세부과정을 나타낸 순서도이다.

도 4는 키생성서버가 접근권리 비밀키를 생성하는 단계의 세부과정을 나타낸 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식

을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

- [0023] 도 1은 본 발명의 일 실시 예에 따른 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 시스템의 블록도이다.
- [0024] 도 1에 도시된 바와 같이, 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 시스템(100)은 키생성 서버(120), 콘텐츠 제공서버(140) 및 적어도 하나의 사용자단말(160)을 포함한다.
- [0025] 키생성서버(120)는 상기 콘텐츠 제공서버(140)로 제공되는 공개 파라미터를 생성하고, 콘텐츠에 접근하고자 하는 사용자단말에 대하여 콘텐츠에 접근 가능 여부를 나타내는 접근권리 비밀키를 생성한다. 이러한 키생성서버(120)는 변수생성모듈, 곱선형함수연산모듈, 공개 파라미터 생성모듈, 전송모듈, 접근구조 집합 획득모듈, 원소 생성모듈 및 접근권리 비밀키 생성모듈을 포함한다.
- [0026] 변수생성모듈은 제1 곱선형 그룹에 속하는 복수 개의 생성원을 생성하고, 상기 복수 개의 생성원들에 대한 집합을 설정하고, 상기 제1 곱선형 그룹에 속하는 임의의 제1 원소 및 제2 원소를 생성하며, 제2 곱선형 그룹에 속하는 임의의 제3 원소 및 제4 원소를 생성하고, 상기 생성원 및 제1 원소에 기초하여 제1 변수를 생성하며, 상기 생성원 및 제2 원소에 기초하여 제2 변수를 생성한다.
- [0027] 곱선형함수연산모듈은 상기 제3 원소와 제1 변수 및 상기 제4 원소와 제2 변수를 각각 곱선형 함수에 적용하여 곱선형 함수값을 생성한다.
- [0028] 공개 파라미터 생성모듈은 상기 생성원, 제1 변수, 제2 변수, 상기 복수 개의 생성원들의 집합 및 곱선형 함수값을 포함하는 공개 파라미터를 생성한다.
- [0029] 전송모듈은 상기 공개 파라미터를 상기 콘텐츠 제공서버(140)로 전송하고, 상기 접근권리 비밀키를 상기 사용자단말(160)로 전송한다.
- [0030] 접근구조 집합 수신모듈은 각 사용자단말의 상기 콘텐츠에 대한 복수 개의 접근구조를 나타내는 접근구조 집합을 사용자단말(160)로부터 수신한다.
- [0031] 원소생성모듈은 제1 곱선형 그룹에 속하는 임의의 제5 원소 및 제6 원소를 생성한다.
- [0032] 접근권리 비밀키 생성모듈은 상기 제5 원소와 제1 원소를 곱한 값을 상기 제6 원소와 제2 원소를 곱한 값을 합산하여 제3 변수를 생성한 후, 상기 제3 변수 및 공개 파라미터에 기초하여 상기 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 생성한다.
- [0033] 콘텐츠 제공서버(140)는 상기 키생성서버(120)로부터 상기 공개 파라미터를 수신하고, 수신한 공개 파라미터에 기초하여 사용자단말(160)로 분배하고자 하는 콘텐츠를 암호화한 후 콘텐츠 암호문을 생성하고, 생성된 콘텐츠 암호문을 상기 사용자단말(160)로 분배한다.
- [0034] 사용자단말(160)는 상기 콘텐츠에 접근하고자 하는 접근구조를 상기 키생성서버(120)에 전송하고, 상기 키생성서버(120)로부터 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키를 수신하며, 수신한 접근권리 비밀키에 기초하여 상기 콘텐츠 제공서버(140)로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠를 이용한다.
- [0035] 이하, 도 2 내지 도 4를 참조하여 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법에 대하여 자세하게 살펴보도록 한다.
- [0036] 먼저, 본 발명의 세부과정을 설명하기에 앞서, 전제되는 조건들에 대하여 간략히 설명하도록 한다.

- [0037] G_1 은 소수 p 를 위수로 갖는 곱선형 그룹(bilinear group)을 나타내는데, 이때 g 는 상기 곱선형 그룹 G_1

의 생성원(generator)이라 하고, $e : G_1 \times G_1 \rightarrow G_2$ 을 곱선형 함수로 정의한다. 이러한, 상기 곱선형 함

수란, 곱선형 그룹 G 와 G_T 에서 모두 이산대수문제(discrete logarithm problem)가 어렵다고 가정할 때, 곱선형성(bilinearity), 비소실성(non-degeneracy) 또는 계산가능성(computability)의 조건을 만족하는 함수를 나타낸다.

- [0038] 도 2는 본 발명의 다른 실시 예에 따른 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법의 순서도이다.

- [0039] 도 2에 도시된 바와 같이, 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법은 먼저, 키생성 서버(120)가 겹선형 그룹에 속하는 생성원 및 복수 개의 임의의 원소를 생성하고, 생성한 생성원 및 복수 개의 임의의 원소를 겹선형 함수에 적용하여 공개 파라미터를 생성한다(S210).
- [0040] 상기 키생성서버(120)가 사용자단말(160)로부터 콘텐츠에 접근하고자 하는 접근구조 집합을 수신하고, 상기 접근구조 집합에 기초하여 상기 콘텐츠에 접근 가능 여부를 나타내는 접근권리 비밀키를 생성한다(S220).
- [0041] 콘텐츠 제공서버(140)가 상기 키생성서버(120)로부터 상기 공개 파라미터를 수신하고, 수신한 공개 파라미터에 기초하여 상기 콘텐츠를 암호화하여 콘텐츠 암호문을 생성한 후, 생성된 콘텐츠 암호문을 사용자단말(160)로 전송한다(S230).
- [0042] 상기 사용자단말(160)이 상기 키생성서버(120)로부터 접근권리 비밀키를 수신하고, 수신한 접근권리 비밀키에 기초하여 상기 콘텐츠 제공서버(140)로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠에 접근한다(S240).
- [0043] 이하, 도 3을 참조하여 과정 S210의 공개 파라미터를 생성하는 단계에 대하여 보다 자세히 살펴보도록 한다.
- [0044] 도 3은 키생성서버가 공개 파라미터를 생성하는 단계의 세부과정을 나타낸 순서도이다.
- [0045] 도 3에 도시된 바와 같이, 키생성서버(120)가 제1 겹선형 그룹에 속하는 복수 개의 생성원을 생성하고, 상기 복수 개의 생성원들에 대한 집합을 설정한다(S211). 즉, 키생성서버(120)가 겹선형 그룹 G 에 속하는 생성원 및 복수 개의 임의의 원소 $g_i, h_{i,1}, h_{i,2}, \dots, h_{i,l_i}$ 를 선택하고, 선택한 생성원 및 임의의 원소들 $g_i, h_{i,1}, h_{i,2}, \dots, h_{i,l_i}$ 에 대한 집합 $H_{i,k}(g_i, h_{i,1}, h_{i,2}, \dots, h_{i,l_i})$ for $i = 1, \dots, u$ 을 설정한다.
- [0046] 이어서, 키생성서버(120)가 상기 제1 겹선형 그룹 Z_p 에 속하는 임의의 제1 원소 z_1 와, 제2 원소 z_2 를 생성하고, 제2 겹선형 그룹 G 에 속하는 임의의 제3 원소 u_1 와, 제4 원소 u_2 를 생성한다(S212).
- [0047] 이후, 상기 키생성서버(120)가 앞서 생성한 상기 생성원 g 및 제1 원소 z_1 에 기초하여 제1 변수 $y_1 = g^{z_1}$ 를 생성하고, 상기 생성원 g 및 제2 원소 z_2 에 기초하여 제2 변수 $y_2 = g^{z_2}$ 를 각각 생성한다(S213).
- [0048] 또한, 상기 키생성서버(120)가 앞서 생성한 상기 제3 원소 u_1 와 제1 변수 y_1 및 상기 제4 원소 u_2 와 제2 변수 y_2 를 각각 겹선형 함수 $e(u_1, g^{z_1})e(u_2, g^{z_2})$ 에 적용하여 이에 따른 겹선형 함수값 Ψ 를 생성한다(S214).
- [0049] 이에 따라, 상기 키생성서버(120)가 상기 생성원 g , 제1 변수 y_1 , 제2 변수 y_2 , 상기 복수 개의 임의의 원소들의 집합 $H_{i,k}$ 및 겹선형 함수값 Ψ 를 포함하는 공개 파라미터 $PP = (g, y_1, y_2, H_{i,k}, \Psi)$ 를 생성한다(S215).
- [0050] 이후, 상기 키생성서버(120)가 앞서 생성한 상기 공개 파라미터 $PP = (g, y_1, y_2, H_{i,k}, \Psi)$ 를 상기 콘텐츠 제공서버(140)로 전송한다(S216).

[0051] 이어서, 상기 키생성서버(120)는 앞서 생성한 상기 제1 원소 z_1 , 제2 원소 z_2 , 제3 원소 u_1 , 제4 원소 u_2 를 포함하는 마스터 비밀키 $MK = (z_1, z_2, u_1, u_2)$ 를 생성하고, 생성한 상기 마스터 비밀키 $MK = (z_1, z_2, u_1, u_2)$ 를 상기 콘텐츠 제공서버(140)로 전송한다.

[0052] 이후, 키생성서버(120)가 복수 개의 사용자단말이 콘텐츠에 대한 접근 가능 여부를 나타내는 접근권리 비밀키 생성단계에 대하여 자세히 살펴보도록 한다.

[0053] 도 4는 키생성서버가 접근권리 비밀키를 생성하는 단계의 세부과정을 나타낸 순서도이다.

[0054] 도 4에 도시된 바와 같이, 상기 키생성서버(120)가 콘텐츠에 접근하고자 하는 사용자단말(160)로부터 상기 콘텐츠에 대한 복수 개의 접근구조를 나타내는 접근구조 AS 의 집합 $S(AS)$ 을 획득한다(S221).

[0055] 이후, 상기 키생성서버(120)가 제1 접선형 그룹 Z_p 에 속하는 임의의 제5 원소 r_j 와, 제6 원소 t_j 를 선택하여 생성한다(S222).

[0056] 이어서, 상기 키생성서버(120)가 상기 접근구조 AS 에 속하는 인덱스값 j 을 이용하여 상기 제5 원소 r_j 와 제1 원소 z_1 를 곱한값 $r_j z_1$ 과, 상기 제6 원소 t_j 와 제2 원소 z_2 를 곱한값 $t_j z_2$ 을 합산하여 제3 변수 R 를 생성한다(S223).

[0057] 이러한, 상기 키생성서버(120)가 앞서 연산한 상기 제3 변수 R 및 공개 파라미터 $PP = (g, y_1, y_2, H_{i,k}, \Psi)$ 를 하기의 수학식 1에 대입하여 상기 콘텐츠에 대한 사용자단말의 접근 가능 여부를 나타내는 접근권리 비밀키 d_{AS} 를 생성한다(S224).

[0058] [수학식 1]

$$d_{AS} = \left(u_1 \prod_{i \in J(AS)} (g_i \prod_{k \in w(iKP)} h_{i,k}^{P_{i,k}})^{r_i}, u_2 \prod_{i \in J(AS)} (g_i \prod_{k \in w(iKP)} h_{i,k}^{P_{i,k}})^{t_i}, g^R, h_{z,k}^{r_{i,k}}, h_{z,k}^{t_{i,k}} \right)$$

[0060] 이에 따라, 상기 키생성서버(120)가 상기 접근권리 비밀키 d_{AS} 를 콘텐츠에 접근하고자 하는 복수 개의 사용자단말(160)로 각각 전송한다(S225).

[0061] 이후, 콘텐츠 제공서버(140)가 상기 키생성서버(120)로부터 상기 공개 파라미터 $PP = (g, y_1, y_2, H_{i,k}, \Psi)$ 를 수신하고, 수신한 공개 파라미터 $PP = (g, y_1, y_2, H_{i,k}, \Psi)$ 에 기초하여 사용자단말(160)로 분배하고자 하는 콘텐츠를 암호화하여 콘텐츠 암호문 CT 을 생성한 후, 생성한 콘텐츠 암호문 CT 을 사용자단말(160)로 전송한다.

[0062] 즉, 콘텐츠의 속성 집합을 $S = iCP_{i \in J(S)}$ 이라 가정하고, 제1 접선형 그룹 Z_p 에 속하는 제7 원소 s

를 선택하여 생성한 후, 상기 제7 원소를 하기의 수학적 식 2에 적용하여 콘텐츠 암호문을 생성한다.

[수학적 식 2]

$$CT = \left(y_1^s, y_2^s, \left(g_i \prod_{k \in w(iCP)} h_{i,k}^{P_{i,k}} \right)^s_{i \in J(S)}, h_{i,k}^s_{i \in J(S), k \in w(iCP)}, \Psi^s M \right)$$

이에 따라, 콘텐츠에 접근하고자 하는 상기 사용자단말(160)이 상기 키생성서버(120)로부터 접근권리 비밀키 d_{AS} 를 수신하고, 수신한 접근권리 비밀키 d_{AS} 에 기초하여 상기 콘텐츠 제공서버(140)로부터 수신한 상기 콘텐츠 암호문을 복호화하여 콘텐츠에 접근한다.

즉, 사용자단말(160)이 콘텐츠의 접근구조 AS 에 대하여 속성집합 S 가 상기 콘텐츠의 속성들을 만족하는지 여부를 확인한다. 이후, 상기 사용자단말(160)은 상기 콘텐츠 제공서버(140)로부터 수신한 콘텐츠 암호문

$$CT = (A, B, C_{i,k \in J(S), k \in w(iCP)}, D)$$

이고, 상기 키생성서버(120)로부터 수신한 접근권리 비밀키가

$$d_{AS} = (d_1, d_2, d_3, \pi_{i,k}, \omega_{i,k})$$

라고 가정한다.

$$CT = (A, B, C_{i,k \in J(S), k \in w(iCP)}, D)$$

이어서, 상기 사용자단말(160)이 상기 콘텐츠 암호문을 확인

한 후, 상기 접근권리 비밀키 $d_{AS} = (d_1, d_2, d_3, \pi_{i,k}, \omega_{i,k})$ 내 와일드카드로 처리해야 하는 부분인

$$U_m = \overline{w}(mCP) / \overline{w}(mKP)$$

에 대하여, 제1 페어링 키

$$\tilde{d}_1 = d_1 \cdot \prod_{j \in U_1} \pi_{j,K}^{P_{i,k}}$$

및 제2 페어링 키

$$\tilde{d}_2 = d_2 \cdot \prod_{j \in U_2} \omega_{j,K}^{P_{i,k}}$$

을 연산한다. 이때, 상기 $P_{i,k}$ 는 콘텐츠의 속성값을 나타낸다.

또한, 콘텐츠 암호문에 사용된 속성 집합 내 와일드카드를 사용하지 않아도 되는 경우에는 상기 제1 페어링 키

$\tilde{d}_1$ 및 제2 페어링 키 $\tilde{d}_2$ 를 이용하는 대신에, 제1 복호화키 d_1 및 제2 복호화 키 d_2 를 이용하여 콘텐츠 암호문에 대한 페어링 연산을 수행할 수 있다.

이후, 상기 사용자단말(160)이 상기 접근권리 비밀키를 하기의 수학적 식 3에 적용하여 복호화된 콘텐츠 암호문

즉, 콘텐츠 M 를 획득하며, 상기 콘텐츠 M 에 접근할 수 있다.

[수학적 식 3]

$$M = D \cdot e(\tilde{d}_1, A) e(\tilde{d}_2, B) / e(d_3, \prod_{i \in J(S)} C_i)$$

이하에서는 IPTV와 같은 응용환경 내 사용자단말의 콘텐츠에 대한 다양한 접근구조에 대하여 자세히 설명하도록 한다.

예를 들어, 첫 번째, 'wildcard'를 사용하지 않는 경우에 대하여 살펴보도록 한다.

[0074]

먼저, 키 정책의 기본 패턴을 $1KP = (Nation, Title, Season)$ 와 같이 정의한다. 이에 따라, 밥 (Bob)이라는 사람이 자신의 사용자단말을 이용하여 '미국 드라마'인 '프렌즈' '시즌 2'를 시청하기 원하는 경우

$$1KP_{Bob} = (US \text{ and } Friends \text{ and } 2)$$

에, 상기 밥의 비밀키와 관련된 키 정책의 접근 구조는 와 같이 표현될 수 있다. 뿐만 아니라, 다른 사용자인 앨리스(Alice)는 상기 밥이 시청하고자 하는 미국 드라마인 프렌즈의 시즌 2중 에피소드 1편과, 2편만을 시청하고 싶다고 가정한다. 이때, 상기 앨리스의 키 정책의 접근

$$2KP = (Episode)$$

구조는 상기 밥의 키 정책 접근구조에 가 더 추가된다. 이에 따라, 상기 앨리스의 최

$$AS_{Alice} = (US \text{ and } Friends \text{ and } 2) \text{ or } (First \text{ and } Second)$$

중 키 정책 접근 구조는 와 같 이 표현될 수 있다. 이때, 상기 밥의 접근 권리 비밀키는

$$d_{AS_{Bob}} = \begin{pmatrix} u_1 \cdot (g_1 \cdot h_{1,1}^{US} \cdot h_{1,2}^{Friends} \cdot h_{1,3}^2)^{r_1}, \\ u_2 \cdot (g_1 \cdot h_{1,1}^{US} \cdot h_{1,2}^{Friends} \cdot h_{1,3}^2)^{t_1}, g^R \end{pmatrix}$$

이고, 상기 앨리스의 접근 권리 비밀키는

$$d_{AS_{Alice}} = \begin{pmatrix} u_1 \cdot (g_1 \cdot h_{1,1}^{US} \cdot h_{1,2}^{Friends} \cdot h_{1,3}^2)^{r'_1} \cdot (g_2 \cdot h_{2,1}^{First})^{r'_2}, \\ u_1 \cdot (g_1 \cdot h_{1,1}^{US} \cdot h_{1,2}^{Friends} \cdot h_{1,3}^2)^{r'_1} \cdot (g_2 \cdot h_{2,1}^{Second})^{r'_2}, \\ (u_2 \cdot (g_1 \cdot h_{1,1}^{US} \cdot h_{1,2}^{Friends} \cdot h_{1,3}^2)^{t_1} \cdot (g_2 \cdot h_{2,1}^{First})^{t_2}, \\ (u_2 \cdot (g_1 \cdot h_{1,1}^{US} \cdot h_{1,2}^{Friends} \cdot h_{1,3}^2)^{t_1} \cdot (g_2 \cdot h_{2,1}^{Second})^{t'_2}, g^R \end{pmatrix}$$

와 같이 표현될

수 있다.

[0075]

이때, 상기 드라마 콘텐츠에 대한 암호문이 하기의 수학식 4와 같다면, 상기 밥과 앨리스는 모두 자신의 접근권 리 비밀키로 콘텐츠 암호문을 복호화할 수 있다.

[0076]

[수학식 4]

$$CT = (y_1^s, y_2^s, (g_1 \cdot h_{1,1}^{US} \cdot h_{1,2}^{Friends} \cdot h_{1,3}^2)^s, (g_2 \cdot h_{2,1}^{First})^s, \Psi^s M)$$

[0077]

[0078]

또한, 상술한 바와 달리, 접근권리 비밀키에 'wildcard'를 사용하는 경우를 살펴해보도록 한다.

[0079]

먼저, 스포츠 채널로서, 키 정책의 기본 접근구조가 $3KP = (Chanel, Program, Season)$ 와

$$4KP = (Home, Visiting)$$

라고 가정한다. 이때, 캐롤(Carol)이 자신의 사용자단말을 이용하여 첼시 팀의 경기를 시청하고자 하는 경우에, 상기 캐롤의 키 접근구조는

$$3KP_{carol} = (ESPN, EPL, 12-13)$$

및

$$4KP_{carol,1} = (Chelsea, *), 4KP_{carol,2} = (*, Chelsea)$$

로 표현될 수 있다. 이때, 상기 캐

롤의 최종 키 접근구조는

$$AS_{carol} = (ESPN \text{ and } EPL \text{ and } 12-13) \text{ and } (Chelsea, *) \text{ or } (*, Chelsea)$$

가 된다. 이때, 상기 캐롤의 접근 권리 비밀키는

$$d_{AS_{card}} = (d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9)$$

$$= \begin{pmatrix} u_1 \cdot (g_3 \cdot h_{3,1}^{ESPN} \cdot h_{3,2}^{EPL} \cdot h_{3,3}^{12-13})^{r_3} \cdot (g_4 \cdot h_{4,1}^{Chelsea})^{r_4}, \\ u_1 \cdot (g_3 \cdot h_{3,1}^{ESPN} \cdot h_{3,2}^{EPL} \cdot h_{3,3}^{12-13})^{r_3} \cdot (g_4 \cdot h_{4,2}^{Chelsea})^{r_4}, \\ u_2 \cdot (g_3 \cdot h_{3,1}^{ESPN} \cdot h_{3,2}^{EPL} \cdot h_{3,3}^{12-13})^{t_3} \cdot (g_4 \cdot h_{4,1}^{Chelsea})^{t_4}, \\ u_2 \cdot (g_3 \cdot h_{3,1}^{ESPN} \cdot h_{3,2}^{EPL} \cdot h_{3,3}^{12-13})^{t_3} \cdot (g_4 \cdot h_{4,2}^{Chelsea})^{t_4}, \\ h_{4,2}^{r_4}, h_{4,1}^{r_4}, h_{4,2}^{t_4} \end{pmatrix}$$

와 같이 표현될 수

있다.

예를 들어, 첼시와 아스날간 경기가 첼시의 홈에서 열린다고 가정하고, 이때, 스포츠 콘텐츠에 대한 속성 집합은 $S = (ESPN, EPL, 12-13), (Chelsea, Arsenal)$ 이 된다. 이러한 스포츠 콘텐츠를 암호

$$CT = \begin{pmatrix} y_1^s, y_2^s, (g_3 \cdot h_{3,1}^{ESPN} \cdot h_{3,2}^{EPL} \cdot h_{3,3}^{12-13})^s, \\ (g_4 \cdot h_{4,1}^{Chelsea} \cdot h_{4,2}^{Arsenal})^s, \Psi^s M \end{pmatrix}$$

화하여 생성한 콘텐츠 암호문은

가 된다.

이때, 상기 캐롤이 자신의 사용자단말을 이용하여 접근권리 비밀키 $d_{AS_{card}}$ 중 d_5 와 d_7 을 이용하여 $h_{4,2}^{Arsenal \cdot r_4}$ 및 $h_{4,2}^{Arsenal \cdot t_4}$ 를 연산하고, 이에 각각 접근권리 비밀키 $d_{AS_{card}}$ 중 d_1 및 d_3 을 곱하여 상기 콘텐츠 암호문에 대한 복호화 연산을 수행한다.

마지막으로, 콘텐츠 암호문에 'wildcard'를 사용한 경우를 살펴보도록 한다.

먼저, 영화 채널로서, 키 정책의 기본 접근구조를 $5KP = (Title, Genre, Rating)$ 이라 정의한다. 영화 제작자인 데이브가 다음 주 영화 채널에 영화 '300'을 방영할 예정이고, 먼저 방영하고자 하는 영화 예고편을 해당 영화 채널을 통해 방영할 계획이라고 가정한다. 이때, 상기 영화채널을 통해 방영되는 영화 예고편은 연령대 제한을 제외한 나머지 사용자들이 자신의 사용자단말을 통해 키 정책의 접근구조와 상관없이 모두 시청할 수 있어야 한다. 예를 들어, 연령대 제한을 나타내는 속성은 R(restricted)와, NC-17(17세 이하 관람불가)이며, 이때의 속성 집합은 $S = (*, *, R), (*, *, NC-17)$ 와 같이 표현될 수 있다. 따라서, 영화 예고편

$$CT = \begin{pmatrix} y_1^s, y_2^s, (g_5 \cdot h_{5,3}^R)^s, (g_5 \cdot h_{5,3}^{NC-17})^s, \\ h_{5,1}^s, h_{5,2}^s, \Psi^s M \end{pmatrix}$$

콘텐츠의 콘텐츠 암호문은

로 나타낼 수 있다.

이에 따라, 등급 제한에 해당하지 않는 사용자는 자신의 사용자단말을 통해 상기 콘텐츠 암호문을 접근권리 비밀키에 기초하여 복호화하여 해당 콘텐츠를 획득할 수 있다.

또한, 이러한 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 콘텐츠의 접근 가능 여부를 나타내는 접근권리 비밀키를 콘텐츠와 함께 암호화하여 사용자단말이 콘텐츠에 대한 접근 가능 여부 및 콘텐츠 수

신을 보다 효율적으로 수신할 수 있는 효과가 있다.

[0086] 또한, 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 콘텐츠 암호문의 복호화 시, 사용자단말이 페어링 연산을 0 또는 1 번만 수행하기 때문에 콘텐츠 암호문의 복호화 시간이 감소하는 효과가 있다.

[0087] 더불어, 본 발명의 사용자단말의 콘텐츠 접근 제어에 따른 콘텐츠 분배 방법 및 시스템은 콘텐츠에 접근하고자 하는 사용자단말로 콘텐츠의 접근구조에 대한 AND, OR, threshold, wildcard 등의 기능을 제공함으로써, 콘텐츠에 대하여 다양한 접근 제어를 수행할 수 있는 효과가 있다.

[0088] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

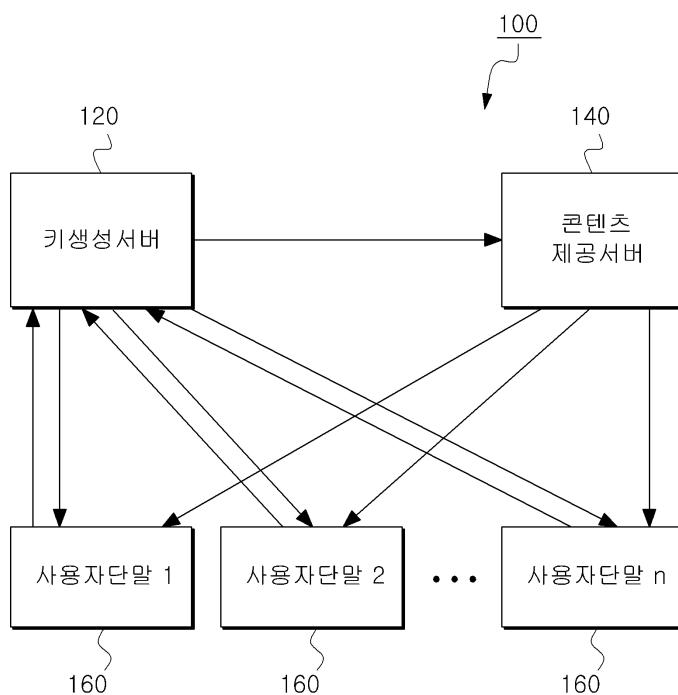
부호의 설명

[0089] 120: 키 생성 서버 140: 콘텐츠 제공 서버

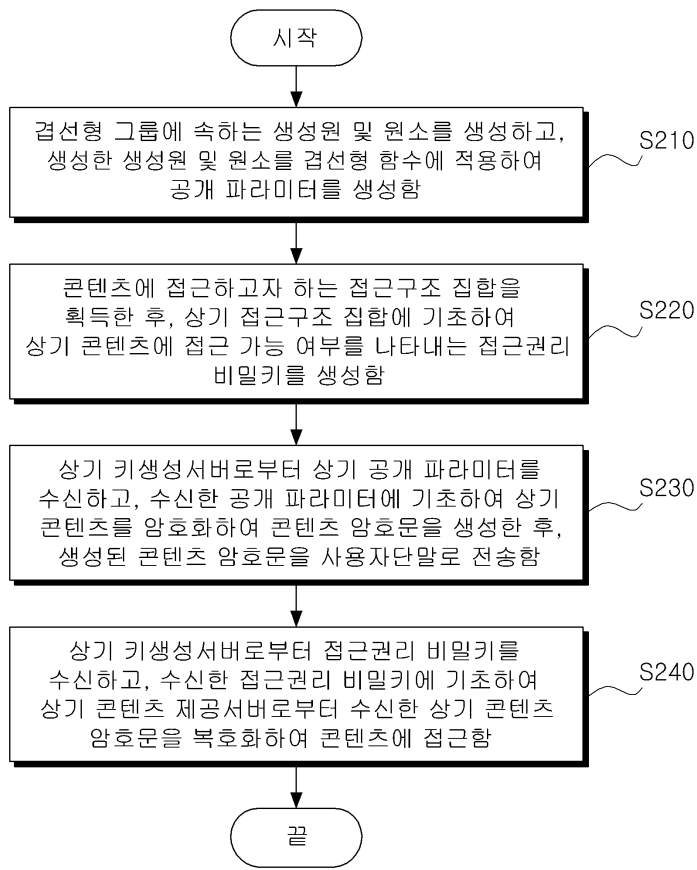
160: 사용자단말

도면

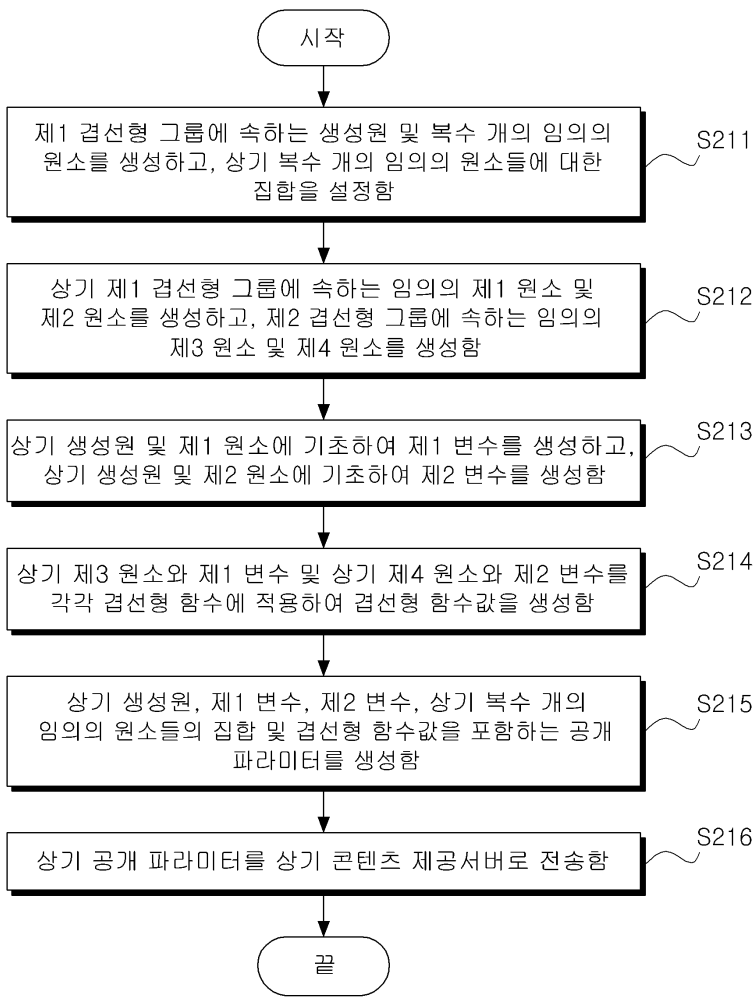
도면1



도면2



도면3



도면4

