(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0072011
(43) 공개일자 2012년07월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/24 (2006.01) *G06F 21/20* (2006.01)
(21) 출원번호 10-2010-0133773
(22) 출원일자 2010년12월23일
심사청구일자 없음
기술이전 희망 : 기술양도, 실시권허여, 기술지도

전체 청구항 수 : 총 12 항

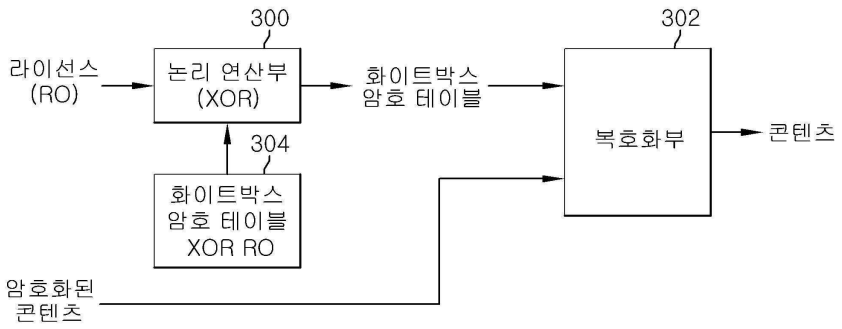
(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
이윤경
대전광역시 유성구 배울2로 19, 대덕테크노밸리 꿈에그린아파트 910동 1202호 (관평동)
김신효
대전광역시 유성구 엑스포로 448, 404동 1106호 (전민동, 엑스포아파트)
(뒷면에 계속)
(74) 대리인
김원준, 제일특허법인

(54) 발명의 명칭 **무결성 검증이 가능한 데이터 암호장치, 복호장치 및 방법**

(57) 요 약

본 발명에서는 무결성 검증이 가능한 데이터의 암호 및 복호에 있어서, 화이트박스 암호 테이블을 이용하여 사용자에 의해 구매된 콘텐츠를 암호화하고, 해당 화이트박스 암호 테이블에 대해서는 콘텐츠의 라이선스 정보를 통해 암호화하여 제공한 후, 라이선스 정보를 통해 콘텐츠를 암호화한 화이트박스 암호 테이블을 복호함으로써 콘텐츠에 대한 암복호화 뿐만 아니라 데이터의 무결성도 검증할 수 있도록 한다. 또한, 본 발명에서는 모든 종류의 디지털 데이터의 무결성을 검증하면서 동시에 암호화된 데이터의 복호화도 가능한 방법을 제시하되, 디지털 데이터를 구매한 클라이언트가 화이트박스 암호 테이블 생성기를 가지고 있지 않아도 무결성 검증이 가능한 암호 및 복호 방법을 제시함으로써 화이트박스 암호의 안정성을 높이면서 많은 양의 데이터에 대한 무결성 검증이 가능하도록 한다.

대 표 도 - 도3



(72) 발명자

정병호

대전광역시 유성구 가정로 65, 102동 1305호 (신성동, 대림두레아파트)

이상우

대전광역시 유성구 배울2로 78, 대덕테크노밸리아파트 603동 804호 (관평동)

문혜란

경기도 광주시 경충대로 1514-11, 이스트빌 3동 402호 (쌍령동)

이석준

대전광역시 유성구 배울1로 119, 대덕테크노밸리 우림필유 1207동 1102호 (용산동)

배근태

대전광역시 서구 둔산대로117번길 66, 908호 (만년동, 골드타워)

황정연

경기도 수원시 권선구 세지로12번길 25-10, 대우연립 10동 201호 (세류동)

조현숙

대전광역시 유성구 관평1로 12, 702동 601호 (관평동)

이 발명을 지원한 국가연구개발사업

과제고유번호	KI001917
부처명	지식경제부
연구사업명	정보통신산업원천기술개발사업
연구과제명	익명성 기반의 u-지식 정보보호 기술 개발
주관기관	한국전자통신연구원
연구기간	2010.03.01 ~ 2011.02.28

특허청구의 범위

청구항 1

화이트박스 암호를 이용한 암호 장치로서,

콘텐츠를 화이트박스 암호 테이블을 이용하여 암호화하는 암호화부와,

상기 화이트박스 암호 테이블을 상기 콘텐츠의 라이선스 정보와 논리 연산을 수행하여 암호화된 화이트박스 암호 테이블을 출력하는 논리 연산부

를 포함하는 무결성 검증이 가능한 암호장치.

청구항 2

제 1 항에 있어서,

상기 논리 연산부는,

상기 화이트박스 암호 테이블을 상기 콘텐츠에 대한 라이선스 정보와 배타적 논리합(exclusive OR) 연산하여 암호화된 화이트박스 암호 테이블을 출력하는 무결성 검증이 가능한 암호장치.

청구항 3

제 1 항에 있어서,

상기 콘텐츠는,

사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 무결성 검증이 가능한 암호장치.

청구항 4

화이트박스 암호를 이용한 복호 장치로서,

콘텐츠의 라이선스 정보와 논리 연산되어 암호화된 화이트박스 암호 테이블을 상기 라이선스 정보와 다시 상기 논리 연산 수행하여 원래의 화이트박스 암호 테이블을 복호하는 논리 연산부와,

상기 논리 연산부를 통해 복호된 화이트박스 암호 테이블을 이용하여 암호화되어 전송되는 상기 콘텐츠를 복호시키는 복호화부

를 포함하는 무결성 검증이 가능한 복호장치.

청구항 5

제 4 항에 있어서,

상기 논리 연산부는,

상기 콘텐츠의 라이선스 정보와 배타적 논리합 연산된 암호화된 화이트박스 암호 테이블을 상기 라이선스 정보와 다시 배타적 논리합 연산하여 원래의 화이트박스 암호 테이블을 복호하는 무결성 검증이 가능한 복호장치.

청구항 6

제 4 항에 있어서,

상기 콘텐츠는,

사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 무결성 검증이 가능한 복호장치.

청구항 7

화이트박스 암호를 이용한 암호 방법으로서,

콘텐츠를 화이트박스 암호 테이블을 이용하여 암호화하는 단계와,

상기 화이트박스 암호 테이블을 상기 콘텐츠에 대한 라이선스 정보와 논리 연산을 수행하여 암호화된 화이트박스 암호 테이블을 출력하는 단계와,

상기 암호화된 콘텐츠를 상기 암호화된 화이트박스 암호 테이블과 함께 전송하는 단계

를 포함하는 무결성 검증이 가능한 암호화 방법.

청구항 8

제 7 항에 있어서,

상기 화이트박스 암호 테이블은,

상기 라이선스 정보와 배타적 논리합 연산이 수행되는 무결성 검증이 가능한 암호화 방법.

청구항 9

제 7 항에 있어서,

상기 콘텐츠는,

사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 무결성 검증이 가능한 암호화 방법.

청구항 10

화이트박스 암호를 이용한 복호화 방법으로서,

암호화된 콘텐츠와 화이트박스 암호 테이블을 수신하는 단계와,

상기 암호화된 화이트박스 암호 테이블을 상기 콘텐츠의 라이선스 정보와 기설정된 논리 연산을 수행하여 복호화하는 단계와,

상기 복호된 화이트박스 암호 테이블을 이용하여 암호화되어 전송되는 상기 콘텐츠를 복호시키는 단계

를 포함하는 무결성 검증이 가능한 복호화 방법.

청구항 11

제 10 항에 있어서,

상기 암호화된 화이트박스 암호 테이블은,

상기 라이선스 정보 혹은 라이선스 정보의 해쉬값과 배타적 논리합 연산이 수행되는 무결성 검증이 가능한 복호화 방법.

청구항 12

제 10 항에 있어서,

상기 콘텐츠는,

사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 무결성 검증이 가능한 복호화 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 데이터 암호(encoding) 및 복호(decoding)에 관한 것으로, 특히 데이터의 암호 및 복호에 있어서 화이트박스 암호 테이블(white box cipher table)을 이용하여 사용자에 의해 구매된 콘텐츠(contents)를 암호화하고, 해당 화이트박스 암호 테이블에 대해서는 콘텐츠의 라이선스(license) 정보를 통해 암호화하여 제공한 후, 라이선스 정보를 통해 콘텐츠를 암호화한 화이트박스 암호 테이블을 복호함으로써 콘텐츠에 대한 암복호화 뿐만 아니라 데이터의 무결성(integrity)도 검증할 수 있도록 하는 화이트박스 암호를 이용한 무결성 검증이 가능한 데이터 암호장치, 복호장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 통상적으로, 현재 사용중인 대부분의 암호 및 복호 알고리즘 및 이들의 구현에 있어서는 데이터의 암호 또는 복호 용도로만 사용 가능하며, 복호된 데이터의 무결성을 검증하기 위해서는 별도의 데이터 무결성 검증용 알고리즘을 이용하여야 하였다.

[0003] 즉, 데이터의 무결성 검증을 위한 무결성 검증용 알고리즘 또한 데이터의 암호 또는 복호의 동작과는 무관하게 데이터의 무결성을 검증하는 용도로만 사용되고 있다.

[0004] 한편, MEDUSA 라는 방법으로 알려진 논문의 내용에 따르면, 화이트 박스 암호 테이블들 중 타입(type)2 테이블의 일부 데이터와 소프트웨어(software) 실행 바이너리 파일(binary file)을 결합하여 소프트웨어 실행 프로그램의 무결성 검증이 가능하다.

발명의 내용

해결하려는 과제

[0005] 그러나, MEDUSA에서는 소프트웨어 실행 프로그램을 가지고 있어야 하므로 화이트박스 암호의 안전성이 무너질 가능성이 크다는 문제가 있고, 무결성 검증이 가능한 소프트웨어 프로그램의 양에도 제한이 있다는 문제점이 있었다.

[0006] 따라서, 본 발명은 데이터의 암호 및 복호에 있어서 화이트박스 암호 테이블을 이용하여 사용자에 의해 구매된 콘텐츠를 암호화하고, 해당 화이트박스 암호 테이블에 대해서는 콘텐츠의 라이선스 정보를 통해 암호화하여 제공한 후, 라이선스 정보를 통해 콘텐츠를 암호화한 화이트박스 암호 테이블을 복호함으로써 콘텐츠에 대한 암복호화 뿐만 아니라 데이터의 무결성도 검증할 수 있도록 하는 화이트박스 암호를 이용한 무결성 검증이 가능한 데이터 암호장치, 복호장치 및 방법을 제공하고자 한다.

과제의 해결 수단

[0007] 상술한 본 발명은 화이트박스 암호를 이용한 암호 장치로서, 콘텐츠를 화이트박스 암호 테이블을 이용하여 암호화하는 암호화부와, 상기 화이트박스 암호 테이블을 상기 콘텐츠의 라이선스 정보와 논리 연산을 수행하여

암호화된 화이트박스 암호 테이블을 출력하는 논리 연산부를 포함한다.

[0008] 또한, 상기 논리 연산부는, 상기 화이트박스 암호 테이블을 상기 콘텐츠에 대한 라이선스 정보와 배타적 논리합(exclusive OR) 연산하여 암호화된 화이트박스 암호 테이블을 출력하는 것을 특징으로 한다.

[0009] 또한, 상기 콘텐츠는, 사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 것을 특징으로 한다.

[0010] 또한, 본 발명은 화이트박스 암호를 이용한 복호 장치로서, 콘텐츠의 라이선스 정보와 논리 연산되어 암호화된 화이트박스 암호 테이블을 상기 라이선스 정보와 다시 상기 논리 연산 수행하여 원래의 화이트박스 암호 테이블을 복호하는 논리 연산부와, 상기 논리 연산부를 통해 복호된 화이트박스 암호 테이블을 이용하여 암호화되어 전송되는 상기 콘텐츠를 복호시키는 복호화부를 포함한다.

[0011] 또한, 상기 논리 연산부는, 상기 콘텐츠의 라이선스 정보와 배타적 논리합 연산된 암호화된 화이트박스 암호 테이블을 상기 라이선스 정보와 다시 배타적 논리합 연산하여 원래의 화이트박스 암호 테이블을 복호하는 것을 특징으로 한다.

[0012] 또한, 상기 콘텐츠는, 사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 것을 특징으로 한다.

[0013] 또한, 본 발명은 화이트박스 암호를 이용한 암호 방법으로서, 콘텐츠를 화이트박스 암호 테이블을 이용하여 암호화하는 단계와, 상기 화이트박스 암호 테이블을 상기 콘텐츠에 대한 라이선스 정보와 논리 연산을 수행하여 암호화된 화이트박스 암호 테이블을 출력하는 단계와, 상기 암호화된 콘텐츠를 상기 암호화된 화이트박스 암호 테이블과 함께 전송하는 단계를 포함한다.

[0014] 또한, 상기 화이트박스 암호 테이블은, 상기 라이선스 정보와 배타적 논리합 연산이 수행되는 것을 특징으로 한다.

[0015] 또한, 상기 콘텐츠는, 사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 것을 특징으로 한다.

[0016] 또한, 본 발명은 화이트박스 암호를 이용한 복호화 방법으로서, 암호화된 콘텐츠와 화이트박스 암호 테이블을 수신하는 단계와, 상기 암호화된 화이트박스 암호 테이블을 상기 콘텐츠의 라이선스 정보와 기설정된 논리 연산을 수행하여 복호화하는 단계와, 상기 복호된 화이트박스 암호 테이블을 이용하여 암호화되어 전송되는 상기 콘텐츠를 복호시키는 단계를 포함한다.

[0017] 또한, 상기 암호화된 화이트박스 암호 테이블은, 상기 라이선스 정보와 혹은 라이선스 정보의 해쉬값과 배타적 논리합 연산이 수행되는 것을 특징으로 한다.

[0018] 또한, 상기 콘텐츠는, 사용자에 의해 온라인 또는 오프라인에서 구매된 멀티미디어 콘텐츠 또는 도서 콘텐츠인 것을 특징으로 한다.

발명의 효과

[0019] 본 발명에서는 무결성 검증이 가능한 데이터의 암호 및 복호에 있어서, 화이트박스 암호 테이블을 이용하여 사용자에 의해 구매된 콘텐츠를 암호화하고, 해당 화이트박스 암호 테이블에 대해서는 콘텐츠의 라이선스 정보를 통해 암호화하여 제공한 후, 라이선스 정보를 통해 콘텐츠를 암호화한 화이트박스 암호 테이블을 복호함으로써 콘텐츠에 대한 암복호화 뿐만 아니라 데이터의 무결성도 검증할 수 있는 이점이 있다.

[0020] 또한, 본 발명에서는 모든 종류의 디지털 데이터의 무결성을 검증하면서 동시에 암호화된 데이터의 복호화도 가능한 방법을 제시하되, 디지털 데이터를 구매한 클라이언트가 화이트박스 암호 테이블 생성기를 가지고 있지 않아도 무결성 검증이 가능한 암호 및 복호 방법을 제시함으로써 화이트박스 암호의 안정성을 높이면서 많은 양의 데이터에 대한 무결성 검증이 가능하도록 하는 이점이 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 실시 예에 따른 화이트박스 암호를 이용한 무결성 검증 및 암복호화 개념도,

도 2는 본 발명의 실시 예에 따른 화이트박스 암호를 이용한 암호장치의 블록 구성도,

도 3은 본 발명의 실시 예에 따른 화이트박스 암호를 이용한 복호장치의 블록 구성도,

도 4는 본 발명의 실시 예에 따른 화이트박스 암호를 이용한 무결성 검증 및 암복호화 개념도,

도 5는 본 발명의 실시 예에 따른 화이트박스 암호 테이블 구조 예시도.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0023] 본 발명의 실시 예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이며, 후술되는 용어들은 본 발명의 실시 예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0024] 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들(실행 엔진)에 의해 수행될 수도 있으며, 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다.

[0025] 그리고, 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명되는 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0026] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능들을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있으며, 몇 가지 대체 실시 예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하며, 또한 그 블록들 또는 단계들이 필요에 따라 해당하는 기능의 역순으로 수행되는 것도 가능하다.

[0027] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예에 대하여 상세하게 설명한다.

[0028] 도 1은 본 발명의 실시 예에 따른 화이트박스 암호 테이블을 이용한 암호 및 복호화의 개념을 도시한 것이다.

[0029] 도 1을 참조하면, 서버(server)에서 화이트박스 암호 테이블 A의 각 값들에 무결성을 검증하고자 하는 데이터를 배타적 논리합(exclusive OR: XOR) 연산한 화이트박스 암호 테이블 B를 클라이언트(client)에 전송한다.

[0030] 그러면, 클라이언트는 전송받은 화이트박스 암호 테이블 B에 무결성을 검증할 데이터를 배타적 논리합(XOR) 연산하게 되는데, 이때 데이터가 수정되지 않았다면 화이트박스 암호 테이블 A를 얻을 수 있고, 데이터가 수정되었다면 화이트박스 암호 테이블 A가 아닌 화이트박스 암호 테이블 A'를 얻게 된다.

[0031] 따라서, 클라이언트가 무결성을 검증 받아야할 데이터를 수정하였다면 화이트박스 암호 테이블 A를 복구할 수 없으므로 화이트박스 암호 테이블을 이용한 암호화 과정 및 복호화 과정을 제대로 수행할 수 없게 된다.

[0032] 위와 같이, 본 발명에서는 화이트박스 암호 테이블을 이용하여, 콘텐츠의 암호화 및 복호화를 수행하는 과정에서 데이터의 무결성 검증도 함께 수행할 수 있게 된다.

[0033] 도 2는 본 발명의 실시 예에 따른 화이트박스 암호를 이용한 데이터 암호장치의 구성을 도시한 것이다.

[0034] 도 2를 참조하면, 서버내 구현되는 암호장치는 암호화부(200)와 화이트박스 암호 테이블을 이용하여 디지털 데이터(digital data)등의 콘텐츠를 암호화 하고, 콘텐츠의 라이선스 등의 데이터와 논리 연산부(202)를 이용하여 콘텐츠 암호화에 사용된 화이트박스를 암호화 한다.

[0035] 이때, 콘텐츠는 암호화부(200)를 통해 화이트박스 암호 테이블로 암호화가 수행되며, 화이트박스 테이블은 라이선스(right object : RO) 혹은 라이선스의 해쉬값과 함께 논리 연산부(202)를 통과함으로써(예를들어 배타적 논리합(XOR) 등의 연산을 수행) 암호화 된다.

[0036] 이와 같이, 화이트박스 암호 테이블을 이용하여 암호화된 콘텐츠와 라이선스(라이선스의 경우 콘텐츠가 화이트박스 암호 테이블을 이용하여 암호화 되었기 때문에 별도의 콘텐츠 복호화 키를 담고 있을 필요가 없으므로 라이선스는 암호화 되지 않아도 된다.)는 통신망을 통해 클라이언트 단말로 전송될 수 있다.

[0037] 도 3은 본 발명의 실시 예에 따른 화이트박스 암호를 이용한 데이터 복호장치의 구성을 도시한 것이다.

[0038] 도 3을 참조하면, 클라이언트에 구현되는 복호장치는 복호화부(302)와 논리 연산부(300) 등을 포함하여 암호화된 콘텐츠와 암호화된 화이트박스 등의 데이터를 복호화한다.

[0039] 먼저 사용자가 온라인상의 서버 등에서 구매한 콘텐츠에 대해 서버로부터 화이트박스 암호 테이블로 암호화된 콘텐츠와 라이선스, 그리고 라이선스와 배타적 논리합 수행된(암호화된) 화이트박스 암호 테이블 XOR RO(304)가 수신된다.

[0040] 이때, 라이선스(RO)는 클라이언트 단말내 구현되는 복호장치의 논리 연산부(300)로 입력되며, 논리 연산부(300)에서는 라이선스와 배타적 논리합 수행된 화이트박스 암호 테이블 XOR RO(304)와 라이선스(RO)를 예를들어 배타적 논리합(XOR) 등의 연산을 수행하여 암호화가 수행되기 전의 화이트박스를 복호한다.

[0041] 이와 같이, 복호된 화이트박스는 복호화부(302)로 입력되며, 복호화부(302)에서는 논리 연산부(300)로부터 복호된 화이트박스와 암호화된 콘텐츠를 복호화부에 입력하여 복호화된 콘텐츠를 얻는다.

[0042] 도 4는 본 발명의 실시 예에 따른 도 2 및 도 3의 데이터 암호 및 복호 과정의 동작 개념을 도시한 것이다.

[0043] 이하, 도 4를 참조하여 화이트박스 암호를 이용한 데이터 암호 및 복호 과정의 동작을 다시 한번 살펴보기로 한다.

[0044] 즉, 사용자가 구매한 콘텐츠의 화이트박스는 화이트박스 암호 테이블의 각 값들에 라이선스(RO)를 배타적 논리합(XOR) 연산 수행함으로써 암호화 되고, 사용자가 구매한 콘텐츠는 라이선스(RO)가 배타적 논리합 연산되기 전의 화이트박스 암호 테이블을 이용하여 암호화된다.

[0045] 위와 같이, 암호화된 화이트박스와 암호화된 콘텐츠(E(contents)), 그리고 라이선스(RO)는 클라이언트로 전송된다.

[0046] 암호화된 콘텐츠와 화이트박스 암호 테이블, 그리고 라이선스(RO)를 수신한 클라이언트 단말에서는, 라이선스(RO)를 통해 화이트박스 암호 테이블을 복호화하는데, 이 과정은 라이선스(RO)를 암호화된 화이트박스 암호 테이블에 배타적 논리합 연산을 수행하여 원래의 화이트박스 암호 테이블을 복구하는 과정을 의미한다.

[0047] 그리고, 암호화된 콘텐츠를 복구된 화이트박스 암호 테이블에 통과시킴으로써 콘텐츠를 복호화하여 이용할 수 있게 된다. 이때, 사용자가 라이선스(RO)를 수정하게 되면 화이트박스 암호 테이블을 제대로 복구할 수 없기 때문에 콘텐츠를 제대로 복호할 수 없게 되어 콘텐츠 이용이 불가능하게 된다.

[0048] 즉, 본 발명에서는 DRM 에이전트(agent) 등에서 하나의 프로세서 내에서 라이선스 등의 데이터에 대한 배타적 논리합 연산과 복호화 연산이 이루어질 때 데이터에 대한 무결성 검증 및 복호화 연산을 동시에 수행할 수 있게 된다.

[0049] 이때, 라이선스 등의 데이터에 대해 배타적 논리합 연산을 수행하는 등의 데이터에 대한 무결성 검증 과정은 도 5에서와 같이 화이트박스 암호 연산의 일부에 포함될 수 있다.

[0050] 상기한 바와 같이, 본 발명에서는 무결성 검증이 가능한 데이터의 암호 및 복호에 있어서, 화이트박스 암호 테이블을 이용하여 사용자에 의해 구매된 콘텐츠를 암호화하고, 해당 화이트박스 암호 테이블에 대해서는 콘

텐츠의 라이선스 정보를 통해 암호화하여 제공한 후, 라이선스 정보를 통해 콘텐츠를 암호화한 화이트박스 암호 테이블을 복호함으로써 콘텐츠에 대한 암복호화 뿐만 아니라 데이터의 무결성도 검증할 수 있도록 한다.

[0051] 또한, 본 발명에서는 모든 종류의 디지털 데이터의 무결성을 검증하면서 동시에 암호화된 데이터의 복호화도 가능한 방법을 제시하되, 디지털 데이터를 구매한 클라이언트가 화이트박스 암호 테이블 생성기를 가지고 있지 않아도 무결성 검증이 가능한 암호 및 복호 방법을 제시함으로써 화이트박스 암호의 안정성을 높이면서 많은 양의 데이터에 대한 무결성 검증이 가능하도록 한다.

[0052] 한편 상술한 본 발명의 설명에서는 구체적인 실시 예에 관해 설명하였으나, 여러 가지 변형이 본 발명의 범위에서 벗어나지 않고 실시될 수 있다. 따라서 발명의 범위는 설명된 실시 예에 의하여 정할 것이 아니고 특허청구범위에 의해 정하여져야 한다.

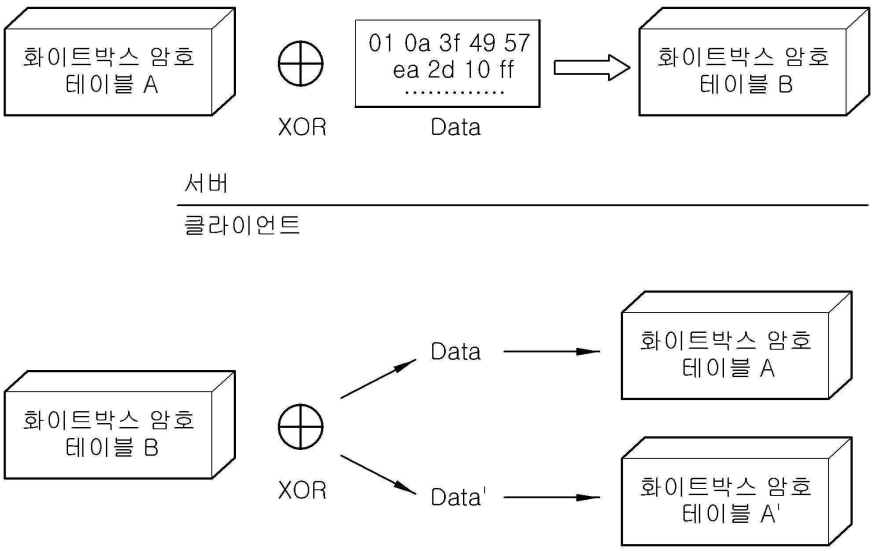
부호의 설명

[0053] 200 : 암호화부 202 : 논리 연산부

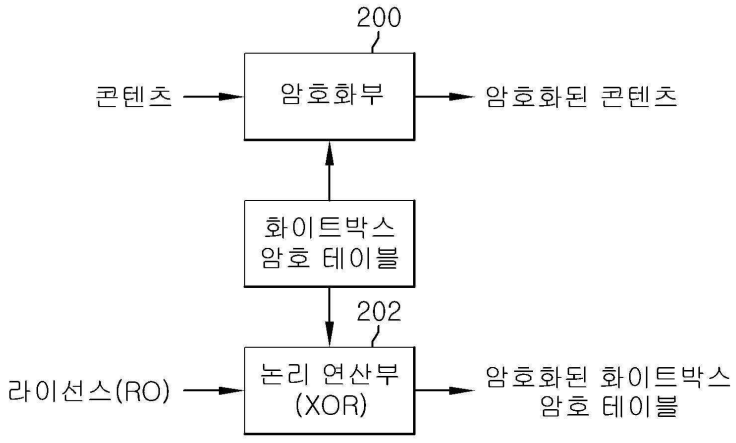
300 : 논리 연산부 302 : 복호화부

도면

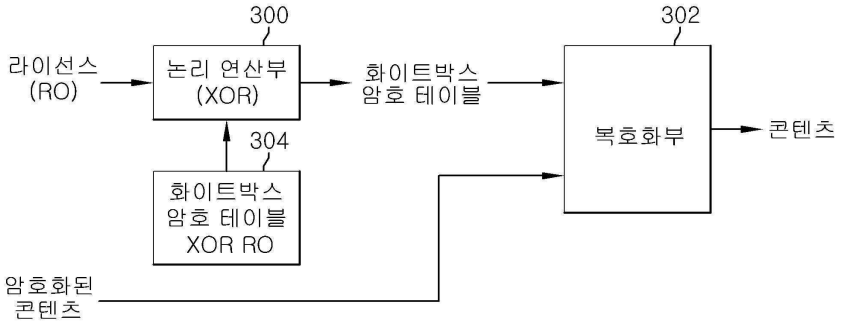
도면1



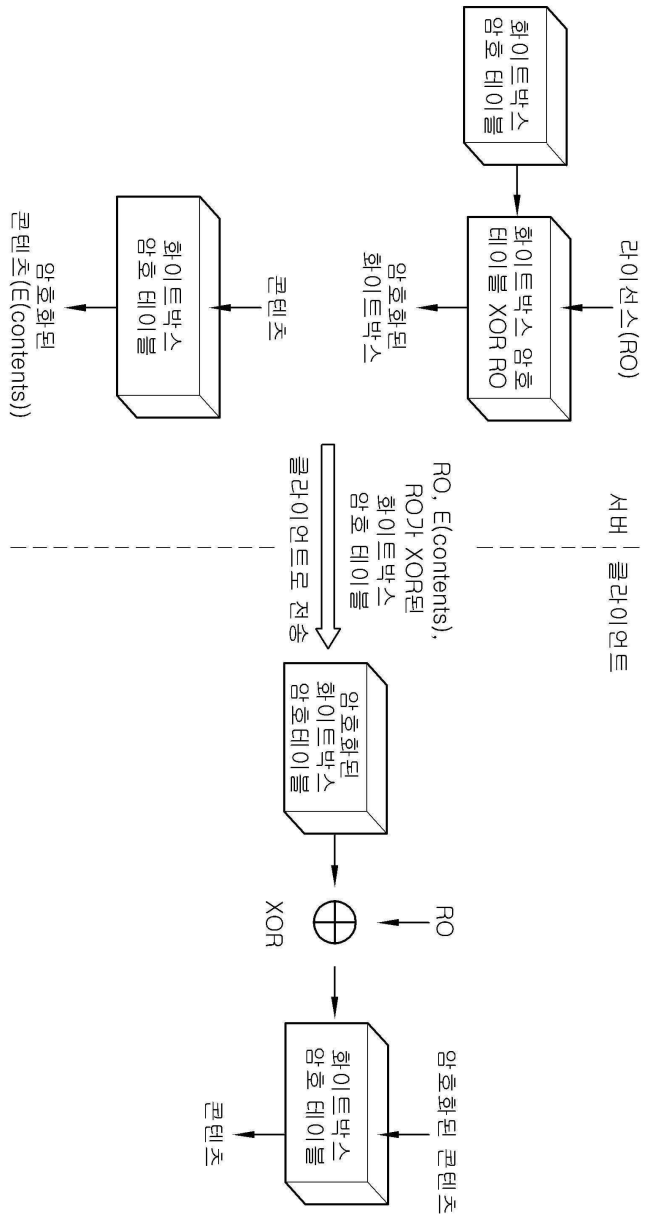
도면2



도면3


300
302
라이선스
(RO)
논리 연산부
(XOR)
화이트박스
암호 테이블
복호화부
콘텐츠
304
화이트박스
암호 테이블
XOR RO
암호화된
콘텐츠

도면4


화이트박스
암호 테이블
화이트박스 암호
테이블 XOR RO
라이선스(RO)
암호화된
화이트박스
화이트박스
암호 테이블
콘텐츠
암호화된
콘텐츠(E(contents))
서버
클라이언트
RO, E(contents),
RO가 XOR된
화이트박스
암호 테이블
클라이언트로 전송
암호화된
화이트박스
암호테이블
XOR
RO
화이트박스
암호 테이블
콘텐츠
암호화된 콘텐츠

도면5