



(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl. H04L 9/28 (2006.01)	(45) 공고일자 (11) 등록번호 (24) 등록일자	2007년05월10일 10-0717005 2007년05월04일
--	-------------------------------------	--

(21) 출원번호	10-2005-0055124	(65) 공개번호	10-2006-0106551
(22) 출원일자	2005년06월24일	(43) 공개일자	2006년10월12일
심사청구일자	2005년06월24일		

(30) 우선권주장 60/668,607 2005년04월06일 미국(US)

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 한성휴
서울 송파구 문정2동 웨미리1단지아파트 102동 1006호

김명선
경기 의왕시 삼동 대우아파트 105동 104호

윤영선
경기 수원시 권선구 권선동 상록아파트 511동 704호

이선남
경기 수원시 영통구 매탄동 1254-7

김봉선
경기 성남시 분당구 금곡동 청솔마을주공9단지아파트 903동 411호

이재흥
경기 수원시 영통구 매탄3동 1250-8 206호

(74) 대리인 리앤목특허법인
이해영

(56) 선행기술조사문헌	
KR1020030085125 A	KR1020050013583 A
US20030142826 A1	WO2004064313 A1

심사관 : 이준석

전체 청구항 수 : 총 17 항

(54) 폐기 키를 결정하는 방법 및 장치와 이것을 이용하여복호화하는 방법 및 장치

(57) 요약

본 발명은 디지털 콘텐츠를 보호하는 분야에 관한 것으로, 본 발명에 따른 폐기 키 결정 방법은 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 적어도 하나 이상의 그룹을 식별하고, 이 그룹에 속하는 노드들 각각의 폐기 여부를 검출함으로써 종래 HBES에서 많은 비트 수를 요구했던 그룹 아이디를 제거할 수 있다.

대표도

도 4

특허청구의 범위

청구항 1.

- (a) 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 단계;
- (b) 상기 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 단계; 및
- (c) 상기 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 단계를 포함하는 것을 특징으로 하는 폐기 키 결정 방법.

청구항 2.

제 1 항에 있어서,

상기 (a) 단계는 다수의 계층들 중 어느 하나의 계층에 해당하는 그룹에 속하는 노드의 위치에 기초하여 상기 계층의 다음 하위 계층에 해당하는 그룹을 식별하는 것을 특징으로 하는 폐기 키 결정 방법.

청구항 3.

제 1 항에 있어서,

상기 (b) 단계는 상기 식별된 그룹의 후손 그룹들에 대한 정보의 종결 여부를 검출하고,

상기 (c) 단계는 상기 (b) 단계에서 상기 후손 그룹들에 대한 정보가 종결된 것으로 검출되면, 상기 후손 그룹들에 속하는 모든 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 한번에 결정하는 것을 특징으로 하는 폐기 키 결정 방법.

청구항 4.

제 3 항에 있어서,

상기 (b) 단계는 상기 식별된 그룹이 리프 그룹인 경우, 상기 식별된 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기된 경우, 또는 상기 식별된 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기되지 않은 경우에 상기 후손 그룹에 대한 정보가 종결된 것으로 검출하는 것을 특징으로 하는 폐기 키 결정 방법.

청구항 5.

제 1 항에 있어서,

상기 (b) 단계는 상기 노드들 중 적어도 하나 이상의 폐기되지 않은 노드의 구간에 관한 정보로부터 상기 노드들 각각의 폐기 여부를 검출하는 것을 특징으로 폐기 키 결정 방법.

청구항 6.

제 1 항에 있어서,

상기 그룹은 하나의 시드 값 및 이 시드 값과 다른 시드 값들 각각이 서로 다른 횟수로 해시된 값들로 구성된 키 세트가 할당된 노드들의 그룹임을 특징으로 하는 폐기 키 결정 방법.

청구항 7.

컨텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 식별부;

상기 식별부에 의해 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 검출부; 및

상기 검출부에 의해 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 결정부를 포함하는 것을 특징으로 하는 폐기 키 결정 장치.

청구항 8.

제 7 항에 있어서,

상기 식별부는 다수의 계층들 중 어느 하나의 계층에 해당하는 그룹에 속하는 노드의 위치에 기초하여 상기 계층의 다음 하위 계층에 해당하는 그룹을 식별하는 것을 특징으로 하는 폐기 키 결정 장치.

청구항 9.

제 7 항에 있어서,

상기 검출부는 상기 식별된 그룹의 후손 그룹들에 대한 정보의 종결 여부를 검출하고,

상기 결정부는 상기 검출부에 의해 상기 후손 그룹들에 대한 정보가 종결된 것으로 검출되면, 상기 후손 그룹들에 속하는 모든 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 한번에 결정하는 것을 특징으로 하는 폐기 키 결정 장치.

청구항 10.

제 1 항 내지 제 6 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 11.

- (a) 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 단계;
- (b) 상기 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 단계;
- (c) 상기 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 단계; 및
- (d) 상기 폐기되지 않은 것으로 결정된 키 세트를 사용하여 암호화된 콘텐츠를 복호화하는 단계를 포함하는 것을 특징으로 하는 복호화 방법.

청구항 12.

제 11 항에 있어서,

상기 (d) 단계는

상기 폐기되지 않은 것으로 결정된 키 세트를 사용하여 암호화된 콘텐츠 키를 복호화하는 단계; 및

상기 복호화된 콘텐츠 키를 사용하여 상기 암호화된 콘텐츠를 복호화하는 단계를 포함하는 것을 특징으로 하는 복호화 방법.

청구항 13.

콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 식별부;

상기 식별부에 의해 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 검출부;

상기 검출부에 의해 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 결정부; 및

상기 결정부에 의해 폐기되지 않은 것으로 결정된 키 세트를 사용하여 암호화된 콘텐츠를 복호화하는 복호화부를 포함하는 것을 특징으로 하는 복호화 장치.

청구항 14.

제 13 항에 있어서,

상기 복호화부는

상기 결정부에 의해 폐기되지 않은 것으로 결정된 키 세트를 사용하여 암호화된 콘텐츠 키를 복호화하는 제 1 복호화부; 및

상기 제 1 복호화부에 의해 복호화된 콘텐츠 키를 사용하여 상기 암호화된 콘텐츠를 복호화하는 제 2 복호화부를 포함하는 것을 특징으로 하는 복호화 장치.

청구항 15.

제 11 항 내지 제 12 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 16.

컨텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들 중 어느 하나 그룹의 후손 그룹들에 대한 정보의 종결 여부를 나타내는 제 1 필드; 및

상기 그룹에 속하는 노드들 각각의 폐기 여부를 나타내는 제 2 필드를 포함하는 것을 특징으로 하는 데이터 구조를 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 17.

제 16 항에 있어서,

상기 제 1 필드는 상기 그룹이 리프 그룹인 경우, 상기 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기된 경우, 또는 상기 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기되지 않은 경우에 상기 후손 그룹에 대한 정보가 종결되었음을 나타내는 것을 특징으로 하는 데이터 구조를 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 디지털 컨텐츠를 보호하는 분야에 관한 것으로, 특히 디지털 컨텐츠를 브로드캐스트 암호화 방식(broadcast encryption scheme)에 따라 효율적으로 복호화하는 장치 및 방법에 관한 것이다.

최근 들어, 인터넷, 지상파, 케이블, 위성 등의 다양한 통신 매체들을 이용한 디지털 컨텐츠의 전송이 급증하고 있고, CD (Compact Disk), DVD(Digital Versatile Disk) 등의 대용량 기록 매체들을 이용한 디지털 컨텐츠의 판매 및 대여가 급증하고 있다. 이에 따라, 디지털 컨텐츠의 저작권을 보호하기 위한 솔루션인 DRM(Digital Rights Management)이 중요한 이슈로 떠오르고 있다. DRM에 관련된 기술들 중, 특히 CD, DVD 등의 기록 매체, 인터넷 등을 이용하여 브로드캐스트되는 디지털 컨텐츠를 암호화함으로써 광범위하게 배포되는 디지털 컨텐츠를 보호하는 브로드캐스트 암호화 방식에 대한 연구가 활발히 진행되고 있다.

일반적으로, 브로드캐스트 암호화 방식은 컨텐츠 키(content key)를 사용하여 컨텐츠를 암호화하고, 디바이스, 사용자, 또는 사용자 그룹 등의 폐기를 관리하기 위한 폐기 키(revocation key)를 사용하여 컨텐츠 암호화에 사용된 컨텐츠 키를 암호화하는 2 단계의 암호화 과정들로 구성된다. 또한, 종래 브로드캐스트 암호화 방식에 따라 암호화된 컨텐츠를 복호화하기 위해서는 폐기 키를 사용하여 암호화된 컨텐츠 키를 복호화하고, 그 결과로써 획득된 컨텐츠 키를 사용하여 암호화된 컨텐츠를 복호화하는 2 단계의 복호화 과정들을 거쳐야 한다.

상기된 폐기 키는 브로드캐스트 암호화 방식이 적용되는 디바이스, 사용자, 또는 사용자 그룹 등에 할당된다. 브로드캐스트 암호화 방식을 따르는 디바이스들 중 폐기 키 노출 등으로 인해 더 이상 브로드캐스트 암호화 방식에 따른 보호가 불가능한 디바이스는 폐기된다. 폐기된 디바이스는 자신이 보유한 폐기 키를 사용하여 브로드캐스트 암호화 방식을 따르는 컨텐츠를 복호화할 수 없다.

다만, 브로드캐스트 암호화 방식은 브로드캐스트 암호화 방식이 적용되는 디바이스, 사용자, 또는 사용자 그룹 등의 개수가 증가하면, 이들 각각에 할당되어야 하는 폐기 키들의 개수가 기하급수적으로 증가한다는 문제점이 있었다. HBES (Hierarchical Hash-Chain Broadcast Encryption Scheme)는 이러한 문제점을 해결하기 위한 변형된 브로드캐스트 암호화 방식이다.

도 1은 일반적인 HBES 키 트리를 도시한 도면이다.

도 1을 참조하면, 일반적인 HBES 키 트리는 L 계층 N 진 트리(L-Layers N-ary tree)이며, 폐기 키의 일종인 HBES 노드 키 세트들이 할당된 노드들의 그룹들이 계층적으로 배열된 구조로 되어 있다. 또한, HBES 키 트리 내의 그룹들에 속하는 노드들 각각이 디바이스, 사용자, 또는 사용자 그룹 등에 대응하며, HBES 노드 키 세트가 할당된다.

특히, HBES 노드 키 세트는 하나의 시드 값 및 이 시드 값과 다른 시드 값들 각각이 서로 다른 횟수로 해시된 값들로 구성된다. 보다 상세하게 설명하면, HBES 키 트리 내의 그룹들 중 어느 하나의 그룹에 속하는 노드들 각각에 첫 번째 시드 값과 이 시드 값이 연쇄적으로 해시된 값들이 할당되고, 다음으로 두 번째 시드 값과 이 시드 값이 연쇄적으로 해시된 값들이 한 노드만큼 천이되어 할당되며, 이 과정은 마지막 시드 값과 이 시드 값이 연쇄적으로 해시된 값들이 할당될 때까지 반복된다.

이와 같이, HBES는 일반 브로드캐스트 암호화 방식에서의 폐기 키를 사용한 암호화 과정들 대부분이 HBES 노드 키 세트의 해시 값들을 사용한 해시 과정들로 대체된다. 이와 같은 특징들로 인하여 HBES는 일반 브로드캐스트 암호화 방식에 비해 훨씬 더 계산이 간단하고, 전송 데이터 량, 및 저장 데이터 량이 적다.

도 2는 일반적인 HBES 키 트리의 일례를 도시한 도면이다.

도 2를 참조하면, 도 2에 도시된 HBES 키 트리는 3 계층 4 진 트리이다. 특히, HBES 키 트리 내의 그룹들에 속하는 노드들 중 X 표시가 된 부분이 폐기된 HBES 노드 키 세트임을 나타낸다.

특히, 종래의 HBES에 따르면, 이와 같은 HBES 노드 키 세트의 폐기 여부에 관한 정보는 폐기된 HBES 노드 키 세트가 할당된 노드, 즉 폐기된 노드가 속하는 그룹의 아이디, 그룹에 속하는 노드들 중 폐기되지 않은 노드가 연속되는 구간의 시작 위치 및 길이로 구성된다. 도 2에 도시된 HBES 키 트리에 대해 이러한 정보를 표현해 보면, 다음과 같다.

그룹 아이디 = 0, 구간의 시작 위치 및 길이 = [1, 2]

그룹 아이디 = 1, 구간의 시작 위치 및 길이 = [3, 3]

그룹 아이디 = 4, 구간의 시작 위치 및 길이 = [2, 3]

그룹 아이디 = 7, 구간의 시작 위치 및 길이 = [3, 3]

그룹 아이디 = 18, 구간의 시작 위치 및 길이 = [0, 3]

실제 구간의 시작 위치 및 길이는 1 ~ 4에 해당하나, 2비트로 표현할 경우 0 ~ 3이 가능하기 때문에 상기된 구간의 시작 위치 및 길이는 0 ~ 3은 1 ~ 4를 의미한다.

상기된 바와 같이, 3 계층 4 진 형태의 HBES 키 트리에서 그룹 아이디를 표현하기 위해서는 5 비트가 필요하다. 그런데, 종래 HBES에 따르면, L 값과 N 값이 증가하면, 그룹 아이디를 표현하기 위한 비트 수가 매우 크게 증가한다는 문제점이 있었다. 예를 들어, 16 계층 16 진 형태의 HBES 키 트리에서 그룹 아이디를 표현하기 위해서는 61 비트가 필요하다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 종래 HBES에서 많은 비트 수를 요구했던 그룹 아이디를 제거함으로써, 이에 따라 HBES 노드 키의 폐기 여부에 관한 정보가 기록된 태그의 크기를 줄일 수 있는 장치, 방법, 및 데이터 구조를 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공하는데 있다. 또한, 상기된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공하는데 있다.

발명의 구성

상기 기술적 과제를 해결하기 위한 본 발명에 따른 폐기 키 결정 방법은 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 단계; 상기 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 단계; 및 상기 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 단계를 포함한다.

상기 다른 기술적 과제를 해결하기 위한 본 발명에 따른 폐기 키 결정 장치는 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 식별부; 상기 식별부에 의해 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 검출부; 및 상기 검출부에 의해 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 결정부를 포함한다.

상기 또 다른 기술적 과제를 해결하기 위하여, 본 발명은 상기된 폐기 키 결정 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 복호화 방법은 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 단계; 상기 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 단계; 상기 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 단계; 및 상기 폐기되지 않은 것으로 결정된 키 세트를 사용하여 암호화된 콘텐츠를 복호화하는 단계를 포함한다.

상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 복호화 장치는 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들이 트리 형태로 계층적으로 배열된 구조에 기초하여 상기 그룹들 중 적어도 하나 이상의 그룹을 식별하는 식별부; 상기 식별부에 의해 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출하는 검출부; 상기 검출부에 의해 검출된 결과에 따라 상기 노드들 각각에 할당된 키 세트들 각각의 폐기 여부를 결정하는 결정부; 및 상기 결정부에 의해 폐기되지 않은 것으로 결정된 키 세트를 사용하여 암호화된 콘텐츠를 복호화하는 복호화부를 포함한다.

상기 또 다른 기술적 과제를 해결하기 위하여, 본 발명은 상기된 복호화 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 데이터 구조를 기록한 컴퓨터로 읽을 수 있는 기록매체는 콘텐츠 보호를 위한 키 세트들이 할당된 노드들의 그룹들 중 어느 하나 그룹의 후손 그룹들에 대한 정보의 종결 여부를 나타내는 제 1 필드; 및 상기 그룹에 속하는 노드들 각각의 폐기 여부를 나타내는 제 2 필드를 포함한다.

이하에서는 도면을 참조하여 본 발명의 바람직한 실시예들을 상세히 설명한다.

본 발명의 바람직한 실시예들에 적용되는 HBES 키 트리는 폐기 키의 일종인 HBES 노드 키 세트들이 할당된 노드들의 그룹들이 L 계층 N 진 트리 형태로 계층적으로 배열된 구조로 되어 있다. 또한, HBES 키 트리 내의 그룹들에 속하는 노드들 각각이 디바이스, 사용자, 또는 사용자 그룹 등에 대응하며, HBES 노드 키 세트가 할당된다.

특히, HBES 노드 키 세트는 하나의 시드 값 및 이 시드 값과 다른 시드 값들 각각이 서로 다른 횟수로 해시된 값들로 구성된다. 보다 상세하게 설명하면, HBES 키 트리 내의 그룹들 중 어느 하나의 그룹에 속하는 노드들 각각에 첫 번째 시드 값과 이 시드 값이 연쇄적으로 해시된 값들이 할당되고, 다음으로 두 번째 시드 값과 이 시드 값이 연쇄적으로 해시된 값들이 한 노드만큼 천이되어 할당되며, 이 과정은 마지막 시드 값과 이 시드 값이 연쇄적으로 해시된 값들이 할당될 때까지 반복된다.

도 3은 본 발명의 바람직한 일 실시예에 따른 패킷의 포맷을 도시한 도면이다.

도 3을 참조하면, 본 실시예에 따른 패킷은 헤더(header)(31), 페이로드(payload)(32), 및 태그(tag)(33)로 구성된다.

헤더(31)는 패킷의 순서를 나타내는 순서 번호가 기록된 필드, 콘텐츠의 암호화에 사용된 콘텐츠 키들의 개수가 기록된 필드, 및 HBES 노드 키 세트에 의해 암호화된 콘텐츠 키들이 기록된 필드로 구성된다. HBES 노드 키 세트는 HBES 키 트리 내의 그룹들에 속하는 각각의 노드에 할당된 HBES 노드 키 세트이다.

페이로드(32)는 콘텐츠 키들에 의해 암호화된 콘텐츠가 기록된 콘텐츠 필드로 구성된다.

태그(33)는 보류 필드(331), 종결 플래그 필드(332), 구간 개수 필드(333), 구간 시작 필드(334), 및 구간 길이 필드(335)로 구성된다.

보류 필드(331)는 일반적으로 컴퓨터, 임베디드 시스템 등이 최소 4 비트 이상의 단위로 데이터를 처리함으로 인하여 발생된 필드로서 어떠한 값도 기록되어 있지 않다. 즉, 보류 필드(331)는 종결 플래그 필드(332)의 길이가 1 비트이기 때문에 발생한 잉여 3 비트에 해당하는 필드이다.

종결 플래그 필드(332)에는 HBES 키 트리 내의 어느 하나 그룹의 후손 그룹들에 대한 정보의 종결 여부를 나타내는 값이 기록된다. 보다 상세하게 설명하면, HBES 키 트리 내의 어느 하나 그룹이 리프 그룹인 경우, HBES 키 트리 내의 어느 하나 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기된 경우, 또는 HBES 키 트리 내의 어느 하나 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기되지 않은 경우에 종결 플래그 필드(332)에 HBES 키 트리 내의 어느 하나 그룹의 후손 그룹에 대한 정보가 종결되었음을 나타내는 값이 기록된다.

구간 개수 필드(333), 구간 시작 필드(334), 및 구간 길이 필드(335)는 HBES 키 트리 내의 어느 하나 그룹에 속하는 노드들 각각의 폐기 여부를 나타내기 위한 필드들이다. 구간 개수 필드(333), 구간 시작 필드(334), 및 구간 길이 필드(335) 각각의 역할에 대한 구체적인 설명은 다음과 같다.

구간 개수 필드(333)에는 HBES 키 트리 내의 어느 하나의 그룹에 속하는 노드들 중 폐기되지 않은 노드가 연속되는 구간의 개수가 기록된다.

구간 시작 필드(334)에는 HBES 키 트리 내의 어느 하나의 그룹에 속하는 노드들 중 폐기되지 않은 노드가 연속되는 구간의 시작 위치가 기록된다.

구간 길이 필드(335)에는 HBES 키 트리 내의 어느 하나의 그룹에 속하는 노드들 중 폐기되지 않은 노드가 연속되는 구간의 길이가 기록된다.

구간 개수 필드(333)에 기록된 구간의 개수만큼의 구간 시작 필드(334)와 구간 길이 필드(335)가 존재한다. 예를 들어, 구간 개수 필드(333)에 기록된 구간의 개수가 2이라면, 2개의 구간 시작 필드들과 구간 길이 필드들이 연속하여 존재한다. 다만, 구간 개수 필드(333)에 기록된 구간의 개수가 0이라면, 구간 시작 필드와 구간 길이 필드는 존재하지 않는다.

도 4는 본 발명의 바람직한 일 실시예에 따른 폐기 키 결정 장치의 구성도이다.

도 4를 참조하면, 본 실시예에 따른 폐기 키 결정 장치는 패킷 해석부(41), 그룹 식별부(42), 폐기 노드 검출부(43), 및 폐기 키 결정부(44)로 구성된다.

패킷 해석부(41)는 도 3에 도시된 패킷을 해석하고, 그 결과에 따라 패킷의 구성을 인지한다. 보다 상세하게 설명하면, 패킷 해석부(41)는 도 3에 도시된 패킷을 해석하고, 그 결과에 따라 패킷이 헤더(31), 페이로드(32), 및 태그(33)로 구성되어 있음을 인지한다. 이어서, 패킷 해석부(41)는 태그(33)를 해석하고, 그 결과에 따라 태그(33)가 보류 필드(331), 종결 플래그 필드(332), 구간 개수 필드(333), 구간 시작 필드(334), 및 구간 길이 필드(335)로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 HBES 키 트리 구조, 즉 HBES 노드 키 세트들이 할당된 노드들의 그룹들이 L 계층 N 진 트리 형태로 계층적으로 배열된 구조에 기초하여 HBES 키 트리 내의 그룹들 중 적어도 하나 이상의 그룹을 식별한다.

보다 상세하게 설명하면, 그룹 식별부(42)는 L 계층들 중 어느 하나의 계층에 해당하는 그룹에 속하는 노드의 위치에 기초하여 이 계층의 다음 하위 계층에 해당하는 그룹을 식별한다. 즉, 그룹 식별부(42)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 첫 번째 그룹을 HBES 키 트리 내의 그룹들 중 제 1 계층에 해당하는 그룹으로 식별한다. 이어서, 그룹 식별부(42)는 제 1 계층에 해당하는 그룹에 속하는 노드들의 위치에 기초하여 제 1 계층의 다음 하위 계층인 제 2 계층에 해당하는 그룹들을 식별한다. 예를 들어, 그룹 식별부(42)는 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드의 후손 그룹을 제 1 계층의 다음 하위 계층인 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹으로 식별한다.

폐기 노드 검출부(43)는 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 중 적어도 하나 이상의 폐기되지 않은 노드의 구간에 관한 정보로부터 이 노드들 각각의 폐기 여부를 검출한다. 즉, 폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 태그(33)의 필드들 중, 구간 개수 필드(333), 구간 시작 필드(334), 및 구간 길이 필드(335)에 기록된 값들을 참조하여 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 각각의 폐기 여부를 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 태그(33)의 필드들 중 종결 플래그 필드(332)에 기록된 값을 참조하여 그룹 식별부(42)에 의해 식별된 그룹의 후손 그룹들에 대한 정보의 종결 여부를 검출한다. 보다 상세하게 설명하면, 폐기 노드 검출부(43)는 종결 플래그 필드(332)에 기록된 값이 그룹 식별부(42)에 의해 식별된 그룹의 후손 그룹에 대한 정보가 종결되었음을 나타내면, 즉 그룹 식별부(42)에 의해 식별된 그룹이 리프 그룹인 경우, 그룹 식별부(42)에 의해 식별된 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기된 경우, 또는 그룹 식별부(42)에 의해 식별된 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기되지 않은 경우에 그룹 식별부(42)에 의해 그룹의 후손 그룹에 대한 정보가 종결되었음을 검출한다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 각각의 폐기 여부를 결정한다. 즉, 폐기 키 결정부(44)는 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 중, 폐기 노드 검출부(43)에 의해 폐기된 것으로 검출된 노드에 할당된 HBES 노드 키 세트를 폐기된 것으로 결정한다.

또한, 폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해, 그룹 식별부(42)에 의해 식별된 그룹의 후손 그룹들에 대한 정보가 종결된 것으로 검출되면, 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 각각의 폐기 여부에 따라 이 후손 그룹들에 속하는 모든 노드들 각각에 할당된 HBES 노드 키 세트들 각각의 폐기 여부를 한번에 결정한다. 즉, 폐기 키 결정부(44)는 그룹 식별부(42)에 의해 식별된 그룹이 리프 그룹인 경우, 그룹 식별부(42)에 의해 식별된 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기된 경우, 또는 그룹 식별부(42)에 의해 식별된 그룹의 후손 그룹들에 속하는 모든 노드들이 폐기되지 않은 경우에 이 후손 그룹들에 속하는 모든 노드들 각각에 할당된 HBES 노드 키 세트들 각각의 폐기 여부를 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 각각의 폐기 여부에 따라 한번에 결정한다.

도 5는 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 일례를 도시한 도면이다.

도 5를 참조하면, 본 실시예에 적용되는 HBES 키 트리는 16 계층 16 진 트리이며, 이하에서도 동일하다. 특히, 도 5에 도시된 HBES 키 트리는 HBES 키 트리 내의 그룹들에 속하는 모든 노드들에 할당된 HBES 노드 키 세트들이 폐기되지 않은 상태이다.

도 3에 도시된 태그(33)로 상기된 HBES 키 트리 상태를 표시하면, 다음과 같다. 제 1 계층에 해당하는 그룹에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 1, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 0, 및 구간 길이 필드(335) = 15로 구성된다.

실제 구간의 시작 위치 및 길이는 1 ~ 16에 해당하나, 4 비트로 표현할 경우 0 ~ 15가 가능하기 때문에 상기된 구간의 시작 위치 및 길이는 0 ~ 15는 1 ~ 16을 의미하며, 이하 동일하다.

패킷 해석부(41)는 제 1 계층에 해당하는 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 1, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 0, 및 구간 길이 필드(335) = 15로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 첫 번째 그룹을 HBES 키 트리 내의 그룹들 중 제 1 계층에 해당하는 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 0, 및 구간 길이 필드(335) = 15를 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 모두가 폐기되지 않았음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 1을 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹의 후손 그룹들에 대한 정보가 종결되었음을 검출한다. 특히, 이 경우는 그룹 식별부(42)에 의해 식별된 그룹의 모든 후손 그룹들에 속하는 노드들이 폐기되지 않은 경우이다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 모두가 폐기되지 않은 것으로 결정한다.

또한, 폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 제 1 계층에 해당하는 그룹의 후손 그룹들에 대한 정보가 종결된 것으로 검출되면, 폐기 노드 검출부(43)에 의해 제 1 계층에 해당하는 그룹에 속하는 노드들 모두가 폐기되지 않은 것으로 검출된 것에 따라 이 후손 그룹들에 속하는 모든 노드들 각각에 할당된 HBES 노드 키 세트들 각각이 폐기되지 않은 것으로 한 번에 결정한다.

도 6은 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 다른 예를 도시한 도면이다.

도 6을 참조하면, 도 6에 도시된 HBES 키 트리는 HBES 키 트리의 각 계층의 그룹들 중 가장 왼쪽 그룹, 특히 이 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트만이 폐기된 상태이고, 나머지는 폐기되지 않은 상태이다.

도 3에 도시된 태그(33)로 상기된 HBES 키 트리 상태를 표시하면, 다음과 같다. 제 1 계층에 해당하는 그룹에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성된다. 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성된다. 이후, 제 3 계층부터 제 15 계층까지에 해당하는 그룹들 중 가장 왼쪽 그룹에 대한 태그(33)들도 상기된 경우와 동일하다. 제 16 계층에 해당하는 그룹들 중 가장 왼쪽 그룹에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 1, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성된다.

패킷 해석부(41)는 제 1 계층에 해당하는 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 제 1 계층에 해당하는 그룹에 대한 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 첫 번째 그룹을 HBES 키 트리 내의 그룹들 중 제 1 계층에 해당하는 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14를 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드가 폐기되었음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 0을 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹의 후손 그룹들에 대한 정보가 종결되지 않았음을 검출한다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트가 폐기된 것으로 결정한다.

다음으로, 패킷 해석부(41)는 제 2 계층에 해당하는 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 제 2 계층에 해당하는 그룹에 대한 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 두 번째 그룹의 선조 노드, 즉 폐기 노드 검출부(43)에 의해 폐기된 것으로 검출된 노드가 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드임을 참조하여 이 두 번째 그룹을 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14를 참조하여 그룹 식별부(42)에 의해 식별된 제 2 계층에 해당하는 가장 왼쪽 그룹에 속하는 노드들 중 가장 왼쪽 노드가 폐기되었음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 0을 참조하여 그룹 식별부(42)에 의해 식별된 제 2 계층에 해당하는 그룹의 후손 그룹들에 대한 정보가 종결되지 않았음을 검출한다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 2 계층에 해당하는 가장 왼쪽 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트가 폐기된 것으로 결정한다.

이후, 제 3 계층부터 제 15 계층까지에 해당하는 그룹들에 대한 태그(33)들에 대해서도 패킷 해석부(41), 그룹 식별부(42), 폐기 노드 검출부(43), 및 폐기 키 결정부(44)에 의해 각 계층에 해당하는 그룹들 중 가장 왼쪽 그룹, 특히 이 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트가 폐기된 것으로 결정된다.

다음으로, 패킷 해석부(41)는 제 16 계층에 해당하는 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 제 2 계층에 해당하는 그룹에 대한 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 1, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 두 번째 그룹의 선조 노드, 즉 폐기 노드 검출부(43)에 의해 폐기된 것으로 검출된 노드가 제 15 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드임을 참조하여 이 두 번째 그룹을 제 16 계층에 해당하는 그룹들 중 가장 왼쪽 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14를 참조하여 그룹 식별부(42)에 의해 식별된 제 16 계층에 해당하는 그룹들 중 가장 왼쪽 그룹, 특히 이 그룹에 속하는 노드들 중 가장 왼쪽 노드가 폐기되었음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 1을 참조하여 그룹 식별부(42)에 의해 식별된 제 16 계층에 해당하는 그룹들 중 가장 왼쪽 그룹의 모든 후손 그룹들에 대한 정보가 종결되었음을 검출한다. 특히, 이 경우는 그룹 식별부(42)에 의해 식별된 제 16 계층에 해당하는 그룹들 중 가장 왼쪽 그룹이 리프 그룹인 경우이다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 16 계층에 해당하는 그룹들 중 가장 왼쪽 그룹, 특히 이 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트가 폐기된 것으로 결정한다.

도 7은 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 또 다른 예를 도시한 도면이다.

도 7을 참조하면, 도 7에 도시된 HBES 키 트리는 HBES 키 트리의 제 16 계층의 각 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트가 균일하게 폐기된 상태이고, 나머지는 폐기되지 않은 상태이다.

도 3에 도시된 태그(33)로 상기된 HBES 키 트리 상태를 표시하면, 다음과 같다. 제 1 계층에 해당하는 그룹에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 및 구간 개수 필드(333) = 0으로 구성된다. 제 2 계층에 해당하는 그룹들 모두에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 및 구간 개수 필드(333) = 0으로 구성된다. 이후, 제 3 계층부터 제 15 계층까지에 해당하는 그룹에 대한 태그(33)들은 그 각각의 상황에 따라 기술될 수 있다.

패킷 해석부(41)는 제 1 계층에 해당하는 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 제 1 계층에 해당하는 그룹에 대한 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 및 구간 개수 필드(333) = 0으로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 첫 번째 그룹을 HBES 키 트리 내의 그룹들 중 제 1 계층에 해당하는 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 0을 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 모두가 폐기되었음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 0을 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹의 후손 그룹들에 대한 정보가 종결되지 않았음을 검출한다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 모두에 할당된 HBES 노드 키 세트들이 폐기된 것으로 결정한다.

다음으로, 패킷 해석부(41)는 제 2 계층에 해당하는 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 제 2 계층에 해당하는 그룹에 대한 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 두 번째 그룹의 선조 노드, 즉 폐기 노드 검출부(43)에 의해 폐기된 것으로 검출된 노드가 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드임을 참조하여 이 두 번째 그룹을 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 0을 참조하여 그룹 식별부(42)에 의해 식별된 제 2 계층에 해당하는 가장 왼쪽 그룹에 속하는 노드들 모두가 폐기되었음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 0을 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹의 후손 그룹들에 대한 정보가 종결되지 않았음을 검출한다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 모두에 할당된 HBES 노드 키 세트들이 폐기된 것으로 결정한다.

이후, 상기된 그룹 이외의 다른 그룹들에 대한 태그(33)들에 대해서도 패킷 해석부(41), 그룹 식별부(42), 폐기 노드 검출부(43), 및 폐기 키 결정부(44)에 의해 그 각각의 상황에 따라 그 그룹들에 속하는 노드들에 할당된 HBES 노드 키 세트의 폐기 여부가 결정된다.

도 8은 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 다른 예를 도시한 도면이다.

도 8을 참조하면, 도 8에 도시된 HBES 키 트리는 HBES 키 트리의 제 2 계층의 그룹들 중 가장 왼쪽 그룹, 특히 이 그룹에 속하는 노드들 중 가장 왼쪽 노드의 모든 후손 그룹들에 속하는 노드들에 할당된 HBES 노드 키 세트가 폐기된 상태이고, 나머지는 폐기되지 않은 상태이다.

도 3에 도시된 태그(33)로 상기된 HBES 키 트리 상태를 표시하면, 다음과 같다. 제 1 계층에 해당하는 그룹에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성된다. 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹에 대한 태그(33)는 보류 필드(331) = 0, 종결 플래그 필드(332) = 1, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성된다.

패킷 해석부(41)는 제 1 계층에 해당하는 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 제 1 계층에 해당하는 그룹에 대한 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 첫 번째 그룹을 HBES 키 트리 내의 그룹들 중 제 1 계층에 해당하는 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14를 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드가 폐기되었음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 0을 참조하여 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹의 후손 그룹들에 대한 정보가 종결되지 않았음을 검출한다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트가 폐기된 것으로 결정한다.

다음으로, 패킷 해석부(41)는 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹에 대한 태그(33)를 해석하고, 그 결과에 따라 제 2 계층에 해당하는 그룹에 대한 태그(33)가 보류 필드(331) = 0, 종결 플래그 필드(332) = 0, 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14로 구성되어 있음을 인지한다.

그룹 식별부(42)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 두 번째 그룹의 선조 노드, 즉 폐기 노드 검출부(43)에 의해 폐기된 것으로 검출된 노드가 제 1 계층에 해당하는 그룹에 속하는 노드들 중 가장 왼쪽 노드임을 참조하여 이 두 번째 그룹을 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹으로 식별한다.

폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 구간 개수 필드(333) = 1, 구간 시작 필드(334) = 1, 및 구간 길이 필드(335) = 14를 참조하여 그룹 식별부(42)에 의해 식별된 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹, 특히 이 그룹에 속하는 노드들 중 가장 왼쪽 노드가 폐기되었음을 검출한다.

또한, 폐기 노드 검출부(43)는 패킷 해석부(32)에서의 해석 결과에 따라 인지된 종결 플래그 필드(332) = 1을 참조하여 그룹 식별부(42)에 의해 식별된 제 2 계층에 해당하는 그룹의 모든 후손 그룹들에 대한 정보가 종결되었음을 검출한다. 특히, 이 경우는 그룹 식별부(42)에 의해 식별된 그룹의 모든 후손 그룹들에 속하는 노드들이 폐기된 경우이다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 제 2 계층에 해당하는 그룹들 중 가장 왼쪽 그룹, 특히 이 그룹에 속하는 노드들 중 가장 왼쪽 노드에 할당된 HBES 노드 키 세트가 폐기된 것으로 결정한다. 또한, 폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 제 2 계층에 해당하는 그룹들 중, 가장 왼쪽 그룹의 모든 후손 그룹들에 대한 정보가 종결된 것으로 검출되면, 폐기 노드 검출부(43)에 의해 제 2 계층에 해당하는 그룹에 속하는 노드들 모두가 폐기된 것으로 검출된 것에 따라 이 후손 그룹들에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 각각이 폐기된 것으로 한 번에 결정한다.

도 9는 종래 기술에 따른 태그의 크기와 본 발명의 바람직한 일 실시예에 따른 태그의 크기의 비교 표를 도시한 도면이다.

도 9를 참조하면, 상기된 도 5, 도 6, 도 7, 및 도 8의 경우 모두에 대해서 종래 기술에 따른 태그의 크기에 비해 본 실시예에 따른 태그의 크기가 매우 감소되었다는 것을 알 수 있다. 특히, 태그가 보다 많은 그룹들에 관한 정보를 포함할수록 그 크기는 훨씬 더 감소된다는 것을 알 수 있다.

도 10은 본 발명의 바람직한 일 실시예에 따른 복호화 장치의 구성도이다.

도 10을 참조하면, 본 실시예에 따른 복호화 장치(10)는 도 4에 도시된 폐기 키 결정 장치(4)를 이용한 하나의 응용례로서, 수신부(101), 패킷 해석부(41), 그룹 식별부(42), 폐기 노드 검출부(43), 폐기 키 결정부(44), 제 1 복호화부(102), 제 2 복호화부(103), 및 콘텐츠 출력부(104)로 구성된다. 따라서, 이하 생략된 내용이라 하더라도 도 4에 도시된 폐기 키 결정 장치(4)에 관하여 이상에서 기술된 내용은 본 실시예에 따른 복호화 장치(10)에도 적용된다.

수신부(101)는 콘텐츠 서버로부터 네트워크 등의 전송 매체를 경유하여 어느 하나의 패킷을 수신한다.

패킷 해석부(41)는 수신부(101)에 수신된 패킷을 해석하고, 그 결과에 따라 패킷의 구성을 인지한다.

그룹 식별부(42)는 패킷 해석부(41)에서의 해석 결과에 따라 인지된 HBES 키 트리 구조에 기초하여 HBES 키 트리 내의 그룹들 중 적어도 하나 이상의 그룹을 식별한다.

폐기 노드 검출부(43)는 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 중 적어도 하나 이상의 폐기되지 않은 노드의 구간에 관한 정보로부터 이 노드들 각각의 폐기 여부를 검출한다.

폐기 키 결정부(44)는 폐기 노드 검출부(43)에 의해 검출된 결과에 따라 그룹 식별부(42)에 의해 식별된 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 각각의 폐기 여부를 결정한다.

제 1 복호화부(102)는 폐기 키 결정부(44)에 의해 폐기되지 않은 것으로 결정된 HBES 노드 키 세트를 사용하여, 패킷 해석부(41)에서의 해석 결과에 따라 인지된 헤더(31)에 기록된 암호화된 콘텐츠 키를 복호화한다.

제 2 복호화부(103)는 제 1 복호화부(102)에 의해 복호화된 콘텐츠 키를 사용하여, 패킷 해석부(41)에서의 해석 결과에 따라 인지된 페이로드(32)에 기록된 암호화된 콘텐츠를 복호화한다.

컨텐츠 출력부(104)는 제 2 복호화부(103)에 의해 복호화된 컨텐츠를 사용자에게 출력한다. 컨텐츠 출력부(104)는 컨텐츠의 특성에 대응하는 방식으로 컨텐츠를 처리하여 사용자에게 출력한다. 예를 들어, 컨텐츠가 압축된 형태인 경우, 컨텐츠 출력부(104)는 컨텐츠의 압축을 풀고, 그 결과를 사용자에게 출력한다.

도 11은 본 발명의 바람직한 일 실시예에 따른 폐기 키 결정 방법의 흐름도이다.

도 11을 참조하면, 본 실시예에 따른 폐기 키 결정 방법은 다음과 같은 단계들로 구성된다. 본 실시예에 따른 폐기 키 결정 방법은 도 4에 도시된 폐기 키 결정 장치(4)에서 시계열적으로 처리되는 단계들로 구성된다. 따라서, 이하 생략된 내용이더라도 도 4에 도시된 폐기 키 결정 장치(4)에 관하여 이상에서 기술된 내용은 본 실시예에 따른 폐기 키 결정 방법에도 적용된다.

111 단계에서 폐기 키 결정 장치(4)는 도 3에 도시된 패킷을 해석하고, 그 결과에 따라 패킷의 구성을 인지한다.

112 단계에서 폐기 키 결정 장치(4)는 111 단계에서의 해석 결과에 따라 인지된 HBES 키 트리 구조에 기초하여 HBES 키 트리 내의 그룹들 중 적어도 하나 이상의 그룹을 식별한다. 보다 상세하게 설명하면, 112 단계에서 폐기 키 결정 장치(4)는 L 계층들 중 어느 하나의 계층에 해당하는 그룹에 속하는 노드의 위치에 기초하여 이 계층의 다음 하위 계층에 해당하는 그룹을 식별한다.

113 단계에서 폐기 키 결정 장치(4)는 112 단계에서 식별된 그룹에 속하는 노드들 중 적어도 하나 이상의 폐기되지 않은 노드의 구간에 관한 정보로부터 이 노드들 각각의 폐기 여부를 검출한다.

114 단계에서 폐기 키 결정 장치(4)는 112 단계에서 식별된 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 중, 113 단계에서 폐기된 것으로 검출된 노드에 할당된 HBES 노드 키 세트를 폐기된 것으로 결정한다.

115 단계에서 폐기 키 결정 장치(4)는 112 단계에서 식별된 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 중, 113 단계에서 폐기된 것으로 검출된 노드 이외의 다른 노드에 할당된 HBES 노드 키 세트를 폐기되지 않은 것으로 결정한다.

116 단계에서 폐기 키 결정 장치(4)는 112 단계에서 식별된 그룹의 후손 그룹들에 대한 정보의 종결 여부를 검출하고, 112 단계에서 식별된 그룹의 후손 그룹들에 대한 정보가 종결되지 않은 것으로 검출되면, 111 단계로 돌아간다.

117 단계에서 폐기 키 결정 장치(4)는 116 단계에서, 112 단계에서 식별된 그룹의 후손 그룹들에 대한 정보가 종결된 것으로 검출되면, 112 단계에서 식별된 그룹에 속하는 노드들 각각의 폐기 여부에 따라 이 후손 그룹들에 속하는 모든 노드들 각각에 할당된 HBES 노드 키 세트들 각각의 폐기 여부를 한번에 결정한다.

도 12a 및 도 12b는 본 발명의 바람직한 일 실시예에 따른 복호화 방법의 흐름도이다.

도 12a 및 도 12b를 참조하면, 본 실시예에 따른 복호화 방법은 다음과 같은 단계들로 구성된다. 본 실시예에 따른 복호화 방법은 도 4에 도시된 복호화 장치(10)에서 시계열적으로 처리되는 단계들로 구성된다. 따라서, 이하 생략된 내용이라도 도 4에 도시된 복호화 장치(10)에 관하여 이상에서 기술된 내용은 본 실시예에 따른 복호화 방법에도 적용된다.

121 단계에서 복호화 장치(10)는 컨텐츠 서버로부터 네트워크 등의 전송 매체를 경유하여 어느 하나의 패킷을 수신한다.

122 단계에서 복호화 장치(10)는 121 단계에서 수신된 패킷을 해석하고, 그 결과에 따라 패킷의 구성을 인지한다.

123 단계에서 복호화 장치(10)는 122 단계에서의 해석 결과에 따라 인지된 HBES 키 트리 구조에 기초하여 HBES 키 트리 내의 그룹들 중 적어도 하나 이상의 그룹을 식별한다. 보다 상세하게 설명하면, 123 단계에서 복호화 장치(10)는 L 계층들 중 어느 하나의 계층에 해당하는 그룹에 속하는 노드의 위치에 기초하여 이 계층의 다음 하위 계층에 해당하는 그룹을 식별한다.

124 단계에서 복호화 장치(10)는 123 단계에서 식별된 그룹에 속하는 노드들 중 적어도 하나 이상의 폐기되지 않은 노드의 구간에 관한 정보로부터 이 노드들 각각의 폐기 여부를 검출한다.

125 단계에서 복호화 장치(10)는 123 단계에서 식별된 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 중, 124 단계에서 폐기된 것으로 검출된 노드에 할당된 HBES 노드 키 세트를 폐기된 것으로 결정한다.

126 단계에서 복호화 장치(10)는 123 단계에서 식별된 그룹에 속하는 노드들 각각에 할당된 HBES 노드 키 세트들 중, 124 단계에서 폐기된 것으로 검출된 노드 이외의 다른 노드에 할당된 HBES 노드 키 세트를 폐기되지 않은 것으로 결정한다.

127 단계에서 복호화 장치(10)는 123 단계에서 식별된 그룹의 후손 그룹들에 대한 정보의 종결 여부를 검출하고, 123 단계에서 식별된 그룹의 후손 그룹들에 대한 정보가 종결되지 않은 것으로 검출되면, 122 단계로 돌아간다.

128 단계에서 복호화 장치(10)는 127 단계에서, 123 단계에서 식별된 그룹의 후손 그룹들에 대한 정보가 종결된 것으로 검출되면, 123 단계에서 식별된 그룹에 속하는 노드들 각각의 폐기 여부에 따라 이 후손 그룹들에 속하는 모든 노드들 각각에 할당된 HBES 노드 키 세트들 각각의 폐기 여부를 한번에 결정한다.

129 단계에서 복호화 장치(10)는 126 단계 및 128 단계에서 폐기되지 않은 것으로 결정된 HBES 노드 키 세트를 사용하여 패킷 해석부(41)에서의 해석 결과에 따라 인지된 헤더(31)에 기록된 암호화된 콘텐츠 키를 복호화한다.

130 단계에서 복호화 장치(10)는 129 단계에서 복호화된 콘텐츠 키를 사용하여, 패킷 해석부(41)에서의 해석 결과에 따라 인지된 페이로드(32)에 기록된 암호화된 콘텐츠를 복호화한다.

131 단계에서 복호화 장치(10)는 130 단계에서 복호화된 콘텐츠를 사용자에게 출력한다.

한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다. 또한, 상술한 본 발명의 실시예에서 사용된 데이터의 구조는 컴퓨터로 읽을 수 있는 기록매체에 여러 수단을 통하여 기록될 수 있다.

상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드 디스크 등), 광학적 판독매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장매체를 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

본 발명에 따르면, HBES 키 트리 구조에 기초하여 그룹을 식별함으로써 종래 HBES에서 많은 비트 수를 요구했던 그룹 아이디를 제거할 수 있으며, 이에 따라 HBES 노드 키의 폐기 여부에 관한 정보가 기록된 태그의 크기를 줄일 수 있다는 효과가 있다. 또한, 본 발명에 따르면, HBES 키 트리 내의 어떤 그룹의 후손 그룹들에 대한 정보의 종결 여부를 나타내는 필드를 도입함으로써 후손 그룹들에 대한 정보를 더 이상 표현할 필요가 없게 되어 HBES 노드 키의 폐기 여부에 관한 정보가 기록된 태그의 크기를 더욱 줄일 수 있다는 효과가 있다.

도면의 간단한 설명

도 1은 일반적인 HBES 키 트리를 도시한 도면이다.

도 2는 일반적인 HBES 키 트리의 일례를 도시한 도면이다.

도 3은 본 발명의 바람직한 일 실시예에 따른 패킷의 포맷을 도시한 도면이다.

도 4는 본 발명의 바람직한 일 실시예에 따른 폐기 키 결정 장치의 구성도이다.

도 5는 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 일례를 도시한 도면이다.

도 6은 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 다른 예를 도시한 도면이다.

도 7은 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 또 다른 예를 도시한 도면이다.

도 8은 본 발명의 바람직한 일 실시예에 적용되는 HBES 키 트리의 다른 예를 도시한 도면이다.

도 9는 종래 기술에 따른 태그의 크기와 본 발명의 바람직한 일 실시예에 따른 태그의 크기의 비교 표를 도시한 도면이다.

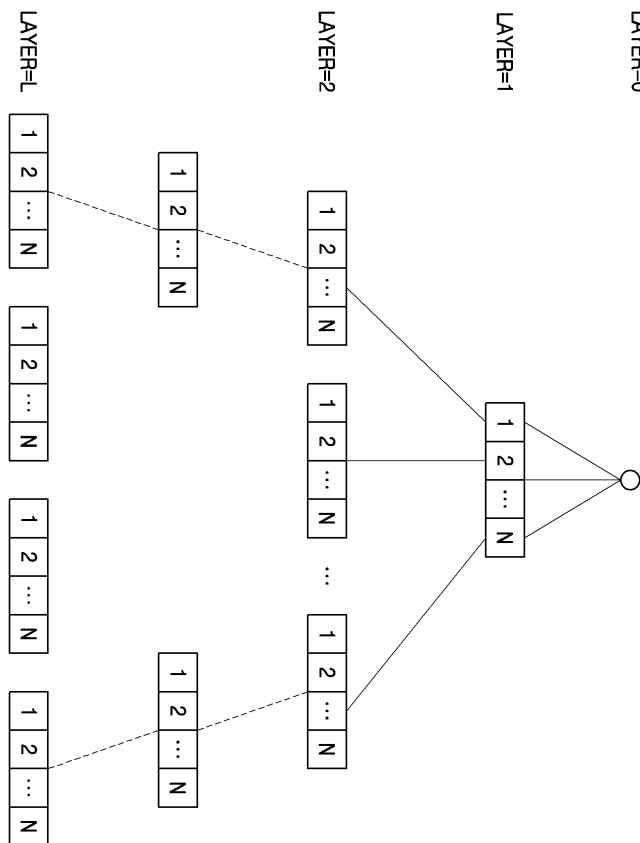
도 10은 본 발명의 바람직한 일 실시예에 따른 복호화 장치의 구성도이다.

도 11은 본 발명의 바람직한 일 실시예에 따른 폐기 키 결정 방법의 흐름도이다.

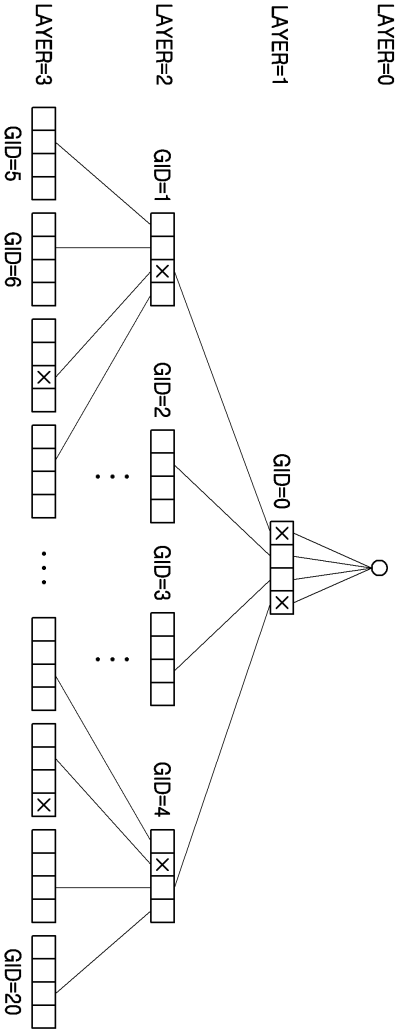
도 12a 및 도 12b는 본 발명의 바람직한 일 실시예에 따른 복호화 방법의 흐름도이다.

도면

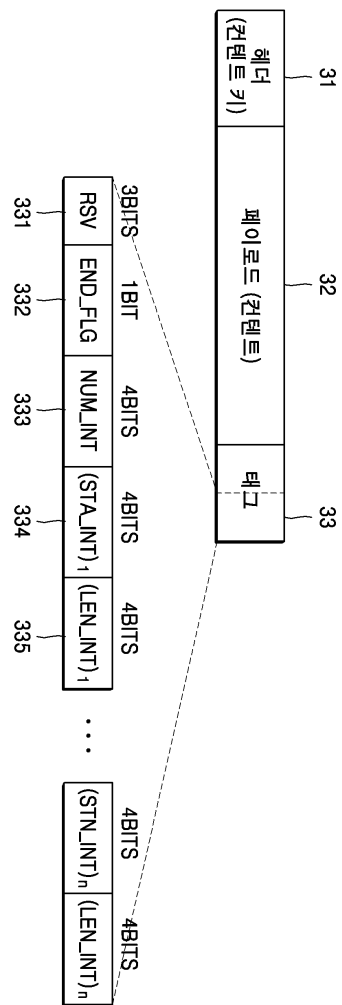
도면1



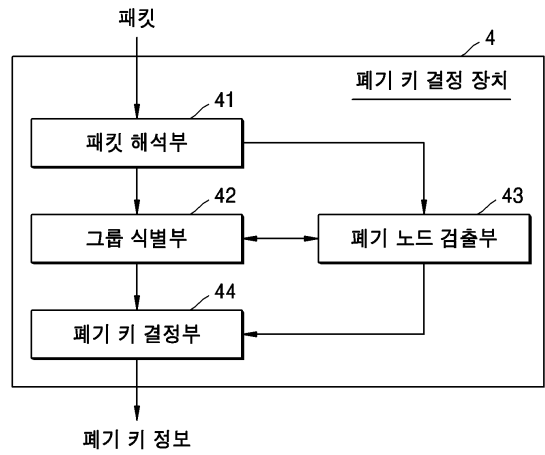
도면2



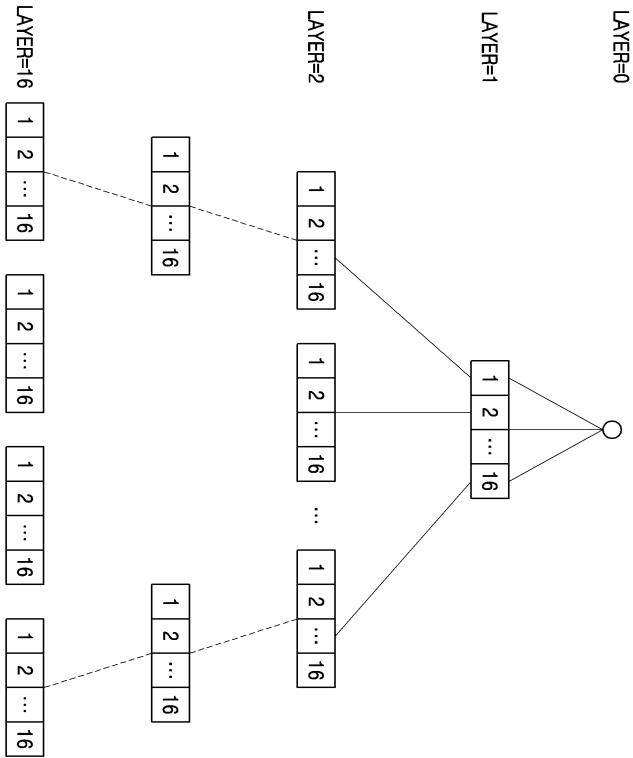
도면3



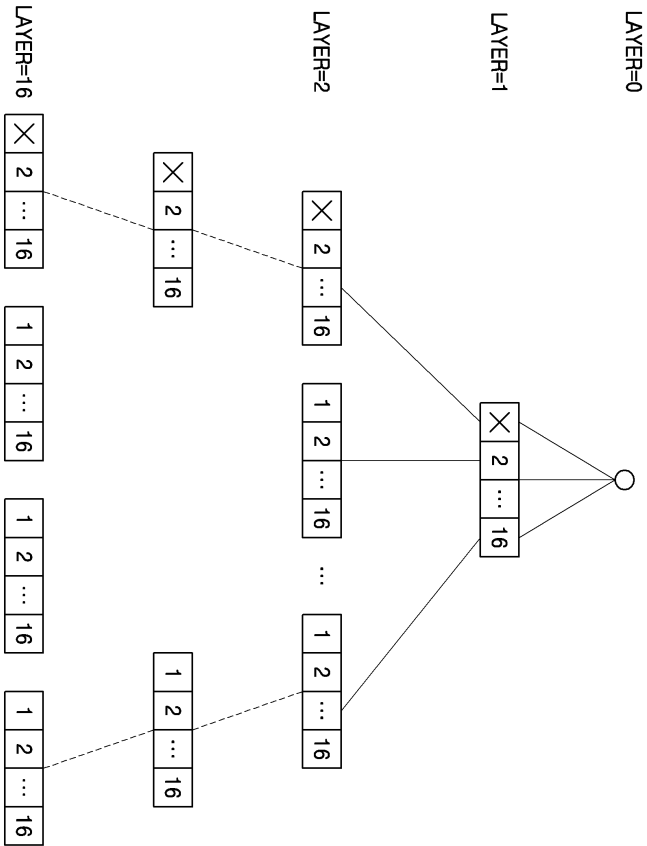
도면4



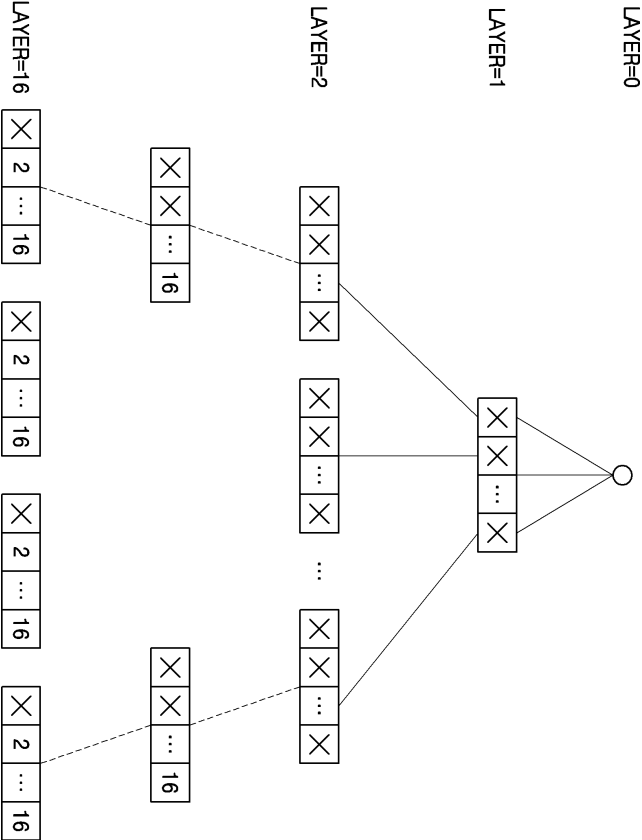
도면5



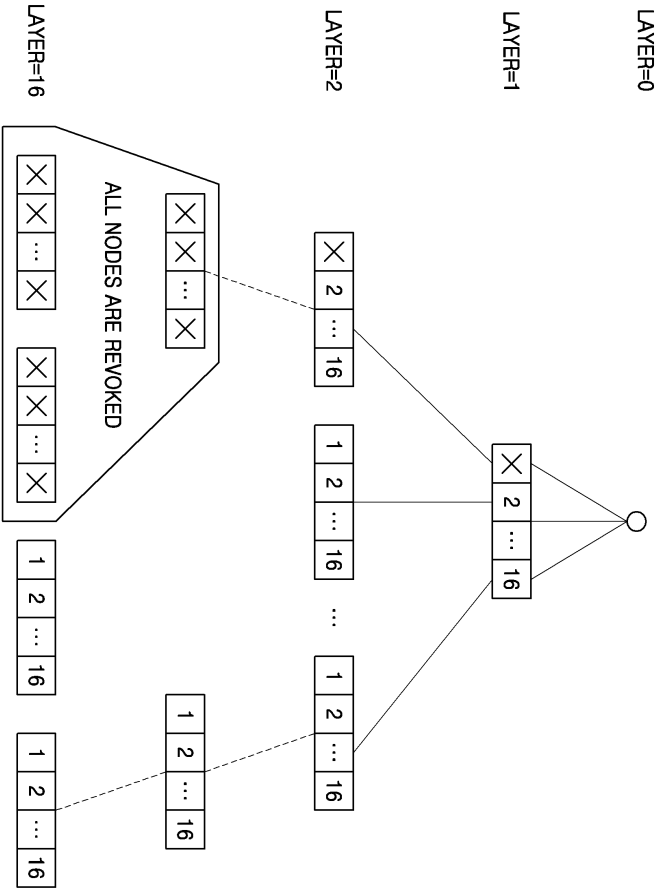
도면6



도면7



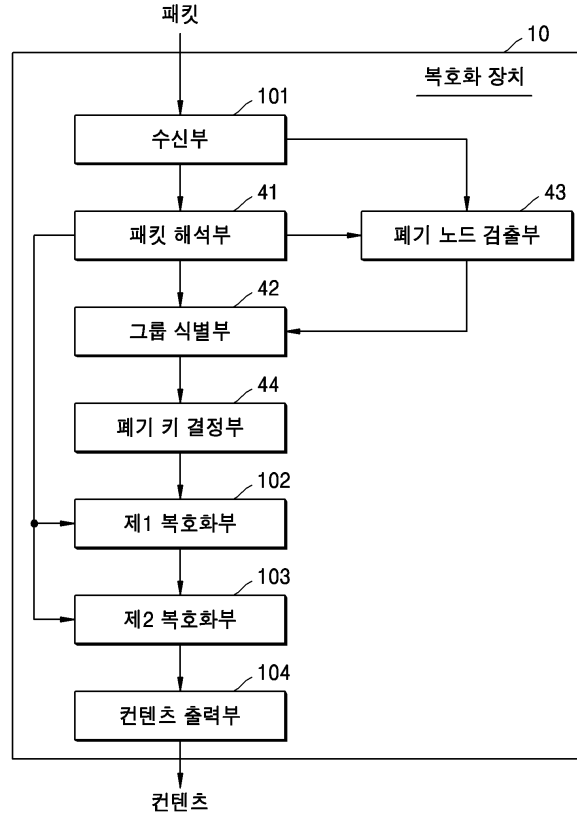
도면8



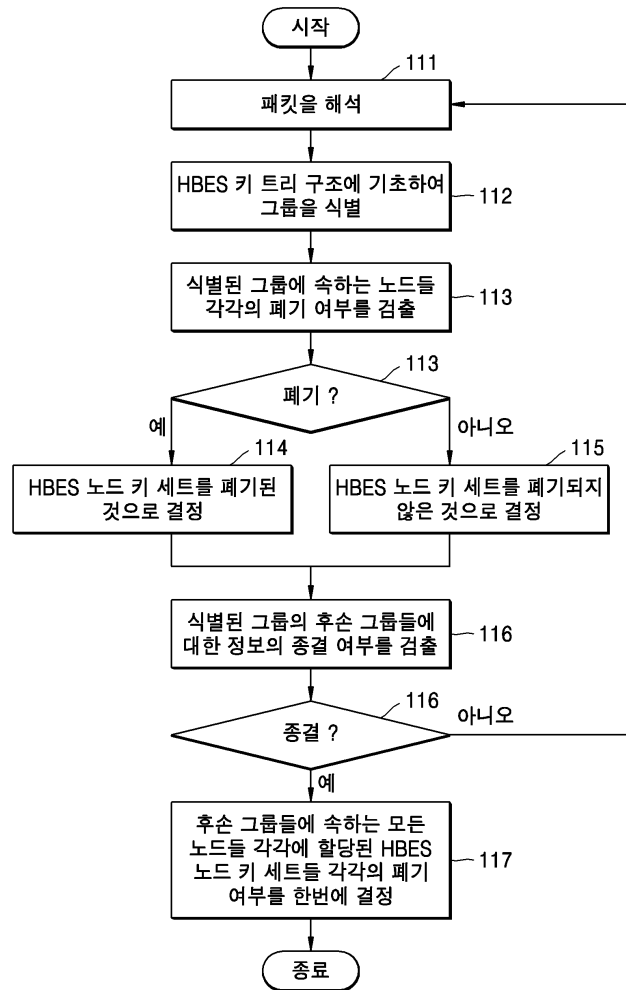
도면9

	종래 기술	본 실시예
도 5의 경우	9	2
도 6의 경우	$9 \times 16 = 144$	$2 \times 16 = 32$
도 7의 경우	$9 \times 16 \times 16 \times 14 = 32256$	$2 \times 17 + 2 \times 16 \times 16 \times 14 = 7202$
도 8의 경우	$9 \times 2 = 18$	$2 + 2 = 4$

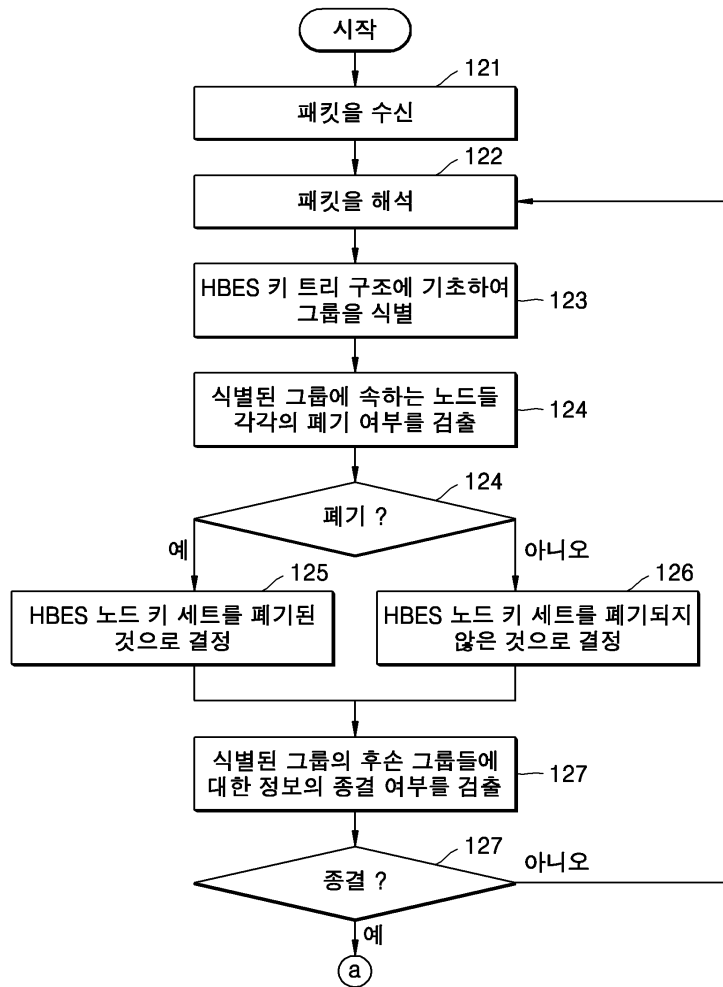
도면10



도면11



도면12a



도면12b

