

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl. ⁷
H04L 9/00

(11) 공개번호 특2002 - 0090318
(43) 공개일자 2002년12월02일

(21) 출원번호 10 - 2002 - 0028630
(22) 출원일자 2002년05월23일

(30) 우선권주장 JP - P - 2001 - 00154787 2001년05월24일 일본(JP)

(71) 출원인 산요 덴키 가부시카가이샤
일본 오사카후 모리구치시 게이한 혼도오리 2쵸메 5반 5고

(72) 발명자 호리우찌게이지
일본기후쥬안빠찌궁안빠찌쥬오호모리180
요시카와다카또시
일본기후쥬오가끼시신덴쥬1 - 16 - 407
히오키도시아끼
일본기후쥬오가끼시다끼시마쥬아피에스오가끼902
호리요시히로
일본기후쥬기후시구라마에5 - 1 - 12

(74) 대리인 장수길
이중희
구영창

심사청구 : 없음

(54) 고유하게 존재하는 콘텐츠 데이터를 백업하는 데이터 단말장치

요약

셀룰라 폰에서, 컨트롤러(1022)는 배신 서버로부터 메모리(1024) 내로 수신된 콘텐츠 데이터를 저장한다. 콘텐츠 데이터가 메모리 카드(110)에 전송될 경우, 난수 키 생성기(1032)가 라이선스 키를 생성하고, 암호화 처리 유닛(1038)에서 상기 라이선스 키를 사용하여 콘텐츠 데이터를 암호화한다. 컨트롤러(1022)는 암호화된 콘텐츠 데이터를 메모리 카드 인터페이스(1026)를 통하여 메모리 카드(110)로 전송한다. 그런다음, 컨트롤러(1022)는 메모리(1024) 내에 저장된 콘텐츠 데이터를 삭제한다. 그 결과, 다른 장치로 전송되는 경우 삭제되어야만 하는 콘텐츠 데이터의 배신을 저작권을 보호하면서 원활하게 할 수 있다.

대표도

도 1

색인어

고유 라이선스, 콘텐츠 ID, 고유 세션, 클래스 증명서, 비밀 복호키

명세서

도면의 간단한 설명

도 1은 통신 시스템을 설명하기 위한 개략도.

도 2는 도1의 통신 시스템에서 통신하기 위한 데이터, 정보 등의 특성을 도시하는 도면.

도 3은 도 1의 데이터 배신 시스템에서 통신하기 위한 데이터, 정보 등의 특성을 도시하는 도면.

도 4는 도 1의 통신 시스템에서 셀룰라 폰의 구조를 개략적으로 도시하는 도면.

도 5는 도 1의 통신 시스템에서 메모리 카드의 구조를 개략적으로 도시하는 블록도.

도 6 및 7은 각각, 도 1의 통신 시스템에서 셀룰라 폰으로부터 메모리 카드로의 콘텐츠 데이터의 저장을 설명하기 위한 제1 및 제2 흐름도.

도 8은 도 1의 통신 시스템에서 메모리 카드로부터 셀룰라 폰으로의 콘텐츠 데이터의 저장을 설명하는 흐름도.

도 9는 도 5의 메모리 카드의 메모리 내의 라이선스 영역 및 데이터 영역을 도시하는 도면.

〈도면의 주요부분에 대한 부호의 설명〉

10: 배신 서버

110: 메모리 카드

1022: 컨트롤러

1024: 메모리

1026: 메모리 카드 인터페이스

1032: 난수 키 생성기

1038: 암호화 처리 유닛

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 취득한 콘텐츠 데이터에 관한 저작권을 보호할 수 있는 데이터 단말 장치에 관한 것으로, 특히 기록 매체로의 복제가 금지된 콘텐츠 데이터의 백업을 제공하는 데이터 단말 장치에 관한 것이다. 더구나, 본 발명은 취득된 콘텐츠 데이터를 기록 매체를 통하여 다른 장치로 전송하는 데이터 단말 장치에 관한 것이다.

최근 인터넷 등의 정보 통신망 등의 발전 덕분에 각 사용자는 셀룰라 폰 등을 채용하는 개인 지향형 단말기를 통하여 네트워크 정보를 쉽게 액세스할 수 있게 되었다.

최근 셀룰라 폰 내에 자바(Java)를 통합시킴으로써, 다양한 콘텐츠 데이터, 예를 들어 화상 데이터를 서버로부터 수신하여 셀룰라 폰의 내장형 메모리 내에 저장하고 이 데이터를 셀룰라 폰의 디스플레이에 제공할 수 있게 되었다. 또한, 게임 소프트웨어를 서버로부터 수신하여 셀룰라 폰의 내장형 메모리 내에 저장할 수 있게 되어 이 셀룰라 폰을 통하여 게임을 즐길 수 있게 되었다.

저작권 보호라는 관점에서 볼 때, 사용자는 셀룰라 폰의 내장형 메모리 내에 저장된 이러한 소프트웨어를 외부 기록 매체에 기록할 수 없고 또는 이 소프트웨어를 다른 셀룰라 폰으로 전송할 수도 없다. 수신된 소프트웨어가 더 이상 필요치 않다면 사용자는 자신의 셀룰라 폰의 내장형 메모리에 저장된 소프트웨어를 삭제해야만 한다.

사용자가 나중에 사용할 목적으로 상기 소프트웨어를 저장하길 원한다 하더라도, 새로운 소프트웨어를 다운받으려한다면 셀룰라 폰의 내장형 메모리의 제한된 용량 때문에 저장되어있던 상기 소프트웨어는 삭제해야만 한다. 사용자가 나중에 다시 상기 삭제된 소프트웨어를 사용하길 원한다면 서버로부터 동일한 소프트웨어를 수신해야만 한다.

또한, 사용자가 자신의 셀룰라 폰을 변경하는 경우를 고려해보자. 이전에 사용된 셀룰라 폰의 소프트웨어를 새로운 셀룰라 폰으로 전송할 수 없기 때문에, 새로운 셀룰라 폰에 동일한 소프트웨어를 사용하기 위해서는 사용자의 새로운 셀룰라 폰에서 서버로부터 동일한 소프트웨어를 수신하여야 한다.

이것은 사용자가 서버로부터 동일한 소프트웨어를 수신하는 데 요금을 다시 지불하여야 함을 의미한다. 이러한 점은 사용자로서는 불합리한 것이다.

또한, 사용자가 자신의 셀룰라 폰에 존재하는 어떤 소프트웨어 프로그램을 다른 사용자에게 인도하기를 원하는 경우에도 소프트웨어를 다른 사용자에게 증여할 수는 없다.

발명이 이루고자 하는 기술적 과제

전술한 점을 고려하여, 본 발명의 목적은 저작권을 보호하면서 다른 장치로 전송하는 경우 삭제되어야 하는 콘텐츠 데이터의 배송을 촉진하는 데이터 단말 장치를 제공하는 데 있다.

본 발명의 양태에 따르면, 데이터 단말 장치는 평문(plaintext)으로 취득된 콘텐츠 데이터의 암호화된 버전인 암호화된 콘텐츠 데이터와 상기 암호화된 콘텐츠 데이터를 복호화하기 위해 필요한 라이선스 키를 생성하고, 상기 암호화된 콘텐츠 데이터와 상기 라이선스 키를 데이터 기록 장치로 전송한다. 상기 데이터 단말 장치는 지시를 입력하기 위한 조작 유닛, 상기 데이터 기록 장치로 데이터를 전송하기 위한 인터페이스, 상기 콘텐츠 데이터를 평문 형태로 저장하는 저장 유닛, 상기 라이선스 키를 생성하고 생성된 라이선스 키를 사용하여 상기 콘텐츠 데이터를 암호화함으로써 상기 암호화된 콘텐츠 데이터를 생성하는 암호화된 콘텐츠 생성 유닛, 상기 라이선스 키를 포함하는 라이선스와, 상기 데이터 기록 장치로부터 상기 라이선스 키 출력 횟수를 1회로 제한하는 제어 정보를 생성하는 라이선스 생성 유닛, 상기 라이선스 생성 유닛에 의해 생성된 라이선스를 암호화하여 암호화된 라이선스를 생성하거나 또는 상기 데이터 기록 장치에 저장된 다른 암호화된 라이선스를 수신하고 복호화하며 다른 라이선스 키를 포함하는 암호화/복호화 처리 유닛, 상기 데이터 기록 장치에 저장된 다른 암호화된 콘텐츠 데이터를 수신하고, 상기 수신된 다른 암호화된 콘텐츠 데이터를 상기 암호화/복호화 처리 유닛으로부터 추출되고 복호화된 다른 라이선스 키를 사용하여 복호화하는 콘텐츠 데이터 복호화기, 및 컨트롤 유닛을 포함한다. 상기 컨트롤 유닛은 상기 조작 유닛을 통해 입력된 상기 데이터 기록 장치로의 상기 콘텐츠 데이터의 전송 요구에 응답하여 상기 저장 유닛으로부터 평문으로 된 상기 콘텐츠 데이터를 상기 암호화된 콘텐츠 생성 유닛 내로 읽어내고, 상기 인터페이스를 통하여 상기 암호화된 콘텐츠 데이터와 상기 암호화된 라이선스를 상기 데이터 기록 장치로 전송하고, 상기 저장 유닛에 저장된 평문으로 된 콘텐츠 데이터를 삭제한다.

본 발명의 데이터 단말 장치에서, 콘텐츠 데이터가 데이터 기록 장치로 전송될 경우 라이선스 키가 생성된다. 생성된 라이선스 키에 의해 생성된 암호화된 콘텐츠 데이터는 데이터 기록 장치로 전송된다. 데이터 단말 장치는 또한 암호화된 콘텐츠 데이터가 데이터 기록 장치로부터 수신되는 경우 데이터 기록 장치에 기록된 라이선스의 출력을 1회만 허가하는 라이선스를 데이터 기록 장치로 전송한다. 그런 다음, 데이터 단말 장치는 저장 유닛에 기억된 콘텐츠를 삭제한다. 즉, 콘텐츠 데이터가 외부 소스로 출력되는 경우 출력 소스에 저장된 이전 콘텐츠 데이터는 실질적으로 삭제된다. 본 발명에서, "실질적으로 삭제된다"는 것의 의미는 사용 횟수를 "0"으로 설정함으로써 데이터 기록 장치로부터 라이선스 키의 제2 출력을 금지한다는 의미를 포함한다. 본 발명에 따르면, 콘텐츠 데이터의 복사를 방지하면서 콘텐츠 데이터가 배신될 수 있다.

바람직하게는, 암호화/복호화 처리 유닛은 인터페이스를 통하여 데이터 기록 장치로부터 제공된 제1 세션 키를 사용하여 라이선스를 암호화하여 암호화된 라이선스를 생성하는 암호화기를 포함한다. 컨트롤 유닛은 데이터 기록 장치로의 암호화된 라이선스의 기록 동작에서, 컨트롤 유닛은 상기 인터페이스를 통하여 상기 데이터 기록 장치로부터 상기 제1 세션 키를 수신하고, 상기 수신된 세션 키를 상기 암호화기에 제공한다.

데이터 기록 장치에서 생성된 제1 세션 키를 사용하여 데이터 기록 장치로 전송될 라이선스가 암호화된다. 본 발명에 의하면, 콘텐츠 데이터가 데이터 기록 장치로 전송될 때 데이터가 덜 누설되는 경향이 있다.

바람직하게는, 상기 암호화/복호화 처리 유닛은 데이터 기록 장치와의 통신을 특정하기 위한 세션 키를 생성하는 세션 키 생성기, 및 상기 세션 키 생성기에 의해 생성된 제2 세션 키를 사용하여 암호화된 데이터를 복호화하는 복호화기를 더 포함한다. 암호화된 라이선스가 데이터 기록 장치로 기록될 때, 상기 세션 키 생성기가 상기 제2 세션 키를 생성한다. 컨트롤 유닛은 상기 인터페이스를 통하여 상기 제2 세션 키를 상기 데이터 기록 장치에 제공한다. 컨트롤 유닛은 인터페이스를 통하여 데이터 기록 장치로부터 상기 제2 세션 키에 의해 암호화된 상기 제1 세션 키를 수신하고, 상기 수신된 제2 세션키를 사용하여 암호화된 제1 세션 키를 복호화기에 제공한다.

데이터 기록 장치로의 콘텐츠 데이터의 전송에서, 세션 키가 데이터 기록 장치에 대해 전송된다. 데이터 단말 장치는 데이터 기록 장치에서 생성되고 자신의 제2 세션 키에 의해 암호화된 제1 세션 키를 데이터 기록 장치로부터 수신한다.

바람직하게는, 암호화/복호화 처리 유닛은 데이터 기록 장치로부터 수신되고 고유한 제1 공개 키를 사용하여 데이터를 암호화하는 다른 암호화기를 더 포함한다. 암호화된 라이선스가 데이터 기록 장치로 기록되는 경우, 복호화기는 상기 제2 세션 키 및 암호화키에 의해 암호화된 상기 제1 세션 키를 상기 제2 세션 키를 사용하여 복호화하고, 상기 제1 세션 키와 상기 제1 공개 키를 추출한다. 다른 암호화기는 상기 제1 공개 키를 사용하여 상기 라이선스 생성 유닛에 의해 생성된 라이선스를 암호화한다. 암호화기는 다른 암호화기의 출력을 수신하고 상기 제1 세션 키를 사용하여 암호화하며, 상기 제1 세션 키를 사용하여 암호화된 라이선스를 생성한다. 컨트롤 유닛은 인터페이스를 통하여 제2 세션 키를 데이터 기록 장치로 제공하고, 인터페이스를 통하여 상기 데이터 기록 장치로부터 상기 제2 세션 키에 의해 암호화된 상기 제1 세션 키를 수신하며, 상기 제2 세션 키에 의해 암호화된 상기 수신된 제1 세션 키와 상기 제1 공개 키를 복호화기에 제공한다.

라이선스가 데이터 기록 장치로 전송되는 경우, 라이선스가 데이터 기록 장치에 보유된 제1 공개 키와 데이터 기록 장치에서 생성된 세션 키에 의해 순차 암호화된다. 본 발명에 의하면, 암호화된 콘텐츠 데이터를 복호화시키기 위해 필요한 라이선스가 충분한 보호하에 데이터 기록 장치로 전송될 수 있다.

바람직하게는, 상기 암호화/복호화 처리 유닛은 제2 공개 키를 사용하여 데이터를 암호화하는 다른 암호화기를 더 포함한다. 암호화된 라이선스가 데이터 기록 장치로 기록될 때, 다른 암호화기는 상기 제2 공개 키를 사용하여 제2 세션 키를 암호화한다. 컨트롤 유닛은 인터페이스를 통하여 데이터 기록 장치로부터 제2 공개 키를 포함하는 인증 데이터를 수

신한다. 수신된 인증 데이터가 적당한 것으로 판정되면 컨트롤 유닛은 수신된 인증 데이터에 포함된 제2 공개 키를 다른 암호화기에 제공하고, 다른 암호화기의 상기 제2 공개 키에 의해 암호화된 제2 세션 키를 인터페이스를 통하여 데이터 기록 장치로 제공하는 것을 특징으로 한다.

자신의 생성된 세션키를 데이터 기록 장치로 전송하는 데 있어, 데이터 단말 장치는 데이터 기록 장치로부터의 인증 데이터의 인증을 행한 다음, 인증 데이터에 포함된 제2 공개 키를 사용하여 자신의 생성 세션 키를 암호화하여 이 암호화된 세션 키를 데이터 기록 장치로 전송한다. 본 발명에 따르면, 불법 집단으로의 데이터 전송을 방지할 수 있다.

바람직하게는, 암호화/복호화 처리 유닛은 데이터 기록 장치와의 통신을 특정하기 위한 세션 키를 생성하는 세션 키 생성기와, 세션 키 생성기에 의해 생성된 세션 키를 사용하여 암호화된 데이터를 복호화하는 복호화기를 포함한다. 다른 암호화된 라이선스가 데이터 기록 장치로부터 판독되는 경우, 세션 키 생성기는 제2 세션 키를 생성한다. 컨트롤 유닛은 상기 세션 키 생성기에 의해 생성된 상기 세션 키를 인터페이스를 통해 데이터 기록 장치로 제공하고, 데이터 기록 장치로부터 세션 키에 의해 암호화된 상기 다른 암호화된 라이선스를 인터페이스를 통해 수신하고, 수신된 다른 암호화된 라이선스를 복호화기에 제공한다.

콘텐츠 데이터가 데이터 기록 장치로부터 수신되는 경우, 데이터 단말 장치는 데이터 기록 장치/로부터 세션키를 송신/수신하고, 데이터 기록 장치로부터 자신의 생성된 세션 키에 의해 암호화된 라이선스 키를 수신한다. 본 발명에 따르면, 데이터 단말 장치는 수신 처리 동안 상호 인증을 행하면서 데이터 기록 장치로부터 콘텐츠 데이터를 수신할 수 있다.

바람직하게는, 데이터 단말 장치는 조작 유닛을 통해 입력되는 수신 요청에 응답하여 상기 데이터 기록 장치에 제공될 인증 데이터를 저장하는 인증 데이터 보유 유닛을 더 포함한다. 컨트롤 유닛은 인증 데이터를 인터페이스를 통하여 데이터 기록 장치로 제공하고, 인증 데이터가 데이터 기록 장치에서 인증될 때 데이터 기록 장치로부터 다른 암호화된 콘텐츠 데이터와 다른 암호화된 라이선스를 수신한다.

콘텐츠 데이터가 데이터 기록 장치로부터 데이터 단말 장치로 전송될 때, 데이터 단말 장치의 인증 데이터가 데이터 기록 장치로 제공된다. 데이터 기록 장치에서 인증 데이터의 인증시, 다른 암호화된 콘텐츠 데이터 및 다른 암호화된 라이선스가 데이터 기록 장치로부터 데이터 단말 장치로 전송된다. 본 발명에 따르면, 부적합한 데이터 단말 장치로의 암호화된 콘텐츠 데이터 및 암호화된 라이선스의 출력을 방지할 수 있다.

본 발명의 전술한 및 다른 목적, 특성, 양태 및 장점들은 첨부된 도면을 참조로 하는 이어지는 발명의 상세한 설명으로부터 좀 더 명백해질 것이다.

발명의 구성 및 작용

이하 도면을 참조하여 본 발명의 실시예를 상세히 설명할 것이다. 도면에서, 동일 또는 대응되는 구성 요소들에는 동일한 참조 부호를 부가하였으며, 이들에 대한 설명을 반복하지 않을 것이다.

도 1은 데이터 단말 장치(셀룰라 폰)가 본 발명에 따른 콘텐츠 데이터를 얻는 통신 시스템의 전체 구성을 도시한 개략도이다.

콘텐츠 데이터는 (동화상 데이터를 포함한) 이미지 데이터, 음성 데이터 및 게임 프로그램과 같이, 데이터 단말 장치의 내장형 메모리에 일시적으로 기억되어 사용되는 모든 데이터를 참조한다.

도 1을 참조하면, 배신 서버(10)는 사용자로부터 자신의 셀룰라 폰(100)을 통해 송신된 프로그램 배신 요청을 캐리어(carrier)(20)를 통해 수신한다. 배신 서버(10)는 수신된 프로그램 배신 요청에 응답하여 프로그램을 캐리어(20)를 통해 셀룰라 폰(100)으로 송신한다. 이 경우, 배신 서버(10)는 프로그램을 셀룰라 폰(100)으로 평문(plaintext)으로

송신한다. 캐리어(20)는 셀룰라 폰(100)으로부터의 프로그램 배신 요청을 배신 서버(10)로 송신하고, 배신 서버(10)로부터의 프로그램을 셀룰라 전화망을 통해 셀룰라 폰(100)으로 송신한다.

셀룰라 폰(100)은 상기 프로그램을 셀룰라 전화망을 통해 수신하고, 수신된 프로그램을 (도시되지 않은) 내장형 메모리에 기억한다. 멜로디와 같은 음성 신호가 셀룰라 폰(100)에서 울려져 데이터 입력을 확인한다. 셀룰라 폰(100)의 사용자는 수신된 프로그램을 실행하여, 자신의 셀룰라 폰(100)의 디스플레이부에 다양한 이미지 데이터를 제공하고, 디스플레이부를 통해 이 프로그램에 따라 게임을 한다. 사용자가 셀룰라 폰(100)의 메모리에 상주하는 프로그램을 그 자신의 메모리 카드(110)에 기억시키고자 하는 경우에, 사용자는 메모리 카드(110)를 셀룰라 폰(100)에 부착하여, 셀룰라 폰(100)이 메모리 카드(110) 안으로 이 프로그램을 저장하도록 설정한다.

내장형 메모리에 기억된 프로그램이 메모리 카드(110)에 기억될 때, 셀룰라 폰(100)은 이후 설명되어지는 바와 같이, 프로그램을 암호화하는데 사용되는 라이선스 키를 발생한다. 내장형 메모리에 기억된 프로그램은 발생된 라이선스 키에 의해 암호화된다. 암호화된 프로그램은 라이선스 키의 사용을 한번으로 제한하는 사용 제어 정보(사용 규칙)와 발생된 라이선스 키를 포함하는 라이선스와 함께 메모리 카드(110)에 기억된다. 암호화된 프로그램과 라이선스가 메모리 카드(110)에 기억된 후에, 셀룰라 폰(100)은 자신의 내장형 메모리로부터 이 프로그램을 삭제한다.

따라서, 셀룰라 폰(100)은 기억된 프로그램을 실행하기 위해 배신 서버(10)로부터 수신된 프로그램을 자신의 내장형 메모리에 기억한다. 프로그램이 사용자의 커맨드에 응답하여 메모리 카드(110)에 기억될 때, 셀룰라 폰(100)은 내장형 메모리로부터 기억된 프로그램을 삭제한다. 따라서, 프로그램은 셀룰라 폰(100)과 메모리 카드(110) 모두에 기억된 상태로 되지 않을 것이다. 프로그램이 메모리 카드(110)로부터 출력되면, 이후에 메모리 카드(110)로부터 프로그램이 더 이상은 출력될 수 없다. 다시 말해서, 프로그램이 메모리 카드(110)에 기억될 때, 셀룰라 폰(100)은 전송 데이터에 라이선스 키의 사용을 1회로 제한하는 사용 제어 정보를 첨부한다. 따라서, 메모리 카드(110)로부터 라이선스 키를 출력하도록 허용된 회수는 단 한번으로 제한된다. 프로그램이 메모리 카드(110)로부터 출력될 때, 즉, 암호화된 프로그램과 라이선스 키가 출력될 때, 메모리 카드(110)에 기억된 라이선스 키의 출력가능한 수는 0으로 설정되어 라이선스 키의 출력을 금지하도록 리셋된다. 그러므로, 이후에는 라이선스 키가 메모리 카드(110)로부터 출력될 수 없다. 이것은 프로그램이 유효 상태로 메모리 카드(110)로부터 추출될 수 없다는 것을 의미한다. 프로그램이 셀룰라 폰(100)으로 출력되는 경우에, 셀룰라 폰(100)과 메모리 카드(110) 모두에 사용가능한 상태로 기억되는 프로그램의 이벤트는 발생되지 않을 것이다. 이 프로그램은 항상 단 하나의 사이트에 기억된다.

메모리 카드(110)는 셀룰라 폰(100)에 대하여 분리가능하고, 셀룰라 폰(100)의 사용자는 적절한 프로그램을 메모리 카드(110)에 기억할 수 있다. 사용자가 자신의 셀룰라 폰(100)을 다른 셀룰라 폰으로 교체하는 경우에도, 사용자는 적합한 프로그램을 갖는 메모리 카드(110)를 자신의 다른 셀룰라 폰(100)에 장착함으로써 그 프로그램을 자신의 다른 셀룰라 폰에서 실행하고 메모리 카드(110)로부터의 프로그램을 다른 셀룰라 폰으로 판독할 수 있다.

또한, 셀룰라 폰(100)의 사용자는 내장형 메모리에 상주하는 프로그램들을 메모리 카드(110)에 기억하여, 메모리 카드(110)의 프로그램들을 다른 사용자에게 제공한다. 그 다음, 메모리 카드(110)에 기억된 프로그램 (사실상 출력될 수 있는 라이선스 키와 암호화된 프로그램)은 다른 사용자의 셀룰라 폰의 내장형 메모리에 기억될 수 있다.

도 2는 도 1의 통신 시스템에서, 배신 서버(10)와 셀룰라 폰(100) 간, 또는 셀룰라 폰(100)과 메모리 카드(110) 간에 사용되는 통신용 데이터, 정보 등의 특성을 도시한 것이다.

먼저, 배신 서버(10)에 의해 배신된 데이터가 설명될 것이다. Dc는 프로그램을 형성한 콘텐츠 데이터를 나타낸다. 콘텐츠 데이터 Dc는 배신 서버(10)로부터 캐리어(20)를 통해 셀룰라 폰(100)으로 평문으로 송신된다. 송신된 콘텐츠 데이터는 데이터 단말 장치(셀룰라 폰) 또는 메모리 카드에 기억된다.

현재의 통신 시스템에서의 라이선스는 암호화된 콘텐츠 데이터를 복호하는데 필요한 라이선스 키 Kc를 포함한다. 라이선스 키 Kc는 셀룰라 폰(100)에 기억된 프로그램이 메모리 카드(110)로 송신될 때 셀룰라 폰(100)에서 발생된다. 라이선스 키 Kc는 셀룰라 폰(100)과 메모리 카드(110) 사이에서 라이선스 키 Kc를 사용하여 암호화되는 암호화된 콘텐츠 데이터 {Dc}Kc와 함께 전송된다. {Y}X의 표현은 데이터 Y가 복호 키 X에 의해 복호가능한 형태로 암호화된 것을 의미한다.

본 통신 시스템에서 라이선스는 또한 기록 장치 (메모리 카드) 내에서 라이선스의 액세스를 제한하는 정보인 액세스 제한 정보 ACm를 포함한다. 특히, 액세스 제한 정보 ACm은 라이선스 키 Kc가 메모리 카드로부터 외부 소스로 출력될 때의 제어 정보이고, 재생가능한 회수 (재생을 위해 라이선스 키가 출력되는 회수)를 포함한다.

또한, 라이선스는 암호화된 콘텐츠 데이터 {Dc}Kc가 셀룰라 폰(100)으로부터 메모리 카드(110)로 전송될 때 셀룰라 폰(100)의 메모리에 기억된 콘텐츠 데이터를 식별하기 위한 관리 코드로서 기능하는 콘텐츠 ID를 포함한다.

또한, 라이선스는 암호화된 콘텐츠 데이터 {Dc}Kc가 셀룰라 폰(100)으로부터 메모리 카드(110)로 전송될 때 발생된 라이선스를 식별하기 위한 관리 코드로서 기능하는 라이선스 ID를 포함한다.

라이선스 키 Kc, 액세스 제한 정보 ACm, 콘텐츠 ID, 및 라이선스 ID는 이하 "라이선스" 로서 총칭해서 참조된다.

간략화를 위해, 액세스 제한 정보 ACm는 라이선스 키의 출력 계수(0:사용 불가, 1: 1회 출력 허가, 라이선스 키의 출력 계수를 0으로 설정함)를 제한하는 사용 회수를 제한한다고 가정한다.

도 3은 도 1의 통신 시스템에서 셀룰라 폰(100)과 메모리 카드(110) 사이에 프로그램을 전송하는데 사용되는 인증용 데이터, 정보 등의 특성을 설명하기 위한 도면이다.

데이터 단말 장치(셀룰라 폰)와 메모리 카드에는 각각 고유한 공개 암호키 KPpy 및 KPmw가 할당된다. 공개 암호키 KPpy 및 KPmw는 데이터 단말 장치에 고유한 비밀 복호키 Kpy와 메모리 카드에 고유한 비밀 복호키 Kmw를 사용하여 복호된다. 이 공개 암호키들과 비밀 복호키들은 데이터 단말 장치와 메모리 카드의 임의의 유형에 따라 상이한 값을 가진다. 이러한 공개 암호키와 비밀 복호키들은 일반적으로 "클래스 키" 로 참조된다. 이들 공개 암호키는 "클래스 공개 암호키" 라 불리고 이들 비밀 복호키는 "클래스 비밀 복호키" 로 불린다. 클래스 키를 공유하는 유닛은 "클래스" 라 불린다. 이 클래스는 제조업자, 제품 유형 및 제조지 등에 따라 상이하다.

Cpy는 데이터 단말 장치 (셀룰라 폰)의 클래스 증명서로서 제공된다. Cmw는 메모리 카드의 클래스 증명서로서 제공된다. 이들 클래스 증명서들은 데이터 단말 장치와 메모리 카드의 각각의 클래스에 대한 상이한 정보를 포함한다. 간섭에 의해 저항 모듈이 파괴되거나 클래스 키에 의한 암호화가 깨진 임의의 클래스, 즉 침해를 입은 비밀 암호키를 갖는 임의의 클래스는 라이선스 취소의 대상이 될 것이다. 데이터 단말 장치의 클래스 공개 암호키와 클래스 증명서는 데이터 단말 장치에 대해서는 인증 데이터 {KPpy//Cpy}KPa의 형태로 그리고 메모리 카드에 대해서는 인증 데이터 {KPmw//Cmw}KPa의 형태로 수송 시에 높이 평가되는 데이터 단말 장치와 메모리 카드에 기록된다. KPa는 전체 배신 시스템에 공통인 공개 인증키이다.

메모리 카드(110)에서 처리되는 데이터를 관리하기 위한 키로는, 모든 메모리 카드 매체용으로 설정된 공개 암호키 KPmcx, 및 이 공개 암호키 KPmcx에 의해 암호화된 데이터를 복호하는데 필요한 고유한 비밀 복호키 Kmcx를 포함한다. 각각의 메모리 카드에 고유한 비밀 복호키와 공개 암호키는 통상 고유 키(unique key)라 불린다. 공개 암호키 KPmcx는 "고유 공개 암호키" 라 불린다. 비밀 복호키는 "고유 비밀 복호키" 라 불린다.

메모리 카드와 메모리 카드 외부의 소스간의 데이터 전송에서 비밀을 유지하기 위한 암호키로서, 공통 키 Ks1 - Ks4가 사용된다. 공통 키 Ks1 - Ks4는 콘텐츠 데이터가 데이터 단말 장치(셀룰라 폰)와 메모리 카드 간에 전송될 때마다, 셀룰라 폰(100)과 메모리 카드(110)에서 발생된다.

여기서, 공통 키 Ks1 - Ks4는 데이터 단말 장치와 메모리 카드 간에 통신 또는 액세스 기반에 대응하는 모든 " 세션(session)" 에 대해 발생된 고유한 공통 키이다. 이들 공통 키 Ks1 - Ks4는 이하 " 세션 키" 라 불린다.

세션 키 Ks1 - Ks4는 모든 세션에 대해 고유한 값을 가짐으로써 데이터 단말 장치와 메모리 카드의 제어 하에 있게 된다. 특히, 세션 키 Ks1은 메모리 카드 안에 프로그램을 기억할 때마다 데이터 단말 장치(셀룰라 폰)에 의해 발생된다. 세션 키 Ks2는 메모리 카드에 프로그램을 기억할 때마다 메모리 카드에 의해 발생된다. 세션 키 Ks3은 셀룰라 폰에 프로그램을 기억할 때마다 메모리 카드에 의해 발생된다. 세션 키 Ks4는 셀룰라 폰에 프로그램을 기억할 때마다 셀룰라 폰에 의해 발생된다. 각 세션에서 이들 세션 키들이 송신/수신된다. 다른 파티의 장치에 의해 발생된 세션 키를 수신하면, 콘텐츠 데이터, 라이선스 키, 등이 수신된 세션 키에 의해 암호화된 형태로 송신된다. 따라서, 세션에서의 보완성이 향상된다.

도 4는 도 1의 셀룰라 폰(100)의 구성을 설명하기 위한 개략적인 블록도이다.

셀룰라 폰(100)은 안테나(1000), 송신기/수신기 유닛(1002), 마이크로폰(1004), AD 컨버터(1006), 음성 부호화기(1008), 음성 재생 유닛(1010), DA 컨버터(1012), 스피커(1016), 키 조작 유닛(1018), 디스플레이부(1020), 컨트롤러(1022), 메모리(1024), 메모리 카드 인터페이스(1026), 복호화 처리 유닛(1028, 1036, 1044 및 1048), 인증키 보유 유닛(1030), 난수 키 생성 유닛(1032), 암호화 처리 유닛(1034, 1038, 1040 및 1042), Kp 보유 유닛(1046), 스위치(1050 및 1052), 및 인증 데이터 보유 유닛(1500)을 포함한다.

안테나(1000)는 셀룰라 전화망에 의해 무선으로 전송된 신호를 수신한다. 송신기/수신기 유닛(1002)은 안테나(1000)로부터의 신호를 수신하여 이 신호를 베이스밴드 신호로 변환하거나, 셀룰라 폰(100)으로부터의 데이터를 변조하여 이 변조된 데이터를 안테나(1000)에 제공한다. 개개의 구성 소자들 중으로부터의 데이터가 버스 BS1을 통해 셀룰라 폰(100)으로 전송된다. 마이크로폰(1004)은 셀룰라 폰(100)의 사용자의 음성 데이터를 입력한다. 음성 데이터는 AD 컨버터(1006)로 출력된다. AD 컨버터(1006)는 음성 데이터를 아날로그 신호에서 디지털 신호로 변환한다. 음성 부호화기(1008)는 선정된 방식에 따라 디지털 신호로 변환된 음성 신호를 부호화한다. 음성 재생 유닛(1010)은 다른 셀룰라 폰으로부터 수신된 음성 신호를 복호화한다. DA 컨버터(1012)는 음성 재생 유닛(1010)으로부터의 음성 신호를 디지털 신호에서 아날로그 신호로 변환하여 음성 신호를 출력한다. 이 음성 데이터는 스피커(1016)를 통해 출력된다.

키 조작 유닛(1018)은 셀룰라 폰(100)에 외부 커맨드를 제공한다. 디스플레이부(1020)는 컨트롤러(1022)로부터 출력된 정보 등을 시각 정보로서 제공한다. 컨트롤러(1022)는 셀룰라 폰(100)의 동작을 버스 BS1을 통해 제어한다. 메모리(1024)는 수신된 콘텐츠 데이터로서 배신 서버(10)로부터의 프로그램을 기억한다. 메모리 카드 인터페이스(1026)는 메모리 카드(110)와 버스 BS1 간의 데이터 전송을 제어한다.

셀룰라 폰(100)으로부터 메모리 카드(110)로 프로그램을 기록하는 (또는 " 기억" 하는) 세션에서는, 복호화 처리 유닛(1028)이 인증키 보유 유닛(1030)으로부터의 공개 인증키 KPa를 사용하여 메모리 카드(110)로부터 수신된 인증 데이터를 복호화한다. 인증키 보유 유닛(1030)은 공개 인증키 KPa를 기억한다. 난수 키 생성 유닛(1032)은 메모리 카드(110)로 프로그램을 기억하는 동작으로, 또는 메모리 카드(110)로부터의 프로그램을 셀룰라 폰(100)으로 기록하는 (또는 " 재기억" 하는) 세션에서, 세션 키 Ks1, Ks4와 라이선스 키 Kc를 발생한다.

암호화 처리 유닛(1034)은 복호화 처리 유닛(1028)에서의 복호에 의해서 얻어진 공개 암호화키 $KPmw$ 를 사용하여 난수 키 생성 유닛(1032)에 의해 발생된 세션 키 $Ks1$ 을 암호화하고, 프로그램을 기억하는 동작에서 암호화된 결과를 버스 BS1 상으로 제공한다. 프로그램 기억 동작에서, 복호화 처리 유닛(1036)은 세션 키 $Ks1$ 에 의해 암호화된 메모리 카드(110)로부터의 암호화된 데이터를 버스 BS1을 통해 수신하고, 세션 키 $Ks1$ 을 사용하여 수신된 암호화된 데이터를 복호한다.

암호화 처리 유닛(1038)은 버스 BS1을 통해 메모리(1024)에 기억된 콘텐츠 데이터를 수신하고, 난수 키 생성 유닛(1032)에 의해서 발생된 라이선스 키 Kc 를 사용하여 수신된 콘텐츠 데이터 Dc 를 암호화한다. 암호화된 콘텐츠 데이터 $\{Dc\}Kc$ 는 버스 BS1 상으로 출력된다. 프로그램 기억 동작에서, 암호화 처리 유닛(1040)은 난수 키 생성 유닛(1032)에 의해 발생된 라이선스 키 Kc , 라이선스를 식별하기 위한 관리 코드인 라이선스 ID, 및 공개 암호키 $KPmcw$ 를 사용하는 액세스 제한 정보 ACm 을 포함한다. 암호화된 데이터 $\{\text{라이선스 ID} // Kc // ACm\}Kmcw$ 는 스위치(1050)의 단자 Ph 로 출력된다.

프로그램 기억 동작에서 암호화 처리 유닛(1042)은 세션 키 $Ks2$ 를 사용하여 스위치(1050)의 단자들 Pa 및 Pb 을 연속적으로 스위칭함으로써 얻어진 암호화된 데이터 $\{\text{라이선스 ID} // Kc // ACm\}Kmcw$ 를 암호화한다.

프로그램 재기억 동작에서, 복호화 처리 유닛(1044)은 메모리 카드(110)로부터의 공개 암호키 KPp 를 사용하여 암호화되는 암호화된 데이터를 버스 BS1을 통해 수신하고, 비밀 복호키 Kp 를 사용하여 수신된 암호화된 데이터를 복호한다. Kp 보유 유닛(1046)은 클래스에 고유한 비밀 복호키 Kp 를 기억한다. 프로그램 재기억 동작에서, 복호화 처리 유닛(1048)은 메모리 카드(110)로부터 버스 BS1을 통해 암호화된 콘텐츠 데이터 $\{Dc\}Kc$ 를 수신하고, 난수 키 생성 유닛(1032)에 의해 발생된 라이선스 키 Kc 를 사용하여 수신된 암호화된 콘텐츠 데이터 $\{Dc\}Kc$ 를 복호한다. 콘텐츠 데이터는 버스 BS1 상으로 출력된다. 인증 데이터 보유 유닛(1500)은 공개 인증키 KPa 를 사용하여 클래스 공개 암호키 $KPp1$ 과 클래스 증명서 $Cp1$ 을 복호함으로써 인증된 합법성을 가질 수 있는 형태로 암호화된 인증 데이터 $\{KPp1 // Cp1\}KPa$ 를 기억한다. 여기서 셀룰라 폰(100)의 클래스 y 는 $y=1$ 인 것으로 가정한다.

각각의 세션에서 셀룰라 폰(100)의 각각의 구성 요소들의 동작은 플로우차트에 기초하여 이후 설명되어질 것이다.

도 5는 도 1의 메모리 카드(110)의 구조를 개략적으로 도시하는 블록도이다. 도 5를 참조하면, 메모리 카드(110)는 인증 데이터 보유 유닛(1400), Kmc 보유 유닛(1402), 복호화 처리 유닛(1404, 1408, 1412, 및 1422), 암호화 처리 유닛(1406 및 1410), 인증 키 보유 유닛(1414), 메모리(1415), $KPmc$ 보유 유닛(1416), 난수 키 생성 유닛(1418), 컨트롤러(1420), Km 보유 유닛(1421), 인터페이스(1424), 단말(1426), 및 스위치(1442 및 1446)를 포함한다.

상술된 바와 같이, $KPmw$ 및 Kmw 는 각각 메모리 카드의 클래스 공개 암호 키 및 클래스 비밀 복호 키로서 제공된다. 또한, 메모리 카드의 클래스 증명서 Cmw 가 제공된다. 메모리 카드(110)에서의 자연수 w 는 $w=5$ 인 것으로 가정한다. 또한, 메모리 카드를 식별하기 위한 자연수 x 는 $x=6$ 인 것으로 가정한다.

그러므로, 인증 데이터 보유 유닛(1400)은 인증 데이터 $\{KPm5 // Cm5\}KPa$ 를 저장한다. 데이터는 버스 BS2를 통해서 메모리 카드(110)의 각각의 구성 요소들 사이에서 전송된다. Kmc 보유 유닛(1402)은 메모리 카드마다의 고유 복호 키 세트인 고유 비밀 복호 키 $Kmc6$ 를 저장한다. 복호화 처리 유닛(1404)은 고유 공개 암호 키 $KPmc6$ 와 쌍을 이루는 메모리 카드(110)의 고유 비밀 복호 키 $Kmc6$ 를 사용하여 버스 BS2 상의 데이터를 복호화한다.

암호화 처리 유닛(1406)은 스위치(1442)에 의해 선택적으로 인가되는 키를 사용하여 스위치(1446)에 의해 선택적으

로 인가된 데이터를 암호화한다. 암호화된 데이터는 버스 BS2 상으로 출력된다. 복호화 처리 유닛(1408)은 인증 키 보유 유닛(1414)으로부터 공개 인증 키 KPa를 수신하여, 공개 인증 키 KPa를 사용해 버스 BS2로부터 인가된 데이터를 복호화하고, 복호화한 결과 및 구해진 클래스 증명서를 컨트롤러(1420)에 제공하고, 구해진 클래스 공개 키를 암호화 처리 유닛(1410)에 제공한다. 암호화 처리 유닛(1410)은 복호화 처리 유닛(1408)에 의해 구해진 클래스 공개 암호 키 K_{ppy}를 사용하여 난수 키 생성 유닛(1418)으로부터 출력된 세션 키 K_{s3}를 암호화한다. 암호화된 키는 버스 BS2 상으로 출력된다.

복호화 처리 유닛(1412)은 버스 BS2로부터 세션 키 K_{s2}로 암호화된 데이터를 수신하고, 난수 키 생성 유닛(1418)에 의해 생성된 세션 키 K_{s2}를 사용하여, 수신된 데이터를 복호화한다. 인증 키 보유 유닛(1414)은 공개 인증 키 KPa를 저장한다. K_{Pmc} 보유 유닛(1416)은 고유 비밀 복호 키 K_{mc6}를 사용하여 복호화될 수 있는 공개 암호 키 K_{Pmc6}를 저장한다. 프로그램을 저장하거나 재저장하는 세션 중에는, 난수 키 생성 유닛(1418)이 세션 키 K_{s2} 및 K_{s3}를 생성한다.

메모리(1415)는 암호화된 콘텐츠 데이터 {Dc}K_c 및 암호화된 콘텐츠 데이터를 사용할 수 있도록 복호화하는 데 요구되는 라이선스 (K_c, AC_m, 라이선스 ID)를 버스 BS2를 통해서 수신하여 저장한다. 메모리(1415)는 라이선스 영역(1415A) 및 데이터 영역(1415B)을 포함한다. 라이선스 영역(1415A)은 라이선스가 기록될 경우의 영역이다. 데이터 영역(1415B)은 암호화된 콘텐츠 데이터 {Dc}K_c, 암호화된 콘텐츠마다의 라이선스 관리를 위해 필요한 라이선스 관리 정보를 기록하는 라이선스 관리 파일, 및 메모리 카드에 저장된 암호화된 콘텐츠 데이터 및 라이선스를 액세스하는 데 필요한 기본 정보를 저장하는 리스트 파일을 저장하기 위한 영역이다. 데이터 영역(1415B)은 외부 소스로부터 직접 액세스될 수 있다. 라이선스 관리 파일 및 리스트 파일에 대한 상세한 내용은 후술될 것이다.

라이선스 영역(1415A)에는, 라이선스 (라이선스 키 K_c, 액세스 제한 정보 AC_m, 및 라이선스 ID)가 기록되어 있는 기록 유닛에서의, 상기 라이선스를 제외한 라이선스 - 엔트리(entry)라고 불림 - 들이 저장된다. 라이선스에 대하여 액세스가 유효하면, 라이선스가 저장될 경우 또는 라이선스가 기록될 경우의 엔트리는 엔트리 번호를 통해 지정된다.

데이터 영역(1415)을 제외한 구조 전체는 불법 변경 방지 모듈 영역(tamper resistant module region)을 형성한다.

컨트롤러(1420)는 데이터를 버스 BS2를 통해서 외부 소스로/로부터 전송하고, 각종 정보를 버스 BS2를 통해서 수신하여 메모리 카드(110)의 동작을 제어한다. K_m 보유 유닛(1421)은 클래스 비밀 복호 키 K_{m5}를 저장한다. 인터페이스(1424)는 단말(1426)을 통해서 신호를 메모리 인터페이스(1026)로/로부터 송신/수신한다. 복호화 처리 유닛(1422)은 K_m 보유 유닛(1421)으로부터의 클래스 비밀 복호 키 K_{m5}를 사용하여 인터페이스(1424)로부터 버스 BS2 상으로 인가된 데이터를 복호화하고, 셀룰라 폰(100)이 프로그램을 저장할 때 생성된 세션 키 K_{s1}을 점점 Pa에 제공한다.

메모리 카드인 기록 장치에 비밀 키를 제공함으로써, 암호화된 라이선스 키 뿐만 아니라 셀룰라 폰(100)으로부터 전송된 콘텐츠 데이터의 관리는 메모리 카드에 기초하여 달성될 수 있다.

도 1의 통신 시스템의 각 세션의 동작을 이하 설명한다.

· 프로그램 저장

도 1의 통신 시스템에 있어서 셀룰라 폰(100)으로부터의 암호화된 콘텐츠 데이터 및 라이선스를 메모리 카드(110)로 기록하는 동작을 이하 설명한다. 또한, 이 동작은 "저장(store)" 이라고 지칭된다.

도 6 및 도 7은 도 1의 통신 시스템에 있어서 셀룰라 폰(100)으로부터의 프로그램을 메모리 카드(100)로 저장하는 동작을 설명하는 흐름도이다.

도 6의 제1 흐름도를 참조하면, 셀룰라 폰(100)의 사용자는 키 조작 유닛(1018)을 통해서 지정한 콘텐츠 데이터를 저장하는 요구를 입력한다 (단계 S100).

콘텐츠 데이터 저장 요구 입력에 응답하여, 컨트롤러(1022)는 버스 BS1과 메모리 카드 인터페이스(1026)를 통해서 인증 데이터 전송 요구를 메모리 카드(110)로 송신한다 (단계 S102). 메모리 카드(110)의 컨트롤러(1420)는 단말(1426), 인터페이스(1424), 및 버스 BS2를 통해서 인증 데이터 전송 요구를 수신한다 (단계 S104). 컨트롤러(1420)는 버스 BS2를 통해서 인증 데이터 보유 유닛(1400)으로부터의 인증 데이터 {K_{Pm5}//C_{m5}}K_{Pa}를 판독하고, 이 인증 데이터 {K_{Pm5}//C_{m5}}K_{Pa}를 버스 BS2, 인터페이스(1424), 및 단말(1426)을 통해서 출력한다 (단계 S106).

셀룰라 폰(100)의 컨트롤러(1022)는 메모리 카드 인터페이스(1026)와 버스 BS1을 통해서 메모리 카드(110)로부터 인증 데이터 {K_{Pm5}//C_{m5}}K_{Pa}를 수신한다 (단계 S108). 수신된 인증 데이터 {K_{Pm5}//C_{m5}}K_{Pa}는 복호화 처리 유닛(1028)에 인가된다. 복호화 처리 유닛(1028)은 인증 키 보유 유닛(1030)으로부터의 공개 인증 키 K_{Pa}를 사용하여 인증 데이터 {K_{Pm5}//C_{m5}}K_{Pa}를 복호화한다 (단계 S110). 컨트롤러(1022)는 적절한 장치를 이용하여 복호화 처리 유닛(1028)의 복호화 처리 결과로부터 그 유효성을 확인하도록, 암호화된 인증 데이터를 수신할 지를 정하는 인증 처리를 수행한다 (단계 S112). 적합한 인증 데이터라고 판정되면, 컨트롤러(1022)는 클래스 공개 암호 키 K_{Pm5} 및 클래스 증명서 C_{m5}를 인증하고 수리한다. 다음으로, 제어는 후속 처리로 진행된다 (단계 S114). 인증 데이터가 적합하지 않은 경우에는, 인증되지 않은 상태로 식별되고, 클래스 공개 암호 키 K_{Pm5} 및 클래스 증명서 C_{m5}를 수리하지 않고 저장 동작을 종료한다 (단계 S162).

인증 처리가 수행되어 프로그램이 저장될 메모리 카드(110)가 적합한 인증 데이터를 갖고 있다고 증명되면, 난수 키 생성 유닛(1032)은 프로그램을 저장하기 위한 세션 키 K_{s1}을 생성한다 (단계 S114). 암호화 처리 유닛(1034)은 복호화 처리 유닛(1028)으로부터의 공개 암호 키 K_{Pm5}를 사용하여 난수 키 생성 유닛(1032)으로부터의 세션 키 K_{s1}을 암호화한다. 암호화된 데이터 {K_{s1}}K_{m5}는 버스 BS1 상으로 출력된다. 컨트롤러(1022)는 라이선스 ID를 생성하고 (단계 S118), 생성된 라이선스 ID 및 암호화된 데이터 {K_{s1}}K_{m5}를 라인센스 ID//{K_{s1}}K_{m5}로서 암호화 처리 유닛(1034)으로부터 메모리 카드(110)로 버스 BS1 및 메모리 카드 인터페이스(1026)를 통해서 전송한다 (단계 S120).

메모리 카드(110)의 컨트롤러(1420)는 단말(1426), 인터페이스(1424), 및 버스 BS2를 통해서 라이선스 ID//{K_{s1}}K_{m5}를 수신한다 (단계 S122). 수신된 암호화된 데이터 {K_{s1}}K_{m5}는 버스 BS2를 거쳐 복호화 처리 유닛(1422)에 인가된다. 복호화 처리 유닛(1422)은 K_m 보유 유닛(1421)으로부터의 비밀 복호 키 K_{m5}를 사용하여, 암호화된 데이터 {K_{s1}}K_{m5}를 복호화하고, 셀룰라 폰(100)에서 생성된 세션 키 K_{s1}을 수리한다 (단계 S124).

컨트롤러(1420)의 제어 하에서, 난수 키 생성 유닛(1418)은 세션 키 K_{s2}를 생성한다 (단계 S126). 암호화 처리 유닛(1406)은 스위치(1442)의 접점 P_a를 통해서 수신된 세션 키 K_{s1}을 사용하여 스위치(1446)의 연속 스위칭 접점 P_c 및 P_d에 의해 수신된 세션 키 K_{s2} 및 공개 암호 키 K_{Pmc6}를 암호화한다. 암호화된 데이터 {K_{s2}//K_{Pmc6}}K_{s1}은 버스 BS2 상으로 출력된다. 컨트롤러(1420)는 암호화된 데이터 {K_{s2}//K_{Pmc6}}K_{s1}을 버스 BS2, 인터페이스(1424), 및 단말(1426)을 통해서 셀룰라 폰(100)으로 전송한다 (단계 S128).

셀룰라 폰(100)의 컨트롤러(1022)는 메모리 카드 인터페이스(1026) 및 버스 BS1을 통해서 암호된 데이터 {K_{s2}//K_{Pmc6}}K_{s1}을 수신한다 (단계 S130). 수신된 암호화된 데이터 {K_{s2}//K_{Pmc6}}K_{s1}은 버스 BS1을 통해서 복호화 처리 유닛(1036)에 인가된다. 복호화 처리 유닛(1036)은 난수 키 생성 유닛(1032)에 의해 생성된 세션 키 K_{s1}을 사용하여 암호화된 데이터 {K_{s2}//K_{Pmc6}}K_{s1}을 복호화하고, 세션 키 K_{s2} 및 공개 암호 키 K_{Pmc6}를 수리한다 (단계 S132).

메모리 카드(110)에서 생성된 세션 키 Ks2 및 메모리 카드(110)에 고유한 공개 암호 키 KPmc6의 수리가 증명되면, 컨트롤러(1022)는 라이선스 키 Kc를 생성하도록 난수 키 생성 유닛(1032)을 제어한다. 난수 키 생성 유닛(1032)은 라이선스 키를 생성한다 (단계 S134). 다음으로, 컨트롤러(1022)는 액세스 제한 정보 ACm을 사용 회수를 "1"로 제한하도록 설정한다 (단계 S136). 컨트롤러(1022)는 버스 BS1을 통해서 메모리(1024)로부터 콘텐츠 데이터 Dc를 판독한다. 판독된 콘텐츠 데이터 Dc는 버스 BS1을 통해서 암호화 처리 유닛(1038)에 인가된다. 암호화 처리 유닛(1038)은 난수 키 생성 유닛(1032)으로부터의 라이선스 키 Kc를 사용하여 버스 BS1을 통해서 수신된 콘텐츠 데이터 Dc를 암호화한다. 암호화된 콘텐츠 데이터 {Dc}Kc는 버스 BS1 상으로 출력된다 (단계 S138). 컨트롤러(1022)는 버스 BS1 상의 암호화된 데이터 {Dc}Kc를 메모리 카드 인터페이스(1026)를 통해서 메모리 카드(110)로 전송한다 (단계 S140).

메모리 카드(110)의 컨트롤러(1420)는 단말(1426), 인터페이스(1424), 및 버스 BS2를 통해서 암호화된 콘텐츠 데이터 {Dc}Kc를 수신한다. 수신된 암호화된 데이터 {Dc}Kc는 버스 BS2를 통해서 메모리(1415)의 데이터 영역(1415B)에 저장된다 (단계 S142).

다음으로, 셀룰라 폰(100)의 컨트롤러(1022)는 버스 BS1을 통해서 메모리(1024)에 저장된 콘텐츠 데이터를 삭제한다 (단계 S144).

도 7의 흐름도를 참조하면, 컨트롤러(1022)는 라이선스 ID 및 액세스 제한 정보 ACm을 버스 BS1을 통해서 암호화 처리 유닛(1040)에 공급한다. 암호화 처리 유닛(1040)은 복호화 처리 유닛(1036)으로부터의 공개 암호 키 KPmc6를 사용하여 버스 BS1을 통해서 수신된 라이선스 ID 및 액세스 제한 정보 ACm 및 난수 키 생성 유닛(1032)로부터의 라이선스 키 Kc를 암호화한다. 암호화된 데이터 {라이선스 ID//Kc//ACm}Kmc6는 스위치(1050)의 접점 Pb로 출력된다 (단계 S146). 다음으로, 암호화 처리 유닛(1042)은 스위치(1052)의 접점 Pc를 통해서 수신된 세션 키 Ks2를 사용하여 스위치(1050)의 접점 Pb를 통해서 수신된 암호화된 데이터 {라이선스 ID//Kc//ACm}Kmc6를 암호화한다. 암호화된 데이터 {{라이선스 ID//Kc//ACm}Kmc6}Ks2는 버스 BS1에 공급된다 (단계 S148). 다음으로, 컨트롤러(1022)는 버스 BS1 상의 암호화된 데이터 {{라이선스 ID//Kc//ACm}Kmc6}Ks2를 메모리 카드 인터페이스(1026)를 통해서 메모리 카드(110)로 전송한다 (단계 S150).

메모리 카드(110)의 컨트롤러(1420)는 단말(1426), 인터페이스(1424), 및 버스 BS2를 통해서 암호화된 데이터 {{라이선스 ID//Kc//ACm}Kmc6}Ks2를 수신한다 (단계 S152). 컨트롤러(1420)는 암호화된 데이터 {{라이선스 ID//Kc//ACm}Kmc6}Ks2를 버스 BS2를 통해서 복호화 처리 유닛(1412)에 제공한다. 복호화 처리 유닛(1412)은 세션 키 Ks2를 사용하여, 암호화된 데이터 {{라이선스 ID//Kc//ACm}Kmc6}Ks2를 복호화하고, 암호화된 데이터 {라이선스 ID//Kc//ACm}Kmc6를 수리한다 (단계 S154). 복호화 처리 유닛(1404)은 Kmc 보유 유닛(1402)으로부터 비밀 복호 키 Kmc6를 사용하여, 복호화 처리 유닛(1412)에 의해 복호화된 암호화된 데이터 {라이선스 ID//Kc//ACm}Kmc6를 복호화하고, 라이선스 ID, 라이선스 키 Kc, 및 액세스 제한 정보 ACm을 수리한다 (단계 S156).

다음으로, 셀룰라 폰(100)의 컨트롤러(1022)는 라이선스를 저장하기 위해 엔트리 번호를 결정한다. 결정된 엔트리 번호 및 저장 요구가 버스 BS1과 메모리 카드 인터페이스(1026)를 통해서 메모리 카드(110)로 전송된다 (단계 S158).

메모리 카드(110)의 컨트롤러(1420)는 단말(1426), 인터페이스(1424), 및 버스 BS2를 통해서 엔트리 번호 및 라이선스 저장 요구를 수신하고, 라이선스 ID, 라이선스 키 Kc, 및 액세스 제한 정보 ACm을 메모리(1415)의 라이선스 영역(1415A)에서 지정된 엔트리에 저장한다 (단계 S160). 다음으로, 메모리 카드(110)로의 프로그램 저장 동작이 종료한다 (단계 S162).

배신 서버(10)로부터 수신되어 셀룰라 폰(100)의 메모리(1024)에 저장된 콘텐츠 데이터 Dc에 대응하는 프로그램을 저장하는 경우에 메모리 카드(110)가 적합한 메모리 카드인지의 여부가 판정된다. 적합한 메모리 카드라고 증명된 경우에만 (도 6의 단계 S112 참조) 콘텐츠 데이터 Dc가 메모리 카드(110)로 전송된다 (도 6의 단계 S140 참조). 따라서, 콘텐츠 데이터 Dc에 대응하는 프로그램은 적합하지 않은 메모리 카드에는 저장되지 않게 되어, 충분히 보호된다.

프로그램이 메모리 카드(110)에 저장될 경우에는, 콘텐츠 데이터 Dc 및 라이선스 (라이선스 키 Kc, 라이선스 ID, 및 액세스 제한 정보 ACm)가 암호화된 형태로 메모리 카드(110)에 전송된다 (도 6의 단계 S140과, 도 7의 단계 S146, S148, 및 S150 참조). 라이선스는 대상 메모리 카드(destination memory card)에 의해 제한된 공개 복호 키 Kmc6를 사용하여 복호화될 수 있는 암호화된 데이터로서 메모리 카드(110)로 전송된다. 프로그램과 라이선스가 암호화된 형태로 메모리 카드(110)로 전송되므로, 충분한 보호가 이루어진다. 암호화된 콘텐츠 데이터 {Dc}Kc 및 암호화된 라이선스가 어떤 원인에 의해서 대상 메모리 카드(110)로부터 추출되더라도, 암호화된 라이선스는 비밀 복호 키 Kmc6 없이는 복호화될 수 없으므로, 필요한 라이선스 키 Kc가 획득될 수 없다. 따라서, 암호화된 콘텐츠 데이터 {Dc}Kc는 콘텐츠 데이터 Dc를 획득하도록 복호화될 수 없다.

암호화된 데이터 {Dc}Kc가 메모리 카드(110)로 전송된 후에, 메모리(1024)에 저장되어 있던 이전의 콘텐츠 데이터 Dc가 삭제된다 (도 6의 단계 S144 참조). 이것은 콘텐츠 데이터 Dc가 메모리 카드(110)에만 저장된다는 것을 의미한다. 프로그램은 사용될 수 있도록 복사될 수 없다. 셀룰라 폰(100)의 난수 키 생성 유닛(1032), 암호화 처리 유닛(1038), 및 복호화 처리 유닛(1048)은 휘발성 메모리로 형성된다. 암호화된 콘텐츠 데이터 {Dc}Kc를 복호화하는 데 필요한 라이선스 키 Kc는 메모리 카드(110)에만 저장된다.

· 프로그램 재저장

메모리 카드(110)에 저장되어 있는 콘텐츠 데이터 Dc를 셀룰라 폰(100)에 기록하는 것은 도 8을 참조로 해서 설명될 것이다. 이 동작은 "재저장" 이라고 불린다. 이 설명은, 도 8의 과정에 앞서 셀룰라 폰(100)의 사용자가 메모리 카드(110)로부터 획득된 콘텐츠(프로그램)를 결정하였고, 콘텐츠 파일을 식별하였고, 메모리 카드(110)의 데이터 영역(1415B)에 기록된 리스트 파일에 따라서, 라이선스 관리 파일을 이미 획득하였다는 가정에 기초한다.

키 조작 유닛(1018)을 통해 암호화된 콘텐츠 데이터 입력을 사용자에게 의해 셀룰라 폰(100)으로 특정화하는 재저장 요구에 응답해서(단계 S200), 컨트롤러(1022)는 버스 BS1을 통해 인증(authentication) 데이터 보유 유닛(1500)으로부터 인증 데이터 {Kp1//Cp1}KPa를 획득한다. 인증 데이터 {Kp1//Cp1}KPa는 메모리 카드 인터페이스(1026)을 통해 메모리 카드(110)로 전송된다(단계 S202).

메모리 카드(110)의 컨트롤러(1420)는 터미널(1426), 인터페이스(1424) 및 버스 BS2를 통해 인증 데이터 {Kp1//Cp1}KPa를 수신한다(단계 S204). 수신된 인증 데이터 {Kp1//Cp1}KPa는 버스 BS2를 통해 복호(decryption) 처리 유닛(1408)에 인가된다. 인증 처리 유닛(1408)은 인증 키 보유 유닛(1414)로부터 공공 인증 키 KPa를 사용하여 수신된 인증 데이터 {Kp1//Cp1}KPa를 복호한다(단계 S206). 컨트롤러(1420)는 복호화 처리 유닛(1408)의 복호된 처리 결과로부터 인증 프로세스를 수행한다. 특히, 인증 데이터 {Kp1//Cp1}KPa가 적절한 인증 데이터인지를 결정하는 인증 프로세스가 처리된다(단계 S208). 복호화 불가능하다면, 제어는 단계 S250으로 진행하고, 재저장 동작은 종료한다.

인증 데이터가 복호될 수 있는 경우에, 메모리 카드(110)의 난수 키 발생 유닛(random number key generation unit; 1418)은 재저장 동작을 위해 세션(session) 키 Ks3을 발생한다(단계 S210). 복호화 처리 유닛(1410)은, 난수 키 발생 유닛(1418)으로부터 세션 키 Ks3을 제공하고, 복호화 처리 유닛(1408)에서 버스 BS2상에서 복호된 공공 암호

화 키 Kp1을 이용해서 암호화된 {Ks3}Kp1을 제공한다. 그리고, 컨트롤러(1420)는 인터페이스(1424) 및 터미널(1426)을 통해 메모리 카드 인터페이스(1026)에 {Ks3}Kp1을 출력한다(단계 S212). 셀룰라 폰(100)의 컨트롤러(1022)는 메모리 카드 인터페이스(1026)를 통해 {Ks3}Kp1을 접수한다(단계 S214). 컨트롤러(1022)는 복호화 처리 유닛(1044)에 복호된 데이터 {Ks3}Kp1을 제공한다. 복호화 처리 유닛(1044)은 Kp 보유 유닛(1046)으로부터 비밀 복호 키 Kp1을 사용해서, 암호화된 데이터 {Ks3}Kp1을 복호하고, 세션 키 Ks3를 접수한다(단계 S216). 복호화 처리 유닛(1044)은 스위치(1052)의 컨택트 Pd에 세션 키 Ks3를 출력한다.

그리고, 난수 키 생성기(1032)는 재저장 동작을 위해 세션 키 Ks4를 발생한다(단계 S218). 세션 키 Ks4는 스위치(1050)의 컨택트 Pa에 대한 출력이다. 암호화 처리 유닛(1042)은 스위치(1050)의 컨택트 Pa를 통해 수신된 세션 키 Ks4를 암호화하도록, 스위치(1052)의 컨택트 Pd를 통해 수신된 세션 키 Ks3를 사용한다. 암호화된 데이터 {Ks4}Ks3는 버스 BS1상에서 출력된다(단계 S220). 컨트롤러(1022)는 버스 BS1상의 암호화된 데이터 {Ks4}Ks3를 메모리 카드 인터페이스(1026)를 통해 메모리 카드(110)로 전송한다(단계 S222).

메모리 카드(110)의 컨트롤러(1420)는 터미널(1426), 인터페이스(1424) 및 버스 BS2를 통해 암호화된 데이터 {Ks4}Ks3를 수신한다(단계 S224). 수신된 암호화된 데이터 {Ks4}Ks3는 버스 BS2를 통해 복호화 처리 유닛(1412)에 인가된다. 복호화 처리 유닛(1412)은 난수 키 발생 유닛(1418)으로부터 세션 키 Ks3를 사용해서 암호화된 데이터 {Ks4}Ks3를 복호하고, 셀룰라 폰(100)에서 발생된 세션 키 Ks4를 접수한다(단계 S226).

이에 응답하여, 셀룰라 폰(100)의 컨트롤러(1022)는 메모리 카드 인터페이스(1026)를 통해 메모리 카드(110)에 암호화된 콘텐츠 데이터 {Dc}Kc의 출력 요구 및 엔트리 번호(entry number)를 전송한다(단계 S228).

메모리 카드(110)의 컨트롤러(1420)는 터미널(1426), 인터페이스(1424) 및 버스 BS2를 통해 엔트리 번호 및 출력 요구를 수신한다. 수신된 엔트리에 저장된 라이선스 ID, 라이선스 키 Kc 및 접근 제한 정보 ACm은 버스 BS2를 통해 획득된다(단계 S230). 컨트롤러(1420)는 접근 제한 정보 ACm에서 사용 횟수의 번호를 참조한다. 사용 번호가 "0"으로 설정되면, 사용이 불가능하다고 결정되고, 즉, 암호화된 데이터 {Dc}Kc가 셀룰라 폰(100)으로 출력될 수 없게 된다. 따라서, 재저장 동작은 종료한다(단계 S250). 컨트롤러(1420)는, 사용 카운트가 "1"로 설정되면, 암호화된 데이터 {Dc}Kc가 셀룰라 폰(100)으로 출력될 수 있다고 결정하고, 다음 단계 S234로 진행한다(단계 S232). 암호화된 콘텐츠 데이터 {Dc}Kc가 메모리 카드(110)에 전송될 때, 사용 카운트가 "1"로 설정(도 6의 단계 S136)되기 때문에, 컨트롤러(1420)는 라이선스 키 Kc가 단계 S232에서 셀룰라 폰(100)으로 출력될 수 있다고 결정한다. 그리고, 컨트롤러(1420)는 접근 제한 정보 ACm의 사용 카운트를 "0"으로 설정, 즉, "사용 불가능"으로 설정하고, 엔트리내의 접근 제한 정보 ACm를 수정한다(단계 S234). 따라서, 라이선스 키 Kc는 이후에 메모리 카드(110)로부터 출력될 수 없다.

컨트롤러(1420)는 버스 BS2를 통해 암호화 처리 유닛(1406)으로 라이선스 키 Kc를 제공한다. 암호화 처리 유닛(1406)은 버스 BS2상에 암호화된 데이터 {Kc}Ks4를 출력하기 위해서, 스위치(1442)의 컨택트 Pb를 통해서 라이선스 키 Ks4를 사용하여 라이선스 키 Kc를 암호화한다. 컨트롤러(1420)는 인터페이스(1424) 및 터미널(1426)을 통해서 셀룰라 폰(100)으로 버스 BS2상의 암호화된 데이터 {Kc}Ks4를 전송한다(단계 S236).

셀룰라 폰(100)의 컨트롤러(1022)는 메모리 카드 인터페이스(1026) 및 버스 BS1을 통해 암호화된 데이터 {Kc}Ks4를 수신하고(단계 S238), 접수된 암호화된 데이터 {Kc}Ks4를 버스 BS1를 통해 복호화 처리 유닛(1036)에 제공한다. 복호화 처리 유닛(1036)은 라이선스 키 Kc를 접수하기 위해서, 난수 키 생성기(1032)로부터 세션 키 Ks4를 사용해서 암호화된 데이터 {Kc}Ks4를 복호한다(단계 S240). 이에 응답해서, 컨트롤러(1022)는 메모리 카드 인터페이스(1026)를 통해서 암호화된 콘텐츠 데이터 {Dc}Kc의 출력 응답을 메모리 카드(110)로 전송한다(단계 S242).

메모리 카드(110)의 컨트롤러(1420)는, 버스 BS2를 통해 메모리(1415)내의 데이터 영역(1415B)으로부터 암호화된 콘텐츠 데이터 {Dc}Kc를 얻기 위해, 터미널(1426), 인터페이스(1424) 및 버스 BS2를 통해 암호화된 콘텐츠 데이터 {Dc}Kc의 출력 요구를 수신하고, 인터페이스(1424) 및 터미널(1426)을 통해 메모리 카드(110)로 암호화된 콘텐츠 데이터 {Dc}Kc를 전송한다(단계 S244).

셀룰라 폰(100)의 컨트롤러(1022)는 메모리 카드 인터페이스(1026)을 통해 암호화된 콘텐츠 데이터 {Dc}Kc를 수신하고(단계 S246), 버스 BS1을 통해 복호화 처리 유닛(1048)로 수신된 암호화된 콘텐츠 데이터 {Dc}Kc를 전송한다. 복호화 처리 유닛(1048)은 콘텐츠 데이터 Dc를 획득하기 위해, 복호화 처리 유닛(1036)으로부터 라이선스 키 Kc를 사용해서 암호화된 콘텐츠 데이터 {Dc}Kc를 복호화한다. 컨트롤러(1022)는 버스 BS1을 통해서 메모리(1024)에 콘텐츠 데이터 Dc를 전송한다(단계 S248). 전체 동작은 종료한다(단계 S250).

콘텐츠 데이터 Dc로서의 메모리 카드(110)내에 저장된 셀룰라 폰(100)으로부터의 프로그램이 메모리 카드(110)로부터 출력되고, 셀룰라 폰(100)에 다시 저장될 때, 콘텐츠 데이터 Dc의 라이선스 사용 카운트는 "0"으로 설정된다(도 8의 단계 S234 참조). 따라서, 라이선스는 출력될 수 없고, 암호화된 콘텐츠 데이터 {Dc}Kc는 이후에 더이상 복호될 수 없다. 이는 실질적으로 메모리 카드(110)로부터 콘텐츠 데이터를 삭제하는 것과 동일하다.

따라서, 콘텐츠 데이터 Dc가 메모리 카드(110)에 저장되면, 라이선스에서 사용 카운트가 "1"로 설정된 암호화된 콘텐츠 데이터 {Dc}Kc는 메모리 카드(110)내에 저장된다. 콘텐츠 데이터 Dc가 메모리 카드(110)로부터 출력되어야 할 때, 메모리 카드(110)내에 저장된 라이선스의 사용 카운트는 라이선스의 출력과 동시에 "0"으로 설정되고, 이에 따라, 사용은 허가되지 않는다. 따라서, 라이선스 출력이 이후에 금지되면, 메모리 카드(110)내에 남아 있는 콘텐츠 데이터 Dc(특히, 암호화된 콘텐츠 데이터 {Dc}Kc 및 라이선스)는 더이상 사용될 수 없다.

결과적으로, 사용될 수 있는 콘텐츠 데이터 Dc는 셀룰라 폰(100)의 내장 메모리로 콘텐츠 데이터의 재저장 동작에서 셀룰라 폰(100)의 내장 메모리내에 저장된 데이터뿐이다.

메모리 카드(110)내에 남아 있는 암호화된 콘텐츠 데이터 {Dc}Kc가 복사되더라도, 라이선스 키 Kc는 메모리 카드(110)로부터 판독될 수 없는 사용에 대한 복사된 암호화된 콘텐츠 데이터 {Dc}Kc를 요구한다. 이는 복사된 암호화된 콘텐츠 데이터 {Dc}Kc가 복호될 수 없고, 콘텐츠 데이터 Dc가 사용될 수 없다는 것을 의미한다.

본 발명은, 또 다른 장치(예를 들어, 셀룰라 폰)로부터 전송된 콘텐츠 데이터 Dc를 저장하는 장치(예를 들어, 메모리 카드)가 콘텐츠 데이터를 출력할 때, 그 자신의 영역에 저장된 콘텐츠 데이터 Dc는 이후에 삭제되거나, 사용이 금지되는 것을 특징으로 한다. 메모리 카드내의 콘텐츠 데이터 Dc의 사용 횟수 번호를 제한하고, 제한된 횟수 번호에 의해 결정된 사용 카운트를 "0"으로 수정함으로써, 콘텐츠 데이터 Dc의 사용을 위해 요구되는 라이선스 키 Kc는 실질적으로 삭제된다. 이 삭제 방법은, 메모리 카드가 셀룰라 폰과 같은 장치에 부착되는 방식으로 사용되고, 메모리 카드에 저장된 콘텐츠 데이터 Dc가 메모리 카드로부터 사용을 위해 출력되어야만 한다는 점에서 장점을 가지고 있다.

메모리 카드로부터 콘텐츠 데이터 Dc의 출력으로서, 메모리 카드로부터 콘텐츠 데이터 Dc를 삭제하는 방식, 또는 삭제와 동등하게 제한된 방식은 본 발명에서 가변적이다.

"0"으로 설정된 사용 카운트를 가지는 라이선스에 상응하는 콘텐츠 데이터가 삭제되는 것과 실질적으로 동등하더라도, 라이선스 키 및 콘텐츠 키는 여전히 메모리 카드내에 존재한다. 셀룰라 폰으로부터 메모리 카드로 전체 콘텐츠 데이터를 전송하라는 요구가 있는 경우, 전체 콘텐츠 데이터를 전송해야 하지 않고, 사용 카운트만을 "1"로 재설정하면 된다. 그러므로, 전송 프로세스의 속도가 증가한다.

프로그램이 셀룰라 폰으로부터 메모리 카드로 저장될 수 있기 때문에, 사용자는, 셀룰라 폰이 바뀌었을 경우, 자신의 또 다른 셀룰라 폰으로 동일한 프로그램을 실행할 수 있다. 사용자가 자신의 셀룰라 폰을 다른 것으로 바꾸었더라도, 사용자는 동일한 프로그램을 배신 서버로부터 다시 수신할 필요가 없다.

또한, 셀룰라 폰으로부터 메모리 카드에 프로그램을 저장함으로써, 사용자의 편의성은 프로그램을 복사하는 것을 금지하면서 증진될 수 있다.

도 9는 메모리 카드(110)의 메모리(1415)내의 라이선스 영역(1415A) 및 데이터 영역(1415B)을 도시한다. 데이터 영역(1415B)에는 리스트 파일(160), 콘텐츠 파일들(1611 - 161n) 및 라이선스 관리 파일들(1621 - 162n)이 저장된다. 콘텐츠 파일들(1611 - 161n)은 수신된 암호화된 콘텐츠 데이터 {Dc}Kc를 하나의 파일로서 기록한다. 라이선스 관리 파일들(1621 - 162n)은 콘텐츠 파일들(1611 - 161n)에 상응해서 각각 기록된다.

암호화된 콘텐츠 데이터 및 셀룰라 폰(100)으로부터의 라이선스를 수신하면, 메모리 카드(110)는 암호화된 콘텐츠 데이터 및 메모리(1415)내의 라이선스를 기록한다.

메모리 카드(110)로 전송된 암호화된 콘텐츠 데이터의 라이선스는 메모리(1415)의 라이선스 영역(1415A)내의 엔트리 번호에 의해 특정되는 영역내에 기록된다. 엔트리 번호는 메모리(1415)내의 데이터 영역(1415B)에 기록된 리스트 파일(160)의 라이선스 관리 파일을 판독함으로써 획득될 수 있다. 상응하는 라이선스는 획득된 엔트리 번호에 따라서 라이선스 영역(1415A)으로부터 판독될 수 있다.

예를 들어, 엔트리 번호 "0"은 콘텐츠 파일(1611)에 상응하는 라이선스 관리 파일(1621)을 판독함으로써 획득될 수 있다. 콘텐츠 파일(1611)에 저장된 암호화된 콘텐츠 데이터 {Dc}Kc의 라이선스는 라이선스 영역(1415A)내의 엔트리 번호 "0"에 의해 특정되는 영역으로부터 획득될 수 있다. 이는 다른 엔트리 번호에 의해 특정되는 영역내에 기록되는 라이선스에도 동일하게 적용된다.

발명의 효과

상술된 설명은 프로그램이 셀룰라 폰으로부터 메모리 카드로 저장되고, 그 후 재저장되는 경우에 기초한다. 본 발명은 프로그램이 셀룰라 폰으로부터 또 다른 셀룰라 폰으로 전송되는 경우도 포함한다. 이 경우에, 내장 메모리에 저장된 프로그램은, 상술된 셀룰라 폰(100)과 유사하게, 프로그램이 다른 셀룰라 폰으로 전송된 후에 삭제되어야 한다.

본 발명의 실시예에 따라서, 배신 서버로부터 프로그램을 수신하는 셀룰라 폰은, 수신된 프로그램이 메모리 카드로 기록되어야 할 때, 그것의 저장된 프로그램을 삭제한다. 메모리 카드는, 프로그램이 셀룰라 폰으로 저장되어야 할 때, 그것의 저장된 프로그램을 사용할 수 없게 한다. 따라서, 프로그램의 복사가 금지되면서, 프로그램은 또 다른 장치로 전송될 수 있다.

본 발명의 콘텐츠 데이터는, 프로그램을 포함하지만, 이로써 제한되는 것은 아니다. 데이터 터미널을 통해 재생산될 수 있는 모든 저작물이 대상이 된다. 상술된 설명은 셀룰라 폰과 메모리 카드 사이의 통신 프로토콜을 가지는 통신 시스템에 기초하였지만, 셀룰라 폰과 배신 서버 사이의 통신 능력이 항상 필요한 것은 아니다. 콘텐츠 데이터는 와이어를 통해 배신 서버로부터 획득될 수 있다. 또한, 콘텐츠 데이터의 재생산 능력이 항상 필요한 것은 아니다.

본 발명이 상세하게 기술되고 예시되었지만, 이것은 도시 및 예시의 방식으로, 제한되는 방식으로 사용된 것은 아니며, 본 발명의 정신 및 범위는 첨부된 청구항에 의해서만 제한된다.

(57) 청구의 범위

청구항 1.

평문(plaintext)으로 취득된 콘텐츠 데이터의 암호화된 버전인 암호화된 콘텐츠 데이터와 상기 암호화된 콘텐츠 데이터를 복호화하기 위해 필요한 라이선스 키를 생성하고, 상기 암호화된 콘텐츠 데이터와 상기 라이선스 키를 데이터 기록 장치(110)에 대해 전송하는 데이터 단말 장치에 있어서,

지시를 입력하기 위한 조작 유닛(1018),

상기 데이터 기록 장치(100)로 데이터를 전송하기 위한 인터페이스(1026),

상기 콘텐츠 데이터를 평문 형태로 저장하는 저장 유닛(1024),

상기 라이선스 키를 생성하고, 생성된 라이선스 키를 사용하여 상기 콘텐츠 데이터를 암호화함으로써 상기 암호화된 콘텐츠 데이터를 생성하는 암호화된 콘텐츠 생성 유닛(1032, 1038),

상기 라이선스 키를 포함하는 라이선스와, 상기 데이터 기록 장치(110)로부터의 상기 라이선스 키 출력 횟수를 1회로 제한하는 제어 정보를 생성하는 라이선스 생성 유닛(1022),

상기 라이선스 생성 유닛(1022)에 의해 생성된 라이선스를 암호화하여 암호화된 라이선스를 생성하거나 또는 상기 데이터 기록 장치(110)에 저장된 다른 암호화된 라이선스를 수신하고 복호화하며 다른 라이선스 키를 포함하는 암호화/복호화 처리 유닛(1028, 1034, 1036, 1038, 1040, 1042, 1044, 1046, 1048),

상기 데이터 기록 장치(110)에 저장된 다른 암호화된 콘텐츠 데이터를 수신하고, 상기 수신된 다른 암호화된 콘텐츠 데이터를 상기 암호화/복호화 처리 유닛(1028, 1034, 1036, 1038, 1040, 1042, 1044, 1046, 1048)로 부터 추출되고 복호화된 다른 라이선스 키를 사용하여 복호화하는 콘텐츠 데이터 복호화기(1048), 및

컨트롤 유닛(1022)

을 포함하고,

상기 컨트롤 유닛(1022)은 상기 조작 유닛(1018)을 통해 입력된 상기 데이터 기록 장치(110)로의 상기 콘텐츠 데이터의 전송 요구에 응답하여 상기 저장 유닛(1024)으로부터 평문으로 된 상기 콘텐츠 데이터를 상기 암호화된 콘텐츠 생성 유닛(1032, 1038) 내로 읽어내고(readout), 상기 인터페이스(1026)을 통하여 상기 암호화된 콘텐츠 데이터와 상기 암호화된 라이선스를 상기 데이터 기록 장치(110)로 전송하고, 상기 저장 유닛(1024)에 저장된 평문으로 된 콘텐츠 데이터를 삭제하는 것을 특징으로 하는 데이터 단말 장치.

청구항 2.

제1항에 있어서, 상기 암호화/복호화 처리 유닛(1028, 1034, 1036, 1038, 1040, 1042, 1044, 1046, 1048)은 상기 인터페이스(1026)를 통하여 상기 데이터 기록 장치(110)로부터 제공된 제1 세션 키를 사용하여 상기 라이선스를 암호화하여 암호화된 라이선스를 생성하는 암호화기(1042)를 포함하고,

상기 컨트롤 유닛(1022)은 상기 인터페이스(1026)를 통하여 상기 데이터 기록 장치(110)로부터 상기 제1 세션 키를 수신하고, 상기 데이터 기록 장치(110)로의 상기 암호화된 라이선스의 기록 동작시 상기 수신된 세션 키를 상기 암호화기에 제공하는 것을 특징으로 하는 데이터 단말 장치.

청구항 3.

제2항에 있어서, 상기 암호화/복호화 처리 유닛(1028, 1034, 1036, 1038, 1040, 1042, 1044, 1046, 1048)은

상기 데이터 기록 장치(110)와의 통신을 특정하기 위해 세션 키를 생성하는 세션 키 생성기(1032), 및

상기 세션 키 생성기(1032)에 의해 생성된 제2 세션 키를 사용하여 암호화된 데이터를 복호화하는 복호화기(1036)

를 더 포함하고,

상기 데이터 기록 장치(110)에 대한 상기 암호화된 라이선스의 기록 동작에서,

상기 세션 키 생성기(1032)가 상기 제2 세션 키를 생성하고,

상기 컨트롤 유닛(1022)은 상기 인터페이스(1026)를 통하여 상기 제2 세션 키를 상기 데이터 기록 장치(110)에 제공하고, 상기 인터페이스를 통하여 상기 데이터 기록 장치(110)로부터 상기 제2 세션 키(1026)에 의해 암호화된 상기 제1 세션 키를 수신하고, 상기 제2 세션 키에 의해 암호화된 상기 수신된 제1 세션 키를 상기 복호화기(1036)에 제공하는 것을 특징으로 하는 데이터 단말 장치.

청구항 4.

제3항에 있어서, 상기 암호화/복호화 처리 유닛(1028, 1034, 1036, 1038, 1040, 1042, 1044, 1046, 1048)은 상기 데이터 기록 장치(110)로부터 수신되고 고유한 제1 공개 키를 사용하여 데이터를 암호화하는 다른 암호화기를 더 포함하고,

상기 암호화된 라이선스를 상기 데이터 기록 장치(110)에 기록하는 동작에서,

상기 복호화기(1036)는 상기 제2 세션 키에 의해 암호화된 상기 제1 세션 키와, 상기 제2 세션 키를 사용하는 상기 제1 공개 키를 복호화하여 상기 제1 세션 키와 상기 제1 공개 키를 추출하고,

상기 다른 암호화기(1046)는 상기 제1 공개 키를 사용하여 상기 라이선스 생성 유닛(1022)에 의해 생성된 라이선스를 암호화하며,

상기 암호화기(1042)는 상기 제1 세션 키를 사용하여 상기 다른 암호화기(1040)의 출력을 수신하고 암호화하며, 상기 제1 세션 키에 의해 암호화된 상기 암호화된 라이선스 키를 생성하고,

상기 컨트롤 유닛(1022)은 상기 제2 세션 키를 상기 인터페이스(1026)를 통하여 상기 데이터 기록 장치(110)로 제공하고, 상기 인터페이스(1026)를 통하여 상기 데이터 기록 장치(110)로부터 상기 제2 세션 키에 의해 암호화된 상기 제1 세션 키를 수신하며, 상기 제2 세션 키에 의해 암호화된 상기 수신된 제1 세션 키와 상기 제1 공개 키를 상기 복호화기(1036)에 제공하는 것을 특징으로 하는 데이터 단말 장치.

청구항 5.

제2항에 있어서, 상기 암호화/복호화 처리 유닛(1028, 1034, 1036, 1038, 1040, 1042, 1044, 1046, 1048)은 제2 공개 키를 사용하여 데이터를 암호화하는 다른 암호화기(1034)를 더 포함하고,

상기 암호화된 라이선스의 상기 데이터 기록 장치(110)로의 기록 동작에서,

상기 다른 암호화기(1034)는 상기 제2 공개 키를 사용하여 상기 제2 세션 키를 암호화하고,

상기 컨트롤 유닛(1022)은 상기 인터페이스(1026)를 통하여 상기 데이터 기록 장치(110)로부터 상기 제2 공개 키를 포함하는 인증 데이터를 수신하고, 상기 수신된 데이터가 적당한 것으로 판정되면 상기 수신된 인증 데이터에 포함된 상기 제2 공개 키를 상기 다른 암호화기(1034)에 제공하고, 상기 다른 암호화기(1034)의 상기 제2 공개 키를 사용하여 암호화된 상기 제2 세션 키를 상기 인터페이스(1026)를 통하여 상기 데이터 기록 장치(110)로 제공하는 것을 특징으로 하는 데이터 단말 장치.

청구항 6.

제1항에 있어서, 상기 암호화/복호화 처리 유닛(1028, 1034, 1036, 1038, 1040, 1042, 1044, 1046, 1048)은
상기 데이터 기록 장치(110)와의 통신을 특정하기 위한 세션 키를 생성하는 세션 키 생성기(1032), 및
상기 세션 키 생성기(1032)에 의해 생성된 세션 키를 사용하여 암호화된 데이터를 복호화하는 복호화기(1036)
를 포함하고,

상기 데이터 기록 장치(110)로부터의 다른 암호화된 라이선스의 판독 동작에서,

상기 세션 키 생성기(1032)는 상기 제2 세션 키를 생성하고,

상기 컨트롤 유닛(1022)은 상기 세션 키 생성기(1032)에 의해 생성된 상기 세션 키를 상기 인터페이스(1026)를 통
해 상기 데이터 기록 장치(110)로 제공하고, 상기 인터페이스(1026)를 통해 상기 데이터 기록 장치(110)로부터 상기
세션 키에 의해 암호화된 상기 다른 암호화된 라이선스를 수신하고, 상기 수신된 다른 암호화된 라이선스를 복호화기에
제공하는 것을 특징으로 하는 데이터 단말 장치.

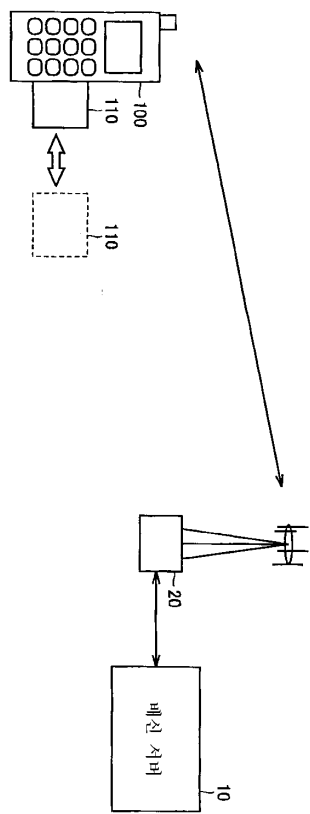
청구항 7.

제6항에 있어서, 상기 조작 유닛(1018)을 통해 입력되는 수신 요청에 응답하여 상기 데이터 기록 장치(110)에 제공될
인증 데이터를 저장하는 인증 데이터 보유 유닛(1030)을 더 포함하고,

상기 컨트롤 유닛(1022)은 상기 인증 데이터를 상기 인터페이스(1026)를 통하여 상기 데이터 기록 장치(110)로 제
공하고, 상기 인증 데이터가 상기 데이터 기록 장치(110)에서 인증되는 경우 상기 데이터 기록 장치(110)로부터 상기
다른 암호화된 콘텐츠 데이터와 상기 다른 암호화된 라이선스를 수신하는 것을 특징으로 하는 데이터 단말 장치.

도면

도면 1



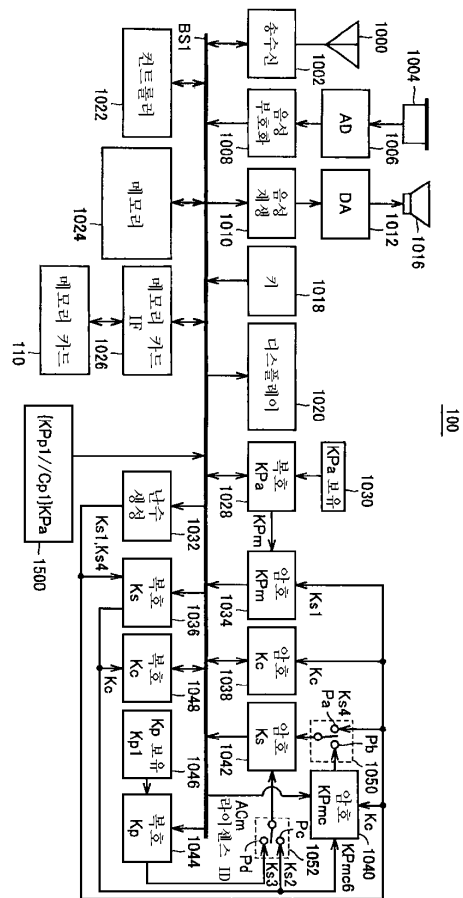
도면 2

기호	종류	속성	특성
Dc	콘텐즈 데이터	고유 콘텐즈	예 : 화상을 표시하기 위한 프로그램, Dc로서 매칭되고 데이터 단말 장치 또는 메모리 카드에 저장된 게임 프로그램
Kc	라이센스	고유 라이센스	라이센스 암호화 콘텐즈 데이터를 부호화하는 부호기
ACm	라이센스	고유 라이센스	제한 정보 라이선스 쿼트에 대한 제한 사항
콘텐즈 ID	라이센스	고유 라이센스	콘텐즈를 특정하기 위한 관리 코드
라이센스 ID	라이센스	고유 라이센스	라이센스를 특정하기 위한 관리 코드
라이센스	라이센스	고유 라이센스	Kc + ACm + 콘텐즈 ID + 라이선스 ID의 중첩

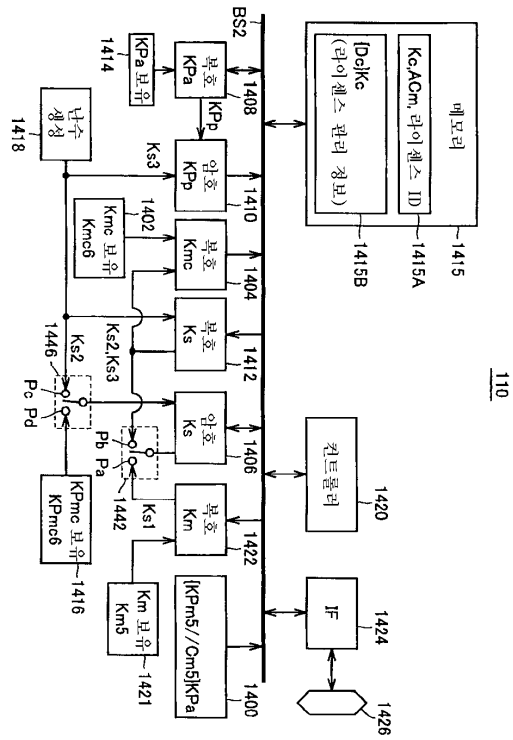
도면 3

데이터 단말 장치	기호	종류	속성	특성
	KPa	공개 인증키	시스템 공용	인증국에서 인증 데이터를 복호하는 기
	Ks1	공통키	채신 공통	메모리 카드로 문텐츠 데이터 및 라이선스의 저장시에 발생
	KPw	공개 암호키	고유 클래스	증명서 Cmw와 함께 인증국에서 암호화된 인증데이터로서 보유되는 w는 클래스를 식별하기 위한 식별자
	Kv	비밀 복호키	고유 클래스	공개 암호키 KPw에 대해 암호화된 데이터를 복호하는 비대칭 복호키
	Ks4	공통키	고유 채신	메모리 카드로부터의 문텐츠 데이터 및 라이선스 수신시에 발생
	Cv	증명서	클래스 증명서	데이터 단말 장치의 클래스 증명서 확인증을 갖는다. (Kv//Cv)KPw의 형식으로 출하시에 기록. * 데이터 단말 장치의 클래스이다 다르다.
메모리 카드	KPa	공개 인증키	시스템 공용	인증국에서 인증 데이터를 복호하는 기.
	KPw	공개 암호키	고유 클래스	데이터 단말 장치의 KPw와 동일
	Kmw	비밀 복호키	고유 클래스	인증 데이터로서 보유. w는 클래스를 식별하는 식별자 암호화 키 KPw에 의해 암호화된 데이터를 복호하는 비대칭 복호키
	KPmw	공개 암호키	개별	메모리 카드로부터 다음 x는 모듈을 식별하기 위한 식별자
	KPmw	공개 암호키	개별	x는 모듈을 식별하기 위한 식별자
	Kmw	비밀 복호키	개별	공개 암호키 KPmw에 대해 암호화된 데이터를 복호하는 비대칭 복호키
	Ks2	공통키	고유 채신	문텐츠 데이터 및 라이선스 수신시에 발생
	Ks3	공통키	고유 채신	데이터 단말 장치로의 문텐츠 데이터 및 라이선스 저장시에 발생
	Cmw	증명서	클래스 증명서	메모리 카드의 클래스 증명서. 인증기들을 갖는다. (Kmw//Cmw)KPw의 형식으로 출하시에 기록. * 메모리 카드의 클래스이다 다르다.

도면 4

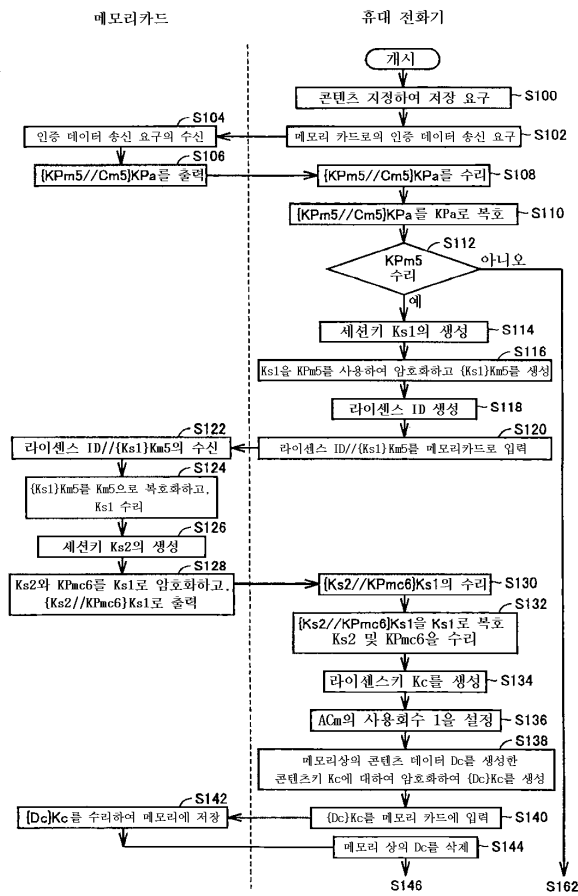


도면 5

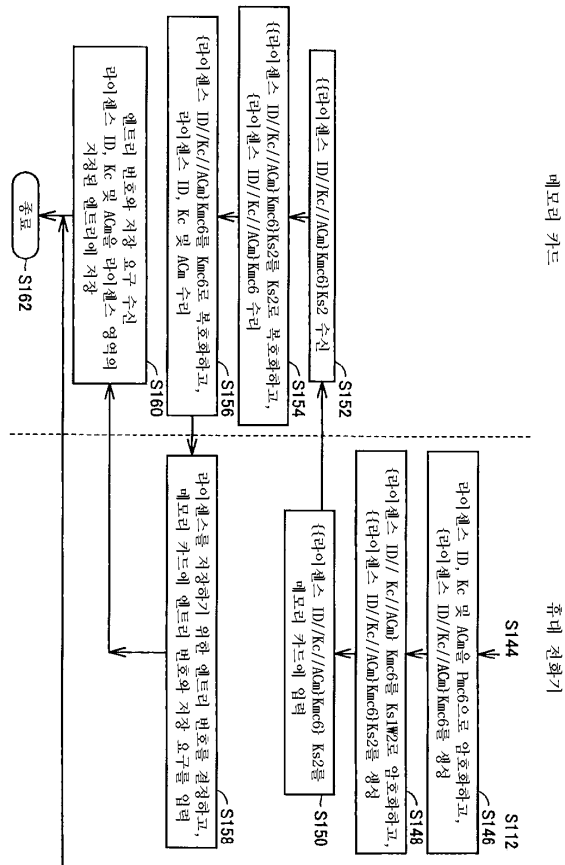


110

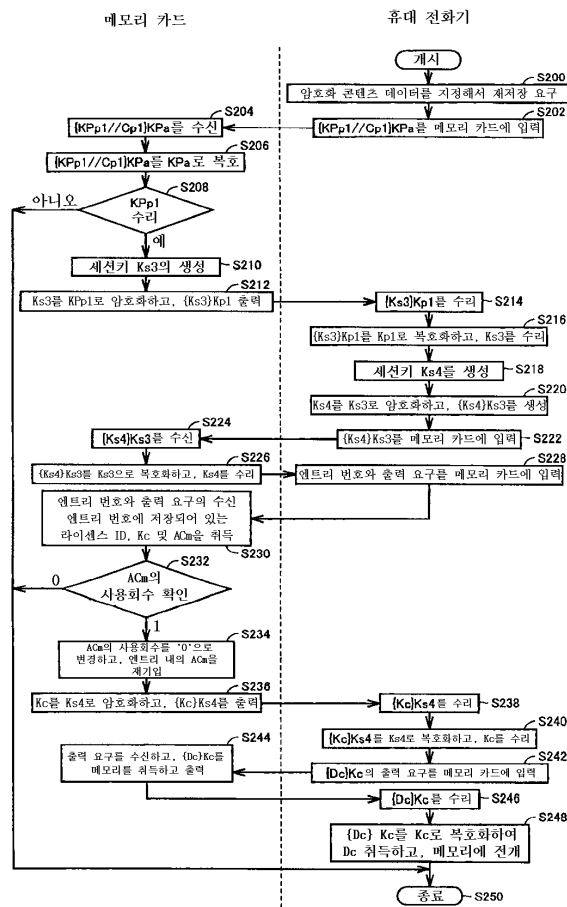
도면 6



도면 7



도면 8



도면 9

