(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06K 17/00 (2006.01)
H04L 9/32 (2006.01)
H04L 9/30 (2006.01)

(11) 공개번호 10-2007-0030709
(43) 공개일자 2007년03월16일

(21) 출원번호 10-2006-0088605
(22) 출원일자 2006년09월13일
심사청구일자 없음

(30) 우선권주장 200510102866.4 2005년09월13일 중국(CN)
200510109693.9 2005년09월20일 중국(CN)

(71) 출원인 엔이씨 (차이나) 씨오., 엘티디.
중국 베이징 똥청취 똥창안째1회 오리엔탈프라자 이3타워 1201호

(72) 발명자 젱 케
중국 100084 베이징 찡후아 사이언스 파크 이노베이션 플라자에이빌딩 11층
후지따 도모유끼
중국 100084 베이징 찡후아 사이언스 파크 이노베이션 플라자에이빌딩 11층
휴에 민유
중국 100084 베이징 찡후아 사이언스 파크 이노베이션 플라자에이빌딩 11층

(74) 대리인 장수길
이중희
구영창

전체 청구항 수 : 총 55 항

(54) 무선 주파수 식별 시스템 및 방법

(57) 요약

본 발명은, 식별 코드 및 한 세트의 검증가능한 데이터가 저장된 무선 주파수 식별 태그와, 상기 검증가능한 데이터의 세트 중 제1 부분을 판독하길 요청하는 판독 요청을 상기 무선 주파수 식별 태그에 전송하는 무선 주파수 식별 판독기를 포함하며, 상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 판독 요청을 수신할 때, 검증가능한 데이터의 세트가 잠금 동작을 수행하지 않는 경우, 검증가능한 데이터의 세트에 대한 잠금 동작을 수행하여 검증가능한 데이터 세트 중 제2 부분 중 임의의 데이터가 판독될 수 없게 되는 무선 주파수 식별 시스템에 관한 것이다.

대표도

도 3

특허청구의 범위

청구항 1.

무선 주파수 식별 시스템에 있어서,

식별 코드와 한 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그, 및

상기 한 세트의 검증가능 데이터의 제1 부분을 판독하라는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 무선 주파수 식별 판독기

를 포함하고,

상기 무선 주파수 식별 태그는 제어 수단을 더 포함하며, 상기 제어 수단은 상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 한 세트의 검증가능 데이터의 제2 부분의 어떠한 데이터도 판독될 수 없게 하는 무선 주파수 식별 시스템.

청구항 2.

제1항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행하기 전에, 상기 한 세트의 검증가능 데이터의 상기 제1 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게끔 하는 무선 주파수 식별 시스템.

청구항 3.

제1항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행한 후에, 상기 한 세트의 검증가능 데이터의 상기 제1 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게끔 하는 무선 주파수 식별 시스템.

청구항 4.

제1항에 있어서,

상기 식별 코드는 상기 무선 주파수 식별 태그를 고유하게 식별하는 무선 주파수 식별 시스템.

청구항 5.

제1항에 있어서,

상기 무선 주파수 식별 태그는 인증해야 할 제품에 부착되며, 상기 식별 코드는 EPC 코드를 포함하는 무선 주파수 식별 시스템.

청구항 6.

제1항에 있어서,

상기 한 세트의 검증가능 데이터 내의 데이터는 상기 식별 코드를 암호화함에 의해 얻어지는 무선 주파수 식별 시스템.

청구항 7.

제1항에 있어서,

상기 한 세트의 검증가능 데이터 내의 데이터는 상기 식별 코드 및 다른 정보를 암호화함에 의해 얻어지는 무선 주파수 식별 시스템.

청구항 8.

제1항에 있어서,

상기 한 세트의 검증가능 데이터의 상기 제1 부분은 상기 한 세트의 검증가능 데이터 중에서 임의로 선택되는 무선 주파수 식별 시스템.

청구항 9.

제1항에 있어서,

상기 한 세트의 검증가능 데이터의 상기 제2 부분은 상기 한 세트의 검증가능 데이터의 상기 제1 부분의 어떠한 데이터도 포함하지 않는 무선 주파수 식별 시스템.

청구항 10.

제1항에 있어서,

싱기 무선 주파수 식별 판독기는 상기 무선 주파수 식별 태그로부터 판독한 상기 한 세트의 검증가능 데이터의 일부에 기초하여 상기 무선 주파수 식별 태그를 인증하는 인증 수단을 더 포함하는 무선 주파수 식별 시스템.

청구항 11.

제1항에 있어서,

상기 한 세트의 검증가능 데이터는 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n을 포함하며, 상기 한 세트의 검증가능 데이터의 상기 제1 부분은 상기 n개 디지털 서명 중 k개 디지털 서명을 포함하고, 상기 한 세트의 검증가능 데이터의 상기 제2 부분은 상기 n개 디지털 서명 중 q개 디지털 서명을 포함하는 무선 주파수 식별 시스템.

청구항 12.

제11항에 있어서,

n이 짝수이면 $k=n*0.5$이고, n이 홀수이면 $k=n*0.5+0.5$ 또는 $k=n*0.5-0.5$인 무선 주파수 식별 시스템.

청구항 13.

제11항에 있어서,

상기 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n의 각 디지털 서명 SIG_i는 S_i 부분 및 C 부분을 포함하고 i=1,..., n인 (S_i, C)의 형식을 취하고, 상기 n개 디지털 서명의 모든 디지털 서명은 하나의 공통 부분 C를 공유하는 무선 주파수 식별 시스템.

청구항 14.

제13항에 있어서,

상기 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n의 각 디지털 서명은 다음과 같이,

순위 v의 그룹 G를 선택하고,

상기 그룹 G의 순위 u(여기서, u≤v)의 서브그룹 선택하고,

상기 순위 u에 기초하여 n개 개인 키 x1, x2,..., xn(여기서, $1<|xi|<u$, i=1,..., n)을 선택하고,

그룹 G의 원소 g를 생성자로서 선택하고,

상기 순위 u 내에서 표시자로서 n개의 정수 r1, r2,..., rn(여기서, $0<|ri|<u$, i=1,..., n)을 선택하고,

상기 순위 u 내에서 임의 정수 r(여기서, $0<|r|<u$)을 선택하고, 및 $C= H(M, g^{r*r1 * r2 * \dots * rn})$(여기서 H는 안전한 해싱 함수이고, M은 상기 식별 코드 및 다른 정보를 나타냄)를 계산하고,

$S_i = r*(r1 * r2 *\dots * rn)/ri - C * xi$을 계산하고,

$(S_1, C), (S_2, C),\dots, (S_n, C)$을 동일 메시지 M에 대한 n개의 디지털 서명으로서 배포하고,

상기 개인 키, 상기 생성자, 및 상기 표시자에 기초하여 공개 키 $y_i=(g^{ri} , g^{ri * xi})$를 계산하고,

상기 공개 키 y_i에 기초하여, $SIG_i=(S_i, C)$가 메시지 M에 대한 유효한 서명인지를 $C' = H(M, (g^{ri})^{si} * (g^{ri * xi})^{C})$를 계산함으로써(C' = C인 경우에는 SIG_i가 메시지 M에 대한 유효한 디지털 서명이고, 그렇지 않은 경우에는 SIG_i는 무효) 검증하는 것에 의해 계산되고 검증되는 무선 주파수 식별 시스템.

청구항 15.

제13항에 있어서,

상기 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n의 각 디지털 서명은 다음과 같이,

순위 v의 그룹 G 선택하고,

상기 그룹 G의 순위 u(여기서, u≤v)의 서브그룹 선택하고,

상기 순위 u에 기초하여 n개 개인 키 x1, x2,..., xn(여기서, $1<|xi|<u$, i=1,..., n)을 선택하고,

그룹 G의 원소 g를 생성자로서 선택하고,

상기 순위 u 내에서 표시자로서 n개의 정수 r1, r2,..., rn(여기서, $0<|ri|<u$, i=1,..., n)을 선택하고,

상기 순위 u 내에서 임의 정수 r(여기서, $0<|r|<u$)을 선택하고, 및 $C= H(M, g^{r*r1 * r2 * \dots * rn})$(여기서 H는 안전한 해싱 함수이고, M은 상기 식별 코드 및 다른 정보를 나타냄)를 계산하고,

$S_i = r*(r1 * r2 *\dots * rn)/(r1 * r2 *\dots * ri) - C * xi$을 계산하고,

$(S_1, C), (S_2, C),\dots, (S_n, C)$을 동일 메시지 M에 대한 n개의 디지털 서명으로서 배포하고,

상기 개인 키, 상기 생성자, 및 상기 표시자에 기초하여 공개 키 $y_i=(g^{r1 * r2 *\dots *ri}, g^{r1 * r2*\dots *ri * xi})$를 계산하고,

상기 공개 키 y_i에 기초하여, $SIG_i=(S_i, C)$가 메시지 M에 대한 유효한 서명인지를 $C' = H(M, (g^{r1 * r2 *\dots *ri})^{si} * (g^{r1 * r2 *\dots * ri * xi})^{C})$를 계산함으로써(C' = C인 경우에는 SIG_i가 메시지 M에 대한 유효한 디지털 서명이고, 그렇지 않은 경우에는 SIG_i는 무효) 검증하는 것에 의해 계산되고 검증되는 무선 주파수 식별 시스템.

청구항 16.

제1항에 있어서,

상기 무선 주파수 식별 태그에는 다른 m개 세트의 검증가능 데이터가 저장되어 있고,

상기 무선 주파수 식별 판독기는 또한 상기 m개 세트의 검증가능 데이터 중 적어도 한 세트의 일부분을 판독하라고 요청하는 적어도 하나 이상의 판독 요청을 송신하고,

상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 적어도 하나 이상의 판독 요청을 수신할 때, 요청한 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 제어 수단이 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 요청된 상기 한 세트의 검증가능 데이터의 다른 부분의 어떠한 서명도 판독될 수 없게 하는 무선 주파수 식별 시스템.

청구항 17.

식별 코드 및 한 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그에 있어서,

상기 무선 주파수 식별 태그는 제어 수단을 더 포함하며, 상기 제어 수단은 상기 무선 주파수 식별 태그가 상기 한 세트의 검증가능 데이터의 제1 부분을 판독하라고 요청하는 판독 요청을 수신할 때, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 한 세트의 검증가능 데이터의 제2 부분의 어떠한 데이터도 판독될 수 없게 하는 무선 주파수 식별 태그.

청구항 18.

제17항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행하기 전에, 상기 한 세트의 검증가능 데이터의 상기 제1 부분이 판독되게끔 하는 무선 주파수 식별 태그.

청구항 19.

제17항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행한 후에, 상기 한 세트의 검증가능 데이터의 상기 제1 부분이 판독되게끔 하는 무선 주파수 식별 태그.

청구항 20.

제17항에 있어서,

상기 식별 코드는 상기 무선 주파수 식별 태그를 고유하게 식별하는 무선 주파수 식별 태그.

청구항 21.

제17항에 있어서,

상기 무선 주파수 식별 태그는 인증해야 할 제품에 부착되며, 상기 식별 코드는 EPC 코드를 포함하는 무선 주파수 식별 태그.

청구항 22.

제17항에 있어서,

상기 한 세트의 검증가능 데이터 내의 데이터는 상기 식별 코드를 암호화함에 의해 얻어지는 무선 주파수 식별 태그.

청구항 23.

제17항에 있어서,

상기 한 세트의 검증가능 데이터 내의 데이터는 상기 식별 코드 및 다른 정보를 암호화함에 의해 얻어지는 무선 주파수 식별 태그.

청구항 24.

제17항에 있어서,

상기 한 세트의 검증가능 데이터의 상기 제2 부분은 상기 한 세트의 검증가능 데이터의 상기 제1 부분의 어떠한 데이터도 포함하지 않는 무선 주파수 식별 태그.

청구항 25.

제1항에 있어서,

상기 한 세트의 검증가능 데이터는 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n을 포함하며, 상기 한 세트의 검증가능 데이터의 상기 제1 부분은 상기 n개 디지털 서명 중 k개 디지털 서명을 포함하고, 상기 한 세트의 검증가능 데이터의 상기 제2 부분은 상기 n개 디지털 서명 중 q개 디지털 서명을 포함하는 무선 주파수 식별 태그.

청구항 26.

제25항에 있어서,

n이 짝수이면 $k=n*0.5$이고, n이 홀수이면 $k=n*0.5+0.5$ 또는 $k=n*0.5-0.5$인 무선 주파수 식별 태그.

청구항 27.

제25항에 있어서,

상기 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n의 각 디지털 서명 SIG_i는 S_i 부분 및 C 부분을 포함하고 i=1,..., n인 (S_i, C)의 형식을 취하고, 상기 n개 디지털 서명의 모든 디지털 서명은 하나의 공통 부분 C를 공유하는 무선 주파수 식별 태그.

청구항 28.

제27항에 있어서,

상기 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n의 각 디지털 서명은 다음과 같이,

순위 v의 그룹 G 선택하고,

상기 그룹 G의 순위 u(여기서, u≤v)의 서브그룹 선택하고,

상기 순위 u에 기초하여 n개 개인 키 x1, x2,..., xn(여기서, $1<|xi|<u$, i=1,..., n)을 선택하고,

그룹 G의 원소 g를 생성자로서 선택하고,

상기 순위 u 내에서 표시자로서 n개의 정수 r1, r2,..., rn(여기서, $0<|ri|<u$, i=1,..., n)을 선택하고,

상기 순위 u 내에서 임의 정수 r(여기서, $0<|r|<u$)을 선택하고, 및 $C= H(M, g^{r*r1 * r2 * \dots * rn})$(여기서, H는 안전한 해싱 함수이고, M은 상기 식별 코드 및 다른 정보를 나타냄)를 계산하고,

$S_i = r*(r1 * r2 *\dots * rn)/ri - C * xi$을 계산하고,

$(S_1, C), (S_2, C), \ldots, (S_n, C)$을 동일 메시지 M에 대한 n개의 디지털 서명으로서 배포하고,

상기 개인 키, 상기 생성자, 및 상기 표시자에 기초하여 공개 키 $y_i=(g^{ri}, g^{ri * xi})$를 계산하고,

상기 공개 키 y_i에 기초하여, $SIG_i=(S_i, C)$가 메시지 M에 대한 유효한 서명인지를 $C' = H(M, (g^{ri})^{si} * (g^{ri * xi})^{C})$를 계산함으로써(C' = C인 경우에는 SIG_i가 메시지 M에 대한 유효한 디지털 서명이고, 그렇지 않은 경우에는 SIG_i는 무효) 검증하는 것에 의해 계산되고 검증되는 무선 주파수 식별 태그.

청구항 29.

제27항에 있어서,

상기 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n의 각 디지털 서명은 다음과 같이,

순위 v의 그룹 G 선택하고,

상기 그룹 G의 순위 u(여기서, u≤v)의 서브그룹 선택하고,

상기 순위 u에 기초하여 n개 개인 키 x1, x2,..., xn(여기서, $1<|xi|<u$, i=1,..., n)을 선택하고,

그룹 G의 원소 g를 생성자로서 선택하고,

상기 순위 u 내에서 표시자로서 n개의 정수 r1, r2,..., rn(여기서, $0<|ri|<u$, i=1,..., n)을 선택하고,

상기 순위 u 내에서 임의 정수 r(여기서, $0<|r|<u$)을 선택하고, 및 $C= H(M, g^{r*r1 * r2 * \ldots * rn})$(여기서 H는 안전한 해싱 함수이고, M은 상기 식별 코드 및 다른 정보를 나타냄)를 계산하고,

$S_i = r*(r1 * r2 *\ldots * rn)/(r1 * r2 *\ldots * ri) - C * xi$을 계산하고,

$(S_1, C), (S_2, C), \ldots, (S_n, C)$을 동일 메시지 M에 대한 n개의 디지털 서명으로서 배포하고,

상기 개인 키, 상기 생성자, 및 상기 표시자에 기초하여 공개 키 $y_i=(g^{r1 * r2 *\ldots *ri}, g^{r1 * r2*\ldots *ri * xi})$를 계산하고,

상기 공개 키 y_i에 기초하여, $SIG_i=(S_i, C)$가 메시지 M에 대한 유효한 서명인지를 $C' = H(M, (g^{r1 * r2 *\ldots *ri})^{si} * (g^{r1 * r2 *\ldots * ri * xi})^{C})$를 계산함으로써(C' = C인 경우에는 SIG_i가 메시지 M에 대한 유효한 디지털 서명이고, 그렇지 않은 경우에는 SIG_i는 무효) 검증하는 것에 의해 계산되고 검증되는 무선 주파수 식별 태그.

청구항 30.

제17항에 있어서,

상기 무선 주파수 식별 태그에는 다른 m개 세트의 검증가능 데이터가 저장되어 있고,

상기 무선 주파수 식별 판독기는 또한 상기 m개 세트의 검증가능 데이터 중 적어도 한 세트의 일부분을 판독하라고 요청하는 적어도 하나 이상의 판독 요청을 송신하고,

상기 무선 주파수 식별 태그가 상기 m개 세트의 검증가능 데이터 중 적어도 한 세트의 일부분을 판독하라고 요청하는 적어도 하나의 판독 요청을 수신할 때, 요청된 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 제어 수단이 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 요청된 상기 한 세트의 검증가능 데이터의 또 다른 부분의 어떠한 서명도 판독될 수 없게 하는 무선 주파수 식별 태그.

청구항 31.

무선 주파수 식별 방법으로서,

식별 코드 및 한 세트의 검증가능 데이터를 무선 주파수 식별 태그에 저장시키는 단계, 및

무선 주파수 식별 판독기에 의해 상기 한 세트의 검증가능 데이터의 제1 부분을 판독하라고 요청하는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 단계

를 포함하고,

상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 한 세트의 검증가능 데이터의 제2 부분의 어떠한 데이터도 판독될 수 없게 하는 무선 주파수 식별 방법.

청구항 32.

제31항에 있어서,

상기 잠금 동작을 수행하기 전에, 상기 한 세트의 검증가능 데이터의 상기 제1 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게끔 하는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 33.

제31항에 있어서,

상기 잠금 동작을 수행한 후에, 상기 한 세트의 검증가능 데이터의 상기 제1 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게끔 하는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 34.

제31항에 있어서,

상기 식별 코드는 상기 무선 주파수 식별 태그를 고유하게 식별하는 무선 주파수 식별 방법.

청구항 35.

제31항에 있어서,

상기 무선 주파수 식별 태그는 인증해야 할 제품에 부착되며, 상기 식별 코드는 EPC 코드를 포함하는 무선 주파수 식별 방법.

청구항 36.

제31항에 있어서,

상기 한 세트의 검증가능 데이터의 데이터를 얻기 위해 상기 식별 코드 암호화하는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 37.

제31항에 있어서,

상기 한 세트의 검증가능 데이터 내의 데이터를 얻기 위해 상기 식별 코드 및 다른 정보를 암호화하는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 38.

제31항에 있어서,

상기 한 세트의 검증가능 데이터 중에서 상기 한 세트의 검증가능 데이터의 상기 제1 부분을 임의로 선택하는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 39.

제31항에 있어서,

상기 한 세트의 검증가능 데이터의 상기 제2 부분은 상기 한 세트의 검증가능 데이터의 상기 제1 부분의 어떠한 데이터도 포함하지 않는 무선 주파수 식별 방법.

청구항 40.

제31항에 있어서,

상기 무선 주파수 식별 판독기가 상기 무선 주파수 식별 태그로부터 판독된 상기 한 세트의 검증가능 데이터의 일부에 기초하여 상기 무선 주파수 식별 태그를 인증하는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 41.

제31항에 있어서,

상기 한 세트의 검증가능 데이터는 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n을 포함하며, 상기 한 세트의 검증가능 데이터의 상기 제1 부분은 상기 n개 디지털 서명 중 k개 디지털 서명을 포함하고, 상기 한 세트의 검증가능 데이터의 상기 제2 부분은 상기 n개 디지털 서명 중 q개 디지털 서명을 포함하는 무선 주파수 식별 방법.

청구항 42.

제41항에 있어서,

n이 짝수이면 $k=n*0.5$이고, n이 홀수이면 $k=n*0.5+0.5$ 또는 $k=n*0.5-0.5$인 무선 주파수 식별 방법.

청구항 43.

제41항에 있어서,

상기 n개의 디지털 서명 SIG_1, SIG_2, ..., SIG_n의 각 디지털 서명 SIG_i는 S_i 부분 및 C 부분을 포함하고 i=1,..., n인 (S_i, C)의 형식을 취하고, 상기 n개 디지털 서명의 모든 디지털 서명은 하나의 공통 부분 C를 공유하는 무선 주파수 식별 방법.

청구항 44.

제43항에 있어서,

상기 n개 디지털 서명의 각 디지털 서명은 다음과 같이,

순위 v의 그룹 G를 선택하고,

상기 그룹 G의 순위 u(여기서, u≤v)의 서브그룹을 선택하고,

상기 순위 u에 기초하여 n개 개인 키 x1, x2,...,xn(여기서, $1<|xi|<u$, i=1,...,n)을 선택하고,

그룹 G의 원소 g를 생성자로서 선택하고,

상기 순위 u 내에서 표시자로서 n개의 정수 r1, r2,...,rn(여기서, $0<|ri|<u$, i=1,...,n)을 선택하고,

상기 순위 u 내에서 임의 정수 r(여기서, $0<|r|<u$)을 선택하고, $C= H(M, g^{r*r1 * r2 * \dots * rn})$(여기서, H는 안전한 해싱 함수이고, M은 상기 식별 코드 및 다른 정보를 나타냄)을 계산하고,

$S_i = r*(r1 * r2 *\dots * rn)/ri - C * xi$를 계산하고,

$(S_1, C), (S_2, C),\dots, (S_n, C)$를 동일 메시지 M에 대한 n개의 디지털 서명으로서 배포하고,

상기 개인 키, 상기 생성자 및 상기 표시자에 기초하여 공개 키 $y_i=(g^{ri} , g^{ri * xi})$를 계산하고,

공개 키 y_i에 기초하여, $SiG_i=(S_I,C)$가 메시지 M에 대한 유효한 서명인지를 $C' = H(M, (g^{ri})^{si} * (g^{ri * xi})^{C})$를 계산함으로써(C'=C인 경우에는 SIG_i가 상기 메시지 M에 대한 유효한 디지털 서명이고, 그렇지 않은 경우에는 SIG_i는 무효) 검증하는 것에 의해 계산되고 검증되는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 45.

제43항에 있어서,

상기 n개 디지털 서명의 각 디지털 서명은 다음과 같이,

순위 v의 그룹 G를 선택하고,

상기 그룹 G의 순위 u(여기서, u≤v)의 서브그룹을 선택하고,

상기 순위 u에 기초하여 n개 개인 키 x1, x2,...,xn(여기서, $1<|xi|<u$, i=1,...,n)을 선택하고,

그룹 G의 요소 g를 생성자로서 선택하고,

상기 순위 u 내에서 표시자로서 n개의 정수 r1, r2,...,rn(여기서, $0<|ri|<u$, i=1,...,n)을 선택하고,

상기 순위 u 내에서 임의 정수 r($0<|r|<u$)을 선택하고, $C= H(M, g^{r*r1 * r2 * \dots * m})$(여기서 H는 안전한 해싱 함수이고, 상기 M은 식별 코드 및 다른 정보를 나타냄)을 계산하고,

$S_i = r*(r1 * r2 *\dots * rn)/(r1 * r2 *\dots * ri) - C * xi$를 계산하며,

$(S_1, C), (S_2, C),\dots, (S_n, C)$를 동일 메시지 M에 대한 n개의 디지털 서명으로서 를 배포하고,

상기 개인 키, 상기 생성자 및 상기 표시자에 기초하여 공개 키 $y_i=(g^{r1 * r2 *\dots *ri}, g^{r1 * r2*\dots *ri * xi})$를 계산하고,

상기 공개 키 y_i에 기초하여, $SiG_i=(S_I,C)$가 메세지 M에 대한 유효한 서명인지를 $C' = H(M, (g^{r1 * r2 *\dots *ri})^{si} * (g^{r1 * r2 *\dots * ri * xi})^{C})$를 계산함으로써(C' = C인 경우에는 SIG_i가 상기 메시지 M에 대한 유효한 디지털 서명이고, 그렇지 않은 경우에는 SIG_i는 무효) 검증하는 것에 의해 계산되고 검증되는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 46.

제31항에 있어서,

상기 무선 주파수 식별 태그에 다른 m개 세트의 검증가능한 데이터를 저장하는 단계를 더 포함하고,

상기 무선 주파수 식별 판독기는 상기 m개 세트의 검증가능 데이터 중 적어도 한 세트의 일부분을 판독하라고 요청하는 적어도 하나 이상의 판독 요청을 더 송신하고,

상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 적어도 하나 이상의 판독 요청을 수신할 때, 요청한 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 제어 수단이 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 요청된 상기 한 세트의 검증가능한 데이터의 다른 부분의 어떠한 서명도 판독될 수 없게 하는 무선 주파수 식별 방법.

청구항 47.

무선 주파수 식별 시스템에 있어서,

식별 코드와 m개 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그, 및

상기 m개 세트의 검증가능 데이터 중 t 세트의 검증가능 데이터의 일부를 판독라는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 무선 주파수 식별 판독기

를 포함하고,

상기 무선 주파수 식별 태그는 제어 수단을 더 포함하며, 상기 제어 수단은 상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 t 세트의 검증가능 데이터 각각의 다른 부분이 판독될 수 없게 하는 무선 주파수 식별 시스템.

청구항 48.

제47항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행하기 전에, 상기 t 세트의 검증가능 데이터 각각의 요청 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게 끔 하는 무선 주파수 식별 시스템.

청구항 49.

제47항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행한 후에, 상기 t 세트의 검증가능 데이터 각각의 요청 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게 하는 무선 주파수 식별 시스템.

청구항 50.

식별 코드 및 m개 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그에 있어서,

상기 무선 주파수 식별 태그는 제어 수단을 더 포함하고, 상기 제어 수단은 상기 m개 세트의 검증가능 데이터 중 t 세트의 검증가능 데이터 각각의 일부를 판독하라고 요청하는 판독 요청을 수신할 때, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 t 세트의 검증가능 데이터의 각각의 다른 부분이 판독될 수 없게 하는 무선 주파수 식별 태그.

청구항 51.

제50항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행하기 전에, 상기 t 세트의 검증가능한 데이터 각각의 요청 부분이 판독되게끔 하는 무선 주파수 식별 태그.

청구항 52.

제50항에 있어서,

상기 제어 수단은 상기 잠금 동작을 수행한 후에, 상기 t 세트의 검증가능 데이터 각각의 요청 부분이 판독되게끔 하는 무선 주파수 식별 태그.

청구항 53.

무선 주파수 식별 방법에 있어서,

식별 코드 및 m개 세트의 검증가능 데이터를 무선 주파수 식별 태그에 저장하는 단계, 및

무선 주파수 식별 판독기에 의해 상기 m개 세트의 검증가능 데이터 중 t 세트의 검증가능 데이터 각각의 일부를 판독하라고 요청하는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 단계

를 포함하고,

상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 t 세트의 검증가능 데이터가 잠금 동작이 수행되지 않은 경우, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 t 세트의 검증가능 데이터 각각의 다른 부분이 판독될 수 없게 하는 무선 주파수 식별 방법.

청구항 54.

제53항에 있어서,

상기 잠금 동작을 수행하기 전에, 상기 t 세트의 검증가능 데이터 각각의 요청 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게끔 하는 단계를 더 포함하는 무선 주파수 식별 방법.

청구항 55.

제53항에 있어서,

상기 잠금 동작을 수행한 후에, 상기 t 세트의 검증가능 데이터 각각의 요청 부분이 상기 무선 주파수 식별 판독기에 의해 판독되게끔 하는 단계를 더 포함하는 무선 주파수 식별 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은, 전반적으로 컴퓨터 시스템에 관한 것이며, 보다 구체적으로는, 무선 주파수 식별(RFID) 시스템 및 무선 주파수 식별 방법에 관한 것이다.

위조(counterfeit)는 제품 제조업자들에게 있어 매우 심각한 문제이다. 오늘날, 예컨대, 와인, 담배, 약, 화장품, CD, DVD, 소프트웨어, 스포츠 용품, 아동 용품, 보석 등의 많은 산업분야에서 위조를 볼 수 있다. 수 십년 동안, 이 산업들은 위조자들과 투쟁하고 있다. 그러나, 위조-방지(anti-counterfeit) 노력의 지속적인 진행에 발맞춰, 서부나 동부 할 것 없이 대부분의 나라에서 믿을 수 없을 만큼 위조가 성행하고 있다.

위조는 순진한 제조업자들에게 이익면에서 막대한 손실뿐만 아니라, 신용면에서 파탄까지도 초래하게 한다. 유감스럽게도 위조품을 구입하여, 그 위조품의 형편없는 품질에 불만을 나타내는 보통의 소비자는, 대부분의 경우, 진품으로부터 위조품을 구별할 수 없으므로, 진짜 제조업자의 제품 품질을 부정적이고 틀리게 평가할 것이다. 최악의 스토리는: 위조자는 돈을 벌고, 죄없는 제조업자는 망하게 된다는 것이다.

제품 제조업자들은 소비자들이 위조 제품들로부터 진품들을 구별하는데 도움을 줄 수 있는 제품 인증 솔루션들을 항상 갈망하고 있다. 소비자가 제품을 인증하기 쉽게 하는 솔루션이 있으면, 위조품들을 시장에서 쉽게 몰아낼 수 있을 것이다.

위조-방지는 특허 출원에서 매우 새로운 논제이며, 많은 솔루션들이 시장에 이미 제공되어 왔다. 컴퓨터 통신 네트워크라는 광범위한 채택 이전에는, 위조-방지 솔루션들은 일반적으로, 예컨대, 특수 인쇄용 잉크, 용지, 직물 및 레이저 라벨 등의 물리적인 수단을 기초로 했다. 위조에 강력히 반대하는 솔루션 제공자들은 그러한 물리적 수단을 주장하고 있다. 그러나, 과거 수십 년간의 이력은 그 제공자들의 주장과는 명백하게 불일치한다. 지폐가 매우 좋은 예이다. 대부분의 진보된 물리적 수단들은 항상 지폐에서 발견될 수 있다. 그러나, 위조 지폐들은 절대 사라지지 않는다. 분명히, 보통의 제품 제조업자들은 지폐 위조-방지에 적용한 높은 비용을 유지할 수 없다. 그러므로, 보통의 제품 제조업자들에 의해 채택된 위조-방지 솔루션들은 매우 취약하다.

과거 20여년 동안, 컴퓨터 통신 네트워크가 소비자 시장에서 성공적으로 진보하고 있다. 글로벌 인터넷 액세스 요금 및 고정/이동 원격통신 요금이 지구상에 살고 있는 대다수의 사람들에게 알맞도록 아주 낮아지고 있다. 결과적으로, 제품이 수반하고 있는 제품 인증 정보를 백엔드 서버로 전송하여, 그 제품이 진품인지 위조품인지를 그 서버에서 판정하도록 하려고 시도하는 점점 더 많은 위조-방지 솔루션들을 놀랍지 않게 볼 수 있다. 예를 들어, 중국 특허출원 제99126659호 및 제0211542호가 이런 종류의 기술을 포함하고 있다.

RFID 태그는 위조에 싸우기 위한 또 다른 떠오르는 별이다. RFID라는 용어는 광범위하게 변화하는 양의 계산 전력, 판독 범위 및 비용을 갖는 무선 및 프로세서 기술들의 조직단위를 포함한다. 공급망 태그들은, 월마트와 미국방부가 대규모의 재판을 시작한 이후로 유명해졌다. 산업체 EPCglobal(www.epcglobaline.org)은 암호법 및 최소의 부가적 특징들에 대한 지원 없이, 극히 제한된 계산, 저장, 및 통신 기능들을 갖는 클래스 0 및 클래스 1 RFID 태그들을 정의하였다.

임의의 RFID 시스템에 대해서는 3개 컴포넌트들: RFID 태그, RFID 판독기, 및 데이터 처리 서브시스템이 기본적이다. RFID 태그는 식별될 대상 위에 위치하며, RFID 시스템의 데이터 캐리어이다. RFID 판독기는 RFID 태그로부터 데이터를 판독하고 RFID 태그에 데이터를 기입할 수 있다. 데이터 처리 서브시스템은 RFID 판독기에 의해 취득된 데이터를 일부 유용한 방식으로 활용한다.

통상적인 RFID 태그는 데이터를 저장하는 마이크로칩 및 무선 주파수 통신을 통해 통신하는 코일형 안테나와 같은 결합 소자를 포함한다. RFID 태그는 능동형이거나 또는 수동형일 수 있다. 능동형 RFID 태그는 온-태그 전원(예를 들어 배터리)을 가지며 통신용의 RF 신호를 능동적으로 송신하는 한편, 수동형 RFID 태그는 RFID 판독기의 질문 신호로부터 그들의 모든 전력을 획득하고 통신용의 RFID 판독기의 신호를 변조하여 반사하거나 로드시킨다. 대부분의 RFID 태그들은, 수동형과 능동형 모두, 그들이 RFID 판독기에 의해서 질문받는 경우에만 통신한다.

통상적인 RFID 판독기는 무선 주파수 통신을 통해 RFID 태그들을 문의하기 위한 무선 주파수 모듈, 제어부, 및 결합 소자를 포함한다. 또한, 다수의 RFID 판독기들에는 이들이 그들의 수신된 데이터를, 예를 들어, 개인용 컴퓨터상에서 동작하는 데이터베이스와 같은 데이터 처리 서브시스템과 통신할 수 있게 하는 인터페이스가 설비된다. RFID 태그와 통신하기 위한 무선 주파수의 사용에 의해 RFID 판독기들이 중소형 거리에서 수동형 RFID 태그들을 판독할 수 있게 하고, 태그들이 부적당한 환경에 위치하고 있고 시야로부터 흐린 경우에도 능동형 RFID 태그들이 중대형 거리에서 판독될 수 있게 한다.

RFID 태그를 활용하는 위조 방지 솔루션은 간단하게 온라인 솔루션 및 오프라인 솔루션으로 분류될 수 있다. 온라인 위조 방지 솔루션에 있어서, 컴퓨터 통신 네트워크도 사용된다. 이러한 솔루션은 보안 수단을 수반할 수도 있고 수반하지 않을 수도 있다. 예를 들면, 중국 특허 출원 200410082611.1호 및 200410024790.3호는 이러한 분류의 기술에 포함되지만, 전자는 보안 수단을 사용하지 않고 후자는 보안 수단을 요청한다. 반면에, 오프라인 솔루션에서는, 컴퓨터 통신 네트워크가 활용되지 않는다, 즉, 오직 RFID 태그 및 판독기만이 활용되어 제품을 인증한다. 이 경우에, 보안 수단은 필수적으로 필요하다. 예를 들면, 중국 특허 출원 03111875.5호 및 200410078160.4호는 이러한 분류의 기술에 포함된다. PCT 특허출원 WO 2005/024967 A2 또한 이러한 경우이다.

기존의 위조 방지 솔루션은 비용, 효율, 유용성 및 보안의 면에서 문제가 있었다.

특히, 통신 네트워크 지원을 필요로 하는 위조 방지 솔루션은 소비자들로부터의 대량의 제품 인증 질의를 처리하기 위해서 고비용의 백엔드 서버를 필요로 하는 문제에 부닥치게 된다. 더욱이, 그 통신 비용이 소비자나 제품 제조자에게 부과될 것이다. 통신 비용이 소비자에게 부과되면, 대부분의 소비자들이 명백한 경제적인 이유로 그러한 솔루션을 버리게 될 것이다. 한편, 통신 비용이 제품 제조자에게 부과되면, 소비자로부터의 대량의 제품 인증 질의로 인해서 제품 제조자의 이익을 줄어들게 된다. 그것만이 아니다. 대부분의 경우에, 소비자와 제품 인증용 백엔드 서버 간의 통신에 상당한 시간이 걸린다. 소비자들은 또한 시간적인 이유로 그러한 종류의 솔루션을 외면하게 된다.

기존의 오프라인 태그 기반 위조 방지 솔루션, 즉 통신 네트워크 지원을 필요로 하지 않는 솔루션은 보안 문제뿐만 아니라 비용 문제에 부닥친다. 그러한 종류의 솔루션에 보안 수단이 포함되어 있다고는 하지만, 실제로는 대부분이 작동하지 않는다. 그러한 종류의 솔루션은 일반적으로 태그가 비밀 정보를 포함하여 복제 방지되어 있다는, 즉 비밀 정보를 포함하는 진짜 태그가 주어지면 그것과 동일한 정보를 포함하는 다른 태그를 제조하기가 어렵다는 가정을 기대한다. 그러한 가정이 진짜라면, 보안 수단이 태그에 저장된 비밀 정보의 위조를 방지하여 비밀 정보 및 태그를 안전하게 보호하기 때문에 상기와 같은 솔루션도 가능할 것이다. 불행하게도, 그러한 가정은 기존의 솔루션에 있어 완전히 틀린 것이다. 기존의 솔루션은 모두 제품 인증을 위해서 태그에 저장된 비밀 정보를 이용한다. 잘 알고 있는 바와 같이, 오프라인 솔루션의 경우, 태그를 인증하고 태그를 부착한 제품의 진정성을 판단하는 것은 판독기이다. 모두가 태그에 저장된 비밀 정보를 인증에 이용하기 때문에, 어느 한 판독기가 위조자에게 차용된다면, 위조자는 판독기에 저장된 비밀 정보를 해석하여 정확하게 그 비밀 정보를 위조 태그에 복제함으로써 결국은 솔루션의 보안을 깨뜨릴 수 있다. 위조자에 의한 공략에 대하여 안전한 판독기를 제조하는 것은 가능하다. 그러나, 그러한 판독기는 너무 비싸다. 마찬가지로, 보안 수단에 의해서 판독기와 태그 간의 무선 통신을 보호하는 것이 어렵다는 것을 쉽게 알 수 있다. 판독기와 태그 간의 무선 통신이 안전하다면, 그것들 간의 인증에 값비싼 판독기와 값비싼 태그가 필요하다. 그 결과, 간단하게 판독기와 태그 간의 개방 무선 통신을 도청하여 태그에 포함된 데이터를 빼낼 수 있다. 결론적으로는, 판독기를 인증하고 판독기에 의해 인증될 수 있는 값비싼 태그를 이용하지 않고 또한 판독기와 태그 간의 무선 채널이 암호화되지 않는다면, RFID 태그는 복제되기 쉽다.

우리는 여기서 값싼 태그들이 적어도 "매우 제한된 연산 전력을 가진 패시브 태그"에 의해 특징 지워진다는 것을 강조한다. 의사 난수의 생성, 해싱 및 암호화(ciphering)과 같은 기본적인 보안 요건들은 그 태그에 이용가능하지 않다. 그러한 값싼 태그에 대해, 데이터의 복제 방지(anti-clone)는 모든 제품 인증 솔루션들에게 괴로운 것일 수 있다. 복제된 태그들은 특히 오프라인 솔루션들에게 치명적이다. 네트워크가 없는 상태에서의 판독기는 진짜 태그와 복제된 태그를 구별할 수 없고, 그것은 가짜 태그가 임의의 진짜 판독기에 의해 제품 인증을 명백히 통과할 것임을 의미한다. 따라서, 복제된 태그가 붙어 있는 위조품이 판독기에 의해 진짜로서 인증될 것이기 때문에, 대량 위조가 불가피하다.

오프라인 RFID 태그들의 테이터 복제 문제를 다루는 일부 솔루션들이 제기되어 왔다. 예를 들어, 일본특허공고 제2005-130059호 공보는 복수의 암호화된 데이터를 제품에 부착된 IC 칩의 저장 영역에 기입하고 칩 안의 암호화된 데이터를 많은 회수에 걸쳐 판독함으로써, 암호화된 데이터의 해독을 어렵게 하고 따라서 데이터 복제를 어느 정도까지 어렵게 하는 솔루션을 개시한다.

그러나, 데이터 복제는 여전히 가능하다. 위조자는 충분히 많은 횟수 동안 반복해서 칩을 판독함으로써 진짜 칩 내에 저장된 모든 암호화된 데이터를 얻을 수 있고, 가짜 칩에 그 데이터를 복제할 수 있다. 그렇게 위조된 칩은 임의의 진짜 판독기에 의해 명백히 제품 인증을 통과할 수 있다.

따라서, RFID 태그에 저장된 데이터의 복제를 방지하고, 저렴함과 효율성 같은 장점들을 가지는 오프라인 인증을 위한 RFID 시스템이 요구된다.

발명이 이루고자 하는 기술적 과제

상기 문제점들을 해결하기 위해, 즉, 저가이며 효율적인 솔루션에 의해 무선 주파수 식별 태그에 저장된 데이터의 복제를 방지하기 위해, 무선 주파수 식별 시스템, 무선 주파수 식별 태그 및 무선 주파수 식별 방법을 제공한다.

발명의 구성

본 발명의 제1 양태에 의하면, 식별 코드와 한 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그, 및 상기 한 세트의 검증가능 데이터의 제1 부분을 판독하라는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 무선 주파수 식별 판독기를 포함하고, 상기 무선 주파수 식별 태그는 제어 수단을 더 포함하며, 상기 제어 수단은 상기 무선 주파수 식별 태그가 상

기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 한 세트의 검증가능 데이터의 제2 부분의 어떠한 데이터도 판독될 수 없게 하는 무선 주파수 식별 시스템이 제공된다.

본 발명의 제2 양태에 의하면, 식별 코드 및 한 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그로서, 상기 무선 주파수 식별 태그는 제어 수단을 더 포함하며, 상기 제어 수단은 상기 무선 주파수 식별 태그가 상기 한 세트의 검증가능 데이터의 제1 부분을 판독하라고 요청하는 판독 요청을 수신할 때, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 한 세트의 검증가능 데이터의 제2 부분의 어떠한 데이터도 판독될 수 없게 하는 무선 주파수 식별 태그가 제공된다.

본 발명의 제3 양태에 의하면, 식별 코드 및 한 세트의 검증가능 데이터를 무선 주파수 식별 태그에 저장시키는 단계, 및 무선 주파수 식별 판독기에 의해 상기 한 세트의 검증가능 데이터의 제1 부분을 판독하라고 요청하는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 단계를 포함하고, 상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 한 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 한 세트의 검증가능 데이터의 제2 부분의 어떠한 데이터도 판독될 수 없게 하는 무선 주파수 식별 방법이 제공된다.

본 발명의 제4 양태에 의하면, 식별 코드와 m개 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그, 및 상기 m개 세트의 검증가능 데이터 중 t 세트의 검증가능 데이터의 일부를 판독라는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 무선 주파수 식별 판독기를 포함하고, 상기 무선 주파수 식별 태그는 제어 수단을 더 포함하며, 상기 제어 수단은 상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 t 세트의 검증가능 데이터 각각의 다른 부분이 판독될 수 없게 하는 무선 주파수 식별 시스템이 제공된다.

본 발명의 제5 양태에 의하면, 식별 코드 및 m개 세트의 검증가능 데이터가 저장된 무선 주파수 식별 태그로서, 상기 무선 주파수 식별 태그는 제어 수단을 더 포함하고, 상기 제어 수단은 상기 m개 세트의 검증가능 데이터 중 t 세트의 검증가능 데이터 각각의 일부를 판독하라고 요청하는 판독 요청을 수신할 때, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작이 수행되지 않은 경우, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 t 세트의 검증가능 데이터의 각각의 다른 부분이 판독될 수 없게 하는 무선 주파수 식별 태그가 제공된다.

본 발명의 제6 양태에 의하면, 식별 코드 및 m개 세트의 검증가능 데이터를 무선 주파수 식별 태그에 저장하는 단계, 및 무선 주파수 식별 판독기에 의해 상기 m개 세트의 검증가능 데이터 중 t 세트의 검증가능 데이터 각각의 일부를 판독하라고 요청하는 판독 요청을 상기 무선 주파수 식별 태그에 송신하는 단계를 포함하고, 상기 무선 주파수 식별 태그가 상기 무선 주파수 식별 판독기로부터 상기 판독 요청을 수신할 때, 상기 t 세트의 검증가능 데이터가 잠금 동작이 수행되지 않은 경우, 상기 t 세트의 검증가능 데이터에 대해 잠금 동작을 수행함으로써, 그 후로는 상기 t 세트의 검증가능 데이터 각각의 다른 부분이 판독될 수 없게 하는 무선 주파수 식별 방법이 제공된다.

본 발명의 실시예들에 따르면, 라디오 주파수 신원확인 태그 내에 잠금 기능이 소개된다. 이에 따라, 라디오 주파수 신원확인 태그 내의 데이터의 복제는 효과적으로 방지되고, 라디오 주파수 신원확인 태크에 저장된 복수의 전자 서명들과 라디오 주파수 신원확인 태그에 의해 수행되는 잠금 기능을 통해 대량 위조품들이 방지될 수 있다.

(실시예)

본 발명의 실시예들이 이하에 설명된다.

도 1은 본 발명의 제1 실시예에 따른 RFID 시스템(100)을 보여주는 간략화된 블록도이다. RFID 시스템(100)은 RFID 태그(101)와 RFID 판독기(101)를 포함하는데, 이들은 무선 주파수 통신을 통해서 서로 통신한다. RFID 태그(101)는 RFID 판독기(102)로부터의 판독 요청 신호로부터 그 전력 모두를 획득하고 응답을 하기 위해 RFID 판독기(102)의 신호를 반사하거나 또는 부하 변조(load modlate)하는 수동 태그(passive tag)이다. RFID 태그(101)는 매우 작은 크기를 갖고 인증될 임의의 제품에 부착될 수 있다. RFID 판독기(102)는 판독 요청과 같은 데이터를 RFID 태그(101)로 보내고, RFID 태그(101)로부터의 임의의 응답 데이터를 수신한다.

도 2는 도 1에 도시된 RFID 태그(101)의 내부 구조를 보여주는 개략도이다. RFID 태그(101)는 마이크로칩(201)과 태그 결합 소자(202)를 포함한다. 마이크로칩(201)은 식별 코드 저장 영역(203), 보조 저장 영역(204), 및 제어 수단(205)을 포함한다. EPC 코드와 같은, RFID 태그(101)를 고유하게 식별하는 속성 식별 코드가 식별 코드 저장 영역에 저장된다.

EPC 코드는 EPCglobal에 의해 정의된다. EPC 코드의 일부분은 RFID 태그(101)가 부착되는 제품의 제조자를 고유하게 식별할 것이다. EPC는 RFID 태그에 저장되는 정보이며, 국제 표준에 관한 두 개의 주요 감독 기관인 UCC 및 국제 EAN에 의해 지원되는 것이다. EPC의 목적은 물리적 세계의 오브젝트에 대한 고유한 식별을 제공하는 것이다. 이는 인터넷에서 IP 어드레스를 통해서 식별하고 조직하고 통신하는 것과 비슷한 방식으로 컴퓨터 네트워크를 통해서 단일 오브젝트를 식별하고 액세스한다. EPC 코드의 구조가 이하에 간략히 설명될 것이다. EPC는 헤드 마크 및 세 개의 데이터 부분으로 구성된 한 세트의 숫자들이다. 헤드 마크는 EPC의 버젼 번호를 표시하고, 미래의 태그들의 서로 다른 길이들과 유형들을 고려해 두고 있다. 제2 부분은 제품 제조자에 해당하는 EPC의 관리자를 표시한다. 제3 부분은 제품의 정확한 범주를 표시하는 제품 클래스를 나타낸다. 제4 부분은 제품 아이템의 시퀀스 번호이다. 예를 들어, EPC 코드 01.11511D7.28A1E6.421CBA30A 에서, 01은 EPC(8비트)의 버젼을 나타내고, 11511D7은 제품 제조자의 식별 코드를 나타내고 전체가 28 비트를 포함하고(2억 6천 8백만 이상의 제조자를 표현할 수 있음), 28A1E6은 제품의 식별 코드를 나타내고 전체가 24비트를 포함하고(각 제조자는 표현된 제품의 클래스를 1천 6백만 개 이상 가질 수 있음), 421CBA30A는 제품 아이템의 시퀀스 번호를 나타내고 전체가 36비트를 포함한다(제품의 각 클래스는 나타낸 아이템을 6백 8십억 개 이상을 가질 수 있음).

검증가능한 데이터뿐만이 아니라 제조 일자와 같은 그외의 보조 정보가 보조 저장 영역(204)에 저장된다. 검증가능한 데이터를 생성하는 다수의 방법이 존재한다. 이것의 예들이 이하에 설명된다.

본 발명의 양호한 실시예에서, 검증가능한 데이터는 디지털 서명이 될 수 있다. 도2에 도시된 대로, 다수(예로 n은 양의 정수이고 1보다 큼)의 디지털 서명 $\{SIG_1, SIG_2, ..., SIG_N\}$이 보조 저장 영역에 저장된다.

각각의 제조자가 적어도 하나의 공개 키를 갖고, 디지털 서명은 EPC 콘텐츠의 디지털 서명이라고 가정한다. 이런 서명들은 제조자의 공개 키에 의해 검증가능하다. 예를 들어, n=2라고 하면, 즉, 저장 영역(204)에 저장된 두 개의 디지털 서명 SIG_1, SIG_2 가 있고, 제조자는 각각이 1024 비트인 두 개의 RSA 공개 키, PK_1, PK_2 를 가진다고 하자. 그러면, SIG_1 및 SIG_2 는, PK_0 및 PK_1 에 의해 검증가능한 EPC의 디지털 서명 및 제조 일자일 수 있다. 각각의 서명은 1024 비트를 필요로 한다. 양호하게는, 하나의 제조자가 단지 하나의 공개 키만을 요청하도록 ECDSA (ANSI X9.62) 유사 메커니즘을 사용하여 서명들이 계산된다. 이 메커니즘에 따르면, 각각의 서명은 만일 160 비트 타원 곡선과 SHA-1을 사용한다면 각각이 예를 들어 160 비트인 두 개의 부분 S 및 C를 가진다. 환언하면, 하나의 디지털 서명은 320 비트만을 소모한다. 그러나, 보안 길이는 1024 비트 RSA 디지털 서명 방식의 보안성에 필적할만하다. 부분 S 및 C에 대한 계산 방법의 예는 이하에 주어질 것이다. 디지털 서명 방식에 대한 이런 여러 선택 및 고려 사항은 당업자에게 잘 알려져 있다.

디지털 서명을 생성하는 것뿐만 아니라 검증가능한 데이터를 생성하는 방법은 대안적으로 업계에 공지된 MAC(Message Authentication Code)일 수 있다. 예를 들어, 보안 해싱 함수 및 메시지 M(EPC 코드 E와 임의의 가능한 추가의 정보를 포함함)이 주어졌을 때, n 피스의 검증가능한 데이터가 MAC_i=hash(M, key, i)(i=1,2,...n)로 계산될 수 있다. MAC_1 ~ MAC_n은 검증가능한 데이터로서 태그에 저장된다. 판독기가 검증가능한 데이터의 피스들 중의 임의의 것, 예를 들어 MAC_j를 판독했을 때, MAC_j가 hash(M, key, j)에 동등한가의 여부는 MAC 값의 시퀀스 번호 j, 관련된 메시지 M 및 판독기 자신의 메모리의 개인 키 "key"에 기초해 검증될 수 있다. 대답이 "YES"이면, 이 MAC 값은 진짜(genuine)이다. 그렇지 않은 경우, 이 MAC 값은 가짜(fake)이다. MAC는 다른 방법, 예컨대, HMAC에 의해 생성될 수 있고, 보안 해시 함수에 대한 많은 선택이 있다. 이들 모두는 본 분야에 공지되어 있다.

또 다른 예로서, 입증 가능한 데이터를 생성하는 방법은 대안적으로는 본 분야에 공지된 대칭 암호화법(symmetric encryption method)일 수 있다. 구체적으로는, 대칭 암호화 함수 SEC, 복호화 함수 SDE, 메시지 M(EPC 코드 E 및 임의의 가능한 추가 정보를 포함함)이 주어지면, n 피스의 입증 가능한 데이터가 D_i = SEC(M, key, i)(여기서, i=1, 2,...n)로서 계산될 수 있다. D_1~D_n이 입증 가능한 데이터로서 태그에 저장된다. 판독기가 입증 가능한 데이터 피스들 중 임의의 하나, 예를 들어, D_j를 판독하는 경우, SDE(D_j, key)가 M 및 j를 복호할 수 있는지의 여부가, 판독기 자체 메모리 내의 개인 키

"key", 관련 메시지 M 및 데이터의 시퀀스 넘버 j에 기초하여 검증될 수 있다. 대답이 "YES"이면, 이 입증 가능한 데이터의 피스는 진짜이다. 그렇지 않은 경우에는, 가짜이다. 대칭 암호화법에 대한 많은 선택이 있는데, 예를 들면, 3DES 및 AES가 있고, 이들 모두 본 분야에 공지되어 있다.

디지털 서명을 이용하지 않고 입증 가능한 데이터를 생성하는 상기 방식들은, 서로 다른 제품에 속하는 다수의 개인 키들이 판독기에 저장되고, 자신의 EPC에서 자신이 제품에 속한다는 것을 선언하는 태그에 저장되어 있는 입증 가능한 데이터가 판독기에 저장되어 있는 제품의 개인 키에 의해 검증될 수 있는 식으로 하여 확장될 수 있다.

디지털 서명을 사용하지 않는 상기 입증 가능한 데이터 생성 방식이 갖는 주된 문제점은, 각 제품이 서로 다른 개인 키를 가지고 있으면, 이들 방식들의 확장성이 매우 나빠진다는 것이다. 판독기가 수천 개 제품의 개인 키를 저장하고 있으면, 큰 보안상의 문제가 될 것이다. 또한, 개인 키들을 보안 방식으로 판독기에 추가하는 것이 어렵다. 한편, 모든 제품들이 하나의 개인 키를 공유하는 방식 또한 확장성이 매우 나쁘다. 그 이유는, 이런 경우에 공통적으로 인식되는 믿을만한 제3자에 의해서만 개인 키가 사용될 수 있고, 이는 제3자가 전체 제조업자의 생산품 전체에 대하여 입증 가능한 데이터를 생성하는 것을 필요로 하고, 또한 이렇게 하는 것은 매우 어렵기 때문이다.

따라서, 본 발명에서는 입증 가능한 데이터로서 디지털 서명을 이용하는 것이 바람직하다.

제어 수단(205)을 이용하여, RFID 태그(101)가 RFID 판독기로부터의 판독 요청을 수신하면, 상황에 따라서, RFID 태그의 보조 저장 영역(204) 내에 저장된 디지털 서명의 일부분이 판독될 수 없게 하는 잠금 동작을 수행한다. 제어 수단(205)의 동작은 도 4와 관련하여 후술한다.

태그 결합 소자(202)는 무선 주파수 통신을 통해 RFID 판독기(102)와 통신하는 코일 안테나일 수 있다.

도 3은 도 1에 도시된 RFID 판독기(102)의 내부 구조를 도시하는 개략적 블록도이다. RFID 판독기(102)는 프로세서(301), 무선 주파수 모듈(302), 판독기 결합 소자(303) 및 메모리(304)를 포함한다. 프로세서(301)는 RFID 판독기(102)를 제어하여, 결합 소자(303)를 통해 판독 요청을 RFID 태그(101)에 송출하기 위한 것이다. 프로세서(301)는 또한 RFID 태그(101)가 부착되어 있는 제품을 인증하도록, RFID 태그(101)로부터 수신된 응답 데이터를 분석하여 RFID 태그(101)를 인증하는 인증부(301-1)를 포함한다. 프로세서(301)의 동작은 도 5와 관련하여 후술한다. 무선 주파수 모듈(302)을 이용하여 프로세서(301)의 제어 하에서 무선 주파수 신호를 생성한다. 판독기 결합 소자(303)를 이용하여, 무선 주파수 신호를 송수신함으로써, RFID 태그(101)와 통신한다. 메모리(304)는 제품들의 공중 키들을 저장하기 위한 것이다. RFID 태그(101)의 보조 저장 영역(204)에 저장된 n개의 디지털 서명에 대응하는 디지털 서명들을 계산하기 위하여 RSA 알고리즘을 이용하는 경우, 메모리(304)에는 n개의 공중 키{PK_1, PK_2, ..., PK_n}가 저장되어 있다. 그러나, 전자 서명을 산출하기 위한 RSA 알고리즘을 사용하는 경우에, 하나의 제조를 위해, 보조 저장 영역(supplementary storage area; 204)에 얼마나 많은 전자 서명이 저장되어 있든지 간에, 그 제조의 전자 서명을 검증하기 위해 메모리(304)에 단지 하나의 공개 키가 저장되도록 요청된다.

도 4는 RFID 판독기(102)로부터 판독 요청을 수신할 때, 도 1에 도시된 RFID 태그(101)의 연산을 도시하는 순서도이다. 단계 401에서, RFID 태그(101)는 RFID 판독기(102)로부터 판독 요청을 수신하고 k 개의 전자 서명을 포함하는 디지털 서명들의 부분 집합 {SIG_{a_1}, SIG_{a_2}, ..., SIG_{a_k}}을 판독하도록 요청되는데, 여기서, k는 양의 정수이고 1≤k≤n이며, {a_1, a_2, ..., a_k} ⊂ {1, 2, ..., n}, 즉, {SIG_{a_1}, SIG_{a_2}, ..., SIG_{a_k}} ⊂ {SIG_1, SIG_2, ..., SIG_n}이다. 단계 402에서, 제어 수단(205)은 전자 서명의 집합 {SIG_1, SIG_2, ..., SIG_n}이 잠금 연산(locking operation)의 수행으로 인해 전자 서명의 또 다른 부분 집합 {SIG_{b_1}, SIG_{b_2}, ..., SIG_{b_k}}에 잠겨 있는지 여부를 결정한다. 만약 잠겨져 있다면, RFID 태그(101)는 단계 403에서 전자 서명의 부분 집합 {SIG_{b_1}, SIG_{b_2}, ..., SIG_{b_k}}를 RFID 판독기(102)로 전송한다. 그 다음, 프로세스는 끝난다. 만약 잠겨져 있지 않다면, 단계 404에서, 제어 수단(205)은 잠금 연산을 수행하여 RFID 태그(101) 내의 전자 서명의 집합 {SIG_1, SIG_2, ..., SIG_n}을 전자 서명의 부분 집합 {SIG_{a_1}, SIG_{a_2}, ..., SIG_{a_k}}로 잠근다. 그 결과, 향후에 판독 요청이 수신될 때, 전자 서명의 부분 집합 {SIG_{a_1}, SIG_{a_2}, ..., SIG_{a_k}}만이 판독될 수 있고, 전자 서명의 집합 {SIG_1, SIG_2, ..., SIG_n} 내의 그 외의 전자 서명들은 더 이상 판독될 수 없다. 다음으로, 단계 405에서, 제어 수단(205)은 RFID 태그(101)가 잠겨져 있는지 여부를 판정한다. 만약 잠겨 있지 않다면, 어떠한 연산도 수행되지 않고 프로세스는 끝난다. 만약 잠겨 있다면 프로세스는 단계 406으로 진행하고, 전자 서명의 부분 집합 {SIG_{a_1}, SIG_{a_2}, ..., SIG_{a_k}}은 RFID 판독기(102)로 송신된다. 그 다음, 프로세스는 끝난다. 본원의 제1 실시예에서, 제어 수단(205)은 예를 들어 다음 방식으로 잠금을 수행한다.

제어 수단(205)은 각각의 전자 서명 SIG_i에 대해 대응 플래그 비트 F_i가 초기값 0을 갖도록 설정하고, SIG_i가 첫 번째로 판독될 때, 그 대응 플래그 비트 F_i는 1로 설정되고, 플래그 비트 1인 전자 서명의 개수는 k에 이르며, 1 이외의 플래그 비트를 갖는 전자 서명은 더 이상 판독될 수 없다. 전자 서명을 판독할 수 없게 하는 방법으로는, 예를 들어 그들을 파기하는 방법, 예컨대, 그들을 0으로 재설정하는 방법을 포함한다. 잠금은 다른 방식으로 수행될 수 있다. 예를 들어, 태그에 명시 플래그 비트가 존재하지 않고 판독할 수 없는 전자 서명 모두 직접 파기되는 것, 예컨대, 0으로 재설정되는 것이다. 모두 0인 전자 서명은 태그에 의해 판독기로 보내질 필요가 없는 전자 서명으로서 결정될 수 있고, 또한 태그에 의해 전송된 경우에는 판독기에 의해 판독이 금지된 전자 서명인 것으로 결정될 수도 있다. 이들 둘 모두, 판독기에서 그 전자 서명들을 판독할 수 없게 하는 효과를 야기한다. 잠금 연산은 소프트웨어, 하드웨어 혹은 그들 둘의 조합에 있어 또 다른 방식으로 수행될 수 있다. 본 발명은 여기서 예로서 기술된 특정한 잠금 방식에 한정되지 않는다. 또한, RFID 태그(101)는 전자 서명의 또 다른 개수, 예컨대, k'개를 판독하도록 요청하는 판독 요청을 수신할 수도 있지만, k'가 k와 동일하든 아니든 간에 RFID 태그(101)는 최대 k개의 전자 서명의 판독을 허용할 것임을 주지해야 한다.

도 4에 도시된 RFID 태그(101)의 연산 순서에 대응하여, 도 5는 판독 요청을 RFID 태그(101)로 전송하고 RFID 태그(101)로부터 수신된 데이터에 기초하여 RFID 태그(101)를 인증하는 RFID 판독기(102)의 연산들을 도시하는 순서도이다. 여기서, RFID 판독기(102)는 RFID 태그(101)로부터 ID 코드, 예컨대, EPC 코드를 성공적으로 판독함으로써, RFID 태그(101)를 유일하게 식별하는 속성을 결정하고, 따라서 메모리에 저장된 어떤 공개 키 혹은 어떤 공개 키 집합이 사용되어 판독 전자 서명을 검증해야 하는지를 결정한다. 단계 501에서, RFID 판독기(102)의 프로세서(301)는 인덱스 집합 {1, 2, ..., n}으로부터 인덱스 부분 집합 {a_1, a_2, ..., a_k}을 랜덤하게 선택한다. 그 후, 단계 502에서, 프로세서(301)는 판독기 결합 소자(303)를 통하여, 디지털 서명 $\{SIG_{a-1}, SIG_{a-2}, ..., SIG_{a_k}\}$의 서브세트를 판독할 것을 요청하는 판독 요청을 RFID 태그(101)에 송신하도록 RFID 판독기(102)를 제어하고, RFID 태그(101)로부터의 응답 데이터를 대기하기 시작한다. 단계 503에서, 프로세서(301)는 복수 회 타임아웃(multiple time out)되었는지 여부를 결정한다. 대답이 "YES"라면, 프로세스는 단계 512로 진행하여, 인증부(301-1)가 RFID 태그(101)는 파괴된(broken) 것으로 판정한다. 태그가 파괴된 것으로 판정되기 전의 타임아웃 횟수는 필요한 대로 선택될 수 있다. 선택의 방식은 공지되어 있다. 단계 503에서, 복수회의 타임아웃이 결정되기(단계 505) 전에 RFID 태그(101)로부터 송신된 디지털 서명 $\{SIG_{b-1}, SIG_{b-2}, ..., SIG_{b-k}\}$의 서브세트가 수신되었다면, 그 후 단계 506에서, 프로세서(301)는 메모리(304)로부터 제조자(manufacturer)에 대응하는 공용키(public key)를 가져온다. 다음, 단계 507에서, 디지털 서명 $\{SIG_{b-1}, SIG_{b-2}, ..., SIG_{b-k}\}$의 서브세트는 제조자의 공용 키들을 이용하여 검증된다. 단계 508에서, 디지털 서명 $\{SIG_{b-1}, SIG_{b-2}, ..., SIG_{b-k}\}$의 서브세트의 유효성(validity)이 판정된다. 유효하지 않다면, 인증부(301-1)는 RFID 태그(101)가 가짜 태그(fake tag)인 것으로 판정하므로, RFID 태그(101)가 부착된 제품은 가짜 제품인 것이다(단계 504). 유효하다면, 그 후 단계 509에서, 인덱스 {b_1, b_2,...,b_k}의 서브세트가 단계 501에서 랜덤하게 선택된 인덱스 {a_1, a_2,...,a_k}의 서브세트와 일치하는지 여부가 판정된다. 대답이 "YES"라면, 인증부(301-1)는 RFID 태그(101)가 진짜 태그(genuine tag)인 것으로 판정한다(단계 510). 그렇지 않으면, 인증부(301-1)는 RFID 태그(101)가 이전에 판독된 것으로 판정한다(단계 511). 상기 프로세스를 통하여, RFID 판독기(102)는 RFID 태그(101)의 진정성(authenticity)을 인증할 수 있다.

상기 설명으로부터, 태그에서 "잠금(locking)" 동작을 수행하는 것의 결과로 태그 복제(tag cloning)가 금지되는 것을 알 수 있다. 먼저, 가짜 제품을 검출하는 확률(probability)을 계산하기 위한 예로서 k=1을 취한다. 위조자(forger)는 진짜 태그에 저장된 모든 n 디지털 서명들 중 하나만 획득할 수 있다. 다른 n-1 디지털 서명들은 절대로 판독되지 않을 것이다. 따라서, 가짜 태그는 하나의 유효한 디지털 서명을 포함할 뿐이다. 따라서, 클로닝된(cloned) 태그는 더 이상 관측되지 않는다. 이러한 가짜 태그가 진정한 판독기(reader)에 의해 인증된 경우에, 판독기는 {1, 2, ... n} 으로부터 i를 랜덤하게 선택하고 SIG_i를 판독할 것을 요청할 것이므로, 가짜 태그는 (n-1)/n의 확률로 검출될 수 있을 것이다. 일반적으로 p 가짜 태그는 $1-(1/n)^p$ 의 확률로 검출될 수 있다. 예로서 n=2를 들자면, 하나의 가짜 태그는 50%의 확률로 검출을 회피할 수 있지만, 1다스(dozen)의 가짜 태그는 0.025%보다 낮은 확률로만 검출을 회피할 수 있다. 또는, 달리 말하면 1다스의 가짜 태그는 99.97%보다 높은 확률로 검출될 수 있다. 만약, $1<k<n*0.5$라면, 가짜 태그가 검출될 확률은 더욱 높아질 것이 명백하다. 만약, $k=n*0.5$라면, 검출 확률이 최고이다. 예를 들어, n=12이면, 즉 12 개의 디지털 서명이 태그 내에 저장되며, k=6이면, 즉, 6개의 디지털 서명이 12개의 디지털 서명으로부터 인증을 위하여 랜덤하게 선택된다. 가짜 태그 내에 6 개 이하의 디지털 서명이 존재하므로, 가짜 태그는 $1-1/C_{12}^{6}$, 즉 99.89% 의 확률로 검출될 수 있다. 이때, 2 개의 디지털 서명은 0.00012%보다 낮은 확률로 검출을 회피할 수 있다. 본 발명에 의해 제공된 잠금 기능을 갖는 RFID 태그를 포함하는 RFID 시스템을 이용하는 제품 인증 솔루션이 많은 위조본들을 효과적이고 효율적으로 억제할 수 있다고 결론짓는 것이 이제는 합리적이다.

본 발명의 제2 실시예에서, RFID 태그는 디지털 서명 세트 {SIG_1, SIG_2, ..., SIG_n} 외에 m-1개의 디지털 서명 세트를 포함하는데, m은 양수이고 m>1 이며, 각각의 디지털 서명 세트의 구성 방식은 디지털 서명 세트 {SIG1, SIG2, ..., SIGn}의 구성 방식과 동일하다. 도 6은 본 발명의 제2 실시예에 따른 RFID 태그 (601) 및 RFID 판독기 (602) 를 포함하는 RFID 시스템 (600) 을 도시한다. 도 7은 본 발명의 제2 실시예에 따른 RFID 태그 (601) 의 내부 구성을 도시하는 개략도이다. 도 8은 본 발명의 제2 실시예에 따른 RFID 판독기 (602) 의 내부 구성을 도시하는 개략도이다. 도 7에 도시한 바와 같이, RFID 태그 (601) 는 마이크로칩 (701) 및 태그 결합 소자(702) 를 포함한다.

마이크로칩(701)은 식별 코드 기억 영역(703), 보조 기억 영역(704) 및 제어 수단(705)을 포함한다. RFID 태그(601)의 보조 기억 영역(704)에는, n개의 디지털 서명의 세트 m개가 기억되어 있으며, n개의 디지털 서명의 세트 m개는 디지털 서명들의 매트릭스 {$SIG_{i,j}$}를 형성하고, 여기서, 1≤i≤m, 1≤j≤n이다. 도 8에 도시된 바와 같이, RFID 판독기(602)는 프로세서(801), 무선 주파수 모듈(802), 판독기 결합 소자(803) 및 메모리(804)를 포함한다. 프로세서(801)는 인증부(801-1)를 더 포함한다.

디지털 서명들의 각각의 세트의 경우, 도 9에 도시된 바와 같이, RFID 태그(601)의 동작들은 도 4와 결합하여 전술한 RFID 태그(101)의 동작들과 유사하다. 도 9는 RFID 판독기(602)로부터의 판독 요청의 수신시 도 6에 도시된 RFID 태그(601)의 동작들을 도시하는 흐름도이다. 단계(901)에서,RFID 태그(601)는 RFID 판독기(602)로부터 판독 요청을 수신하고, i번째 디지털 서명 세트 {SIG_{i,a_1}, SIG_{i,a_2},⋯,SIG_{i,a_k}}의 디지털 서명들의 서브세트를 판독하도록 요청받으며, 여기서, 1≤i≤m, 1≤k≤n 및 {a_1, a_2, ⋯, a_k} ⊂ {1, 2, ⋯, n}, 즉, {SIG_{i,a_1}, SIG_{i,a_2},⋯,SIG_{i,a_k}} ⊂ {$SIG_{i,1}$, $SIG_{i,2}$,⋯,$SIG_{i,n}$}이다. 단계(902)에서, 제어 수단(705)은, 잠금 동작을 수행한 것으로 인해 i번째 디지털 서명 세트 {$SIG_{i,1}$, $SIG_{i,2}$,⋯,$SIG_{i,n}$}가 디지털 서명들의 다른 서브세트 {SIG_{i,b_1}, SIG_{i,b_2},⋯,SIG_{i,b_k}}로 잠겨졌는지를 판정한다. i번째 디지털 서명 세트가 잠겨진 것으로 판정된 경우, 단계(903)에서 RFID 태그(601)는 디지털 서명들의 서브세트 {SIG_{i,b_1}, SIG_{i,b_2},⋯,SIG_{i,b_k}}를 RFID 판독기(602)에 송신한다. 그러고 나서, 프로세스는 종료한다. i번째 디지털 서명 세트가 잠겨지지 않았다면, 단계(904)에서, 제어 수단(705)은 잠금 동작을 수행하여, RFID 태그(601) 내의 i번째 디지털 서명 세트 {$SIG_{i,1}$, $SIG_{i,2}$,⋯,$SIG_{i,n}$}를 디지털 서명들의 서브세트 {SIG_{i,a_1}, SIG_{i,a_2},⋯,SIG_{i,a_k}}로 잠근다. 그 결과로서, 판독 요청이 추후에 수신되면, 디지털 서명들의 서브세트 {SIG_{i,a_1}, SIG_{i,a_2},⋯,SIG_{i,a_k}}만이 판독될 수 있고, i번째 디지털 서명 세트 {$SIG_{i,1}$, $SIG_{i,2}$,⋯,$SIG_{i,n}$} 내의 다른 디지털 서명들은 더 이상 판독될 수 없다. 다음으로, 단계(905)에서, 제어 수단(705)은 RFID 태그(601) 내의 i번째 디지털 서명 세트가 잠겨졌는지를 판정한다. RFID 태그(601) 내의 i번째 디지털 서명 세트가 잠겨지지 않았다면, 어떠한 동작도 수행되지 않고 프로세스는 종료한다. RFID 태그(601) 내의 i번째 디지털 서명 세트가 잠겨졌다면, 프로세스는 단계(906)로 진행하고, 단계(906)에서, 디지털 서명들의 서브세트 {SIG_{i,a_1}, SIG_{i,a_2},⋯,SIG_{i,a_k}}가 RFID 판독기(602)에 전송된다. 본 발명의 제2 실시예에서, 제어 수단(705)은, 예를 들어, 제어 수단(705)이 각 디지털 서명 $SIG_{i,j}$에 대하여 대응하는 플래그 비트 $F_{i,j}$를 초기값 0으로 설정하고, SIG_i가 처음으로 판독되면, 그의 대응하는 플래그 비트 $F_{i,j}$는 1로 설정되고, 플래그 비트가 1인 i번째 세트 내의 디지털 서명들의 수가 k에 도달하면, 플래그 비트가 1이 아닌 i번째 세트 내의 디지털 서명들은 더 이상 판독될 수 없는 방식으로 잠금을 수행한다. 디지털 서명들을 판독불가능하게 하기 위한 방법들은 예를 들어 디지털 서명들을 0들로 리셋하는 것과 같이 디지털 서명들을 파기하는 것을 포함한다. 잠금은 다른 방법들로 수행될 수 있다. 예를 들어, 태그 내에 명시적 플래그 비트들이 존재하지 않으며, 모든 판독불가능한 디지털 서명들이 직접 파기 예를 들어, 0들로 리셋된다. 모두 0들로 되어 있는 디지털 서명들은 판독기에 전송될 필요가 없는 디지털 서명들로서 태그에 의해 판정될 수 있거나, 또는 태그에 의해 전송되고 있는 경우에 판독되는 것이 금지된 디지털 서명들로서 판독기에 의해 판정될 수 있다. 양방 모두 디지털 서명들이 판독기에 판독불가능하게 되는 결과를 가져온다. 잠금 동작은 소프트웨어, 하드웨어 또는 이들의 조합으로 다른 방법들로 수행될 수 있다는 것이 이 기술분야의 당업자들에게 자명하다. 본 발명은 예들로서 본 명세서에 예시된 특정 잠금 방법들로 한정되지 않는다. RFID 태그(601)는 i번째 세트의 디지털 서명들의 다른 수 예를 들어, k'를 판독하도록 요청하는 판독 요청을 수신하는 것이 또한 가능하지만, k'가 k와 동일하고 안 하고는 문제가 되지 않으며, RFID 태그(601)는 i번째 세트의 많아야 k개의 디지털 서명들이 판독되는 것을 허용할 것이라는 것을 주지하자. 또한, RFID 태그(601)는 i번째 디지털 서명 세트를 판독하는 판독 요청을 수신하고, i>m인 것이 가능하다. 이 경우, RFID 태그(601)의 제어 수단(705)은 오류 요청으로서 판독 요청을 판정하고, 그것에 응답하지 않을 것이다.

도 9에 도시된 RFID 태그(601)의 동작 흐름에 대응하여, 도 10은 RFID 태그(601)에 판독 요청을 전송하고 RFID 태그(601)로부터 수신한 데이터에 기초하여 RFID 태그(601)를 인증하는 RFID 판독기(602)의 동작들을 도시하는 흐름도이다.

본 명세서에서는, RFID 판독기(602)는 식별 코드, 예를 들어, EPC 코드를 RFID 태그(601)로부터 성공적으로 판독하였고, 이에 따라 RFID 태그(601)를 고유하게 식별하는 속성을 결정하였으며, 따라서 판독 디지털 서명들을 검증하기 위해 이용되어야 하는, 메모리 내에 기억된 공개키 또는 공개키 세트를 결정하였다는 것을 가정한다. 단계(1001)에서, RFID 판독기(602)의 프로세서(801) 내의 카운터(도시되지 않음)의 값 i가 1로 설정된다. 다음으로, 단계(1002)에서, 프로세서(801)는 지수들의 세트 {1, 2, …, n}로부터 지수들의 서브세트 {a_1, a_2, …, a_k}를 랜덤하게 선택한다. 다음으로, 단계(1003)에서, 프로세서(801)는 RFID 판독기(602)를 제어하여 판독기 결합 소자(803)를 통해 RFID 태그(601)에 판독 요청을 전송함으로써, i번째 디지털 서명 세트의 디지털 서명들의 서브세트 $\{SIG_{i,a_1}, SIG_{i,a_2},\cdots,SIG_{i,a_k}\}$를 판독하도록 요청하고, RFID 태그(601)로부터의 응답 데이터를 기다리기 시작한다. 단계(1004)에서, 프로세서(801)는 복수회 타임 아웃되었는지를 판정한다. 그 대답이 "예"이면, 단계(1005)에서, 프로세스는 단계(1015)로 진행하고, 단계(1015)에서, 인증부(801-1)는 파기(break)될 RFID 태그(601)를 판정한다. 태그가 파기되어야 하는 것으로 판정되기 전의 타임 아웃의 횟수는 필요에 따라 선택될 수 있다. 선택 방법은 이 기술분야의 당업자들에게 잘 알려져 있다. 만약 단계(1004)에서, 다수의 타임 아웃 횟수가 결정되기 전에(단계(1006)) RFID 태그(601)로부터 전송된 디지털 서명들의 서브세트 $\{SIG_{i,b_1}, SIG_{i,b_2},\cdots,SIG_{i,b_k}\}$가 수신되었다면, 단계(1007)에서, 프로세서(801)는 메모리(804)로부터 제조자에 대응하는 공개 키들을 인출한다. 다음으로, 단계(1008)에서, 디지털 서명들의 서브세트 $\{SIG_{i,b_1}, SIG_{i,b_2},\cdots,SIG_{i,b_k}\}$가 제조자의 공개키들을 이용하여 검증된다. 단계(1009)에서, 디지털 서명들의 서브세트 $\{SIG_{i,b_1}, SIG_{i,b_2},\cdots,SIG_{i,b_k}\}$의 유효성이 판정된다. 디지털 서명들의 서브세트 $\{SIG_{i,b_1}, SIG_{i,b_2},\cdots,SIG_{i,b_k}\}$가 유효하지 않다면, 인증부(801-1)는, RFID 태그(601)가 가짜(fake) 태그이고, 이에 따라 그 RFID 태그(601)가 부착되어 있는 제품이 가짜 제품임을 판정한다(단계(1005)). 그것이 유효하면, 단계 1010에서, 하위 인덱스 세트 {b_1, b_2, ..., b_k}이 단계 1001에서 무작위로 선택된 하위 인덱스 세트 {a_1, a_2, ..., a_k}와 동일한지가 판정된다. 대답이 "예"이면, 인증부(801-1)는 RFID 태그(601)가 진짜 태그라고 판단한다(단계 1011). 아니면, 프로세서는 단계 1012에서 카운터의 값 i를 1만큼 증분시키고, 단계 1013에서 i>m인지를 판정한다. i>m이면, 인증부(801-1)는 RFID 태그(601)가 단계 1014 전에 판독되었다고 판단하고, 아니면 프로세스는 단계1002로 돌아가서 단계 1002 및 후속 흐름을 반복한다. 상기 프로세스를 통해, RFID 판독기(602)는 RFDI 태그(601)를 인증할 수 있다.

다수의 디지털 서명 세트를 채택하는 이점은 명확하다. m 세트인 경우, 적어도 m회 동안 판독기에 의해 실제 제품이 믿을만한 것으로 인증될 것이라는 점을 보장할 수 있다. 이것은 때로 제품이 선물로 구입되고, 소비되기 전에 여러 사람들을 거칠 수 있기 때문에 유용하다. 이러한 구성에서, 구매자 또는 최종 소비자뿐만 아니라, 중간업자들은 제품을 인증하도록 의도할 수도 있다. m 세트가 태그에 저장되면, 적어도 m명이 제품을 믿을만한 것으로 증명할 것이다.

상기 제2 실시예에 대한 대안으로서, 인증시, FRID 판독기(602)는 매번 RFID 태그(601) 내의 복수의 디지털 서명 세트를 판독하도록 요청하고 복수의 디지털 서명 세트에 대한 판독 결과들에 기초하여 태그를 인증할 수 있다. 예를 들어, RFID 판독기(602)는 제1 디지털 서명 세트의 하위 디지털 서명 세트 $\{SIG_{1,a_1}, SIG_{1,a_2}, ..., SIG_{1,a_k}\}$를 판독하도록 요청하고, 이어서 태그로부터 반환된 하위 디지털 서명 세트 $\{SIG_{1,b_1}, SIG_{1,b_2}, ..., SIG_{1,b_k}\}$를 수신한 후, 제2 디지털 서명 세트의 하위 디지털 서명 세트 $\{SIG_{2,a_1}, SIG_{2,a_2}, ..., SIG_{2,a_k}\}$를 판독하도록 요청하고 이어서 태그로부터 반환된 하위 디지털 서명 세트 $\{SIG_{2,b_1}, SIG_{2,b_2}, ..., SIG_{2,b_k}\}$를 수신하며, 등등 계속해서, t번째 디지털 서명 세트의 하위 디지털 서명 세트 $\{SIG_{t,a_1}, SIG_{t,a_2}, ..., SIG_{t,a_k}\}$을 판독하도록 요청하고, 이어서 태그로부터 반환된 $\{SIG_{t,b_1}, SIG_{t,b_2}, ..., SIG_{t,b_k}\}$을 수신한다. t개의 디지털 서명 세트들을 수신한 후, RFID 판독기(602)는 이하와 같이 판단한다. 반환된 t개의 디지털 서명 세트들의 임의의 디지털 서명이 무효이면, RFID 태그(601)가 파손된 것으로 판정될 수 있고; 모든 디지털 서명이 유효이면, 그리고 $1\le i\le t$를 만족하는 임의의 i에 대해, 하위 인덱스 세트 {b_1, b_2, ..., b_k}이 하위 인덱스 세트 {a_1, a_2, ..., a_k}과 동일하면, 태그는 진짜 태그로 판정될 수 있고; 아니면, 태그가 전에 판독되었다고 판정될 수 있다.

대안의 방식의 이점은 위조 제품이 검출될 수 있는 가능성을 상당히 증가시킨다는 것이다. 또한, 위조 제품들을 검출할 가능성을 계산하기 위한 예로서 k=1이라고 하자. 하나의 가짜 태그에 대해, 그것에 의해 반환된 t 세트 내의 t 디지털 서명들이 판독기에 의해 요청된 t 디지털 서명들과 완전히 일치할 가능성은 $(1/n)^t$이다. 따라서, 위조 태그는 $1-(1/n)^t$의 확률로 검출가능할 것이다. 또한 예로서 n=2로 하면, t=12인 경우, 하나의 가짜 태그는 99.97%의 확률로 검출가능할 것이다.

당연히, 검출 확률은 태그가 진짜로서 인증될 수 있는 횟수를 감소시키는 것을 희생으로 하여 증가될 수 있다. 예를 들어, 태그 내에 m=24 디지털 서명 세트가 존재한다고 가정하자. 각각의 인증에 대해, 판독기가 하나의 디지털 서명 세트를 판독하도록 요청한다면, 태그는 적어도 24회 믿을만한 것으로서 인증될 수 있다. 그러나, 각 인증에 대해 판독기가 12개의 디지털 서명 세트를 판독하도록 요청하면, 단지 태그는 적어도 2회 믿을만한 것으로서 인증될 수 있다.

본 발명의 제3 실시예를 이하에 설명한다. 제3 실시예는 RFID 판독기가 RFID 태그에 판독 요청을 보내는 경우, 한번에 다수의 디지털 서명을 포함하는 하위 디지털 서명 세트를 요청하지 않지만 매번 하나의 디지털 서명을 요청한다는 점에서 제1 실시예와 상이하다. 이 실시예는 잠금에 의해 제1 실시예와 동일한 태그-클론 방지 효과를 실현하고, 또한 RFID 태그의 간단한 구현의 이점을 소유한다. 이러한 실시예는 도 11 내지 15를 참조하여 설명될 것이다.

도 11은 발명의 제3 실시예에 따른 RFID 시스템(1100)을 도시한다. 제1 실시예에서와 같이, RFID 시스템(1100)은 RFID 태그(1101) 및 RFID 판독기(1102)를 포함한다.

도 12는 도 11에 도시된 RFID 태그(1101)의 내부 구조를 도시하는 개략도이다. 제1 실시예에서와 같이, RFID 태그(1101)는 마이크로칩(1201) 및 태그 결합 소자(1202)를 포함한다. 마이크로칩(1201)은 EPC 코드 저장 영역(1203), 보완 저장 영역(1204) 및 제어 수단(1205)을 포함한다.

도 13은 도 11에 도시된 RFID 판독기(1102)의 내부 구조를 도시하는 개략적인 블럭도이다. 제1 실시예에서와 같이, RFID 판독기(1102)는 프로세서(1301), 무선 주파수 모듈(1302), 판독기 결합 소자(1303) 및 메모리(1304)를 포함한다. 프로세서(1301)는 인증부(1301-1)를 더 포함한다.

도 14는 RFID 판독기(1102)로부터 디지털 서명 SIG_i에 대한 판독 요청을 수신했을 때, 도 11에 도시된 RFID 태그(1101)의 동작들을 도시하는 흐름도이다. 본 실시예에서는, 상술한 바와 같이, RFID 태그(1101)에 n(n>1)개의 디지털 서명들의 세트 $\{SIG_1, SIG_2, ..., SIG_n\}$가 저장되어 있고, RFID 판독기(1102)는 그 메모리(1304)에 RFID 태그(1101)와 관련된 제품의 제조업자에 대응하는 적어도 하나의 공개 키를 저장하고 프로세서(1301)의 제어 하에서 RFID 태그(1101)로 판독 요청들을 보낸다고 가정한다. 또한, 인증부(1301-1)에 의해 확실성에 대한 결론이 그려지기 전에 k개의 디지털 서명들이 판독되어야 한다고 가정한다. 단계 1401에서, RFID 태그(1101)는 SIG_i를 판독하도록 요청하는 RFID 판독기(1102)로부터의 판독 요청을 수신한다. 단계 1402에서, RFID 태그(1101)의 제어 수단(1205)은 잠겨진 디지털 서명들의 수 x를 결정한다. 그 후 단계 1403에서, 제어 수단(1205)은 x가 k와 동일한지를 판정한다. 결과가 긍정이면, 즉 x=k이면, 단계 1404에서, RFID 태그(1101)는 태그 결합 소자(1202)를 통해 RFID 판독기(1102)에 태그가 잠겨져 있다는 것을 나타내는 플래그 Tag_Is_Locked를 보낸다. 다음으로, 단계 1405에서, RFID 태그(1101)의 제어 수단(1205)이 SIG_i가 잠겨져 있는지의 여부를 판정한다. 만약 잠겨져 있다면, 단계 1406에서 RFID 태그(1101)가 SIG_i를 태그 결합 소자(1202)를 거쳐 RFID 판독기(1102)에 송신한다. 처리가 종료되고 RFID 태그(1101)가 스탠바이 상태로 복귀하여 RFID 판독기(1102)로부터 다음 판독 요청을 대기한다. 단계 1405에서 SIG_i가 잠겨져 있지 않은 것으로 판정되면, 동작이 수행되지 않고 처리는 종료되며 RFID 태그(1101)는 스탠바이 상태로 복귀한다. 반면에, 단계 1403에서 제어 수단(1205)의 결과가 부정이면, 즉 x가 k와 같지 않으면, 단계 1407에서 제어 수단(1205)이 x가 k보다 작은지의 여부를 판정한다. 그 결과가 부정이면, 동작이 수행되지 않고 RFID 태그는 스탠바이 상태로 복귀된다. 그 결과가 긍정이면, 단계 1408에서 RFID 태그(1101)가 플래그 Tag_Not_Locked를 태그 결합 소자(1201)를 거쳐 RFID 판독기(1102)에 송신하여, 태그가 잠겨져 있지 않았음을 나타낸다. 단계 1409에서 제어 수단(1205)이 SIG_i를 잠근다. 본 발명의 제3 실시예에서, 제어 수단(1205)은 예를 들어 다음의 방식으로 잠금을 수행한다. 각 디지털 서명이 처음으로 판독될 때 제어 수단(1205)은 대응하는 플래그 비트 F_i를 각 디지털 서명 SIG_i에 대하여 초기값 0으로 설정하고, 그 대응하는 플래그 비트가 1로 설정되고, 플래그 비트 1을 갖는 디지털 서명의 수가 k에 도달할 때 1 이외의 플래그 비트를 갖는 디지털 서명이 더 이상 판독될 수 없다. 판독할 수 없는 디지털 서명을 랜더링하기 위한 방식은 예를 들어 이들을 소실시키는 것, 즉 이들을 제로로 재설정하는 것을 포함한다. 잠금 동작이 다른 방식으로 소프트웨어, 하드웨어 또는 이들의 결합으로 실행될 수 있다는 것은 당업자에게 자명하다. 본 발명은 예시와 같이 여기서 개시된 특정 잠금 방식에 한정되지 않는다. SIG_i가 단계 1409에서 잠겨지면, 처리는 단계 1405로 진행하고 단계 1405에서 종료까지의 상술된 흐름이 수행된다. 마지막으로, RFID 태그(1101)는 스탠바이 상태로 복귀하여, RFID 판독기(1102)로부터 다음의 판독 요청을 대기한다. RFID 태그(1101)가 디지털 서명의 또 다른 수, 즉 k'를 판독하도록 요청하는 판독 요청을 수신하지만, k'가 k와 같거나 또는 같지 않을지라도, RFID 태그(1101)는 많아야 k 디지털 서명이 판독되도록 할 것이 가능하다는 점을 주지하자.

도 14에 나타낸 RFID 태그(1101)의 동작 흐름에 대응하여, 도 15는 판독 요청을 RFID 태그(1101)에 보내고 RFID 태그(1101)로부터 수신된 데이터에 기초하여 RFID 태그(1101)를 인증하는 RFID 판독기(1102)의 동작을 나타내는 흐름도이다. RFID 판독기(1102)는 식별 코드, 즉 EPC 코드를 RFID 태그(1101)로부터 성공적으로 판독하여, RFID 태그(1101)를 고유하게 식별하는 속성을 판정하고, 그러므로 메모리에 저장된 공개 키 또는 공개 키들이 판독된 디지털 서명들을 검증하는데 사용되어야 한다는 것이 가정된다. 먼저, 단계 1501에서, RFID의 판독기(1102)의 프로세서(1301)가 k 지표를 포함

하는 지표의 서브세트 {a_1, a_2, …, a_k}를 랜덤하게 선택한다. 단계 1502에서, 프로세서(1301)는 1을 포함하는 카운터(도시안됨)의 값 i를 설정한다, 즉 i=1로 하며, 여기서 i 값은 지표들의 서브세트에 첨자로 나타낸다. 그리고 단계 1503에서, 프로세서(1301)는 무선 주파수 모듈(1302)이 a_i번째 서명 SIG_{a_i}를 판독하도록 요청하는 판독 요청을 생성하고 그 판독 요청을 판독기 결합 소자(1303)를 거쳐 RFID 태그(1101)에 보내도록 지시한다. 단계 1504에서, RFID 판독기(1102)는 RFID 태그(1101)로부터 잠금 상태의 플래그를 수신한다. 단계 1505에서, 프로세서(1301)는 i가 1과 같은지의 여부를 판정하고 RFID 태그(1101)가 수신된 플래그에 기초하여 잠겨져 있는지의 여부를 판정한다. i가 1과 같지 않거나 RFID 태그(1101)가 잠겨져 있지 않으면, 단계 1506에서 RFID 태그(1101)로부터 송신된 SIG_{a_i}가 수신되어 있는지의 여부를 프로세서(1301)가 판정한다. 수신되어 있으면, 단계 1507에서 프로세서(1301)는 SIG_{a_i}가 유효한지의 여부를 판정한다. 여기서 유효성을 판정하는 방식은 다음과 같다. 프로세서(1301)가 RFID 태그(1101)와 관련되는 제품의 제조사에 속하는 미리 결정된 하나 이상의 공개 키들을 판독하고, 하나 이상의 공개 키들을 갖는 디지털 서명을 검증한다. 디지털 서명이 유효하면, 단계 1508에서 값 i가 1 만큼 증가되고, 단계 1509에서 프로세서(1301)가 i가 k보다 큰지의 여부를 판정한다. i>k이면, 처리는 단계 1501로 진행하고, 여기서 프로세서(1301)의 인증부(1301-1)는 RFID 태그(1101)가 진짜 태그인 것을 판정한다. 단계 1509에서의 결과가 i가 k보다 크지 않으면, 프로세서는 단계 1503으로 복귀하고 흐름은 반복된다. 반면에, 단계 1506 또는 1507에서의 결과가 부정이면, 단계 1518에서 프로세서(1301)의 인증부(1301-1)가 RFID 태그(1101)가 거짓 태그임 것으로 판정할 수 있다. 반면에, 단계 1505에서 결과가 긍정이면, 즉 i=1이면 태그가 잠겨지고, 단계 1511에서 RFID 판독기(1102)가 i번째 서명 SIG_i에 대한 판독 요청을 판독기 결합 소자(1301)를 거쳐 RFID 태그(1101)에 보내도록 프로세서(1301)가 지시한다. 다음으로, 단계 1512에서 RFID 태그로부터 수신된 SIG_i가 수신되었는지의 여부가 판정된다. 수신되면, 단계 1513에서 프로세서(1301)가 SIG_i가 유효한지의 여부를 판정한다. 유효성 판정에 대한 방식은 상술된 바와 동일하다. 무효하면, 처리는 단계 1518로 진행하고, 인증부(1301-1)는 RFID 태그(1101)가 거짓 태그인 것으로 판정한다. 단계 1513에서 SIG_i가 유효한 것으로 판정되면, 단계 1514에서 프로세서(1301)가 i값을 1만큼 증가시킨다. 한편, SIG_i가 단계 1512에서 수신되지 않으면 처리는 단계 1514로 진행하고, 프로세서(1301)가 i값을 1만큼 증가시킨다. 그리고 단계 1515에서 프로세서(1301)가 i가 n보다 큰 지의 여부를 판정한다. i가 n보다 크지 않으면, 처리는 단계 1511로 복귀하고, 단계는 i가 1만큼 증가되는 조건 하에서 반복된다. i>n이면, 단계 1516에서 프로세서(1301)가 수신된 서명의 수가 k와 같은지의 여부를 판정한다. 답이 "예"이면, 단계 1517에서 인증부(1301-1)는 RFID 태그(1101)가 이전에 판독된 것으로 판정한다. 그렇지 않으면, RFID 태그(1101)가 거짓 태그인 것으로 판정될 수 있고 처리는 단계 1518로 진행한다. 단계 1510에서, 단계 1518 또는 단계 1517에서, 인증부(1301-1)가 RFID 태그(1101)의 인증을 판정한 후 인증 처리는 종료된다.

도 16은 본 발명의 제4 실시예에 따른 RFID 시스템(1600)을 도시한다. 제2 실시예에서와 같이, RFID 시스템(1600)은 RFID 태그(1601) 및 RFID 판독기(1602)를 포함한다.

도 17은 도 16에 도시한 RFID 태그(1601)의 내부 구조를 나타내는 개략도이다. 제2 실시예에서와 같이, RFID 태그(1601)는 마이크로칩(1701) 및 태그 결합 소자(1702)를 포함한다. 마이크로칩(1701)은 EPC 코드 저장 영역(1703), 보조 저장 영역(1704) 및 제어 수단(1705)을 포함한다.

도 18은 도 16에 도시한 RFID 판독기(1602)의 내부 구조를 나타내는 개략 블록도이다. 제2 실시예에서와 같이, RFID 판독기(1602)는 프로세서(1801), 무선 주파수 모듈(1802), 판독기 접속 소자(1803) 및 메모리(1804)를 포함한다. 프로세서(1801)는 인증부(1801-1)를 더 포함한다.

도 19는, RFID 판독기(1602)로부터 디지털 서명 $SIG_{j,i}$에 대한 판독 요청 수신 시, 도 16에 도시한 RFID 태그(1601)의 동작을 도시하는 흐름도이다. 이 실시예에서는, 전술한 바와 같이, RFID 태그(1601)에 저장된 n(n>1) 디지털 서명의 m 세트가 존재하고, 이는 디지털 서명의 매트릭스 $\{SIG_{j,i}\}$, $1 \le j \le m$, $1 \le i \le n$을 형성한다고 가정한다. 단계(1901)에서, RFID 태그(1601)는 $SIG_{j,i}$를 판독하는 것을 요청하는 RFID 판독기(1602)로부터 판독 요청을 수신한다. 단계(1902)에서, RFID 태그(1601)의 제어 수단(1705)은 j가 m보다 작은지 여부를 판정한다. 그 결과가 부정이면, 작동은 실행되지 않고, RFID(1601)는 대기 상태로 돌아간다. 단계(1902)에서의 결과가 긍정이면, 단계(1903)에서, 제어 수단(1705)은 잠겨진 디지털 서명의 수 x를 결정한다. 그러면, 단계 (1094)에서, 제어 수단(1705)은 x가 k와 동일한지 여부를 판정한다. 그 결과가 긍정이면, 즉 x=k이면, 단계(1905)에서, RFID 태그(1601)는 태그 결합 소자(1702)를 통해 플래그 Set_Is_Locked를 RFID 판독기(1602)에 송신하여, j번째 세트가 잠겨졌음을 나타낸다. 그 다음, 단계(1906)에서, RFID 태그(1601)의 제어 수단(1705)은 $SIG_{j,i}$가 잠겨졌는지 여부를 판정한다. 잠겨져 있으면, 단계(1907)에서, RFID 태그(1601)는 태그 결합 소자(1702)를 통해 $SIG_{j,i}$를 RFID 판독기(1602)에 송신한다. 그 프로세스가 종료되고, RFID 태그(1601)가 대기 상태가 되면,

RFID 판독기(1602)로부터의 그 다음 판독 요청을 대기한다. 단계(1906)에서 $SIG_{j,i}$는 잠겨져 있지 않았다고 판정되면, 동작은 실행되지 않고, 그 프로세스는 종료되며, RFID 태그(1601)는 대기 상태로 돌아간다. 이에 반해, 단계(1904)에서 제어 수단(1705)에 의한 결과가 부정이면, 즉 x가 k와 동일하지 않으면, 단계(1908)에서, 제어 수단(1705)은 x가 k보다 작은지를 판정한다. 그 결과가 긍정이면, 작동은 실행되지 않고, RFID 태그(1601)는 대기 상태로 돌아간다. 그 결과가 긍정이면, 단계(1909)에서, RFID 태그(1601)는 태그 결합 소자(1702)를 통해 플래그 Set_Not_Locked를 RFID 판독기(1602)에 송신하여, j번째 세트가 잠겨져 있지 않음을 나타낸다. 그러면, 단계(1910)에서, 제어 수단은 $SIG_{j,i}$를 잠근다. 본 발명의 일 실시예에서, 제어 수단(1705)은 예를 들어, 다음과 같은 방식으로 잠금을 수행한다: 제어 수단(1705)은, 각 디지털 서명 $SIG_{j,i}$에 대해 대응하는 플래그 비트 $F_{j,i}$를 초기값 0으로 설정하고, 각 디지털 서명이 최초로 판독될 때, 그 대응하는 플래그 비트는 1로 설정되고, 일 세트에서 플래그 비트 1을 갖는 디지털 서명의 수가 k에 도달하면, 그 세트에서 1 이외의 플래그 비트를 갖는 디지털 서명은 더 이상 판독될 수 없다. 판독불가능한 디지털 서명을 렌더링하기 위한 방법은, 예를 들어, 이 서명을 0으로 리셋하는 것과 같이 서명을 무효로 하는(destroying) 방법을 포함한다. 잠금 동작이 소프트웨어, 하드웨어, 또는 이들의 조합으로 다른 방식으로도 수행될 수 있다는 것은 당업자에게 명백한 것이다. 본 발명은 본 명세서에서 예로서 설명된 특정한 잠금 방법으로 제한되는 것은 아니다. $SIG_{j,i}$가 단계 1910에서 잠겨지면, 프로세스는 단계 1906으로 진행하여, 단계 1906으로부터 종료까지의 상술한 플로우가 수행된다. 마지막으로, RFID 태그(1601)는 대기 상태로 돌아가고, RFID 판독기(1602)로부터 다음에 판독될 요청을 대기한다. 또한, RFID 태그(1601)가 또 다른 수, 예를 들어, j^{th} 세트의 디지털 서명의 k'를 판독하도록 요청하는 판독 요청을 수신할 수도 있지만, k'가 k와 동일한 지 여부에 관계없이, RFID 태그(1601)는 j^{th} 세트의 디지털 서명에서 최대한 k가 판독되도록 허용할 것이라는 점을 주지해야 한다. 또한, RFID 태그(1601)는 디지털 서명의 j^{th} 세트를 판독하기 위한 판독 요청을 수신하고, 여기에서 j는 m보다 크다(j>m). 이 경우에, RFID 태그(1601)의 제어 수단(1705)은 판독 요청을 잘못된 것으로 판단하여, 그에 응답하지 않을 것이다.

도 19에 도시된 RFID 태그(1601)의 동작 플로우에 대응해서, 도 20은, RFID 태그(1601)에 판독 요청을 보내고, RFID 태그(1601)로부터 수신된 데이터에 기초해서 RFID 태그(1601)를 인증하기 위한 RFID 판독기(1602)의 동작을 도시하는 흐름도이다. 본 명세서에서는, RFID 판독기(1602)가 RFID 태그(1601)로부터 식별 코드, 예를 들어, EPC 코드를 성공적으로 판독하고, 이에 따라, RFID 태그(1601)를 특별히 식별하는 속성을 결정하고, 따라서, 메모리에 저장된 공개 키(또는 키들) 중 어느 것이 판독 디지털 서명을 검증하기 위해 사용되어야만 하는 지를 결정한다고 가정된다. 단계 2001에서, RFID 판독기(1602)의 프로세서(1801)는 그에 포함된 제1 카운터(도시 생략)의 값 j를 1로 설정하고, 즉, j=1로 하고, 여기에서 값 j는 세트의 첨자(suffix)를 나타낸다. 다음으로, 단계 2002에서, 프로세서(1801)는 k 인덱스를 포함하는 인덱스의 서브세트 {a_1, a_2, ..., a_k}를 임의로 선택한다. 단계 2003에서, 프로세서(1801)는 그에 포함된 제2 카운터(도시 생략)의 값 i를 1로 설정하고, 즉, i=1로 하고, 여기에서 값 i는 인덱스의 서브세트에 대한 첨자를 나타낸다. 단계 2004에서, 프로세서(1801)는 무선 주파수 모듈(1802)이, j^{th} 세트의 a_i^{th} 서명 SIG_{j,a_i}를 판독하라고 요청하는 판독 요청을 생성하도록 지시하고, 이 판독 요청을 판독기 접속 소자(1803)를 통해 RFID 태그(1601)로 보낸다. 단계 2005에서, RFID 판독기(1602)는 RFID 태그(1601)로부터 잠금 상태의 플래그를 수신한다. 단계 2006에서, 프로세서(1801)는 i가 1과 동일한지 여부를 판정하고, RFID 태그(1601)의 디지털 서명의 j^{th} 세트가 수신된 플래그에 기초해서 잠겨졌는지 여부를 판정한다. i가 1과 동일하지 않거나, j^{th} 세트가 잠겨져 있지 않았다면, 다음으로 단계 2007에서, 프로세서(1801)는, RFID 태그(1601)로부터 보내진 SIG_{j,a_i}가 수신되었는 지 여부를 판정한다. SIG_{j,a_i}가 수신되었으면, 그 다음 단계 2008에서, 프로세서(1801)는 SIG_{j,a_i}가 유효한지를 판정한다. 여기서 유효성을 판정하는 방식은 다음과 같다. 프로세서(1801)는 사전에 RFID 태그(1601)와 관련된 제품의 제조자에 속하는 것으로 판정된 하나 이상의 공개 키를 판독하고, 하나 이상의 공개 키를 가지고서 디지털 서명을 검증한다. 디지털 서명이 유효한 경우에는, 단계 2009에서 제2 카운터의 값 i가 1 만큼 증가되고, 단계 2010에서 프로세서(1801)는 i가 k보다 큰지 여부를 판정한다. i>k인 경우에는 프로세스는 단계 2011로 진행하고, 프로세서(1801)의 인증부(1801-1)는 RFID 태그(1601)가 진정한 태그인 것으로 판정한다. 단계 2010에서의 결과에서 i가 k보다 크지 않은 경우에는, 프로세스는 단계 2004로 돌아가 플로우를 반복한다. 반면에, 단계 2007 또는 2008에서의 결과가 부정적인 경우에는 인증부(1801-1)는 RFID 태그(1601)가 위조 태그인 것으로 판정할 수 있다(단계 2021). 반면에, 단계 2006에서 결과가 긍정적인 경우, 즉 i=1이고 j번째 세트가 잠겨져 있는 경우에는, 단계 2012에서 프로세서(1801)는 j번째 세트의 i번째 서명 $SIG_{j,i}$에 대한 판독 요청을 판독기 접속 소자(1803)를 통해서 RFID 태그(1601)에 전송할 것을 RFID 판독기(1602)에 명령한다. 그 후에, 단계 2013에서 RFID 태그(1601)로부터 전송된 $SIG_{j,i}$가 수신되었는지 여부가 판정된다. 수신된 경우에는, 단계 2014에서 프로세서(1801)는 $SIG_{j,i}$가 유효한지 여부를 판정한다. 유효성을 판정하는 방식은 전술한 바와 동일하다. 유효하지 않은 경우에는 인증부(1801-1)는 RFID 태그(1601)가 위조 태그인 것으로 판정한다. 단계 2014에서 $SIG_{j,i}$가 유효한 것으로 판정된 경우에는, 단계 2015에서 프로세서(1801)는 i의 값을 1 만큼 증가시킨다. 반면에, 단계 2013에서 $SIG_{j,i}$가 수신되지 않은 경우에는, 역시 프로세스는 단계 2015로 진행하여 프로세서(1801)는 제2 카운

터의 값 i를 1 만큼 증가시킨다. 그 후, 단계 2016에서, 프로세서(1801)는 i가 n보다 큰지 여부를 판정한다. i가 n보다 크지 않은 경우에는, 프로세스는 단계 2012로 되돌아가서 i가 1 만큼 증가되었다는 조건하에 그 단계와 그 후속 단계들이 반복된다. i>n인 경우에는 단계 2017에서 프로세서(1801)는 수신된 서명의 수가 k와 동일한지 여부를 판정한다. 그 대답이 "아니오"인 경우에는 인증부(1801-1)는 RFID 태그(1601)가 가짜 태그인 것으로 판정한다(단계 2021). 그 대답이 "예"인 경우, 즉 수신된 서명의 수가 k와 동일한 경우에는, 프로세서(1801)는 단계 2018에서 제1 카운터의 값 j를 1 만큼 증가시키고, 단계 2019에서 j가 m보다 큰지 여부를 판정한다. j>m으로 판정된 경우에는 인증부(1801-1)는 RFID 태그(1601)가 이전에 판독된 것으로 판정한다(단계 2020). 그렇지 않은 경우에는 프로세스는 단계 2002로 되돌아가서 j의 값이 1 만큼 증가되었다는 조건하에 단계 2002 및 후속하는 단계들이 반복된다. 단계 2011, 단계 2021 또는 단계 2020에서, 인증부(1801-1)가 RFID 태그(1601)의 진정성에 대한 판정을 한 후에 인증 프로세스는 종료한다.

전술한 실시예에서, 검증가능한 데이터는 디지털 서명이다. 그러나, 다른 형태의 검증가능한 데이터에 대하여, 인증을 통과한 진정한 태그를 가지며 이러한 태그가 복제되는 것을 방지하는 기술적인 효과가 본 발명에 의해서 제안되는 "잠금" 기능을 통해서 획득될 수 있음은 본 기술분야의 당업자에게 명확하다. 본 기술분야의 당업자는 본 명세서를 참조하여 다양한 형태의 검증가능한 데이터를 이용하여 본 발명의 기술적인 솔루션을 용이하게 실시할 수 있다.

본 발명에 따른 제품을 인증하는 RFID 시스템 및 상기 RFID 시스템을 이용한 제품 인증에 대한 실시예에 대해 상술하였다. 위에서 지적한 바와 같이, ECDSA 및 SHA-1 등의 바람직한 디지털 서명 방안에 있어서, 하나의 서명은 보조 저장 영역의 320 비트를 차지한다. 따라서, 12개의 디지털 서명은 보조 저장 영역의 3840 비트를 필요로 한다. 태그 메모리 소모가 줄어들 수 있다면, 태그 비용은 그에 따라 줄어들 수 있다. 큰 부피의 제품이 큰 부피의 태그를 필요로 한다는 사실로부터 단지 1센트만이라도 태그 비용을 줄이는 것이 중요하다는 것을 즉시 확인할 수 있다.

본 발명의 제5 실시예에서는, 서명을 저장하기 위한 RFID 태그 메모리 소모를 추가로 줄일 수 있는 방법을 제공한다. 도 21은 개선된 방법을 통해 디지털 서명을 계산함으로써 얻어지는 RFID 태그(2100)의 내부 구조를 도시하는 도면이다. 이러한 RFID 태그는 마이크로칩(2101) 및 태그 접속 소자(2102)를 포함한다. 마이크로칩(2101)은 식별 코드 저장 영역(2103), 보조 저장 영역(2104) 및 제어 수단(2105)을 포함한다. 보조 저장 영역(2104)에는 한 세트의 n개의 디지털 서명 $\{SIG_1, SIG_2, ..., SIG_n\}$이 저장되어 있다. 도 21에는 간결하게 하기 위해 단지 2개의 디지털 서명만이 도시되어 있다. 상기 세트의 디지털 서명 $\{SIG_1, SIG_2, ..., SIG_n\}$에서의 각각의 디지털 서명 SIG_i는 Si 부분과 C 부분을 포함한 $(S_i, C)(i = 1, ..., n)$ 형태를 띠며, 각각의 디지털 서명은 다음과 같이 계산 및 입증된다.

즉, 순위 v의 그룹(추가로 후술함) G를 선택하고, 상기 그룹 G의 순위 u(여기서, u≤v임)의 서브그룹을 선택하고, 상기 순위 u를 토대로 n개의 개인키 x1, x2, ..., xn(여기서, $1<|xi|<u$, i = 1, ..., n임)을 선택하고, 생성자로서 그룹 G의 요소 g를 선택하고, 상기 순위 u 내의 표시자로서 n개의 정수 r1, r2, ..., rn(여기서, $0<|ri|<u$, i = 1, ..., n임)을 선택하고, 상기 순위 u내의 임의 정수 r(여기서, $0<|r|<u$)을 선택하고, $C = H(M, g^{r*r1*r2*...*rn})$(여기서, H는 보안 해시 함수이고, M은 식별 코드 및 그 밖의 정보를 나타냄)를 계산하고, $S_i = r*(r1*r2*...*rn)/ri-C*xi$를 계산하고, 동일한 메시지 M에 대한 n개의 디지털 서명으로서 $(S_1, C), (S_2, C), ..., (S_n, C)$를 공개하고, 상기 개인키, 상기 생성자 및 상기 표시자를 토대로 공개키 $y_i = (g^{ri}, g^{ri*xi})$를 계산하고, 공개키 y_i를 토대로, $C' = H(M, (g^{ri})^{si}*(g^{ri*xi})^C)$를 계산함으로써 $SIG_i=(S_i, C)$가 메시지 M에 대한 유효 서명인지를 입증하며, C' = C라면, SIG_i는 메시지 M에 대해 유효한 디지털 서명이고, 그렇지 않다면, SIG_i는 유효하지 않은 디지털 서명이라고 하거나, 또는 순위 v의 그룹 G를 선택하고, 상기 그룹 G의 순위 u(여기서, u≤v임)의 서브그룹을 선택하고, 상기 순위 u를 토대로 n개의 개인 키 x1, x2, ..., xn(여기서, $1<|xi|<u$, i = 1, ..., n임)을 선택하고, 생성자로서 그룹 G의 요소 g를 선택하고, 상기 순위 u내의 표시자로서 n개의 정수 r1, r2, ..., rn(여기서, $0<|ri|<u$, i = 1, ..., n임)을 선택하고, 상기 순위 u내의 임의 정수 r(여기서, $0<|r|<u$)을 선택하고, $C = H(M, g^{r*r1*r2*...*rn})$(여기서, H는 보안 해시 함수이고, M은 식별 코드 및 그 밖의 정보를 나타냄)를 계산하고, $S_i = r*(r1*r2*...*rn)/(r1*r2*...*ri)-C*xi$를 계산하고, 동일한 메시지 M에 대한 n개의 디지털 서명으로서 $(S_1, C), (S_2, C), ..., (S_n, C)$를 공개하고, 상기 개인키, 상기 생성자 및 상기 표시자를 토대로 공개키 $y_i = (g^{r1*r2*...*ri}, g^{r1*r2*...*ri*xi})$를 계산하고, 공개키 y_i를 토대로, $C' = H(M, (g^{r1*r2*...*ri})^{si}*(g^{r1*r2*...*ri*xi})^C)$를 계산함으로써 $SIG_i=(S_i, C)$가 메시지 M에 대한 유효 서명인지를 입증하며, C' = C라면, SIG_i는 메시지 M에 대해 유효한 디지털 서명이고, 그렇지 않다면, SIG_i는 유효하지 않은 디지털 서명이다.

본 명세서 및 청구범위에 걸쳐, "그룹"은 특별한 지시가 없으면 다음과 같은 수학적 개념을 의미한다:

그룹(G, ◇)는 다음의 세개의 원리를 만족하는 G의 이진 연산 ◇을 갖는 세트 G로 구성된다:

(i) 그룹 연산은 결합 법칙을 따른다. 즉, G의 모든 원소 a, b, c에 대하여 a◇(b◇c)=(a◇b)◇c이다:

(ii) G의 모든 원소 a에 대하여 a◇e=e◇a=a가 되도록 G의 항등 원소 e가 존재한다:

(iii) G의 각 원소 a에 대하여, a◇a-1=a-1◇a=e가 되도록 a의 역원이라 불리는 G의 원소 a-1이 존재한다.

예를 들면, 덧셈 연산을 하는 정수 Z의 세트가 하나의 그룹을 형성한다. 항등 원소는 0이고 정수 a의 역원은 정수 -a이다. 더 많은 정보를 위해서는, 온라인상의 http://www.cacr.math.uwaterloo.co/hac/에서 이용가능한 "응용 암호화 핸드북(Handbook of Applied Cryptography)을 참조하면 된다.

MD5 및 SHA-1과 같은 보안 해싱 알고리즘의 다수의 후보가 존재하고, 부가의 정보가 해싱에 삽입될 수 있다는 것을 주목하자. 또한, "Meta-E1Gamal signature schemes, Proc. 2nd ACM conference on Computer and Communications security, pp. 96-107, 1994"에 공지된 바와 같이 Si를 계산하는 다른 등식이 이용가능하고 적용할 수 있다는 것을 주목하자. 이들 모두 당업자에게 공지되어 있다.

본 실시예의 방법의 이점은 자명하다. 160 비트 타원 곡선 및 SHA-1을 사용할 때, 모든 서명에 의해 공통의 C를 공유하기 때문에, 현재 열두 개의 서명은 단지 2080 비트만을 필요로 하지만, 적용 전에 이러한 접근법은 3840 비트가 필요하다. C의 크기를 보안 레벨을 손상하지 않는 128 비트로 약간 감소하면, 2k 비트의 태그 메모리는 저장될 열 두 개의 서명에 정확히 충분하다.

일반적으로, 태그에 저장된 n>1의 서명에 대하여, 이들은 하나의 C를 공유할 수 있다. 제품 제조자는 현재 n개의 공개키를 필요로 한다. 바람직한 경우에, 즉, x1=x2=...=xn=x일 때, 공개키는 본 출원인의 무기명 공개키 특허 출원(중국 특허 출원번호 제200410090903.X호)에 공개된 원리에 따라 생성된다.

C를 공유하지 않는 이전 접근법과 비교하여, RFID 태그 보조 저장 영역의 절약분은 (n-1)/2n이라는 것을 검증하는 것은 용이하다. 예를 들면, n=12이면, RFID 태그의 보조 저장 영역의 45.8%가 오프(off)이다.

서명 세트를 이용할 때, 모든 서명은 이들이 동일한 세트이거나 또는 그렇지 않은 경우에 관계없이 하나의 C를 공유할 수 있다는 것은 주목할 만하다. 상기 세트는 사실상 물리적 분류가 아닌 논리적 분류이다.

전술한 설명으로부터 알 수 있는 바와 같이, 본 발명의 실시예에 따라, "잠금" 함수를 RFID 태그에 도입한다. 그 결과로서, 저가로 태그를 복제하는 것이 금지되고 RFID 태그에 저장된 다수의 디지털 서명 및 RFID 태그에 의해 실행된 "잠금" 함수에 기초하여 대량의 위조를 방해한다.

부가하여, 다수의 서명을 세트로 분할하고 RFID 태그에 저장한다. 서명 세트를 도입함으로써, 진정한 태그가 적어도 m번 동안 원본으로 검증될 수 있다는 것이 보장되며, 여기에서, m은 서명 세트의 수이다.

또한, 다수의 서명을 저장하기 위해 소모되는 RFID 태그 메모리는 공개 키 및 하나의 부분 C를 공유하는 서명 생성 방법에 의해 상당히 감소된다.

본 발명은 특정의 바람직한 실시예를 참조하여 설명되었지만, 첨부된 청구범위에 정의된 바와 같이 본 발명의 사상 및 범위를 벗어나지 않으면서 다양한 수정이 이루어질 수 있다는 것을 당업자는 이해할 수 있을 것이다.

발명의 효과

본 발명의 실시예들에 따르면, 라디오 주파수 신원확인 태그 내에 잠금 기능이 소개된다. 이에 따라, 라디오 주파수 신원확인 태그 내의 데이터의 복제는 효과적으로 방지되고, 라디오 주파수 신원확인 태크에 저장된 복수의 전자 서명들과 라디오 주파수 신원확인 태그에 의해 수행되는 잠금 기능을 통해 대량 위조품들이 방지될 수 있다.

도면의 간단한 설명

도 1은 본 발명의 제1 실시예에 따른 RFID 태그(101) 및 RFID 판독기(102)를 포함하는 RFID 시스템(100)을 도시하는 도면.

도 2는 본 발명의 제1 실시예에 따른 RFID 태그(101)의 내부 구조를 도시하는 개략도.

도 3은 본 발명의 제1 실시예에 따른 RFID 판독기(102)의 내부 구조를 나타내는 개략도.

도 4는 RFID 판독기(102)로부터 판독 요청의 수신 시, RFID 태그(101)의 동작들을 나타내는 흐름도.

도 5는 RFID 태그(101)에 판독 요청을 송신하고, 판독된 디지털 서명들에 기초하여 RFID 태그(101)를 인증하기 위한 RFID 판독기(102)의 동작들을 나타내는 흐름도.

도 6은 본 발명의 제2 실시예에 따른 RFID 태그(601) 및 RFID 판독기(602)를 포함하는 RFID 시스템(600)을 나타내는 도면.

도 7은 본 발명의 제2 실시예에 따른 RFID 태그(601)의 내부 구조를 나타내는 개략도.

도 8은 본 발명의 제2 실시예에 따른 RFID 판독기(602)의 내부 구조를 나타내는 개략도.

도 9는 RFID 판독기(602)로부터 판독 요청의 수신 시, RFID 태그(601)의 동작들을 나타내는 흐름도.

도 10은 RFID 태그(601)에 판독 요청을 송신하고, 판독된 디지털 서명들에 기초하여 RFID 태그(601)를 인증하기 위한 RFID 판독기(602)의 동작들을 나타내는 흐름도.

도 11은 본 발명의 제3 실시예에 따른 RFID 태그(1101) 및 RFID 판독기(1102)를 포함하는 RFID 시스템(1100)을 나타내는 도면.

도 12는 본 발명의 제3 실시예에 따른 RFID 태그(1101)의 내부 구조를 나타내는 개략도.

도 13은 본 발명의 제3 실시예에 따른 RFID 판독기(1102)의 내부 구조를 나타내는 개략도.

도 14는 RFID 판독기(1102)로부터 판독 요청의 수신 시, RFID 태그(1101)의 동작들을 나타내는 흐름도.

도 15는 RFID 태그(1101)에 판독 요청을 송신하고, 판독된 디지털 서명들에 기초하여 RFID 태그(1101)를 인증하기 위한 RFID 판독기(1102)의 동작들을 나타내는 흐름도.

도 16은 본 발명의 제4 실시예에 따른 RFID 태그(1601) 및 RFID 판독기(1602)를 포함하는 RFID 시스템(1600)을 나타내는 도면.

도 17은 본 발명의 제4 실시예에 따른 RFID 태그(1601)의 내부 구조를 나타내는 개략도.

도 18은 본 발명의 4 실시예에 따른 RFID 판독기(1602)의 내부 구조를 나타내는 개략도.

도 19는 RFID 판독기(1602)로부터 판독 요청의 수신 시, RFID 태그(1601)의 동작들을 나타내는 흐름도.

도 20은 RFID 태그(1601)에 판독 요청을 송신하고, 판독된 디지털 서명들에 기초하여 RFID 태그(1601)를 인증하기 위한 RFID 판독기(1602)의 동작들을 나타내는 흐름도.

도 21은 본 발명의 제5 실시예에 따른 RFID의 메모리 비용의 감소를 나타내는 도면.

<도면의 주요 부분에 대한 부호의 설명>

101: RFID 태그

102: RFID 판독기

202: 태그 결합 소자

203: EPC

205: 제어 수단

301: 프로세서

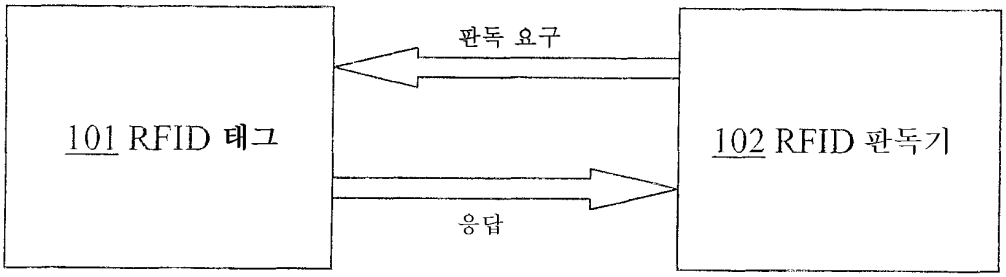
302: RF 모듈

303: 판독기 결합 소자

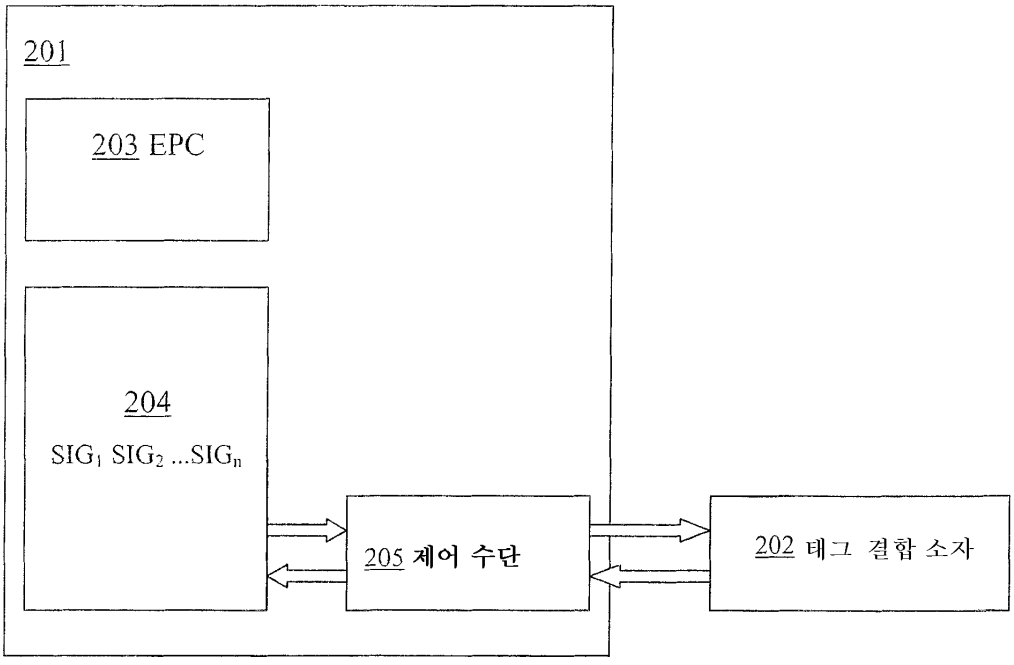
304: 메모리

도면

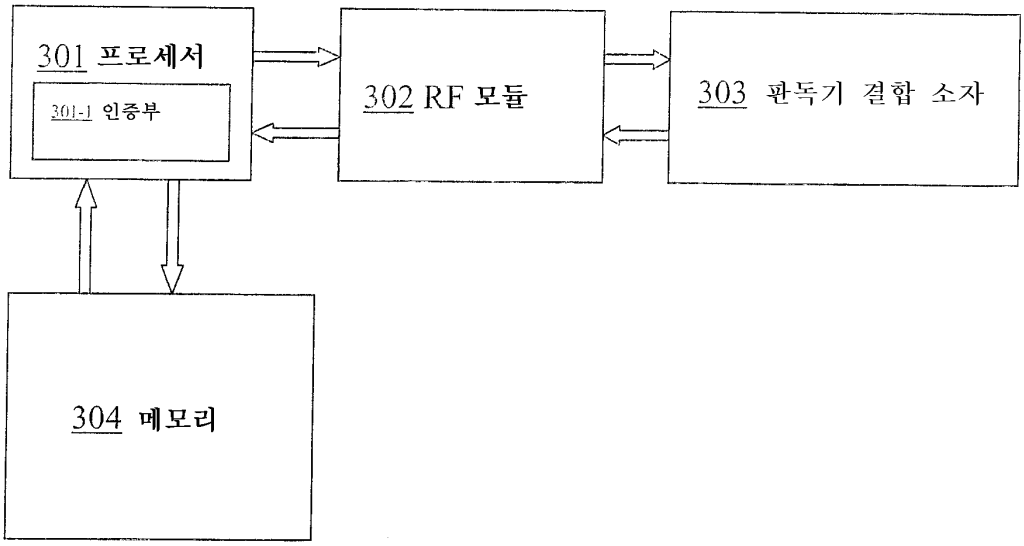
도면1



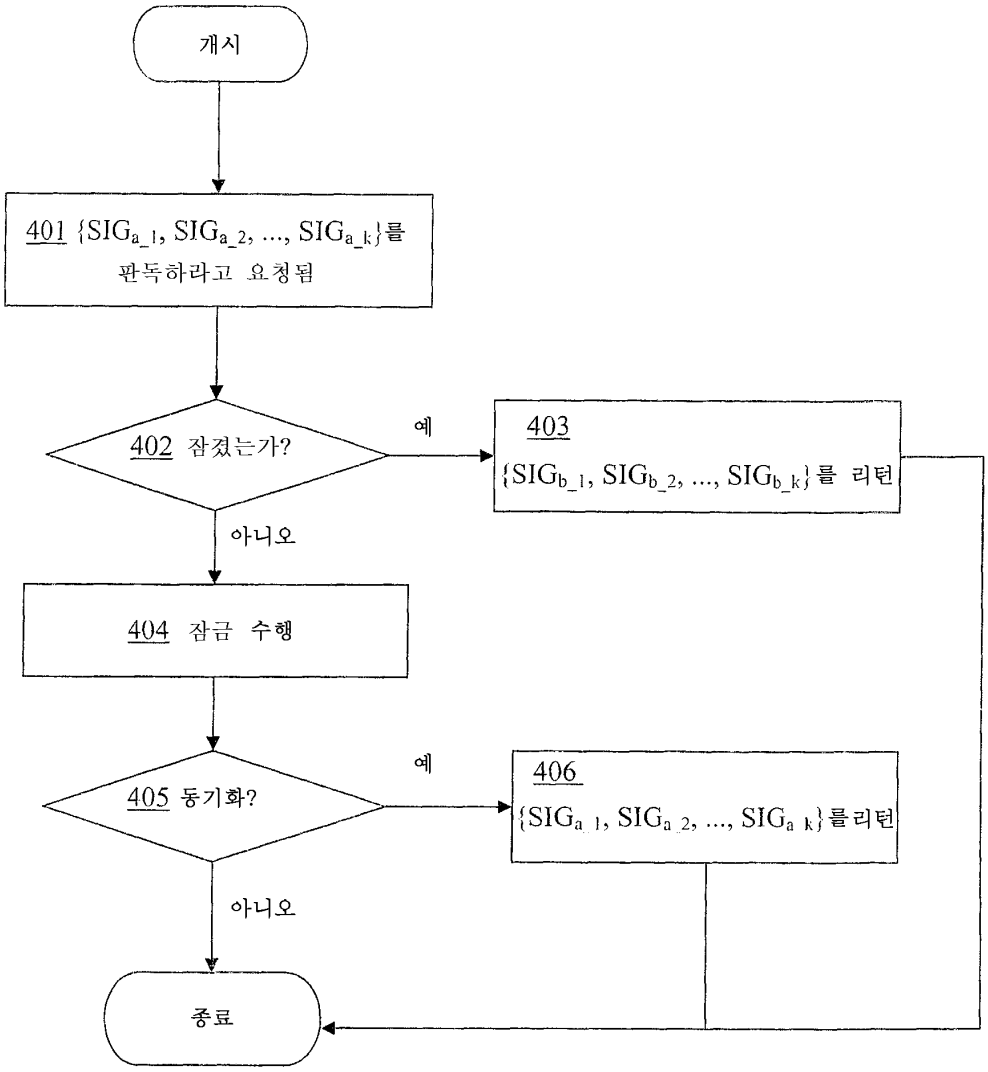
도면2



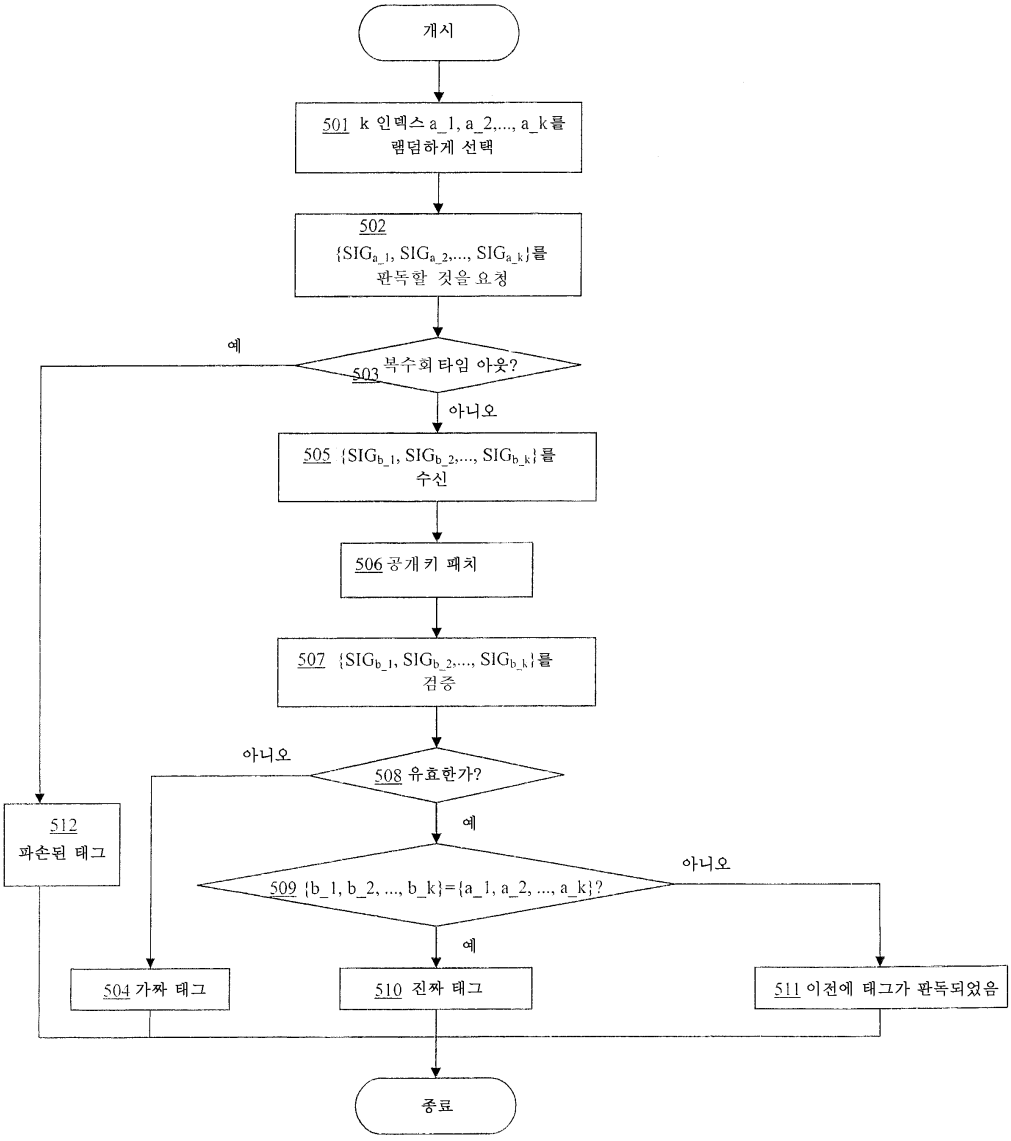
도면3


301 프로세서
301-1 인증부
302 RF 모듈
303 판독기 결합 소자
304 메모리

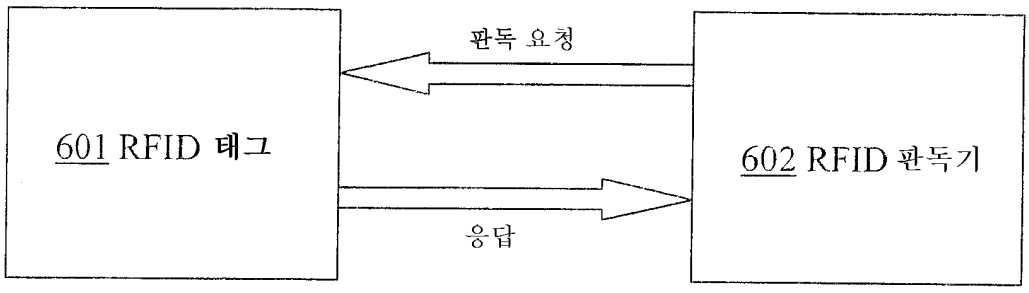
도면4


개시
401 {SIGa_1, SIGa_2, ..., SIGa_k}를 판독하라고 요청됨
402 잠겼는가?
예
403 {SIGb_1, SIGb_2, ..., SIGb_k}를 리턴
아니오
404 잠금 수행
405 동기화?
예
406 {SIGa_1, SIGa_2, ..., SIGa_k}를리턴
아니오
종료

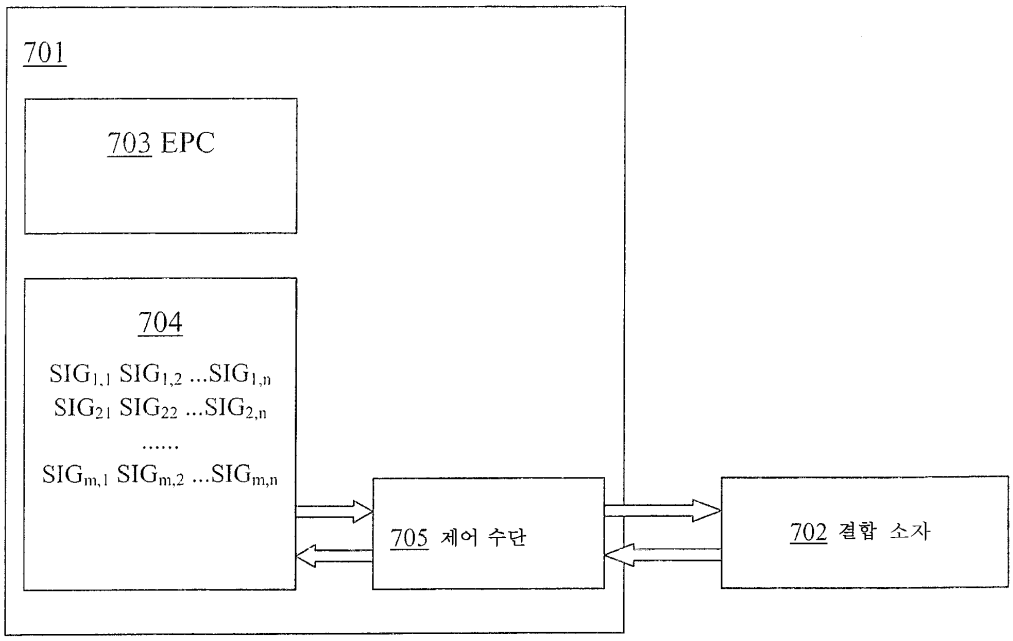
도면5


개시
501 k 인덱스 a_1, a_2,..., a_k를 랜덤하게 선택
502 {SIG$_{a_1}$, SIG$_{a_2}$,..., SIG$_{a_k}$}를 판독할 것을 요청
503 복수회 타임 아웃?
예
아니오
505 {SIG$_{b_1}$, SIG$_{b_2}$,..., SIG$_{b_k}$}를 수신
506 공개키 패치
507 {SIG$_{b_1}$, SIG$_{b_2}$,..., SIG$_{b_k}$}를 검증
508 유효한가?
아니오
예
509 {b_1, b_2, ..., b_k}={a_1, a_2, ..., a_k}?
아니오
예
512 파손된 태그
504 가짜 태그
510 진짜 태그
511 이전에 태그가 판독되었음
종료

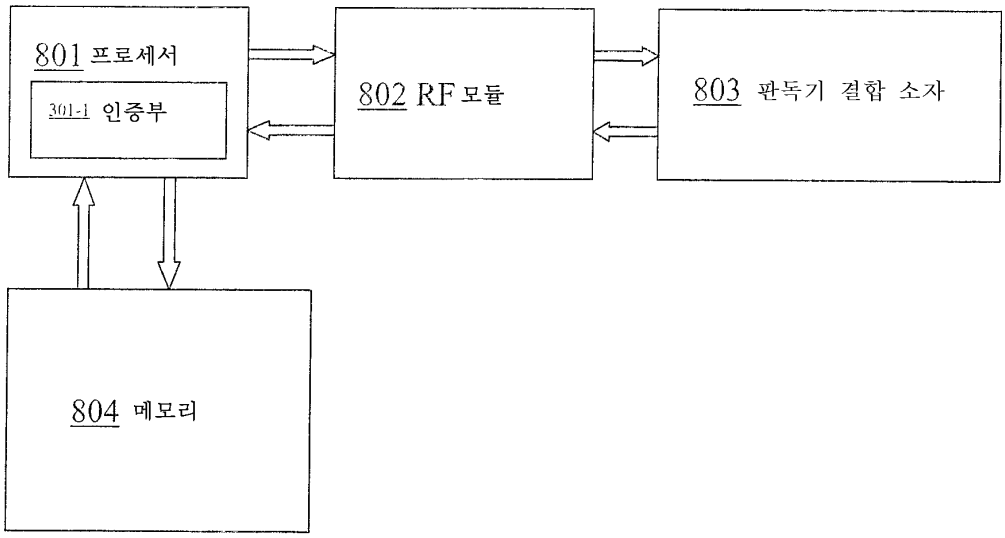
도면6


601 RFID 태그
판독 요청
응답
602 RFID 판독기

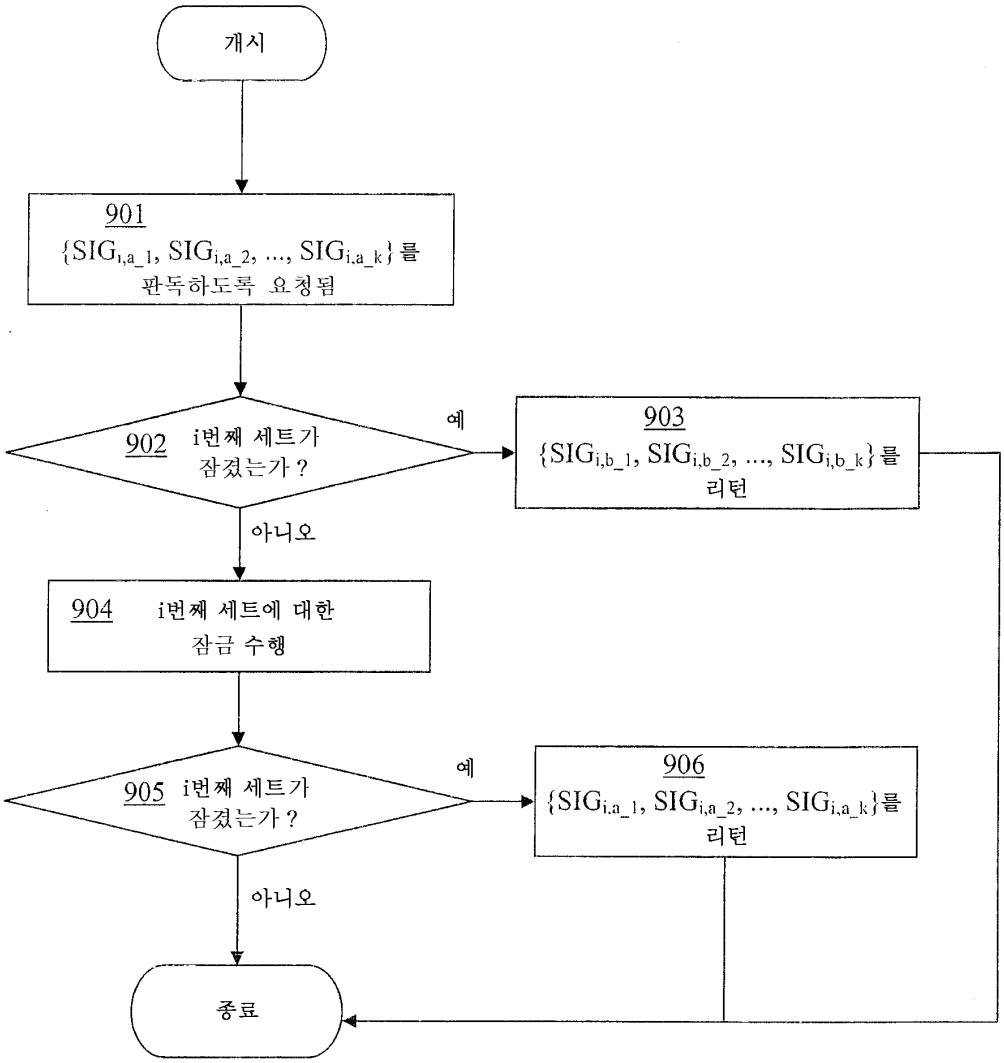
도면7


701
703 EPC
704
$SIG_{1,1}$ $SIG_{1,2}$ ...$SIG_{1,n}$
SIG_{21} SIG_{22} ...$SIG_{2,n}$
.....
$SIG_{m,1}$ $SIG_{m,2}$ ...$SIG_{m,n}$
705 제어 수단
702 결합 소자

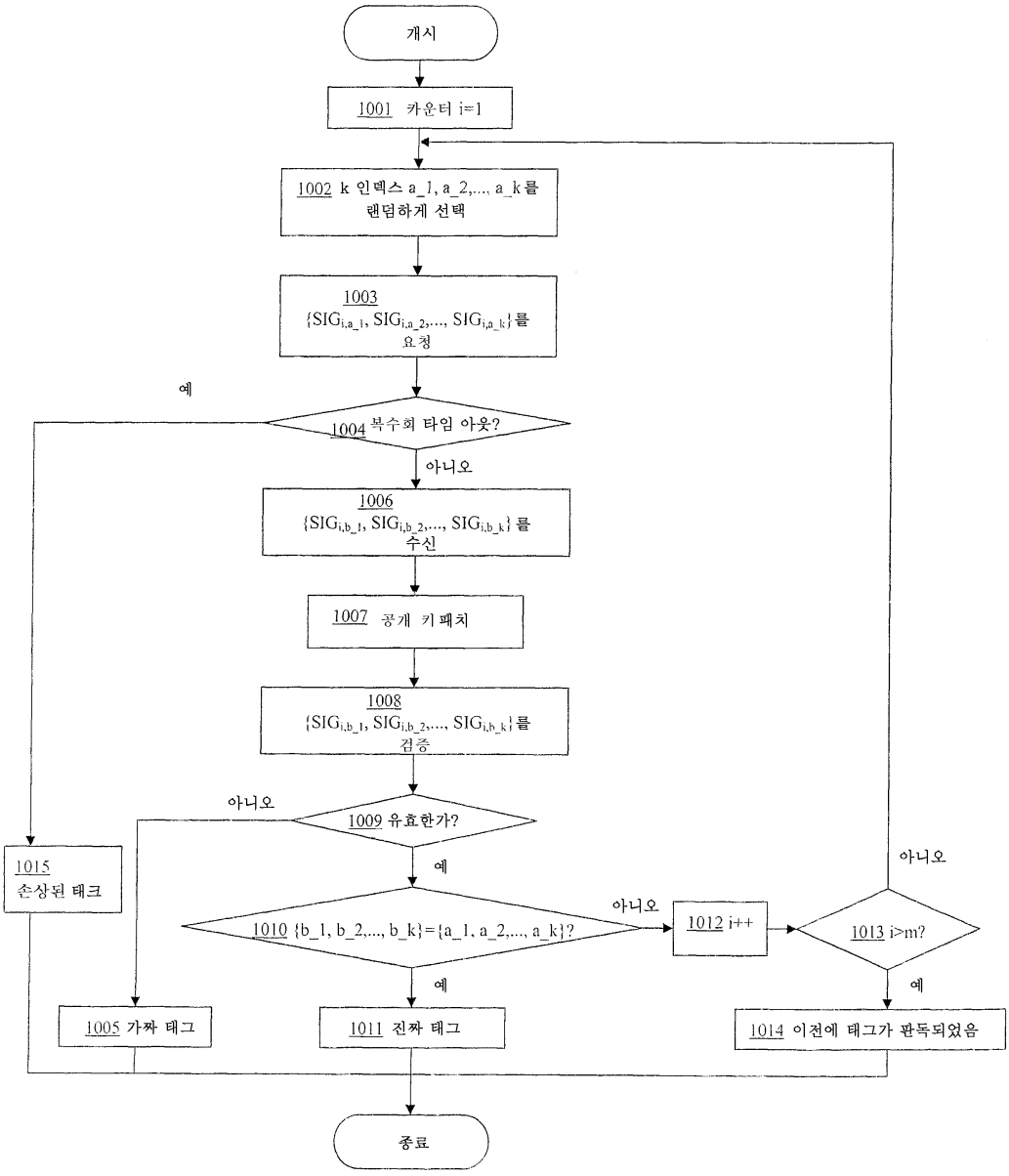
도면8


801 프로세서
301-1 인증부
802 RF 모듈
803 판독기 결합 소자
804 메모리

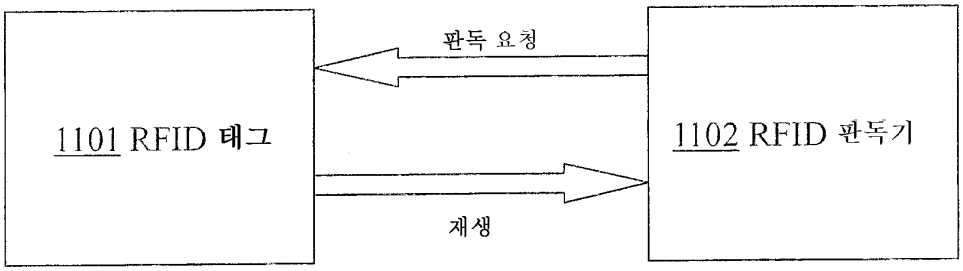
도면9


개시
901
{SIGi,a_1, SIGi,a_2, ..., SIGi,a_k}를 판독하도록 요청됨
902 i번째 세트가 잠겼는가?
예
903
{SIGi,b_1, SIGi,b_2, ..., SIGi,b_k}를 리턴
아니오
904 i번째 세트에 대한 잠금 수행
905 i번째 세트가 잠겼는가?
예
906
{SIGi,a_1, SIGi,a_2, ..., SIGi,a_k}를 리턴
아니오
종료

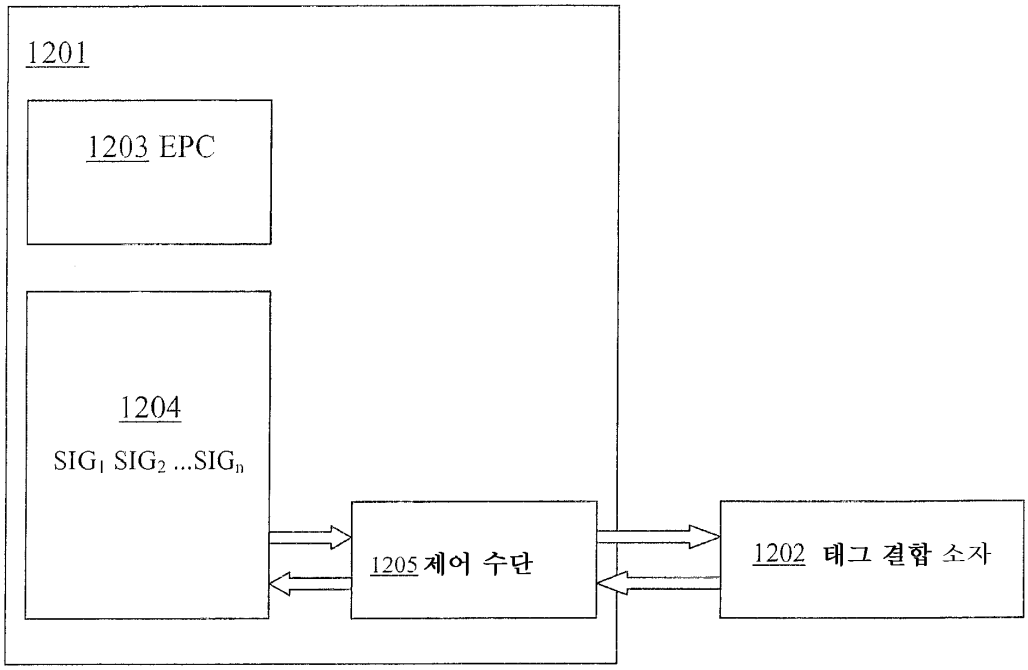
도면10


개시
1001 카운터 i=1
1002 k 인덱스 a_1, a_2,..., a_k를 랜덤하게 선택
1003 {SIG_i,a_1, SIG_i,a_2,..., SIG_i,a_k}를 요청
예
1004 복수회 타임 아웃?
아니오
1006 {SIG_i,b_1, SIG_i,b_2,..., SIG_i,b_k}를 수신
1007 공개 키 패치
1008 {SIG_i,b_1, SIG_i,b_2,..., SIG_i,b_k}를 검증
아니오
1009 유효한가?
예
1015 손상된 태크
1010 {b_1, b_2,..., b_k}={a_1, a_2,..., a_k}?
아니오
1012 i++
1013 i>m?
아니오
예
예
1005 가짜 태그
1011 진짜 태그
1014 이전에 태그가 판독되었음
종료

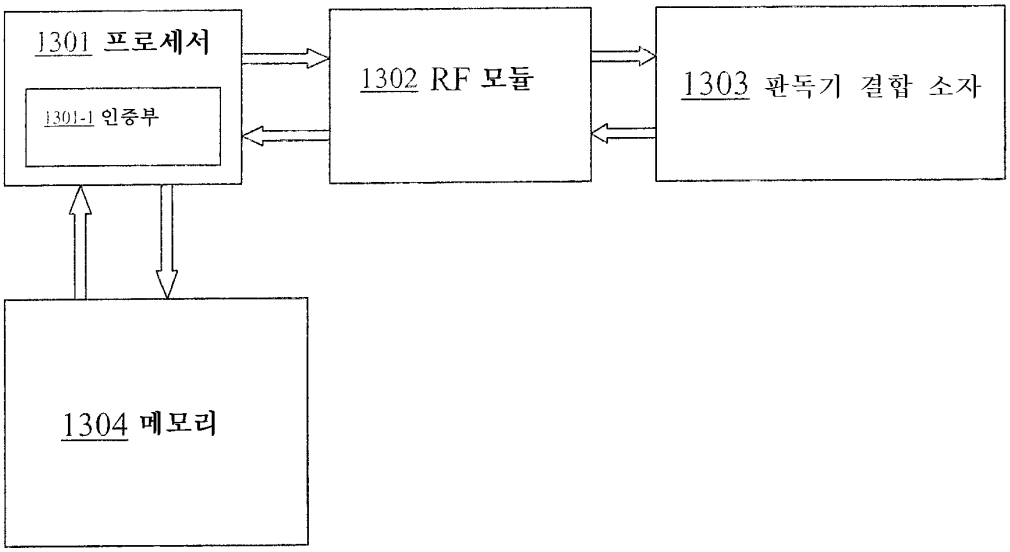
도면11


1101 RFID 태그
판독 요청
재생
1102 RFID 판독기

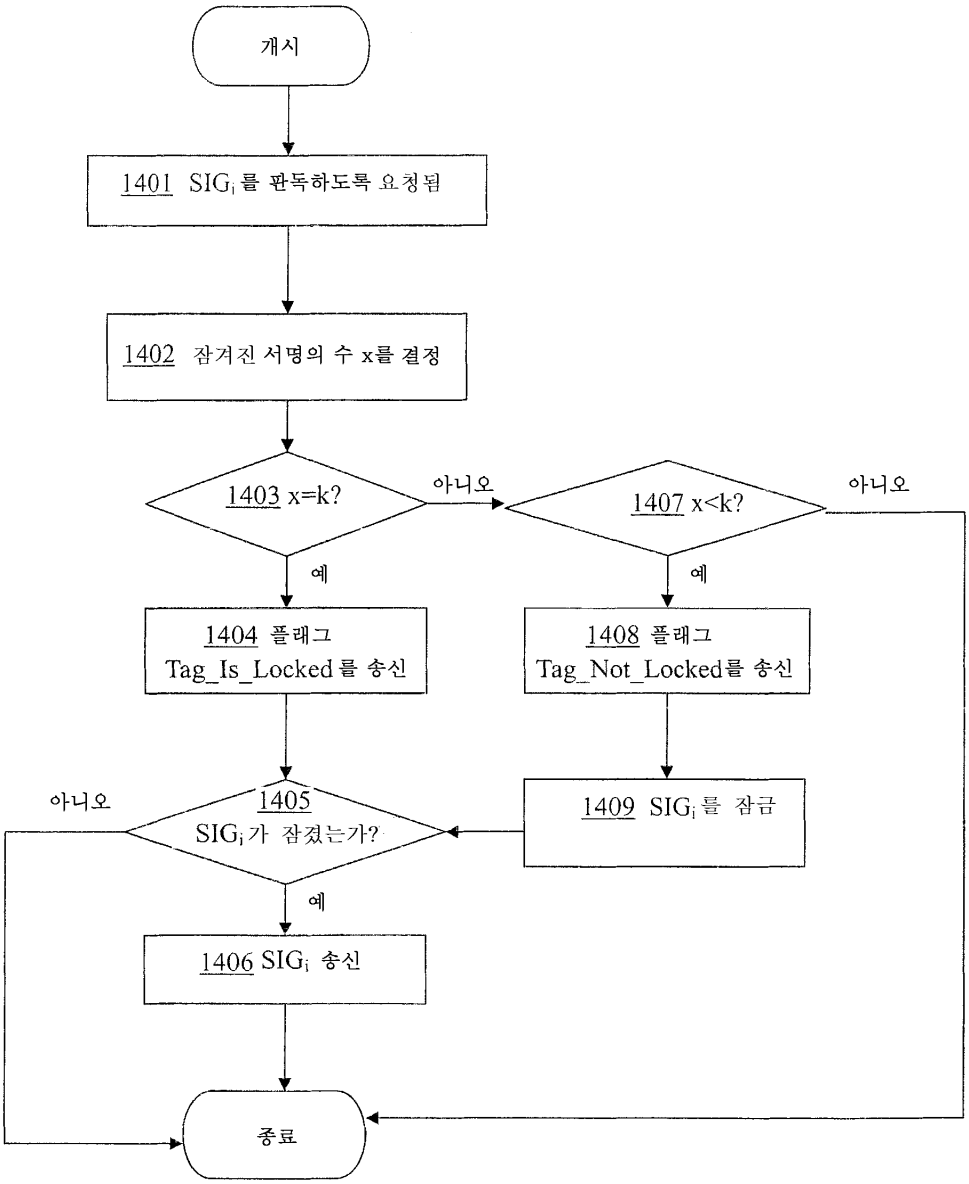
도면12


1201
1203 EPC
1204
SIG1 SIG2 ...SIGn
1205 제어 수단
1202 태그 결합 소자

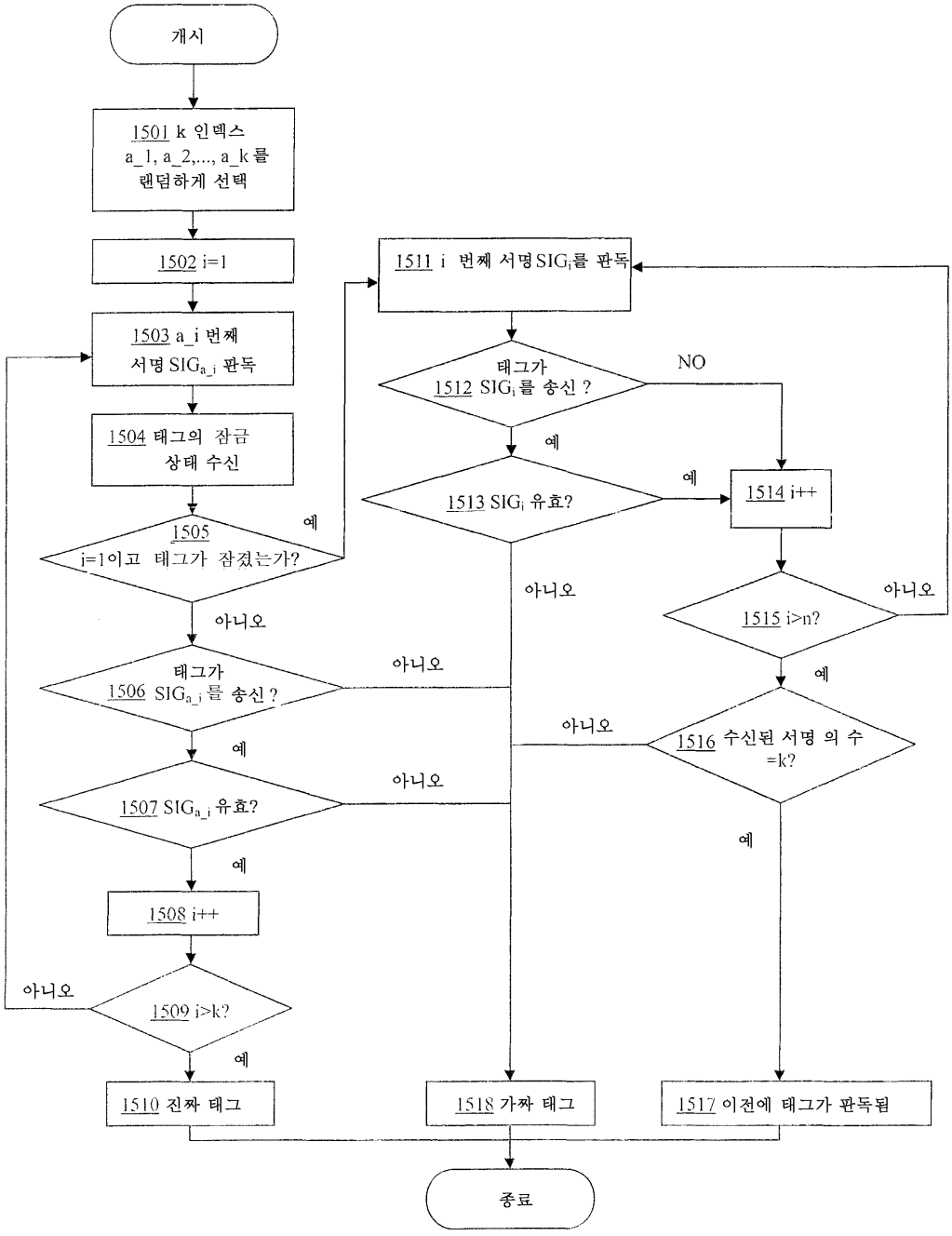
도면13


1301 프로세서
1301-1 인증부
1302 RF 모듈
1303 판독기 결합 소자
1304 메모리

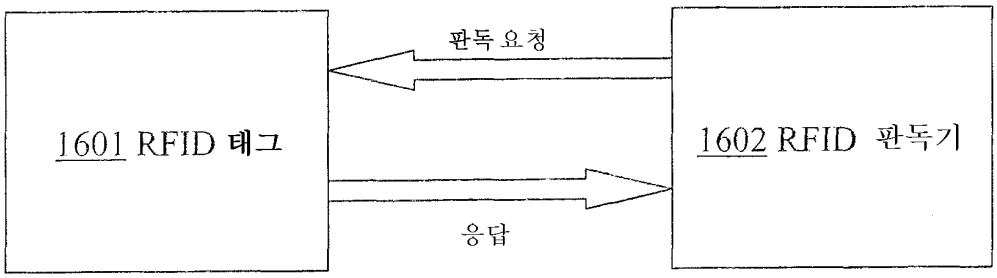
도면14


개시
1401 SIGi를 판독하도록 요청됨
1402 잠겨진 서명의 수 x를 결정
1403 x=k?
아니오
1407 x<k?
아니오
예
예
1404 플래그 Tag_Is_Locked를 송신
1408 플래그 Tag_Not_Locked를 송신
1405 SIGi가 잠겼는가?
아니오
1409 SIGi를 잠금
예
1406 SIGi 송신
종료

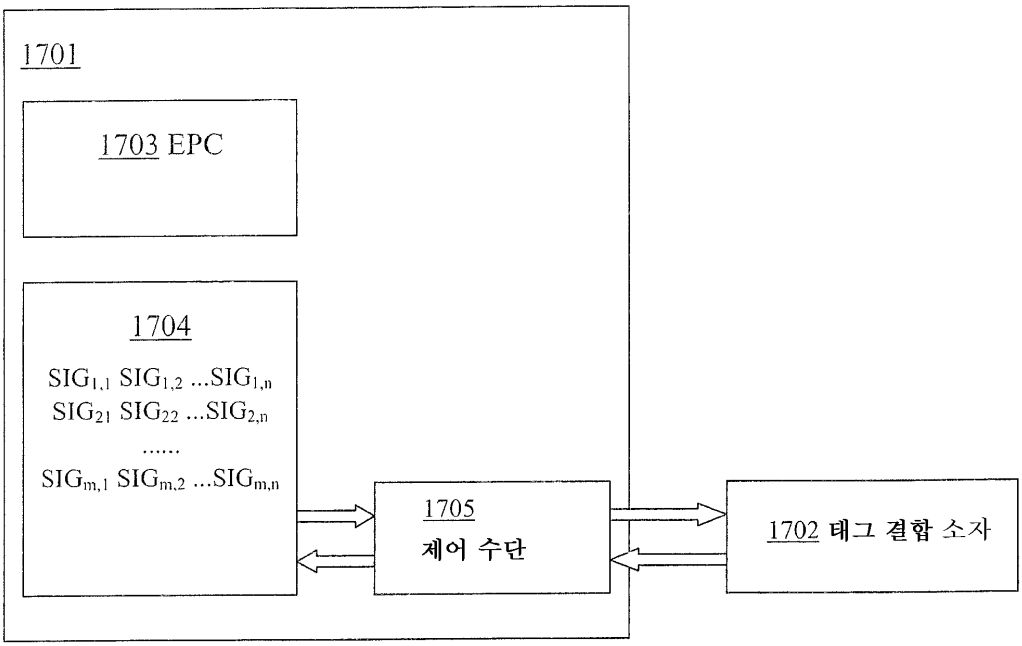
도면15


개시
1501 k 인덱스 a_1, a_2,..., a_k를 랜덤하게 선택
1502 i=1
1503 a_i 번째 서명 SIG$_{a_i}$ 판독
1504 태그의 잠금 상태 수신
1505 i=1이고 태그가 잠겼는가?
예
아니오
태그가 1506 SIG$_{a_i}$를 송신?
아니오
예
1507 SIG$_{a_i}$ 유효?
아니오
예
1508 i++
아니오
1509 i>k?
예
1510 진짜 태그
1511 i 번째 서명 SIG$_i$를 판독
태그가 1512 SIG$_i$를 송신?
NO
예
1513 SIG$_i$ 유효?
예
1514 i++
아니오
1515 i>n?
아니오
예
1516 수신된 서명 의 수 =k?
아니오
예
1517 이전에 태그가 판독됨
아니오
1518 가짜 태그
종료

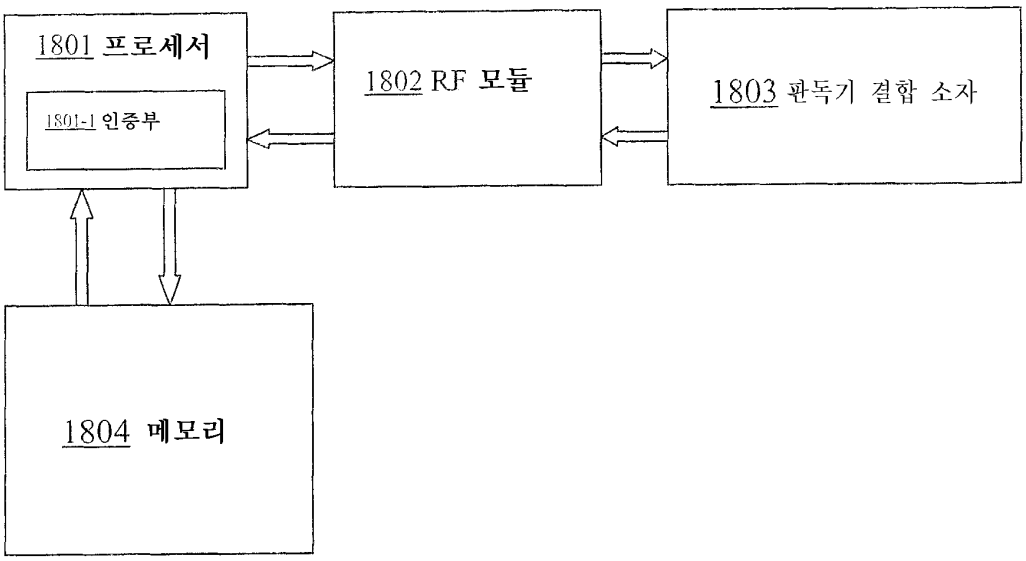
도면16


1601 RFID 태그
판독 요청
응답
1602 RFID 판독기

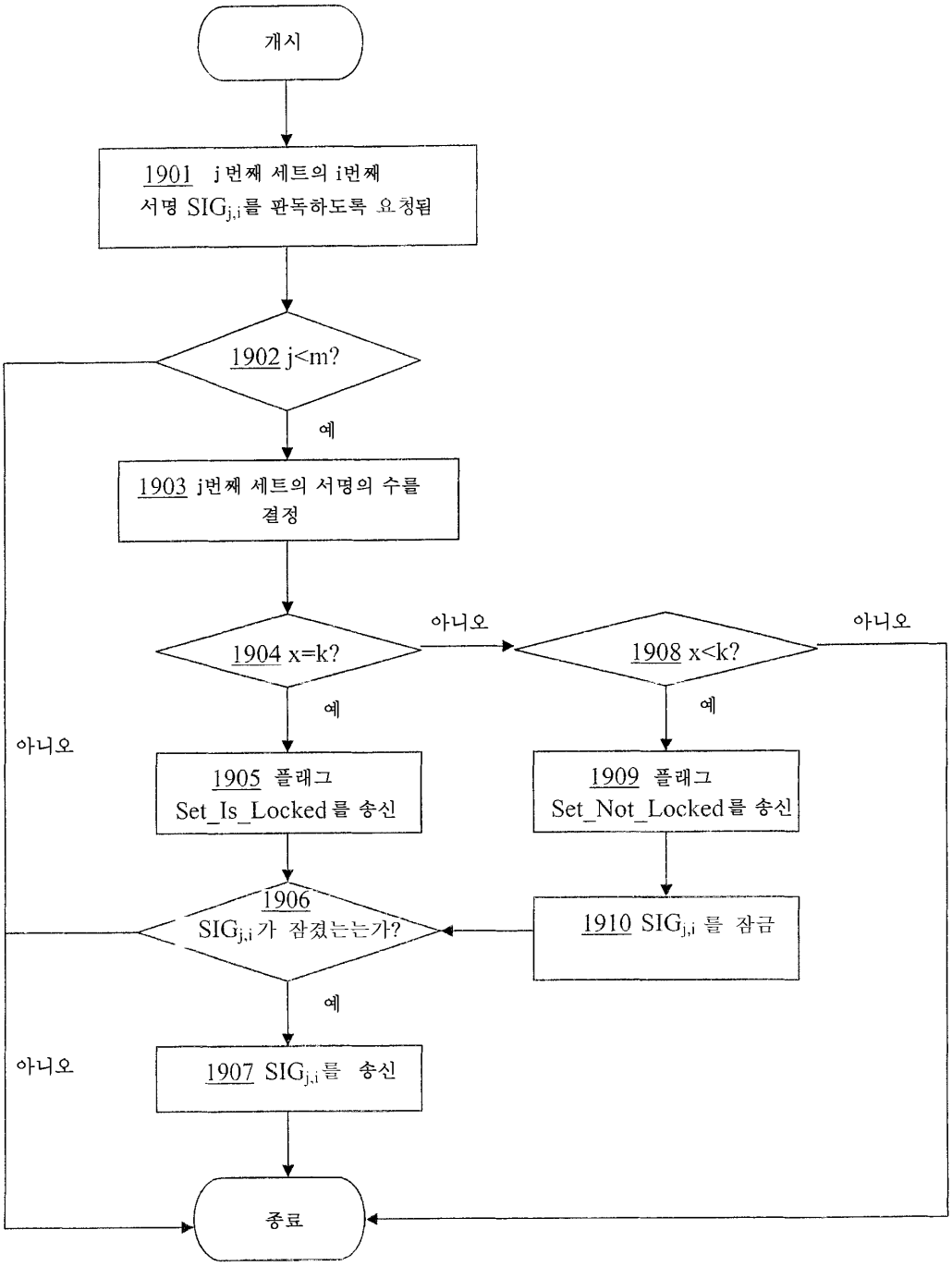
도면17


1701
1703 EPC
1704
$SIG_{1,1}$ $SIG_{1,2}$ ...$SIG_{1,n}$
SIG_{21} SIG_{22} ...$SIG_{2,n}$
.....
$SIG_{m,1}$ $SIG_{m,2}$ ...$SIG_{m,n}$
1705
제어 수단
1702 태그 결합 소자

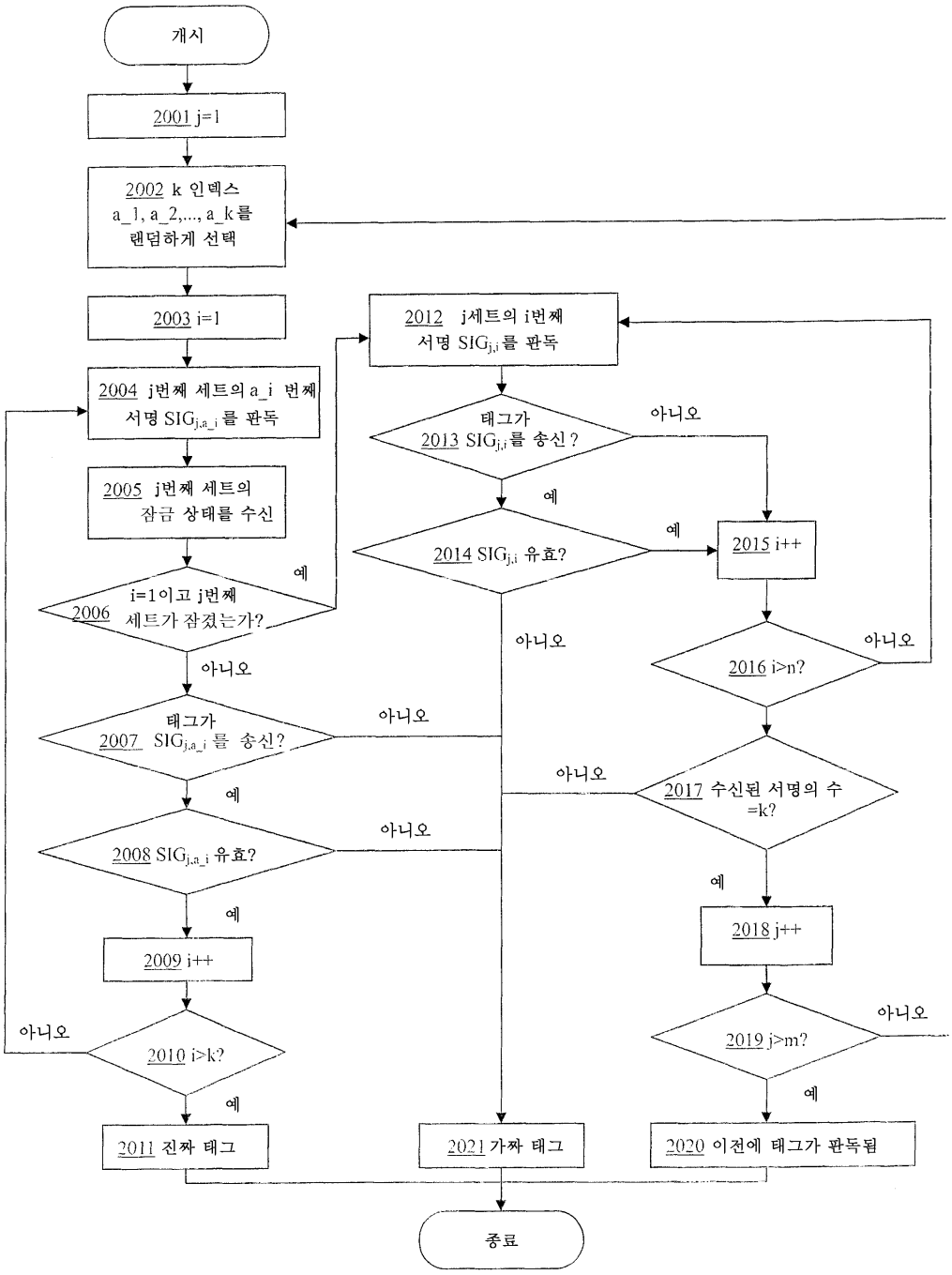
도면18


1801 프로세서
1801-1 인증부
1802 RF 모듈
1803 판독기 결합 소자
1804 메모리

도면19


개시
1901 j번째 세트의 i번째 서명 $SIG_{j,i}$를 판독하도록 요청됨
1902 j<m?
예
1903 j번째 세트의 서명의 수를 결정
1904 x=k?
아니오
예
1905 플래그 Set_Is_Locked를 송신
1906 $SIG_{j,i}$가 잠겼는는가?
아니오
예
1907 $SIG_{j,i}$를 송신
1908 x<k?
아니오
예
1909 플래그 Set_Not_Locked를 송신
1910 $SIG_{j,i}$를 잠금
아니오
종료

도면20


개시
2001 j=1
2002 k 인덱스 a_1, a_2,..., a_k를 랜덤하게 선택
2003 i=1
2004 j번째 세트의 a_i 번째 서명 SIG$_{j,a_i}$를 판독
2005 j번째 세트의 잠금 상태를 수신
2006 i=1이고 j번째 세트가 잠겼는가?
예
아니오
2007 태그가 SIG$_{j,a_j}$를 송신?
아니오
예
2008 SIG$_{j,a_i}$ 유효?
아니오
예
2009 i++
2010 i>k?
아니오
예
2011 진짜 태그
2012 j세트의 i번째 서명 SIG$_{j,i}$를 판독
2013 태그가 SIG$_{j,i}$를 송신?
아니오
예
2014 SIG$_{j,i}$ 유효?
예
아니오
2015 i++
2016 i>n?
아니오
2017 수신된 서명의 수 =k?
아니오
예
2018 j++
2019 j>m?
아니오
예
2020 이전에 태그가 판독됨
2021 가짜 태그
종료

도면21