(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/20 (2006.01)
H04L 9/14 (2006.01)
H04L 9/00 (2006.01)

(45) 공고일자 2007년07월09일
(11) 등록번호 10-0737385
(24) 등록일자 2007년07월03일

(21) 출원번호 10-2006-0054856
(22) 출원일자 2006년06월19일
심사청구일자 2006년06월19일

(65) 공개번호
(43) 공개일자

(73) 특허권자 경희대학교 산학협력단
경기도 용인시 기흥구 서천동 1 경희대학교 수원캠퍼스내

(72) 발명자 홍충선
경기 용인시 상현동 성원상떼빌 233-101

이재원
전남 화순군 화순읍 벽라리 150-1번지

(74) 대리인 특허법인다인

(56) 선행기술조사문헌
KR1020010102541 A
KR1020030019356 A
KR1020040004833 A
US20050152538 A1

심사관 : 이준석

전체 청구항 수 : 총 8 항

(54) 무선 센서 네트워크에서 키 데이터의 송신 방법

(57) 요약

본 발명은 무선 센서 네트워크에서 키를 송신하는 방법에 관한 것으로, 보다 구체적으로 보안 레벨에 따라 서로 다른 수의 블록으로 분할된 키 데이터와 스크램블(scramble) 데이터를 서로 혼합하여 키 데이터를 송신하는 방법에 관한 것이다.

본 발명에 따른 키 데이터 송신 방법은 보안 레벨에 따라 키 데이터와 스크램블 데이터를 조합하여 생성된 다수의 키 조합 데이터를 이용하여 키 데이터를 센서 노드에 송신하고, 센서 노드는 보안 레벨에 따라 수신한 키 조합 데이터에서 키 데이터를 추출하여 키 데이터를 생성함으로써, 무선 센서 네트워크에서 기지국과 센서 노드들 사이에서 안전하고 간단하게 키 데이터를 수신할 수 있다.

대표도

도 2

특허청구의 범위

청구항 1.

송신하고자 하는 키(key) 데이터를 보안 레벨(k)에 따라 소정 수의 블록으로 분할하는 단계;

상기 키 데이터와 동일한 크기를 가지며 무작위로 생성되는 스크램블 키 데이터를 상기 키 데이터와 동일한 수의 블록으로 분할하는 단계; 및

상기 키 데이터 블록과 스크램블 키 데이터 블록을 서로 혼합하여 생성되는, 상기 키 데이터와 동일한 크기를 가지는 다수의 키 조합 데이터를 송신하는 단계를 포함하며,

상기 보안 레벨에 따라 분할되는 상기 키 데이터와 스크램블 키 데이터의 블록 수(Ks)는 아래의 수학식(1)에 의해 계산되며,

[수학식 1]

$Ks = (n)^k$, n은 자연수

상기 키 조합 데이터는 n의 수만큼 생성되는 것을 특징으로 하는 키 데이터 송신 방법.

청구항 2.

제 1 항에 있어서, 상기 보안 레벨은

송신하고자 하는 키 데이터의 무결성 코드의 생성 여부와 암호화 여부에 따라 결정되는 것을 특징으로 하는 키 데이터 송신 방법.

청구항 3.

삭제

청구항 4.

제 2 항에 있어서,

상기 n의 값은 2인 것을 특징으로 하는 키 데이터 송신 방법.

청구항 5.

제 4 항에 있어서,

상기 키 데이터 블록의 절반은 첫 번째 키 조합 데이터의 홀수 번째 블록에 채워지고 상기 스크램블 키 데이터 블록의 절반은 상기 첫 번째 키 조합 데이터 그룹의 짝수 번째 블록에 채워지며,

상기 키 데이터의 나머지 절반은 두 번째 키 조합 데이터의 홀수 번째 블록에 채워지고 상기 스크램블 키 데이터의 나머지 절반은 상기 두 번째 키 조합 데이터의 짝수 번째 블록에 채워지는 것을 특징으로 하는 키 데이터 송신 방법.

청구항 6.

다수의 키 조합 데이터를 수신하는 단계;

상기 수신되는 다수의 키 조합 데이터를 보안 레벨(k)에 따라 소정 수의 블록으로 각각 분할하는 단계;

상기 분할된 키 조합 데이터의 블록들 중에서 키 데이터 블록을 추출하는 단계; 및

상기 추출된 키 데이터 블록을 조합하여 키 데이터를 생성하는 단계를 포함하며,

상기 보안 레벨에 따라 분할되는 상기 키 조합 데이터의 블록 수(Ks)는 수학식(1)

[수학식1]

$Ks = (n)^k$,n은 자연수

에 의해 계산되는 것을 특징으로 하는 키 데이터 수신 방법.

청구항 7.

제 6 항에 있어서, 상기 보안 레벨은

송신하고자 하는 키 데이터의 무결성 코드의 생성 여부와 암호화 여부에 따라 결정되는 것을 특징으로 하는 키 데이터 수신 방법.

청구항 8.

삭제

청구항 9.

제 7 항에 있어서,

상기 n의 값은 2인 것을 특징으로 하는 키 데이터 수신 방법.

청구항 10.

제 9 항에 있어서,

상기 수신되는 첫 번째 키 조합 데이터의 홀수 번째 블록과 두 번째 키 조합 데이터의 홀수 번째 블록을 키 데이터 블록으로 추출하며,

상기 첫 번째 키 조합 데이터에서 추출된 키 데이터 블록과 두 번째 키 조합 데이터에서 추출된 키 데이터 블록을 순서대로 조합하여 키 데이터를 생성하는 키 데이터 수신 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 무선 센서 네트워크에서 각 센서 노드에 키를 송신하는 방법에 관한 것으로, 보다 구체적으로 보안 레벨에 따라 서로 다른 수의 블록으로 분할된 키 데이터와 스크램블(scramble) 데이터를 서로 혼합하여 키 데이터를 송신하는 방법에 관한 것이다.

무선 센서 네트워크는 지능형 빌딩 또는 공장 내의 환경 제어, 생산 공정 자동 제어, 물류 관리, 병원에서의 물품 및 정보 관리, 환자 상태의 원격 감지 등 여러 분야에서 사용되고 있다. 최근에는 유비쿼터스 무선 네트워크의 핵심적인 인프라 기술로서 그 중요성이 부각되고 있다.

이러한 무선 센서 네트워크의 중요한 이슈는 기기의 소형화, 감지 능력의 향상, 안전하고 빠른 라우팅, 전력 제어 등과 함께 인증 및 보안의 문제를 빼놓을 수 없다. 무선 센서 네트워크에서 기지국에 접속되어 있는 센서 노드들 사이에서 데이터를 송수신하고자 할 때 무선 송수신이라는 특징 때문에, 누구나 쉽게 중간에서 송수신되는 데이터를 해킹할 수 있다.

상기와 같은 무선 센서 네트워크의 보안상 문제점을 해결하기 위해 기지국과 센서 노드들 사이에서 또는 센서 노드들 사이에서 공유하는 키를 사용한다. 키는 크게 센서 노드들 사이에 공유하는 키와 여러 센서 노드들로 구성된 네트워크 내에서 공유하는 키로 구분된다. 네트워크에 접속되어 있는 센서 노드들은 모두 이러한 키를 반드시 가지고 있어야 하며 키는 센서 노드를 인증하거나 데이터의 송수신시 데이터의 암호화/복호화를 위해 사용된다.

도 1은 종래의 키 분배 방법의 일 예를 설명하는 도면이다.

도 1을 참고로, 무선 센서 네트워크의 기지국(1)은 무작위로 다수의 키를 생성하여 키 풀(pool)을 구성하고, 키 풀의 다수 키들 중에서 무작위로 선택된 소정 수의 키를 센서 노드(3, 5, 7)에 각각 송신한다. 센서 노드(3)와 센서 노드(5)가 서로 통신하는 경우, 센서 노드(3)와 센서 노드(5)는 기지국으로부터 임의로 수신한 여러 키들 중에서 서로 일치하는 키를 검색하고 데이터의 송수신시 검색된 키를 이용하여 서로를 인증하거나 송수신되는 데이터를 암호화/복호화한다. 또한 기지국(1)은 다른 기지국(1')과 접속되어 있으며, 기지국(1')에 있는 센서 노드와 기지국(1)에 있는 센서 노드의 통신을 중계하기도 한다.

한편, 종래의 키 분배 방법의 다른 예에서는 키 풀을 구성하여 임의로 생성된 키를 직접 송신하는 대신 각 센서 노드에 분배된 수학적인 다항식을 이용하여 각 센서 노드에 일치하는 키를 계산하고, 상기 계산된 키를 이용하여 서로를 인증하거나 송수신되는 데이터를 암호화/복호화한다.

종래의 키 분배 방법의 또 다른 예에서는 각 센서 노드들을 그리드(grid) 형태로 위치시킨 다음 그리드 상에 센서 노드가 위치하는 x, y 좌표에 따라 쉽게 일치하는 키를 계산하고 계산된 키를 이용하여 서로를 인증하거나 송수신되는 데이터를 암호화/복화화한다.

발명이 이루고자 하는 기술적 과제

그러나 기지국에서 생성된 다수의 키들 중에서 무작위로 선택된 여러 키를 센서 노드들에 분배함으로써, 센서 노드들 간에 일치하는 키를 항상 가지고 있지 않을 수 있으며 일치하는 키를 가질 확률에 의존한다는 단점을 가진다.

또한, 수학적인 다항식을 이용하여 서로 일치하는 키를 계산하는 방법은 키를 직접 송신하지 않는다는 장점은 있지만 복잡한 연산을 통해 일치하는 키를 계산함으로써 최소 사양의 센서 노드에는 적합하지 않다.

한편, 센서 노드가 위치한 좌표에 의해 일치하는 키를 계산하는 방법은 동일한 좌표 상에 위치하는 센서 노드들 사이에서 쉽게 일치하는 키를 찾을 수 있다는 장점이 있으나, 센서 노드의 물리적인 위치에 기초하여 일치하는 키를 계산함으로써 GPS 또는 그 밖의 장치를 이용하여 각 센서 노드의 위치를 파악하여야 하는 단점을 가진다.

따라서 본 발명이 이루고자 하는 목적은 키 데이터와 무작위로 생성된 스크램블 데이터를 보안 레벨에 따라 서로 다른 알고리즘으로 혼합하여 안전하게 송신하는 방법을 제공하는 것이다.

본 발명이 이루고자 하는 다른 목적은 보안 레벨에 따라 서로 다른 알고리즘으로 키 데이터와 스크램블 데이터가 혼합되어 있는 키 조합 데이터에서 키 데이터를 추출하여 키 데이터를 수신하는 방법을 제공하는 것이다.

발명의 구성

상기 본 발명의 목적을 달성하기 위한 키 데이터 송신 방법은 송신하고자 하는 키(key) 데이터를 보안 레벨에 따라 소정 수의 블록으로 분할하고 상기 키 데이터와 동일한 크기를 가지며 무작위로 생성되는 스크램블 키 데이터를 상기 키 데이터와 동일한 수의 블록으로 분할한다. 상기 키 데이터 블록과 스크램블 키 데이터 블록을 서로 혼합하여 생성되는 다수의 키 조합 데이터를 송신하는 단계를 포함한다.

상기 본 발명의 목적을 달성하기 위한 키 데이터 수신 방법은 다수의 키 조합 데이터를 수신하고 수신된 다수의 키 조합 데이터를 보안 레벨에 따라 소정 수의 블록으로 각각 분할한다. 분할된 키 조합 데이터의 블록들 중에서 키 데이터 블록을 추출하고 추출된 키 데이터 블록을 조합하여 키 데이터를 생성한다.

이하 첨부된 도면을 참고로 본 발명에 따른 키 데이터의 송수신 방법에 대해 보다 구체적으로 설명한다.

도 2는 본 발명의 일 실시예에 따른 키 데이터의 송신 방법을 설명하는 흐름도이다.

도 2를 참고로, 무선 네트워크에서 송신되는 데이터에 대한 보안의 중요성에 따라 보안 레벨을 설정한다(단계 1). [표1]은 보안의 중요성에 따라 설정된 보안 레벨의 예를 도시하고 있다.

[표 1]

보안레벨(k)	데이터 암호화	무결성 코드 생성
0	x	x
1	x	o
2	o	x
3	o	o

보안의 중요성에 따라 데이터를 암호화하거나 무결성 코드(Message Integrity Code)를 생성한다. 무결성 코드란 송신되는 데이터가 제3자에 인가되지 않은 방법으로 변경되었는지의 여부를 확인할 수 있는 코드이다. 데이터를 암호화하지 않고 무결성 코드도 생성하지 않는 보안 레벨을 0, 데이터를 암호화하지 않고 무결성 코드만 생성하는 보안 레벨을 1, 데이터를 암호화하고 무결성 코드는 생성하지 않는 보안 레벨을 2, 데이터를 암호화하고 무결성 코드도 생성하는 보안 레벨을 3으로 설정한다. 즉, 보안 레벨(k)은 송신되는 데이터의 암호화 여부와 무결성 코드의 생성 여부에 따라 서로 다르게 설정된다.

예를 들어, 보안 레벨 1은 데이터는 암호화되지 않고 데이터의 무결성 코드만 생성하는 것으로, 암호화할 만큼 중요하지 않은 데이터들이 송수신되는 무선 센서 네트워크에서 유용한 보안 레벨이다. 한편, 보안 레벨 3은 데이터를 암호화하고 무결성 코드도 생성되는 것으로, 보안이 절대적으로 유지되어야 하는 무선 센서 네트워크에서 유용한 보안 레벨이다.

송신하고자 하는 키 데이터 및 키 데이터와 혼합되는 스크램블(scramble) 데이터를 생성한다(단계 3). 본 발명의 일 예에서 키 데이터와 스크램블 데이터는 해쉬(harsh) 함수에 의해 무작위로 생성되며 키 데이터와 스크램블 데이터는 동일한 크기로 생성되는 것을 특징으로 한다. 도 3과 도 4는 각각 해쉬 함수에 의해 생성된 키 데이터와 스크램블 데이터의 일 예를 도시하고 있다. 도 3과 도 4에 일 예로 도시된 키 데이터와 스크램블 데이터의 크기는 16바이트이다.

생성된 키 데이터와 스크램블 데이터를 소정 수의 블록으로 분할한다(단계 5 및 단계 7). 키 데이터와 스크램블 데이터가 분할되는 블록의 수(Ks)는 설정된 보안 레벨(k)에 따라 아래의 수학식(1)과 같이 계산된다.

[수학식 1]

$Ks = (n)^k$, n은 자연수

예를 들어, 설정된 보안 레벨이 0이면 생성된 키 데이터는 분할되지 않으며 생성된 키 데이터는 스크램블 데이터와 서로 혼합되지 않고 센서 노드에 송신된다. 한편, 설정된 보안 레벨이 2이면 생성된 키 데이터와 스크램블 데이터는 $(n)^2$의 블록 수로 분할된다.

본 발명이 적용되는 분야에 따라 생성되는 키 데이터와 스크램블 데이터의 크기는 달라질 수 있으며, 생성된 키 데이터와 스크램블 데이터의 크기 또는 실시예에 따라 n의 값은 서로 다르게 설정될 수 있다.

분할된 키 데이터 블록과 스크램블 데이터 블록을 서로 혼합하여 다수의 키 조합 데이터를 생성한다(단계 8). 생성된 키 조합 데이터는 키 데이터와 동일한 크기로 생성되는 것을 특징으로 한다. 생성된 다수의 키 조합 데이터를 이용하여 센서 노드에 키 데이터를 송신한다(단계 9).

도 5는 본 발명에 따른 키 조합 데이터의 생성 예를 설명하기 위한 도면이다.

도 5를 참고로, n의 값이 2이고 보안 레벨(k)이 2인 경우 생성된 도 3의 키 데이터와 도 4의 스크램블 데이터는 각각 4개의 블록으로 분할된다.

도 5의 (a)는 4개로 각각 분할된 키 데이터 블록과 스크램블 데이터 블록으로 생성되는 첫 번째 키 조합 데이터를 도시하고 있다. 분할된 4개의 키 데이터 블록들 중 처음 2 블록은 첫 번째 키 조합 데이터의 홀수 번째 블록에 배치된다. 분할된 4개의 스크램블 데이터 블록들 중 처음 2 블록은 첫 번째 키 조합 데이터의 짝수 번째 블록에 배치된다.

도 5의 (b)는 4개로 각각 분할된 키 데이터 블록과 스크램블 데이터 블록으로 생성되는 두 번째 키 조합 데이터를 도시하고 있다. 분할된 4개의 키 데이터 블록들 중 나머지 2 블록은 두 번째 키 조합 데이터의 홀수 번째 블록에 배치된다. 분할된 4개의 스크램블 데이터 블록들 중 나머지 2 블록은 두 번째 키 조합 데이터의 짝수 번째 블록에 배치된다.

도 5의 (a)와 (b)에 도시되어 있는 것과 같이, 송신하고자 하는 키 데이터는 스크램블 데이터와 조합되어 2개의 키 조합 데이터를 생성하며, 송신하고자 하는 키 데이터는 키 조합 데이터를 이용하여 센서 노드로 송신된다.

도 6은 본 발명에 따른 키 조합 데이터의 다른 생성 예를 설명하기 위한 도면이다.

도 6을 참고로, n의 값이 3이고 보안 레벨(k)이 1인 경우 키 데이터와 스크램블 데이터는 각각 3개의 블록으로 분할된다.

도 6(a)는 3개로 각각 분할된 키 데이터 블록과 스크램블 데이터 블록으로 생성되는 첫 번째 키 조합 데이터를 도시하고 있다. 분할된 3개의 키 데이터 블록들 중 처음 블록은 첫 번째 키 조합 데이터의 첫 번째 블록에 배치된다. 분할된 3개의 스크램블 데이터 블록들 중 두 번째 블록과 세 번째 블록은 첫 번째 키 조합 데이터의 두 번째 블록과 세 번째 블록에 배치된다.

도 6(b)는 3개로 각각 분할된 키 데이터 블록과 스크램블 데이터 블록으로 생성되는 두 번째 키 조합 데이터를 도시하고 있다. 분할된 3개의 키 데이터 블록들 중 두 번째 블록은 두 번째 키 조합 데이터의 두 번째 블록에 배치된다. 분할된 3개의 스크램블 데이터 블록들 중 첫 번째 블록과 세 번째 블록은 두 번째 키 조합 데이터의 첫 번째 블록과 세 번째 블록에 배치된다.

도 6(c)는 3개로 각각 분할된 키 데이터 블록과 스크램블 데이터 블록으로 생성되는 세 번째 키 조합 데이터를 도시하고 있다. 분할된 3개의 키 데이터 블록들 중 세 번째 블록은 세 번째 키 조합 데이터의 세 번째 블록에 배치된다. 분할된 3개의 스크램블 데이터 블록들 중 첫 번째 블록과 두 번째 블록은 세 번째 키 조합 데이터의 첫 번째 블록과 두 번째 블록에 배치된다.

도 6(a), 6(b) 및 6(c)에 도시되어 있는 것과 같이, 송신하고자 하는 키 데이터는 스크램블 데이터와 조합되어 3개의 키 조합 데이터를 생성하며, 송신하고자 하는 데이터는 키 조합 데이터를 이용하여 센서 노드에 송신된다. 본 발명이 적용되는 분야에 따라 다양한 키 데이터 블록과 스크램블 데이터 블록의 조합 방법이 사용될 수 있으며 이는 본 발명의 범위에 속한다.

도 7은 본 발명의 일 실시예에 따른 키 데이터의 수신 방법을 설명하는 흐름도이다.

도 7을 참고로, 무선 센서 네트워크의 기지국으로부터 다수의 키 조합 데이터를 수신한다(단계 11). 무선 센서 네트워크에서 보안 레벨이 설정되어 있는 경우(단계 13), 수신된 키 조합 데이터를 보안 레벨에 따라 소정 수의 블록으로 분할한다(단계 15). 무선 센서 네트워크에서 키 조합 데이터를 송신하는 기지국과 키 조합 데이터를 수신하는 센서 노드는 서로 동일한 보안 레벨로 설정된다.

설정된 보안 레벨에 따라 계산되는 상기 수학식(1)에 의해 블록 수(Ks)가 결정되고 결정된 블록 수에 따라 수신한 다수의 키 조합 데이터를 각각 분할한다(단계 15). 분할된 키 조합 데이터 블록들 중에서 키 데이터 블록을 추출하고(단계 17), 추출된 키 데이터 블록을 조합하여 키 데이터를 생성한다(단계 19). 분할된 키 조합 데이터 블록들 중에서 키 데이터 블록은 기지국에서 키 조합 데이터를 생성하는 알고리즘과 반대로 수행함으로써 추출할 수 있다.

예를 들어, 도 5의 (a)와 (b)에 도시된 2개의 키 조합 데이터를 수신하는 경우, 첫 번째 키 조합 데이터와 두 번째 키 조합 데이터를 각각 4개의 블록으로 분할한다. 4개로 분할된 첫 번째 키 조합 데이터의 블록들 중 홀수 번째 블록을 키 데이터 블록으로 추출하고, 4개로 분할된 두 번째 키 조합 데이터의 블록들 중 홀수 번째 블록을 키 데이터 블록으로 각각 추출한다. 첫 번째 키 조합 데이터 블록에서 추출된 키 데이터 블록들과 두 번째 키 조합 데이터 블록에서 추출된 키 데이터 블록들을 순서대로 조합하여 키 데이터를 생성한다.

한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성 가능하고, 컴퓨터로 읽을 수 있는 기록 매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장 매체(예를 들어, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장 매체를 포함한다.

본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

본 발명에 따른 키 데이터 송수신 방법은 보안 레벨에 따라 키 데이터와 스크램블 데이터를 조합하여 생성된 다수의 키 조합 데이터를 이용하여 키 데이터를 센서 노드에 송신하고 키 조합 데이터를 수신한 센서 노드는 보안 레벨에 따라 수신한 키 조합 데이터에서 키 데이터를 추출하여 키 데이터를 생성함으로써, 무선 센서 네트워크에서 기지국과 센서 노드들 사이에서 안전하고 간단하게 키 데이터를 송수신할 수 있다.

또한 본 발명에 따른 키 데이터 송수신 방법은 보안 레벨에 따라 키 데이터와 스크램블 데이터의 조합 복합도를 조절할 수 있기 때문에, 무선 센서 네트워크의 보안 중요성에 따라 보안 정도를 유연하게 조절할 수 있다.

도면의 간단한 설명

도 1은 종래 키 데이터의 분배 방법의 일 예를 설명하는 도면이다.

도 2는 본 발명의 일 실시예에 따른 키 데이터의 송신 방법을 설명하는 흐름도이다.

도 3과 도 4는 각각 해쉬 함수에 의해 생성된 키 데이터와 스크램블 데이터의 일 예를 도시하고 있다.

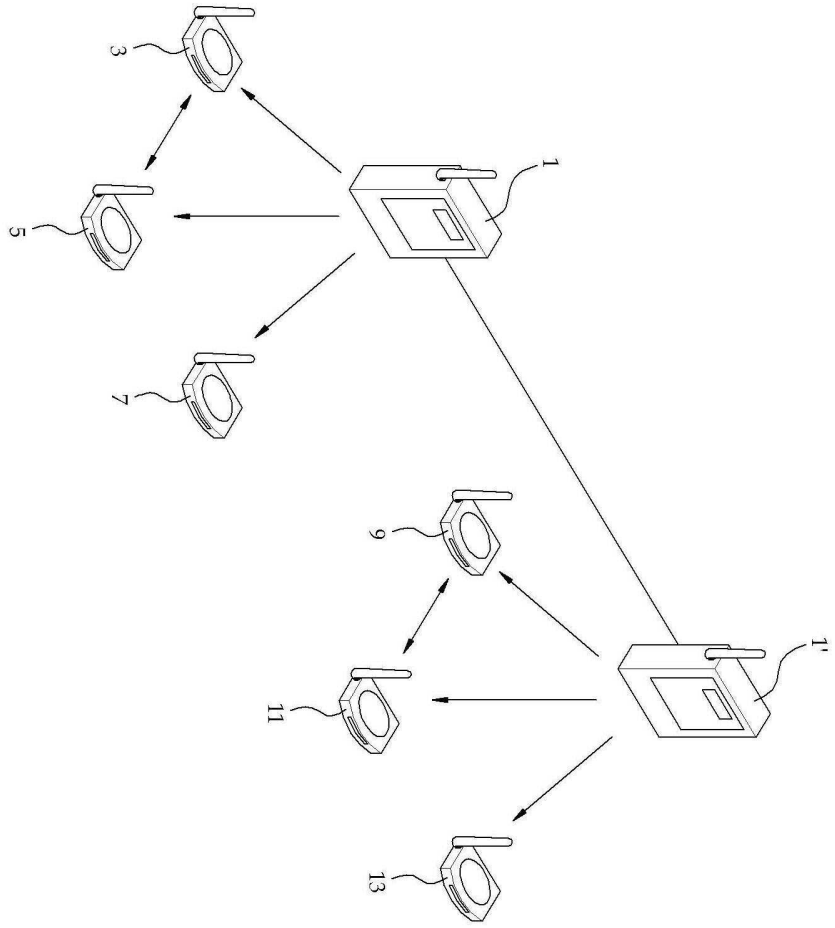
도 5는 본 발명에 따른 키 조합 데이터의 생성 예를 설명하기 위한 도면이다.

도 6은 본 발명에 따른 키 조합 데이터의 다른 생성 예를 설명하기 위한 도면이다.

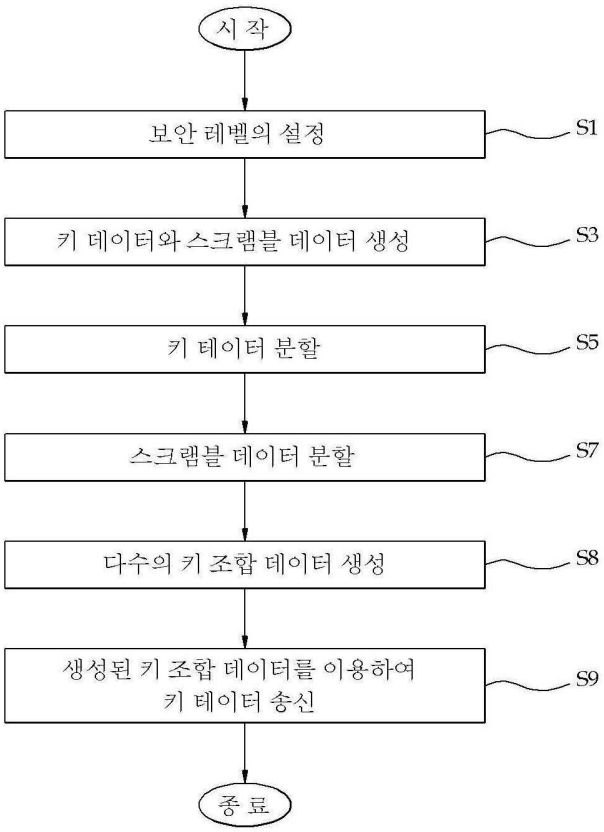
도 7은 본 발명의 일 실시예에 따른 키 데이터의 수신 방법을 설명하는 흐름도이다.

도면

도면1



도면2



도면3

키 데이터

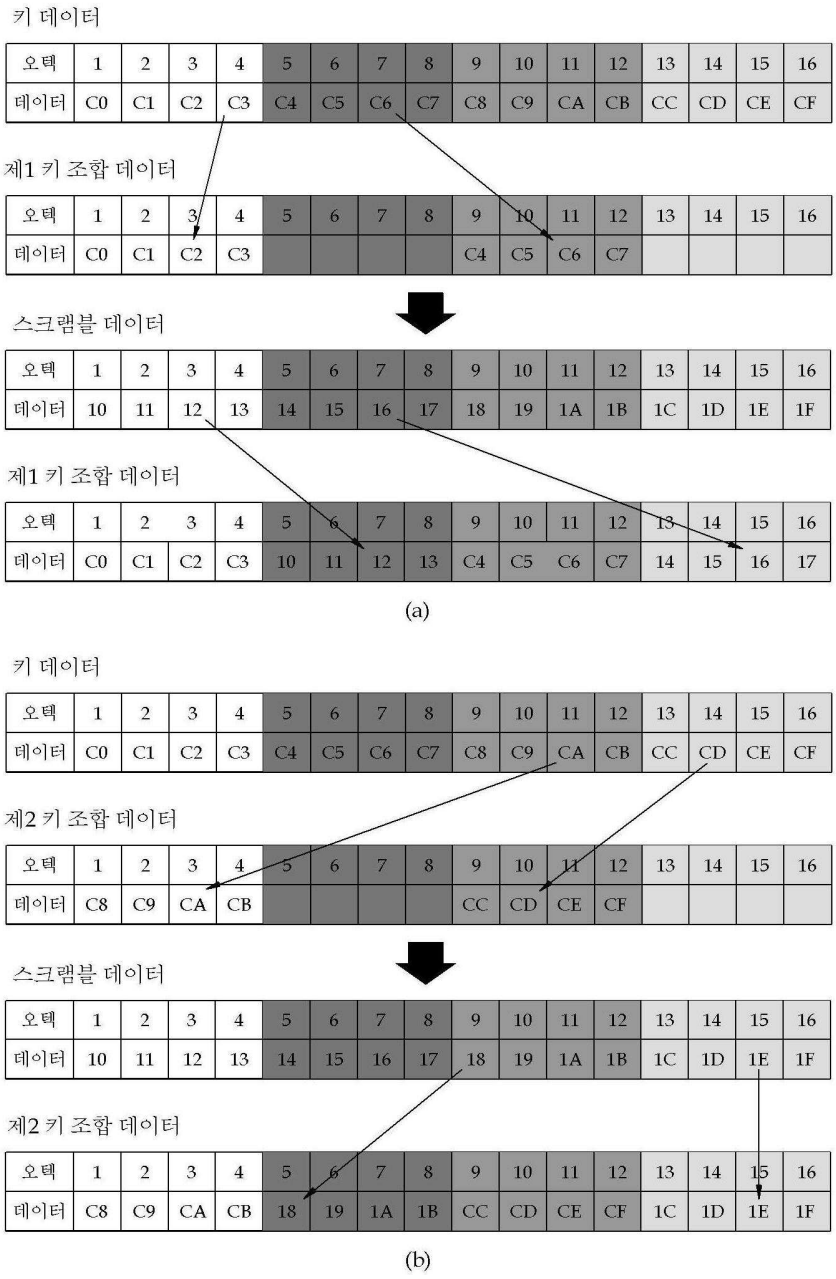
오택	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
데이터	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	CE	CF

도면4

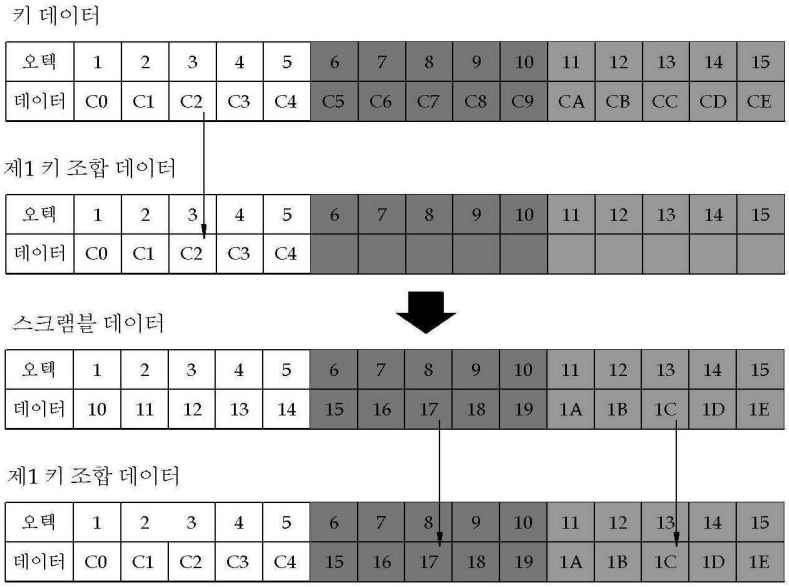
스크램블 데이터

오택	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
데이터	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F

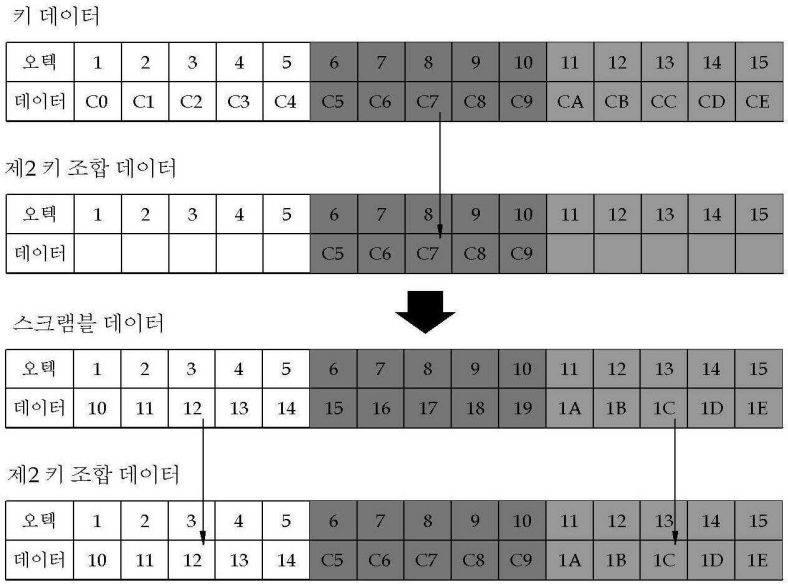
도면5


키 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF
제1 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 C0 C1 C2 C3 C4 C5 C6 C7
스크램블 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
제1 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 C0 C1 C2 C3 10 11 12 13 C4 C5 C6 C7 14 15 16 17
(a)
키 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF
제2 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 C8 C9 CA CB CC CD CE CF
스크램블 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
제2 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
데이터 C8 C9 CA CB 18 19 1A 1B CC CD CE CF 1C 1D 1E 1F
(b)

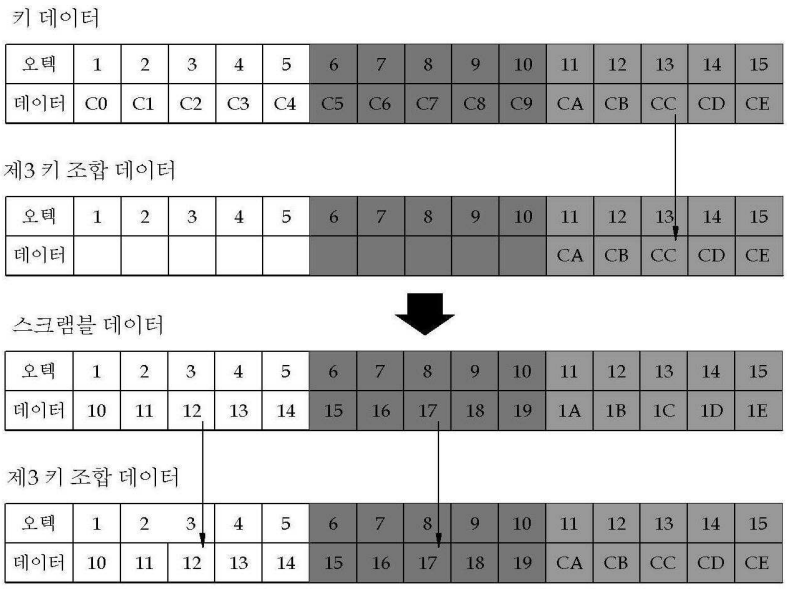
도면6a


키 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE
제1 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 C0 C1 C2 C3 C4
스크램블 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E
제1 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 C0 C1 C2 C3 C4 15 16 17 18 19 1A 1B 1C 1D 1E

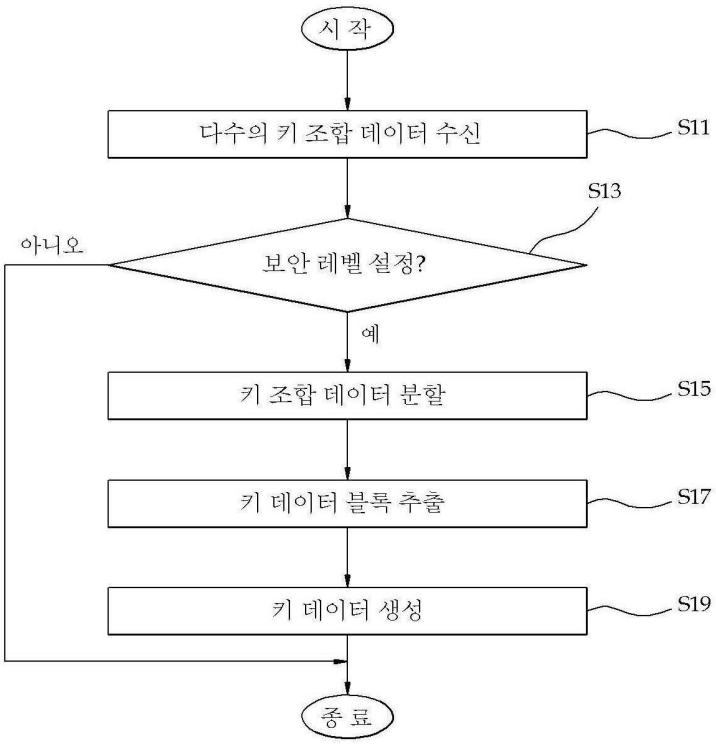
도면6b


키 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE
제2 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 C5 C6 C7 C8 C9
스크램블 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E
제2 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 10 11 12 13 14 C5 C6 C7 C8 C9 1A 1B 1C 1D 1E

도면6c


키 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE
제3 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 CA CB CC CD CE
스크램블 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E
제3 키 조합 데이터
오택 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
데이터 10 11 12 13 14 15 16 17 18 19 CA CB CC CD CE

도면7


시 작
다수의 키 조합 데이터 수신
S11
S13
보안 레벨 설정?
아니오
예
키 조합 데이터 분할
S15
키 데이터 블록 추출
S17
키 데이터 생성
S19
종 료