(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년09월03일
(11) 등록번호 10-2702344
(24) 등록일자 2024년08월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/0858 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2021-0006692
(22) 출원일자 2021년01월18일
심사청구일자 2021년01월18일
(65) 공개번호 10-2022-0040349
(43) 공개일자 2022년03월30일
(30) 우선권주장
1020200122661 2020년09월23일 대한민국(KR)
(56) 선행기술조사문헌
KR100584170 B1*
US20160285621 A1*
Krendelev, S. et al.,"Block cipher based on modular arithmetic and methods of information compression" Journal of Physics: Conference Series. Vol. 913. No. 1.(2017.09.15.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
노광석
서울특별시 도봉구 시루봉로 71, 107동 106호(방학동, 청구아파트)
허준
서울특별시 강남구 광평로10길 6, 206동 103호(일원동, 한솔마을아파트)
(74) 대리인
이대호, 박건홍

전체 청구항 수 : 총 11 항 심사관 : 양종필

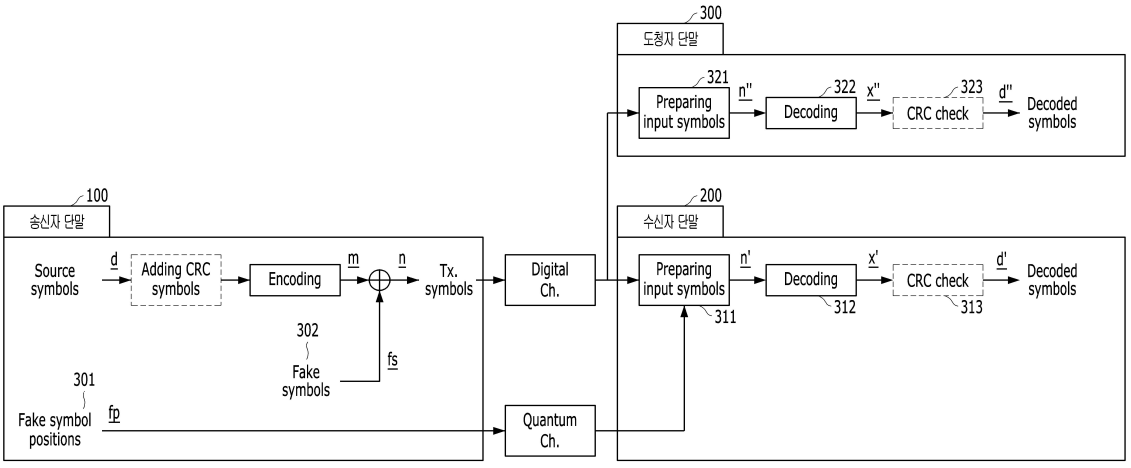
(54) 발명의 명칭 **보안이 강화된 데이터 전송 방법**

(57) 요 약

본 개시의 몇몇 실시예에 따라, 송신자 단말의 프로세서에 의해 수행되는 보안이 강화된 데이터 전송 방법이 개시된다. 상기 방법은: 퀀텀 채널(quantum channel)을 통해 수신자 단말로 전송된 키 시퀀스(key sequence) 및 전송할 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2

(뒷면에 계속)

대 표 도



정보를 생성하는 단계; 복수 개의 소스 심볼(source symbol)을 부호화(encoding)하여, 오류정정부호 및 복수 개의 부호화된 심볼(encoded symbol)을 획득하는 단계; 상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는 단계; 및 상기 적어도 하나의 페이크 심볼, 상기 복수 개의 부호화된 심볼 중 상기 적어도 하나의 페이크 심볼로 변경되지 않은 나머지 심볼 및 상기 오류정정부호를 디지털 채널(digital channel)을 통해 수신자 단말로 전송하는 단계;를 포함할 수 있다.

(52) CPC특허분류
H04L 9/0863 (2013.01)
H04L 2209/34 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711093219
과제번호	IITP-2020-2015-0-00385
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터지원사업
연구과제명	무결점 보안을 위한 지상/위성 양자통신 기술개발
기 여 율	1/1
과제수행기관명	고려대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

송신자 단말의 프로세서에 의해 수행되는 보안이 강화된 데이터 전송 방법에 있어서,

퀀텀 채널(quantum channel)을 통해 수신자 단말로 전송된 키 시퀀스(key sequence) 및 전송할 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계;

복수 개의 소스 심볼(source symbol)을 부호화(encoding)하여, 오류정정부호 및 복수 개의 부호화된 심볼(encoded symbol)을 획득하는 단계;

상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는 단계; 및

상기 적어도 하나의 페이크 심볼, 상기 복수 개의 부호화된 심볼 중 상기 적어도 하나의 페이크 심볼로 변경되지 않은 나머지 심볼 및 상기 오류정정부호를 디지털 채널(digital channel)을 통해 수신자 단말로 전송하는 단계;

를 포함하고,

상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는 단계는,

상기 적어도 하나의 페이크 심볼 각각의 제 1 위치를 인식하는 단계;

상기 복수 개의 부호화된 심볼 중 상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼을 인식하는 단계; 및

상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각을 상기 적어도 하나의 페이크 심볼 각각으로 대체하는 단계;

를 포함하는,

보안이 강화된 데이터 전송 방법.

청구항 2

제 1 항에 있어서,

상기 키 시퀀스는,

상기 송신자 단말에서 상기 수신자 단말로 랜덤 값이 상기 퀀텀 채널을 통해 전송되는 경우, 상기 랜덤 값을 기초로 생성되는,

보안이 강화된 데이터 전송 방법.

청구항 3

제 1 항에 있어서,

상기 퀀텀 채널을 통해 수신자 단말로 전송된 키 시퀀스 및 전송할 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계는,

상기 키 시퀀스의 길이 및 상기 전송할 심볼의 개수를 제 1 수학식의 입력 값으로 하여, 상기 제 1 정보를 생성

하는 단계; 및

상기 전송할 심볼의 개수를 제 2 수학식의 입력 값으로 하여, 상기 제 2 정보를 생성하는 단계;

를 포함하고,

상기 제 1 수학식은 $f = \left\lfloor \frac{len(key)}{\lceil \log_2 n \rceil} \right\rfloor$ 이고,

상기 f는 상기 페이크 심볼의 개수이고, 상기 len(key)는 상기 키 시퀀스의 길이이고, 상기 n은 상기 전송할 심볼의 개수이고,

상기 제 2 수학식은 $p = \lceil \log_2 n \rceil$ 이고,

상기 p는 상기 페이크 심볼의 위치를 비트(bit)로 나타낸 값이고, 상기 n은 상기 전송할 심볼의 개수인,

보안이 강화된 데이터 전송 방법.

청구항 4

삭제

청구항 5

삭제

청구항 6

제 1 항에 있어서,

상기 복수 개의 소스 심볼을 부호화하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득하는 단계는,

상기 복수 개의 소스 심볼에 기초하여, 적어도 하나의 CRC(Cyclic Redundancy Check) 심볼을 생성하는 단계; 및

상기 복수 개의 소스 심볼 및 상기 CRC 심볼을 부호화 하여, 상기 오류정정부호 및 상기 복수 개의 부호화된 심볼을 획득하는 단계;

를 포함하는,

보안이 강화된 데이터 전송 방법.

청구항 7

제 1 항에 있어서,

상기 복수 개의 소스 심볼을 부호화하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득하는 단계는,

상기 복수 개의 소스 심볼 각각을 symbol-wise XOR하여, 상기 오류정정부호 및 상기 복수 개의 부호화된 심볼을 획득하는 단계;

를 포함하고,

상기 오류정정부호는,

전송 채널에서 발생하는 전송 신호의 오류를 정정하는 기능을 제공하는,

보안이 강화된 데이터 전송 방법.

청구항 8

삭제

청구항 9

송신자 단말의 프로세서에 의해 수행되는 보안이 강화된 데이터 전송 방법에 있어서,

퀀텀 채널(quantum channel)을 통해 수신자 단말로 전송된 키 시퀀스(key sequence) 및 전송할 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계;

복수 개의 소스 심볼(source symbol)을 부호화(encoding)하여, 오류정정부호 및 복수 개의 부호화된 심볼(encoded symbol)을 획득하는 단계;

상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는 단계; 및

상기 적어도 하나의 페이크 심볼, 상기 복수 개의 부호화된 심볼 중 상기 적어도 하나의 페이크 심볼로 변경되지 않은 나머지 심볼 및 상기 오류정정부호를 디지털 채널(digital channel)을 통해 수신자 단말로 전송하는 단계;

를 포함하고,

상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는 단계는,

상기 적어도 하나의 페이크 심볼 각각의 제 1 위치를 인식하는 단계;

상기 복수 개의 부호화된 심볼 중 상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼을 인식하는 단계;

상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각과 상기 적어도 하나의 페이크 심볼 각각을 연산하는 단계; 및

상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각을 상기 연산 결과 값 각각으로 대체하는 단계;

를 포함하는,

보안이 강화된 데이터 전송 방법.

청구항 10

수신자 단말의 프로세서에 의해 수행되는 보안이 강화된 데이터 수신 방법에 있어서,

디지털 채널(digital channel)을 통해 복수 개의 심볼 및 오류정정부호를 송신자 단말로부터 수신하는 단계;

상기 송신자 단말로부터 퀀텀 채널(quantum channel)을 통해 사전에 수신된 키 시퀀스 및 상기 복수 개의 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계;

상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 심볼 중에서 적어도 하나의 페이크 심볼을 제거하는 단계; 및

상기 복수 개의 심볼 중에서 상기 적어도 하나의 페이크 심볼이 제거된 나머지 심볼 및 상기 오류정정부호를 이용하여, 복호화된 심볼(decoded symbol)을 획득하는 단계;

를 포함하고,

상기 송신자 단말로부터 퀀텀 채널(quantum channel)을 통해 사전에 수신된 키 시퀀스 및 상기 복수 개의 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계는,

상기 키 시퀀스의 길이 및 상기 복수 개의 심볼의 개수를 제 1 수학식의 입력 값으로 하여, 상기 제 1 정보를 생성하는 단계; 및

상기 복수 개의 심볼의 개수를 제 2 수학식의 입력 값으로 하여, 상기 제 1 정보를 생성하는 단계;

를 포함하고,

상기 제 1 수학식은 $f = \left\lfloor \frac{len(key)}{\lceil \log_2 n \rceil} \right\rfloor$ 이고,

상기 f는 상기 페이크 심볼의 개수이고, 상기 len(key)는 상기 키 시퀀스의 길이이고, 상기 n은 상기 복수 개의 심볼의 개수이고,

상기 제 2 수학식은 $p = \lceil \log_2 n \rceil$ 이고,

상기 p는 상기 페이크 심볼의 위치를 비트(bit)로 나타낸 값이고, 상기 n은 상기 복수 개의 심볼의 개수인,

보안이 강화된 데이터 수신 방법.

청구항 11

제 10 항에 있어서,

상기 키 시퀀스는,

상기 송신자 단말에서 상기 수신자 단말로 랜덤 값이 상기 퀀텀 채널을 통해 전송되는 경우, 상기 랜덤 값을 기초로 생성되는,

보안이 강화된 데이터 수신 방법.

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

제 10 항에 있어서,

상기 복수 개의 심볼 중에서 상기 적어도 하나의 페이크 심볼이 제거된 나머지 심볼 및 상기 오류정정부호를 이용하여, 복호화된 심볼을 획득하는 단계는,

상기 오류정정부호를 이용하여, 상기 적어도 하나의 페이크 심볼이 제거된 위치에 대응하는 심볼을 복원하는 단계; 및

복원된 심볼 및 상기 나머지 심볼을 복호화하여, 상기 복호화된 심볼을 획득하는 단계;

를 포함하는,

보안이 강화된 데이터 수신 방법.

청구항 16

제 10 항에 있어서,

상기 복수 개의 심볼은,

복수 개의 부호화된 심볼(encoded symbol) 및 상기 적어도 하나의 페이크 심볼을 포함하고,

상기 복수 개의 부호화된 심볼은,

복수 개의 소스 심볼에 기초하여 생성된 적어도 하나의 CRC(Cyclic Redundancy Check) 심볼 및 상기 복수 개의 소스 심볼이 상기 송신자 단말에 의해 부호화된 심볼인,

보안이 강화된 데이터 수신 방법.

청구항 17

제 16 항에 있어서,

상기 나머지 심볼을 복호화함에 따라, 상기 CRC 심볼을 포함하는 상기 복호화된 심볼을 획득한 경우, 상기 CRC 심볼을 이용하여 정상적으로 복호화 되었는지 여부를 인식하는 단계;

를 더 포함하는,

보안이 강화된 데이터 수신 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 보안이 강화된 데이터 전송 방법에 관한 것으로, 구체적으로 데이터를 전송할 때 양자키분배 프로토콜을 이용하는 방법에 관한 것이다.

배 경 기 술

[0002] 오류정정부호(FEC, Forward Error Correction)는 전송 채널에서 발생하는 전송 신호의 오류 등을 정정하는 기능을 제공한다. 특히, 전송한 신호가 사라지는 것으로 모델링되는 erasure channel을 사용하는 application layer FEC에서는 전송이 된 신호는 오류가 없는 것으로 간주하고, 오류가 있는 신호는 하위 layer의 Cyclic Redundancy Check(CRC)를 통해 해당 신호를 제거한 뒤 사용하게 된다. 대표적으로 Luby Transform(LT) code와 3GPP MBMS, DVB-IPTV, IETF 등의 여러 표준에서 사용하는 Raptor code가 있다.

[0003] 도 1은 LT code를 설명하기 위한 도면이다. 도 1을 참조하면, LT code는 source symbol을 이용하여 CRC 심볼을 생성 및 추가한 뒤 부호화를 수행한다. 전송된 신호는 수신단에서 채널에 의해 발생한 erased symbol을 제거한 뒤 복호화를 수행하고 CRC check 후에 원래 신호를 복원할 수 있다. 이 때, CRC는 선택적으로 사용할 수 있다.

[0004] 구체적으로, 송신자 블록은 LT encoding 블록이고, 수신자 블록인 LT decoding 블록은 합법적인 수신자의 블록이라고 가정하고 이하 설명한다. 송신자 블록은 Adding CRC symbols(101)을 수행할 수 있다. 구체적으로, 송신자 블록은 source block을 기반으로 application layer의 CRC symbol을 생성한다. 다만, 송신자 블록은 CRC symbol을 선택적으로 사용할 수 있다. 즉, 송신자 블록은 CRC symbol을 생성하지 않을 수 있다.

[0005] 송신자 블록은 LT code의 부호화 블록(102)을 포함할 수 있다. 여기서, 부호화 블록(102)은 encoded symbol m을 생성할 수 있다. 그리고, 송신자 블록은 encoded symbol을 디지털 채널을 통해 수신자 블록으로 전송할 수 있다.

[0006] 수신자 블록은 Preparing input symbols(111)을 수행할 수 있다. 구체적으로, 수신자 블록은 LT code의 복호화를 위해 하위 layer에서의 CRC check를 통해 erased symbol을 파악할 수 있다. 그리고, 수신자 블록은 erased symbol을 제외한 나머지 수신 심볼을 복호화에 사용하기 위해 준비할 수 있다.

[0007] 수신자 블록은 복호화 블록(112)을 포함할 수 있다. 여기서, 복호화 블록(112)은 erased symbol을 제외한 나머지 수신 심볼을 이용하여 복호화를 수행할 수 있다. 그리고, 수신자 블록은 Adding CRC symbols(101)에 대응되는 기능을 수행할 수 있다. 즉, 수신자 블록은 CRC symbols가 신호에 포함된 경우, CRC Check(113)를 수행할 수 있다. 최종적으로, 수신자 블록이 수행한 CRC Check(113)의 결과에 이상이 없으면 성공적인 source symbol 전송이 이루어진다.

[0008] 한편, 양자키분배 프로토콜(Quantum Key Distribution(QKD) protocol)은 도청자의 무한한 계산 능력, 저장공간

을 가정하더라도, 양자역학적 특성으로 인해 도청 불가능한 random 키를 송/수신자가 공유함으로써 보안(security)을 제공하는 프로토콜이다. 예를 들어, 대표적인 QKD protocol인 BB84 프로토콜은 이론적으로 완벽한 보안을 제공한다.

[0009] 다른 한편, Random Number Generator(RNG)는 random한 숫자열을 제공하며, 일반적으로 Pseudo-RNG(PRNG), True RNG(TRNG), Quantum RNG(QRNG)로 구분한다. PRNG는 랜덤한 시드 값을 기반으로 deterministic mathematical algorithm을 통해 숫자열을 생성한다. 그러나, deterministic mathematical algorithm으로 인해 pattern이 발생하게 된다. TRNG는 노이즈, 주사위 던지기 같은 chaotic 동작이나 제어 불가능하고 예측 불가능한 값을 이용하여 숫자열을 생성한다. QRNG는 양자 고유의 비결정적인 양자 프로세스에 의해 숫자열을 생성한다. TRNG와 QRNG에서 생성한 숫자열은 예측 불가능하고 패턴이 없는 특성을 갖게 된다.

[0010] 또 다른 한편, Secure Forward Error Correction(secure FEC)는 도청을 효과적으로 막는 무결성, 인증 등을 위한 암호화 기법을 오류정정부호에 적용한 기법이다. secure FEC는 오류정정부호의 부호화/복호화에 사용하는 코드 구조의 일부 정보를 암호화 기법을 통해 수신자에게 전달하여 정상적인 수신자가 복호화를 수행할 수 있게 하며, 비정상적인 수신자인 도청자는 암호화된 코드 구조 일부 정보를 알 수 없으므로 오류정정부호의 복호화가 불가능하다.

[0011] 도 2는 기존 secure FEC 기법을 설명하기 위한 도면이다. 도 2를 참조하면, 송신자와 수신자는 reference database를 공유하고 이를 FEC encoding에 사용하는 source packet에 더해 부호화한 후 송신자에게 전송한다. 그리고, 수신자는 공유하고 있는 reference database를 이용하여 복호화를 수행하여 source packet을 복원하게 된다. 이 때, 공유하는 reference database는 암호화 기법 등을 통해 도청자가 도청하지 못하는 것으로 가정한다.

[0012] 상술한 바와 같이, 디지털 통신에서 오류정정부호는 도청을 효과적으로 막는 무결성, 인증 등을 위한 추가적인 암호화 기능을 이용할 뿐 오류정정부호 자체는 도청을 막는 기능을 제공하지 않는다. 암호화 기능을 오류정정부호와 결합한 secure FEC 기법은 암호화 기법을 통해 전송되는 정보가 도청자에게 도청되지 않는다는 가정으로 구성되어 있다.

[0013] 따라서, 암호화 기법을 통해 전송되는 정보가 도청자에게 도청되지 않는다는 가정을 하지 않더라도 완벽한 보안을 제공하는 오류정정부호를 처리하기 위한 방법 및 장치에 대한 연구의 필요성이 당업계에 존재할 수 있다.

선행기술문헌

비특허문헌

[0014] (비특허문헌 0001) C. H. Shih, Y. Y. Xu, and Y. TienWang, ”Secure and Reliable IPTV Multimedia Transmission Using Forward Error Correction,” International Journal of Digital Multimedia Broadcasting, Volume 2012, Article ID 720791, 2012.

발명의 내용

해결하려는 과제

[0015] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 보안성이 높은 데이터 전송 방법을 제공하고자 한다.

[0016] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0017] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 송신자 단말의 프로세서에 의해 수행되는 보안이 강화된 데이터 전송 방법이 개시된다. 상기 방법은: 퀀텀 채널(quantum channel)을 통해 수신자 단말로 전송된 키 시퀀스(key sequence) 및 전송할 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계; 복수 개의 소스 심볼(source symbol)을 부호화(encoding)하여, 오류정정부호 및 복수 개의 부호화된 심볼(encoded symbol)을 획득하는 단계; 상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는

단계; 및 상기 적어도 하나의 페이크 심볼, 상기 복수 개의 부호화된 심볼 중 상기 적어도 하나의 페이크 심볼로 변경되지 않은 나머지 심볼 및 상기 오류정정부호를 디지털 채널(digital channel)을 통해 수신자 단말로 전송하는 단계;를 포함할 수 있다.

[0018] 또한, 상기 키 시퀀스는, 상기 송신자 단말에서 상기 수신자 단말로 랜덤 값이 상기 퀀텀 채널을 통해 전송되는 경우, 상기 랜덤 값을 기초로 생성될 수 있다.

[0019] 또한, 상기 퀀텀 채널을 통해 수신자 단말로 전송된 키 시퀀스 및 전송할 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계는, 상기 키 시퀀스의 길이 및 상기 전송할 심볼의 개수를 제 1 수학식의 입력 값으로 하여, 상기 제 1 정보를 생성하는 단계; 및 상기 전송할 심볼의 개수를 제 2 수학식의 입력 값으로 하여, 상기 제 1 정보를 생성하는 단계;를 포함할 수 있다.

[0020] 또한, 상기 제 1 수학식은 $f = \left\lfloor \frac{len(key)}{\lceil \log_2 n \rceil} \right\rfloor$ 이고, 상기 f는 상기 페이크 심볼의 개수이고, 상기 len(key)는 상기 키 시퀀스의 길이이고, 상기 n은 상기 전송할 심볼의 개수일 수 있다.

[0021] 또한, 상기 제 2 수학식은 $p = \lceil \log_2 n \rceil$ 이고, 상기 p는 상기 페이크 심볼의 위치를 비트(bit)로 나타낸 값이고, 상기 n은 상기 전송할 심볼의 개수일 수 있다.

[0022] 또한, 상기 복수 개의 소스 심볼을 부호화하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득하는 단계는, 상기 복수 개의 소스 심볼에 기초하여, 적어도 하나의 CRC(Cyclic Redundancy Check) 심볼을 생성하는 단계; 및 상기 복수 개의 소스 심볼 및 상기 CRC 심볼을 부호화 하여, 상기 오류정정부호 및 상기 복수 개의 부호화된 심볼을 획득하는 단계;를 포함할 수 있다.

[0023] 또한, 상기 복수 개의 소스 심볼을 부호화하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득하는 단계는, 상기 복수 개의 소스 심볼 각각을 symbol-wise XOR하여, 상기 오류정정부호 및 상기 복수 개의 부호화된 심볼을 획득하는 단계;를 포함하고, 상기 오류정정부호는, 전송 채널에서 발생하는 전송 신호의 오류를 정정하는 기능을 제공할 수 있다.

[0024] 또한, 상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는 단계는, 상기 적어도 하나의 페이크 심볼 각각의 제 1 위치를 인식하는 단계; 상기 복수 개의 부호화된 심볼 중 상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼을 인식하는 단계; 및 상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각을 상기 적어도 하나의 페이크 심볼 각각으로 대체하는 단계;를 포함할 수 있다.

[0025] 또한, 상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경하는 단계는, 상기 적어도 하나의 페이크 심볼 각각의 제 1 위치를 인식하는 단계; 상기 복수 개의 부호화된 심볼 중 상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼을 인식하는 단계; 상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각과 상기 적어도 하나의 페이크 심볼 각각을 연산하는 단계; 및 상기 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각을 상기 연산 결과 값 각각으로 대체하는 단계;를 포함할 수 있다.

[0026] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 수신자 단말의 프로세서에 의해 수행되는 보안이 강화된 데이터 전송 방법이 개시된다. 상기 방법은: 디지털 채널(digital channel)을 통해 복수 개의 심볼 및 오류정정부호를 송신자 단말로부터 수신하는 단계; 상기 송신자 단말로부터 퀀텀 채널(quantum channel)을 통해 사전에 수신된 키 시퀀스 및 상기 복수 개의 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보를 생성하는 단계; 상기 제 1 정보 및 상기 제 2 정보에 기초하여, 상기 복수 개의 심볼 중에서 적어도 하나의 페이크 심볼을 제거하는 단계; 및 상기 복수 개의 심볼 중에서 상기 적어도 하나의 페이크 심볼이 제거된 나머지 심볼 및 상기 오류정정부호를 이용하여, 복호화된 심볼(decoded symbol)을 획득하는 단계;를 포함할 수 있다.

[0027] 또한, 상기 키 시퀀스는, 상기 송신자 단말에서 상기 수신자 단말로 랜덤 값이 상기 퀀텀 채널을 통해 전송되는 경우, 상기 랜덤 값을 기초로 생성될 수 있다.

[0028] 또한, 상기 송신자 단말로부터 퀀텀 채널(quantum channel)을 통해 사전에 수신된 키 시퀀스 및 상기 복수 개의 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 상기 페이크 심볼의 위치에 대한 제 2 정보

를 생성하는 단계는, 상기 키 시퀀스의 길이 및 상기 복수 개의 심볼의 개수를 제 1 수학식의 입력 값으로 하여, 상기 제 1 정보를 생성하는 단계; 및 상기 복수 개의 심볼의 개수를 제 2 수학식의 입력 값으로 하여, 상기 제 1 정보를 생성하는 단계;를 포함할 수 있다.

[0029] 또한, 상기 제 1 수학식은 $f = \left\lfloor \frac{len(key)}{\lceil \log_2 n \rceil} \right\rfloor$ 이고, 상기 f는 상기 페이크 심볼의 개수이고, 상기 len(key)는 상기 키 시퀀스의 길이이고, 상기 n은 상기 복수 개의 심볼의 개수일 수 있다.

[0030] 또한, 상기 제 2 수학식은 $p = \lceil \log_2 n \rceil$ 이고, 상기 p는 상기 페이크 심볼의 위치를 비트(bit)로 나타낸 값이고, 상기 n은 상기 복수 개의 심볼의 개수일 수 있다.

[0031] 또한, 상기 복수 개의 심볼 중에서 상기 적어도 하나의 페이크 심볼이 제거된 나머지 심볼 및 상기 오류정정부호를 이용하여, 복호화된 심볼을 획득하는 단계는, 상기 오류정정부호를 이용하여, 상기 적어도 하나의 페이크 심볼이 제거된 위치에 대응하는 심볼을 복원하는 단계; 및 복원된 심볼 및 상기 나머지 심볼을 복호화하여, 상기 복호화된 심볼을 획득하는 단계;를 포함할 수 있다.

[0032] 또한, 상기 복수 개의 심볼은, 복수 개의 부호화된 심볼(encoded symbol) 및 상기 적어도 하나의 페이크 심볼을 포함하고, 상기 복수 개의 부호화된 심볼은, 복수 개의 소스 심볼에 기초하여 생성된 적어도 하나의 CRC(Cyclic Redundancy Check) 심볼 및 상기 복수 개의 소스 심볼이 상기 송신자 단말에 의해 부호화된 심볼일 수 있다.

[0033] 또한, 상기 방법은, 상기 나머지 심볼을 복호화함에 따라, 상기 CRC 심볼을 포함하는 상기 복호화된 심볼을 획득한 경우, 상기 CRC 심볼을 이용하여 정상적으로 복호화 되었는지 여부를 인식하는 단계;를 더 포함할 수 있다.

[0034] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

발명의 효과

[0035] 본 개시는 양자키분배 프로토콜을 사용하여, 암호화된 정보에 대한 도청을 방지할 수 있다. 구체적으로, 도청자는 탈취한 데이터에 대하여 무차별 대입 방식(brute-force)으로만 복호화를 수행할 수 있다.

[0036] 한편, Shannon 이론에 따르면 메세지 길이만큼의 일회용 암호(one-time pad)를 사용하면 완벽한 보안을 달성할 수 있다. 종래 secure FEC 기법은 FEC 부/복호화에 사용하고자 하는 정보(예를 들어, 도 2에서의 reference database)를 암호화시키기 때문에 송신자가 전송하는 메세지 길이가 길어질수록 암호화 기법을 통해 전송되는 정보의 전송량이 증가하게 되어 보안성을 늘리는데 한계가 존재할 수 있다. 하지만, 본 개시는 erasure channel 특성을 반영한 분배된 key 이용 방식 이용하여 매우 적은 양의 random key를 전송하게 되어 보안성의 한계를 극복할 수 있다.

[0037] 구체적으로, QKD는 전송하고자 하는 정보를 양자 채널을 통해 직접적으로 전송하는 것이 아니라 random key를 전송하는 방식이다. 따라서, 종래 secure FEC 방식에서 숨기고자 하는 정보를 직접적으로 QKD를 통해 전송할 수 없다. 반면, 본 개시는 random key를 이용하여 secure FEC를 구성함으로써 QKD를 통한 보안성을 제공할 수 있다.

[0038] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0039] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 특정 세부사항들 없이 실시될 수 있음은 명백할 것이다. 다른 예시들에서, 공지의 구조들 및 장치들이 하나 이상의 양상들의 기재를 용이하게 하기 위해 블록도 형태로 도시된다.

도 1은 기존 LT code를 설명하기 위한 도면이다.

도 2는 기존 secure FEC 기법을 설명하기 위한 도면이다.

도 3은 본 개시의 몇몇 실시예에 따른 송신자 단말 및 수신자 단말의 블록 구성도이다.

도 4는 본 개시의 몇몇 실시예에 따른 보안이 강화된 데이터 전송 방법을 설명하기 위한 도면이다.

도 5는 본 개시의 몇몇 실시예에 따른 송신자 단말이 수행하는 보안이 강화된 데이터 전송 방법의 일례를 설명하기 위한 흐름도이다.

도 6은 본 개시의 몇몇 실시예에 따른 송신자 단말이 페이크 심볼 개수와 페이크 심볼의 위치를 설정하는 방법의 일례를 설명하기 위한 도면이다.

도 7은 본 개시의 몇몇 실시예에 따른 송신자 단말이 페이크 심볼을 이용하여 transmit symbol을 생성하는 방법의 일례를 설명하기 위한 도면이다.

도 8은 본 개시의 몇몇 실시예에 따른 도청자 단말이 페이크 심볼이 포함된 심볼을 복호화 하는 방법의 일례를 설명하기 위한 도면이다.

도 9는 본 개시의 몇몇 실시예에 따른 수신자 단말이 수행하는 보안이 강화된 데이터 전송 방법의 일례를 설명하기 위한 흐름도이다.

도 10은 본 개시의 추가적인 몇몇 실시예에 따른 보안이 강화된 데이터 전송 방법을 설명하기 위한 도면이다.

도 11은 함수 블록과 CRC 심볼을 연산하는 방법의 일례를 설명하기 위한 도면이다.

도 12 및 도 13은 본 개시의 보안이 강화된 데이터 전송 방법에 대한 시뮬레이션 결과를 설명하기 위한 도면이다.

도 14는 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0040] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

[0041] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.

[0042] 비록 제 1, 제 2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제 1 소자나 구성요소는 본 개시의 기술적 사상 내에서 제 2 소자나 구성요소 일 수도 있음은 물론이다.

[0043] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0044] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는

A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0045] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0046] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.

[0047] 어떤 구성 요소가 다른 구성 요소에 “연결되어” 있다거나 “접속되어” 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 “직접 연결되어” 있다거나 “직접 접속되어”있다고 언급된 때에는, 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0048] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 “모듈” 및 “부”는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0049] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로써 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.

[0050] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0052] 도 3은 본 개시의 몇몇 실시예에 따른 송신자 단말 및 수신자 단말의 블록 구성도이다.

[0053] 도 3을 참조하면, 송신자 단말(100)은 프로세서(110), 통신부(120) 및 메모리(130)를 포함할 수 있다. 다만, 상술한 구성 요소들은 송신자 단말(100)을 구현하는데 있어서 필수적인 것은 아니어서, 송신자 단말(100)은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0054] 송신자 단말(100)은 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0055] 송신자 단말(100)의 프로세서(110)는 통상적으로 송신자 단말(100)의 전반적인 동작을 제어한다. 프로세서(110)는 송신자 단말(100)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(130)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.

[0056] 또한, 프로세서(110)는 메모리(130)에 저장된 응용 프로그램을 구동하기 위하여, 송신자 단말(100)의 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 프로세서(110)는 상기 응용 프로그램의 구동을 위하여, 송신자 단말(100)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작시킬 수 있다.

[0057] 송신자 단말(100)의 통신부(120)는, 송신자 단말(100)과 수신자 단말(200) 사이의 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 또한, 상기 통신부(120)는, 송신자 단말(100)을 하나 이상의 네트워크에 연결하는 하나 이상의 모듈을 포함할 수 있다.

[0058] 송신자 단말(100)과 수신자 단말(200) 사이의 통신을 연결하는 네트워크는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크일 수 있다.

[0059] 본 개시의 실시예들에 따른 네트워크는 유선 및 무선 등과 같은 그 통신 양태를 가리지 않고 구성될 수 있으며, 단거리 통신망(LAN: Local Area Network), 원거리 통신망(WAN: Wide Area Network) 등 다양한 통신망으로 구성될 수 있다. 또한, 상기 네트워크는 공지의 월드와이드웹(WWW:World Wide Web)일 수 있으며, 적외선

(IrDA:Infrared Data Association) 또는 블루투스(Bluetooth)와 같이 단거리 통신에 이용되는 무선 전송 기술을 이용할 수도 있다.

[0060] 본 명세서에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 다른 네트워크들에서도 사용될 수 있다.

[0061] 송신자 단말(100)의 메모리(130)는 프로세서(110)의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들을 임시 또는 영구 저장할 수도 있다. 메모리(130)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적 어도 하나의 타입의 저장매체를 포함할 수 있다. 이러한 메모리(130)는 프로세서(110)에 제어에 의하여 동작 될 수 있다.

[0062] 본 개시의 몇몇 실시예에 따르면, 송신자 단말(100)의 프로세서(110)는 부호화된 특정 데이터 및 적어도 하나의 페이크 심볼을 수신자 단말(200)로 전송하도록 통신부(120)를 제어할 수 있다. 그리고, 송신자 단말(100)의 프로세서(110)는 QKD를 통해 페이크 심볼의 개수 및 위치에 대한 정보를 확인할 수 있는 정보를 전송하도록 통신부(120)를 제어할 수 있다.

[0063] 이 경우, 수신자 단말(200)은 페이크 심볼의 개수 및 위치에 대한 정보를 이용해 부호화된 특정 데이터를 복호화할 수 있다.

[0064] 반면, 도청자 단말(미도시)은 송신자 단말(100)에서 수신자 단말(200)로 전송된 부호화된 특정 데이터를 탈취하더라도, QKD를 통해 전송된 정보를 탈취할 수 없다.

[0065] 따라서, 도청자 단말은 페이크 심볼의 위치를 파악할 수 없어, 부호화된 특정 데이터의 복호화가 어려워 성능 열화를 발생될 수 있다.

[0066] 이하, 송신자 단말(100)이 수행하는 보안이 강화된 데이터 전송 방법에 대한 설명은 도 4 내지 도 7을 참조하여 후술한다.

[0067] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시예들은 별도의 소프트웨어 모듈들로 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 송신자 단말(100)의 메모리(130)에 저장되고, 송신자 단말(100)의 프로세서(110)에 의해 실행될 수 있다.

[0068] 수신자 단말(200)은 프로세서(210), 통신부(220) 및 메모리(230)를 포함할 수 있다. 다만, 상술한 구성 요소들은 수신자 단말(200)을 구현하는데 있어서 필수적인 것은 아니어서, 수신자 단말(200)은 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0069] 수신자 단말(200)은 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0070] 수신자 단말(200)의 프로세서(210)는 통상적으로 수신자 단말(200)의 전반적인 동작을 제어한다. 프로세서(210)는 수신자 단말(200)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(230)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.

[0071] 또한, 프로세서(210)는 메모리(230)에 저장된 응용 프로그램을 구동하기 위하여, 수신자 단말(200)의 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 프로세서(210)는 상기 응용 프로그램의 구동을 위하여, 수신자 단말(200)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작시킬 수 있다.

[0072] 수신자 단말(200)의 통신부(220)는, 수신자 단말(200)과 송신자 단말(100) 사이의 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 또한, 상기 통신부(220)는, 수신자 단말(200)을 하나 이상의 네트워크에 연결하는 하나 이상의 모듈을 포함할 수 있다.

[0073] 수신자 단말(200)과 수신자 단말(100) 사이의 통신을 연결하는 네트워크는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크일 수 있다.

[0074] 수신자 단말(200)의 메모리(230)는 프로세서(210)의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들을 임시 또는 영구 저장할 수도 있다. 메모리(230)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적 어도 하나의 타입의 저장매체를 포함할 수 있다. 이러한 메모리(230)는 프로세서(210)에 제어에 의하여 동작 될 수 있다.

[0075] 본 개시의 몇몇 실시예에 따르면, 수신자 단말(200)의 프로세서(210)는 통신부(220)를 통해 부호화된 특정 데이터 및 적어도 하나의 페이크 심볼을 송신자 단말(100)로부터 수신할 수 있다. 그리고, 수신자 단말(200)의 프로세서(210)는 QKD를 통해 페이크 심볼의 개수 및 위치에 대한 정보를 확인할 수 있는 정보를 수신할 수 있다.

[0076] 이 경우, 수신자 단말(200)의 프로세서는 페이크 심볼의 개수 및 위치에 대한 정보를 획득하고, 부호화된 특정 데이터에서 페이크 심볼을 제거한 후, 복호화를 수행할 수 있다.

[0077] 반면, 도청자 단말(미도시)은 부호화된 특정 데이터를 탈취하더라도, QKD를 통해 전송된 정보를 탈취할 수 없다. 따라서, 도청자 단말은 페이크 심볼의 위치를 파악할 수 없어, 부호화된 특정 데이터의 복호화가 어려워 성능 열화를 발생될 수 있다.

[0078] 이하, 수신자 단말(200)이 수행하는 보안이 강화된 데이터 전송 방법에 대한 설명은 도 4 및 도 8을 참조하여 후술한다.

[0079] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시예들은 별도의 소프트웨어 모듈들로 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 수신자 단말(200)의 메모리(230)에 저장되고, 수신자 단말(200)의 프로세서(210)에 의해 실행될 수 있다.

[0081] 도 4는 본 개시의 몇몇 실시예에 따른 보안이 강화된 데이터 전송 방법을 설명하기 위한 도면이다.

[0082] 본 개시의 보안이 강화된 데이터 전송 방법은 도 1에 도시된 LT code에 기반할 수 있다. 구체적으로, 본 개시의 보안이 강화된 데이터 전송 방법은 LT code에서 페이크 심볼(fake symbol)과 관련된 세부 과정들이 추가될 수 있다.

[0083] 여기서, 페이크 심볼은 도청자 단말(300)의 도청을 방해하기 위한 심볼일 수 있다. 본 개시의 보안이 강화된 데이터 전송 방법은 페이크 심볼의 위치를 QKD를 통해 전송된 random key를 이용하여 설정할 수 있다. 이 경우, 도청자 단말(300)은 페이크 심볼의 정확한 위치를 알 수 없게 된다.

[0084] 따라서, 본 개시의 보안이 강화된 데이터 전송 방법은 도청자 단말(300)이 정확하게 페이크 심볼을 제거하지 못하게 하여 LT 복호화에 의한 도청자 측의 성능 열화를 발생시킬 수 있다.

[0085] 도 4를 참조하면, 페이크 심볼 위치(Fake symbol positions, 301)는 random key를 통해 송신자 단말(100) 측에서 수신자 단말(200) 측으로 전송될 수 있다. 여기서, 송신자 단말(100)은 LT encoding 블록일 수 있다. 그리고, 수신자 단말(200)은 LT decoding 블록일 수 있다.

[0086] 본 개시의 몇몇 실시예에 따르면, QKD는 실제 퀀텀 채널(quantum channel)과 디지털 채널(digital channel)을 둘 다 사용한다. 특히, QKD는 디지털 채널을 통해 송신자 단말(100)과 수신자 단말(200)의 공통된 양자 정보를 추출하기 위해 polarizer 또는 basis를 전송하게 된다. 그러나, 도 4에서는 key가 도청당하지 않고 전송된다는 것을 표현하기 위해 간략하게 양자 채널(Quantum Ch.) 만을 통해 전송하는 것으로 도시하였다.

[0087] 오염된 임의의 값인 페이크 심볼(302)은 페이크 심볼 위치(301)에 해당하는 encoded symbol과 XOR 연산 될 수 있다. 다만, 이에 한정되는 것은 아니고, 페이크 심볼(302)은 페이크 심볼 위치(301)에 해당하는 부호화된 심볼(encoded symbol)의 자리에 대입될 수도 있다.

[0088] 즉, 송신자 단말(100)은 도청자 단말(300)의 도청을 방해하기 위해 부호화된 심볼에 페이크 심볼을 포함시킬 수 있다. 그리고, 송신자 단말(100)은 페이크 심볼이 포함된 부호화된 심볼에 대한 LT code 관련 정보를 수신자 단말(200)에게 전송할 수 있다.

[0089] 이하, 송신자 단말(100)이 LT code 관련 정보를 수신자 단말(200)에게 전송하는 방법에 대한 설명은 도 5 내지

도 7을 참조하여 후술한다.

[0090] 한편, 수신자 단말(200)은 LT code의 복호화를 위해 하위 layer에서의 CRC check를 통해 파악된 erased symbol 뿐만 아니라 페이크 심볼 위치에 해당하는 심볼을 erased symbol로 파악할 수 있다. 즉, 수신자 단말(200)은 LT code에서 페이크 심볼을 제거할 수 있다. 여기서, 페이크 심볼은 수신자 단말(200)에 의해 제거되기 때문에 송신자 단말(100)이 수행한 페이크 심볼과 부호화된 심볼과의 연산 또는 대체 등은 중요한 요소가 아닐 수 있다.

[0091] 수신자 단말(200)은 erased symbol을 제외한 나머지 수신 심볼을 복호화에 사용하기 위해 준비(311)할 수 있다.

[0092] 다음으로, 수신자 단말(200)은 erased symbol을 제외한 나머지 수신 심볼을 이용하여 복호화(312)를 수행할 수 있다. 그리고, 수신자 단말(200)은 CRC Check(313)를 수행하여, 복호화의 성공 여부를 판단할 수 있다. 최종적으로, 수신자 단말(200)이 수행한 CRC Check(313)의 결과에 이상이 없으면(즉, 복호화가 성공했다고 판단한 경우), 성공적인 source symbol 전송이 이루어진 것으로 판단할 수 있다.

[0093] 이하, 수신자 단말(200)이 LT code 관련 정보를 송신자 단말(100)로부터 수신하는 방법에 대한 설명은 도 8을 참조하여 후술한다.

[0094] 한편, 도청자 단말(300)은 LT code의 복호화를 위해 하위 layer에서의 CRC check를 통해 파악된 erased symbol을 파악할 수 있다. 도청자 단말(300)은 페이크 심볼을 사용함을 알게 된 경우, 페이크 심볼이 있을 만한 위치를 erased symbol로 파악할 수 있다. 즉, 도청자 단말(300)은 페이크 심볼의 위치를 정확하게 알 수 없기 때문에, 페이크 심볼의 위치를 임의로 예측할 수밖에 없다. 그리고, 도청자 단말(300)은 임의로 예측한 페이크 심볼을 erased symbol로 파악할 수 있다.

[0095] 다음으로, 도청자 단말(300)은 erased symbol을 제외한 나머지 수신 심볼을 이용하여 복호화(322)를 수행할 수 있다. 그리고, 도청자 단말(300)은 CRC Check(323)를 수행하여, 복호화의 성공 여부를 판단할 수 있다.

[0096] 도청자 단말(300)은 복호화에 실패했다고 판단한 경우, 페이크 심볼 다른 위치를 예측하고, erased symbol로 파악한 뒤, 나머지 수신 심볼을 이용하여, 복호화(322) 및 CRC Check(323)하는 과정을 반복할 수 있다.

[0097] 즉, 도청자 단말(300)은 페이크 심볼의 위치가 정확하게 일치할 때까지 상술한 과정들을 반복해야하기 때문에 성능 열화가 발생할 수 있다. 또한, 도청자 단말(300)은 성능 열화로 인해 페이크 심볼의 위치를 찾는 것이 사실상 불가능할 수 있다.

[0098] 따라서, 본 개시의 보안이 강화된 데이터 전송 방법은 도청자로부터 완벽 보안을 기대할 수 있다.

[0100] 도 5는 본 개시의 몇몇 실시예에 따른 송신자 단말이 수행하는 보안이 강화된 데이터 전송 방법의 일례를 설명하기 위한 흐름도이다. 도 6은 본 개시의 몇몇 실시예에 따른 송신자 단말이 페이크 심볼 개수와 페이크 심볼의 위치를 설정하는 방법의 일례를 설명하기 위한 도면이다. 도 7은 본 개시의 몇몇 실시예에 따른 송신자 단말이 페이크 심볼을 이용하여 transmit symbol을 생성하는 방법의 일례를 설명하기 위한 도면이다. 도 8은 본 개시의 몇몇 실시예에 따른 도청자 단말이 페이크 심볼이 포함된 심볼을 복호화 하는 방법의 일례를 설명하기 위한 도면이다.

[0101] 먼저, 도 5를 참조하면, 송신자 단말(100)의 프로세서(110)는 페이크 심볼의 개수에 대한 제 1 정보 및 페이크 심볼의 위치에 대한 제 2 정보를 생성할 수 있다(S110).

[0102] 구체적으로, 송신자 단말(100)의 프로세서(110)는 퀀텀 채널(quantum channel)을 통해 수신자 단말로 전송된 키 시퀀스(key sequence) 및 전송할 심볼의 개수를 이용하여, 제 1 정보 및 제 2 정보를 생성할 수 있다. 여기서, 키 시퀀스는 송신자 단말(100)에서 수신자 단말(200)로 랜덤 값이 퀀텀 채널을 통해 전송되는 경우, 랜덤 값을 기초로 생성될 수 있다. 다만, 이에 한정되는 것은 아니다.

[0103] 좀더 구체적으로, 송신자 단말(100)의 프로세서(110)는 키 시퀀스의 길이 및 전송할 심볼의 개수를 제 1 수학식(수학식 1)의 입력 값으로 하여, 제 1 정보를 생성할 수 있다.

수학식 1

[0104] $$f = \left\lfloor \frac{len(key)}{\lceil \log_2 n \rceil} \right\rfloor$$

[0105] 여기서, f는 상기 페이크 심볼의 개수이고, len(key)는 키 시퀀스의 길이이고, n은 전송할 심볼의 개수를 의미할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0106] 한편, 송신자 단말(100)의 프로세서(110)는 전송할 심볼의 개수를 제 2 수학식(수학식 2)의 입력 값으로 하여, 제 2 정보를 생성할 수 있다.

수학식 2

[0108] $$p = \lceil \log_2 n \rceil$$

[0109] 여기서, p는 페이크 심볼의 위치를 비트(bit)로 나타낸 값이고, n은 전송할 심볼의 개수를 의미할 수 있다. 추가적으로, p는 심볼이 지워지는 위치(erasure position)를 bit로 나타낸 값일 수도 있다. 즉, 키 시퀀스는 p단위로 나눠질 수 있다. 그리고, 지워지는 위치가 n보다 크다면 modulo-n 연산을 통해 n보다 작게 설정될 수 있다.

[0110] 자세히 예를 들어, 도 6을 참조하면, n=1000, len(key)=32인 경우 키 시퀀스의 일부를 버려서 f=3이 되고, 각 erasure position은 125, 23, 5가 될 수 있다. 여기서, 23은 $\lceil \log_2 n \rceil$ 표현으로는 1023이지만 n=1000보다 크기 때문에 modulo-1000 연산을 통해 생성된 값일 수 있다.

[0111] 따라서, 송신자 단말(100)과 수신자 단말(200) 각각은 한번의 키 분배를 통해 생성된 erasure position이 송신자와 수신자 각각이 미리 설정한 최소 f값(fmin) 또는, 최대 f값(fmax)보다 크다면 erasure position을 분리하여 여러 번의 source blocks 전송에 사용할 수 있다.

[0112] 예를 들어, f=17이고, fmax=5로 설정한 경우 하나의 키 시퀀스를 분해하여 i-번째 source block에 사용하려면, 수학식 3을 통해 f1=4, f2=4, f3=4, f4=5으로 나눌 수 있다.

수학식 3

$$m = \left\lfloor \frac{f}{f_{max}} \right\rfloor$$

$$f_i = f_{max}, \; i = 1, \ldots, m$$

[0114] $$if \;\; m * f_{max} \; != f, then \;\; f_i = f_i \; - 1, \qquad i = 1, \ldots, m * f_{max} - f,$$

[0115] 여기서, fi는 i-번째 source block에 사용하는 fake symbol의 개수를 의미한다.

[0116] 다른 예를 들어, f=17이고, fmin=3로 설정한 경우, 수학식 4를 통해 f1=4, f2=4, f3=3, f4=3, f5=3으로 나눌 수 있다.

수학식 4

$$m = \left\lfloor \frac{f}{f_{min}} \right\rfloor$$

$$f_i = f_{min}, \; i = 1, \ldots, m$$

[0118] $$if \;\; m * f_{min} \; != f, then \;\; f_i = f_i \; + 1, \qquad i = 1, \ldots, f - m * f_{min},$$

[0119] 여기서, 상기 fi는 i-번째 source block에 사용하는 fake symbol의 개수를 의미한다.

[0120] 본 개시의 몇몇 실시예에 따르면, f-value(fmax 및 fmin)의 범위는 도청자의 erasure position의 추정 복잡도

와 fake symbol 개수에 따른 Block Error Rate(BLER), QKD 전송률을 고려하여 정해질 수 있다.

[0121] 본 개시의 몇몇 실시예에 따르면, QKD의 전송 주기인 Tp는 수학식 5를 이용하여 결정할 수 있다.

수학식 5

[0123] $$Tp = \frac{Z*8*Y/X}{f*\lceil \log_2 n \rceil}$$

[0124] 디지털 채널과 퀀텀 채널을 통한 전송률이 각각 X Mbps, Y Mbps이고, source block 크기는 Z MB, symbol 개수는 n, fake symbol 개수는 f인 경우, Z MB를 디지털 채널을 통해 전송하는데 필요한 시간은 Z*8/1024 (s)가 필요하다. 동일시간 동안 퀀텀 채널을 통해서는 Z*8*Y/X (Mbit)를 전송할 수 있다. 페이크 심볼의 위치는 $\lceil \log_2 n \rceil$ bit로 표현 가능하므로 다음과 같은 전송 주기 Tp를 갖는다.

수학식 6

[0126] $$Tp = \frac{80K}{5*10} = 1,600$$

[0127] 예를 들어, 수학식 6를 참조하면, 디지털 채널을 Tb번 사용 시 퀀텀 채널을 1번만 사용하면 된다. 예를 들어, X=1000, Y=10, Z=1, n=1024, f=5인 경우 퀀텀 채널을 통해 80Kbit를 전송할 수 있으므로 디지털 채널 1600번 사용 시 퀀텀 채널 1번을 사용하면 된다.

[0128] 즉, QKD 전송 속도가 digital 대비 느리더라도 페이크 심볼 위치를 표현하는 bit 길이가 길지 않을 뿐만 아니라, 후술될 도 12 및 도 13의 성능 그래프에서 볼 수 있듯이 security를 위한 페이크 심볼의 개수가 크지 않기 때문에 QKD를 통한 key를 페이크 심볼 위치로 충분히 사용할 수 있다.

[0129] 송신자 단말(100)과 수신자 단말(200)은 상기에서의 페이크 심볼 위치를 복잡한 암호화 기법을 사용하지 않고 secure random key를 이용하여 쉽게 알 수 있다. 반면, 도청자 단말(300)은 페이크 심볼 위치를 모르기 때문에, 임의의 심볼을 지운 후 복호화(decoding)를 수행하는 것을 복호화가 성공할 때까지 반복해야 한다. 여기서, 도청자는 복호화의 성공/실패 여부는 CRC를 통해 알 수 있다.

[0130] 설명의 편의를 위해, 도청자가 모든 페이크 심볼을 지웠을 경우에 복호화가 성공하는 것으로 가정하고, 이하 설명한다.

[0131] 도청자는, 전송 심볼의 개수가 n이고, 페이크 심볼의 개수가 f일 경우, 최대 $\sum_{i=1}^{f}\binom{n}{i}$번의 심볼을 지운 후 복호화를 수행해야 한다. 예를 들어, n=1000 (information symbol size k=500, code rate=0.5), f=3인 경우, decoding은 최대 1000+499,500+166,167,000=166,667,500번을 수행해야 한다. 만약 복호화 1회 당 수행시간이 1ms이 소요된다면 총 46시간의 복호화 시간이 필요하게 된다. 도청자 단말(300)은 심볼을 independently and identically distributed(i.i.d.)로 지우기 때문에 복호화의 평균 수행 횟수는 최대 수행 횟수의 절반이 될 수 있다.

[0132] 표 1은 n과 f에 따른 최대 decoding 수행 횟수를 나타낸다. 일반적으로 n이 커지면 복호화 소요시간이 증가하지만 본 개시에서는 비교의 편의를 위해 복호화 1회 시도 당 소요 시간이 1ms인 복호화기(decoder) 사용을 가정한다. 마지막 열은 최대 복호화 수행 횟수 대비 도청자가 정확한 f 값을 알았을 때의 복호화 수행 횟수의 비를 나타낸다.

표 1

[0133]

	number of decoding	processing time (hour)	$\frac{\binom{n}{f}}{\sum_{i=1}^{f}\binom{n}{i}}$
n=500, f=3	2.1×10^{7}	5.8	99.4%
n=500, f=4	2.6×10^{9}	720.5	99.2%
n=500, f=5	2.6×10^{11}	7.2×10^{4}	99.0%
n=1000, f=3	1.7×10^{7}	46.3	99.7%
n=1000, f=4	4.2×10^{10}	1.2×10^{4}	99.6%
n=1000, f=5	8.3×10^{12}	2.3×10^{6}	99.5%
n=2000, f=3	1.3×10^{9}	370.4	99.8%
n=2000, f=4	6.7×10^{11}	1.9×10^{5}	99.8%
n=2000, f=5	2.7×10^{14}	7.4×10^{7}	99.7%

[0134] 표 1에서는 n과 f가 커질수록 복호화 수행 횟수가 지수적으로 증가한다. 특히, f값에 매우 민감하게 증가하는 것을 확인할 수 있다. 따라서, 송신자 단말(100)은 도청자 단말(300)의 복잡도를 높이기 위해 symbol dimension을 조정하여 n을 증가시키거나, 페이크 심볼 위치가 공유되는 횟수를 증가시킴으로써 f를 증가시킬 수 있다. 예를 들어, 송신자 단말(100)은 소스 데이터 블록의 길이가 1MB인 경우, 각각의 심볼 크기가 1KB 인 1024개의 심볼을 사용되거나, 또는 n을 증가시키기 위해 4096개의 256B 심볼을 사용할 수 있다.

[0135] 도청자 단말(300)은 n이 f에 비해 매우 큰 경우, 정확한 f 값을 알더라도, 정확한 페이크 심볼 위치를 모르기 때문에, 전체 복호화 소요시간의 99%이상을 차지하게 된다. 따라서, 도청자 단말(300)에게 f 값이 노출되더라도 전체 복호화 소요시간에는 거의 변화가 없게 된다. 또한, 도청자가 f값을 모르는 경우에는, 도청자가 추정하는 f가 실제 f보다 크게 심볼을 지우는 경우, 즉 over-erasure 상황에서는 복호화 시도 횟수가 지수적으로 증가하기 때문에 도청자는 실제 f보다 작은 값을 가정하고 복호화를 수행할 수 있다. 그러나, 이 경우에도 f가 가장 큰 경우가 99%이상의 decoding 소요시간을 차지하기 때문에 전체적인 복호화 소요시간에는 거의 변화가 없게 된다.

[0136] 즉, 본 개시의 송신자 단말(100)의 프로세서(110)는 수신자 단말(200)과 공유된 몇몇 값들 및 상술한 예시들과 같은 특정 수학식을 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 페이크 심볼의 위치에 대한 제 2 정보를 생성할 수 있다. 여기서, 수신자 단말(200)과 공유된 몇몇 값(예컨대, 키 시퀀스의 길이 등)은 퀀텀 채널을 통해 전송됨에 따라 생성되기 때문에, 도청자 단말(300)이 알아낼 수 없는 정보이다.

[0137] 따라서, 본 개시의 송신자 단말(100)의 프로세서(110)는 도청자 단말(300)이 알아낼 수 없는 정보를 이용하여 페이크 심볼의 개수 및 위치를 설정하여, 도청자 단말(300)이 페이크 심볼의 개수 및 위치를 알아내는 것을 막고, 정상적인 복호화를 어렵게 할 수 있다.

[0138] 다시 도 5를 참조하면, 송신자 단말(100)의 프로세서(110)는 제 1 정보 및 제 2 정보를 생성한 후, 복수 개의 소스 심볼을 부호화하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득할 수 있다(S120).

[0139] 구체적으로, 송신자 단말(100)의 프로세서(110)는 복수 개의 소스 심볼 각각을 symbol-wise XOR하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득할 수 있다. 여기서, 오류정정부호는 전송 채널에서 발생하는 전송 신호의 오류를 정정하는 기능을 제공할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0140] 본 개시의 추가적인 몇몇 실시예에 따르면, 송신자 단말(100)의 프로세서(110)는 오류정정부호 및 복수 개의 부

호화된 심볼을 획득하기 이전에, 복수 개의 소스 심볼에 기초하여, 적어도 하나의 CRC(Cyclic Redundancy Check) 심볼을 생성할 수 있다. 그리고, 프로세서(110)는 복수 개의 소스 심볼 및 CRC 심볼을 부호화 하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득할 수 있다. 여기서, CRC 심볼은 수신자 단말(200)에서 복호화를 수행한 후, 복호화가 정상적으로 수행되었는지 확인하는데 이용될 수 있다. 다만, 이에 한정되는 것은 아니다.

[0141] 본 개시의 몇몇 실시예에 따르면, 송신자 단말(100)의 프로세서(110)는 오류정정부호 및 부호화된 심볼을 획득한 후, 제 1 정보 및 제 2 정보에 기초하여, 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경할 수 있다(S130).

[0142] 일례로, 프로세서(110)는 적어도 하나의 페이크 심볼 각각의 제 1 위치를 인식할 수 있다. 또한, 프로세서(110)는 복수 개의 부호화된 심볼 중 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼을 인식할 수 있다. 또한, 프로세서(110)는 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각과 적어도 하나의 페이크 심볼 각각을 연산(예컨대, XOR 연산)할 수 있다. 그리고, 프로세서(110)는 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각을 연산 결과 값(예컨대, XOR 연산 결과 값) 각각으로 대체할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0143] 다른 일례로, 프로세서(110)는 제 1 정보를 이용하여, 적어도 하나의 페이크 심볼 각각의 제 1 위치를 인식할 수 있다. 또한, 프로세서(110)는 복수 개의 부호화된 심볼 중 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼을 인식할 수 있다. 그리고, 프로세서(110)는 제 1 위치에 대응하는 적어도 하나의 부호화된 심볼 각각을 적어도 하나의 페이크 심볼 각각으로 대체할 수 있다.

[0144] 예를 들어, 도 7를 참조하면, 원형 도형 각각은 소스 심볼(또는, 입력 심볼(input symbol))을 나타낸다. 사각형 도형 각각은 부호화된 심볼을 나타낸다. 그리고, 원형 도형 및 사각형 도형 각각을 연결한 선은 부호화된 심볼을 생성하기 위해 사용된 소스 심볼을 나타낸다.

[0145] 구체적으로, 송신자 단말(100)의 프로세서(110)는 소스 심볼들을 XOR 연산하여 부호화된 심볼을 생성할 수 있다. 즉, 부호화된 심볼 값은 소스 심볼 값을 symbol-wise XOR를 수행한 값일 수 있다. 그리고, 프로세서(110)는 페이크 심볼 위치의 심볼 값을 페이크 심볼로 대체할 수 있다. 예를 들어, 도 4에 도시된 바와 같이, 송신자 단말(100)의 프로세서(110)는 페이크 심볼 위치가 3인 경우, 3번째 위치한 심볼 값을 페이크 심볼 값인 16으로 대체하여, 수신자 단말(200)로 전송할 전송 심볼(transmit symbol)을 구성할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0146] 한편, 도 8을 참조하면, 도청자 단말(300)은 전송 심볼을 도청하여, 복호화를 수행할 수 있다. 구체적으로, 도청자 단말(300)은 MP(message passing) 복호화 기법을 이용하여, 도청한 심볼을 복호화 할 수 있다.

[0147] 구체적으로, 도청자 단말(300)은 MP 복호화 기법을 통해, 연결된 선이 하나인 수신된 심볼(received symbol) 노드에 연결된 복호화된 심볼 값에 수신된 심볼 값을 복사(여기서, 16)한 후 해당 선을 지울 수 있다. 또한, 도청자 단말(300)은 해당 node에 연결된 수신된 심볼 노드의 symbol 값에 copy한 값을 XOR한 후 해당 선을 지울 수 있다. 그리고, 도청자는 연결된 선이 하나인 수신된 심볼 노드를 찾아 복호화된 심볼 값이 모두 결정될 때까지 반복할 수 있다.

[0148] 즉, 연결된 선이 하나인 received symbol 값은 페이크 심볼이고, 페이크 심볼이 복호화된 심볼 값에 복사됨으로, 다음 과정들이 무의미해지며, 복호화는 성공할 수 없다. 또한, 상술한 과정들이 반복되어 도청자 측의 성능 열화가 발생될 수 있다.

[0149] 다시 도 5를 참조하면, 송신자 단말(100)의 프로세서(110)는 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경한 경우, 적어도 하나의 페이크 심볼, 복수 개의 부호화된 심볼 중 적어도 하나의 페이크 심볼로 변경되지 않은 나머지 심볼 및 오류정정부호를 디지털 채널을 통해 수신자 단말로 전송하도록 통신부(120)를 제어할 수 있다(S140).

[0150] 즉, 본 개시의 송신자 단말(100)의 프로세서(110)는 부호화된 심볼 중 일부를 페이크 심볼로 변경한 후, 이를 전송하기 때문에 데이터 전송의 보안성을 높일 수 있다.

[0152] 도 9는 본 개시의 몇몇 실시예에 따른 수신자 단말이 수행하는 보안이 강화된 데이터 전송 방법의 일례를 설명하기 위한 흐름도이다.

[0153] 도 9를 참조하면, 수신자 단말(200)의 프로세서(210)는 디지털 채널을 통해 복수 개의 심볼 및 오류정정부호를

송신자 단말(100)로부터 수신할 수 있다(S210).

[0154] 이 경우, 프로세서(210)는 송신자 단말(100)로부터 퀀텀 채널을 통해 사전에 수신된 키 시퀀스 및 복수 개의 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 페이크 심볼의 위치에 대한 제 2 정보를 생성할 수 있다(S220).

[0155] 여기서, 제 1 정보 및 제 2 정보를 생성하는 방법은 송신자 단말(100)과 동일한 방법을 통해 생성할 수 있다. 이에 대한 설명은 도 5 내지 도 7을 참조하여 자세히 설명한 바, 구체적인 설명은 생략한다.

[0156] 한편, 수신자 단말(200)의 프로세서(210)는 제 1 정보 및 제 2 정보를 생성한 후, 제 1 정보 및 제 2 정보에 기초하여, 복수 개의 심볼 중에서 적어도 하나의 페이크 심볼을 제거할 수 있다(S230).

[0157] 그리고, 수신자 단말(200)의 프로세서(210)는 복수 개의 심볼 중에서 상기 적어도 하나의 페이크 심볼이 제거된 나머지 심볼 및 상기 오류정정부호를 이용하여, 복호화된 심볼(decoded symbol)을 획득할 수 있다(S240).

[0158] 구체적으로, 프로세서(210)는 오류정정부호를 이용하여, 적어도 하나의 페이크 심볼이 제거된 위치에 대응하는 심볼을 복원할 수 있다. 그리고, 프로세서(210)는 복원된 심볼 및 나머지 심볼을 복호화하여, 복호화된 심볼을 획득할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0159] 본 개시의 추가적인 몇몇 실시예에 따르면, 수신자 단말(200)로 수신된 복수 개의 심볼은 복수 개의 부호화된 심볼 및 상기 적어도 하나의 페이크 심볼을 포함할 수 있다. 그리고, 복수 개의 부호화된 심볼은 복수 개의 소스 심볼에 기초하여 생성된 적어도 하나의 CRC(Cyclic Redundancy Check) 심볼 및 복수 개의 소스 심볼이 송신자 단말(100)에 의해 부호화된 심볼일 수 있다.

[0160] 이 경우, 수신자 단말(200)의 프로세서(210)는 나머지 심볼을 복호화함에 따라, CRC 심볼을 포함하는 복호화된 심볼을 획득할 수 있다. 그리고, 프로세서(210)는 CRC 심볼을 이용하여 정상적으로 복호화 되었는지 여부를 인식할 수 있다.

[0162] 도 10은 본 개시의 추가적인 몇몇 실시예에 따른 보안이 강화된 데이터 전송 방법을 설명하기 위한 도면이다. 도 11은 함수 블록과 CRC 심볼을 연산하는 방법의 일례를 설명하기 위한 도면이다.

[0163] 도 10의 설명에서는 도 3을 참조하여 설명한 보안이 강화된 데이터 전송 방법에서 추가적으로 random key를 이용하여 보안성을 더욱 높이는 방법을 설명한다.

[0164] 본 개시의 보안이 강화된 데이터 전송 방법에서 사용하는 QKD는 직접적으로 정보를 전송하는 protocol이 아니다. 따라서, 본 개시의 보안 오류정정부호를 처리하기 위한 방법은 random key를 Random Number Generator(RNG) 또는, Hash 함수와 같은 함수의 seed value를 이용한다. 즉, 본 개시의 보안 오류정정부호를 처리하기 위한 방법은 random key를 이용하여 seed value를 계속 변경하여 예측불가능하고 패턴이 불규칙한 random number를 만들고, 이를 이용한다.

[0165] 도 10을 참조하면, 송신자 단말(100)은 소스 심볼(source symbol)을 기반으로 CRC를 생성하여 소스 심볼에 추가(901)할 수 있다. 그리고, 송신자 단말(100)은 함수 블록(Func. Block, 902)을 이용하여, RNG 또는 Hash 함수와 같은 임의의 함수 값을 생성할 수 있다. 여기서, 함수 블록(902)은 random key를 기반으로 출력된 함수 값(fv)이 예측이 불가능 하거나 패턴이 불규칙한 특징을 만족하는 함수를 의미할 수 있다.

[0166] 한편, 송신자 단말(100)은 함수 블록(902)에서 생성된 fv와 CRC가 추가된 소스 심볼의 심볼열을 symbol-wise XOR 또는 convolution을 통해 두 개의 시퀀스(sequence)를 연산하여 새로운 시퀀스를 만드는 과정을 통해 부호화의 입력으로 사용할 수 있다.

[0167] 예를 들어, 길이가 동일한 시퀀스에 대한 symbol-wise XOR 연산을 위해 함수 블록(902)에서 $\text{modulo} - 2^{\text{len(CRC)}}$ 을 통해 fv를 생성할 수 있다. 여기서, len(CRC)는 CRC 심볼*심볼의 차원(dimension)을 나타낸다.

[0168] 한편, 수신자 단말(200)은 송신자 단말(100)의 함수 블록(902)과 동일한 함수 블록(911)을 가질 수 있다. 그리고, 수신자는 QKD를 통해 송신자로부터 공유받은 랜덤 시퀀스를 함수 블록(911)의 시드 값(seed value)으로 사용할 수 있다. 그리고, 수신자 단말(200)은 함수 블록(911)에서 출력되는 함수 값과 복호화된 값을 이용하여 CRC Check(912)를 수행할 수 있다.

[0169] 다른 한편, 도청자 단말(300)은 도청한 심볼을 복호화할 수 있다. 그리고, 도청자 단말(300)은 복호화된 값에 대하여 CRC Check(921)를 수행하여, 복호화의 성공 여부를 판단할 수 있다. 하지만, 도청자 단말(300)은 함수

블록(902 또는 911)에서 생성된 함수 값(fv)을 알 수 없기 때문에 정상적인 CRC Check(921)를 수행할 수 없다. 즉, 도청자는 CRC 심볼이 오염된 것과 동일하게 되어, CRC 심볼을 통한 복호화 성공 여부 확인이 불가능하게 된다.

[0170] 도 10을 참조하면, len(CRC)=12, CRC value=3458, pseudo RNG의 output value=6100인 경우를 가정하면, fv=2004가 되고 이를 CRC symbol과 연산하는 과정의 예시를 도시하였다.

[0171] 먼저, Shannon 이론에 따르면 message 길이와 random key 길이가 같은 경우 완벽 보안이 가능하게 된다.

[0172] message인 CRC 심볼과 랜덤 키(random key)인 fv의 길이가 같은 것을 예시하였다. 이 경우, 페이크 심볼과 CRC 심볼의 오염 기법을 동시에 사용하면 도청자는 $\binom{n}{f} * 2^{len(CRC)}$ 번의 복호화를 수행해야 한다.

[0173] 즉, 도청자 단말(200)이 복호화를 수행하는 것은 사실상 불가능에 가까울 수 있다.

[0175] 도 12 및 도 13은 본 개시의 보안이 강화된 데이터 전송 방법에 대한 시뮬레이션 결과를 설명하기 위한 도면이다.

[0176] 도 12 및 도 13은, LT code 기반의 secure FEC를 사용하는 기법에 대해 source data에 대한 수신자 단말(200)과 도청자 단말(300)의 Block Error Rate(BLER)을 나타낸다.

[0177] 시뮬레이션 환경은 다음과 같다. LT code의 parameter로써, delta=0.2, constant value=0.05인 RSD distribution을 사용하고, source data의 크기 (=source symbol 개수 x symbol dimension)는 500Kbit, source symbol 개수 k=250, 500, 1000, 그리고 code rate=1/2을 사용한다. LT decoding을 MP decoding 기법을 사용한다.

[0178] 구체적으로, 도 12는 페이크 심볼 비율에 따른 수신자 단말(200)과 도청자 단말(300)의 BLER에 대한 그래프이다. 그리고, 그래프 상에서 수신자 단말(200)은 Bob으로 기재하고, 도청자 단말(300)은 Eve로 기재하였다.

[0179] 좀더 구체적으로, 도 12에서는 k=500일 때의 erasure rate에 따른 BLER을 나타낸다. f=0은 본 개시의 보안이 강화된 데이터 전송 방법을 사용하지 않는 것을 나타내고 나머지는 부호화된 심볼 대비 페이크 심볼의 비율을 나타낸다. 예를 들어, f_0.01은 페이크 심볼 비율이 1%인 것을 나타낸다. 수신자 단말(200)은 정확하게 페이크 심볼을 제거하기 때문에 페이크 심볼을 사용하지 않는 경우와 비교하여 1% 만큼의 심볼이 덜 수신된 효과와 동일하게 되어 약간의 성능 저하가 발생하게 된다.

[0180] 그러나, 도청자 단말(300)은 페이크 심볼 비율이 0.5%인 f_0.005의 경우에 복호화가 성공되는 것은 거의 없는 것으로 나타난다.

[0181] 한편, 도 13은 동일한 개수의 페이크 심볼에 대해 k에 따른 도청자의 BLER에 대한 그래프이다.

[0182] 좀더 구체적으로, 도 13을 참조하면, 페이크 심볼을 사용하지 않는 경우, 일반적으로 알려진대로 코드 길이, 즉 k가 클수록 성능이 좋아지게 된다. 그러나, 페이크 심볼을 사용하면 code 길이보다 페이크 심볼의 개수에 따라 성능이 결정됨을 알 수 있다.

[0183] 즉, 도청자 단말(300)의 복호화를 막기위해서는 k(심볼의 개수)보다 f(페이크 심볼의 개수)가 더 중요한 것을 파악할 수 있다.

[0184] 예를 들어, 도시된 바와 같이 f가 5인 경우, BLER은 1에 상당히 근접하여, 도청자 단말(300)이 사실상 복호화를 수행하지 못하는 것을 확인할 수 있다.다만, 이에 한정되는 것은 아니다.

[0186] 도 14는 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도를 도시한다.

[0187] 본 개시내용이 일반적으로 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어와 관련하여 전술되었지만, 당업자라면 본 개시내용 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로서 구현될 수 있다는 것을 잘 알 것이다.

[0188] 일반적으로, 본 명세서에서의 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로시져, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된

장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.

[0189] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘다에 위치할 수 있다.

[0190] 컴퓨터는 통상적으로 다양한컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체 로서, 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다.

[0191] 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는 데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.

[0192] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.

[0193] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.

[0194] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇 가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.

[0195] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)-이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 섀시(도시 생략) 내에서 외장형 용도로 구성될 수 있음-, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 예를 들어, USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘 다를 포함한다.

[0196] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 저장 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 집 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 저장 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터

실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.

[0197] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.

[0198] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.

[0199] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.

[0200] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 서버 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원거리 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.

[0201] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 서버에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0202] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순하게 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0203] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a,b,g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5 GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

[0204] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 "소프트웨어"로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될

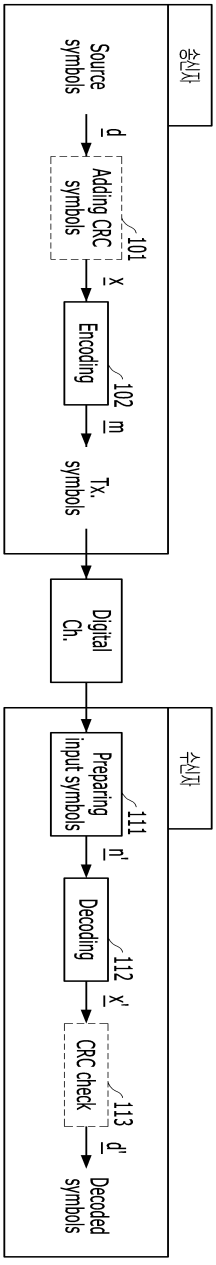
수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

[0205] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조 물품(article)으로 구현될 수 있다. 용어 "제조 물품"은 임의의 컴퓨터-판독가능 장치로부터 액세스 가능한 컴퓨터 프로그램 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장 매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트립, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 용어 "기계-판독가능 매체"는 명령(들) 및/또는 데이터를 저장, 보유, 및/또는 전달할 수 있는 무선 채널 및 다양한 다른 매체를 포함하지만, 이들로 제한되는 것은 아니다.

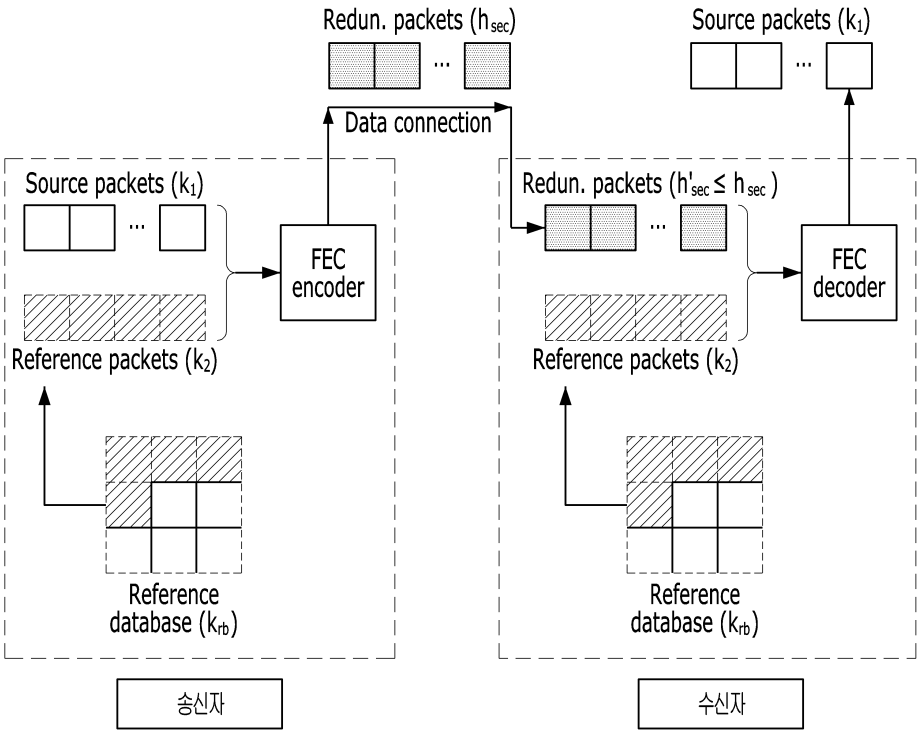
[0207] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

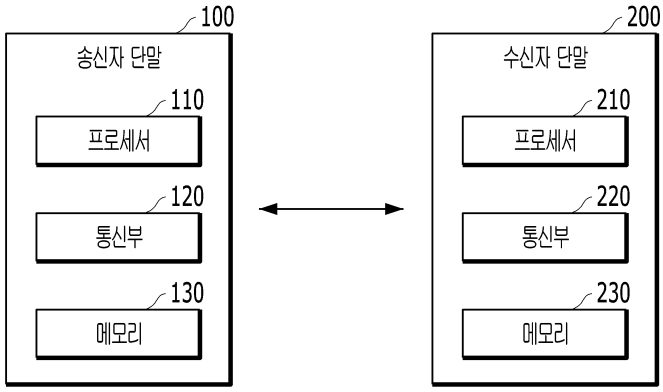
도면1


송신자
Source symbols
d
Adding CRC symbols
101
x
Encoding
102
m
Tx. symbols
Digital Ch.
수신자
Preparing input symbols
111
n'
Decoding
112
x'
CRC check
113
d'
Decoded symbols

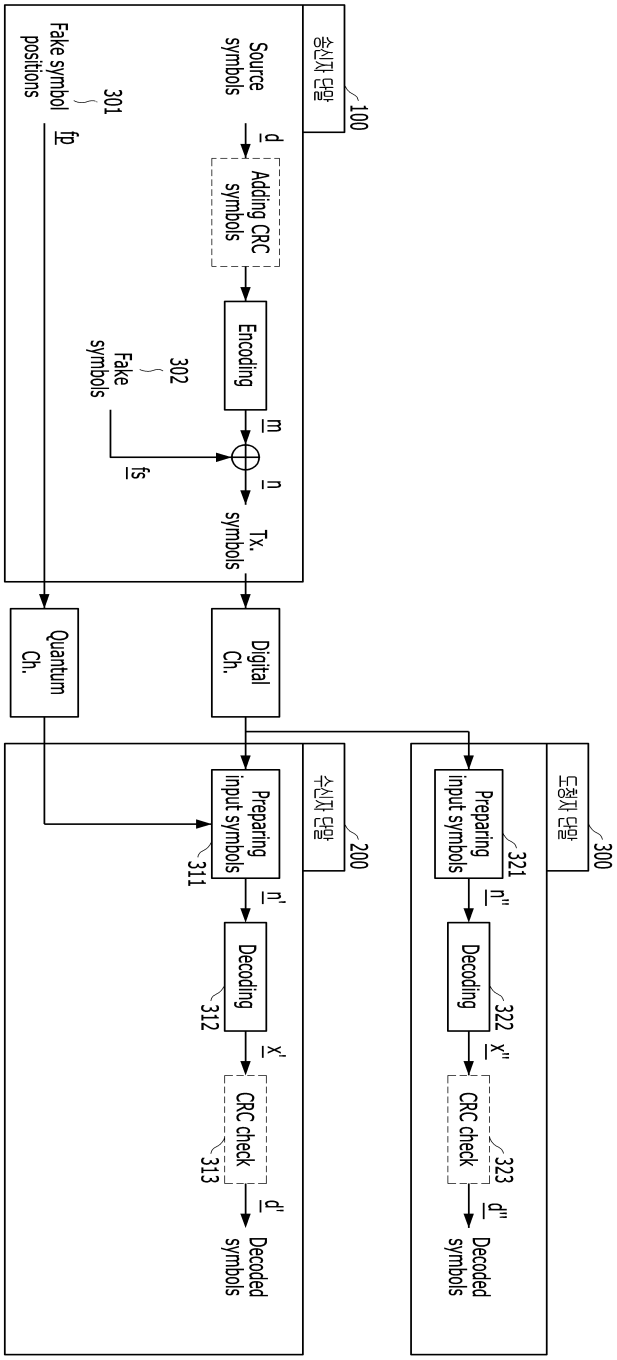
도면2


Redun. packets (h_{sec})
Source packets (k_1)
Data connection
Source packets (k_1)
FEC encoder
Redun. packets ($h'_{sec} \leq h_{sec}$)
FEC decoder
Reference packets (k_2)
Reference packets (k_2)
Reference database (k_{rb})
Reference database (k_{rb})
송신자
수신자

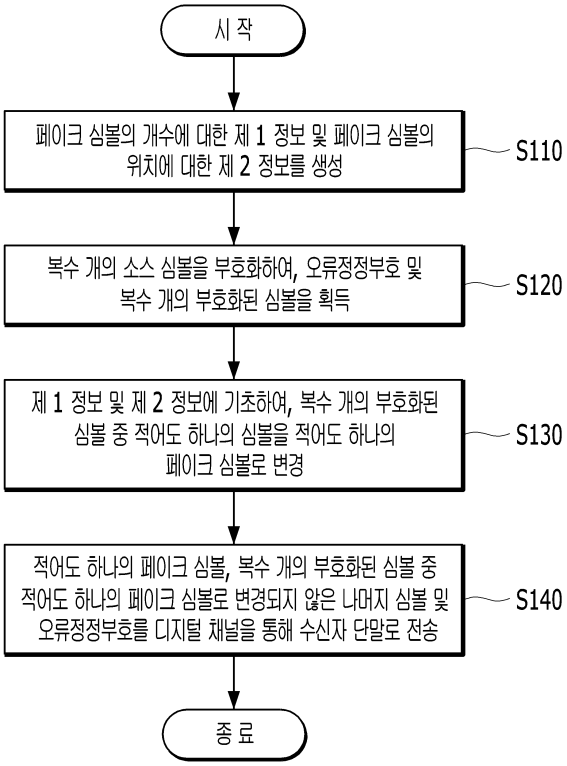
도면3


100
송신자 단말
110
프로세서
120
통신부
130
메모리
200
수신자 단말
210
프로세서
220
통신부
230
메모리

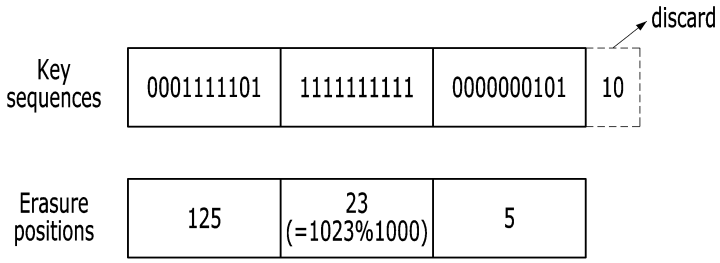
도면4


송신자 단말
100
Source symbols
d
Adding CRC symbols
Encoding
m
Fake symbol positions
301
fp
Fake symbols
302
fs
n
Tx. symbols
Quantum Ch.
Digital Ch.
수신자 단말
200
Preparing input symbols
311
n'
Decoding
312
x'
CRC check
313
d'
Decoded symbols
도청자 단말
300
Preparing input symbols
321
n''
Decoding
322
x''
CRC check
323
d''
Decoded symbols

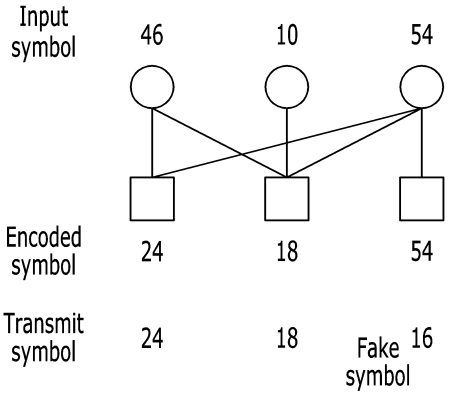
도면5


시 작
페이크 심볼의 개수에 대한 제 1 정보 및 페이크 심볼의 위치에 대한 제 2 정보를 생성
S110
복수 개의 소스 심볼을 부호화하여, 오류정정부호 및 복수 개의 부호화된 심볼을 획득
S120
제 1 정보 및 제 2 정보에 기초하여, 복수 개의 부호화된 심볼 중 적어도 하나의 심볼을 적어도 하나의 페이크 심볼로 변경
S130
적어도 하나의 페이크 심볼, 복수 개의 부호화된 심볼 중 적어도 하나의 페이크 심볼로 변경되지 않은 나머지 심볼 및 오류정정부호를 디지털 채널을 통해 수신자 단말로 전송
S140
종 료

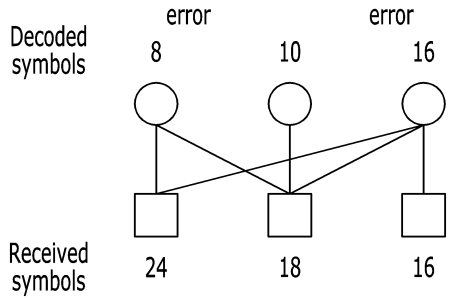
도면6


discard
Key sequences
0001111101
1111111111
0000000101
10
Erasure positions
125
23 (=1023%1000)
5

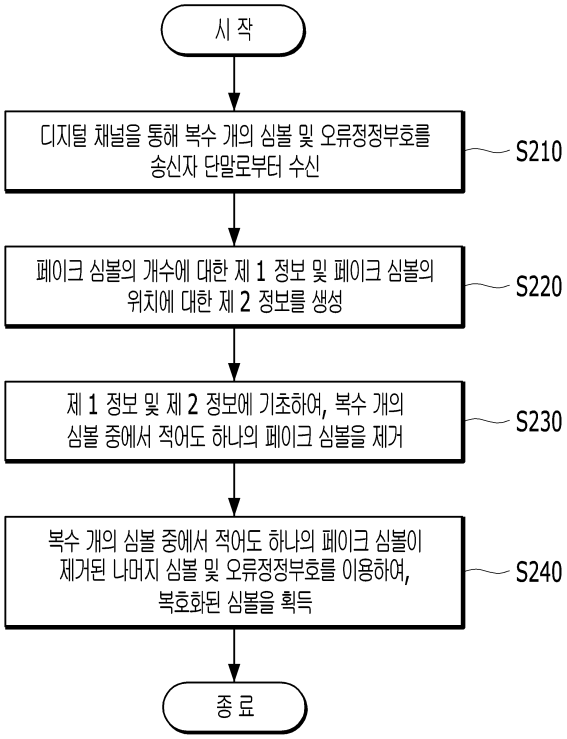
도면7


Input symbol
46
10
54
Encoded symbol
24
18
54
Transmit symbol
24
18
Fake symbol
16

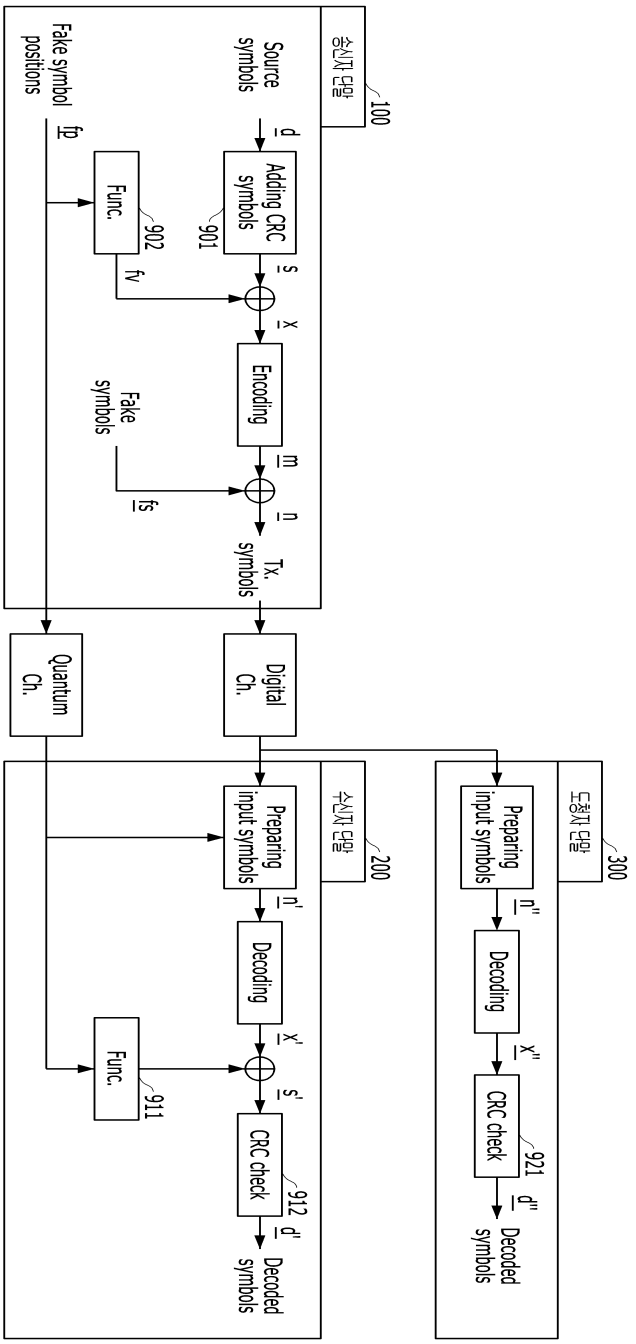
도면8


error
error
Decoded symbols
8
10
16
Received symbols
24
18
16

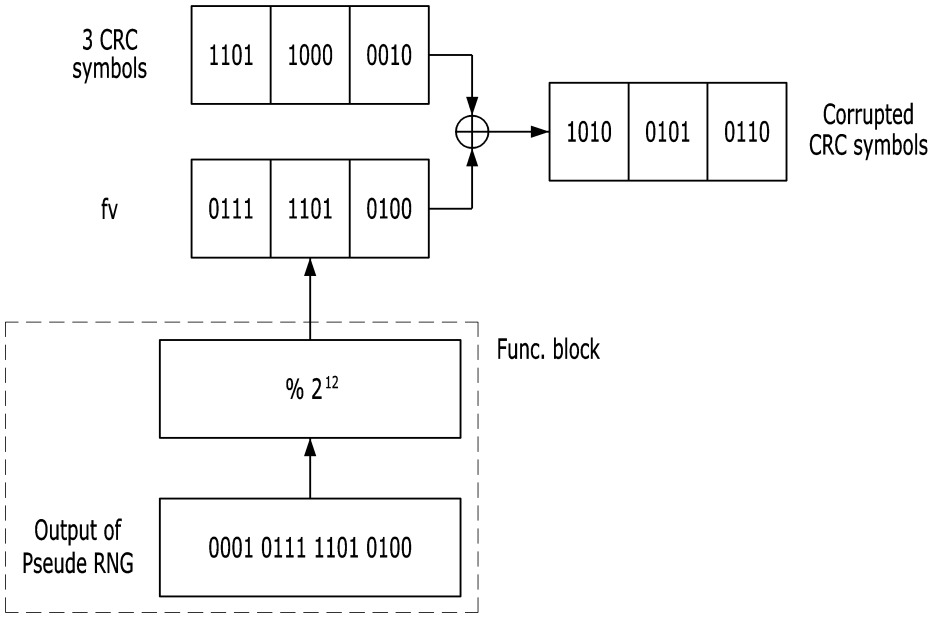
도면9


시 작
디지털 채널을 통해 복수 개의 심볼 및 오류정정부호를 송신자 단말로부터 수신
S210
페이크 심볼의 개수에 대한 제 1 정보 및 페이크 심볼의 위치에 대한 제 2 정보를 생성
S220
제 1 정보 및 제 2 정보에 기초하여, 복수 개의 심볼 중에서 적어도 하나의 페이크 심볼을 제거
S230
복수 개의 심볼 중에서 적어도 하나의 페이크 심볼이 제거된 나머지 심볼 및 오류정정부호를 이용하여, 복호화된 심볼을 획득
S240
종 료

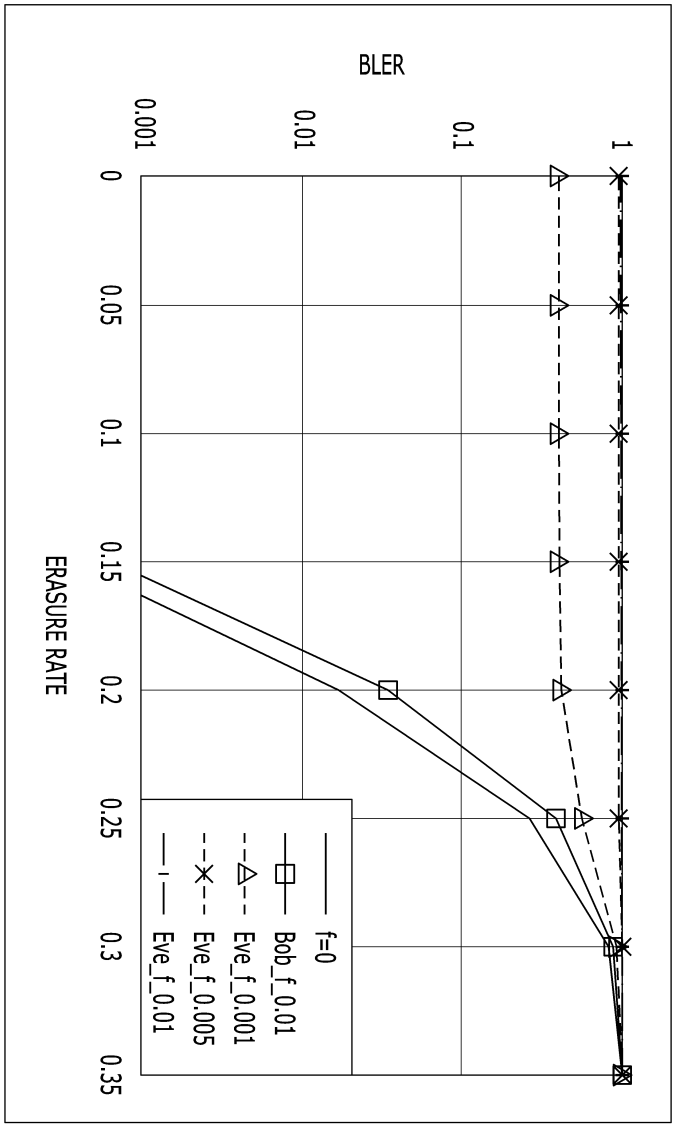
도면10


송신자 단말
100
Source symbols
d
Adding CRC symbols
901
s
Func.
902
fv
fp
Fake symbol positions
x
Encoding
Fake symbols
fs
m
n
Tx. symbols
Quantum Ch.
Digital Ch.
수신자 단말
200
Preparing input symbols
n'
Decoding
x'
Func.
911
s'
CRC check
912
d'
Decoded symbols
도청자 단말
300
Preparing input symbols
n''
Decoding
x''
CRC check
921
d''
Decoded symbols

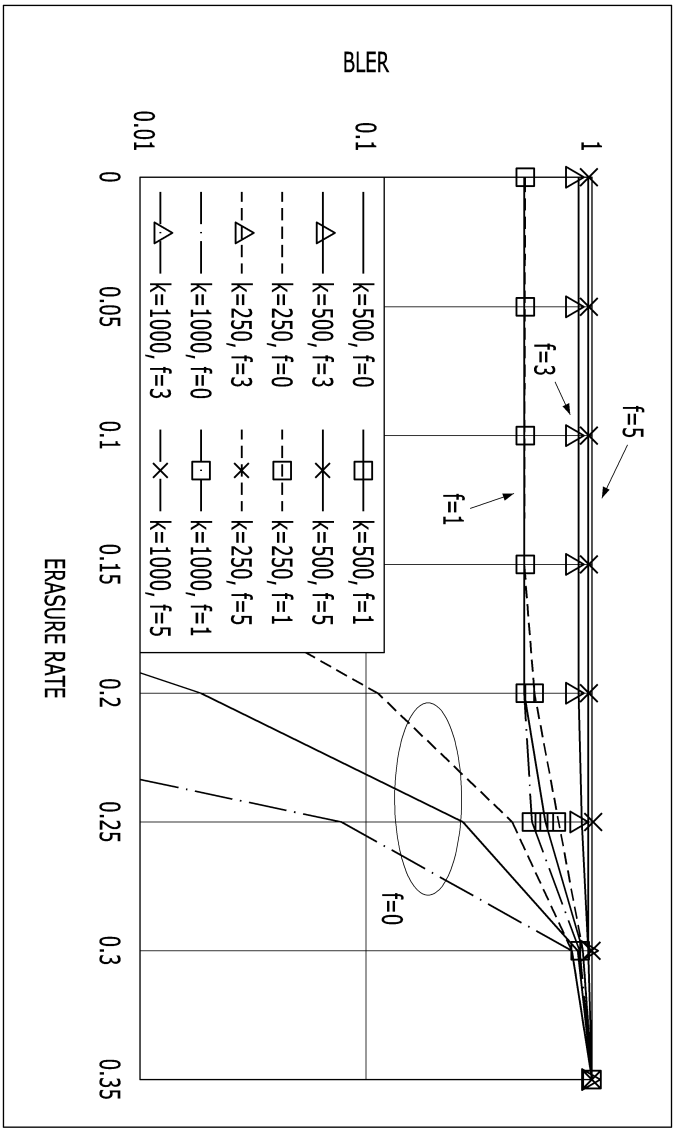
도면11


3 CRC symbols
1101
1000
0010
1010
0101
0110
Corrupted CRC symbols
fv
0111
1101
0100
Func. block
% 2^12
Output of Pseude RNG
0001 0111 1101 0100

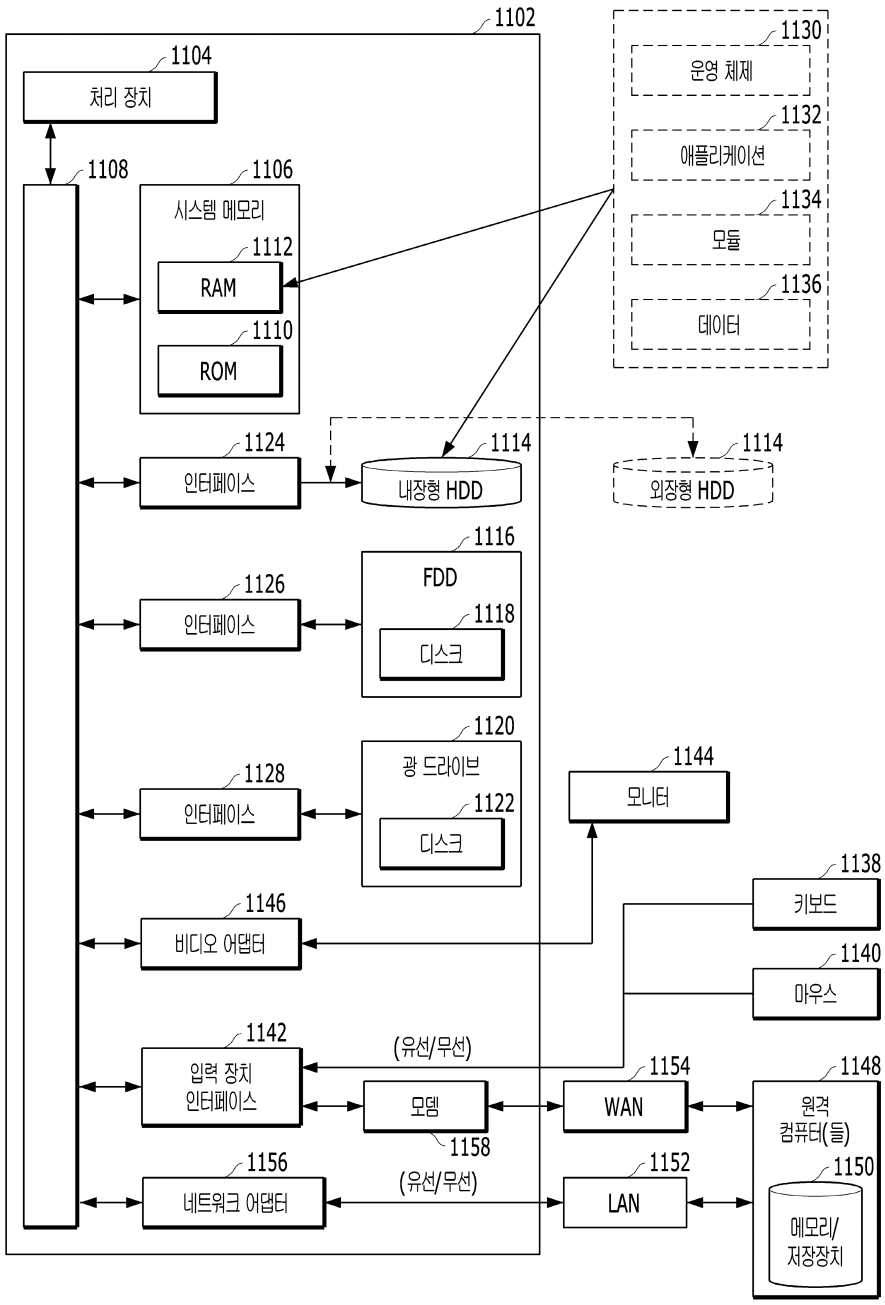
도면12


BLER
0.001
0.01
0.1
1
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
ERASURE RATE
f=0
Bob_f_0.01
Eve_f_0.001
Eve_f_0.005
Eve_f_0.01

도면13


BLER
ERASURE RATE
1
0.1
0.01
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
f=5
f=3
f=1
f=0
k=500, f=0
k=500, f=1
k=500, f=3
k=500, f=5
k=250, f=0
k=250, f=1
k=250, f=3
k=250, f=5
k=1000, f=0
k=1000, f=1
k=1000, f=3
k=1000, f=5

도면14


1102
1104
처리 장치
1108
1106
시스템 메모리
1112
RAM
1110
ROM
1130
운영 체제
1132
애플리케이션
1134
모듈
1136
데이터
1124
인터페이스
1114
내장형 HDD
1114
외장형 HDD
1116
FDD
1126
인터페이스
1118
디스크
1120
광 드라이브
1128
인터페이스
1122
디스크
1144
모니터
1138
키보드
1146
비디오 어댑터
1140
마우스
1142
입력 장치
인터페이스
(유선/무선)
모뎀
1158
1154
WAN
1148
원격
컴퓨터(들)
1156
네트워크 어댑터
(유선/무선)
1152
LAN
1150
메모리/
저장장치