(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0058366
(43) 공개일자 2018년06월01일

(51) 국제특허분류(Int. Cl.)
H04L 9/12 (2006.01) *G06F 21/60* (2013.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/12 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2016-0157232
(22) 출원일자 2016년11월24일
심사청구일자 2016년11월24일

(71) 출원인
서울대학교산학협력단
서울특별시 관악구 관악로 1 (신림동)
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
노종선
서울특별시 강남구 광평로10길 15 상록수아파트 109동 406호
이위직
서울특별시 관악구 관악로17길 8, 1102호
김영식
광주광역시 서구 풍암2로 62 금호2차아파트 201동 1005호
(74) 대리인
김효성

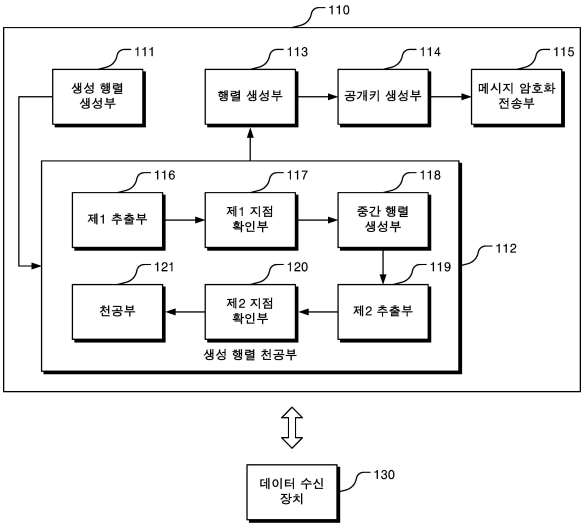
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치 및 방법**

(57) 요 약

생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치 및 방법이 개시된다. 본 발명은 리드-뮬러(Reed-Muller: RM) 코드의 생성 행렬로부터 특정 지점의 열에 위치하는 비트 값들을 천공한 후 천공된 생성 행렬을 이용하여 생성된 공개키를 통해 메시지의 암호화를 수행함으로써, 생성 행렬의 구조가 변경됨으로 인해 RM 코드의 구조에 기반한 제3자로부터의 공격을 방어할 수 있어서, 기존의 McEliece 암호화 시스템이 특수한 구조를 갖는 RM 코드의 생성 행렬을 그대로 사용함으로 인해서 발생하는 보안상의 취약성을 해소할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/30 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711037819
부처명 미래창조과학부
연구관리전문기관 미래창조과학부
연구사업명 정보보호핵심원천기술개발
연구과제명 (창조씨앗 1단계) IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연구
기 여 율 1/1
주관기관 서울대학교 산학협력단
연구기간 2016.04.01 ~ 2016.12.31

명 세 서

청구범위

청구항 1

t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 리드-뮬러(Reed-Muller: RM) 코드를 기초로 k x n(k와 n은 자연수) 크기의 생성 행렬 G - 상기 생성 행렬 G의 각 행은 RM 코드로 구성되어 있음 - 를 생성하는 생성 행렬 생성부;

상기 생성 행렬 G로부터 a(a는 자연수)개의 선정된(predetermined) 지점의 열에 위치하는 비트 값들을 천공(puncturing)하여 천공된 생성 행렬 G_D - 상기 천공된 생성 행렬 G_D의 크기는 k x (n-a)임 - 를 생성하는 생성 행렬 천공부;

k x k 크기의 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 순열 행렬 P를 생성하는 행렬 생성부;

상기 스크램블링 행렬 S, 상기 천공된 생성 행렬 G_D 및 상기 순열 행렬 P를 곱하여 공개키 K_{pub}($K_{pub}=SG_DP$)를 생성하는 공개키 생성부; 및

데이터 수신 장치로 전송할 메시지 m을 상기 공개키 K_{pub}를 기초로 암호화를 수행하여 암호화 메시지 c를 생성한 후 상기 암호화 메시지 c를 상기 데이터 수신 장치로 전송하는 메시지 암호화 전송부

를 포함하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치.

청구항 2

제1항에 있어서,

상기 생성 행렬 천공부는

상기 생성 행렬 G를 구성하는 각 행에 존재하는 RM 코드들 중 최소 해밍 무게(Hamming Weight)를 갖는 제1 코드를 추출하는 제1 추출부;

상기 제1 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제1 지점을 확인하는 제1 지점 확인부;

상기 생성 행렬 G로부터 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들을 추출하여 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들로 구성된 제1 행렬을 생성하는 중간 행렬 생성부;

상기 제1 행렬을 구성하는 각 행에 존재하는 코드들 중 최소 해밍 무게를 갖는 제2 코드를 추출하는 제2 추출부;

상기 제2 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제2 지점을 확인하는 제2 지점 확인부; 및

상기 생성 행렬 G로부터 상기 적어도 하나의 제2 지점에 해당되는 열에 위치하는 비트 값들을 천공함으로써, 상기 a개의 선정된 지점의 열에 위치하는 비트 값들에 대한 천공을 수행하는 천공부

를 포함하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치.

청구항 3

제1항에 있어서,

상기 메시지 암호화 전송부는

$t-\frac{a}{2}$ 이하의 해밍 무게를 가지면서 n-a 비트의 길이를 갖는 랜덤 벡터 e를 생성하고, 상기 메시지 m에 상기 공개키 K_{pub}를 곱한 결과 값 c'과 상기 랜덤 벡터 e의 합을 연산(2진 연산임)함으로써, 상기 암호화 메시지 c를

생성하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치.

청구항 4

제3항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 공개키에 대응하는 개인키로 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 저장하고 있고, 상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 메모리 상에 저장되어 있는 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 기초로 복호화를 수행하여 상기 메시지 m을 복호화하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치.

청구항 5

제4항에 있어서,

상기 데이터 수신 장치는

상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 순열 행렬 P의 역행렬 P^{-1}을 곱하여 cP^{-1}을 연산하고, 상기 a개의 선정된 지점에 대한 정보와 상기 생성 행렬 G를 기초로 상기 cP^{-1}에 대한 오류 정정을 수행하여 상기 메시지 m과 상기 스크램블링 행렬 S가 곱해진 mS를 연산한 후 상기 mS에 대해 상기 스크램블링 행렬 S의 역행렬 S^{-1}을 곱하여 상기 메시지 m을 복호화하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치.

청구항 6

t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 리드-뮬러(Reed-Muller: RM) 코드를 기초로 k x n(k와 n은 자연수) 크기의 생성 행렬 G - 상기 생성 행렬 G의 각 행은 RM 코드로 구성되어 있음 - 를 생성하는 단계;

상기 생성 행렬 G로부터 a(a는 자연수)개의 선정된(predetermined) 지점의 열에 위치하는 비트 값들을 천공(puncturing)하여 천공된 생성 행렬 G_D - 상기 천공된 생성 행렬 G_D의 크기는 k x (n-a)임 - 를 생성하는 단계;

k x k 크기의 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 순열 행렬 P를 생성하는 단계;

상기 스크램블링 행렬 S, 상기 천공된 생성 행렬 G_D 및 상기 순열 행렬 P를 곱하여 공개키 K_{pub}($K_{pub}=SG_DP$)를 생성하는 단계; 및

데이터 수신 장치로 전송할 메시지 m을 상기 공개키 K_{pub}를 기초로 암호화를 수행하여 암호화 메시지 c를 생성한 후 상기 암호화 메시지 c를 상기 데이터 수신 장치로 전송하는 단계

를 포함하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법.

청구항 7

제6항에 있어서,

상기 천공된 생성 행렬 G_D를 생성하는 단계는

상기 생성 행렬 G를 구성하는 각 행에 존재하는 RM 코드들 중 최소 해밍 무게(Hamming Weight)를 갖는 제1 코드를 추출하는 단계;

상기 제1 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제1 지점을 확인하는 단계;

상기 생성 행렬 G로부터 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들을 추출하여 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들로 구성된 제1 행렬을 생성하는 단계;

상기 제1 행렬을 구성하는 각 행에 존재하는 코드들 중 최소 해밍 무게를 갖는 제2 코드를 추출하는 단계;

상기 제2 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제2 지점을 확인하는 단계; 및

상기 생성 행렬 G로부터 상기 적어도 하나의 제2 지점에 해당되는 열에 위치하는 비트 값들을 천공함으로써, 상기 a개의 선정된 지점의 열에 위치하는 비트 값들에 대한 천공을 수행하는 단계

를 포함하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법.

청구항 8

제6항에 있어서,

상기 암호화 메시지 c를 상기 데이터 수신 장치로 전송하는 단계는

$t-\frac{a}{2}$ 이하의 해밍 무게를 가지면서 n-a 비트의 길이를 갖는 랜덤 벡터 e를 생성하고, 상기 메시지 m에 상기 공개키 K_{pub}를 곱한 결과 값 c'과 상기 랜덤 벡터 e의 합을 연산(2진 연산임)함으로써, 상기 암호화 메시지 c를 생성하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법.

청구항 9

제8항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 공개키에 대응하는 개인키로 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 저장하고 있고, 상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 메모리 상에 저장되어 있는 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 기초로 복호화를 수행하여 상기 메시지 m을 복호화하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법.

청구항 10

제9항에 있어서,

상기 데이터 수신 장치는

상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 순열 행렬 P의 역행렬 P^{-1}을 곱하여 cP^{-1}을 연산하고, 상기 a개의 선정된 지점에 대한 정보와 상기 생성 행렬 G를 기초로 상기 cP^{-1}에 대한 오류 정정을 수행하여 상기 메시지 m과 상기 스크램블링 행렬 S가 곱해진 mS를 연산한 후 상기 mS에 대해 상기 스크램블링 행렬 S의 역행렬 S^{-1}을 곱하여 상기 메시지 m을 복호화하는 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치.

청구항 11

제6항 내지 제10항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 리드-뮬러(Reed-Muller: RM) 코드의 생성 행렬을 사용하는 McEliece 암호화 시스템에서 제3자로부터의 공격을 방어함으로써, 보안을 강화하기 위한 기술과 관련된다.

배 경 기 술

[0002] 최근, 다양한 형태의 정보가 생성되고 유통됨에 따라, 해킹이나 잘못된 경로로의 정보 전달로 인해 중요한 정보

가 제3자에게 노출되는 등의 피해가 발생하고 있다.

[0003] 특히, 정보의 전달과정에서 군사 정보나 개인 정보 등과 같은 중요 정보에 어떠한 방어 기제가 적용되어 있지 않은 상태에서 이러한 중요 정보가 우연히 제3자에게 전달된다면, 제3자가 손쉽게 중요 정보에 접근할 수 있어, 큰 피해가 발생할 수 있다.

[0004] 최근에는 이러한 중요 정보의 노출을 방지하기 위해, 중요 정보를 소정의 암호화키를 이용하여 암호화한 후 이를 상대방에게 전달하는 기법 등이 도입되고 있다.

[0005] 일반적인 데이터 암호화 방식은 데이터 전송측과 데이터 수신측이 동일한 비밀키를 공유하고 있다가, 데이터 전송측이 비밀키로 데이터를 암호화해서 전송하면, 데이터 수신측이 동일한 비밀키로 데이터를 복호화하는 방식이 사용된다.

[0006] 하지만, 이러한 대칭키 기반의 암호화 방식은 비밀키의 전달 및 공유 과정에서 해당 비밀키가 노출될 위험성이 존재한다는 점에서 보안에 취약한 약점이 존재한다.

[0007] 이러한 대칭키 기반의 암호화 방식의 단점을 해소하기 위해서, 공개키와 개인키라는 비대칭키를 활용한 데이터 암호화 방식이 도입되었다. 비대칭키 기반의 데이터 암호화 방식은 데이터 전송측이 공개키로 데이터를 암호화해서 데이터 수신측으로 전송하면, 데이터 수신측이 상기 공개키에 대응하는 개인키로 데이터를 복호화하거나 데이터 전송측이 개인키로 데이터를 암호화해서 데이터 수신측으로 전송하면, 데이터 수신측이 상기 공개키로 데이터를 복호화하는 방식이 사용된다.

[0008] 이러한 비대칭키 기반의 데이터 암호화 방식은 데이터 전송측과 데이터 수신측이 서로 다른 암호화키를 가지고 있다는 점에서 암호화키 노출에 따른 위험성을 최소화할 수 있다.

[0009] 최근에는 이러한 비대칭키 기반의 암호화 방식이 적용된 시스템으로, McEliece 암호화 시스템이 도입되고 있다. McEliece 암호화 시스템은 데이터 전송 장치가 t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 선형 코드에 대한 k x n(k와 n은 자연수) 크기의 생성 행렬 G와 k x k 크기의 스크램블링 행렬 S 및 n x n 크기의 순열 행렬 P를 활용해서 공개키 K_{pub}을 만들고, 데이터 수신 장치로 전송할 메시지 m을 상기 공개키 K_{pub}로 암호화하여 암호화 메시지 c를 생성한 후 상기 암호화 메시지 c를 상기 데이터 수신 장치로 전송하면, 상기 데이터 수신 장치가 메모리 상에 기 저장하고 있는 상기 생성 행렬 G, 상기 스크램블링 행렬 S 및 상기 순열 행렬 P를 개인키로 활용해서 상기 암호화 메시지에 대한 복호화를 수행함으로써, 상기 메시지 m을 복원하는 시스템이다.

[0010] 관련해서, McEliece 암호화 시스템에서의 데이터 암호화와 복호화 방식에 대해 간단히 설명하면 다음과 같다.

[0011] 우선, 데이터 전송 장치가 사용하는 공개키는 K_{pub}은 하기의 수학식 1과 같이 정의된다.

수학식 1

[0013] $$K_{pub} = SGP$$

[0015] 여기서, 상기 수학식 1에서 생성 행렬 G는 t비트의 코드에 대한 오류 정정 능력을 갖는 (n, k) 선형 코드 C에 대한 k x n 크기의 생성 행렬이고, S는 랜덤하게 결정된 k x k 크기를 갖는 스크램블링 행렬이며, P는 랜덤하게 결정된 n x n 크기를 갖는 순열 행렬이다.

[0016] 이때, 데이터 수신 장치는 메모리 상에서 상기 공개키 K_{pub}에 대응하는 개인키로 상기 생성 행렬 G, 상기 스크램블링 행렬 S 및 상기 순열 행렬 P를 각각 저장하고 있다.

[0017] 이러한 상황 하에서 데이터 전송 장치는 상기 데이터 수신 장치로 전송할 메시지 m에 대해서 k길이를 갖는 이진 스트링 데이터로 인코딩한 후 상기 인코딩된 메시지 m에 대해 하기의 수학식 2에 따른 암호화 연산을 수행함으로써, 암호화 메시지 c를 생성할 수 있다.

수학식 2

[0019] $$c = mK_{pub} + e$$

[0021] 여기서, e는 t 이하의 해밍 무게(Hamming Weight)를 가지면서, n비트의 길이를 갖는 랜덤 벡터이고, "+"는 2진 연산이다.

[0022] 그리고, 해밍 무게란 데이터를 구성하는 비트열에서 "1"이라는 비트 값의 개수를 의미한다.

[0023] 이렇게, 상기 암호화 메시지 c가 생성되면, 상기 데이터 전송 장치는 상기 데이터 수신 장치로 상기 암호화 메시지 c를 전송함으로써, 데이터 암호화 전송을 완료한다.

[0024] 이렇게, 상기 데이터 전송 장치로부터 상기 암호화 메시지 c가 상기 데이터 수신 장치로 전송되면, 상기 데이터 수신 장치는 메모리 상에 저장되어 있는 상기 생성 행렬 G, 상기 스크램블링 행렬 S 및 상기 순열 행렬 P를 활용해서 상기 암호화 메시지에 대한 복호화를 수행하게 된다.

[0025] 관련해서, 상기 데이터 수신 장치는 상기 암호화 메시지 c가 수신되면, 하기의 수학식 3과 같이 상기 암호화 메시지 c에 대해 상기 순열 행렬 P의 역행렬인 P^{-1}을 곱하여 cP^{-1}을 연산한다.

수학식 3

[0027] $$cP^{-1} = mSG + eP^{-1}$$

[0029] 그러고 나서, 상기 데이터 수신 장치는 cP^{-1}으로부터 상기 생성 행렬 G를 이용해서 오류 정정을 위한 데이터 디코딩을 수행하여 mS를 연산할 수 있다.

[0030] 여기서, 상기 e는 t 이하의 해밍 무게를 갖는 벡터이고, P는 순열 행렬이므로, eP^{-1}도 t 이하의 해밍 무게를 갖기 때문에 결론적으로 cP^{-1}은 mSG라는 부호어에서 t개 이하의 비트 값에 대해 오류가 발생한 것으로 볼 수 있어서, 상기 데이터 수신 장치는 메모리 상에 저장되어 있는 t비트의 코드에 대한 오류 정정 능력을 갖는 (n, k) 선형 코드 C의 생성 행렬인 G를 이용하여 cP^{-1}에 대해 오류 정정을 수행함으로써, mS를 디코딩할 수 있다.

[0031] 이렇게, mS의 연산이 완료되면, 상기 데이터 수신 장치는 하기의 수학식 4와 같이 메모리 상에 저장되어 있는 상기 스크램블링 행렬 S의 역행렬인 S^{-1}을 mS에 곱함으로써, 원본 메시지인 m을 최종적으로 복호화할 수 있다.

수학식 4

[0033] $$mSS^{-1} = m$$

[0035] 최근에는 이러한 McEliece 암호화 시스템에서 상기 생성 행렬 G와 관련해서, 리드-뮬러(Reed-Muller: RM) 코드의 생성 행렬을 사용하는 경우가 많다. RM 코드는 오류 정정 코드로 사용되는 선형 코드로, RM(r, m)으로 표현되는 RM 코드는 길이가 2^m이고, m개의 기본 코드를 가지게 되며, 상기 m개의 기본 코드들 간의 곱을 갖는 코드 역시 RM의 기본 코드가 될 수 있다. 그리고, r은 기본 코드들 간의 곱에 사용될 수 있는 기본 코드의 최대 개수를 의미한다. 예컨대, m=4, r=4라고 할 때, RM 코드의 길이는 16이 되고, 이때, 상기 RM 코드는 2^4으로 표시되므로, 4개의 기본 코드 R1, R2, R3, R4(각 기본 코드의 길이는 16임)를 가지게 된다. 이때, 4개의 기본 코드 R1, R2, R3, R4 간의 곱을 연산한 RM 코드 역시 기본 코드가 될 수 있다. 여기서, r=4이기 때문에 4개의 기본 코드 R1, R2, R3, R4에 대해서는 또 다른 추가 기본 코드를 생성하기 위해서 상기 4개의 기본 코드들 간의 곱에 사용 가능한 최대 개수가 4개가 되기 때문에, 4개의 기본 코드 R1, R2, R3, R4 상호 간의 곱을 최대 4개까지 조합하여 연산함으로써, 추가적인 기본 코드들을 생성할 수 있다. 관련해서, RM(4, 4)에 대해서는 R1, R2, R3, R4에 해당되는 4개의 기본 코드와 R1R2, R1R3, R1R4, R2R3, R2R4, R3R4, R1R2R3, R1R2R4, R1R3R4, R2R3R4, R1R2R3R4로 구성된 11개의 기본 코드를 생성할 수 있고, RM 코드의 특성상 비트 값이 모두 "1"로 구성된 코드도 기본 코드로 가져야 하기 때문에 결과적으로 총 16개의 기본 코드들이 생성될 수 있다. 이때, McEliece 암호화 시스템에서는 이러한 총 16개의 기본 코드들을 활용해서 메시지를 암호화할 때 사용할 생성 행렬 G를 생성할 수 있다.

[0036] 이러한 RM 코드는 높은 오류 정정 능력을 가지고 있기 때문에 암호 시스템의 보안성을 높이는데 유용하게 사용될 수 있다. 하지만, RM 코드는 그 구조가 특수하기 때문에 RM 코드로부터 데이터 복호화에 사용되는 개인키에 대한 추측이 용이하게 되어, McEliece 암호화 시스템에서 RM 코드를 그대로 사용한다면, 중요 데이터가 노출될 위험성이 높아질 수 있다.

[0037] 관련해서, 선행 문헌인 "Cryptanalysis of the Sidelnikov cryptosystem", Lorenz Minder 외 1인, "Advances in cryptology - Eurocrypt 2007", LNCS vol. 4515에서는 RM 코드의 특성에 기초하여 McEliece 암호화 시스템에서 순열 행렬 P를 찾아내는 공격 방법에 대해 개시하고 있고, "The failure of McEliece PKC based on Reed-Muller codes.", I. V. Chizhov 외 1인, Prikl. Diskr. Mat. Suppl., 2013, Issue 6, Pages 48-49에서는 상기 공격 방법에서 그 과정을 단축시키는 방법에 대해서 개시하고 있다.

[0038] 따라서, RM 코드를 사용하는 McEliece 암호화 시스템에서 RM 코드의 특수성에 기초한 해커의 공격을 방어할 수 있도록 하는 방법에 대한 연구가 필요하다.

선행기술문헌

비특허문헌

[0039] (비특허문헌 0001) 1. "Cryptanalysis of the Sidelnikov cryptosystem", Lorenz Minder 외 1인, "Advances in cryptology - Eurocrypt 2007", LNCS vol. 4515(2007년)

(비특허문헌 0002) 2. "The failure of McEliece PKC based on Reed-Muller codes.", I. V. Chizhov 외 1인, Prikl. Diskr. Mat. Suppl., 2013, Issue 6, Pages 48-49(2013년 10월 9일)

(비특허문헌 0003) 3. "가변 길이를 갖는 리드 뮬러 부호 설계에 관한 연구", 노태균 외 3인, 한국통신학회 2015년도 추계종합학술발표회(2015년)

발명의 내용

해결하려는 과제

[0040] 본 발명에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치 및 방법은 리드-뮬러(Reed-Muller: RM) 코드의 생성 행렬로부터 특정 지점의 열에 위치하는 비트 값들을 천공한 후 천공된 생성 행렬을 이용하여 생성된 공개키를 통해 메시지의 암호화를 수행함으로써, 생성 행렬의 구조가 변경됨으로 인해 RM 코드의 구조에 기반한 제3자로부터의 공격을 방어할 수 있어서, 기존의 McEliece 암호화 시스템이 특수한 구조를 갖는 RM 코드의 생성 행렬을 그대로 사용함으로 인해서 발생하는 보안상의 취약성을 해소하고자 한다.

과제의 해결 수단

[0041] 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치는 t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 리드-뮬러(Reed-Muller: RM) 코드를 기초로 k x n(k와 n은 자연수) 크기의 생성 행렬 G - 상기 생성 행렬 G의 각 행은 RM 코드로 구성되어 있음 - 를 생성하는 생성 행렬 생성부, 상기 생성 행렬 G로부터 a(a는 자연수)개의 선정된(predetermined) 지점의 열에 위치하는 비트 값들을 천공(puncturing)하여 천공된 생성 행렬 G_D - 상기 천공된 생성 행렬 G_D의 크기는 k x (n-a)임 - 를 생성하는 생성 행렬 천공부, k x k 크기의 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 순열 행렬 P를 생성하는 행렬 생성부, 상기 스크램블링 행렬 S, 상기 천공된 생성 행렬 G_D 및 상기 순열 행렬 P를 곱하여 공개키 K_{pub}(K_{pub}=SG_DP)를 생성하는 공개키 생성부 및 데이터 수신 장치로 전송할 메시지 m을 상기 공개키 K_{pub}를 기초로 암호화를 수행하여 암호화 메시지 c를 생성한 후 상기 암호화 메시지 c를 상기 데이터 수신 장치로 전송하는 메시지 암호화 전송부를 포함한다.

[0042] 또한, 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법은 t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 RM 코드를 기초로 k x n(k와 n은 자연수) 크기의 생성 행렬 G - 상기 생성 행렬 G의 각 행은 RM 코드로 구성되어 있음 - 를 생성하는 단계, 상기 생성 행렬 G로부터 a(a는 자연수)개의 선정된 지점의 열에 위치하는 비트 값들을 천공하여 천공된 생성 행렬 G_D - 상기 천공된 생성 행렬 G_D의 크기는 k x (n-a)임 - 를 생성하는 단계, k x k 크기의 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 순열 행렬 P를 생성하는 단계, 상기 스크램블링 행렬 S, 상기 천공된 생성 행렬 GD 및 상기 순열 행렬 P를 곱하여 공개키 K_{pub}(K_{pub}=SG_DP)를 생성하는 단계 및 데이터 수신 장치로 전송할 메시지 m을 상기 공개키 K_{pub}를 기초로 암호화를 수행하여 암호화 메시지 c를 생성한 후 상기 암호화 메시지 c를 상기 데이터 수신 장치로 전송하는 단계를 포함한다.

발명의 효과

[0043] 본 발명에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치 및 방법은 리드-뮬러(Reed-Muller: RM) 코드의 생성 행렬로부터 특정 지점의 열에 위치하는 비트 값들을 천공한 후 천공된 생성 행렬을 이용하여 생성된 공개키를 통해 메시지의 암호화를 수행함으로써, 생성 행렬의 구조가 변경됨으로 인해 RM 코드의 구조에 기반한 제3자로부터의 공격을 방어할 수 있어서, 기존의 McEliece 암호화 시스템이 특수한 구조를 갖는 RM 코드의 생성 행렬을 그대로 사용함으로 인해서 발생하는 보안상의 취약성을 해소할 수 있다.

도면의 간단한 설명

[0044] 도 1은 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0045] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0046] 도 1은 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치의 구조를 도시한 도면이다.

[0047] 도 1을 참조하면, 본 발명에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치(110)는 생성 행렬 생성부(111), 생성 행렬 천공부(112), 행렬 생성부(113), 공개키 생성부(114) 및 메시지 암호화 전송부(115)를 포함한다.

[0048] 생성 행렬 생성부(111)는 t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 리드-뮬러(Reed-Muller: RM) 코드를 기초로 k x n(k와 n은 자연수) 크기의 생성 행렬 G를 생성한다.

[0049] 이때, 생성 행렬 생성부(111)는 t 비트의 코드에 대한 오류 정정 능력을 갖는 n길이의 RM 기본 코드들을 생성하고, 상기 기본 코드들을 서로 곱한 결과 값들과 "1"의 비트 값으로 구성된 코드를 추가 RM 기본 코드들로 생성함으로써, 해당 RM 기본 코드들을 기초로 k x n 크기의 상기 생성 행렬 G를 생성할 수 있다.

[0050] 이로 인해, 상기 생성 행렬 G의 각 행은 RM 코드로 구성되어 있다.

[0051] 생성 행렬 천공부(112)는 상기 생성 행렬 G로부터 a(a는 자연수)개의 선정된(predetermined) 지점의 열에 위치하는 비트 값들을 천공(puncturing)하여 천공된 생성 행렬 G_D를 생성할 수 있다.

[0052] 여기서, 상기 천공된 생성 행렬 G_D의 크기는 k x (n-a)이 된다.

[0053] 이때, 본 발명의 일실시예에 따르면, 생성 행렬 천공부(112)는 제1 추출부(116), 제1 지점 확인부(117), 중간 행렬 생성부(118), 제2 추출부(119), 제2 지점 확인부(120) 및 천공부(121)를 포함할 수 있다.

[0054] 제1 추출부(116)는 상기 생성 행렬 G를 구성하는 각 행에 존재하는 RM 코드들 중 최소 해밍 무게(Hamming Weight)를 갖는 제1 코드를 추출한다.

[0055] 제1 지점 확인부(117)는 상기 제1 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제1 지점을 확인한다.

[0056] 중간 행렬 생성부(118)는 상기 생성 행렬 G로부터 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들을 추출하여 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들로 구성된 제1 행렬을 생성한다.

[0057] 제2 추출부(119)는 상기 제1 행렬을 구성하는 각 행에 존재하는 코드들 중 최소 해밍 무게를 갖는 제2 코드를 추출한다.

[0058] 제2 지점 확인부(120)는 상기 제2 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제2 지점을 확인한다.

[0059] 천공부(121)는 상기 생성 행렬 G로부터 상기 적어도 하나의 제2 지점에 해당되는 열에 위치하는 비트 값들을 천공함으로써, 상기 a개의 선정된 지점의 열에 위치하는 비트 값들에 대한 천공을 수행한다.

[0060] 예컨대, 상기 생성 행렬 G가 8 x 16 크기의 생성 행렬인 것으로 가정하고, 상기 생성 행렬 G를 구성하는 8개의 행들에 존재하는 RM 코드들 중 3행에 위치하는 코드가 최소 해밍 무게를 갖는 코드라고 하는 경우, 제1 추출부(116)는 3행에 위치하는 RM 코드를 상기 제1 코드로 추출할 수 있다.

[0061] 그러고 나서, 제1 지점 확인부(117)는 상기 제1 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제1 지점을 확인할 수 있다.

[0062] 관련해서, 상기 제1 코드를 "1111111100000000"이라고 하면, 제1 지점 확인부(117)는 상기 제1 코드로부터 상기 적어도 하나의 제1 지점으로 "1~8번열"의 지점을 확인할 수 있다.

[0063] 그리고, 중간 행렬 생성부(118)는 8 x 16 크기를 갖는 상기 생성 행렬 G로부터 상기 적어도 하나의 제1 지점인 "1~8번열"에 해당되는 열에 위치하는 비트 값들을 추출하여 "1~8번열"에 해당되는 열에 위치하는 비트 값들로 구성된 제1 행렬을 생성할 수 있다. 이때, 상기 제1 행렬은 8 x 16 크기를 갖는 상기 생성 행렬 G에서 "1~8번열"에 해당되는 열의 성분들을 추출한 행렬이므로, 8 x 8 크기를 갖게 된다.

[0064] 이렇게, 제1 행렬이 생성되면, 제2 추출부(119)는 상기 제1 행렬을 구성하는 각 행에 존재하는 코드들 중 최소 해밍 무게를 갖는 제2 코드를 추출할 수 있다.

[0065] 관련해서, 상기 제1 행렬을 구성하는 8개의 행들에 존재하는 코드들 중 5행에 위치하는 코드가 최소 해밍 무게를 갖는 코드라고 하는 경우, 제2 추출부(119)는 5행에 위치하는 코드를 상기 제2 코드로 추출할 수 있다.

[0066] 그러고 나서, 제2 지점 확인부(120)는 상기 제2 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제2 지점을 확인할 수 있다.

[0067] 관련해서, 상기 제2 코드를 "11000000"이라고 하면, 제2 지점 확인부(120)는 상기 제2 코드로부터 상기 적어도

하나의 제2 지점으로 "1~2번열"의 지점을 확인할 수 있다.

[0068] 그 이후, 천공부(121)는 8 x 16 크기를 갖는 상기 생성 행렬 G로부터 상기 적어도 하나의 제2 지점인 "1~2번열"에 해당되는 열에 위치하는 비트 값들을 천공함으로써, 8 x 16 크기를 갖는 상기 생성 행렬 G에서 "1~2번열"이라는 2개의 열에 위치하는 비트 값들이 천공된 생성 행렬 G_D를 생성할 수 있다.

[0069] 이때, 상기 천공된 생성 행렬 G_D는 8 x 16 크기를 갖는 상기 생성 행렬 G에서 "1~2번열"에 위치하는 비트 값들이 천공되었기 때문에 상기 천공된 생성 행렬 G_D 크기는 8 x 14가 된다.

[0070] 이렇게, 상기 천공된 생성 행렬 G_D가 생성되면, 행렬 생성부(113)는 k x k 크기의 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 순열 행렬 P를 생성한다.

[0071] 여기서, 행렬 생성부(113)는 "1"과 "0"의 코드 값을 성분으로 갖는 k x k 크기의 상기 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 상기 순열 행렬 P를 랜덤하게 생성할 수 있다.

[0072] 그리고, 공개키 생성부(114)는 하기의 수학식 5와 같이, 상기 스크램블링 행렬 S, 상기 천공된 생성 행렬 G_D 및 상기 순열 행렬 P를 곱하여 공개키 K_{pub}를 생성할 수 있다.

수학식 5

[0074] $$K_{pub} = SG_DP$$

[0076] 그 이후, 메시지 암호화 전송부(115)는 데이터 수신 장치(130)로 전송할 메시지 m을 상기 공개키 K_{pub}를 기초로 암호화를 수행하여 암호화 메시지 c를 생성한 후 상기 암호화 메시지 c를 데이터 수신 장치(130)로 전송할 수 있다.

[0077] 이때, 본 발명의 일실시예에 따르면, 메시지 암호화 전송부(115)는 $t-\frac{a}{2}$ 이하의 해밍 무게를 가지면서 n-a 비트의 길이를 갖는 랜덤 벡터 e를 생성하고, 상기 메시지 m에 상기 공개키 K_{pub}를 곱한 결과 값 c'과 상기 랜덤 벡터 e의 합을 연산(2진 연산임)함으로써, 상기 암호화 메시지 c를 생성할 수 있다.

[0078] 관련해서, 메시지 암호화 전송부(115)는 하기의 수학식 6과 같은 연산을 수행함으로써, 상기 암호화 메시지 c를 생성할 수 있다.

수학식 6

[0080] $$c = mK_{pub} + e$$

[0082] 여기서, e는 $t-\frac{a}{2}$ 이하의 해밍 무게를 가지면서, n-a 비트의 길이를 갖는 랜덤 벡터이고, "+"는 2진 연산이다.

[0083] 이렇게, 상기 암호화 메시지 c가 생성되어, 메시지 암호화 전송부(115)에 의해 데이터 수신 장치(130)로 상기 암호화 메시지 c가 전송되면, 데이터 수신 장치(130)는 상기 암호화 메시지 c로부터 원본 메시지 m를 복호화할

수 있는데, 본 발명의 일실시예에 따르면, 데이터 수신 장치(130)는 상기 암호화 메시지 c를 복호화하기 위해 메모리 상에 상기 공개키에 대응하는 개인키로 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 미리 저장하고 있을 수 있다.

[0084] 이때, 데이터 수신 장치(130)는 상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 메모리 상에 저장되어 있는 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 기초로 복호화를 수행하여 상기 메시지 m을 복호화할 수 있다.

[0085] 이때, 본 발명의 일실시예에 따르면, 데이터 수신 장치(130)는 상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 순열 행렬 P의 역행렬 P^{-1}을 곱하여 cP^{-1}을 연산하고, 상기 a개의 선정된 지점에 대한 정보와 상기 생성 행렬 G를 기초로 상기 cP^{-1}에 대한 오류 정정을 수행하여 상기 메시지 m과 상기 스크램블링 행렬 S가 곱해진 mS를 연산한 후 상기 mS에 대해 상기 스크램블링 행렬 S의 역행렬 S^{-1}을 곱하여 상기 메시지 m을 복호화할 수 있다.

[0086] 관련해서, 데이터 수신 장치(130)는 상기 암호화 메시지 c가 수신되면, 하기의 수학식 7에 따라 상기 암호화 메시지 c에 대해 상기 순열 행렬 P의 역행렬 P^{-1}을 곱하여 cP^{-1}을 연산할 수 있다.

수학식 7

[0088] $$cP^{-1} = mSG_D + eP^{-1}$$

[0090] 그러고 나서, 데이터 수신 장치(130)는 cP^{-1}에 대해, 상기 천공된 생성 행렬 G_D에서 비트 값이 천공된 열에 대한 지점인 상기 a개의 선정된 지점에 대한 정보와 상기 생성 행렬 G를 이용해서 오류 정정을 위한 데이터 디코딩을 수행함으로써, mS를 연산할 수 있다.

[0091] 여기서, 상기 e는 $t-\frac{a}{2}$ 이하의 해밍 무게를 갖는 벡터이고, P는 순열 행렬이므로, eP^{-1}도 $t-\frac{a}{2}$ 이하의 해밍 무게를 갖기 때문에 결론적으로 cP^{-1}은 mSG라는 부호어가 있을 때, 상기 생성 행렬 G에서 상기 a개의 선정된 지점의 열들이 모두 천공됨에 따라 a개의 오류가 발생했다고 볼 수 있음과 동시에 eP^{-1}에 의해 $t-\frac{a}{2}$ 이하의 추가 오류가 발생한 것으로 볼 수 있다.

[0092] 이때, 상기 생성 행렬 G에서 상기 a개의 선정된 지점의 열들이 모두 천공됨에 따라 발생한 것으로 볼 수 있는 a개의 오류는 오류 발생 위치를 알고 있기 때문에 오류 정정 능력의 1/2만 사용하여서 복구가 가능하므로, 상기 a개의 오류와 $t-\frac{a}{2}$ 이하의 추가 오류는 t비트의 코드에 대한 오류 정정 능력을 갖는 RM 코드로부터 디코딩을 통해 오류 정정이 가능하다.

[0093] 따라서, 데이터 수신 장치(130)는 메모리 상에 저장되어 있는 t비트의 코드에 대한 오류 정정 능력을 갖는 RM 코드의 생성 행렬인 G를 이용하여 cP^{-1}에 대해 오류 정정을 수행함으로써, 최종적으로 mS를 디코딩할 수 있다.

[0094] 이렇게, mS의 연산이 완료되면, 데이터 수신 장치(130)는 하기의 수학식 8과 같이 메모리 상에 저장되어 있는 상기 스크램블링 행렬 S의 역행렬인 S^{-1}을 mS에 곱함으로써, 원본 메시지인 m을 최종적으로 복호화할 수 있다.

수학식 8

[0096] $$mSS^{-1} = m$$

[0098] 지금까지 설명한 실시예와 같이, 본 발명에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치(110)는 기존의 McEliece 암호화 시스템이 특수한 구조를 갖는 RM 코드의 생성 행렬을 그대로 사용함으로써, 키 노출 가능성이 높아질 수 있는 단점이 있는 것에 비해, RM 코드의 생성 행렬로부터 특정 지점의 열에 위치하는 비트 값들을 천공한 후 천공된 생성 행렬을 이용하여 생성된 공개키를 통해 메시지의 암호화를 수행함으로써, 생성 행렬의 구조가 변경됨으로 인해 RM 코드의 구조에 기반한 제3자로부터의 공격을 방어할 수 있는 장점이 있다.

[0099] 도 2는 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법을 도시한 순서도이다.

[0100] 단계(S210)에서는 t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 RM 코드를 기초로 k x n(k와 n은 자연수) 크기의 생성 행렬 G(상기 생성 행렬 G의 각 행은 RM 코드로 구성되어 있음)를 생성한다.

[0101] 단계(S220)에서는 상기 생성 행렬 G로부터 a(a는 자연수)개의 선정된 지점의 열에 위치하는 비트 값들을 천공하여 천공된 생성 행렬 G_D(상기 천공된 생성 행렬 G_D의 크기는 k x (n-a)임)를 생성한다.

[0102] 이때, 본 발명의 일실시예에 따르면, 단계(S220)에서는 상기 생성 행렬 G를 구성하는 각 행에 존재하는 RM 코드들 중 최소 해밍 무게를 갖는 제1 코드를 추출하는 단계, 상기 제1 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제1 지점을 확인하는 단계, 상기 생성 행렬 G로부터 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들을 추출하여 상기 적어도 하나의 제1 지점에 해당되는 열에 위치하는 비트 값들로 구성된 제1 행렬을 생성하는 단계, 상기 제1 행렬을 구성하는 각 행에 존재하는 코드들 중 최소 해밍 무게를 갖는 제2 코드를 추출하는 단계, 상기 제2 코드를 구성하는 비트열에서 "1"의 비트 값이 위치하는 적어도 하나의 제2 지점을 확인하는 단계 및 상기 생성 행렬 G로부터 상기 적어도 하나의 제2 지점에 해당되는 열에 위치하는 비트 값들을 천공함으로써, 상기 a개의 선정된 지점의 열에 위치하는 비트 값들에 대한 천공을 수행하는 단계를 포함할 수 있다.

[0103] 단계(S230)에서는 k x k 크기의 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 순열 행렬 P를 생성한다.

[0104] 단계(S240)에서는 상기 스크램블링 행렬 S, 상기 천공된 생성 행렬 GD 및 상기 순열 행렬 P를 곱하여 공개키 K_{pub}(Kpub=SG_DP)를 생성한다.

[0105] 단계(S250)에서는 데이터 수신 장치로 전송할 메시지 m을 상기 공개키 K_{pub}를 기초로 암호화를 수행하여 암호화 메시지 c를 생성한 후 상기 암호화 메시지 c를 상기 데이터 수신 장치로 전송한다.

[0106] 이때, 본 발명의 일실시예에 따르면, 단계(S250)에서는 $t-\frac{a}{2}$ 이하의 해밍 무게를 가지면서 n-a 비트의 길이를 갖는 랜덤 벡터 e를 생성하고, 상기 메시지 m에 상기 공개키 K_{pub}를 곱한 결과 값 c'과 상기 랜덤 벡터 e의 합을 연산(2진 연산임)함으로써, 상기 암호화 메시지 c를 생성할 수 있다.

[0107] 또한, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 메모리 상에 상기 공개키에 대응하는 개인키로 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 저장하고 있고, 상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 메모리 상에 저장되어 있는 상기 생성 행렬 G, 상기 스크램블링 행렬 S, 상기 순열 행렬 P 및 상기 a개의 선정된 지점에 대한 정보를 기초로 복호화를 수행하여 상기 메시지 m을 복호화할 수 있다.

[0108] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 상기 암호화 메시지 c가 수신되면, 상기 암호화 메시지 c에 대해 상기 순열 행렬 P의 역행렬 P^{-1}을 곱하여 cP^{-1}을 연산하고, 상기 a개의 선정된 지점에 대한 정

보와 상기 생성 행렬 G를 기초로 상기 cP^{-1}에 대한 오류 정정을 수행하여 상기 메시지 m과 상기 스크램블링 행렬 S가 곱해진 mS를 연산한 후 상기 mS에 대해 상기 스크램블링 행렬 S의 역행렬 S^{-1}을 곱하여 상기 메시지 m을 복호화할 수 있다.

[0109] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법은 도 1을 이용하여 설명한 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0110] 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0111] 또한, 본 발명의 일실시예에 따른 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0112] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0113] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0114] 110: 생성 행렬의 천공에 기초한 암호화키를 사용하는 데이터 암호화 장치

111: 생성 행렬 생성부 112: 생성 행렬 천공부

113: 행렬 생성부 114: 공개키 생성부

115: 메시지 암호화부 116: 제1 추출부

117: 제1 지점 확인부 118: 중간 행렬 생성부

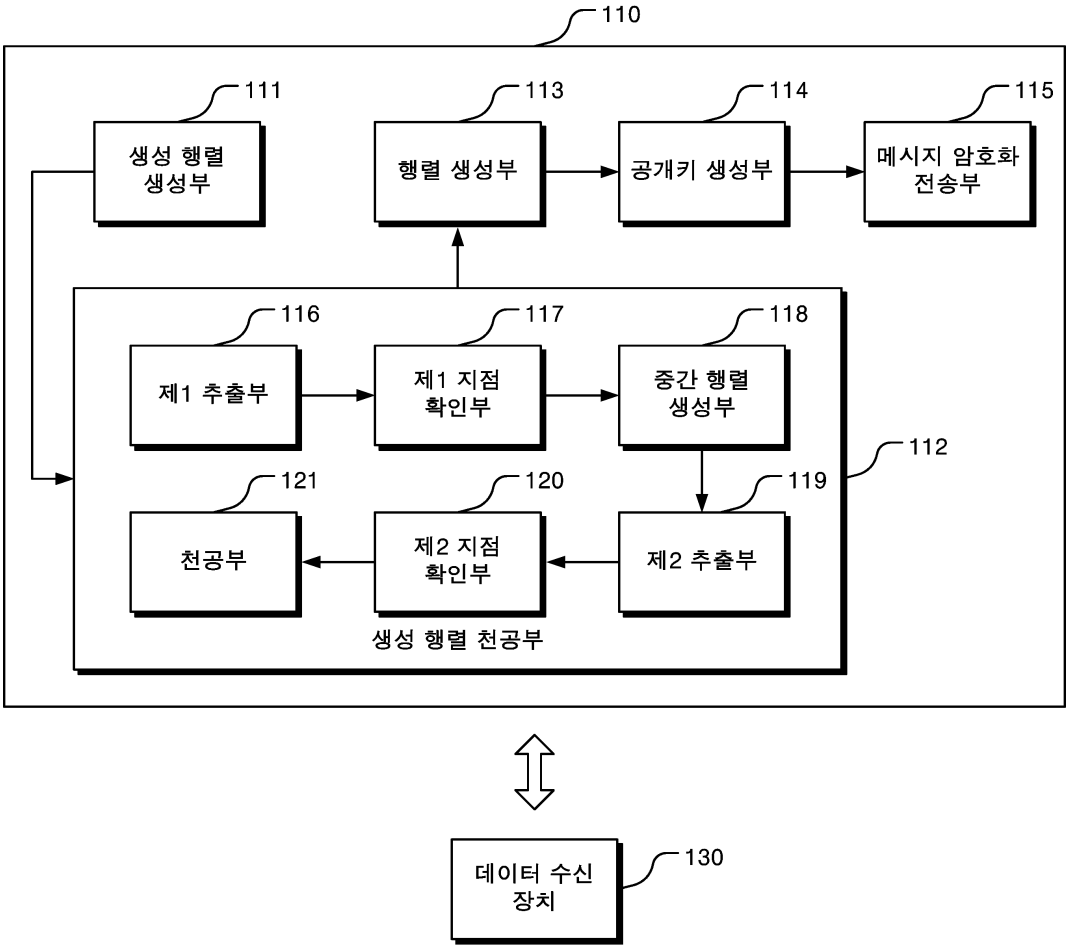
119: 제2 추출부 120: 제2 지점 확인부

121: 천공부

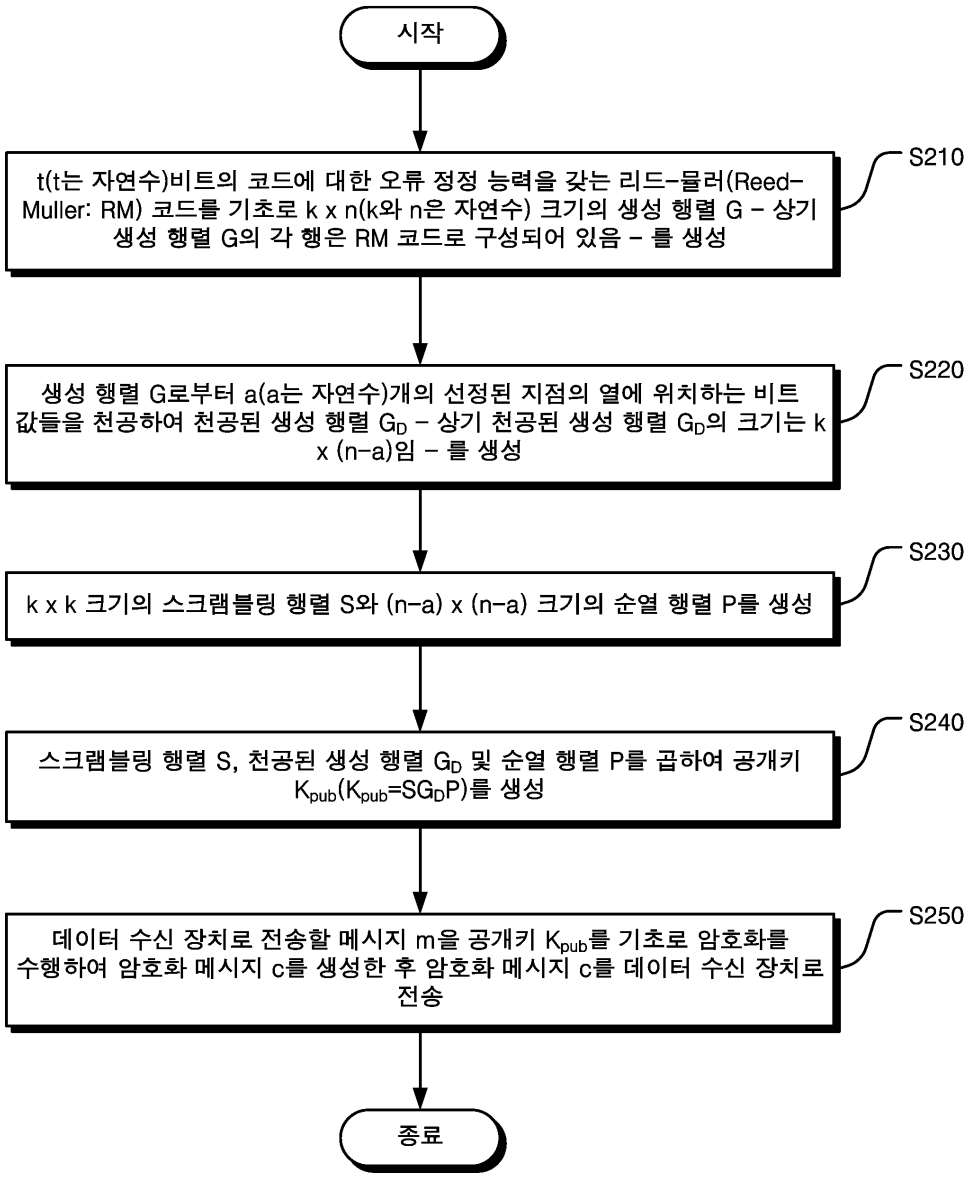
130: 데이터 수신 장치

도면

도면1


110
111
생성 행렬 생성부
113
행렬 생성부
114
공개키 생성부
115
메시지 암호화 전송부
116
제1 추출부
117
제1 지점 확인부
118
중간 행렬 생성부
112
121
천공부
120
제2 지점 확인부
119
제2 추출부
생성 행렬 천공부
130
데이터 수신 장치

도면2


시작
t(t는 자연수)비트의 코드에 대한 오류 정정 능력을 갖는 리드-뮬러(Reed-Muller: RM) 코드를 기초로 k x n(k와 n은 자연수) 크기의 생성 행렬 G - 상기 생성 행렬 G의 각 행은 RM 코드로 구성되어 있음 - 를 생성
S210
생성 행렬 G로부터 a(a는 자연수)개의 선정된 지점의 열에 위치하는 비트 값들을 천공하여 천공된 생성 행렬 G_D - 상기 천공된 생성 행렬 G_D의 크기는 k x (n-a)임 - 를 생성
S220
k x k 크기의 스크램블링 행렬 S와 (n-a) x (n-a) 크기의 순열 행렬 P를 생성
S230
스크램블링 행렬 S, 천공된 생성 행렬 G_D 및 순열 행렬 P를 곱하여 공개키 K_{pub}(K_{pub}=SG_DP)를 생성
S240
데이터 수신 장치로 전송할 메시지 m을 공개키 K_{pub}를 기초로 암호화를 수행하여 암호화 메시지 c를 생성한 후 암호화 메시지 c를 데이터 수신 장치로 전송
S250
종료