



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0129306
(43) 공개일자 2019년11월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2018-0053757
(22) 출원일자 2018년05월10일
심사청구일자 2018년05월10일

(71) 출원인
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
김영식
광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호
(74) 대리인
김효성

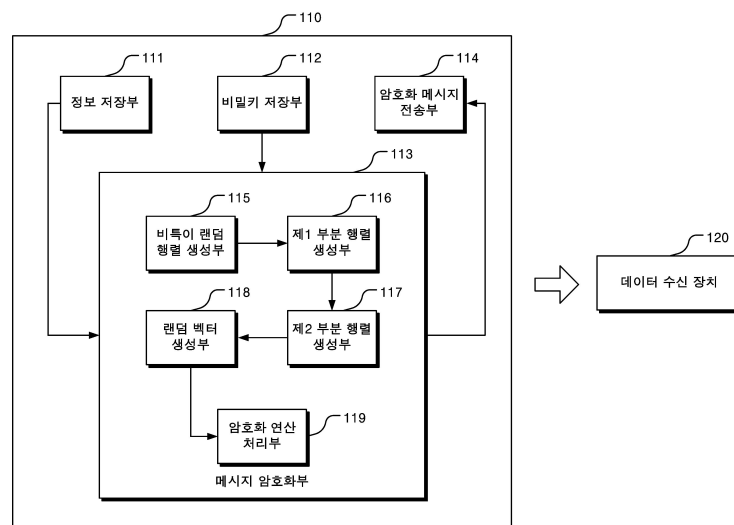
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치 및 그 동작 방법

(57) 요약

거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치 및 그 동작 방법이 개시된다. 본 발명에 따른 거듭 행렬(involutory matrix) 기반의 비밀키 암호화가 가능한 데이터 전송 장치 및 그 동작 방법은 거듭 행렬의 특성에 기반하여 설계된 비밀키를 기초로 메시지를 암호화해서 데이터 수신 장치로 전송함으로써, 상기 데이터 수신 장치가 상기 비밀키를 기초로 단순한 복호화 연산을 수행하는 방식으로 원본 데이터의 복원이 가능하도록 지원할 수 있어, 비교적 낮은 연산 성능을 갖는 기기들 간의 데이터 송수신시에도 높은 보안성을 제공할 수 있다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 1711065572

부처명 과학기술정보통신부

연구관리전문기관 한국연구재단

연구사업명 정보보호핵심원천기술개발(R&D)

연구과제명 (창조씨앗 2단계) IoT 및 클라우드 컴퓨팅을 위한 경량 포스트 양자 암호 시스템 연구

기 여 율 1/1

주관기관 조선대학교 산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

$N \times N$ (여기서, N 은 4이상의 자연수) 크기의 '1'과 '0'의 코드 값으로 구성된 거듭 행렬(involutory matrix) G 와 선정된(predetermined) 해시 함수가 저장되어 있는 정보 저장부;

$K \times K$ (여기서, K 는 2이상 N 미만의 크기를 갖는 자연수) 크기의 비특이(nonsingular) 랜덤 행렬을 생성하기 위해서 미리 지정된 시드(seed) 데이터와 $N \times N$ 크기의 '1'과 '0'의 코드 값으로 구성된 랜덤 순열 행렬 P 및 K 개의 미리 지정된 인덱스 값들이 비밀키로 저장되어 있는 비밀키 저장부;

K 비트의 크기를 갖는 메시지 M 에 대한 데이터 암호화 전송 명령이 인가되면, 상기 거듭 행렬 G 및 상기 선정된 해시 함수와 함께 상기 비밀키로 저장되어 있는 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 기초로 상기 메시지 M 을 암호화하여 암호화 메시지 c 를 생성하는 메시지 암호화부; 및

상기 암호화 메시지 c 를 데이터 수신 장치로 전송하는 암호화 메시지 전송부

를 포함하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치.

청구항 2

제1항에 있어서,

상기 메시지 암호화부는

상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 $K \times K$ 크기의 '1'과 '0'의 코드 값으로 구성된 비특이 랜덤 행렬 S 를 생성하는 비특이 랜덤 행렬 생성부;

상기 거듭 행렬 G 를 구성하는 N 개의 행들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K 개의 행들을 선택하여 상기 K 개의 행들 각각을 구성하는 N 개의 성분들만으로 구성된 $K \times N$ 크기의 제1 부분 행렬 R_A 를 생성하는 제1 부분 행렬 생성부;

상기 거듭 행렬 G 를 구성하는 N 개의 행들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응되지 않는 위치 상에 존재하는 $N-K$ 개의 행들을 선택하여 상기 $N-K$ 개의 행들 각각을 구성하는 N 개의 성분들만으로 구성된 $(N-K) \times N$

크기의 제2 부분 행렬 R_{A^c} 를 생성하는 제2 부분 행렬 생성부;

$N-K$ 의 크기를 갖는 랜덤 벡터 e 를 생성하는 랜덤 벡터 생성부; 및

상기 비특이 랜덤 행렬 S , 상기 제1 부분 행렬 R_A , 상기 제2 부분 행렬 R_{A^c} , 상기 랜덤 벡터 e 및 상기 랜덤 순열 행렬 P 를 기초로 상기 메시지 M 에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c 에 대한 생성을 처리하는 암호화 연산 처리부

를 포함하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치.

청구항 3

제2항에 있어서,

상기 암호화 연산 처리부는

하기의 수학식 1의 연산에 기초하여 상기 메시지 M 에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c 에 대한 생성을 처리하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치.

[수학식 1]

$$c = (MSR_A \oplus eR_A c)P$$

청구항 4

제3항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 거듭 행렬 G와 상기 선정된 해시 함수를 저장하고 있음과 동시에 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K개의 미리 지정된 인덱스 값들을 상기 비밀키로 저장하고 있으며,

상기 암호화 메시지 c가 수신되면, 상기 메모리 상에 저장되어 있는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성한 후 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 K x K 크기의 '1'과 '0'의 코드 값으로 구성된 상기 비트이 랜덤 행렬 S를 생성하고,

상기 거듭 행렬 G를 구성하는 N개의 열들 중 상기 K개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K개의 열들을 선택하여 상기 K개의 열들 각각을 구성하는 N개의 성분들만으로 구성된 N x K 크기의 제3 부분 행렬 C_A를 생성하며,

그 이후, 상기 비트이 랜덤 행렬 S, 상기 제3 부분 행렬 C_A 및 상기 메모리 상에 저장되어 있는 상기 랜덤 순열 행렬 P를 기초로 상기 암호화 메시지 c에 대한 복호화 연산을 수행함으로써, 상기 메시지 M을 복원하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치.

청구항 5

제4항에 있어서,

상기 데이터 수신 장치는

하기의 수학식 2의 연산에 기초하여 상기 암호화 메시지 c에 대한 복호화 연산을 수행함으로써, 상기 메시지 M을 복원하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치.

[수학식 2]

$$M = cP^T C_A S^{-1}$$

여기서, P^T는 상기 랜덤 순열 행렬 P의 전치 행렬, S⁻¹은 상기 비트이 랜덤 행렬 S의 역행렬임.

청구항 6

제1항에 있어서,

상기 거듭 행렬 G는 2 x 2 크기의 커널 행렬 F(여기서, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$)의 n-fold 크로네커 곱인 $F^{\otimes n}$ (여기서, $n = \log_2 N$)으로 연산되는 행렬로서 하기의 수학식 3의 조건을 만족하는 행렬인 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치.

[수학식 3]

$$GG = I_N$$

여기서, I_N은 N x N 크기의 항등 행렬임.

청구항 7

N x N(여기서, N은 4이상의 자연수) 크기의 '1'과 '0'의 코드 값으로 구성된 거듭 행렬(involutory matrix) G

와 선정된(predetermined) 해시 함수가 저장되어 있는 정보 저장부를 유지하는 단계;

$K \times K$ (여기서, K 는 2이상 N 미만의 크기를 갖는 자연수) 크기의 비특이(nonsingular) 랜덤 행렬을 생성하기 위해서 미리 지정된 시드(seed) 데이터와 $N \times N$ 크기의 '1'과 '0'의 코드 값으로 구성된 랜덤 순열 행렬 P 및 K 개의 미리 지정된 인덱스 값들이 비밀키로 저장되어 있는 비밀키 저장부를 유지하는 단계;

K 비트의 크기를 갖는 메시지 M 에 대한 데이터 암호화 전송 명령이 인가되면, 상기 거듭 행렬 G 및 상기 선정된 해시 함수와 함께 상기 비밀키로 저장되어 있는 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 기초로 상기 메시지 M 을 암호화하여 암호화 메시지 c 를 생성하는 단계; 및

상기 암호화 메시지 c 를 데이터 수신 장치로 전송하는 단계

를 포함하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법.

청구항 8

제7항에 있어서,

상기 암호화 메시지 c 를 생성하는 단계는

상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 $K \times K$ 크기의 '1'과 '0'의 코드 값으로 구성된 비특이 랜덤 행렬 S 를 생성하는 단계;

상기 거듭 행렬 G 를 구성하는 N 개의 행들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K 개의 행들을 선택하여 상기 K 개의 행들 각각을 구성하는 N 개의 성분들만으로 구성된 $K \times N$ 크기의 제1 부분 행렬 R_A 를 생성하는 단계;

상기 거듭 행렬 G 를 구성하는 N 개의 행들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응되지 않는 위치 상에 존재하는 $N-K$ 개의 행들을 선택하여 상기 $N-K$ 개의 행들 각각을 구성하는 N 개의 성분들만으로 구성된 $(N-K) \times N$ 크기의 제2 부분 행렬 R_{A^c} 를 생성하는 단계;

$N-K$ 의 크기를 갖는 랜덤 벡터 e 를 생성하는 단계; 및

상기 비특이 랜덤 행렬 S , 상기 제1 부분 행렬 R_A , 상기 제2 부분 행렬 R_{A^c} , 상기 랜덤 벡터 e 및 상기 랜덤 순열 행렬 P 를 기초로 상기 메시지 M 에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c 에 대한 생성을 처리하는 단계

를 포함하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법.

청구항 9

제8항에 있어서,

상기 암호화 메시지 c 에 대한 생성을 처리하는 단계는

하기의 수학식 4의 연산에 기초하여 상기 메시지 M 에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c 에 대한 생성을 처리하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법.

[수학식 4]

$$c = (MSR_A \oplus eR_{A^c})P$$

청구항 10

제9항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 거듭 행렬 G 와 상기 선정된 해시 함수를 저장하고 있음과 동시에 상기 시드 데이터, 상기 랜

덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 상기 비밀키로 저장하고 있으며,

상기 암호화 메시지 c 가 수신되면, 상기 메모리 상에 저장되어 있는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성한 후 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 $K \times K$ 크기의 '1'과 '0'의 코드 값으로 구성된 상기 비특이 랜덤 행렬 S 를 생성하고,

상기 거듭 행렬 G 를 구성하는 N 개의 열들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K 개의 열들을 선택하여 상기 K 개의 열들 각각을 구성하는 N 개의 성분들만으로 구성된 $N \times K$ 크기의 제3 부분 행렬 C_A 를 생성하며,

그 이후, 상기 비특이 랜덤 행렬 S , 상기 제3 부분 행렬 C_A 및 상기 메모리 상에 저장되어 있는 상기 랜덤 순열 행렬 P 를 기초로 상기 암호화 메시지 c 에 대한 복호화 연산을 수행함으로써, 상기 메시지 M 을 복원하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법.

청구항 11

제10항에 있어서,

상기 데이터 수신 장치는

하기의 수학식 5의 연산에 기초하여 상기 암호화 메시지 c 에 대한 복호화 연산을 수행함으로써, 상기 메시지 M 을 복원하는 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법.

[수학식 5]

$$M = cP^T C_A S^{-1}$$

여기서, P^T 는 상기 랜덤 순열 행렬 P 의 전치 행렬, S^{-1} 은 상기 비특이 랜덤 행렬 S 의 역행렬임.

청구항 12

제7항에 있어서,

상기 거듭 행렬 G 는 2×2 크기의 커널 행렬 F (여기서, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$)의 n -fold 크로네커 곱인 $F^{\otimes n}$ (여기서, $n = \log_2 N$)으로 연산되는 행렬로서 하기의 수학식 6의 조건을 만족하는 행렬인 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법.

[수학식 6]

$$GG = I_N$$

여기서, I_N 은 $N \times N$ 크기의 항등 행렬임.

청구항 13

제7항 내지 제12항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 14

제7항 내지 제12항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

본 발명은 데이터 송수신 과정에서 비밀키를 기반으로 데이터의 암호화/복호화가 가능하도록 지원하는 기술들과 관련

[0001]

된다.

배경 기술

- [0002] 최근, 다양한 형태의 정보가 생성되고 유통됨에 따라, 해킹이나 잘못된 경로로의 정보 전달로 인해 중요한 정보가 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] 기존의 비밀키로 데이터를 암호화하고 복호화하는 방식은 AES(Advanced Encryption Standard) 암호화 알고리즘이 주로 사용되는데, 해당 알고리즘은 사물인터넷 환경에서 활용되는 센서와 같은 제한된 연산 성능을 갖는 기기에서 활용되기에 적절하지 못한 측면이 존재한다.
- [0007] 따라서, 기존의 AES 암호화 알고리즘보다 경량화되면서도 안전한 데이터 송수신을 보장할 수 있는 암복호화 기법에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

- [0008] 본 발명에 따른 거듭 행렬(involutory matrix) 기반의 비밀키 암호화가 가능한 데이터 전송 장치 및 그 동작 방법은 거듭 행렬의 특성에 기반하여 설계된 비밀키를 기초로 메시지를 암호화해서 데이터 수신 장치로 전송함으로써, 상기 데이터 수신 장치가 상기 비밀키를 기초로 단순한 복호화 연산을 수행하는 방식으로 원본 데이터의 복원이 가능하도록 지원하여, 비교적 낮은 연산 성능을 갖는 기기들 간의 데이터 송수신시에도 높은 보안성을 제공할 수 있도록 한다.

과제의 해결 수단

- [0009] 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치는 $N \times N$ (여기서, N 은 4 이상의 자연수) 크기의 '1'과 '0'의 코드 값으로 구성된 거듭 행렬(involutory matrix) G 와 선정된(predetermined) 해시 함수가 저장되어 있는 정보 저장부, $K \times K$ (여기서, K 는 2이상 N 미만의 크기를 갖는 자연수) 크기의 비특이(nonsingular) 랜덤 행렬을 생성하기 위해서 미리 지정된 시드(seed) 데이터와 $N \times N$ 크기의 '1'과 '0'의 코드 값으로 구성된 랜덤 순열 행렬 P 및 K 개의 미리 지정된 인덱스 값들이 비밀키로 저장되어 있는 비밀키 저장부, K 비트의 크기를 갖는 메시지 M 에 대한 데이터 암호화 전송 명령이 인가되면, 상기 거듭 행렬 G 및 상기 선정된 해시 함수와 함께 상기 비밀키로 저장되어 있는 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 기초로 상기 메시지 M 을 암호화하여 암호화 메시지 c 를 생성하는 메시지 암호화부 및 상기 암호화 메시지 c 를 데이터 수신 장치로 전송하는 암호화 메시지 전송부를 포함한다.
- [0010] 또한, 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법은 $N \times N$ (여기서, N 은 4이상의 자연수) 크기의 '1'과 '0'의 코드 값으로 구성된 거듭 행렬 G 와 선정된 해시 함수가 저장되어 있는 정보 저장부를 유지하는 단계, $K \times K$ (여기서, K 는 2이상 N 미만의 크기를 갖는 자연수) 크기의 비특이 랜덤 행렬을 생성하기 위해서 미리 지정된 시드 데이터와 $N \times N$ 크기의 '1'과 '0'의 코드 값으로 구성된 랜덤 순열 행렬 P 및 K 개의 미리 지정된 인덱스 값들이 비밀키로 저장되어 있는 비밀키 저장부를 유지하는 단계, K 비트의 크기를 갖는 메시지 M 에 대한 데이터 암호화 전송 명령이 인가되면, 상기 거듭 행렬 G 및 상기 선정된 해시 함수와 함께 상기 비밀키로 저장되어 있는 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 기초로 상기 메시지 M 을 암호화하여 암호화 메시지 c 를 생성하는 단계 및 상기 암호화 메시지 c 를 데이터 수신 장치로 전송하는 단계를 포함한다.

발명의 효과

[0011] 본 발명에 따른 거듭 행렬(involutory matrix) 기반의 비밀키 암호화가 가능한 데이터 전송 장치 및 그 동작 방법은 거듭 행렬의 특성에 기반하여 설계된 비밀키를 기초로 메시지를 암호화해서 데이터 수신 장치로 전송함으로써, 상기 데이터 수신 장치가 상기 비밀키를 기초로 단순한 복호화 연산을 수행하는 방식으로 원본 데이터의 복원이 가능하도록 지원할 수 있어, 비교적 낮은 연산 성능을 갖는 기기들 간의 데이터 송수신시에도 높은 보안성을 제공할 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 발명의 일실시예에 따른 거듭 행렬(involutory matrix) 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 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.

[0014] 도 1은 본 발명의 일실시예에 따른 거듭 행렬(involutory matrix) 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 구조를 도시한 도면이다.

[0015] 도 1을 참조하면, 본 발명에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치(110)는 정보 저장부(111), 비밀키 저장부(112), 메시지 암호화부(113) 및 암호화 메시지 전송부(114)를 포함한다.

[0016] 정보 저장부(111)에는 $N \times N$ (여기서, N 은 4이상의 자연수) 크기의 '1'과 '0'의 코드 값으로 구성된 거듭 행렬(involutory matrix) G 와 선정된(predetermined) 해시 함수가 저장되어 있다.

[0017] 여기서, 거듭 행렬(involutory matrix)이란 자신과 자신의 역행렬이 동일한 행렬을 의미하는 것으로, $N \times N$ 크기의 거듭 행렬이 존재한다고 하였을 때, 하기의 수학식 1과 같은 조건을 만족하는 행렬을 의미한다.

수학식 1

$$GG = I_N$$

[0019]

[0021] 여기서, I_N 은 $N \times N$ 크기의 항등 행렬이다.

[0022] 이러한 거듭 행렬은 다음의 특성을 가지고 있다.

[0023] 우선, $N \times N$ 크기의 거듭 행렬 G 를 구성하는 N 개의 행들 각각과 N 개의 열들 각각의 인덱스 값을 순차적으로 '1, 2, 3, ..., N '이라고 가정하자.

[0024] 이때, 상기 거듭 행렬 G 를 구성하는 상기 N 개의 행들 중 K 개의 임의의 인덱스 값들에 대응하는 위치 상에 존재하는 K 개의 행들을 선택하여 상기 K 개의 행들 각각을 구성하는 N 개의 성분들만으로 구성된 $K \times N$ 크기의 부분 행렬을 R_k 라고 하자.

[0025] 그리고, 상기 거듭 행렬 G 를 구성하는 상기 N 개의 행들 중 상기 K 개의 인덱스 값들에 대응되지 않는 나머지 위

치 상에 존재하는 N-K개의 행들을 선택하여 상기 N-K개의 행들 각각을 구성하는 N개의 성분들만으로 구성된 (N-K) x N 크기의 부분 행렬을 R_A^c 라고 하자.

[0026] 그리고, 상기 거듭 행렬 G를 구성하는 N개의 열들 중 상기 K개의 인덱스 값들에 대응하는 위치 상에 존재하는 K개의 열들을 선택하여 상기 K개의 열들 각각을 구성하는 N개의 성분들만으로 구성된 N x K 크기의 부분 행렬을 C_A 라고 하자.

[0027] 마지막으로, 상기 거듭 행렬 G를 구성하는 N개의 열들 중 상기 K개의 인덱스 값들에 대응되지 않는 나머지 위치 상에 존재하는 N-K개의 열들을 선택하여 상기 N-K개의 열들 각각을 구성하는 N개의 성분들만으로 구성된 N x (N-K) 크기의 부분 행렬을 C_A^c 라고 하자.

[0028] 이때, R_A , R_A^c , C_A , C_A^c 에 대해서는 하기의 수학식 2와 같은 성질을 만족하게 된다.

수학식 2

$$\begin{aligned} R_A C_A &= I_K \\ R_A^c C_A &= 0_{(N-K) \times K} \\ R_A C_A^c &= 0_{K \times (N-K)} \\ R_A^c C_A^c &= I_{N-K} \end{aligned}$$

[0030]

[0032] 여기서, I_K 는 K x K 크기를 갖는 항등행렬, $0_{(N-K) \times K}$ 은 (N-K) x K 크기를 갖는 영행렬, $0_{K \times (N-K)}$ 는 K x (N-K) 크기를 갖는 영행렬, I_{N-K} 는 N-K 크기를 갖는 항등행렬을 의미한다.

[0033] 이러한 거듭 행렬 G는 상기 수학식 1과 상기 수학식 2를 만족하는 행렬로, 본 발명의 일실시예에 따르면, 정보 저장부(111) 상에 저장되는 상기 거듭 행렬 G는 극 부호(polar code)의 2 x 2 크기의 커널 행렬 F(여기서, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$)의 n-fold 크로네커 곱인 $F^{\otimes n}$ (여기서, $n = \log_2 N$)을 연산함으로써 생성할 수 있다.

[0034] 비밀키 저장부(112)는 K x K(여기서, K는 2이상 N미만의 크기를 갖는 자연수) 크기의 비특이(nonsingular) 랜덤 행렬을 생성하기 위해서 미리 지정된 시드(seed) 데이터와 N x N 크기의 '1'과 '0'의 코드 값으로 구성된 랜덤 순열 행렬 P 및 K개의 미리 지정된 인덱스 값들이 비밀키로 저장되어 있다.

[0035] 여기서, 상기 시드 데이터는 다음의 과정을 통해서 생성될 수 있다.

[0036] 우선, k 비트의 크기를 갖는 랜덤 벡터 L과 카운터 값 i를 연결한 데이터를 정보 저장부(111) 상에 저장되어 있는 상기 선정된 해시 함수에 입력으로 인가함으로써, 해시 값을 연산해 본다.

[0037] 이때, 상기 카운터 값 i를 '0'에서부터 '1'씩 증가시키면서 해시 값을 연산해보는데, 해시 값의 크기가 K^2 비트 이상이 되는지 확인해 본 후 해시 값의 크기가 K^2 비트 이상이 되지 않을 경우에 상기 카운터 값 i를 증가시키는 방식으로 해시 값의 연산을 반복 수행함으로써, K^2 비트 이상의 해시 값을 찾아낸다.

[0038] 이렇게, 해시 값이 찾아지면, 해시 값을 구성하는 '1'과 '0'의 각 비트 코드를 K x K 크기의 행렬의 각 성분으로 하나씩 배치시켜서 행렬을 생성한 후 해당 행렬의 역행렬의 존재 여부를 검사하게 된다.

[0039] 만약, 해당 행렬의 역행렬이 존재하는 경우에, 상기 카운터 값 i를 다시 증가시켜서 해시 값을 연산한 후 연산

된 해시 값을 기초로 행렬을 생성해 내고, 해당 행렬의 역행렬이 존재하는지 여부를 검사하는 방식의 과정을 반복 수행해서, 역행렬이 존재하지 않는 즉, 비특이 행렬이 나올 때까지 상기 과정을 반복 수행하여 최종 비특이 랜덤 행렬을 생성해 낸다.

- [0040] 이렇게, 최종적으로 비특이 랜덤 행렬의 생성이 완료되면, 해당 비특이 랜덤 행렬이 생성된 시점에서 사용된 상기 랜덤 벡터 L과 카운터 값 i를 상기 시드 데이터로 결정한 후 비밀키 저장부(112) 상에 상기 시드 데이터를 비밀키의 한 종류로 저장해 둘 수 있다.
- [0041] 메시지 암호화부(113)는 K비트의 크기를 갖는 메시지 M에 대한 데이터 암호화 전송 명령이 인가되면, 상기 거듭 행렬 G 및 상기 선정된 해시 함수와 함께 상기 비밀키로 저장되어 있는 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K개의 미리 지정된 인덱스 값들을 기초로 상기 메시지 M을 암호화하여 암호화 메시지 c를 생성한다.
- [0042] 이때, 본 발명의 일실시예에 따르면, 메시지 암호화부(113)는 비특이 랜덤 행렬 생성부(115), 제1 부분 행렬 생성부(116), 제2 부분 행렬 생성부(117), 랜덤 벡터 생성부(118) 및 암호화 연산 처리부(119)를 포함할 수 있다.
- [0043] 비특이 랜덤 행렬 생성부(115)는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 K x K 크기의 '1'과 '0'의 코드 값으로 구성된 비특이 랜덤 행렬 S를 생성한다.
- [0044] 관련해서, 앞서 설명한 바와 같이, 상기 시드 데이터는 상기 선정된 해시 함수에 입력으로 인가되었을 때, K²비트 이상의 크기를 갖는 해시 값이 생성되도록 지정된 입력 데이터이기 때문에, 비특이 랜덤 행렬 생성부(115)는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 K²비트 이상의 크기를 갖는 해시 값을 생성한 후 상기 해시 값을 구성하는 K²개 이상의 '1'과 '0'의 코드 값들을 K x K 크기의 행렬의 각 성분에 하나씩 순차적으로 배치함으로써, 상기 K x K 크기의 비특이 랜덤 행렬 S를 생성할 수 있다.
- [0045] 제1 부분 행렬 생성부(116)는 상기 거듭 행렬 G를 구성하는 N개의 행들 중 상기 K개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K개의 행들을 선택하여 상기 K개의 행들 각각을 구성하는 N개의 성분들만으로 구성된 K x N 크기의 제1 부분 행렬 R_A를 생성한다.
- [0046] 제2 부분 행렬 생성부(117)는 상기 거듭 행렬 G를 구성하는 N개의 행들 중 상기 K개의 미리 지정된 인덱스 값들에 대응되지 않는 위치 상에 존재하는 N-K개의 행들을 선택하여 상기 N-K개의 행들 각각을 구성하는 N개의 성분들만으로 구성된 (N-K) x N 크기의 제2 부분 행렬 R_A^c 를 생성한다.
- [0047] 랜덤 벡터 생성부(118)는 N-K의 크기를 갖는 랜덤 벡터 e를 생성한다.
- [0048] 암호화 연산 처리부(119)는 상기 비특이 랜덤 행렬 S, 상기 제1 부분 행렬 R_A, 상기 제2 부분 행렬 R_A^c , 상기 랜덤 벡터 e 및 상기 랜덤 순열 행렬 P를 기초로 상기 메시지 M에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c에 대한 생성을 처리한다.
- [0049] 이때, 본 발명의 일실시예에 따르면, 암호화 연산 처리부(119)는 하기의 수학식 3의 연산에 기초하여 상기 메시지 M에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c에 대한 생성을 처리할 수 있다.

수학식 3

$$c = (MSR_A \oplus eR_A^c)P$$

[0051]

- [0053] 여기서, ' $\oplus$ '은 배타적 논리합 연산을 의미하며, 본 발명에서 발생하는 행렬 연산에서의 합계는 모두 비트 연산에 대한 것으로 배타적 논리합 연산으로 수행된다.

- [0054] 이렇게, 상기 암호화 메시지 c 가 생성되면, 암호화 메시지 전송부(114)는 상기 암호화 메시지 c 를 데이터 수신 장치(120)로 전송한다.
- [0055] 이렇게, 데이터 수신 장치(120)로 상기 암호화 메시지 c 가 전송되면, 데이터 수신 장치(120)는 상기 암호화 메시지 c 로부터 원 메시지인 메시지 M 의 복원을 수행할 수 있는데, 데이터 수신 장치(120)가 상기 암호화 메시지 c 에 대해서 복호화를 수행하는 과정을 설명하면 다음과 같다.
- [0056] 우선, 데이터 수신 장치(120)는 메모리 상에 상기 거듭 행렬 G 와 상기 선정된 해시 함수를 저장하고 있음과 동시에 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 상기 비밀키로 저장하고 있다.
- [0057] 이때, 데이터 수신 장치(120)로 상기 암호화 메시지 c 가 수신되면, 데이터 수신 장치(120)는 상기 메모리 상에 저장되어 있는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성한 후 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 $K \times K$ 크기의 '1'과 '0'의 코드 값으로 구성된 상기 비특이 랜덤 행렬 S 를 생성할 수 있다.
- [0058] 관련해서, 상기 시드 데이터는 상기 선정된 해시 함수에 입력으로 인가되었을 때, K^2 비트 이상의 크기를 갖는 해시 값이 생성되도록 지정된 입력 데이터이기 때문에, 데이터 수신 장치(120)는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 K^2 비트 이상의 크기를 갖는 해시 값을 생성한 후 상기 해시 값을 구성하는 K^2 개 이상의 '1'과 '0'의 코드 값들을 $K \times K$ 크기의 행렬의 각 성분 하나씩 순차적으로 배치함으로써, 상기 $K \times K$ 크기의 비특이 랜덤 행렬 S 를 생성할 수 있다.
- [0059] 그리고, 데이터 수신 장치(120)는 상기 거듭 행렬 G 를 구성하는 N 개의 열들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K 개의 열들을 선택하여 상기 K 개의 열들 각각을 구성하는 N 개의 성분들만으로 구성된 $N \times K$ 크기의 제3 부분 행렬 C_A 를 생성할 수 있다.
- [0060] 그 이후, 데이터 수신 장치(120)는 상기 비특이 랜덤 행렬 S , 상기 제3 부분 행렬 C_A 및 상기 메모리 상에 저장되어 있는 상기 랜덤 순열 행렬 P 를 기초로 상기 암호화 메시지 c 에 대한 복호화 연산을 수행함으로써, 상기 메시지 M 을 복원할 수 있다.
- [0061] 이때, 본 발명의 일실시예에 따르면, 데이터 수신 장치(120)는 하기의 수학식 4의 연산에 기초하여 상기 암호화 메시지 c 에 대한 복호화 연산을 수행함으로써, 상기 메시지 M 을 복원할 수 있다.

수학식 4

$$M = cP^T C_A S^{-1}$$

[0063]

여기서, P^T 는 상기 랜덤 순열 행렬 P 의 전치 행렬, S^{-1} 은 상기 비특이 랜덤 행렬 S 의 역행렬이다.

[0066] 여기서, 상기 수학식 4의 연산 과정을 자세히 나타내면, 하기의 수학식 5와 같이 표현할 수 있다.

수학식 5

$$\begin{aligned} cP^T C_A S^{-1} &= ((MSR_A \oplus eR_A c)P)P^T C_A S^{-1} \\ &= (MSR_A P \oplus eR_A cP)P^T C_A S^{-1} \\ &= MSR_A PP^T C_A S^{-1} \oplus eR_A cPP^T C_A S^{-1} \end{aligned}$$

[0068]

[0070] 여기서, $PP^T = I$ 이기 때문에, 상기 수학식 5는 하기의 수학식 6과 같이 표현될 수 있다.

수학식 6

$$\begin{aligned} cP^T C_A S^{-1} &= MSR_A PP^T C_A S^{-1} \oplus eR_A cPP^T C_A S^{-1} \\ &= MSR_A C_A S^{-1} \oplus eR_A cC_A S^{-1} \end{aligned}$$

[0072]

[0074] 이때, 상기 거듭 행렬 G에 대해서는 상기 수학식 2에서 나타낸 바와 같은 성질에 따라, $R_A C_A = I_K$ 와 $R_A cC_A = 0_{(N-K) \times K}$ 을 만족하기 때문에, 상기 수학식 6은 하기의 수학식 7과 같이 표현될 수 있다.

수학식 7

$$\begin{aligned} cP^T C_A S^{-1} &= MSR_A C_A S^{-1} \oplus eR_A cC_A S^{-1} \\ &= MSI_K S^{-1} \\ &= MSS^{-1} \\ &= M \end{aligned}$$

[0076]

[0078] 이로 인해, 결국 데이터 수신 장치(120)는 상기 수학식 4에서 나타낸 연산을 수행함으로써, 원래 메시지인 메시지 M을 복원해 낼 수 있다.

[0079] 결국, 본 발명에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치(110)는 거듭 행렬의 특성에 기반하여 설계된 비밀키를 기초로 메시지를 암호화해서 데이터 수신 장치(120)로 전송함으로써, 데이터 수신 장치(120)가 상기 비밀키를 기초로 단순한 복호화 연산을 수행하는 방식으로 원본 데이터의 복원이 가능하도록 지원할 수 있어, 비교적 낮은 연산 성능을 갖는 기기들 간의 데이터 송수신시에도 높은 보안성을 제공할 수 있다.

[0080] 본 발명의 일실시예에 따르면, 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치(110)는 데이터 수신 장치(120)로 전송할 메시지가 K비트의 크기를 갖지 않는 메시지인 경우, K비트의 크기를 갖는 메시지로 만들기 위한 전처리 과정을 수행할 수 있다. 예컨대, K비트 크기 미만의 원본 메시지가 존재한다고 하였을 때, 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치(110)는 난수화 패딩 알고리즘인 OAEP(Optimal Asymmetric Encryption Padding) 알고리즘 등을 이용하여 원본 메시지에 소정의 데이터를 패딩함으로써, K비트 크기의 메시지로 만든 후 본 발명에 따른 거듭 행렬 기반의 비밀키 암호화 처리를 수행할 수 있다.

[0081] 도 2는 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법을 도시한 순서도이다.

[0082] 단계(S210)에서는 $N \times N$ (여기서, N은 4이상의 자연수) 크기의 '1'과 '0'의 코드 값으로 구성된 거듭 행렬 G와 선정된 해시 함수가 저장되어 있는 정보 저장부를 유지한다.

- [0083] 단계(S220)에서는 $K \times K$ (여기서, K 는 2이상 N 미만의 크기를 갖는 자연수) 크기의 비특이 랜덤 행렬을 생성하기 위해서 미리 지정된 시드 데이터와 $N \times N$ 크기의 '1'과 '0'의 코드 값으로 구성된 랜덤 순열 행렬 P 및 K 개의 미리 지정된 인덱스 값들이 비밀키로 저장되어 있는 비밀키 저장부를 유지한다.
- [0084] 단계(S230)에서는 K 비트의 크기를 갖는 메시지 M 에 대한 데이터 암호화 전송 명령이 인가되면, 상기 거듭 행렬 G 및 상기 선정된 해시 함수와 함께 상기 비밀키로 저장되어 있는 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 기초로 상기 메시지 M 을 암호화하여 암호화 메시지 c 를 생성한다.
- [0085] 단계(S240)에서는 상기 암호화 메시지 c 를 데이터 수신 장치로 전송한다.
- [0086] 이때, 본 발명의 일실시예에 따르면, 단계(S230)에서는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 $K \times K$ 크기의 '1'과 '0'의 코드 값으로 구성된 비특이 랜덤 행렬 S 를 생성하는 단계, 상기 거듭 행렬 G 를 구성하는 N 개의 행들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K 개의 행들을 선택하여 상기 K 개의 행들 각각을 구성하는 N 개의 성분들만으로 구성된 $K \times N$ 크기의 제1 부분 행렬 R_A 를 생성하는 단계, 상기 거듭 행렬 G 를 구성하는 N 개의 행들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응되지 않는 위치 상에 존재하는 $N-K$ 개의 행들을 선택하여 상기 $N-K$ 개의 행들 각각을 구성하는 N 개의 성분들만으로 구성된 $(N-K) \times N$ 크기의 제2 부분 행렬 R_{A^c} 를 생성하는 단계, $N-K$ 의 크기를 갖는 랜덤 벡터 e 를 생성하는 단계 및 상기 비특이 랜덤 행렬 S , 상기 제1 부분 행렬 R_A , 상기 제2 부분 행렬 R_{A^c} , 상기 랜덤 벡터 e 및 상기 랜덤 순열 행렬 P 를 기초로 상기 메시지 M 에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c 에 대한 생성을 처리하는 단계를 포함할 수 있다.
- [0087] 이때, 본 발명의 일실시예에 따르면, 상기 암호화 메시지 c 에 대한 생성을 처리하는 단계는 상기 수학식 3의 연산에 기초하여 상기 메시지 M 에 대한 암호화 연산을 수행함으로써, 상기 암호화 메시지 c 에 대한 생성을 처리할 수 있다.
- [0088] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 메모리 상에 상기 거듭 행렬 G 와 상기 선정된 해시 함수를 저장하고 있음과 동시에 상기 시드 데이터, 상기 랜덤 순열 행렬 P 및 상기 K 개의 미리 지정된 인덱스 값들을 상기 비밀키로 저장하고 있을 수 있다.
- [0089] 이때, 상기 데이터 수신 장치는 상기 암호화 메시지 c 가 수신되면, 상기 메모리 상에 저장되어 있는 상기 시드 데이터를 상기 선정된 해시 함수에 입력으로 인가하여 해시 값을 생성한 후 상기 해시 값을 구성하는 '1'과 '0'의 코드 값을 기초로 $K \times K$ 크기의 '1'과 '0'의 코드 값으로 구성된 상기 비특이 랜덤 행렬 S 를 생성하고, 상기 거듭 행렬 G 를 구성하는 N 개의 열들 중 상기 K 개의 미리 지정된 인덱스 값들에 대응하는 위치 상에 존재하는 K 개의 열들을 선택하여 상기 K 개의 열들 각각을 구성하는 N 개의 성분들만으로 구성된 $N \times K$ 크기의 제3 부분 행렬 C_A 를 생성할 수 있다.
- [0090] 그 이후, 상기 데이터 수신 장치는 상기 비특이 랜덤 행렬 S , 상기 제3 부분 행렬 C_A 및 상기 메모리 상에 저장되어 있는 상기 랜덤 순열 행렬 P 를 기초로 상기 암호화 메시지 c 에 대한 복호화 연산을 수행함으로써, 상기 메시지 M 을 복원할 수 있다.
- [0091] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 상기 수학식 4의 연산에 기초하여 상기 암호화 메시지 c 에 대한 복호화 연산을 수행함으로써, 상기 메시지 M 을 복원할 수 있다.
- [0092] 또한, 본 발명의 일실시예에 따르면, 상기 거듭 행렬 G 는 2×2 크기의 커널 행렬 F (여기서, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$)의 n -fold 크로네커 곱인 $F^{\otimes n}$ (여기서, $n = \log_2 N$)으로 연산되는 행렬로서 상기 수학식 1의 조건을 만족하는 행렬일 수 있다.
- [0093] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법은 도 1을 이용하여 설명한 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터

전송 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0094] 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0095] 또한, 본 발명의 일실시예에 따른 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치의 동작 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.

[0096] 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.

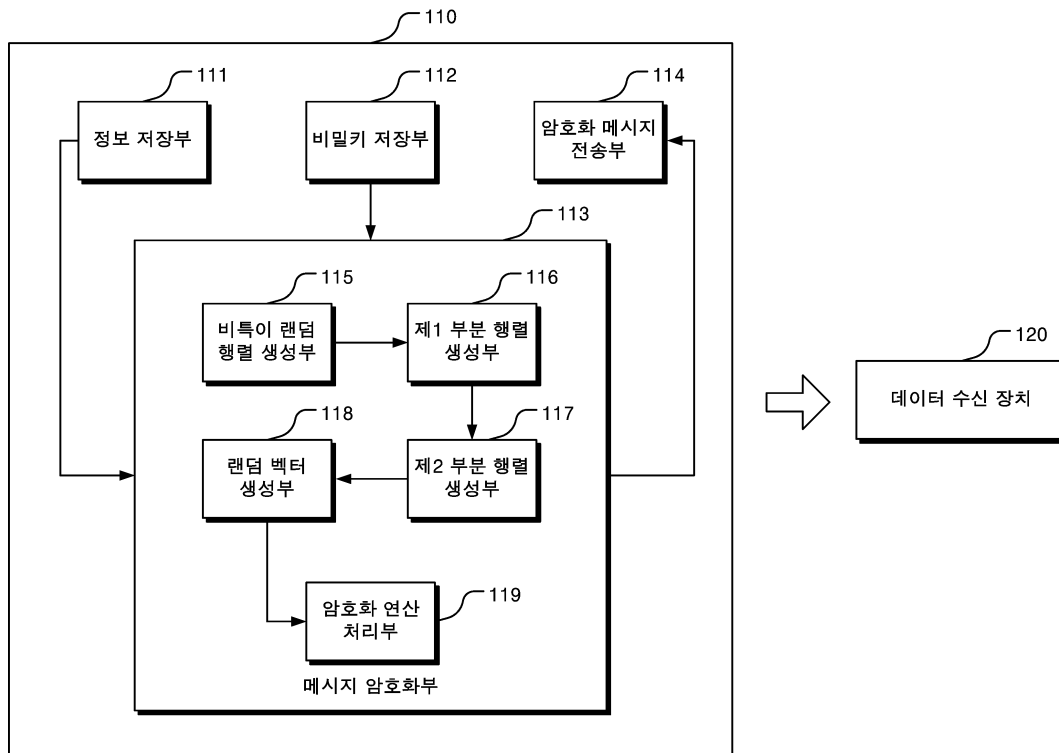
[0097] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0098] 110: 거듭 행렬 기반의 비밀키 암호화가 가능한 데이터 전송 장치
111: 정보 저장부 112: 비밀키 저장부
113: 메시지 암호화부 114: 암호화 메시지 전송부
115: 비특이 랜덤 행렬 생성부 116: 제1 부분 행렬 생성부
117: 제2 부분 행렬 생성부 118: 랜덤 벡터 생성부
119: 암호화 연산 처리부
120: 데이터 수신 장치

도면

도면1



도면2

