(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년12월14일
(11) 등록번호 10-1093359
(24) 등록일자 2011년12월06일

(51) Int. Cl.
H04L 9/12 (2006.01) *H04L 9/22* (2006.01)
(21) 출원번호 10-2009-7014694
(22) 출원일자(국제출원일자) 2007년12월14일
심사청구일자 2009년07월14일
(85) 번역문제출일자 2009년07월14일
(65) 공개번호 10-2009-0100399
(43) 공개일자 2009년09월23일
(86) 국제출원번호 PCT/US2007/087526
(87) 국제공개번호 WO 2008/076861
국제공개일자 2008년06월26일
(30) 우선권주장
11/611,827 2006년12월15일 미국(US)
(56) 선행기술조사문헌
US04979832 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
콸콤 인코포레이티드
미국 캘리포니아 샌디에고 모어하우스 드라이브5775 (우 92121-1714)
(72) 발명자
잰트맨, 알렉산더
미국 92121 캘리포니아 샌디에고 모어하우스 드라이브 5775
로즈, 그레고리, 고든
미국 92121 캘리포니아 샌디에고 모어하우스 드라이브 5775
(뒷면에 계속)
(74) 대리인
남상선

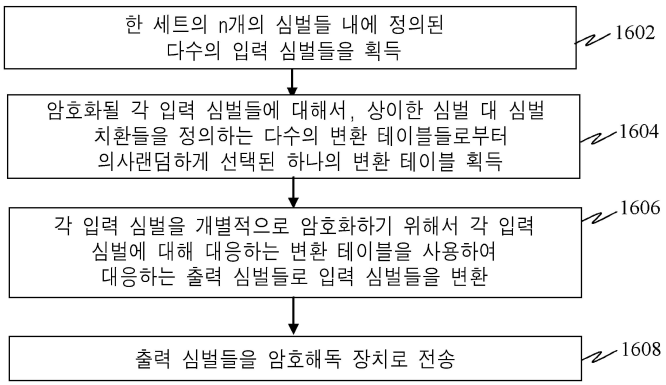
전체 청구항 수 : 총 31 항 심사관 : 양종필

(54) 조합 결합기 암호화 방법

(57) 요 약

본 발명은 암호화된 심벌들의 보안을 안전하게 하기 위한 효율적인 암호화 방법을 제공한다. 각 평문 심벌은 의사랜덤하게 선택된 개별적인 변환 테이블을 사용하여 암호화된다. 모든 가능한 심벌들의 치환을 변환 테이블로서 미리 저장하기 보다는, 변환 테이블은 의사랜덤 번호 및 심벌 셔플링 알고리즘에 기반하여 온-더-플라이 방식으로 효율적으로 생성될 수 있다. 수신 장치는 수신된 암호화된 심벌들을 암호해독하기 위해서 온-더-플라이 방식으로 역 변환 테이블들을 유사하게 생성할 수 있다.

대 표 도 - 도16



(72) 발명자

최, 재희

미국 92121 캘리포니아 샌디에고 모어하우스 드라이브 5775

뉴렌버그, 존, 더블유., 2세

미국 92121 캘리포니아 샌디에고 모어하우스 드라이브 5775

특허청구의 범위

청구항 1

암호화 장치상에서의 동작 방법으로서,

다수의 입력 심벌들을 획득하는 단계;

암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환(permutation)들을 정의하는 다수의 변환 테이블들 중 의사랜덤하게 선택된 변환 테이블을 획득하는 단계; 및

각 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하는 단계를 포함하며,

상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되며, 여기서 N은 양의 정수이고, 변환 테이블은 N개의 심벌들의 치환이며,

암호화될 입력 심벌들 각각에 대해 의사랜덤하게 선택된 변환 테이블을 획득하는 상기 단계는

암호화될 제1 입력 심벌에 대한 제1 의사랜덤 번호를 획득하는 단계; 및

N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대응되는 변환 테이블로서 상기 치환을 이용하는 단계를 포함하는, 동작 방법.

청구항 2

제1항에 있어서,

암호화될 입력 심벌들 각각에 대해 의사랜덤하게 선택된 변환 테이블을 획득하는 상기 단계는

제1 입력 심벌에 대해 의사랜덤하게 선택된 제1 변환 테이블을 획득하는 단계; 및

제2 입력 심벌에 대해 의사랜덤하게 선택된 제2 변환 테이블을 획득하는 단계를 포함하며,

입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하는 상기 단계는

상기 제1 변환 테이블을 사용하여 상기 제1 입력 심벌을 제1 출력 심벌로 변환하는 단계; 및

상기 제2 변환 테이블을 사용하여 상기 제2 입력 심벌을 제2 출력 심벌로 변환하는 단계를 포함하는, 동작 방법.

청구항 3

삭제

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 제1 의사랜덤 번호는

상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고;

상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜

덤 번호들을 획득하고; 그리고

상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나눔으로써 획득되는, 동작 방법.

청구항 6

제1항에 있어서,

N개의 심벌들 세트를 셔플링하는 상기 단계는

N개의 심벌들 세트의 모든 심벌들로 치환 벡터 P를 초기화하는 단계; 및

상기 제1 의사랜덤 번호에 기반하여 상기 치환 벡터에서 심벌들을 셔플링하는 단계를 포함하는, 동작 방법.

청구항 7

제1항에 있어서,

상기 출력 심벌들을 암호해독 장치로 전송하는 단계를 더 포함하는, 동작 방법.

청구항 8

제1항에 있어서,

암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들 중에서 의사랜덤하게 선택된 제2 변환 테이블을 획득하는 단계; 및

각 입력 심벌을 추가적으로 개별적으로 암호화하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하는 단계를 더 포함하는, 동작 방법.

청구항 9

암호화 장치로서,

다수의 입력 심벌들을 획득하기 위한 수단;

암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환(permutation)을 정의하는 다수의 변환 테이블들 중 의사랜덤하게 선택된 변환 테이블을 획득하기 위한 수단;

각 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하기 위한 수단;

암호화될 제1 입력 심벌에 대한 제1 의사랜덤 번호를 획득하기 위한 수단; 및

N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대응되는 변환 테이블로서 상기 치환을 이용하기 위한 수단을 포함하는, 암호화 장치.

청구항 10

제9항에 있어서,

제1 입력 심벌에 대해 의사랜덤하게 선택된 제1 변환 테이블을 획득하기 위한 수단;

제2 입력 심벌에 대해 의사랜덤하게 선택된 제2 변환 테이블을 획득하기 위한 수단;

상기 제1 변환 테이블을 사용하여 상기 제1 입력 심벌을 제1 출력 심벌로 변환하기 위한 수단; 및

상기 제2 변환 테이블을 사용하여 상기 제2 입력 심벌을 제2 출력 심벌로 변환하기 위한 수단을 더 포함하는, 암호화 장치.

청구항 11

삭제

청구항 12

제9항에 있어서,

상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하기 위한 수단 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하기 위한 수단 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리기 위한 수단;

상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하기 위한 수단; 및

상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누는 수단을 더 포함하는, 암호화 장치.

청구항 13

제9항에 있어서,

상기 출력 심벌들을 암호해독 장치로 전송하는 수단을 더 포함하는, 암호화 장치.

청구항 14

제9항에 있어서,

암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들 중에서 의사랜덤하게 선택된 제2 변환 테이블을 획득하기 위한 수단; 및

각 입력 심벌을 추가적으로 개별적으로 암호화하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하기 위한 수단을 더 포함하는, 암호화 장치.

청구항 15

암호화 장치로서,

입력 심벌 스트림을 수신하기 위한 입력 인터페이스;

상기 입력 인터페이스에 연결된 처리 회로로서, 상기 처리회로는 상기 입력 인터페이스로부터 다수의 입력 심벌들을 획득하고; 암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환(permutation)을 정의하는 다수의 변환 테이블들 중 의사랜덤하게 선택된 변환 테이블을 획득하고; 그리고 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하도록 구성되는, 처리 회로;

상기 처리 회로에 연결되며, 암호화될 제1 입력 심벌에 대한 키 스트림 생성기로부터 제1 의사 랜덤 번호를 획득하도록 구성된 키 스트림 생성기; 및

상기 처리 회로에 연결되며, N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대한 변환 테이블로서 상기 치환을 사용하도록 구성된 변환 테이블 생성기를 포함하는, 암호화 장치.

청구항 16

제15항에 있어서,

상기 출력 심벌들을 전송하기 위해 상기 처리 회로에 연결된 출력 인터페이스를 더 포함하는, 암호화 장치.

청구항 17

제15항에 있어서,

상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되며, 여기서 N은 양의 정수이고, 변환 테이블은 N개의 심벌들의 치환인, 암호화 장치.

청구항 18

삭제

청구항 19

제17항에 있어서,

상기 처리 회로는

제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고;

상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하고; 그리고

상기 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누도록 더 구성되는, 암호화 장치.

청구항 20

제17항에 있어서,

상기 처리 회로는

암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들 중에서 의사랜덤하게 선택된 제2 변환 테이블을 획득하고; 및

각 입력 심벌을 추가적으로 개별적으로 암호화하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하도록 더 구성되는, 암호화 장치.

청구항 21

프로세서에 의해 실행되는 경우, 프로세서로 하여금

다수의 입력 심벌들을 획득하게 하고;

암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환(permutation)을 정의하는 다수의 변환 테이블들 중 의사랜덤하게 선택된 변환 테이블을 획득하게 하고;

입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하게 하고;

암호화될 제1 입력 심벌에 대한 제1 의사랜덤 번호를 획득하게 하고; 그리고

N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대한 상기 변환 테이블로서 상기 치환을 이용하도록 하는,

심벌 암호화를 위한 하나 이상의 명령들을 갖는 프로그램을 저장하기 위한 컴퓨터로 읽을 수 있는 매체.

청구항 22

제21항에 있어서,

상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되며, 여기서 N은 양의 정수이고, 변환 테이블은 N개의 심벌들의 치환인, 컴퓨터로 읽을 수 있는 매체.

청구항 23

삭제

청구항 24

제22항에 있어서,

프로세서에 의해 실행되는 경우, 프로세서로 하여금

제1 입력 심벌에 대한 의사랜덤 번호를 생성하게 하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하게 하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리게 하고;

상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하게 하고; 그리고

상기 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누게 하는 하나 이상의 명령들을 더 포함하는, 컴퓨터로 읽을 수 있는 매체.

청구항 25

제21항에 있어서,

프로세서에 의해 실행되는 경우, 프로세서로 하여금

암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들 중에서 의사랜덤하게 선택된 제2 변환 테이블을 획득하게 하고; 그리고

각 입력 심벌을 추가적으로 개별적으로 암호화하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하게 하는 하나 이상의 명령들을 더 포함하는, 컴퓨터로 읽을 수 있는 매체.

청구항 26

심벌들을 암호해독하기 위한 방법으로서,

N개의 심벌들 세트 내에 정의된 다수의 입력 심벌들을 획득하는 단계;

암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중 의사랜덤하게 선택된 역 변환 테이블을 획득하는 단계; 및

각 입력 심벌을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하는 단계를 포함하며,

상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이며, 상기 방법은

암호해독될 제1 입력 심벌에 대한 제1 의사 랜덤 번호를 획득하는 단계; 및

N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대한 상기 역 변환 테이블로서 상기 치환을 이용하는 단계를 더 포함하는, 암호해독 방법.

청구항 27

삭제

청구항 28

제26항에 있어서,

상기 제1 의사랜덤 번호는

상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고;

상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하고; 그리고

상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나눔으로써 획득되는, 암호해독 방법.

청구항 29

제26항에 있어서,

암호해독될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중에서 의사랜덤하게 선택된 제2 역 변환 테이블을 획득하는 단계; 및

각 입력 심벌을 추가적으로 개별적으로 암호해독 하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 역 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하는 단계를 더 포함하는, 암호해독 방법.

청구항 30

암호해독 장치로서,

N개의 심벌들 세트 내에 정의된 다수의 입력 심벌들을 획득하기 위한 수단;

암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중 의사랜덤하게 선택된 역 변환 테이블을 획득하기 위한 수단; 및

각 입력 심벌을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하기 위한 수단을 포함하며,

상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이며, 상기 장치는

암호해독될 제1 입력 심벌에 대한 제1 의사 랜덤 번호를 획득하기 위한 수단; 및

N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대한 상기 역 변환 테이블로서 상기 치환을 이용하는 수단을 더 포함하는, 암호해독 장치.

청구항 31

삭제

청구항 32

제30항에 있어서,

상기 제1 의사랜덤 번호는

상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하기 위한 수단 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하기 위한 수단 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리기 위한 수단;

상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하기 위한 수단; 및

상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누기 위한 수단에 의해 획득되는, 암호해독 장치.

청구항 33

제30항에 있어서,

암호해독될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중에서 의사랜덤하게 선택된 제2 역 변환 테이블을 획득하기 위한 수단; 및

각 입력 심벌을 추가적으로 개별적으로 암호해독 하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 역 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하기 위한 수단을 더 포함하는, 암호해독 장치.

청구항 34

암호해독 장치로서,

입력 심벌 스트림을 수신하기 위한 입력 인터페이스; 및

상기 입력 인터페이스에 연결된 처리 회로를 포함하며,

상기 처리 회로는

N개의 심벌들 세트 내에 정의된 다수의 입력 심벌들을 획득하고;

암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중 의사랜덤하게 선택된 역 변환 테이블을 획득하고; 그리고

각 입력 심벌을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하도록 구성되며,

상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이며, 상기 장치는

상기 처리 회로에 연결되며, 암호해독될 제1 입력 심벌에 대한 키 스트림 생성기로부터 제1 의사 랜덤 번호를 획득하도록 구성된 키 스트림 생성기; 및

상기 처리 회로에 연결되며, N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대한 역 변환 테이블로서 상기 치환을 사용하도록 구성된 역 변환 테이블 생성기를 더 포함하는, 암호해독 장치.

청구항 35

삭제

청구항 36

제34항에 있어서,

상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이며, 상기 처리 회로는

제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ;

상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고;

상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하고; 그리고

상기 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누도록 더 구성되는, 암호해독 장치.

청구항 37

제34항에 있어서,

상기 처리 회로는

암호해독될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중에서 의사랜덤하게 선택된 제2 역 변환 테이블을 획득하고; 그리고

각 입력 심벌을 추가적으로 개별적으로 암호해독 하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 역 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하도록 더 구성되는, 암호해독 장치.

청구항 38

프로세서에 의해 실행되는 경우, 프로세서로 하여금

N개의 심벌들 세트 내에 정의된 다수의 입력 심벌들을 획득하게 하고 - 여기서, 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환임 -;

암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중 의사랜덤하게 선택된 역 변환 테이블을 획득하게 하고;

각 입력 심벌을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하고;

암호해독될 제1 입력 심벌에 대한 제1 의사 랜덤 번호를 획득하게 하고; 그리고

N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대한 상기 역 변환 테이블로서 상기 치환을 이용하게 하는,

심벌들을 암호해독하기 위한 하나 이상의 명령들을 포함하는 프로그램을 저장하기 위한 컴퓨터로 읽을 수 있는 매체.

청구항 39

삭제

청구항 40

제38항에 있어서,

프로세서에 의해 실행되는 경우, 프로세서로 하여금

암호해독될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중에서 의사랜덤하게 선택된 제2 역 변환 테이블을 획득하게 하고; 그리고

각 입력 심벌을 추가적으로 개별적으로 암호해독 하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 역 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하게 하는 하나 이상의 명령들을 더 포함하는, 컴퓨터로 읽을 수 있는 매체.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 보안 통신에 관한 것으로서, 특히 변환 테이블들을 효율적으로 생성함으로써 심벌들을 안전하게 보호하는 스트림 암호화 방법에 관한 것이다.

배 경 기 술

[0002] 스트림 암호화는 일반적으로 의사랜덤 번호들의 키 스트림을 생성하고, 이들을 평문 심벌들과 결합함으로써 암호화된 출력 또는 암호화문을 생성한다. 일반적으로, 이진 키 스트림 심벌들 및 이진 평문 심벌들은 배타적-OR(XOR) 연산을 사용하여 비트 단위로 조합되는데, 왜냐하면 배타적-OR(XOR) 연산이 셀프-인버시브(self-inversive) 특성이 있기 때문이다. 그러나 평문 심벌들에 대한 비트-단위 암호화를 수행하기 보다는, 전체 평문 심벌을 암호화하는 것이 종종 바람직하다. 따라서, XOR 연산을 사용될 수 없다. 일반적으로, 평문 심벌이 키 스트림 심벌 모듈로 n에 추가되어 암호화문 심벌을 획득한다. 하지만, 특정 심벌의 위치를 파악한 활성 공격자는 전송된 암호화문 심벌로부터 감산함으로써 그 심벌을 변경할 수 있다. 예를 들어, 한 세트의 평문 디지트(0 내지 9)는 키스트림 모듈로 10으로부터 의사랜덤하게 생성된 디지트(0 내지 9)에 각 디지트를 더함으로써 암호화될 수 있다. 그러나 특정 평문에 대해 디지트가 "1"이었지만, 출력 암호화문 디지트가 "7"임을 알고 있는 공격자는 키 스트림 디지트가 "6"임을 결정하고, 그 특정 심벌 위치에 대해 그들이 선택한 임의의 다른 디지트를 정확하게 암호화할 수 있다. 공격자는 평문 심벌 및 키 스트림 심벌들이 조합되는 방식을 결정할 수 있기 때문에, 이러한 부분적인 암호해독은 나머지 암호화된 정보에 대한 보안을 약화시킨다. 즉, 암호화문 심벌과 평문 심벌 사이의 관계가 노출되면, 나머지 암호화문 심벌들에 대한 보안이 훼손되는데, 왜냐하면 그 정보를 통해 공격자는 다른 암호화문 심벌들을 해독할 수 있기 때문이다. 또한, 간단한 수학 연산(예를 들며, 가산, 감산, 승산 등)은 평문 심벌 및 키 스트림 심벌을 쉽고 효율적으로 결합하지만, 보다 복잡한 수학 함수를 사용하는 것은 암호화에 있어서 상당한 지연을 초래하고 보다 큰 처리 자원들을 필요로 한다.

[0003] 따라서, 하나의 암호화 심벌이 노출되고 깨지더라도 다른 심벌들의 보안을 약화시키지 않는 효율적인 암호화 방법이 요구된다.

발명의 상세한 설명

[0004] 데이터를 안전하게 보호하기 위해 암호화 장치에서 동작하는 방법이 제공된다. 다수의 입력 심벌들이 암호화 장치에 의해 획득된다. 암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들로부터 의사랜덤하게 선택된 변환 테이블이 획득된다. 입력 심벌들은 각 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 변환 테이블을 사용하여 대응하는 출력 심벌들로 변환된다. 출력 심벌들은 암호화 장치로 전송된다.

[0005] 또한, 암호화될 입력 심벌들 각각에 대해 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들로부터 의사랜덤하게 선택된 제2 변환 테이블이 획득된다. 출력 심벌들은 입력 심벌 각각을 추가적으로 개별적으로 암호화하기 위해서 출력 심벌들 각각에 대해 그들의 대응하는 제2 변환 테이블을 사용하여 대응하는 제2 출력 심벌들로 변환된다.

[0006] 일 예에서, 암호화될 입력 심벌들 각각에 대해 의사랜덤하게 선택된 변환 테이블을 획득하는 단계는 (a) 제1 입력 심벌에 대해 의사랜덤하게 선택된 제1 변환 테이블을 획득하는 단계; 및/또는(b) 제2 입력 심벌에 대해 의사랜덤하게 선택된 제2 변환 테이블을 획득하는 단계를 포함한다. 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하는 단계는 (a) 상기 제1 변환 테이블을 사용하여 상기 제1 입력 심벌을 제1 출력 심벌로 변환하는 단계; 및/또는(b) 상기 제2 변환 테이블을 사용하여 상기 제2 입력 심벌을 제2 출력 심벌로 변환하는 단계를 포함한다. 여기서 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되며, 여기서 N은 양의 정수이고, 변환 테이블은 N개의 심벌들의 치환이다.

[0007] 다른 실시예에서, 암호화될 입력 심벌들 각각에 대해 의사랜덤하게 선택된 변환 테이블을 획득하는 단계는 (a) 암호화될 제1 입력 심벌에 대한 제1 의사랜덤 번호를 획득하는 단계; 및/또는(b) N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대해 상기 변환 테이블로서 상기 치환을 이용하는 단계를 포함한다.

[0008] 이 구현에서, 제1 의사랜덤 번호는 (a) 상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기

의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ; (b) 상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ; (c) 상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고; (d) 상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하고; 그리고/또는 (e) 상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나눔으로써 획득된다. N개의 심벌들 세트를 셔플링하는 단계는 (a) N개의 심벌들 세트의 모든 심벌들로 치환 벡터 P를 초기화하는 단계; 및/또는 (b) 상기 제1 의사랜덤 번호에 기반하여 상기 치환 벡터에서 심벌들을 셔플링하는 단계를 포함한다.

[0009] 입력 인터페이스 및 처리 회로를 포함하는 암호화 장치가 또한 제공된다. 상기 입력 장치는 입력 심벌 스트림을 수신하는 기능을 수행한다. 상기 처리 회로는 (a) 상기 입력 인터페이스로부터 다수의 입력 심벌들을 획득하고; (b) 암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환(permutation)을 정의하는 다수의 변환 테이블들 중 의사랜덤하게 선택된 변환 테이블을 획득하고; 그리고/또는(c) 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하도록 구성된다. 상기 암호화 장치는 상기 출력 심벌들을 전송하기 위해 상기 처리 회로에 연결된 출력 인터페이스를 포함할 수 있다.

[0010] 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되며, 여기서 N은 양의 정수이고, 변환 테이블은 N개의 심벌들의 치환이다. 상기 암호화 장치는 또한 (a) 상기 처리 회로에 연결되며, 암호화될 제1 입력 심벌에 대한 키 스트림 생성기로부터 제1 의사 랜덤 번호를 획득하도록 구성된 키 스트림 생성기; 및/또는(b) 상기 처리 회로에 연결되며, N개의 심벌들 세트의 상이한 치환을 획득하고, 상기 제1 심벌에 대한 변환 테이블로서 상기 치환을 사용하기 위해서 N개의 심벌들 세트를 셔플링하도록 구성된 변환 테이블 생성기를 더 포함할 수 있다.

[0011] 일 예에서, 상기 처리 회로는 (a)상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ; (b) 상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ; (c)상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고; (d) 상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하고; 그리고/또는 (e) 상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누도록 더 구성될 수 있다.

[0012] 일 구현에서, 암호화 장치의 처리 회로는 또한 (a)암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들 중에서 의사랜덤하게 선택된 제2 변환 테이블을 획득하고; 및/또는(b) 각 입력 심벌을 추가적으로 개별적으로 암호화하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하도록 더 구성될 수 있다.

[0013] 결과적으로, (a) 다수의 입력 심벌들을 획득하기 위한 수단; (b) 암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환(permutation)을 정의하는 다수의 변환 테이블들 중 의사랜덤하게 선택된 변환 테이블을 획득하기 위한 수단; (c) 각 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하기 위한 수단; 및/또는 (d) 상기 출력 심벌들을 암호해독 장치로 전송하는 수단을 포함하는 암호화 장치가 제공된다. 상기 암호화 장치는 또한 (a) 암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들 중에서 의사랜덤하게 선택된 제2 변환 테이블을 획득하기 위한 수단; 및/또는(b) 각 입력 심벌을 추가적으로 개별적으로 암호화하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하기 위한 수단을 더 포함할 수 있다.

[0014] 일 구현에서, 상기 암호화 장치는 (a) 제1 입력 심벌에 대해 의사랜덤하게 선택된 제1 변환 테이블을 획득하기 위한 수단; (b) 제2 입력 심벌에 대해 의사랜덤하게 선택된 제2 변환 테이블을 획득하기 위한 수단; (c) 상기 제1 변환 테이블을 사용하여 상기 제1 입력 심벌을 제1 출력 심벌로 변환하기 위한 수단; 및/또는(d) 상기 제2 변환 테이블을 사용하여 상기 제2 입력 심벌을 제2 출력 심벌로 변환하기 위한 수단을 포함할 수 있다.

[0015] 일 예에서, 상기 암호화 장치는 또한 (a) 암호화될 제1 입력 심벌에 대한 제1 의사랜덤 번호를 획득하기 위한 수단; 및/또는(b) N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기

제1 입력 심벌에 대해 상기 변환 테이블로서 상기 치환을 이용하기 위한 수단을 포함할 수 있다.

[0016] 프로세서에 의해 실행되는 경우, 프로세서로 하여금 (a) 다수의 입력 심벌들을 획득하게 하고; (b) 암호화될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환(permutation)을 정의하는 다수의 변환 테이블들 중 의사랜덤하게 선택된 변환 테이블을 획득하게 하고; 그리고/또는(c) 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하게 하도록 하는, 심벌 암호화를 위한 하나 이상의 명령들을 포함하는 기계-판독가능한 매체가 제공된다. 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되며, 여기서 N은 양의 정수이고, 변환 테이블은 N개의 심벌들의 치환이다.

[0017] 상기 기계 판독가능한 매체는 프로세서에 의해 실행되는 경우, 프로세서로 하여금 (a) 암호화될 제1 입력 심벌에 대한 제1 의사랜덤 번호를 획득하게 하고; 및/또는(b) N개의 심벌들 세트의 상이한 치환을 획득하고, 상기 제1 입력 심벌에 대해 상기 변환 테이블로서 상기 치환을 이용하기 위해서 N개의 심벌들 세트를 셔플링하도록 하는 하나 이상의 명령들을 더 포함할 수 있다.

[0018] 일 구현에서, 상기 기계 판독가능한 매체는 프로세서에 의해 실행되는 경우, 프로세서로 하여금 (a) 상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하게 하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ; (b) 상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하게 하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ; (c) 상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리게 하고; (d) 상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하게 하고; 그리고/또는(e) 상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누게 하는 하나 이상의 명령들을 더 포함할 수 있다.

[0019] 심벌들을 암호해독하기 위한 방법이 또한 제공된다. n개의 심벌들 세트 내에 정의된 다수의 입력 심벌들이 획득된다. 암호해독될 입력 심벌들 각각에 대해 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들로부터 의사랜덤하게 선택된 변환 테이블이 선택된다. 그리고 나서, 입력 심벌들은 입력 심벌 각각각을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대해 그들의 대응하는 역 변환 테이블을 사용하여 대응하는 출력 심벌들로 변환된다. 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이다. 상기 방법은 또한 (a) 암호해독될 제1 입력 심벌에 대한 제1 의사 랜덤 번호를 획득하는 단계; 및/또는(b) N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대해 상기 역 변환 테이블로서 상기 치환을 이용하는 단계를 더 포함할 수 있다.

[0020] 일 예에서, 상기 제1 의사랜덤 번호는 (a) 상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ; (b) 상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ; (c) 상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고; (d) 상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하고; 그리고/또는(e) 상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나눔으로써 획득될 수 있다.

[0021] 다른 구현에서, 상기 방법은 (a) 암호해독될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중에서 의사랜덤하게 선택된 제2 역 변환 테이블을 획득하는 단계; 및/또는(b) 각 입력 심벌을 추가적으로 개별적으로 암호해독 하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 역 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하는 단계를 더 포함할 수 있다.

[0022] 입력 인터페이스 및 처리 회로를 포함하는 암호해독 장치가 제공된다. 상기 입력 인터페이스는 입력 심벌 스트림을 수신한다. 상기 처리 회로는 (a) N개의 심벌들 세트 내에 정의된 다수의 입력 심벌들을 획득하고; (b) 암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중 의사랜덤하게 선택된 역 변환 테이블을 획득하고; 그리고/또는(c) 각 입력 심벌을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하도록 구성된다.

[0023] 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N

개의 심벌들의 치환이다. 상기 암호해독 장치는 (a)상기 처리 회로에 연결되며, 암호해독될 제1 입력 심벌에 대한 키 스트림 생성기로부터 제1 의사 랜덤 번호를 획득하도록 구성된 키 스트림 생성기; 및/또는(b) 상기 처리 회로에 연결되며, N개의 심벌들 세트의 상이한 치환을 획득하고, 상기 제1 심벌에 대한 역 변환 테이블로서 상기 치환을 사용하기 위해서 N개의 심벌들 세트를 셔플링하도록 구성된 역 변환 테이블 생성기를 더 포함할 수 있다.

[0024] 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이다. 상기 처리 회로는 (a) 상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하고 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ; (b) 상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하고 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ; (c) 상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리고; (d) 상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하고; 그리고/또는(e) 상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누도록 더 구성될 수 있다.

[0025] 다른 예에서, 처리 회로는 (a) 암호해독될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중에서 의사랜덤하게 선택된 제2 역 변환 테이블을 획득하고; 그리고/또는(b) 각 입력 심벌을 추가적으로 개별적으로 암호해독 하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 역 변환 테이블을 사용하여 출력 심벌들을 대응하는 제2 출력 심벌들로 변환하도록 더 구성될 수 있다.

[0026] 결과적으로, (a) N개의 심벌들 세트 내에 정의된 다수의 입력 심벌들을 획득하기 위한 수단; (b) 암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중 의사랜덤하게 선택된 역 변환 테이블을 획득하기 위한 수단; 및/또는(c) 각 입력 심벌을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하기 위한 수단을 포함하는 암호해독 장치가 제공된다. 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이다. 상기 암호해독 장치는 (a) 암호해독될 제1 입력 심벌에 대한 제1 의사 랜덤 번호를 획득하기 위한 수단; 및/또는(b) N개의 심벌들 세트의 상이한 치환을 획득하기 위해서 N개의 심벌들 세트를 셔플링하고, 상기 제1 입력 심벌에 대해 상기 역 변환 테이블로서 상기 치환을 이용하는 수단을 더 포함할 수 있다. 상기 제1 의사랜덤 번호는 (a) 상기 제1 입력 심벌에 대한 의사랜덤 번호를 생성하기 위한 수단 - 여기서, 상기 의사랜덤 번호는 k비트 길이를 가지며, k는 양의 정수임 - ; (b) 상기 의사랜덤 번호가 최대수 Pmax 내에 존재하는지 여부를 결정하기 위한 수단 - 여기서, Pmax는 최대 임계치 2^k 보다 작은 N!(팩토리얼)의 가장 큰 배수임 - ; (c) 상기 의사랜덤 번호가 최대수 Pmax 보다 크면, 상기 의사랜덤 번호를 버리기 위한 수단; (d) 상기 최대수 Pmax 이하인 수용가능한 의사랜덤 번호가 획득될 때까지 상기 제1 입력 심벌에 대한 상이한 의사랜덤 번호들을 획득하기 위한 수단; 및/또는(e) 상기 제1 의사랜덤 번호를 획득하기 위해서 상기 수용가능한 의사랜덤 번호를 모듈로 N!(팩토리얼)로 나누기 위한 수단에 의해 획득된다.

[0027] 프로세서에 의해 실행되는 경우, 프로세서로 하여금 (a) N개의 심벌들 세트 내에 정의된 다수의 입력 심벌들을 획득하게 하고; (b) 암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중 의사랜덤하게 선택된 역 변환 테이블을 획득하게 하고; 그리고/또는(c) 각 입력 심벌을 개별적으로 암호해독하기 위해서 입력 심벌들 각각에 대한 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환하게 하는, 심벌들을 암호해독하기 위한 하나 이상의 명령들을 포함하는, 기계 판독가능한 매체가 제공된다. 상기 다수의 입력 심벌들은 N개의 심벌들 세트에 의해 정의되고, 여기서 N은 양의 정수이며 역 변환 테이블은 N개의 심벌들의 치환이다.

[0028] 상기 기계 판독가능한 매체는 프로세서에 의해 실행되는 경우, 프로세서로 하여금 (a) 암호해독될 제1 입력 심벌에 대한 제1 의사 랜덤 번호를 획득하게 하고; 그리고/또는(b) N개의 심벌들 세트의 상이한 치환을 획득하고, 상기 제1 입력 심벌에 대해 상기 역 변환 테이블로서 상기 치환을 이용하기 위해 N개의 심벌들 세트를 셔플링하게 하는 하나 이상의 명령들을 더 포함할 수 있다.

[0029] 다른 예에서, 상기 기계 판독가능한 매체는 프로세서에 의해 실행되는 경우, 프로세서로 하여금 (a) 암호해독될 입력 심벌들 각각에 대해, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들 중에서 의사랜덤하게 선택된 제2 역 변환 테이블을 획득하게 하고; 그리고/또는(b) 각 입력 심벌을 추가적으로 개별적으로 암호해독 하기 위해서 상기 출력 심벌들 각각에 대해 그들의 대응하는 제2 역 변환 테이블을 사용하여 출력 심벌들을

대응하는 제2 출력 심벌들로 변환하게 하는 하나 이상의 명령들을 더 포함할 수 있다.

실 시 예

[0050] 다음 설명에서, 특정 설명들은 본 발명의 실시예에 대한 보다 상세한 이해를 제공하기 위해서 제시된다. 그러나 당업자는 본 발명이 이러한 특정 설명 없이도 실행될 수 있음을 잘 이해할 수 있을 것이다. 예를 들어, 회로들은 불필요한 설명으로 인해 본 발명의 본질을 희석하는 것을 방지하기 위해서 블록도에서 제시되지 않을 수도 있다.

[0051] 또한, 본 실시예들은 흐름도, 흐름 다이아그램, 구조 다이아그램, 또는 블록 다이아그램과 같은 제시되는 처리 단계로서 제시될 수 있다. 비록 흐름도가 순차적인 단계의 동작으로 제시되지만, 이러한 동작들은 병렬적으로 또는 동시에 수행될 수 있다. 또한, 동작 순서는 재배열될 수 있다. 그 동작이 완료될 때, 이러한 처리는 종료된다. 이러한 처리는 방법, 함수, 프로시져, 서브루틴, 서브프로그램 등에 대응할 수 있다. 처리가 함수에 대응하는 경우, 그 종료는 호출 함수 또는 메인 함수로 이러한 함수의 리턴에 대응한다.

[0052] 또한, 저장 매체는 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 자기 디스크 저장 매체, 광학 저장 매체, 플래쉬 메모리 장치, 및/또는 정보 저장을 위한 다른 기계 판독가능한 매체들을 포함하는 하나 이상의 데이터 저장 장치를 나타낸다. 용어 "기계 판독가능한 매체"는 휴대용 또는 고정 저장 장치, 광학 저장 장치, 무선 채널, 및 명령(들) 및/또는 데이터를 저장, 포함, 또는 전달할 수 있는 다양한 다른 매체들을 포함하지만, 이들로 제한되는 것은 아니다.

[0053] 또한, 다양한 구성들이 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 또는 이들의 조합에 의해 구현될 수 있다. 소프트웨어, 펌웨어, 미들웨어, 또는 마이크로코드로 구현되는 경우, 제시된 임무들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들은 저장 매체 또는 다른 저장 수단과 같은 기계-판독가능한 매체에 저장될 수 있다. 프로세서는 정의된 임무를 수행할 수 있다. 코드 세그먼트는 프로시져, 함수, 서브루틴, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령, 데이터 구조, 또는 프로그램 세그먼트들의 조합을 나타낸다. 코드 세그먼트는 정보, 데이터, 인수, 파라미터, 또는 메모리 컨텐츠를 전달 및/또는 수신함으로써 하드웨어 회로에 연결되거나, 다른 코드 세그먼트에 연결될 수 있다. 정보, 인수, 파라미터, 데이터 등은 메모리 공유, 메모리 전달, 토큰 전달, 및 네트워크 전송을 포함하는 적절한 수단을 통해 전달, 포워딩, 또는 전송될 수 있다. 제시된 방법은 하드웨어, 소프트웨어, 또는 이둘 모두로 구현될 수 있다.

[0054] 여기 제시된 실시예에 관련하여 기술된 다양한 예시적인 논리 블록, 모듈, 회로, 엘리먼트, 및/또는 컴포넌트들은 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적회로(ASIC), 필드 프로그램어블 게이트 어레이(FPGA) 또는 다른 프로그램어블 논리 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 여기 제시된 기능들을 수행하기 위해 설계된 임의의 조합을 통해 구현되거나 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로 이러한 프로세서는 임의의 기존 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 컴포넌트들의 조합(예를 들어, DSP 및 마이크로프로세서의 조합), 다수의 마이크로프로세서, DSP와 연결된 하나 이상의 마이크로프로세서, 또는 임의의 다른 이러한 구성으로 구현될 수 있다.

[0055] 여기 제시된 방법들 또는 알고리즘은 하드웨어, 프로세서에 의해 실행가능한 소프트웨어 모듈, 또는 이 둘의 조합으로, 처리 유닛, 프로그래밍 명령 또는 다른 명령들의 형태로 직접 구현될 수 있고, 단일 장치에 포함되거나, 다수의 장치들에 걸쳐 분산될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래쉬 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드디스크, 탈착형 디스크, CD-ROM, 또는 공지된 임의의 형태의 저장 매체에 상주할 수 있다. 저장 매체는 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체로 정보를 기록할 수 있도록 프로세서에 연결될 수 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다.

[0056] 일 특징은 고객 전화 라인과 직렬로 삽입될 수 있고, 2-팩터 인증 방식에서 제2 팩터로 동작하고 DTMF 톤들을 암호화하는, 소형 폼-팩터 보안 장치를 제공하여, 민감한 정보의 노출을 방지한다. 상기 장치는 전화기의 정상 동작을 방해하지 않는다. 상기 장치는 은행들이 관련된 지불 서비스 및 은행들에 대한 브랜딩 기회를 또한 제공할 수 있는 소형 폼팩터 인클로져(enclosure)를 포함한다. 상기 장치는 자신이 연결된 전화 라인으로부터 전력이 공급된다. 일 구성에서, 다수의 이러한 장치들은 다수의 상이한 장치들(예를 들면, 은행들)과의 안전한 통신을 제공하기 위해서 전화 라인을 따라 연결되거나, 연쇄적으로 연결된다.

[0057] 다른 특징은 암호화된 심벌들의 보안을 보호하는 효율적인 암호화 방법을 제공한다. 각각의 평문 심벌은 별개의 의사랜덤하게 선택된 변환 테이블을 사용하여 암호화된다. 변환 테이블들로서 모든 가능한 심벌들의 치환을

사전 저장하기 보다는, 변환 테이블들은 의사 랜덤 번호 및 심벌 셔플링(shuffling) 알고리즘에 기반하여 온-더-플라이(on-the-fly) 방식으로 효율적으로 생성된다. 수신 장치는 수신된 암호화된 심벌들을 암호해독하기 위해서 온-더-플라이방식으로 역 변환 테이블들을 유사하게 생성할 수 있다.

[0058] **DTMF 톤들의 보안**

[0059] 도1은 일 시스템을 보여주며, 여기서 보안 장치(102)는 전화기(104) 및 보안 서버(110) 사이의 특정 통신들을 안전하게 하기 위해서 전화기(104)에 통신 라인을 따라 연결될 수 있다. 보안 장치(102)는 전화기(104) 및 통신 네트워크(106) 사이의 전화 라인 상에 직렬로 또는 라인 내에 연결될 수 있는 소형 폼팩터 장치일 수 있다. 보안 장치(102)는 전화기(104)에 인접 또는 근접한 전화 라인에 연결될 수 있다.

[0060] 일 예에서, 보안 장치(102)는 계좌 및/또는 발행 기관(108)(예를 들면, 은행, 신용카드 회사 등)과 관련될 수 있다. 예를 들어, 은행은 이러한 보안 장치(102)를 자신의 고객들에게 발행할 수 있고, 각 보안 장치는 고객 또는 고객의 계좌와 고유하게 관련된다. 발행 기관(108)은 고객들과의 전화 거래들을 용이하게 하는 보안 서버(110)를 가질 수 있다.

[0061] 도2는 도1의 발행 기관(108)에 속하는 보안 서버(110) 및 전화기(104) 사이의 특정 통신들을 안전하게 하기 위한 방법을 보여주는 흐름도이다. 보안 장치(102)는 활성 동작 모드 및 비활성(수동) 동작 모드를 가질 수 있다. 보안 장치(102)가 발행 기관(108)(예를 들면, 보안 서버(110))을 제외한 다른 사람에게 전화하는데 사용되는 경우, 보안 장치(102)는 비활성화되고, DTMF 톤들을 포함하는 호(call)는 변경되지 않고 단지 보안 장치(102)를 통해 전달된다. 그러나 전화기(104)가 발행 기관(208)으로 호를 개시하는 경우, 보안 서버(110)(예를 들면, 보안 서버(110))는 보안 장치(210)를 웨이크 업하는 활성화 신호를 전송한다. 활성화 신호는 보안 장치(102)가 우연하게 트리거링되지 않는 것을 보장하기 위해서 충분히 길고 및/또는 고유하다(예를 들어, 충분한 디지트 또는 심벌들을 가짐). 일 예에서, 이러한 활성화 신호는 실제로 임의의 정보를 전달하지는 않고, 단지 보안 장치가 비활성(수동) 모드에서 활성 모드로 전환하는 것을 트리거 또는 활성화한다. 예를 들어, 활성화 신호는 보안 장치(102)에 의해 인지되는 짧은 음악 또는 톤일 수 있다. 보안 장치(102)는 보안 서버(110)로부터 이러한 활성화 신호(예를 들면, 고유한 한 세트의 DTMF 톤들)를 청취 및 인지하여 활성 모드(212)로 전환한다. 일 예에서, 활성화 신호 수신시에, 보안 장치(102)는 전화기로부터 보안 서버(110)로의 모든 DTMF 톤들의 암호화를 시작할 수 있다.

[0062] 일 구현에서, 챌린지-응답 방식이 보안 장치(102) 및 보안 서버(110) 사이에서 구현될 수 있다. 활성화 신호뿐만 아니라, 보안 서버(110)는 랜덤 챌린지를 보안 장치로 전송할 수 있다(214). 보안 장치(102)는 챌린지를 수신하여, 응답(예를 들면, 챌린지에 대한 응답 및 식별자)을 생성하고(216), 이러한 응답을 보안 서버(110)로 전송할 수 있다. 이러한 응답은 보안 장치(102)와 관련된 식별자 및 챌린지에 대한 응답을 포함할 수 있다. 보안 장치(102)는 전화기(104)로부터 보안 서버(110)로의 뒤이은 DTMF 톤들을 암호화하는데 사용될 수 있는 세션 키를 생성할 수 있다.

[0063] 이러한 응답은 보안 서버(110)에 보안 서버가 관련된 보안 장치와 통신하고 있음을 알린다. 보안 서버(110)는 식별자를 이용하여 특정 고객의 계좌를 검색하고(220), 이를 통해 고객이 수동으로 자신의 계좌를 확인하는 수고를 덜어준다(예를 들어, 고객이 자신의 계좌 번호를 입력하는 수고를 덜어줌). 보안 서버(110)는 사용자를 인증하기 위해서 또한 이러한 응답이 랜덤 챌린지 및 인증 키(보안 장치(102) 및 보안 서버(110) 모두에 제공됨)에 기반하여 정확한 것인지를 검증한다. 보안 장치(102)는 사용자 전화기에 근접하게 위치하기 때문에(예를 들어, 사용자 가정 내부에 위치함), 공격자는 공격을 개시하기 위해서는 이를 훔쳐야만 할 것이다.

[0064] 동일한 챌린지 및 응답을 사용함으로써, 보안 서버(110)는 보안 장치(102)가 계산한 것(224)과 동일한 세션 키(226)를 생성한다. 보안 장치(102)로부터 수신된 응답을 보안 서버(110)가 동의하지 않으면(또는 응답을 수신하지 않으면), 호는 보다 엄격한 식별 및/또는 인증을 위해 다른 경로로 디버팅될 수 있다. 즉, 보안 장치(102)는 자신의 응답을 수신된 랜덤 챌린지 및 인증 키에 기반하여 계산한다. 그리고 나서, 보안 서버(110)는 (랜덤 챌린지 및 인증 키에 기반하여) 로컬 응답을 계산함으로써 수신된 응답을 검증하고, 이를 보안 장치(102)로부터 수신된 응답과 비교할 수 있다.

[0065] 챌린지-응답이 적절하게 인증되면, 보안 서버(110)는 새로이 유도된 세션 키를 사용하여 인증된 확인을 전송한다(228). 이러한 확인은 보안 장치(102)에게 전화기(104)로부터 오는 DTMF 톤들의 암호화를 개시할 것을 알린다. 보안 서버로부터의 확인에 문제가 있으면(예를 들어, 특정 최대 시간 내에 보안 장치(102)로부터 확인이

수신되지 않거나, 확인이 실패되는 등의 문제가 있으면), 보안 장치(102)는 사용자에 대한 경고 신호를 생성한다. 예를 들어, 챌린지-응답 인증이 실패하면, 불빛이 플래시 되거나(온 상태가 됨), 알람이 울릴 수 있다. 또한, 보안 장치(102)가 활성이고 및/또는 챌린지-응답이 성공적으로 인증됨을 표시하기 위해서 불빛(예를 들어, 다이오드 LED를 방사하는 불빛)이 점등될 수 있다.

[0066] 챌린지-응답이 성공적으로 인증되면, 일 예에서 세션 키가 전화기(104)로부터 보안 서버로의 전송들을 암호화하기 위해서 보안 서버(102)에 의해 사용될 수 있다. 암호화가 시작되면, 보안 장치는 전화기로부터 오는 DTMF 톤들을 포착하여(232) 암호화된 DTMF 톤들을 전송한다(234). 이러한 DTMF 톤들의 암호화의 일 예에서, 전화기(104)로부터의 DTMF 톤들은 상이한 DTMF 톤들로 변환되고, 그리고 나서 이러한 변환된 상이한 DTMF 톤들은 보안 서버(110)로 전송된다. 다른 구성에서, DTMF 톤들은 보안 장치(102)에 의해 디지털 심벌들로 변환되고, 이러한 변환된 디지털 심벌들은 암호화되어 보안 서버(110)로 전송된다. 보안 장치(102)는 또한 다른 신호들(비-DTMF 톤들 또는 신호들)을 수정 또는 암호화하지 않고 양방향에서 이러한 다른 신호들을 전달할 수 있다. 사용자에게 요청될 수 있는 첫 번째 것들 중 하나가 사용자의 계좌와 관련된 PIN 번호를 입력하는 것이면, 이러한 PIN 번호와 관련된 DTMF 톤들은 암호화되어 인증을 위한 제2 팩터를 형성할 수 있다. 유사하게, 보안 서버(110)는 세션 키를 사용하여 보안 장치를 통해 전화기로부터 수신된 DTMF 톤들을 암호해독 할 수 있다(236).

[0067] 대안적인 구성에서, 보안 장치(102)는 특정 발행 기관(108)과 관련된 특정 전화 번호(들)를 인지하도록 구성될 수 있다. 보안 장치(102)가 전화기가 이러한 특정 전화 번호를 다이얼링 하였다고 인지하면, 보안 장치(102)는 자동적으로 활성 모드로 스위칭하여, 전화기로부터 보안 서버(110)로의 모든 DTMF 톤들을 암호화할 수 있다.

[0068] 보안 장치(102)는 호가 종결될 때까지 전화기(104)로부터의 DTMF 톤들의 암호화를 계속하고, 호가 종결되는 시점에서 보안 장치(102)는 비활성 모드로 다시 스위칭하고, 여기서 보안 장치(102)는 모든 DTMF 톤들이 변경되지 않고 전달되도록 한다.

[0069] 보안 장치(102)는 소형 폼팩터를 가질 수 있고, 전화 라인 내로 쉽게 플러깅(plug) 될 수 있다. 사용자는 상이한 위치들로부터(예를 들면, 가정, 직장 등) 계좌에 안전하게 액세스할 수 있도록 하기 위해서 하나의 기관 또는 계좌와 관련된 다수의 보안 장치들을 가질 수 있다. 사용자는 또한 다양한 상이한 기관들 및/또는 계좌들과 관련된 다수의 보안 장치들을 가질 수 있다. 이러한 다수의 보안 장치들은 전화 라인을 따라 직렬로 연결될 수 있다. 체인 내의 하나의 보안 장치는 그 체인 내의 다른 보안 장치로 신호들을 단순히 전달한다. 체인 내의 하나의 보안 장치가 보안 서버에 의해 활성화되면, 이러한 보안 장치는 전화기로부터의 DTMF 톤들을 암호화한다.

[0070] 다른 예에서, 보안 장치(102)는 하나의 전화기 또는 위치로부터 다수의 사용자들을 서빙할 수 있다. 이러한 경우, 보안 서버는 보안 장치가 다수의 사용자들 또는 계좌들과 관련됨을 식별할 수 있다. 각 사용자들 사이를 구분하기 위해서, 보안 서버는 사용자로 하여금 PIN 또는 특정 사용자 또는 계좌를 식별하는 다른 식별자를 입력할 것을 요청하는 음성 프롬프트(prompt)를 전송할 수 있다.

[0071] 도3은 전송기간 동안 DTMF 톤들을 안전하게 할 수 있는 텔레-서비스 보안 서버의 일 예에 대한 블록도이다. 보안 서버(302)는 (소형 및/또는 저전력 마이크로프로세서와 같은) 처리 회로(304)를 포함할 수 있다. 보안 서버(302)는 보안 서버(302)를 통신 네트워크로 연결하는데 사용되는 제1 통신 모듈(306)을 포함할 수 있다. 인증 모듈(308)은 인증 서버(302)가 통신하는 인증 장치를 인증 서버(302)가 인증할 수 있도록 하여준다. DTMF 암호해독 모듈(308)은 보안 서버(302)가 보안 장치로부터 수신된 암호화된 DTMF 톤들을 암호해독할 수 있도록 하여준다.

[0072] 도4는 전화 장치로부터의 DTMF 톤들을 안전하게 하기 위한 보안 서버상에서의 동작 방법을 보여준다. 호가 DTMF를 인에이블한 전화기로부터 수신된다(402). 활성화 신호가 DTMF를 인에이블한 전화기와 관련된 보안 장치로 전송된다(404). 보안 장치는 DTMF를 인에이블한 전화기 근처에 위치한다. 그리고 나서 보안 장치는 보안 서버에 의해 인증된다. 예를 들어, 챌린지 신호가 보안 장치(406)로 전송된다. 보안 서버는 응답이 보안 장치(408)로부터 수신되는지 여부를 결정한다. 응답이 수신되지 않으면, 보안 서버는 어떠한 보안 장치도 전화 라인에 존재하지 않는다고 가정한다(410). 이와 달리 응답이 수신되면, 보안 서버는 수신된 응답이 성공적으로 인증될 수 있는지를 결정한다(412). 응답이 성공적으로 인증될 수 없으면, 인증이 실패한다(414). 그렇지 않고 응답이 성공적으로 인증되면, 세션 키가 생성된다(416). 세션 키에 의해 인증되는 확인 메시지가 보안 장치로 전송된다(418). 보안 서버는 보안 장치로부터 암호화된 DTMF 톤들을 수신할 수 있다(420). 그리고 나서, 보안 서버는 전화기에 의해 전송된 정보를 획득하기 위해서 수신된 DTMF 톤들을 암호해독할 수 있다(422). 이러한 DTMF 톤들은 원 DTMF 톤들을 암호화함으로써 전송기간 동안 도청자로부터 보호되는 기밀 정보(예를 들면,

계좌 번호, 패스워드, PIN 등)를 나타낼 수 있다.

[0073] 도5는 전송기간 동안 DTMF 톤들을 보호하기 위해서 구성될 수 있는 보안 장치의 일 예에 대한 블록도이다. 보안 장치(502)는 소형 및/또는 저전력 마이크로프로세서와 같은 처리 회로(504)를 포함할 수 있다. 보안 장치(502)는 보안 장치가 연결되는 전화 라인에 의해 전력이 제공될 수 있다. 제1 통신 인터페이스 A(506)는 보안 장치(502)를 전화기에 연결하는데 사용될 수 있다. 제2 통신 인터페이스 B(508)는 보안 장치(502)를 통신 네트워크에 연결하는데 사용될 수 있다. 수동 동작 모드에서, 보안 장치(502)는 모든 DTMF 톤들이 변경되지 않고 전달되도록 한다. 처리 회로(504)는 (예를 들어, 보안 서버로부터) 활성화 신호를 청취하도록 구성될 수 있다. DTMF 검출기(510)는 보안 장치를 활성 동작 모드로 스위칭하기 위한 DTMF 활성화 신호를 검출하도록 구성될 수 있다. 활성 모드에서, 보안 장치(502)는 보안 서버로부터의 인증 챌린지에 응답하도록 구성될 수 있다.

[0074] 활성 모드에서, DTMF 검출기(510)는 (예를 들어, 전화기로부터) 통신 인터페이스 A(506)를 통해 수신되는 DTMF 톤들을 검출하도록 또한 구성될 수 있다. 하나 이상의 DTMF 톤들이 검출되면, DTMF 톤들은 DTMF 암호화 모듈(512)에 의해 암호화되거나 수정된다. 그리고 나서, 암호화된 DTMF 톤들은 통신 인터페이스 B(508)를 통해 보안 서버로 전송된다.

[0075] 도6은 전화기 장치로부터의 DTMF 톤들을 안전하게 하기 위해 보안 장치상에서 동작되는 방법을 보여준다. 전화기 및 보안 서버 사이에 호가 개시되는 경우 보안 장치에 전력이 공급된다(602). 즉, 호가 만들어질 때, 통신 라인에 전력이 제공되기 때문에, 보안 장치는 그 전력을 통신 라인으로부터 끌어낸다. 수동 동작 모드에서, 보안 장치는 DTMF 톤들이 제1 통신 인터페이스 및 제2 통신 인터페이스 사이에서 변경되지 않고 전달되도록 한다(604). 예를 들어, 제1 통신 인터페이스는 전화기에 연결되고, 제2 통신 인터페이스는 제2 통신 인터페이스에 연결된다. 보안 장치는 (DTMF) 활성화 신호가 보안 서버로부터 수신되는지 여부를 결정하기 위해서 전송들을 모니터링 한다(606). 보안 장치는 활성화 신호가 수신되지 않는 경우 수동 모드에서 동작을 계속한다. DTMF 활성화 신호가 수신되면, 보안 장치는 활성 동작 모드로 변경한다(608). 보안 장치는 또한 보안 서버로부터의 다른 신호들을 청취할 수 있다(610).

[0076] 보안 장치는 보안 서버로부터 챌린지를 수신할 수 있다(612). 보안 장치는 챌린지에 대한 응답으로 응답한다(614). 응답이 유효하면, 보안 장치는 보안 서버가 보안 장치를 성공적으로 인증하였음을 표시하는 확인을 수신할 수 있다.

[0077] 활성화되고 적절하게 인증되면, 보안 장치는 전화기로부터의 DTMF 톤들을 청취한다. DTMF 톤들이 제1 통신 인터페이스를 통해 (보안 장치가 연결된) 전화기로부터 수신되면(618), 수신된 DTMF 톤들은 상이한 DTMF 톤들로 암호화된다(620). 일 예에서, 전화기로부터의 DTMF 톤들은 상이한 DTMF 톤들로 변환되고, 이러한 변환된 상이한 DTMF 톤들은 보안 서버로 전송된다. 다른 구성에서, DTMF 톤들은 보안 장치(102)에 의해 디지털 심벌들로 변환되고, 이러한 변환된 디지털 심벌들은 암호화되어 보안 서버로 전송된다. 그리고 나서, 암호화된 DTMF 톤들은 제2 통신 인터페이스를 통해 보안 서버로 전송된다(622). 보안 장치는 호가 종료할 때까지 전화기로부터의 DTMF 톤들의 암호화를 계속하고, 호 종료시에 보안 장치는 수동 모드로 다시 리턴한다(624). 보안 장치(102)는 전화기로부터의 암호화되지 않은 DTMF 톤이 보안 서버로 전달되는 것을 방지한다. 일 예에서, 보안 장치(102)는 활성인 동안 전화기로부터의 모든 입력들(예를 들면, 전송들)을 차단할 수 있다. 이러한 경우, 고객 또는 보안 서버 중 하나가 입력들을 재연결(예를 들면, 보안 장치(102)로부터의 전송들의 허용)하기 위한 조건이 존재할 수 있으며, 이러한 조건의 일 예는 고객이 상담원과 통화할 필요가 있을 때이다.

[0078] **셀룰러 전화 보안 방식**

[0079] 도7은 보안 서버를 통해 자신을 인증하도록 구성된 이동 통신 장치의 블록도이다. 이동 통신 장치(702)는 통신 모듈(706) 및 사용자 입력 인터페이스(708)에 연결된 처리 회로(704)를 포함한다. 통신 모듈(706)은 이동 통신 장치(702)가 무선 통신 네트워크(710)를 통해 통신하는 것을 인에이블한다. 처리 회로(704)는 호 기간 동안 하나 이상의 보안 서버를 통해 자신을 인에이블하도록 구성될 수 있다. 예를 들어, 이동 통신 장치는 금융 기관 또는 은행이 이동 통신 장치(702)의 사용자를 인증하는 것을 허용하는 사용자 식별자 및/또는 인증 키를 가지고 구성될 수 있다. 인증 키 및/또는 사용자 식별자는 금융기관 또는 은행에 의해 미리(예를 들면, 셋업 또는 구성기간 동안) 제공될 수 있다. 또한, 처리 회로(704)는 인증 절차를 완료하기 위해서 PIN, 패스워드, 또는 다른 입력을 사용자로부터 요청할 수 있다.

[0080] 도8은 통신 네트워크를 통해 텔레-서비스 스테이션(804)에 대해 이동 통신 장치(802)를 인증하기 위한 방법을

보여주는 흐름도이다. 이동 통신 장치(802)는 이동 전화기일 수 있고, 텔레-서비스 스테이션(804)은 은행 또는 금융 기관과 관련된 보안 서버를 포함할 수 있다. 이동 통신 장치(802) 및 텔레-서비스 스테이션(804) 각각은 동일한 인증 키를 가질 수 있다.

[0081] 이동 통신 장치는 텔레-서비스 스테이션에 관련된 발행 기관으로 호를 개시한다(806). 이러한 발행 기관은 은행 또는 금융기관일 수 있다. 텔레-서비스 스테이션은 이동 통신 장치로 랜덤 챌린지를 전송한다(808). 그리고 나서, 이동 통신 장치는 랜덤 챌린지 및 인증 키에 기반하여 응답을 생성하고(809), 그 응답 및 (가능하게는) 사용자 식별자를 텔레-서비스 스테이션으로 전송한다(810). 그리고 나서, 텔레-서비스 스테이션은 이동 통신 장치로부터의 응답이 정확한지 여부를 검증한다(812). 이는 텔레-서비스 스테이션이 자신의 인증 키 및 랜덤 인증 챌린지에 기반하여 검증 값을 계산하고 이를 이동 통신 장치로부터 수신된 응답과 비교함으로써 이뤄질 수 있다. 응답이 성공적으로 인증되면, 인증 확인이 이동 통신 장치로 전송될 수 있다(814). 이동 통신 장치는 텔레-서비스 스테이션으로부터 민감한 정보(예를 들면, 은행 계좌 기록 등)를 요청할 수 있다. 이동 통신 장치가 성공적으로 인증되면, 텔레-서비스 스테이션은 요청된 민감한 정보를 이동 통신 장치로 제공한다(818). 이러한 방식으로, 이동 통신 장치(예를 들면, 이동 전화기)는 호 기간 동안 민감한 정보의 전송을 안전하게 하기 위해서 텔레-서비스 스테이션에 의해 인증될 수 있다.

[0082] **위협 모델들**

[0083] 여기서 제시되는 보안 장치 및/또는 방법에 의해 다뤄지는 위협의 일 타입은 도청 공격이다. 이러한 공격에서, 공격자는 녹음기를 전화 라인에 부착하여 전화기 상에 사용자가 입력하는 번호들과 관련된 DTMF 톤들을 청취한다., 이러한 DTMF 톤들은 다른 개인 및/또는 비밀 정보들 중에서 호출되는 은행, 사용자의 고객 및/또는 계좌 번호, 개인 식별 번호(PIN), 주민번호를 식별할 수 있다. 그리고 나서, 공격자는 이러한 정보를 사용하여 사용자 계좌로부터 부정한 거래들을 수행할 수 있다. 여기 제시된 보안 장치는 DTMF 톤들을 암호화하고 추가적인 인증을 제공함으로써 이러한 공격에 대처할 수 있다. 대부분의 기관들(예를 들면, 은행 등)은 인증을 위한 2가지 팩터들(예를 들면, 보안 장치의 소유 및 PIN에 대한 지식)을 사용할 수 있기 때문에, 다른 민감한 정보를 질의할 필요가 거의 없다. 암호화된 DTMF 톤들을 단순히 가로채는 것은 대응하는 계좌 번호, PIN 등에 대한 어떠한 것도 제공하지 못한다.

[0084] 예를 들어 호가 의도된 수신자(예를 들면, 의도된 은행)로 전달되는 것을 방지함으로써 호의 처리를 방해하고자 하는 공격자는 의도하는 수신자 행세를 하고, 호출자에게 모든 민감한 정보를 입력할 것을 요청한다. 이러한 공격에 대처하기 위해서, 보안 장치는 "암호화 개시" 신호(즉, 인증된 정보)가 수신 기관으로부터 수신된 후에 보안 표시자(예를 들면, 불빛)를 켤 수 있다. 호출자(예를 들어, 고객)는 임의의 민감한 정보 또는 기밀 정보를 입력하기 전에 보안 장치가 그 톤들을 암호화하고 있음을 확인하기 위해서 보안 표시자를 단순히 검사한다.

[0085] 다른 타입의 공격은 세션 하이젝킹 공격이고, 여기서 공격자는 사용자가 의도된 수신자(예를 들면, 은행)와 통신을 설정하여 보안 표시자를 활성화할 때까지 기다리고, 그리고 나서 이러한 통화에 개입한다. 그리고 나서, 공격자는 이러한 통화에 문제가 발생한 것처럼 가장하고, 사용자가 음성으로 민감한 정보를 제공할 것을 요청한다. 대안적으로, 공격자는 톤 단위(tone by tone) 암호화 패턴을 설정하도록 하기 위해서 사용자에게 (공격자에게 이미 알려진) 특정 응답들을 입력하도록 요청하고, 그리고 나서 톤 단위 변환들을 사용하여 은행에 대한 자신의 응답을 암호화할 수 있다. 이러한 타입의 공격에 대처하기 위해서, 톤 단위 암호화는 의사 랜덤 방식, 순환적 방식, 및/또는 번호 대 톤 관계의 발견을 방지하는 다른 방식에 따라 변경 또는 수정될 수 있다.

[0086] **메시지 및 세션 인증**

[0087] 보안 장치는 예를 들어, 메시지 인증 코드(MAC) 함수를 사용함으로써 메시지 인증 및 세션 키 유도를 수행하도록 구성될 수 있다. 예를 들어, 보안 서버는 MACk(챌린지)의 단일 인보케이션(invocation)으로부터의 출력을 분할함으로써 호출자의 보안 장치를 인증할 수 있다. 예를 들어, 전형적인 MAC 함수는 32 DTMF 톤들로서 표현될 수 있는 128 비트 출력을 리턴할 수 있다. 보안 서버 및 보안 장치가 MAC을 계산한 후에, 보안 서버는 첫 번째 16 DTMF 톤들(MAC의 일부를 나타냄)을 보안 장치로 전송하고, 응답하여, 보안 장치는 다른 16 DTMF 톤들(MAC의 다른 부분을 나타냄)을 다시 전송한다. 이러한 방식으로, 보안 서버 및 보안 장치 모두는 이들이 인증되고 합법적이라는 것을 서로에 대해 증명할 수 있다.

[0088] 유사하게, 세션 키는 Session Key = MACk (인증 키 ‖ 챌린지)가 되도록 각 측에 의해 계산될 수 있고, 여기서 인증 키는 보안 장치 내로 사전에 로딩된다. 보안 장치가 자신의 응답을 보안 서버로 전송할 때, 세션 키가 공개되는 것을 방지하기 위해서, 응답은 추가적인 정보를 포함할 수 있다. 예를 들어, 응답은 Response = MACk ("여분 정보 스트링" ‖ 인증 키 ‖ 챌린지)일 수 있다.

[0089] **스트림 암호화**

[0090] 본 발명의 다른 특징은 암호화된 심벌들을 안전하게 하는 효율적인 암호화 방법을 제공하는 것이다. 각각의 평문 심벌은 별개의 의사랜덤하게 선택된 변환 테이블을 사용하여 암호화된다. 모든 가능한 심벌들의 치환을 번역 테이블들로서 사전에 저장하는 것이 아니라, 변환 테이블들은 의사 랜덤 번호 및 심벌 셔플링 알고리즘에 기반하여 온 더 플라이 방식으로 효율적으로 생성될 수 있다. 수신 장치는 수신된 암호화된 심벌들을 암호해독하기 위해서 온 더 플라이 방식으로 역 변환 테이블들을 유사하게 생성할 수 있다.

[0091] 이러한 암호화 알고리즘은 다양한 방식으로 구현될 수 있다. 예를 들어, 전화 보안 장치는 DTMF 톤들을 디지털 값들로 전환하고, 각 디지털 값에 대해 의사랜덤하게 선택된 변환 테이블을 사용함으로써 디지털 값들을 암호화할 수 있다. 그리고 나서, 암호화된 디지털 값들은 디지털 형태로 또는 암호화된 디지털 값들과 관련된 DTMF 톤들로서 보안 서버(예를 들면, 텔레-서비스 스테이션)로 전송될 수 있다.

[0092] DTMF 톤들은 디지털 심벌들에 의해(또는 디지털 심벌과 관련되어) 표현될 수 있기 때문에, 이들은 예를 들어 스트림 암호화에 의해 안전하게 될 수 있다. 다양한 예들에서, 스트림 암호화는 카운터 모드의 암호화 표준(AES), 출력 피드백(OFB), 또는 암호 텍스트 피드백(CFB) 모드들과 같은 블록 암호에 의해 생성된 키 스트림을 사용할 수 있다. 예를 들어, MAC 함수는 CBC-MAC 모드의 블록 암호를 통해 구현될 수 있다. 예를 들어, 보안 장치가 하드웨어에서 구현된 AES를 가지는 경우 이는 장점을 갖는다.

[0093] 이러한 기능들이 소프트웨어로 구현되면, 비-선형 SOBER(NLS)와 같은 전용 스트림 암호를 사용하는 것이 바람직하다. 스트림 암호는 또한 암호화될 데이터를 키 또는 임시(nonce) 입력으로서 사용하고, 그리고 나서 출력 키 스트림을 생성함으로써, 효율이 낮기는 하지만, MAC 함수로서 사용될 수 있다. 생성된 키 스트림의 길이는 필요한 만큼 길 수 있기 때문에, 응답 및 세션 키 모두는 하나의 호에서 생성될 수 있다.

[0094] (스트림 모드에서 진정한 스트림 암호 또는 블록 암호를 사용하는) 기존의 스트림 암호화는 일반적으로 의사 랜덤 번호들의 키 스트림을 생성하고, 암호화된 출력 또는 암호문을 형성하기 위해서 이들을 평문(즉, DTMF 톤들의 디지털 표현)과 결합하는 동작으로 진행된다. 일반적으로, 키 스트림 및 평문은 배타적-OR(XOR) 연산을 사용하여 결합되는데, 왜냐하면 배타적-OR(XOR) 연산은 셀프-인버스(self-inverse) 특성이 있기 때문이다. 그러나 기존의 DTMF를 인에이블한 전화기는 10 개 이상의 키들을 가지고, 각 키는 고유한 톤을 갖는다. 따라서, XOR 연산은 키 스트림으로 이러한 DTMF 톤들을 암호화하는데 사용될 수 없다. 대신, 전화기 키들과 관련된 DTMF 톤들은 암호화된 심벌 또는 암호문을 생성하기 위해서 키 스트림으로부터 획득된 의사 랜덤 번호들/심벌들에 추가될 수 있는 상이한 디지털 심벌들로 변환(또는 상이한 디지털 심벌들과 관련)될 수 있다. 그러나 특정 디지트의 위치를 알고 있는 활동하는 공격자는 전송된 암호문 번호로부터 감산함으로써 그 번호를 변경할 수 있다. 예를 들어, 특정 DTMF 톤에 대해 입력이 "1"이지만, 출력은 "7"임을 알고 있는 공격자는 이러한 톤에 대해 생성된 의사 랜덤 번호가 "6"임을 결정하고, 그리고 나서 그 특정 디지트 위치에 대해 그들이 선택한 임의의 문자를 정확하게 암호화할 수 있다.

[0095] **조합 결합기**

[0096] 본 발명의 일 특징은 암호화될 각 평문 심벌에 대해 의사랜덤하게 선택 또는 생성된 변환 테이블을 획득 또는 생성하기 위해서 키 스트림을 사용하는 것을 제공한다. 키 스트림으로부터 의사 랜덤 번호를 취하고 평문을 동일한 방식으로 변경(예를 들면, 모듈 n 합산)하는 대신에, 본 발명의 일 특징은 다수의 변환 테이블들 중 하나를 의사랜덤하게 선택함으로써 입력 스트림의 각 평문 심벌을 변환하는 것을 제공한다. 변환 테이블들은 한 세트의 번호들 또는 심벌들의 상이한 가능한 치환들을 제공할 수 있다. 이는 여기서 조합 결합기로 지칭된다.

[0097] 도9는 암호화될 각 심벌에 대한 변환 테이블을 의사 랜덤하게 선택함으로써 평문 심벌들을 안전하게 보호하기 위한 조합 결합기의 블록도이다. 암호화 생성기(902)는 의사 랜덤 번호들/심벌들의 키 스트림 Si(904)를 생성하기 위해서 사용된다. 키 스트림(904)의 의사 랜덤 번호들은 입력 스트림의 각 평문 입력 심벌 Pi(908)에 대

해, 다수의 가능한 변환 테이블들로부터 상이한 변환 테이블(906)을 생성 또는 획득하기 위해서 사용된다. 평문 입력 심벌(908)을 의사 랜덤 출력으로 변환함으로써, 암호화된 출력 심벌 Ci(910)가 생성된다.

[0098] 이러한 변환 동작은 키 스트림(904)의 제어하에 평문 입력 심벌들(908)의 치환을 정의한다. 변환 테이블(906)은 n개의 엘리먼트들로 구성된 벡터로 표현될 수 있고, 평문 입력 심벌(908)의 변환은 변환 테이블(906)의 p번째 엘리먼트를 참조함으로써 이뤄질 수 있다. 암호화된 출력 심벌 Ci가 주어지면, 역 치환 테이블을 생성하거나, 심벌 Ci를 포함하는 엔트리에 대한 테이블을 검색하고 그 인덱스를 p로서 리턴함으로써 역 변환이 이뤄질 수 있다.

[0099] 일반적으로, n개의 평문 심벌들로 구성된 한 세트에 대해서, n!(팩토리얼) 개의 가능한 치환들이 존재한다. 하나의 치환이 모든 가능한 치환들 세트로부터 랜덤하게 선택되고, 평문 입력 심벌 Pi(908)를 암호화된 출력 심벌 Ci(910)(암호문으로 지칭됨)로 변환하기 위한 변환 테이블(906)로 사용될 수 있다. 입력 스트림의 각 평문 심벌에 대해서, 의사 랜덤하게 선택된 변환 테이블이 선택된다. 그리고 나서, 암호화된 출력 심벌 Ci(910)을 목격하고 이것이 특정 평문 심벌에 대응한다고 알고 있는 공격자는 다른 평문 심벌들 및 대응하는 암호화된 심벌들 사이의 대응관계에 대해 여전히 알지 못한다. 즉, 공격자가 확인할 수 있는 모든 정보는 암호화된 심벌의 변경이 이들이 알고 있는 것과는 다른 평문 심벌을 만들어낸다는 것이고, 어떤 다른 평문 심벌이 될 것인지는 알지 못한다. 따라서, 의사 랜덤하게 선택된 변환 테이블들은 평문 입력 심벌들과 암호화된 출력 심벌들(암호문) 사이의 관계를 숨기며, 공격자는 특정한 단일 평문 심벌 대 암호문 심벌 변환에 대한 지식을 이용할 수 없다.

[0100] 전화 뱅킹을 안전하게 보호하기 위한 일 예에서, 전화기로부터 보안 장치에 의해 수신된 각 DTMF 톤은 디지털 평문 심벌로 변환(또는 디지털 평문 심벌과 관련)된다. 그리고 나서, 평문 심벌은 암호화된 심벌을 획득하기 위해서 (키 스트림으로부터의 하나 이상의 의사 랜덤 번호들에 기반하여 획득된) 변환 테이블에 의해 변환된다. 그리고 나서, 암호화된 심벌은 (디지털 형태 또는 암호화된 심벌에 대응하는 DTMF 톤으로서) 보안 서버로 전송되고, 보안 서버에서 암호화된 심벌은 역 변환 테이블에 의해 암호해독된다. 역 변환 테이블은 동일한 키 스트림을 생성하는 보안 장치 및 보안 서버 모두의 암호 생성기들을 동기화함으로써 생성 또는 획득될 수 있다. 일 예에서, 암호 생성기들은 동일한 시드(예를 들면, 세션 키 등)를 사용함으로써 동기화될 수 있다.

[0101] 일 예에서, 다수의 변환 테이블들이 보안 장치 및/또는 보안 서버에 의해 사전에 생성되거나 및/또는 저장될 수 있다. 온-더-플라이 방식으로 새로운 변환 테이블(즉, 입력 심벌들의 치환)을 생성하기 보다는, 변환 테이블은 사전에 생성되어 저장될 수 있다. 키 스트림(904)의 의사 랜덤 값들/심벌들은 암호화될 각 평문 심벌들에 대한 사전-생성된 변환 테이블들 중 하나를 선택하는데 사용될 수 있다. 사전-생성된 변환 테이블들은 모든 치환 또는 n개의 평문 심벌들 세트에 대한 치환들의 서브세트를 정의할 수 있다.

[0102] 다른 예에서, 사용되는 변환 테이블은 변환 테이블을 형성하기 위해서 키 스트림을 사용하고, 심벌들을 의사랜덤하게 셔플링(shuffling)함으로써 온 더 플라이 방식으로 생성될 수 있다. 이러한 해법들은 n! 개의 테이블들이 존재하고, 이러한 테이블들 중 하나를 선택하는데 필요한 키 스트림의 량은 셔플링을 통해 이러한 테이블을 생성하는데 필요한 량과 동일하다 점에서, 등가적이다.

[0103] 도10은 평문 심벌을 암호화된 심벌로 변환하기 위한 심벌 대 심벌 변환 테이블(1002)의 일 예를 보여주는 도이다. 이러한 예에서, 16개의 평문 심벌들이 상이한 암호화된 심벌로 변환된다. 이진(binary) 표현은 본 예에서 16개의 평문 심벌들이 4 비트 암호화된 심벌들을 사용하여 암호화될 수 있음을 단지 예시하기 위해서 제시된다. 다른 예에서, 보다 많거나 적은 수의 평문 심벌들이 암호화되는 경우, 상이한 수의 비트들이 각 심벌에 대해 사용될 수 있다. 예를 들어, 최대 256개의 평문 심벌들에 대해서, 각각의 암호화된 심벌을 생성하기 위해서 키 스트림으로부터 8개의 비트들이 추출될 수 있다.

[0104] 본 발명의 또 다른 특징은 특정 변환 테이블 내에서 평문 심벌들 및 암호화된 심벌들 사이에 일 대 일 대응을 제공하는 것이다. 즉, 특정 변환 테이블 내에서 어떠한 2개의 평문 심벌들도 동일한 암호화된 심벌로 전환되지 않는다. 이는 암호해독 장치가 암호화된 심벌을 원래의 평문 심벌로 정확하게 암호해독할 수 있도록 하여준다.

[0105] 암호해독 장치에서, 심벌 대 심벌 역 변환 테이블이 생성되어 암호화 장치의 심벌 대 심벌 역 변환을 수행하고, 이를 통해 수신된 암호화된 심벌들을 암호해독한다.

[0106] 도11은 암호화된 심벌들(1106)을 획득하기 위해서 상이한 변환 테이블들(1104)을 사용하여 평문 심벌들(1102)이 암호화되는 방법의 일 예를 보여준다. 각각의 평문 심벌 P0,P1,P2,P3,...Pi에 대해서, 상이한 변환 테이블들(1104)(각각은 상이한 심벌들 치환을 가짐)이 암호화된 심벌들 C0,C1,C2,C3,...Ci를 획득하기 위해서 사용된다.

[0107] 한 세트에 보다 작은 수의 심벌들이 존재하는 경우, 이러한 심벌들의 모든 가능한 치환들을 리스트하고(즉, 사전-생성하고), 치환으로부터 하나의 변환 테이블을 선택하기 위해서 (키 스트림으로부터) 인덱스를 사용하는 것이 가능하다. 예를 들어, 한 세트에 12개의 가능한 심벌들이 존재하는 경우, 생성되는 가능한 치환들의 수는 12!(479,001,600) 이다. 하나의 치환을 충분히 선택하기 위해서, 바이어스 없이 하나의 변환 테이블로서 하나의 치환을 선택하는데 32비트 키 스트림이면 충분하다. 그러나 이러한 방법은 한 세트 내의 심벌들의 수가 증가하면 비효율적이게 된다. 예를 들어, 한 세트 내에 256개의 가능한 심벌들이 존재하는 경우, 생성되는 가능한 치환들의 수는 256!($8.5x10^{506}$) 이고, 이는 변환 테이블로서 치환들 중 하나를 선택하기 위해서 의사 랜덤 키 스트림으로부터 1684 비트 이상을 취해야한다.

[0108] 도12는 n개의 심벌들로 구성된 한 세트에 대한 다수의 가능한 치환들로부터 하나의 변환 테이블을 선택하기 위한 알고리즘을 보여주며, 여기서 n은 양의 정수이다. 이러한 예에서, 범위 0 및 2k-1에 균일하게 분포된 k비트 길이(예를 들어, 8 비트, 32 비트 등) 의사 랜덤 키 스트림 값들을 제공하는 암호 생성기가 사용될 수 있다. 이러한 키 스트림은 의사 랜덤 번호 w를 획득하기 위해서 사용된다(1202). n!은 2^k로 균일하게 나눠지지 않을 수 있기 때문에, 의사 랜덤 번호 w는 바이어스들을 도입하지 않고 직접 사용될 수 없다. 이러한 이유로, 최대 임계치 Pmax가 2^k보다 작은 n!의 가장 큰 배수로 정의된다. 의사 랜덤 번호 w가 이러한 최대 임계치 Pmax 보다 작으면, w는 바이어스를 도입하지 않고 사용될 수 있다. 이와 달리, 의사 랜덤 번호 w가 이러한 최대 임계치 Pmax 이상이면, w는 버려지고 최대 임계치 Pmax 보다 작은 새로운 의사 랜덤 번호 w가 선택될 때까지 새로운 의사 랜덤 번호 w가 선택된다(1204).

[0109] 의사 랜덤 번호 w는 모듈로 n! 분할되어 w=w modulo (n!)이 된다(1206). 따라서, 치환(즉, 변환 테이블)을 획득하기 위해서 사용될 수 있는 바이어스되지 않은 의사 랜덤 번호 w가 범위 0 내지 n!에서 획득된다.

[0110] 사전-생성된 치환들을 저장하고 의사 랜덤 번호 w를 사용하여 하나의 이런 치환을 선택하기 보다는, 본 발명의 일 특징은 변환 테이블을 생성하기 위해서 베이스(base) 치환의 심벌들을 셔플링함으로써 하나의 치환을 생성하는 것을 제공한다. 베이스 치환 벡터 P는 심벌 세트의 모든 값들로 초기화되어 P = [0,1,2,...n-1}이 된다(1208). 그리고 나서 의사 랜덤 번호 w를 사용하여 베이스 치환 벡터 P의 심벌들을 셔플링하기 위해서, 심벌 셔플링 알고리즘(1020)이 사용된다.

[0111] 심벌 셔플링 알고리즘(1200)의 일 예는 카운터 i를 n-1로 초기화하는 것이며, 여기서 n은 세트 내의 심벌들의 수이다. 카운터 i>0이면, 의사 랜덤 번호 w=w/(i+1)이고, 변수 j=w modulo (i+1)이고, 치환 벡터 P의 값들은 셔플링되어 $P_t[i]=P_{t-1}[j]$이고 $P_t[j]=P_{t-1}[i]$가 된다. 다른 심벌 셔플링 알고리즘들이 본 발명의 영역을 벗어남이 없이 사용될 수 있다.

[0112] 치환 벡터 P가 셔플링되면, 예를 들어 입력 심벌 스트림을 암호화하기 위해서 변환 테이블로서 치환 벡터 P를 사용할 수 있는 임의의 애플리케이션에 치환 벡터 P가 제공될 수 있다(1212).

[0113] 도13은 하나의 평문 심벌을 암호화하기 위해서 다수의 변환 테이블들을 사용함으로써 심벌 인증을 달성할 수 있는 다른 암호화 방식을 보여주는 블록도이다. 즉, 평문 입력 심벌 Pi(1302)는 제1 암호 생성기(1308)로부터 획득된 제1 키 스트림 Si'(1306)에 기반하여 생성 또는 선택될 수 있는 변환 테이블 A1(1304)에 의해 암호화되어 제1 암호화된 출력 심벌 Ci'(1310)를 획득한다. 그리고 나서, 제1 암호화된 출력 심벌 Ci'(1310)는 제2 암호 생성기(1316)로부터 획득된 제2 키 스트림 Si(1314)에 기반하여 생성 또는 선택되고, 제2 암호화된 출력 심벌 Ci(1318)를 획득하기 위해서 사용되는, 제2 변환 테이블 A2(1312)에 대한 입력으로서 작용한다. 이러한 방식으로, 리던던시가 제1 암호화된 출력 심벌 Ci'(1310)을 인증하기 위해서 사용될 수 있다. 즉, 심벌 Ci'(1310) 및 Ci(1318)을 함께 사용함으로써, 심벌 Ci(1318)은 Ci'(1310)을 인증한다. 따라서, 공격자가 예를 들어 심벌 Ci'(1310)을 변경하는데 성공하더라도, 공격자는 심벌 Ci(1318)에 의해 적절하게 인증되지 않을 것이다.

[0114] 도14는 암호화된 심벌들(1408)의 대응하는 쌍을 획득하도록 각 평문 심벌(1402)을 암호화하기 위해서 다수의 변환 테이블(1404 및 1406)이 사용되는 방법을 보여주는 도이다. 변화 테이블들(1404 및 1406)은 각 평문 심벌 Pi를 한 쌍의 심벌들 Ci'/Ci로 암호화하기 위해서 의사 랜덤하게 선택 및/또는 생성될 수 있음에 유의하라.

[0115] 도15는 평문 심벌 Pn을 한 쌍의 심벌들 Cn' 및 Cn로 변환 또는 암호화하기 위해서 2개의 변환 테이블들이 사용되는 방법의 일 예의 보여주는 도이다. 예를 들어, 제1 평문 심벌 Pn='5'에 대해서, 제1 변환 테이블 A1(1502)는 제1 출력 심벌 Cn'=8을 제공한다(즉, '5'는 '8'로 변환된다). 그리고 나서, 제1 출력 심벌 '8'은 제2 변환 테이블 A2(1504)에 대한 입력으로서 작용하여 제2 출력 심벌 Cn=7을 획득한다(즉, '8'은 '7'로 변환된다).

제2 출력 심벌 Cn이 제1 출력 심벌 Cn'에 기반하여 생성되었기 때문에, 리던던트 심벌들 Cn 및 Cn'이 인증을 위해 사용될 수 있다. 이러한 심벌들 중 하나 또는 둘 모두가 전송기간 동안 공격자에 의해 변경되면, 인증은 실패한다. 예를 들어, Cn'이 '8'에서 '4'로 공격자에 의해 수정되면, 심벌 Cn' 및 Cn='47'을 수신하는 수신자는 Cn='7'은 Cn'는 '4'가 아니라 '8'을 의미하여야 함을 발견할 것이다.

[0116] 제2 평문 심벌 P(n+1)은 제1 평문 심벌 및 제2 평문 심벌이 동일한 경우에도 완전히 상이한 변환 테이블들을 가질 수 있다. 예를 들어, 제2 평문 심벌 P(n+1)='5'의 경우, 제1 변환 테이블 B1(1506)은 제3 출력 심벌 C(n+1)'='*'를 제공한다(즉, '5'는 '*'로 변환됨). 제3 출력 심벌 C(n+1)'='*'은 제4 출력 심벌 C(n+1)='1'을 획득하기 위해서 제2 변환 테이블 B2(1508)에 대한 입력으로서 작용한다(즉, '*'는 '1'로 변환됨). 전과 같이, 심벌 쌍 C(n+1)' 및 C(n+1)의 리던던트한 사용은 인증의 일 형태로 기능할 수 있다.

[0117] 도16은 일 예에 따른 평문 암호화 수행을 위한 방법을 보여준다. n개의 심벌들 세트 내에 정의된 다수의 입력 심벌들이 획득된다(1602). 상이한 심벌 대 심벌 치환들을 정의하는 다수의 변환 테이블들로부터 의사 랜덤하게 선택된 변환 테이블이 암호화될 각 입력 심벌들에 대해 획득된다(1604). 입력 심벌들은 각 입력 심벌을 개별적으로 암호화하기 위해서 입력 심벌들 각각에 대해 그들의 상응하는 변환 테이블을 사용하여 상응하는 출력 심벌들로 변환된다. 그리고 나서, 출력 심벌들은 암호해득 장치(1608)로 전송될 수 있다.

[0118] 이러한 방법의 일 예에서, 제1 평문 심벌이 획득되고, 여기서 제1 평문 심벌은 세트 내의 n개의 심벌들 중 하나일 수 있다. n개의 심벌들을 n개의 심벌들의 상이한 치환으로 변환하는 제1 변환 테이블이 획득된다. 제1 변환 테이블은 n개의 심벌들을 셔플링하기 위해서 의사 랜덤 번호를 사용함으로써 의사 랜덤하게 생성될 수 있다. 그리고 나서, 제1 평문 심벌은 제1 변환 테이블을 사용하여 제1 출력 심벌로 변환된다.

[0119] n개의 심벌들을 제1 변환 테이블과는 다른 n개의 심벌들의 치환으로 변환하는 제2 변환 테이블이 획득된다. 제1 출력 심벌은 제2 변환 테이블을 사용하여 제2 출력 심벌로 변환된다. 그리고 나서, 암호화된 심벌은 제1 및/또는 제2 출력 심벌들에 기반하여 전송된다.

[0120] 도17은 단일 평문 심벌을 획득하기 위해서 하나 이상의 역 변환 테이블들을 사용함으로써 암호화된 심벌들 Ci가 암호해독되는 방법을 보여주는 블록도이다. 즉, 암호화된 입력 심벌 Ci(1702)은 제1 암호 생성기(1708)로부터 획득된 제1 키 스트림 Si'(1706)에 기반하여 생성 또는 선택될 수 있는 제1 역 변환 테이블 A1(1704)에 의해 암호해독되어 제1 암호해독된 출력 심벌 Ci'(1710)을 획득한다. 그리고 나서, 제1 암호해독된 출력 심벌 Ci'(1710)은 제2 암호 생성기(1716)로부터 획득된 제2 키 스트림 Si(1704)에 기반하여 생성 또는 선택될 수 있고, 평문 출력 심벌 Pi(1718)을 획득하는데 사용되는, 제2 역 변환 테이블 A2(1712)에 대한 입력으로 작용한다.

[0121] 대안적인 구현에서, 예를 들어, Ci=(x,y)인 경우, 암호화된 심벌들 x 및 y는 평문 출력 심벌 Pi를 획득하기 위해서 이들이 암호화된 순의 역순으로 암호해독된다.

[0122] 도18은 일 예에 따른 심벌 암호해독을 수행하는 방법을 보여준다. n개의 심벌들 세트 내에 정의된 다수의 (암호화된) 입력 심벌들이 획득된다(1802). 암호해독될 입력 심벌들 각각에 대해서, 상이한 심벌 대 심벌 치환들을 정의하는 다수의 역 변환 테이블들로부터, 의사랜덤하게 선택된 역 변환 테이블이 획득된다(1804). 각 입력 심벌을 개별적으로 암호해독하기 위해서 각 입력 심벌들에 대해 그들의 대응하는 역 변환 테이블을 사용하여 입력 심벌들을 대응하는 출력 심벌들로 변환한다(1806).

[0123] 이러한 방법의 일 예에서, 제1 암호화된 심벌(입력 심벌)이 획득되고, 여기서 제1 암호화된 심벌은 세트 내의 n개의 심벌들 중 하나이다. n개의 심벌들을 n개의 심벌들의 상이한 치환으로 변환하는 제1 역 변환 테이블이 또한 획득된다. 제1 역 변환 테이블은 n개의 심벌들을 셔플링하기 위해서 의사 랜덤 번호에 의해 의사 랜덤하게 생성될 수 있다. 제1 암호화된 심벌은 제1 역 변환 테이블을 사용하여 제1 출력 심벌로 변환된다. n개의 심벌들을 제1 변환 테이블과는 다른 n개의 심벌들의 치환으로 변환하는 제2 역 변환 테이블이 획득된다. 제1 출력 심벌은 제2 역 변환 테이블을 사용하여 제2 출력 심벌로 변환된다. 그리고 나서, 평문 심벌이 제1 및/또는 제2 출력 심벌들에 기반하여 획득될 수 있다.

[0124] 도19는 일 예에 따른 암호화 모듈을 보여주는 블록도이다. 암호화 모듈(1902)은 시드를 키 스트림 생성기(1906)에 제공하도록 구성된 처리회로(1904)를 포함할 수 있다. 키 스트림 생성기(1906)는 처리 회로(1904)로 전송되는 의사 랜덤 번호들 또는 심벌들의 키 스트림을 생성한다. 처리 회로(1904)에 연결된 입력 인터페이스(1908)는 평문 심벌 스트림을 수신할 수 있다. 평문 심벌 스트림을 암호화하기 위해서, 처리 회로(1904)는 키 스트림으로부터 획득된 의사 랜덤 번호를 사용하여 변환 테이블 생성기(1910)로부터 변환 테이블을 획득하도록 구성된다. 변환 테이블 생성기(1910)는 변환 테이블을 제공하기 위해서 의사 랜덤, 넌-바이어스된 방식으로 베

이스 테이블의 심벌들을 예를 들어 셔플링 및/또는 조합하기 위해 의사 랜덤 번호를 사용하도록 구성될 수 있다. 그리고 나서, 처리 회로(1904)는 변환 테이블을 한 번 사용하여 제1 평문 심벌을 암호화된 심벌 스트림의 제1 암호화된 심벌로 변환한다. 암호화된 심벌 스트림은 처리 회로(1904)에 연결된 출력 인터페이스(1912)를 통해 전송될 수 있다. 평문 심벌 스트림의 각 평문 심벌에 대해서, 그 심벌을 변환하는 상이한 변환 테이블이 생성되고 사용될 수 있다.

[0125] 도20은 일 예에 따른 암호해독 모듈을 보여주는 블록도이다. 암호해독 모듈(2002)은 시드를 키 스트림 생성기(2006)로 제공하도록 구성된 처리 회로(2004)를 포함할 수 있다. 키 스트림 생성기(2006)는 처리 회로(2004)로 전송되는 의사 랜덤 번호들 또는 심벌들의 키 스트림을 생성한다. 처리 회로(2004)에 연결된 입력 인터페이스(2008)는 암호화된 심벌 스트림을 수신할 수 있다. 암호화된 심벌 스트림을 암호해독하기 위해서, 처리 회로(2004)는 역 변환 테이블 생성기(2010)로부터 변환 테이블을 획득하기 위해 키 스트림으로부터 획득된 의사랜덤 번호를 사용하도록 구성될 수 있다. 역 변환 테이블 생성기(2010)는 변환 테이블을 제공하기 위해서 의사 랜덤, 넌-바이어스된 방식으로 예를 들어 심벌들을 셔플링 및/또는 조합하기 위해서 의사 랜덤 번호를 사용하도록 구성될 수 있다. 그리고 나서, 처리 회로(2004)는 역 변환 테이블을 한 번 사용하여 제1 암호화된 심벌을 평문 심벌 스트림의 제1 평문 심벌로 변환한다. 평문 심벌 스트림은 처리 회로(2004)에 연결된 출력 인터페이스(2012)를 통해 전송될 수 있다.

[0126] 암호화 모듈(1902) 및 암호해독 모듈(2002)은 심벌을 각각 적절하게 암호화 및 암호해독하도록 하기 위해서, 이들은 동일한 키 스트림 생성기를 가지고 상보적인 변환 테이블 생성기들을 가질 수 있다. 키 스트림 생성기들(1906 및 2006)을 동기화하기 위해서, 공통 시드가 암호화 모듈 및 암호해독 모듈 사이의 특정 통신 세션에 대해 (예를 들어, 보안 인증 방식에 의해) 설정될 수 있다. 예를 들어, 세션 키가 키 스트림 생성기들(1906 및 2006)에 대한 시드로 사용될 수 있다.

[0127] 여기 제시된 실시예들 중 일부는 DTMF 톤들의 암호화를 참조하지만, 여기 제시된 암호화 방법은 전송되는 정보를 안전하게 보호하기 위해서 다양한 다른 타입의 통신 시스템들에서 구현될 수 있다.

[0128] 도1-18에 제시된 하나 이상의 컴포넌트, 단계, 및/또는 기능부들은 하나의 컴포넌트, 단계, 및/또는 기능부로 재배열 및/또는 결합될 수 있고, 수개의 컴포넌트, 단계, 및/또는 기능부로 분리될 수 있으며, 이들 모두 본 발명의 영역 내에 속한다. 추가적인 엘리먼트, 컴포넌트, 단계, 및/또는 기능부가 본 발명의 영역을 벗어남이 없이 추가될 수 있다. 도1,2,3,5,7,9,13,17,19 및/또는 20에 제시된 장치, 디바이스, 및/또는 컴포넌트들은 도2,4,6,8,10,11,12,14,15,16 및/또는 18에 제시된 방법, 특징, 또는 단계들 중 하나 이상을 수행하도록 구성될 수 있다.

[0129] 당업자는 여기 제시된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이 둘의 조합으로 구현될 수 있음을 잘 이해할 수 있을 것이다. 하드웨어 및 소프트웨어의 이러한 상호교환성을 명확하게 설명하기 위해서, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들이 그들의 기능의 관점에서 서술되었다. 이러한 기능이 하드웨어로 구현되는지 아니면 소프트웨어로 구현되는지는 전체 시스템에 부가되는 디자인 제한 및 특정 애플리케이션에 기반한다.

[0130] 전술한 실시예들이 단지 일 예들일 뿐이며, 본 발명이 이들로 제한되는 것은 아니다. 이러한 예들에 대한 설명은 단지 예시적인 본 발명의 권리범위를 한정하지는 않는다. 따라서, 본 발명의 다양한 변형이 가능함을 당업자는 잘 이해할 수 있을 것이다.

[0131]

도면의 간단한 설명

[0030] 도1은 전화기 및 보안 서버 사이의 특정 통신들을 안전하게 하기 위해서 전화기에 통신 라인을 따라 보안 장치가 연결되는 시스템을 보여주는 도이다.

[0031] 도2는 도1의 발행 기관에 속하는 보안 서버와 전화기 사이의 특정 통신을 안전하게 하기 위한 방법에 대한 흐름도이다.

[0032] 도3은 전송기간 동안 DTMF 톤들을 안전하게 하는 것을 인에이블할 수 있는 텔레-서비스 보안 서버의 일 예에 대한 블록도이다.

[0033] 도4는 전화기 장치로부터 DTMF 톤들을 안전하게 하기 위해 보안 서버에서 동작하는 방법을 보여주는 도이다.

[0034] 도5는 전송기간 동안 DTMF 톤들을 보호하기 위해서 구성될 수 있는 보안 장치의 일 예에 대한 블록도이다.

[0035] 도6은 전화기 장치로부터 DTMF 톤들을 안전하게 하기 위해서 보안 장치상에서 동작하는 방법을 보여주는 도이다.

[0036] 도7은 보안 서버를 통해 자신을 인증하도록 구성된 이동 통신 장치의 블록도이다.

[0037] 도8은 통신 네트워크를 통해 텔레-서비스 스테이션에 대해 이동 통신 장치를 인증하기 위한 방법에 대한 흐름도이다.

[0038] 도9는 암호화될 각 심벌에 대한 변환 테이블을 의사랜덤하게 선택함으로써 평문 심벌들을 안전하게 하기 위한 조합 결합기의 블록도이다.

[0039] 도10은 평문 심벌을 암호화된 심벌로 변환하기 위한 심벌 대 심벌 변환 테이블의 일 예를 보여주는 도이다.

[0040] 도11은 암호화된 심벌들을 획득하기 위해서 상이한 변환 테이블들을 사용하여 평문 심벌들이 암호화되는 방법에 대한 일 예를 보여주는 도이다.

[0041] 도12는 한 세트의 n개의 심벌들에 대한 다수의 가능한 치환들로부터 변환 테이블을 선택하기 위한 알고리즘을 보여주는 도이다.

[0042] 도13은 하나의 평문 심벌을 암호화하기 위해서 다수의 변환 테이블을 사용함으로써 심벌 인증을 달성할 수 있는 다른 암호화 방식을 보여주는 블록도이다.

[0043] 도14는 대응하는 암호화된 심벌을 획득하기 위해서 다수의 변환 테이블들이 각 평문 심벌을 암호화하는데 사용될 수 있는 방법을 보여주는 도이다.

[0044] 도15는 평문 심벌을 암호화된 심벌로 변환 또는 암호화하기 위해서 2개의 변환 테이블들이 사용될 수 있는 방법의 일 예를 보여주는 도이다.

[0045] 도16은 일 예에 따라 평문 암호화를 수행하기 위한 방법을 보여주는 도이다.

[0046] 도17은 하나의 평문 심벌을 획득하기 위해서 하나 이상의 역 변환 테이블들을 사용하여 암호화된 심벌들이 암호해독될 수 있는 방법을 보여주는 블록도이다.

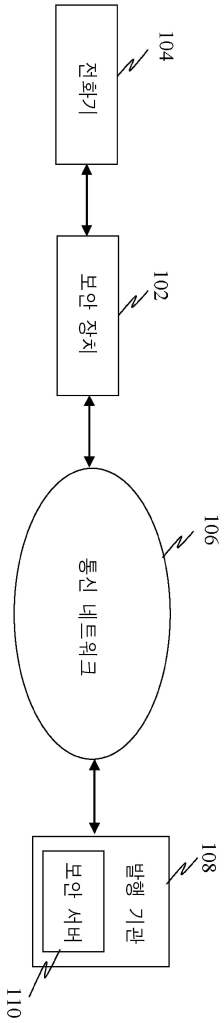
[0047] 도18은 일 예에 따라 평문 암호화를 수행하는 방법을 보여주는 도이다.

[0048] 도19는 일 예에 따른 암호화 모듈을 보여주는 블록도이다.

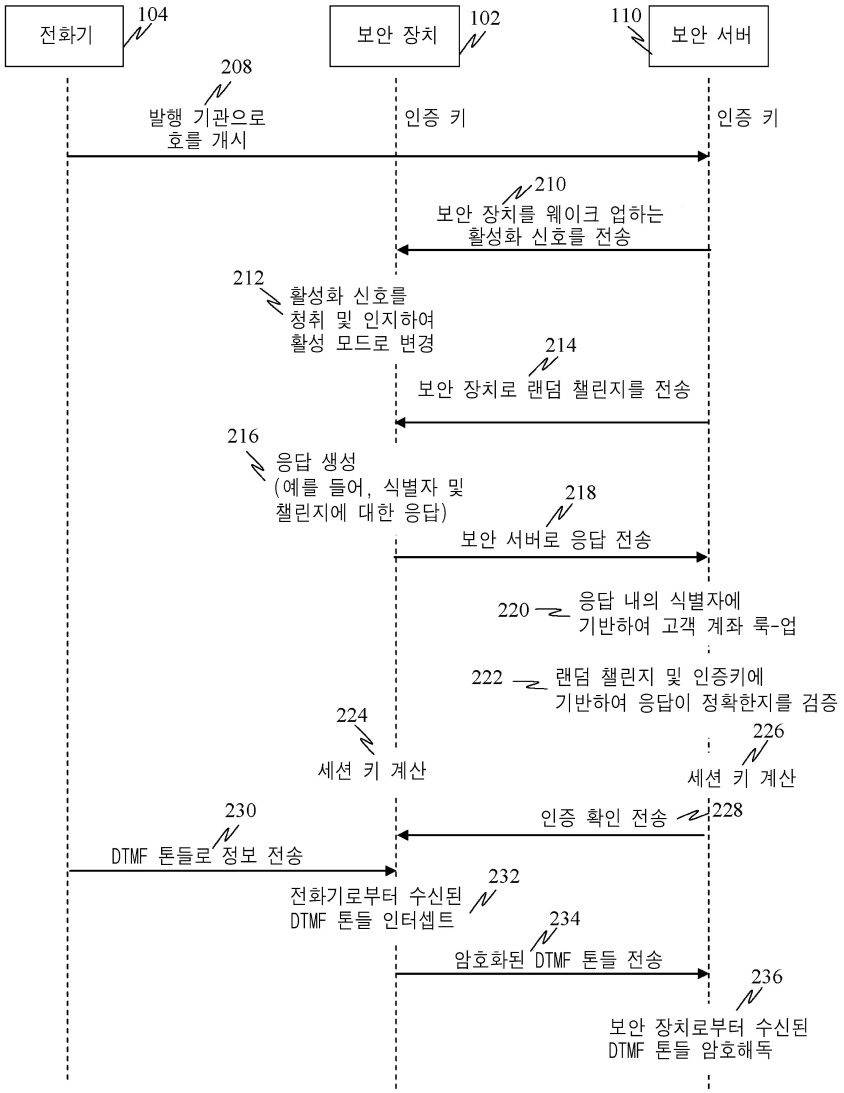
[0049] 도20은 일 예에 따라 암호해독 모듈을 보여주는 블록 다이아그램이다.

도면

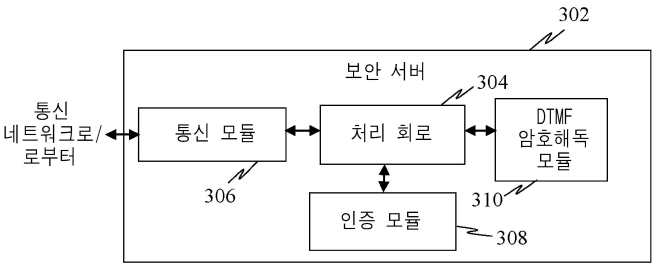
도면1



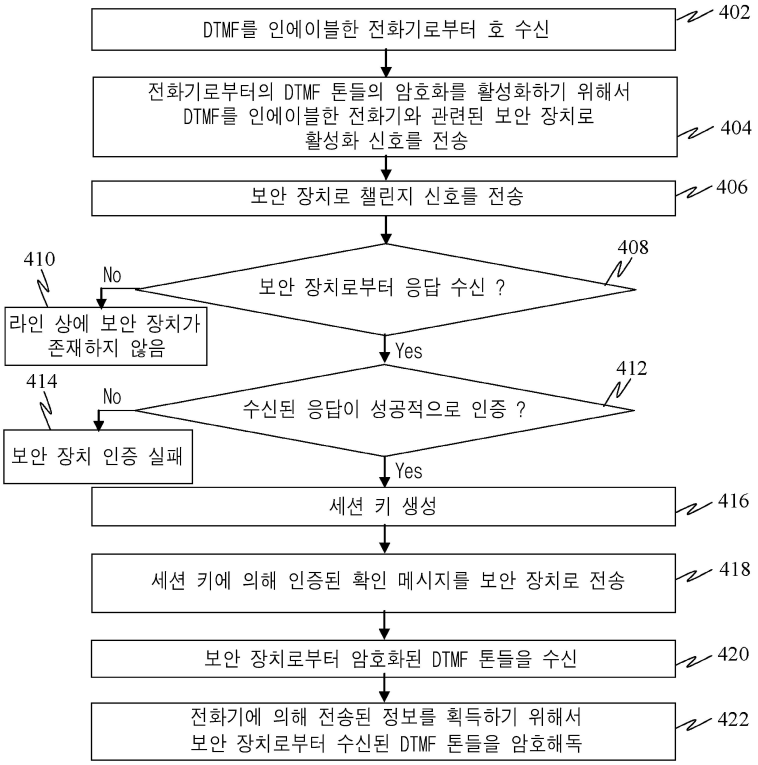
도면2


전화기
104
보안 장치
102
110
보안 서버
208
발행 기관으로
호를 개시
인증 키
인증 키
210
보안 장치를 웨이크 업하는
활성화 신호를 전송
212
활성화 신호를
청취 및 인지하여
활성 모드로 변경
214
보안 장치로 랜덤 챌린지를 전송
216
응답 생성
(예를 들어, 식별자 및
챌린지에 대한 응답)
218
보안 서버로 응답 전송
220
응답 내의 식별자에
기반하여 고객 계좌 룩-업
222
랜덤 챌린지 및 인증키에
기반하여 응답이 정확한지를 검증
224
세션 키 계산
226
세션 키 계산
230
DTMF 톤들로 정보 전송
인증 확인 전송
228
232
전화기로부터 수신된
DTMF 톤들 인터셉트
234
암호화된 DTMF 톤들 전송
236
보안 장치로부터 수신된
DTMF 톤들 암호해독

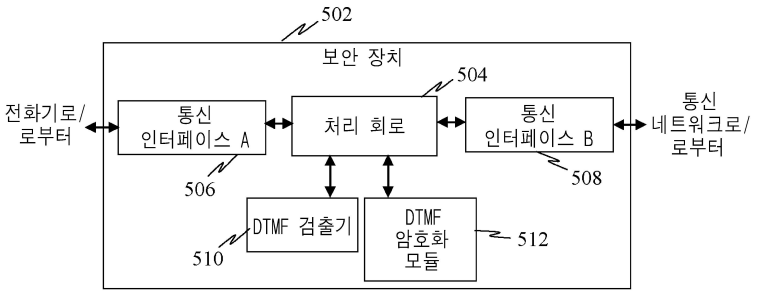
도면3


302
보안 서버
304
통신
네트워크로/
로부터
통신 모듈
처리 회로
DTMF
암호해독
모듈
306
310
인증 모듈
308

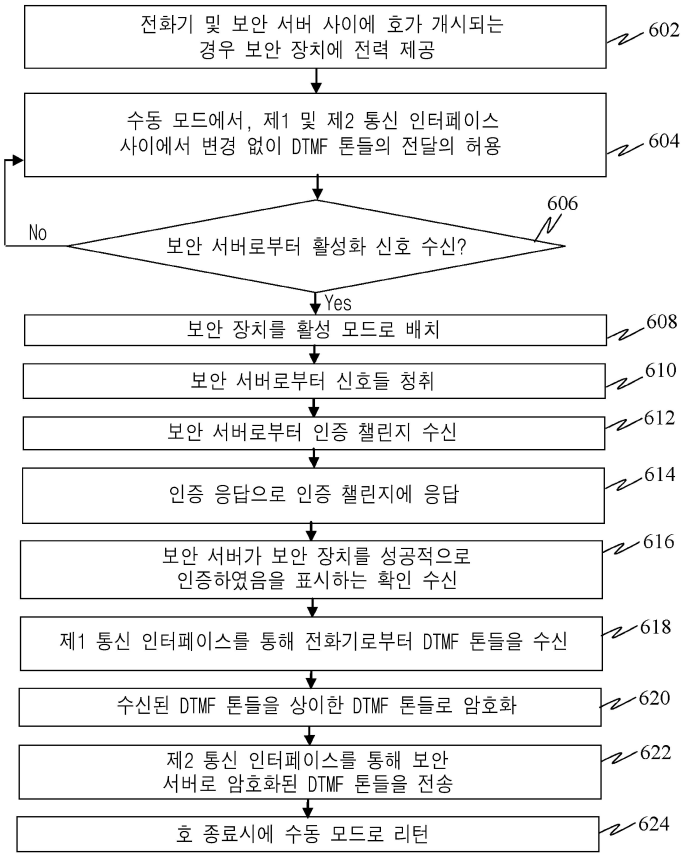
도면4


DTMF를 인에이블한 전화기로부터 호 수신
402
전화기로부터의 DTMF 톤들의 암호화를 활성화하기 위해서
DTMF를 인에이블한 전화기와 관련된 보안 장치로
활성화 신호를 전송
404
보안 장치로 챌린지 신호를 전송
406
410
No
보안 장치로부터 응답 수신 ?
408
라인 상에 보안 장치가
존재하지 않음
Yes
414
No
수신된 응답이 성공적으로 인증 ?
412
보안 장치 인증 실패
Yes
세션 키 생성
416
세션 키에 의해 인증된 확인 메시지를 보안 장치로 전송
418
보안 장치로부터 암호화된 DTMF 톤들을 수신
420
전화기에 의해 전송된 정보를 획득하기 위해서
보안 장치로부터 수신된 DTMF 톤들을 암호해독
422

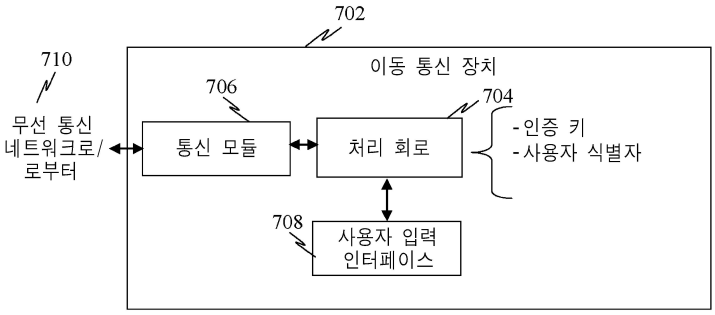
도면5


502
보안 장치
504
전화기로/
로부터
통신
인터페이스 A
처리 회로
통신
인터페이스 B
통신
네트워크로/
로부터
506
508
DTMF 검출기
510
DTMF
암호화
모듈
512

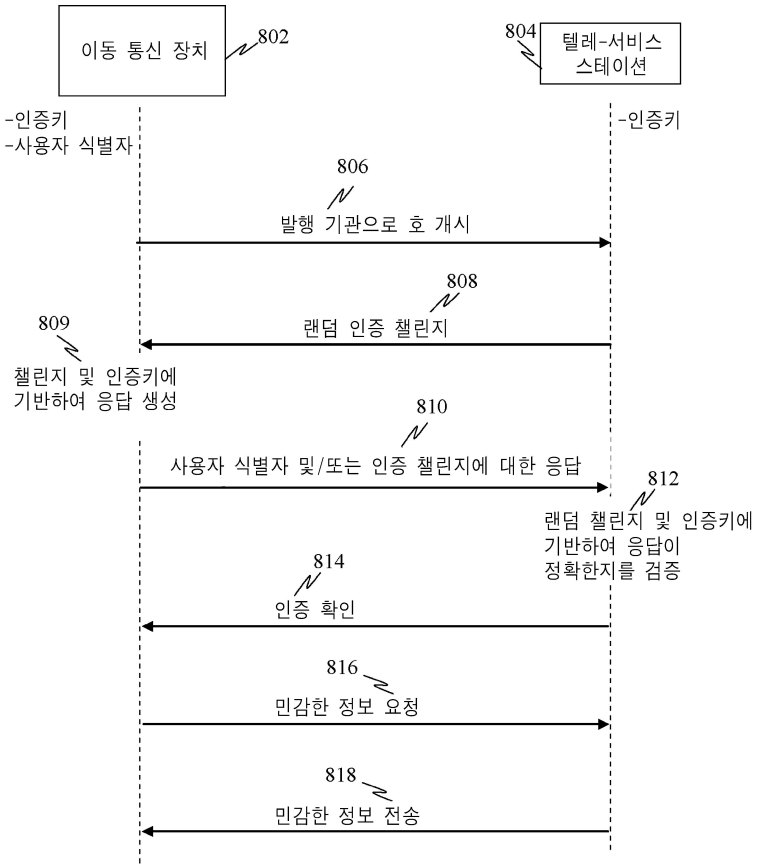
도면6


전화기 및 보안 서버 사이에 호가 개시되는 경우 보안 장치에 전력 제공
602
수동 모드에서, 제1 및 제2 통신 인터페이스 사이에서 변경 없이 DTMF 톤들의 전달의 허용
604
606
No
보안 서버로부터 활성화 신호 수신?
Yes
보안 장치를 활성 모드로 배치
608
보안 서버로부터 신호들 청취
610
보안 서버로부터 인증 챌린지 수신
612
인증 응답으로 인증 챌린지에 응답
614
보안 서버가 보안 장치를 성공적으로 인증하였음을 표시하는 확인 수신
616
제1 통신 인터페이스를 통해 전화기로부터 DTMF 톤들을 수신
618
수신된 DTMF 톤들을 상이한 DTMF 톤들로 암호화
620
제2 통신 인터페이스를 통해 보안 서버로 암호화된 DTMF 톤들을 전송
622
호 종료시에 수동 모드로 리턴
624

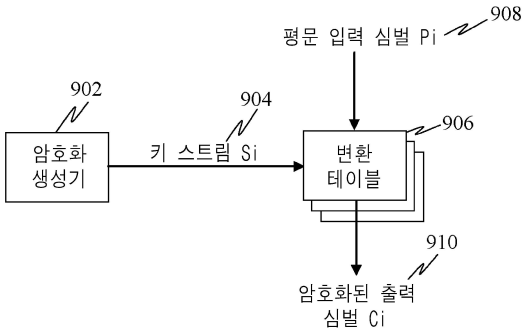
도면7


702
이동 통신 장치
710
무선 통신 네트워크로/로부터
706
통신 모듈
704
처리 회로
-인증 키
-사용자 식별자
708
사용자 입력 인터페이스

도면8


이동 통신 장치
802
804
텔레-서비스 스테이션
-인증키
-사용자 식별자
-인증키
806
발행 기관으로 호 개시
808
랜덤 인증 챌린지
809
챌린지 및 인증키에 기반하여 응답 생성
810
사용자 식별자 및/또는 인증 챌린지에 대한 응답
812
랜덤 챌린지 및 인증키에 기반하여 응답이 정확한지를 검증
814
인증 확인
816
민감한 정보 요청
818
민감한 정보 전송

도면9

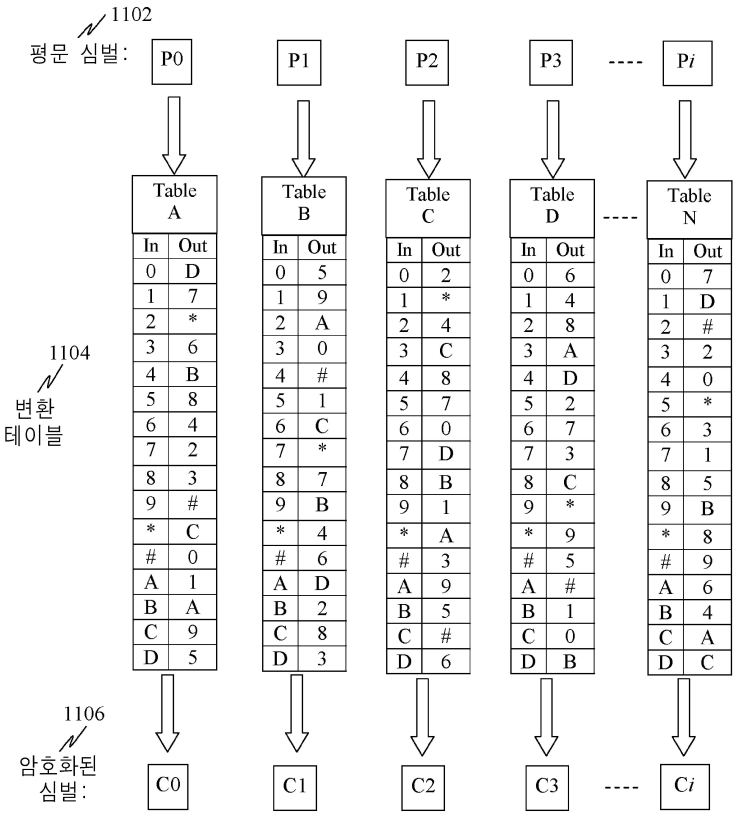

평문 입력 심벌 Pi
908
902
암호화 생성기
904
키 스트림 Si
906
변환 테이블
910
암호화된 출력 심벌 Ci

도면10

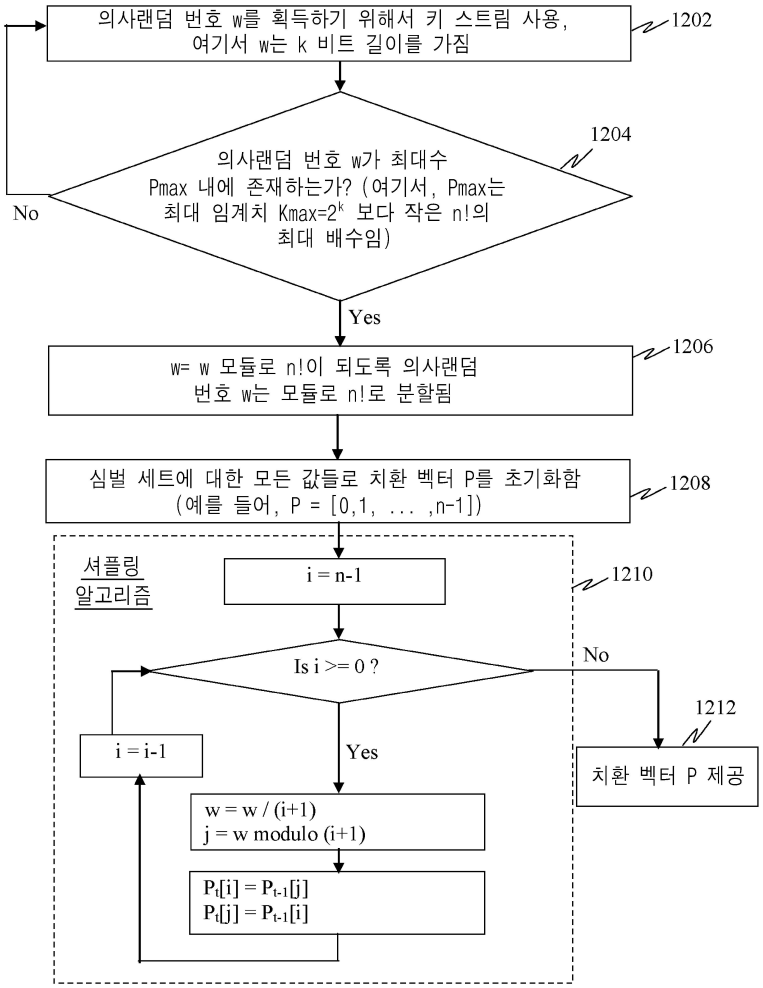
평문 심벌	평문 심벌의 이진 표현	암호화된 이진 심벌	이진 암호화된 심벌들의 이진 표현
0	0000	5	0101
1	0001	9	1001
2	0010	A	1100
3	0011	0	0000
4	0100	#	1011
5	0101	1	0001
6	0110	C	1110
7	0111	*	1010
8	1000	7	0111
9	1001	B	1101
*	1010	4	0100
#	1011	6	0110
A	1100	D	1111
B	1101	2	0001
C	1110	8	1000
D	1111	3	0011

1002

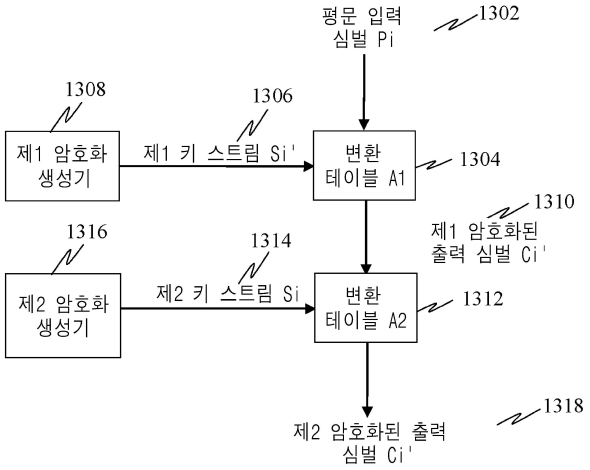
도면11



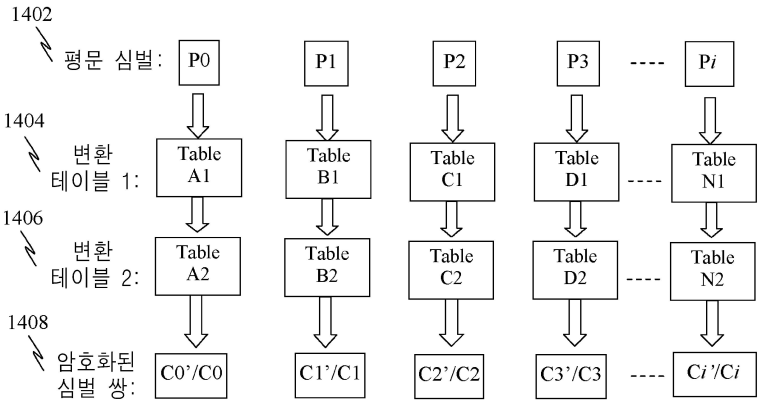
도면12


의사랜덤 번호 w를 획득하기 위해서 키 스트림 사용, 여기서 w는 k 비트 길이를 가짐
1202
의사랜덤 번호 w가 최대수 Pmax 내에 존재하는가? (여기서, Pmax는 최대 임계치 Kmax=2^k 보다 작은 n!의 최대 배수임)
1204
No
Yes
w= w 모듈로 n!이 되도록 의사랜덤 번호 w는 모듈로 n!로 분할됨
1206
심벌 세트에 대한 모든 값들로 치환 벡터 P를 초기화함 (예를 들어, P = [0,1, ... ,n-1])
1208
셔플링 알고리즘
i = n-1
1210
Is i >= 0 ?
No
Yes
i = i-1
w = w / (i+1)
j = w modulo (i+1)
Pt[i] = Pt-1[j]
Pt[j] = Pt-1[i]
1212
치환 벡터 P 제공

도면13

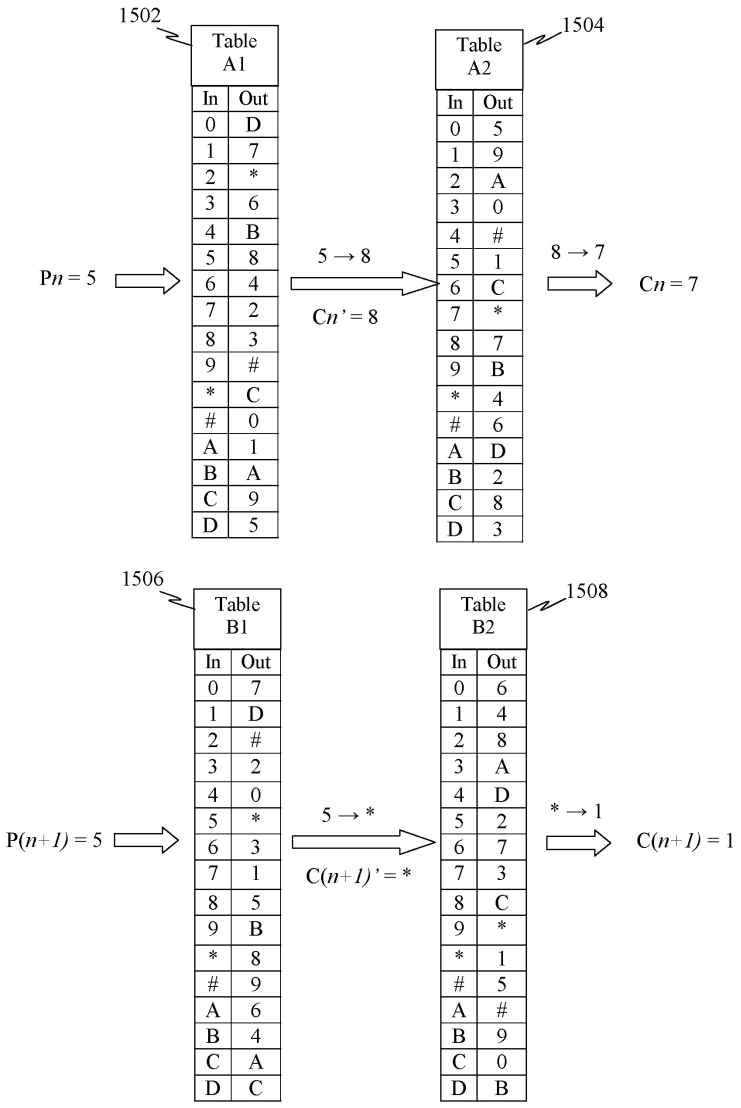

평문 입력 심벌 Pi
1302
1308
제1 암호화 생성기
1306
제1 키 스트림 Si'
변환 테이블 A1
1304
1310
제1 암호화된 출력 심벌 Ci'
1316
제2 암호화 생성기
1314
제2 키 스트림 Si
변환 테이블 A2
1312
제2 암호화된 출력 심벌 Ci'
1318

도면14

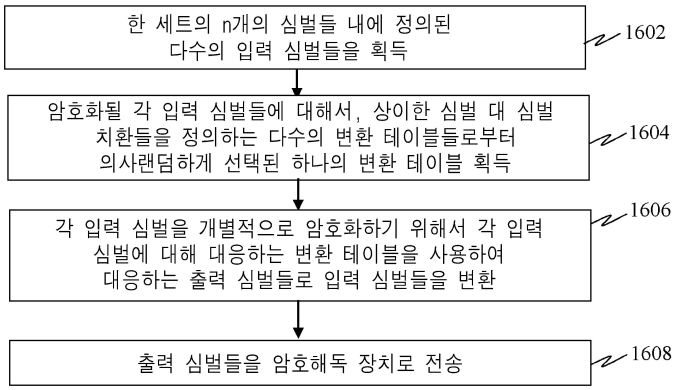

1402
평문 심벌:
P0
P1
P2
P3

Pi
1404
변환 테이블 1:
Table A1
Table B1
Table C1
Table D1
Table N1
1406
변환 테이블 2:
Table A2
Table B2
Table C2
Table D2
Table N2
1408
암호화된 심벌 쌍:
C0'/C0
C1'/C1
C2'/C2
C3'/C3
Ci'/Ci

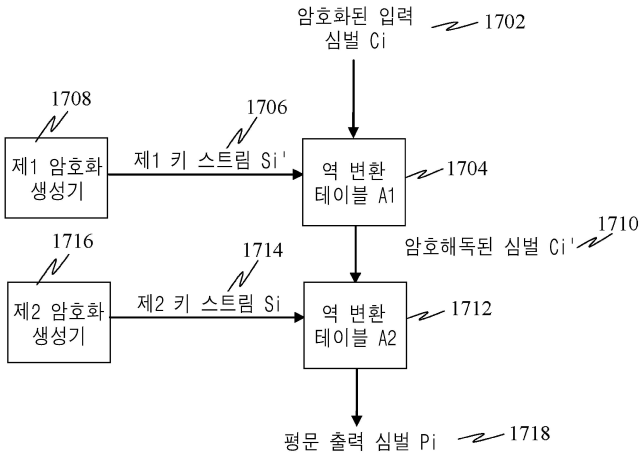
도면15


1502
Table A1
In Out
0 D
1 7
2 *
3 6
4 B
5 8
6 4
7 2
8 3
9 #
* C
# 0
A 1
B A
C 9
D 5
Pn = 5
5 → 8
Cn' = 8
1504
Table A2
In Out
0 5
1 9
2 A
3 0
4 #
5 1
6 C
7 *
8 7
9 B
* 4
# 6
A D
B 2
C 8
D 3
8 → 7
Cn = 7
1506
Table B1
In Out
0 7
1 D
2 #
3 2
4 0
5 *
6 3
7 1
8 5
9 B
* 8
# 9
A 6
B 4
C A
D C
P(n+1) = 5
5 → *
C(n+1)' = *
1508
Table B2
In Out
0 6
1 4
2 8
3 A
4 D
5 2
6 7
7 3
8 C
9 *
* 1
# 5
A #
B 9
C 0
D B
* → 1
C(n+1) = 1

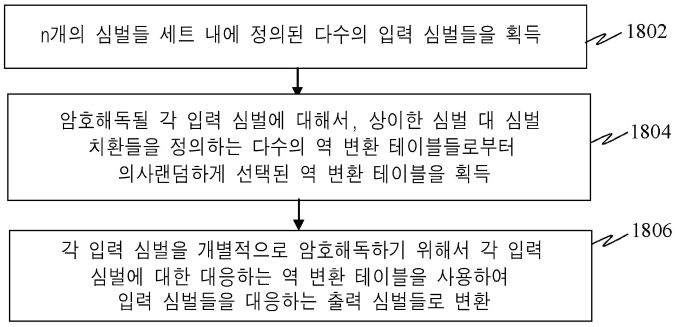
도면16



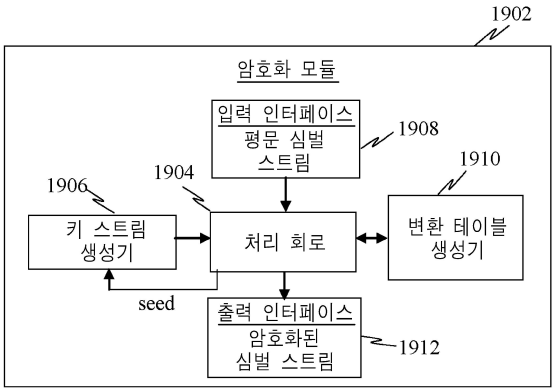
도면17



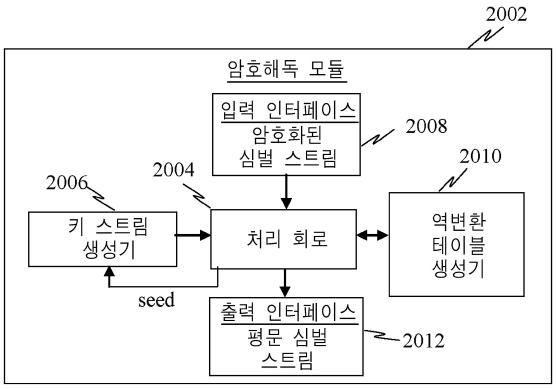
도면18



도면19


1902
암호화 모듈
입력 인터페이스
평문 심벌
스트림
1908
1910
1906
1904
키 스트림
생성기
처리 회로
변환 테이블
생성기
seed
출력 인터페이스
암호화된
심벌 스트림
1912

도면20


2002
암호해독 모듈
입력 인터페이스
암호화된
심벌 스트림
2008
2010
2006
2004
키 스트림
생성기
처리 회로
역변환
테이블
생성기
seed
출력 인터페이스
평문 심벌
스트림
2012