(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0058310
(43) 공개일자 2015년05월28일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 9/00* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 63/0428 (2013.01)
H04L 63/123 (2013.01)
(21) 출원번호 10-2015-7009352
(22) 출원일자(국제) 2013년09월12일
심사청구일자 없음
(85) 번역문제출일자 2015년04월10일
(86) 국제출원번호 PCT/US2013/059524
(87) 국제공개번호 WO 2014/043392
국제공개일자 2014년03월20일
(30) 우선권주장
61/701,384 2012년09월14일 미국(US)
13/764,524 2013년02월11일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
제이콥슨, 데이비드 엠.
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
브럼리, 빌리 비.
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

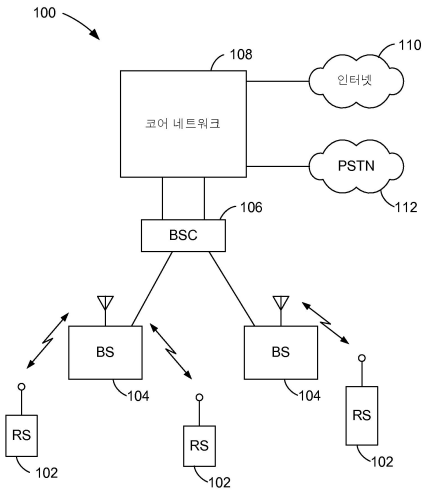
전체 청구항 수 : 총 80 항

(54) 발명의 명칭 **메시지 데이터를 보호하기 위한 장치 및 방법**

(57) 요 약

메시지 데이터를 보호하기 위한 방법이 개시된다. 상기 방법에서, 메시지 데이터에는 메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들이 패딩된다. 패딩된 메시지 데이터는 압축된 데이터를 생성하도록 압축된다. 압축된 데이터의 길이는 패딩 비트들에 의존한다. 압축된 데이터는 암호화된 메시지 데이터를 생성하도록 암호화된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/1475 (2013.01)
H04L 69/04 (2013.01)
H04L 9/002 (2013.01)
H04L 9/3223 (2013.01)
H04L 9/3242 (2013.01)
H04L 2209/16 (2013.01)
H04L 2209/20 (2013.01)
H04L 2209/30 (2013.01)

명 세 서

청구범위

청구항 1

메시지 데이터를 보호하기 위한 방법으로서,

상기 메시지 데이터 상에서 수행되는 결정론적 함수(deterministic function)에 기초하여 생성된 패딩 비트들(padding bits)을 상기 메시지 데이터에 패딩하는 단계,

압축된 데이터를 생성하기 위해, 패딩된 메시지 데이터를 압축하는 단계 - 상기 압축된 데이터의 길이는 상기 패딩 비트들에 의존함 - , 및

암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하는 단계를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 2

제 1 항에 있어서,

상기 결정론적 함수는 해시(hash) 함수를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 3

제 1 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱(prefixed)되는,

메시지 데이터를 보호하기 위한 방법.

청구항 4

제 1 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝(end)이 수신기에 의해 결정되게 허용하도록 제약되는,

메시지 데이터를 보호하기 위한 방법.

청구항 5

원격 스테이션으로서,

메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들을 상기 메시지 데이터에 패딩하기 위한 수단,

압축된 데이터를 생성하기 위해, 패딩된 메시지 데이터를 압축하기 위한 수단 - 상기 압축된 데이터의 길이는 상기 패딩 비트들에 의존함 - , 및

암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하기 위한 수단을 포함하는,

원격 스테이션.

청구항 6

제 5 항에 있어서,

상기 결정론적 함수는 해시 함수를 포함하는,

원격 스테이션.

청구항 7

제 5 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱되는,

원격 스테이션.

청구항 8

제 5 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약되는,

원격 스테이션.

청구항 9

원격 스테이션으로서,

프로세서를 포함하고, 상기 프로세서는,

메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들을 상기 메시지 데이터에 패딩하고,

압축된 데이터를 생성하기 위해, 패딩된 메시지 데이터를 압축하고 - 상기 압축된 데이터의 길이는 상기 패딩 비트들에 의존함 - , 그리고

암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하도록 구성되는,

원격 스테이션.

청구항 10

제 9 항에 있어서,

상기 결정론적 함수는 해시 함수를 포함하는,

원격 스테이션.

청구항 11

제 9 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱되는,

원격 스테이션.

청구항 12

제 9 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약되는,

원격 스테이션.

청구항 13

컴퓨터-판독 가능 매체를 포함하는 컴퓨터 프로그램 물건으로서,

상기 컴퓨터-판독 가능 매체는,

컴퓨터로 하여금, 메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들을 상기 메시지 데이터에 패딩하게 하기 위한 코드,

컴퓨터로 하여금, 압축된 데이터를 생성하기 위해, 패딩된 메시지 데이터를 압축하게 하기 위한 코드 - 상기

압축된 데이터의 길이는 상기 패딩 비트들에 의존함 - , 및

컴퓨터로 하여금, 암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는,

컴퓨터 프로그램 물건.

청구항 14

제 13 항에 있어서,

상기 결정론적 함수는 해시 함수를 포함하는,

컴퓨터 프로그램 물건.

청구항 15

제 13 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱되는,

컴퓨터 프로그램 물건.

청구항 16

제 13 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약되는,

컴퓨터 프로그램 물건.

청구항 17

메시지 데이터를 보호하기 위한 방법으로서,

상기 메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택하는 단계,

압축된 데이터를 생성하기 위해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 상기 메시지 데이터를 압축하는 단계 - 상기 압축된 데이터의 길이는 상기 압축 파라미터 값에 의존함 - , 및

암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하는 단계를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 18

제 17 항에 있어서,

상기 압축 파라미터 값은 최대 체인 길이 값인,

메시지 데이터를 보호하기 위한 방법.

청구항 19

제 17 항에 있어서,

상기 결정론적 함수는 해시 함수를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 20

제 17 항에 있어서,

상기 메시지 데이터를 압축하는 단계는,

패딩된 메시지 데이터를 생성하기 위해 상기 결정론적 함수에 기초하여 선택된 다수의 패딩 비트들을 상기 메시지 데이터에 패딩하는 단계, 및

상기 패딩된 메시지 데이터에 대해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용함으로써 상기 압축된 데이터를 생성하는 단계를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 21

제 20 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱되는,

메시지 데이터를 보호하기 위한 방법.

청구항 22

제 20 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약되는,

메시지 데이터를 보호하기 위한 방법.

청구항 23

원격 스테이션으로서,

메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택하기 위한 수단,

압축된 데이터를 생성하기 위해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 상기 메시지 데이터를 압축하기 위한 수단 - 상기 압축된 데이터의 길이는 상기 압축 파라미터 값에 의존함 - , 및

암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하기 위한 수단을 포함하는,

원격 스테이션.

청구항 24

제 23 항에 있어서,

상기 압축 파라미터 값은 최대 체인 길이 값인,

원격 스테이션.

청구항 25

제 23 항에 있어서,

상기 결정론적 함수는 해시 함수를 포함하는,

원격 스테이션.

청구항 26

제 23 항에 있어서,

상기 메시지 데이터를 압축하기 위한 수단은,

패딩된 메시지 데이터를 생성하기 위해 상기 결정론적 함수에 기초하여 선택된 다수의 패딩 비트들을 상기 메시지 데이터에 패딩하기 위한 수단, 및

상기 패딩된 메시지 데이터에 대해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용함으로써 상기 압축된 데이터를 생성하기 위한 수단을 포함하는,

원격 스테이션.

청구항 27

제 26 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱되는,

원격 스테이션.

청구항 28

제 26 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약되는,

원격 스테이션.

청구항 29

원격 스테이션으로서,

프로세서를 포함하고, 상기 프로세서는,

메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택하고,

압축된 데이터를 생성하기 위해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 상기 메시지 데이터를 압축하고 - 상기 압축된 데이터의 길이는 상기 압축 파라미터 값에 의존함 - , 그리고

암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하도록 구성되는,

원격 스테이션.

청구항 30

제 29 항에 있어서,

상기 압축 파라미터 값은 최대 체인 길이 값인,

원격 스테이션.

청구항 31

제 29 항에 있어서,

상기 결정론적 함수는 해시 함수를 포함하는,

원격 스테이션.

청구항 32

제 29 항에 있어서,

상기 프로세서는,

패딩된 메시지 데이터를 생성하기 위해 상기 결정론적 함수에 기초하여 선택된 다수의 패딩 비트들을 상기 메시지 데이터에 패딩하고, 그리고

상기 패딩된 메시지 데이터에 대해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용함으로써 상기 압축된 데이터를 생성하도록 추가로 구성되는,

원격 스테이션.

청구항 33

제 32 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱되는,

원격 스테이션.

청구항 34

제 32 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약되는,

원격 스테이션.

청구항 35

컴퓨터-판독 가능 매체를 포함하는 컴퓨터 프로그램 물건으로서,

상기 컴퓨터-판독 가능 매체는,

컴퓨터로 하여금, 메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택하게 하기 위한 코드,

컴퓨터로 하여금, 압축된 데이터를 생성하기 위해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 상기 메시지 데이터를 압축하게 하기 위한 코드 - 상기 압축된 데이터의 길이는 상기 압축 파라미터 값에 의존함 - , 및

컴퓨터로 하여금, 암호화된 메시지 데이터를 생성하기 위해 상기 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는,

컴퓨터 프로그램 물건.

청구항 36

제 35 항에 있어서,

상기 압축 파라미터 값은 최대 체인 길이 값인,

컴퓨터 프로그램 물건.

청구항 37

제 35 항에 있어서,

상기 결정론적 함수는 해시 함수를 포함하는,

컴퓨터 프로그램 물건.

청구항 38

제 35 항에 있어서,

프로세서는,

패딩된 메시지 데이터를 생성하기 위해 상기 결정론적 함수에 기초하여 선택된 다수의 패딩 비트들을 상기 메시지 데이터에 패딩하고, 그리고

상기 패딩된 메시지 데이터에 대해 상기 압축 알고리즘 및 선택된 압축 파라미터 값을 사용함으로써 상기 압축된 데이터를 생성하도록 추가로 구성되는,

컴퓨터 프로그램 물건.

청구항 39

제 38 항에 있어서,

상기 패딩 비트들은 상기 메시지 데이터에 프리픽싱되는,

컴퓨터 프로그램 물건.

청구항 40

제 38 항에 있어서,

상기 패딩 비트들은 상기 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약되는,

컴퓨터 프로그램 물건.

청구항 41

메시지 데이터를 보호하기 위한 방법으로서,

제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 상기 메시지 데이터를 압축하는 단계,

제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 상기 압축된 데이터를 패딩하는 단계 - 상기 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 상기 데이터 바이트들의 패드 수는 상기 메시지 데이터의 해시에 기초하여 결정됨 - , 및

암호화된 메시지 데이터를 생성하기 위해 상기 패딩된 압축된 데이터를 암호화하는 단계를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 42

제 41 항에 있어서,

상기 메시지 데이터의 해시는 상기 메시지 데이터의 키잉된 해시(keyed hash)인,

메시지 데이터를 보호하기 위한 방법.

청구항 43

제 42 항에 있어서,

상기 메시지 데이터의 키잉된 해시는 HMAC(Hashing for Message Authentication) 암호 해시 함수를 사용하여 수행되는,

메시지 데이터를 보호하기 위한 방법.

청구항 44

제 42 항에 있어서,

상기 키잉된 해시는 키 도출 함수를 사용하여 도출된 난독화 키(obfuscation key)를 사용하는,

메시지 데이터를 보호하기 위한 방법.

청구항 45

제 44 항에 있어서,

상기 난독화 키는 교환된 비밀 값으로부터 생성되는,

메시지 데이터를 보호하기 위한 방법.

청구항 46

제 44 항에 있어서,

상기 키 도출 함수는 상기 난독화 키를 생성하기 위해 암호화 키 및 인증 키를 사용하는,

메시지 데이터를 보호하기 위한 방법.

청구항 47

제 46 항에 있어서,

상기 암호화 키 및 상기 인증 키는 교환된 비밀 값 및 복수의 비-비밀 값들로부터 생성되는,

메시지 데이터를 보호하기 위한 방법.

청구항 48

제 41 항에 있어서,

상기 데이터 바이트들의 패드 수는 1 내지 32의 수를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 49

제 41 항에 있어서,

상기 메시지 데이터는 TLS(Transport Layer Security) 프로토콜 메시지를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 50

제 41 항에 있어서,

상기 메시지 데이터는 SSL(Secure Socket Layer) 프로토콜 메시지를 포함하는,

메시지 데이터를 보호하기 위한 방법.

청구항 51

원격 스테이션으로서,

제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 메시지 데이터를 압축하기 위한 수단,

제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 상기 압축된 데이터를 패딩하기 위한 수단 - 상기 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 상기 데이터 바이트들의 패드 수는 상기 메시지 데이터의 해시에 기초하여 결정됨 - , 및

암호화된 메시지 데이터를 생성하기 위해 상기 패딩된 압축된 데이터를 암호화하기 위한 수단을 포함하는,

원격 스테이션.

청구항 52

제 51 항에 있어서,

상기 메시지 데이터의 해시는 상기 메시지 데이터의 키잉된 해시인,

원격 스테이션.

청구항 53

제 52 항에 있어서,

상기 메시지 데이터의 키잉된 해시는 HMAC(Hashing for Message Authentication) 암호 해시 함수를 사용하여 수행되는,

원격 스테이션.

청구항 54

제 52 항에 있어서,

상기 키잉된 해시는 키 도출 함수를 사용하여 도출된 난독화 키를 사용하는,

원격 스테이션.

청구항 55

제 54 항에 있어서,

상기 난독화 키는 교환된 비밀 값으로부터 생성되는,

원격 스테이션.

청구항 56

제 54 항에 있어서,

상기 키 도출 함수는 상기 난독화 키를 생성하기 위해 암호화 키 및 인증 키를 사용하는,

원격 스테이션.

청구항 57

제 56 항에 있어서,

상기 암호화 키 및 상기 인증 키는 교환된 비밀 값 및 복수의 비-비밀 값들로부터 생성되는,

원격 스테이션.

청구항 58

제 51 항에 있어서,

상기 데이터 바이트들의 패드 수는 1 내지 32의 수를 포함하는,

원격 스테이션.

청구항 59

제 51 항에 있어서,

상기 메시지 데이터는 TLS(Transport Layer Security) 프로토콜 메시지를 포함하는,

원격 스테이션.

청구항 60

제 51 항에 있어서,

상기 메시지 데이터는 SSL(Secure Socket Layer) 프로토콜 메시지를 포함하는,

원격 스테이션.

청구항 61

원격 스테이션으로서,

프로세서를 포함하고, 상기프로세서는,

제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 메시지 데이터를 압축하고,

제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 상기 압축된 데이터를 패딩하고 - 상기 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 상기 데이터 바이트들의 패드 수는 상기 메시지 데이터의 해시에 기초하여 결정됨 - , 그리고

암호화된 메시지 데이터를 생성하기 위해 상기 패딩된 압축된 데이터를 암호화하도록 구성되는,

원격 스테이션.

청구항 62

제 61 항에 있어서,

상기 메시지 데이터의 해시는 상기 메시지 데이터의 키잉된 해시인,

원격 스테이션.

청구항 63

제 62 항에 있어서,

상기 메시지 데이터의 키잉된 해시는 HMAC(Hashing for Message Authentication) 암호 해시 함수를 사용하여 수행되는,

원격 스테이션.

청구항 64

제 62 항에 있어서,

상기 키잉된 해시는 키 도출 함수를 사용하여 도출된 난독화 키를 사용하는,

원격 스테이션.

청구항 65

제 64 항에 있어서,

상기 난독화 키는 교환된 비밀 값으로부터 생성되는,

원격 스테이션.

청구항 66

제 64 항에 있어서,

상기 키 도출 함수는 상기 난독화 키를 생성하기 위해 암호화 키 및 인증 키를 사용하는,

원격 스테이션.

청구항 67

제 66 항에 있어서,

상기 암호화 키 및 상기 인증 키는 교환된 비밀 값 및 복수의 비-비밀 값들로부터 생성되는,

원격 스테이션.

청구항 68

제 61 항에 있어서,

상기 데이터 바이트들의 패드 수는 1 내지 32의 수를 포함하는,

원격 스테이션.

청구항 69

제 61 항에 있어서,

상기 메시지 데이터는 TLS(Transport Layer Security) 프로토콜 메시지를 포함하는,

원격 스테이션.

청구항 70

제 61 항에 있어서,

상기 메시지 데이터는 SSL(Secure Socket Layer) 프로토콜 메시지를 포함하는,

원격 스테이션.

청구항 71

컴퓨터-판독 가능 매체를 포함하는 컴퓨터 프로그램 물건으로서,

상기 컴퓨터-판독 가능 매체는,

컴퓨터로 하여금, 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 메시지 데이터를 압축하게 하기 위한 코드,

컴퓨터로 하여금, 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 상기 압축된 데이터를 패딩하게 하기 위한 코드 - 상기 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 상기 데이터 바이트들의 패드 수는 상기 메시지 데이터의 해시에 기초하여 결정됨 - , 및

컴퓨터로 하여금, 암호화된 메시지 데이터를 생성하기 위해 상기 패딩된 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는,

컴퓨터 프로그램 물건.

청구항 72

제 71 항에 있어서,

상기 메시지 데이터의 해시는 상기 메시지 데이터의 키잉된 해시인,

컴퓨터 프로그램 물건.

청구항 73

제 72 항에 있어서,

상기 메시지 데이터의 키잉된 해시는 HMAC(Hashing for Message Authentication) 암호 해시 함수를 사용하여 수행되는,

컴퓨터 프로그램 물건.

청구항 74

제 72 항에 있어서,

상기 키잉된 해시는 키 도출 함수를 사용하여 도출된 난독화 키를 사용하는,

컴퓨터 프로그램 물건.

청구항 75

제 74 항에 있어서,

상기 난독화 키는 교환된 비밀 값으로부터 생성되는,

컴퓨터 프로그램 물건.

청구항 76

제 74 항에 있어서,

상기 키 도출 함수는 상기 난독화 키를 생성하기 위해 암호화 키 및 인증 키를 사용하는,

컴퓨터 프로그램 물건.

청구항 77

제 76 항에 있어서,

상기 암호화 키 및 상기 인증 키는 교환된 비밀 값 및 복수의 비-비밀 값들로부터 생성되는,

컴퓨터 프로그램 물건.

청구항 78

제 71 항에 있어서,

상기 데이터 바이트들의 패드 수는 1 내지 32의 수를 포함하는,

컴퓨터 프로그램 물건.

청구항 79

제 71 항에 있어서,

상기 메시지 데이터는 TLS(Transport Layer Security) 프로토콜 메시지를 포함하는,

컴퓨터 프로그램 물건.

청구항 80

제 71 항에 있어서,

상기 메시지 데이터는 SSL(Secure Socket Layer) 프로토콜 메시지를 포함하는,

컴퓨터 프로그램 물건.

발명의 설명

기 술 분 야

[0001] 본 출원은 2012년 9월 14일자로 출원된 미국 가출원 제 61/701,384 호의 이점을 주장하고, 상기 가출원은 인용에 의해 본원에 통합된다.

[0002] 본 발명은 일반적으로 압축 및 암호화된 메시지 데이터를 보호하는 것에 관한 것이다.

배 경 기 술

[0003] 암호화 및 압축된 메시지의 길이가 정보를 발견하는데 이용될 수 있기 때문에 압축을 사용하는 보안 접속(예를 들면, SSL/TLS)에 대한 공격이 이루어질 수 있다. 공격자가 비압축된 메시지 내의 일부 텍스트를 제어할 수 있을 때, 공격자는, 그가 가장 짧은 암호화된 메시지를 발생시키는 것을 발견할 때까지 디지트들(또는 바이트들)을 통해 사이클링할 수 있다. 예를 들면, 암호화된 메시지는 "비밀=4528715"와 같은 태그를 포함할 수 있다. 공격자가 삽입한 비압축된 메시지가 "비밀=4"일 때, "비밀=0"과 같은 다른 가능한 디지트들에 대한 것보다 압축이 더 양호해질 것이고, 따라서 암호화된 메시지의 길이가 더 짧아질 것이다. 제 1 디지트를 발견한 후에, 공격자는, 그가 더 짧은 길이, 예를 들면, "비밀=45"를 발생시키는 것을 발견할 때까지 다음의 가능한 디지트들(또는 바이트들)을 통해 사이클링할 수 있다. 이어서, 공격자는, 민감한 정보 모두가 발견될 때까지, 다음의 디지트(또는 바이트)를 통해 사이클링할 수 있다.

[0004] 따라서, 압축된 메시지의 길이가 압축 및 암호화된 데이터 스트림으로부터 결정될 수 없도록 압축뿐만 아니라 암호화되는 메시지를 보호하기 위한 기술에 대한 필요성이 존재한다.

발명의 내용

[0005] 본 발명의 일 양상은 메시지 데이터를 보호하기 위한 방법에 존재할 수 있다. 상기 방법에서, 메시지 데이터에는 메시지 데이터 상에서 수행되는 결정론적 함수(deterministic function)에 기초하여 생성된 패딩 비트들이 패딩된다. 패딩된 메시지 데이터는 압축된 데이터를 생성하도록 압축된다. 압축된 데이터의 길이는 패딩 비트들에 의존한다. 압축된 데이터는 암호화된 메시지 데이터를 생성하도록 암호화된다.

[0006] 본 발명의 더 상세한 양상들에서, 결정론적 함수는 해시(hash) 함수를 포함할 수 있다. 패딩 비트들은 메시지 데이터에 프리픽싱(prefixed) 또는 프리펜딩(prepended)될 수 있다. 패딩 비트들은 패딩 비트들의 끝(end)이

수신기에 의해 결정되게 허용하도록 제약될 수 있다.

[0007] 본 발명의 다른 양상은, 메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들을 메시지 데이터에 패딩하기 위한 수단, 압축된 데이터를 생성하기 위해, 패딩된 메시지 데이터를 압축하기 위한 수단 - 압축된 데이터의 길이는 패딩 비트들에 의존함 - , 및 암호화된 메시지 데이터를 생성하기 위해 압축된 데이터를 암호화하기 위한 수단을 포함하는 원격 스테이션에 존재할 수 있다.

[0008] 본 발명의 다른 양상은, 메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들을 메시지 데이터에 패딩하고, 압축된 데이터를 생성하기 위해, 패딩된 메시지 데이터를 압축하고 - 압축된 데이터의 길이는 패딩 비트들에 의존함 - , 그리고 암호화된 메시지 데이터를 생성하기 위해 압축된 데이터를 암호화하도록 구성된 프로세서를 포함하는 원격 스테이션에 존재할 수 있다.

[0009] 본 발명의 다른 양상은, 컴퓨터로 하여금, 메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들을 메시지 데이터에 패딩하게 하기 위한 코드, 컴퓨터로 하여금, 압축된 데이터를 생성하기 위해, 패딩된 메시지 데이터를 압축하게 하기 위한 코드 - 압축된 데이터의 길이는 패딩 비트들에 의존함 - , 및 컴퓨터로 하여금, 암호화된 메시지 데이터를 생성하기 위해 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는 컴퓨터-판독 가능 매체를 포함하는 컴퓨터 프로그램 물건에 존재할 수 있다.

[0010] 본 발명의 다른 양상은, 메시지 데이터를 보호하기 위한 방법에 존재할 수 있다. 상기 방법에서, 압축 알고리즘의 압축 파라미터 값은 메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 선택된다. 메시지 데이터는 압축된 데이터를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 압축된다. 압축된 데이터의 길이는 압축 파라미터 값에 의존한다. 압축된 데이터는 암호화된 메시지 데이터를 생성하기 위해 암호화된다.

[0011] 본 발명의 더 상세한 양상들에서, 압축 파라미터 값은 최대 체인 길이 값일 수 있다. 결정론적 함수는 해시 함수를 포함할 수 있다. 메시지 데이터를 압축하는 것은 패딩된 메시지 데이터를 생성하기 위해 결정론적 함수에 기초하여 선택된 다수의 패딩 비트들을 메시지 데이터에 패딩하는 것, 및 패딩된 메시지 데이터에 대해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용함으로써 압축된 데이터를 생성하는 것을 포함할 수 있다. 패딩 비트들은 메시지 데이터에 프리픽싱될 수 있다. 패딩 비트들은 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약될 수 있다.

[0012] 본 발명의 다른 양상은, 메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택하기 위한 수단, 압축된 데이터를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 메시지 데이터를 압축하기 위한 수단 - 압축된 데이터의 길이는 압축 파라미터 값에 의존함 - , 및 암호화된 메시지 데이터를 생성하기 위해 압축된 데이터를 암호화하기 위한 수단을 포함하는 원격 스테이션에 존재할 수 있다.

[0013] 본 발명의 다른 양상은, 메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택하고, 압축된 데이터를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 메시지 데이터를 압축하고 - 압축된 데이터의 길이는 압축 파라미터 값에 의존함 - , 그리고 암호화된 메시지 데이터를 생성하기 위해 압축된 데이터를 암호화하도록 구성되는 프로세서를 포함하는 원격 스테이션에 존재할 수 있다.

[0014] 본 발명의 다른 양상은, 컴퓨터로 하여금, 메시지 데이터 상에서 수행되는 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택하게 하기 위한 코드, 컴퓨터로 하여금, 압축된 데이터를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 메시지 데이터를 압축하게 하기 위한 코드 - 압축된 데이터의 길이는 압축 파라미터 값에 의존함 - , 및 컴퓨터로 하여금, 암호화된 메시지 데이터를 생성하기 위해 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는 컴퓨터-판독 가능 매체를 포함하는 컴퓨터 프로그램 물건에 존재할 수 있다.

[0015] 본 발명의 다른 양상은, 메시지 데이터를 보호하기 위한 방법에 존재할 수 있다. 상기 방법에서, 메시지 데이터는 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 압축된다. 압축된 데이터는 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 패딩되고, 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정된다. 패딩된 압축된 데이터는 암호화된 메시지 데이터를 생성하기 위해 암호화된다.

[0016] 본 발명의 더 상세한 양상들에서, 메시지 데이터의 해시는 메시지 데이터의 키잉된 해시(keyed hash)일 수

있다. 메시지 데이터의 키잉된 해시는 HMAC(Hashing for Message Authentication) 암호 해시 함수를 사용하여 수행될 수 있고, 키 도출 함수를 사용하여 도출된 난독화 키(obfuscation key)를 사용할 수 있다. 난독화 키는 교환된 비밀 값으로부터 생성될 수 있다. 키 도출 함수는 난독화 키를 생성하기 위해 암호화 키 및 인증 키를 사용할 수 있다. 암호화 키 및 인증 키는 교환된 비밀 값 및 복수의 비-비밀 값들로부터 생성될 수 있다. 데이터 바이트들의 패드 수는 1로부터 32까지의 수를 포함할 수 있다.

[0017] 본 발명의 다른 더 상세한 양상들에서, 패딩된 압축된 데이터를 생성하기 위해 압축된 데이터를 패딩하는 것은 메시지 데이터의 결정론적 함수에 기초하여 수정된 압축 알고리즘을 사용하는 것을 포함할 수 있다. 메시지 데이터는 TLS(Transport Layer Security) 프로토콜 메시지 또는 SSL(Secure Socket Layer) 프로토콜 메시지를 포함할 수 있다.

[0018] 본 발명의 다른 양상은, 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 메시지 데이터를 압축하기 위한 수단, 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 압축된 데이터를 패딩하기 위한 수단을 포함하는 원격 스테이션에 존재할 수 있고, 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정된다.

[0019] 본 발명의 다른 양상은 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 메시지 데이터를 압축하고, 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 압축된 데이터를 패딩하도록 구성된 프로세서를 포함하는 원격 스테이션에 존재할 수 있고, 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정된다.

[0020] 본 발명의 다른 양상은, 컴퓨터로 하여금, 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터를 생성하기 위해 메시지 데이터를 압축하게 하기 위한 코드, 컴퓨터로 하여금, 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터를 생성하기 위해 압축된 데이터를 패딩하게 하기 위한 코드를 포함하는 컴퓨터-판독 가능 매체를 포함하는 컴퓨터 프로그램 물건에 존재할 수 있고, 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정된다.

도면의 간단한 설명

[0021] 도 1은 무선 통신 시스템의 예의 블록도이다.

도 2는 본 발명에 따라 메시지 데이터를 보호하기 위한 방법의 흐름도이다.

도 3은 메시지 데이터를 보호하기 위한 방법에서의 데이터의 흐름도이다.

도 4는 프로세서 및 메모리를 포함하는 컴퓨터의 블록도이다.

도 5는 본 발명에 따라 메시지 데이터를 보호하기 위한 다른 방법의 흐름도이다.

도 6은 메시지 데이터를 보호하기 위한 다른 방법에서의 데이터의 흐름도이다.

도 7은 본 발명에 따라 메시지 데이터를 보호하기 위한 다른 방법의 흐름도이다.

도 8은 메시지 데이터를 보호하기 위한 다른 방법에서의 데이터의 흐름도이다.

도 9는 메시지 데이터를 보호하기 위한 다른 방법에서의 데이터의 흐름도이다.

도 10은 메시지 데이터를 보호하기 위한 다른 방법에서 데이터의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 단어 "예시적인"은 "예, 예시, 또는 예증으로서 기능하는"을 의미하도록 본원에 이용된다. "예시적인"으로서 본원에 설명된 어떠한 실시예도 반드시 다른 실시예들에 비해 선호되거나 또는 유리한 것으로서 해석되는 것은 아니다.

[0023] 도 2 및 도 3을 참조하면, 본 발명의 일 양상은 메시지 데이터(310)를 보호하기 위한 방법(200)에 존재할 수 있다. 상기 방법에서, 메시지 데이터에는 메시지 데이터 상에서 수행되는 결정론적 함수(330)에 기초하여 생성된 패딩(padding) 비트들(320)이 패딩된다(단계 210). 패딩된 메시지 데이터(335)는 압축된 데이터(340)를 생성하도록 압축된다(단계 220). 압축된 데이터의 길이는 패딩 비트들에 의존한다. 압축된 데이터는 암호화된 메시지 데이터(350)를 생성하도록 암호화된다(단계 230). 암호화 함수(380)는 압축된 데이터를 암호화하기 위해 암

호화 키를 사용한다. 상기 방법은, 압축된 메시지의 길이가 압축 및 암호화된 데이터 스트림으로부터 결정될 수 없도록, 압축뿐만 아니라 암호화되는 메시지를 보호한다.

[0024] 본 발명의 더 상세한 양상들에서, 결정론적 함수(330)는 해시 함수를 포함할 수 있다. 패딩 생성기(360)는 패딩된 메시지의 길이를 결정하기 위해 해시 함수로부터 몇몇의 비트들을 취한다. 해시 함수로부터의 비트들은 랜덤형(radnom-like)이다. 결과적으로, 압축된 데이터(350)는 랜덤형 길이를 갖는다. 또한, 해시 함수로부터의 비트들은, 해시 함수로부터의 이러한 비트들의 랜덤형 속성으로 인해 거의 없어지게 압축되지는 않을 것이다. 패딩 비트들(320)은 메시지 데이터(310)에 프리픽싱(prefixed) 또는 프리펜딩(prepended)될 수 있다.

[0025] 패딩 비트들(320)은 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약될 수 있다. 예를 들면, 마지막을 제외한 모든 패딩 바이트들의 최상위 비트는 0으로 강제될 수 있고, 마지막 바이트의 최상위 비트는 1로 강제될 수 있다. 메시지 수신기는 이러한 패턴에 의해 패딩의 끝을 결정할 수 있을 것이다. 다른 예로서, 첫 번째 5 개의 비트들에 패딩의 길이가 부여될 수 있다. (최대 길이가 32 바이트들이라고 가정함.) 비트들 중 나머지는 해시 함수(330)에서 비롯될 수 있다. 압축 함수(370) 및 압축 파라미터 값(390)은 도 6에 관련하여 아래에 설명된다.

[0026] 추가로 도 4를 참조하면, 본 발명의 다른 양상은 메시지 데이터 상에서 수행되는 결정론적 함수(330)에 기초하여 생성된 패딩 비트들(320)을 메시지 데이터(310)에 패딩하기 위한 수단(410), 압축된 데이터(340)를 생성하기 위해 패딩된 메시지 데이터(335)를 압축하기 위한 수단(410) – 압축된 데이터의 길이는 패딩 비트들에 의존함 – , 및 암호화된 메시지 데이터(350)를 생성하기 위해 압축된 데이터를 암호화하기 위한 수단(410)을 포함하는 원격 스테이션(102)에 존재할 수 있다.

[0027] 본 발명의 다른 양상은, 메시지 데이터 상에서 수행되는 결정론적 함수(330)에 기초하여 생성된 패딩 비트들(320)을 메시지 데이터(310)에 패딩하고, 압축된 데이터(340)를 생성하기 위해 패딩된 메시지 데이터(335)를 압축하고 – 압축된 데이터의 길이는 패딩 비트들에 의존함 – , 그리고 암호화된 메시지 데이터(350)를 생성하기 위해 압축된 데이터를 암호화하도록 구성된 프로세서(410)를 포함하는 원격 스테이션(102)에 존재한다.

[0028] 본 발명의 다른 양상은, 컴퓨터(400)로 하여금, 메시지 데이터 상에서 수행되는 결정론적 함수에 기초하여 생성된 패딩 비트들(320)을 메시지 데이터(310)에 패딩하게 하기 위한 코드, 컴퓨터로 하여금, 압축된 데이터(340)를 생성하기 위해 패딩된 메시지 데이터(335)를 압축하게 하기 위한 코드 – 압축된 데이터의 길이는 패딩 비트들에 의존함 – , 및 컴퓨터(400)로 하여금, 암호화된 메시지 데이터(350)를 생성하기 위해 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는 컴퓨터-판독 가능 매체(420)를 포함하는 컴퓨터 프로그램 물건에 존재할 수 있다.

[0029] 도 5 및 도 6을 참조하면, 본 발명의 다른 양상은 메시지 데이터(610)를 보호하기 위한 방법(500)에 존재할 수 있다. 상기 방법에서, 압축 함수(670)의 압축 알고리즘의 압축 파라미터 값(690)은 메시지 데이터 상에서 수행되는 결정론적 함수(630)를 사용하여 선택된다(단계 510). 메시지 데이터는 압축된 데이터(640)를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 압축된다(단계 520). 압축된 데이터의 길이는 압축 파라미터 값에 의존한다. 압축된 데이터는 암호화된 메시지 데이터(650)를 생성하도록 암호화된다(단계 530). 암호화 함수(680)는 압축된 데이터를 암호화하기 위해 암호화 키 및 암호화 알고리즘을 사용한다.

[0030] 본 발명의 더 상세한 양상들에서, 압축 파라미터 값은 최대 체인 길이 값일 수 있다. 결정론적 함수는 해시 함수(630)를 포함할 수 있다. 압축 함수(670)는 압축 동안에 많은 선택들을 할 수 있다. 웹 상의 데이터의 압축에서 일반적으로 사용되는 DEFLATE 함수는, 0으로부터 9까지의 범위에서 압축이 얼마나 공격적(aggressive)이어야 하는지를 나타내는 파라미터를 갖는다. 몇몇의 비트들은 해시 함수로부터 취해지고, 해당 범위로 감소되고, 압축 함수에 대한 요청의 일부가 될 수 있다. 이것은, 임의의 것이 메시지 데이터에서 변경된 경우에 압축 함수가 상이하게 작동하게 할 것이다.

[0031] DEFLATE 함수에서, 몇몇의 값들은 내부 튜닝 파라미터들, 즉, good_length, max_lazy, nice_length 및 max_chain으로서 사용될 수 있다. 예를 들면, max_chain 값은 그 값이 찾을 가장 긴 체인 등을 제어한다. DEFLATE 함수는, 표로부터 선택되는 0 내지 9의 단일 정수로서 대신에 이러한 튜닝 파라미터들을 개별적으로 수용하도록 수정될 수 있다. 튜닝 파라미터들은 해시 함수(630)의 출력으로부터의 비트들 중 일부를 사용하여 선택될 수 있다.

[0032] 메시지 데이터(610)를 압축하는 것은 패딩된 메시지 데이터를 생성하기 위해 결정론적 함수에 기초하여 선택된

다수의 패딩 비트들을 메시지 데이터에 패딩하는 것, 및 패딩된 메시지 데이터 상에서 압축 알고리즘 및 선택된 압축 파라미터 값을 사용함으로써 압축된 데이터(640)를 생성하는 것을 포함할 수 있다. 패딩 비트들은 메시지 데이터에 프리픽싱될 수 있다. 패딩 비트들은 패딩 비트들의 끝이 수신기에 의해 결정되게 허용하도록 제약될 수 있다. 패딩 및/또는 압축 효과를 랜덤화하는 것은 그러한 길이-누설 타입 공격들로부터 보호될 수 있다.

[0033] 본 발명의 다른 양상은, 메시지 데이터(610) 상에서 수행되는 결정론적 함수(630)를 사용하여 압축 알고리즘의 압축 파라미터 값(690)을 선택하기 위한 수단(410), 압축된 데이터(640)를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 메시지 데이터를 압축하기 위한 수단(410) - 압축된 데이터의 길이는 압축 파라미터 값에 의존함 - , 및 암호화된 메시지 데이터(650)를 생성하기 위해 압축된 데이터를 암호화하기 위한 수단을 포함하는 원격 스테이션(102)에 존재할 수 있다.

[0034] 본 발명의 다른 양상은, 메시지 데이터(610) 상에서 수행되는 결정론적 함수(630)를 사용하여 압축 알고리즘의 압축 파라미터 값(690)을 선택하고, 압축된 데이터(640)를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 메시지 데이터를 압축하고 - 압축된 데이터의 길이는 압축 파라미터 값에 의존함 - , 그리고 암호화된 메시지 데이터(650)를 생성하기 위해 압축된 데이터를 암호화하도록 구성된 프로세서(410)를 포함하는 원격 스테이션(102)에 존재할 수 있다.

[0035] 본 발명의 다른 양상은, 컴퓨터(400)로 하여금, 메시지 데이터(610) 상에서 수행되는 결정론적 함수(630)를 사용하여 압축 알고리즘의 압축 파라미터 값(690)을 선택하게 하기 위한 코드, 컴퓨터로 하여금, 압축된 데이터(640)를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 메시지 데이터를 압축하게 하기 위한 코드 - 압축된 데이터의 길이는 압축 파라미터 값에 의존함 - , 및 컴퓨터로 하여금, 암호화된 메시지 데이터(650)를 생성하기 위해 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는 컴퓨터-판독 가능 매체(420)를 포함하는 컴퓨터 프로그램 물건에 존재할 수 있다.

[0036] 도 7 내지 도 10을 참조하면, 본 발명의 다른 양상은 메시지 데이터(810)를 보호하기 위한 방법(700)에 존재할 수 있다. 상기 방법에서, 메시지 데이터는 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터(840)를 생성하도록 압축된다(단계 710). 압축된 데이터는 제 2 수의 데이터 바이트들(837)을 포함하는 패딩된 압축된 데이터(835)를 생성하도록 패딩되고 - 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일함 - , 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정된다(단계 720). 패딩된 압축된 데이터는 암호화된 메시지 데이터(850)를 생성하도록 암호화된다(단계 730).

[0037] 본 발명의 더 상세한 양상들에서, 메시지 데이터(810)의 해시(830)는 메시지 데이터의 키잉된(keyed) 해시(935)일 수 있다. 메시지 데이터의 키잉된 해시는 HMAC(Hashing for Message Authentication) 암호 해시 함수를 사용하여 수행될 수 있고, 키 도출 함수를 사용하여 도출된 난독화(obfuscation) 키를 사용할 수 있다. 난독화 키는 교환된 비밀 값으로부터 생성될 수 있다. 키 도출 함수는 난독화 키를 생성하기 위해 암호화 키 및 인증 키를 사용할 수 있다. 암호화 키 및 인증 키는 교환된 비밀 값 및 복수의 비-비밀 값들로부터 생성될 수 있다. 데이터 바이트들의 패드 수는 1로부터 32까지의 수를 포함할 수 있다.

[0038] 비압축된 텍스트(810)의 해시 또는 유사한 함수가 계산될 수 있다. 해시 값으로부터, 일부 패딩(837)의 길이가 일부 산술 또는 논리 연산에 의해 결정될 수 있다. 예를 들면, 연산은 해시의 마지막 유효(last significant) 5 비트들만을 사용할 수 있다. 이것은 0 내지 31의 수일 것이고, 이것은 부가될 수 있는 패딩(837)의 바이트들의 수일 것이다. 길이가 각각의 시험 디지트(trial digit)에 대해 다수의 바이트들만큼 변동될 것이고, 정확히 그 길이가 가장 짧은 것일 가능성이 없기 때문에, 이러한 기술은 이러한 타입의 공격을 좌절시킬 것이다. 해시 함수는 난독화 키(obfuscation key)와 같은 비밀을 포함할 수 있다. HMAC는 비밀을 포함하는 해시형 함수이다(때때로 HMAC는 키잉된 해시로 불린다).

[0039] 비밀은 세션 설정의 부분으로서 도출될 수 있다. 세션 설정 동안에 암호화 키 및 인증 키를 도출하는 것은 일반적인데, 이러한 키들은 길이-난독화 키를 도출하는데 사용될 수 있다. 길이-난독화 키는 패딩의 길이의 계산의 부분일 것이다. 공격자가 길이-난독화 키를 알지 못하기 때문에, 공격자는 패딩의 길이를 계산할 수 없다.

[0040] 일 양상은 압축 함수의 연산을 수정하는 것을 수반할 수 있다. 압축 함수들은 일반적으로 많은 결정들을 내릴 수 있다. 예를 들면, 압축 함수는 최근에 접한(encountered) 스트링들의 "사전들(dictionaries)"을 종종 구축한다. 그러나, 저장이 제한되기 때문에, 사전 내의 하나 이상의 엔트리들은 빈번한 간격들로 폐기되어야 한다.

최근에 가장 덜 본 스트링은 종종 폐기를 위해 선택된다. 그러나, 선택은 메시지의 해시에 의존하여 이루어질 수 있다. 실제 압축 알고리즘에서, 이루어질 수 있는 많은 다른 선택들이 존재할 수 있다. 메시지의 해시(또는 키잉된 해시)에 의존하여 이들 선택 중 일부 또는 전부를 행하는 것은 많은 "잡음"을 길이에 도입시킬 수 있다.

[0041] 실제 보안 통신 시스템들에서, 일반적으로 프리-마스터 비밀(pre-master secret)이라 불리는 비밀 값을 교환하고, 이어서 비밀 값과 몇몇의 비-비밀 값들을 결합하기 위해 키 도출 함수를 사용하여, 암호화 키 및 인증 키를 생성하는 프로토콜이 존재한다. 패딩 난독화 키와 같은 제 3 키는 암호화 키 및 인증 키로부터 도출될 수 있다.

[0042] 본 발명의 다른 더 상세한 양상들에서, 패딩된 압축된 데이터를 생성하기 위해 압축된 데이터(840)를 패딩하는 것은 메시지 데이터(810)의 결정론적 함수에 기초하여 수정된 압축 알고리즘(845)을 사용하는 것을 포함할 수 있다. 메시지 데이터는 TLS(Transport Layer Security) 프로토콜 메시지, 또는 SSL(Secure Socket Layer) 프로토콜 메시지를 포함할 수 있다. 해시 함수(830), 패딩 생성기(860) 및 암호화 함수(880)는 도 3에 관련하여 앞서 설명되었다. 패딩 수는 난수 생성기(1035)로부터의 난수에 기초하여 결정될 수 있다.

[0043] 본 발명의 다른 양상은 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터(840)를 생성하기 위해 메시지 데이터(810)를 압축하기 위한 수단(410), 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터(835)를 생성하기 위해 압축된 데이터를 패딩하기 위한 수단(410) - 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정됨 - , 및 암호화된 메시지 데이터(850)를 생성하기 위해 패딩된 압축된 데이터를 암호화하기 위한 수단(410)을 포함하는 원격 스테이션(102)에 존재할 수 있다.

[0044] 본 발명의 다른 양상은 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터(840)를 생성하기 위해 메시지 데이터(810)를 압축하고, 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터(835)를 생성하기 위해 압축된 데이터를 패딩하고 - 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정됨 - , 그리고 암호화된 메시지 데이터(850)를 생성하기 위해 패딩된 압축된 데이터를 암호화하도록 구성된 프로세서(410)를 포함하는 원격 스테이션(102)에 존재할 수 있다.

[0045] 본 발명의 다른 양상은, 컴퓨터(400)로 하여금, 제 1 수의 데이터 바이트들을 포함하는 압축된 데이터(840)를 생성하기 위해 메시지 데이터(810)를 압축하게 하기 위한 코드, 컴퓨터로 하여금, 제 2 수의 데이터 바이트들을 포함하는 패딩된 압축된 데이터(835)를 생성하기 위해 압축된 데이터를 패딩하게 하기 위한 코드 - 제 2 수는 데이터 바이트들의 "제 1 수" + "패드 수"와 동일하고, 데이터 바이트들의 패드 수는 메시지 데이터의 해시에 기초하여 결정됨 - , 및 컴퓨터로 하여금, 암호화된 메시지 데이터(850)를 생성하기 위해 패딩된 압축된 데이터를 암호화하게 하기 위한 코드를 포함하는 컴퓨터-판독 가능 매체(420)를 포함하는 컴퓨터 프로그램 물건에 존재할 수 있다.

[0046] 원격 스테이션(102)은 프로세서(410), 메모리 및/또는 디스크 드라이브와 같은 저장 매체(420)를 포함하는 컴퓨터(400), 디스플레이(430) 및 키패드(440)와 같은 입력 및 무선 접속부(450)를 포함할 수 있다.

[0047] 도 1을 참조하면, 무선 원격 스테이션(RS)(102)(예를 들어, 모바일 스테이션(MS))은, 무선 통신 시스템(100)의 하나 이상의 기지국들(BS)(104)과 통신할 수 있다. 무선 통신 시스템(100)은 하나 이상의 기지국 컨트롤러들(BSC)(106), 및 코어 네트워크(108)를 더 포함할 수 있다. 코어 네트워크는 적합한 백홀들을 통해서 인터넷(110) 및 PSTN(Public Switched Telephone Network)(112)에 접속될 수 있다. 통상적인 무선 모바일 스테이션은, 핸드헬드 전화기, 또는 랩탑 컴퓨터를 포함할 수 있다. 무선 통신 시스템(100)은, CDMA(code division multiple access), TDMA(time division multiple access), FDMA(frequency division multiple access), SDMA(space division multiple access), PDMA(polarization division multiple access), 또는 당업계에 알려진 다른 변조 기법들과 같은 다수의 다중 액세스 기법들 중 어느 하나를 사용할 수 있다.

[0048] 당업자들은 정보 및 신호들이 다양한 상이한 기술들 및 기법들 중 임의의 것을 이용하여 표현될 수 있다는 것을 이해할 것이다. 예를 들어, 전술한 설명 전반에 걸쳐 참조될 수 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 자기 입자들, 광 필드들 또는 광 입자들, 또는 이들의 임의의 결합에 의해 표현될 수 있다.

[0049] 또한, 당업자들은 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및

알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어 또는 이 둘의 조합들로서 구현될 수 있다는 것을 이해할 것이다. 하드웨어와 소프트웨어의 이러한 상호 교환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 좌우된다. 당업자들은 설명된 기능을 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 구현할 수 있으나, 이러한 구현 결정들은 본 발명의 범위를 벗어나게 하는 것으로 해석되어서는 안된다.

[0050] 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 및 회로들은 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적 회로(ASIC), 필드 프로그래머블 게이트 어레이(FPGA) 또는 다른 프로그래머블 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들 또는 본원에서 설명된 기능들을 수행하도록 설계된 이들의 임의의 조합으로 구현되거나 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로 이 프로세서는 임의의 종래의 프로세서, 컨트롤러, 마이크로컨트롤러 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들어, DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 연결된 하나 이상의 마이크로프로세서들 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

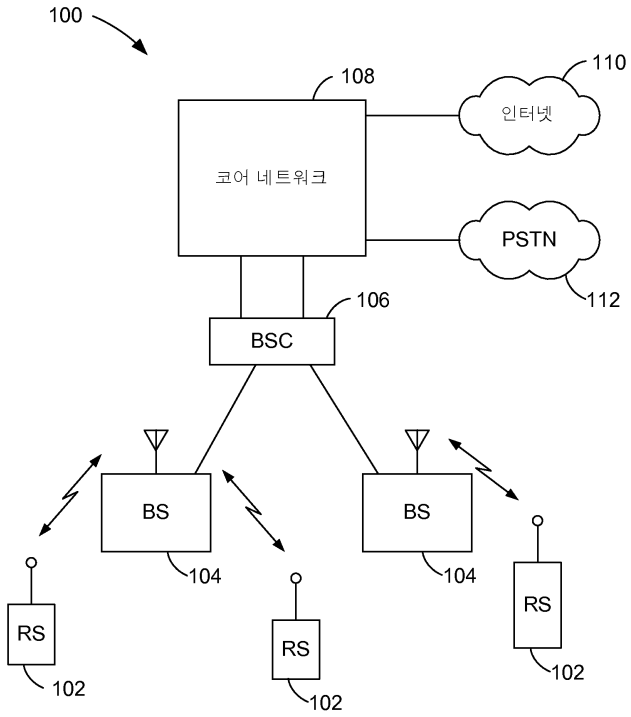
[0051] 본원에 개시된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 직접 하드웨어로 구현되거나, 프로세서에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이 둘의 조합으로 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 탈착식 디스크, CD-ROM, 또는 당업계에 공지된 임의의 다른 형태의 저장 매체에 존재할 수 있다. 예시적인 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있도록, 프로세서에 연결된다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다. 프로세서 및 저장 매체는 ASIC에 상주할 수 있다. ASIC는 사용자 단말에 상주할 수 있다. 대안적으로, 프로세서 및 저장 매체는 사용자 단말 내에서 이산 컴포넌트들로서 상주할 수 있다.

[0052] 하나 이상의 예시적인 실시예들에서, 설명된 기능들은 하드웨어로, 소프트웨어로, 펌웨어로, 또는 이들의 임의의 조합으로 구현될 수 있다. 컴퓨터 프로그램 물건으로서 소프트웨어로 구현되는 경우, 상기 기능들은 컴퓨터-판독가능 매체 상에 하나 이상의 명령들 또는 코드로서 저장되거나 또는 이들을 통해 송신될 수 있다. 컴퓨터-판독가능 매체들은 비-일시적 컴퓨터 저장 매체들 및 하나의 장소에서 다른 장소로의 컴퓨터 프로그램의 전송을 가능하게 하는 임의의 매체를 포함하는 통신 매체들 모두를 포함한다. 저장 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있다. 한정이 아닌 예로서, 이러한 컴퓨터-판독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장부, 자기 디스크 저장부 또는 다른 자기 저장 디바이스들, 또는 컴퓨터에 의해 액세스될 수 있고 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 운반 또는 저장하는데 이용될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속수단(connection)이 컴퓨터-판독가능 매체로 적절하게 명명된다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 트위스트 페어, 디지털 가입자 라인(DSL), 또는 적외선, 라디오 및 마이크로파와 같은 무선 기술들을 이용하여 웹사이트, 서버 또는 다른 원격 소스로부터 송신되면, 동축 케이블, 광섬유 케이블, 트위스트 페어, DSL, 또는 적외선, 라디오 및 마이크로파와 같은 무선 기술들이 매체의 정의 내에 포함된다. 본원에 이용되는 것과 같은, 디스크(disk) 및 디스크(disc)는 콤팩트 디스크(CD; compact disc), 레이저 디스크(laser disc), 광학 디스크(optical disc), 디지털 다기능 디스크(DVD: digital versatile disc), 플로피 디스크(floppy disk) 및 블루-레이 디스크(blu-ray disc)를 포함하며, 여기서 디스크(disk)들은 통상적으로 자기적으로 데이터를 재생하는 반면에 디스크(disc)들은 레이저들을 통해 광학적으로 데이터를 재생한다. 전술한 것들의 조합들이 또한 컴퓨터-판독가능 매체의 범위 내에 포함되어야 할 것이다.

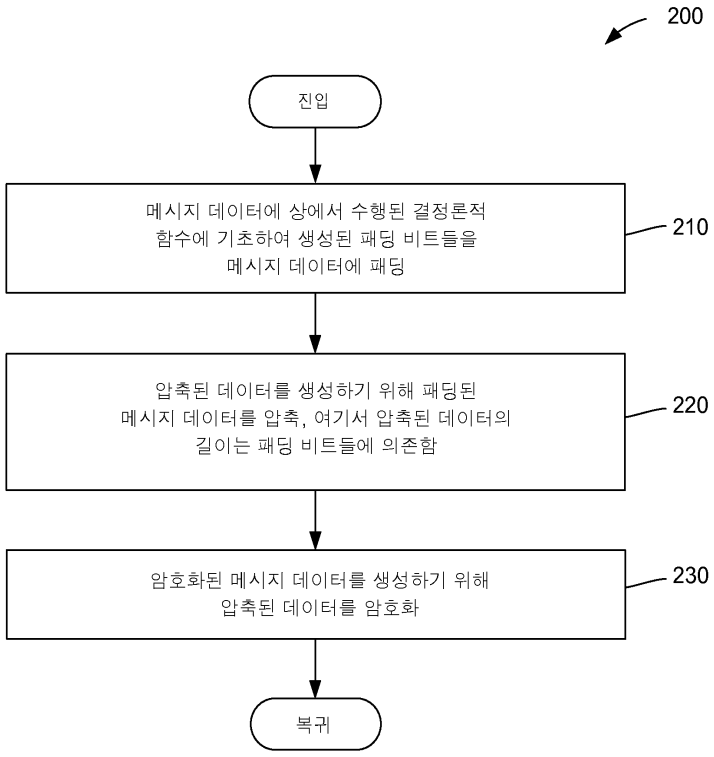
[0053] 개시된 실시예들의 이전 설명은 임의의 당업자가 본 발명을 실시하거나 이용하는 것을 가능하게 하기 위해 제공된다. 이러한 실시예들에 대한 다양한 변형들은 당업자들에게 쉽게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 발명의 사상 또는 범위에서 벗어나지 않고 다른 실시예들에 적용될 수 있다. 따라서, 본 발명은 본원에 도시된 실시예들로 제한되는 것으로 의도되는 것이 아니라, 본원에 개시된 원리들 및 신규의 특징들에 일치하는 최광의의 범위가 부여되어야 한다.

도면

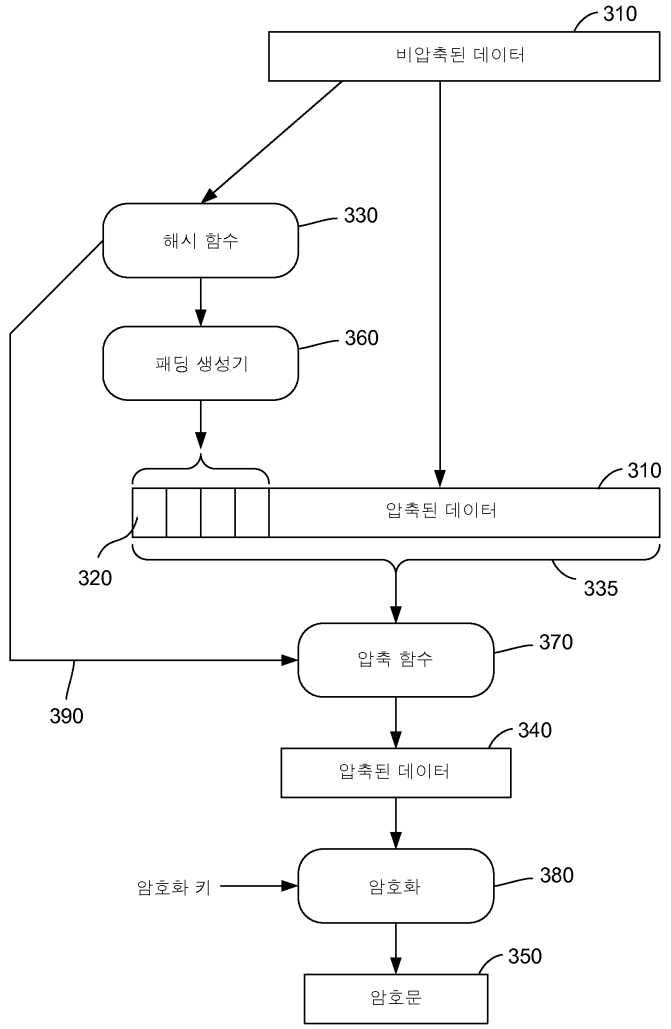
도면1


100
108
110
인터넷
코어 네트워크
PSTN
112
106
BSC
BS
BS
104
104
RS
RS
RS
102
102
102

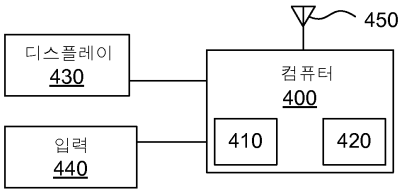
도면2


200
진입
메시지 데이터에 상에서 수행된 결정론적
함수에 기초하여 생성된 패딩 비트들을
메시지 데이터에 패딩
210
압축된 데이터를 생성하기 위해 패딩된
메시지 데이터를 압축, 여기서 압축된 데이터의
길이는 패딩 비트들에 의존함
220
암호화된 메시지 데이터를 생성하기 위해
압축된 데이터를 암호화
230
복귀

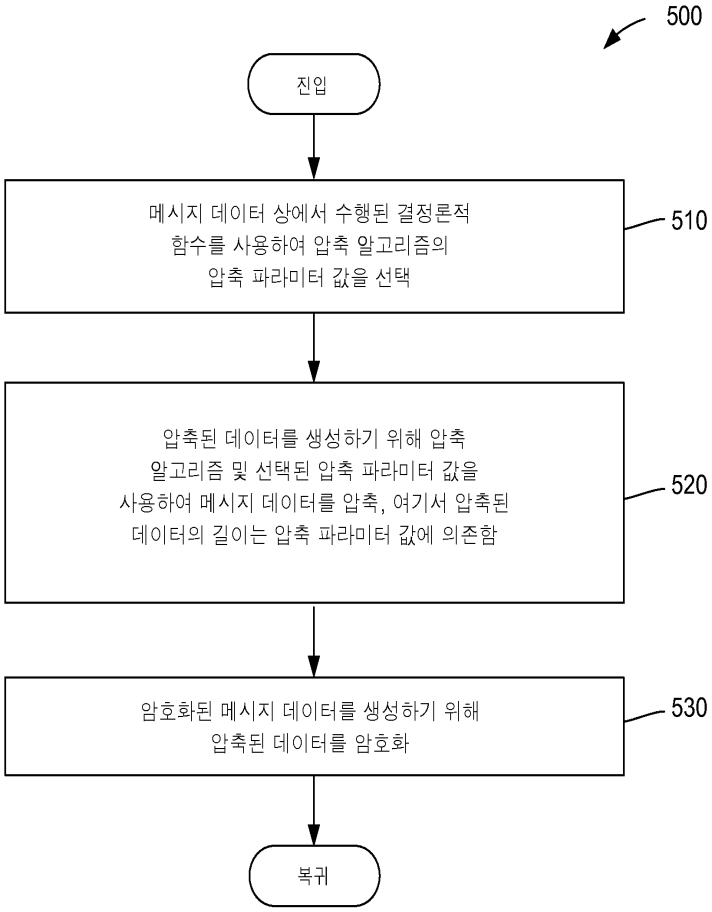
도면3


310
비압축된 데이터
330
해시 함수
360
패딩 생성기
310
압축된 데이터
320
335
370
압축 함수
390
340
압축된 데이터
암호화 키
380
암호화
350
암호문

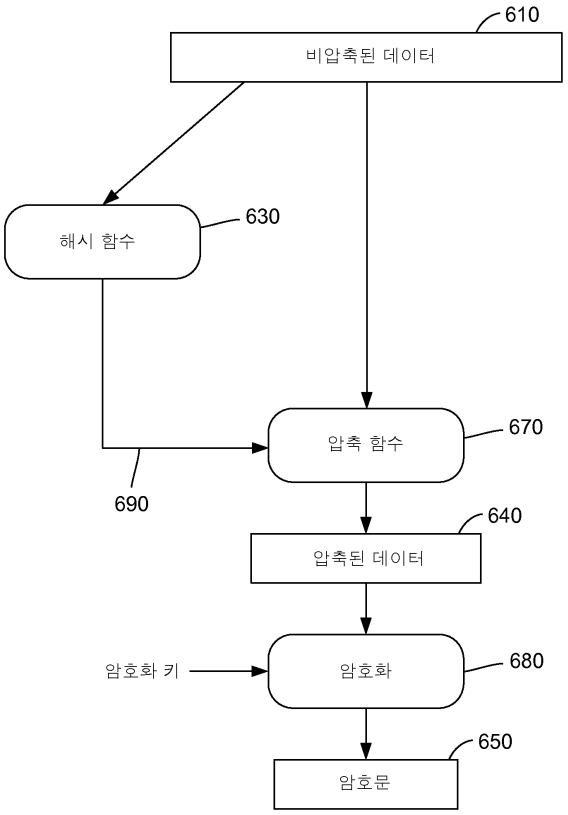
도면4


450
디스플레이
430
컴퓨터
400
410
420
입력
440

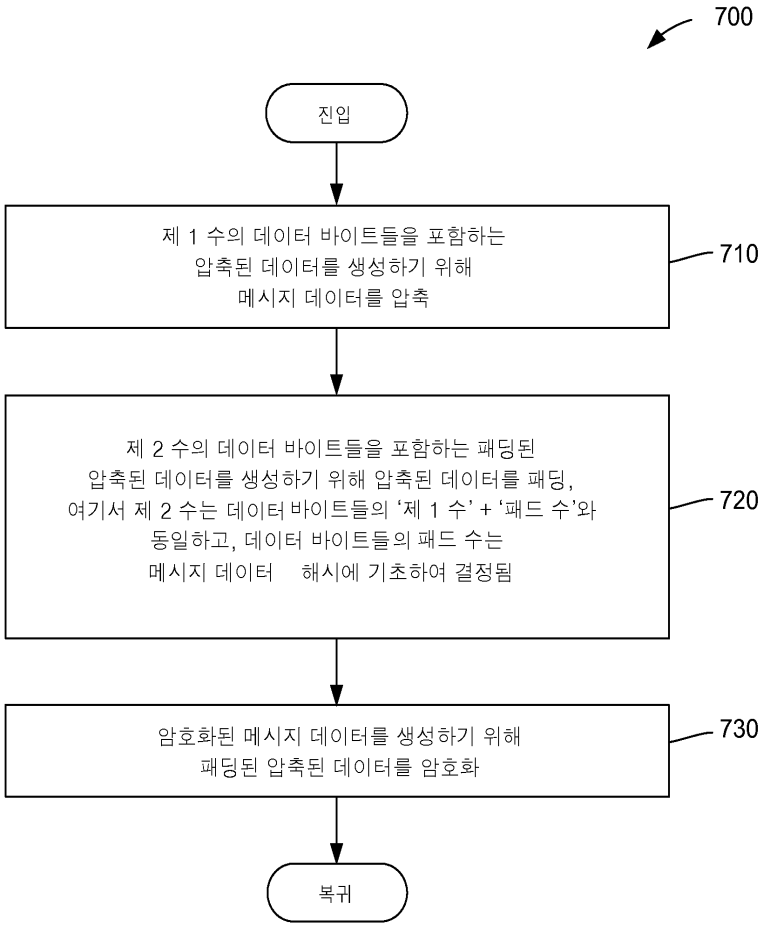
도면5


500
진입
메시지 데이터 상에서 수행된 결정론적 함수를 사용하여 압축 알고리즘의 압축 파라미터 값을 선택
510
압축된 데이터를 생성하기 위해 압축 알고리즘 및 선택된 압축 파라미터 값을 사용하여 메시지 데이터를 압축, 여기서 압축된 데이터의 길이는 압축 파라미터 값에 의존함
520
암호화된 메시지 데이터를 생성하기 위해 압축된 데이터를 암호화
530
복귀

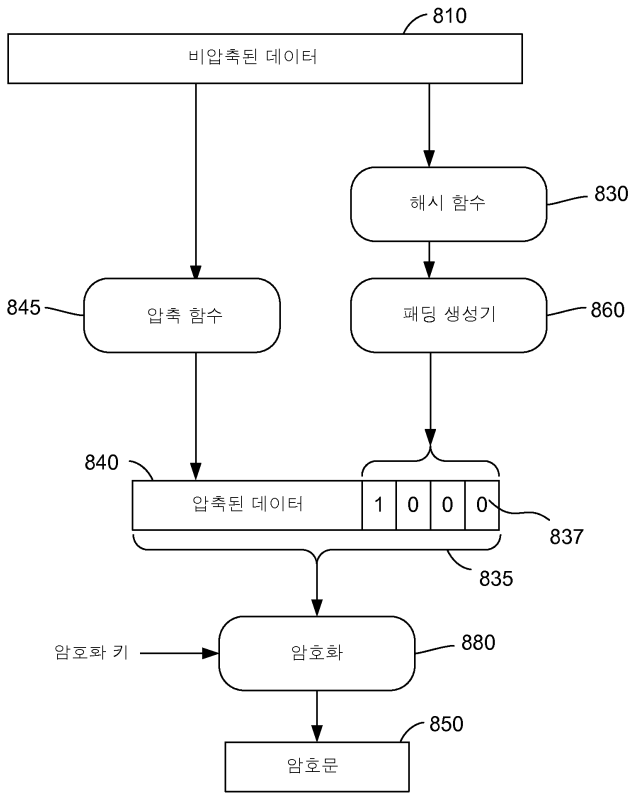
도면6


610
비압축된 데이터
630
해시 함수
670
압축 함수
690
640
압축된 데이터
암호화 키
680
암호화
650
암호문

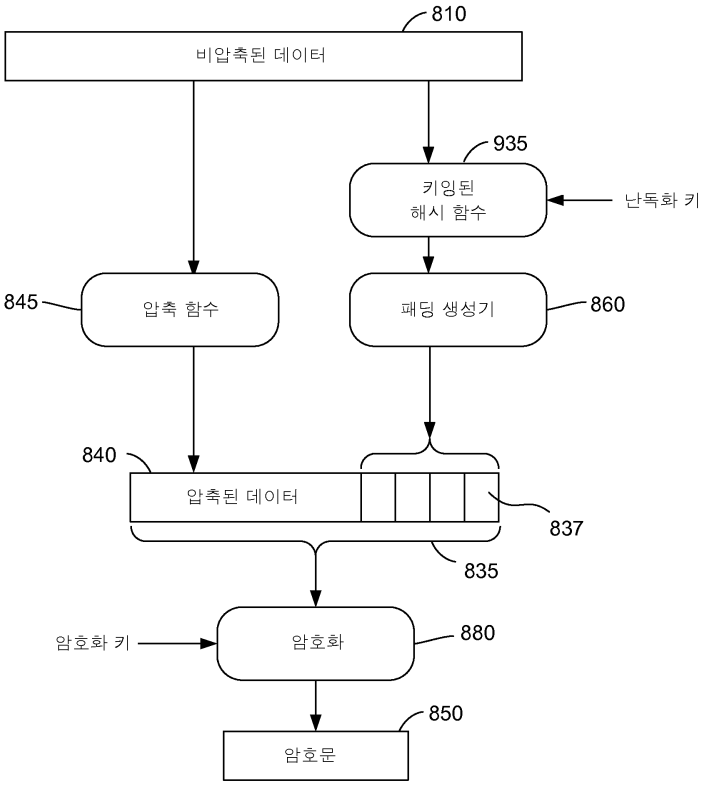
도면7


700
진입
제 1 수의 데이터 바이트들을 포함하는
압축된 데이터를 생성하기 위해
메시지 데이터를 압축
710
제 2 수의 데이터 바이트들을 포함하는 패딩된
압축된 데이터를 생성하기 위해 압축된 데이터를 패딩,
여기서 제 2 수는 데이터 바이트들의 '제 1 수' + '패드 수'와
동일하고, 데이터 바이트들의 패드 수는
메시지 데이터 해시에 기초하여 결정됨
720
암호화된 메시지 데이터를 생성하기 위해
패딩된 압축된 데이터를 암호화
730
복귀

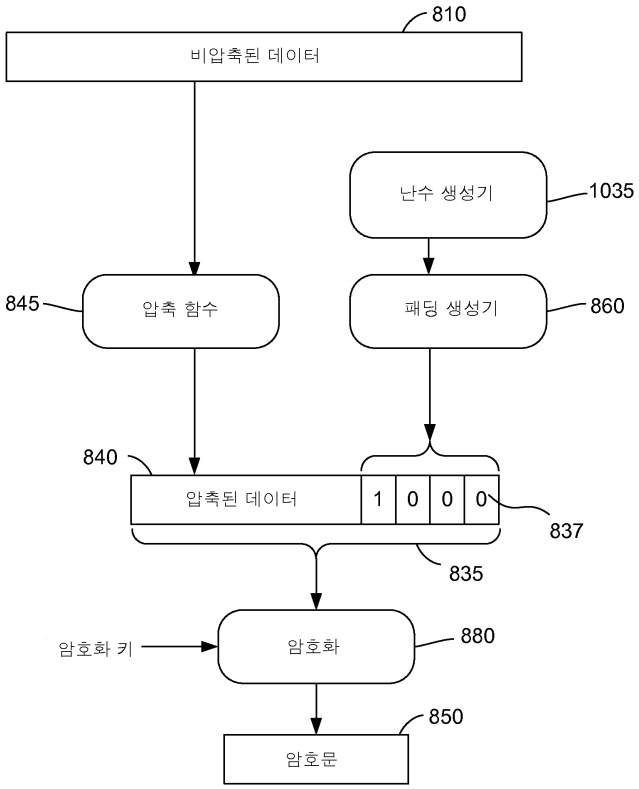
도면8


810
비압축된 데이터
해시 함수
830
845
압축 함수
패딩 생성기
860
840
압축된 데이터
1
0
0
0
837
835
암호화 키
암호화
880
850
암호문

도면9


810
비압축된 데이터
935
키잉된
해시 함수
난독화 키
845
압축 함수
패딩 생성기
860
840
압축된 데이터
837
835
암호화 키
암호화
880
850
암호문

도면10


810
비압축된 데이터
난수 생성기
1035
845
압축 함수
패딩 생성기
860
840
압축된 데이터
1
0
0
0
837
835
암호화 키
암호화
880
850
암호문