(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0048860
(43) 공개일자 2016년05월04일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 12/14* (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/0869 (2013.01)
G06F 12/1408 (2013.01)
(21) 출원번호 10-2016-7007529
(22) 출원일자(국제) 2014년08월27일
심사청구일자 없음
(85) 번역문제출일자 2016년03월22일
(86) 국제출원번호 PCT/US2014/052877
(87) 국제공개번호 WO 2015/031458
국제공개일자 2015년03월05일
(30) 우선권주장
14/014,962 2013년08월30일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
안사리, 비잔
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
시아오, 루
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

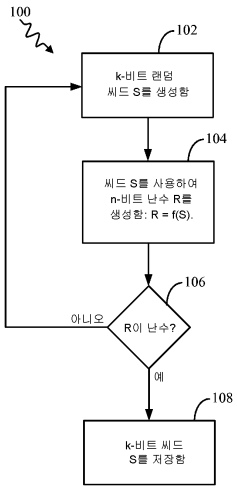
전체 청구항 수 : 총 38 항

(54) 발명의 명칭 **소수 생성 및 저장을 위한 방법들 및 장치들**

(57) 요 약

하나의 특징은, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고, 이 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 －k는 n 미만임－, 그리고 난수 R가 소수인지의 여부를 결정함으로써, 소수를 생성하기 위한 방법에 관련된다. 생성되는 난수 R가 소수임이 결정될 때까지, 단계들은 반복되고, 생성되는 난수 R가 소수임이 결정될 때, 이 난수 R를 생성하는데 사용된 난수 씨드 S가 메모리 회로에 저장된다. 추후에, 저장된 난수 씨드 S는 메모리 회로로부터 리트리빙될 수 있고, 그리고 소수는 난수 씨드 S에 기초하여 재생성된다. 일 예에서, 생성된 난수 R은 추가로, 보안 메모리 회로에 저장될 수 있는 비밀 키 k_S에 기초한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3033 (2013.01)

명 세 서

청구범위

청구항 1

방법으로서,

생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로,

k개 비트들을 갖는 난수 씨드 S를 생성하고,

상기 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 -k는 n 미만임-, 그리고

상기 난수 R가 소수인지의 여부를 결정함으로써,

소수를 생성하는 단계; 및

소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 메모리 회로에 저장하는 단계

를 포함하는,

방법.

청구항 2

제 1 항에 있어서,

상기 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하는 단계; 및

상기 난수 씨드 S에 기초하여 상기 소수를 재생성하는 단계

를 더 포함하는,

방법.

청구항 3

제 2 항에 있어서,

상기 소수에 기초하여 암호 키를 생성하는 단계

를 더 포함하는,

방법.

청구항 4

제 1 항에 있어서,

상기 씨드 S를 저장한 이후에, 메모리 회로로부터 상기 난수 R를 삭제하는 단계

를 더 포함하는,

방법.

청구항 5

제 1 항에 있어서,

상기 난수 R를 생성하는 것은 추가로, 비밀 키 k_S에 기초하는,

방법.

청구항 6

제 5 항에 있어서,

소수인 것으로 결정된 난수 R를 생성하는데 사용된 상기 비밀 키 k_S를 보안 메모리 회로에 저장하는 단계

를 더 포함하는,

방법.

청구항 7

제 1 항에 있어서,

암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 상기 난수 씨드 S가 저장되는,

방법.

청구항 8

제 1 항에 있어서,

상기 씨드 S에 기초하여 난수 R를 생성하는 것은,

입력으로서 상기 씨드 S를 수신하고 출력으로서 상기 난수 R를 생성하는 일방향 함수 f를 실행하는 것

을 포함하고,

상기 일방향 함수 f는 보안 해시 함수 및/또는 블록 암호 중 적어도 하나인,

방법.

청구항 9

장치로서,

메모리 회로; 및

상기 메모리 회로에 통신 가능하게 커플링된 프로세싱 회로

를 포함하고,

상기 프로세싱 회로는,

생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로,

k개 비트들을 갖는 난수 씨드 S를 생성하고,

상기 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 －k는 n 미만임－, 그리고

상기 난수 R가 소수인지의 여부를 결정함으로써,

소수를 생성하고; 그리고

소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 상기 메모리 회로에 저장하도록

구성되는,

장치.

청구항 10

제 9 항에 있어서,

상기 프로세싱 회로는 추가로,

상기 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하고; 그리고

상기 난수 씨드 S에 기초하여 상기 소수를 재생성하도록

구성되는,

장치.

청구항 11

제 10 항에 있어서,

상기 프로세싱 회로는 추가로,

상기 소수에 기초하여 암호 키를 생성하도록

구성되는,

장치.

청구항 12

제 9 항에 있어서,

암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 상기 난수 씨드 S가 저장되는,

장치.

청구항 13

제 9 항에 있어서,

소수인 것으로 결정된 난수 R를 생성하는 것은 추가로, 비밀 키 k_S에 기초하고, 그리고 상기 프로세싱 회로는 추가로, 상기 비밀 키 k_S를 보안 메모리 회로에 저장하도록 구성되는,

장치.

청구항 14

장치로서,

생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로,

k개 비트들을 갖는 난수 씨드 S를 생성하고,

상기 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 －k는 n 미만임－, 그리고

상기 난수 R가 소수인지의 여부를 결정함으로써,

소수를 생성하기 위한 수단; 및

소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 메모리 회로에 저장하기 위한 수단

을 포함하는,

장치.

청구항 15

제 14 항에 있어서,

상기 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하기 위한 수단; 및

상기 난수 씨드 S에 기초하여 상기 소수를 재생성하기 위한 수단

을 더 포함하는,

장치.

청구항 16

제 14 항에 있어서,

암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 상기 난수 씨드 S가 저장되는,

장치.

청구항 17

제 14 항에 있어서,

소수인 것으로 결정된 난수 R를 생성하는 것은 추가로, 비밀 키 k_S에 기초하고, 그리고 상기 장치는, 상기 비밀 키 k_S를 보안 메모리 회로에 저장하기 위한 수단을 더 포함하는,

장치.

청구항 18

하나 또는 그 초과의 명령들이 저장되어 있는 컴퓨터-판독가능 저장 매체로서,

상기 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로,

k개 비트들을 갖는 난수 씨드 S를 생성하고,

상기 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 －k는 n 미만임－, 그리고

상기 난수 R가 소수인지의 여부를 결정함으로써,

소수를 생성하게 하고; 그리고

소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 메모리 회로에 저장하게 하는,

컴퓨터-판독가능 저장 매체.

청구항 19

제 18 항에 있어서,

상기 명령들은 추가로, 상기 프로세서로 하여금,

상기 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하게 하고; 그리고

상기 난수 씨드 S에 기초하여 상기 소수를 재생성하게 하는,

컴퓨터-판독가능 저장 매체.

청구항 20

방법으로서,

k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하는 단계;

각각이 상기 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 상기 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하는 단계;

각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하는 단계 －n은 k + g 미만이고, 상기 복수의 난수들 R_i 각각은 상기 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함－;

상기 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하는 단계 －상기 난수 R_P는 상기 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 상기 제2 씨드 S_P는 상기 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 상기 난수 씨드 S에 기초함－; 및

상기 난수 씨드 S 및 상기 보충 씨드 T_P를 메모리 회로에 저장하는 단계

를 포함하는,

방법.

청구항 21

제 20 항에 있어서,

상기 복수의 난수들 R_i은 추가로, 비밀 키 k_S에 기초하고, 그리고 상기 방법은 상기 비밀 키 k_S를 보안 메모리 회로에 저장하는 단계를 더 포함하는,

방법.

청구항 22

제 20 항에 있어서,

상기 메모리 회로로부터 저장된 난수 씨드 S 및 상기 보충 씨드 T_P를 리트리빙하는 단계; 및

상기 난수 씨드 S 및 상기 보충 씨드 T_P에 기초하여 소수 난수 R_P를 재생성하는 단계

를 더 포함하는,

방법.

청구항 23

제 22 항에 있어서,

암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 상기 난수 씨드 S 및 상기 보충 씨드 T_P가 저장되고, 그리고 상기 방법은,

상기 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하는 단계;

상기 소수 난수 R_P에 기초하여 암호 키를 생성하는 단계; 및

상기 암호 키를 상기 암호 키 생성 프로세스에 제공하는 단계

를 더 포함하는,

방법.

청구항 24

제 21 항에 있어서,

상기 복수의 제2 씨드들 S_i 중 상이한 제2 씨드들에 기초하여 상기 복수의 난수들 R_i을 생성하는 단계는,

입력들로서 상기 복수의 제2 씨드들 S_i 각각을 수신하고 출력들로서 상기 복수의 난수들 R_i을 생성하는 일방향 함수 f를 실행하는 단계

를 포함하고,

상기 일방향 함수 f는 보안 해시 함수 및/또는 블록 암호 중 적어도 하나인,

방법.

청구항 25

제 21 항에 있어서,

상기 복수의 난수들 R_i 중 적어도 하나의 난수가 소수가 아님을 결정하는 단계;

g개 비트들을 갖는 다른 보충 씨드 T_2를 생성하는 단계;

상기 보충 씨드 T_2 및 상기 난수 씨드 S에 기초하여 다른 제2 씨드 S_2를 생성하는 단계;

n개 비트들을 갖는 다른 난수 R_2를 생성하는 단계 -상기 난수 R_2는 상기 제2 씨드 S_2에 기초함-;

상기 난수 R_2가 소수임을 결정하는 단계; 및

상기 보충 씨드 T_2를 상기 메모리 회로에 저장하는 단계

를 더 포함하는,

방법.

청구항 26

제 25 항에 있어서,

상기 메모리 회로로부터 저장된 난수 씨드 S 및 상기 보충 씨드 T_2를 리트리빙하는 단계; 및

상기 난수 씨드 S 및 상기 보충 씨드 T_2에 기초하여 상기 소수 난수 R_2를 재생성하는 단계

를 더 포함하는,

방법.

청구항 27

제 25 항에 있어서,

미리결정된 수의 소수들에 대한 요청을 수신하는 단계; 및

각각이 상이한 소수들과 연관되는 다수의 보충 씨드들이 상기 미리결정된 수와 동일한 수로 저장될 때까지, 다른 보충 씨드 T_2를 생성하는 방법 단계, 상기 보충 씨드 T_2 및 상기 난수 씨드 S에 기초하여 다른 제2 씨드 S_2를 생성하는 방법 단계, n개 비트들을 갖는 다른 난수 R_2를 생성하는 방법 단계 -상기 난수 R_2는 상기 제2 씨드 S_2에 기초함-, 상기 난수 R_2가 소수임을 결정하는 방법 단계, 및 상기 보충 씨드 T_2를 상기 메모리 회로에 저장하는 방법 단계를 반복하는 단계

를 더 포함하는,

방법.

청구항 28

장치로서,

메모리 회로; 및

상기 메모리 회로에 통신 가능하게 커플링된 프로세싱 회로

를 포함하고,

상기 프로세싱 회로는,

k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하고,

각각이 상기 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 상기 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하고,

각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하고 -n은 k + g 미만이고, 상기 복수의 난수들 R_i 각각은 상기 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함-,

상기 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하고 －상기 난수 R_P는 상기 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 상기 제2 씨드 S_P는 상기 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 상기 난수 씨드 S에 기초함－; 그리고

상기 난수 씨드 S 및 상기 보충 씨드 T_P를 메모리 회로에 저장하도록

구성되는,

장치.

청구항 29

제 28 항에 있어서,

상기 복수의 난수들 R_i은 추가로, 비밀 키 k_S에 기초하고, 그리고 상기 프로세싱 회로는 추가로, 상기 비밀 키 k_S를 보안 메모리 회로에 저장하도록 구성되는,

장치.

청구항 30

제 28 항에 있어서,

상기 프로세싱 회로는 추가로,

상기 메모리 회로로부터 저장된 난수 씨드 S 및 상기 보충 씨드 T_P를 리트리빙하고; 그리고

상기 난수 씨드 S 및 상기 보충 씨드 T_P에 기초하여 소수 난수 R_P를 재생성하도록

구성되는,

장치.

청구항 31

제 30 항에 있어서,

암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 상기 난수 씨드 S 및 상기 보충 씨드 T_P가 저장되고, 그리고 상기 프로세싱 회로는 추가로,

상기 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하고;

상기 소수 난수 R_P에 기초하여 암호 키를 생성하고; 그리고

상기 암호 키를 상기 암호 키 생성 프로세스에 제공하도록

구성되는,

장치.

청구항 32

제 28 항에 있어서,

상기 복수의 제2 씨드들 S_i 중 상이한 제2 씨드들에 기초하여 상기 복수의 난수들 R_i을 생성하는 것은, 상기 프로세싱 회로가 추가로,

입력들로서 상기 복수의 제2 씨드들 S_i 각각을 수신하고 출력들로서 상기 복수의 난수들 R_i을 생성하는 일방향 함수 f를 실행하도록 구성되는 것

을 포함하고,

상기 일방향 함수 f는 보안 해시 함수 및/또는 블록 암호 중 적어도 하나인,

장치.

청구항 33

제 28 항에 있어서,

상기 프로세싱 회로는 추가로,

상기 복수의 난수들 R_i 중 적어도 하나의 난수가 소수가 아님을 결정하고;

g개 비트들을 갖는 다른 보충 씨드 T_2를 생성하고;

상기 보충 씨드 T_2 및 상기 난수 씨드 S에 기초하여 다른 제2 씨드 S_2를 생성하고;

n개 비트들을 갖는 다른 난수 R_2를 생성하고 －상기 난수 R_2는 상기 제2 씨드 S_2에 기초함－;

상기 난수 R_2가 소수임을 결정하고; 그리고

상기 보충 씨드 T_2를 상기 메모리 회로에 저장하도록

구성되는,

장치.

청구항 34

제 33 항에 있어서,

상기 프로세싱 회로는 추가로,

상기 메모리 회로로부터 저장된 난수 씨드 S 및 상기 보충 씨드 T_2를 리트리빙하고; 그리고

상기 난수 씨드 S 및 상기 보충 씨드 T_2에 기초하여 상기 소수 난수 R_2를 재생성하도록

구성되는,

장치.

청구항 35

장치로서,

k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하기 위한 수단;

각각이 상기 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 상기 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하기 위한 수단;

각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하기 위한 수단 －n은 k + g 미만이고, 상기 복수의 난수들 R_i 각각은 상기 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함－;

상기 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하기 위한 수단 －상기 난수 R_P는 상기 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 상기 제2 씨드 S_P는 상기 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 상기 난수 씨드 S에 기초함－; 및

상기 난수 씨드 S 및 상기 보충 씨드 T_P를 메모리 회로에 저장하기 위한 수단

을 포함하는,

장치.

청구항 36

제 35 항에 있어서,

상기 메모리 회로로부터 저장된 난수 씨드 S 및 상기 보충 씨드 T_P를 리트리빙하기 위한 수단; 및

상기 난수 씨드 S 및 상기 보충 씨드 T_P에 기초하여 소수 난수 R_P를 재생성하기 위한 수단

을 더 포함하는,

장치.

청구항 37

하나 또는 그 초과의 명령들이 저장되어 있는 컴퓨터-판독가능 저장 매체로서,

상기 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 상기 프로세서로 하여금,

k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하게 하고;

각각이 상기 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 상기 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하게 하고;

각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하게 하고 －n은 k + g 미만이고, 상기 복수의 난수들 R_i 각각은 상기 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함－;

상기 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하게 하고 －상기 난수 R_P는 상기 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 상기 제2 씨드 S_P는 상기 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 상기 난수 씨드 S에 기초함－; 그리고

상기 난수 씨드 S 및 상기 보충 씨드 T_P를 메모리 회로에 저장하게 하는,

컴퓨터-판독가능 저장 매체.

청구항 38

제 37 항에 있어서,

상기 명령들은 추가로, 상기 프로세서로 하여금,

상기 메모리 회로로부터 저장된 난수 씨드 S 및 상기 보충 씨드 T_P를 리트리빙하게 하고; 그리고

상기 난수 씨드 S 및 상기 보충 씨드 T_P에 기초하여 소수 난수 R_P를 재생성하게 하는,

컴퓨터-판독가능 저장 매체.

발명의 설명

기 술 분 야

[0001] [0001] 다양한 특징들은 암호 기법(cryptography)에 관한 것이고, 더욱 구체적으로는, 소수들의 생성 및 효율적인 저장을 위한 방법들 및 장치들에 관한 것이다.

배 경 기 술

[0002] [0002] 많은 암호 보안 알고리즘들, 예컨대, RSA(Rivest Shamir Adleman) 알고리즘은 암호 키들을 활용하여 동작한다. 이러한 키들은 통상적으로, 비교적 커다란(예컨대, 512개 비트, 1,024개 비트 등) 소수들을 요구할 수 있는 키 생성 프로세스들을 사용하여 생성된다. 그러나, 소수 생성은 느린 프로세스이고, 그리고 소수 생성과 연관된 프로세싱 시간은 통상적으로 키 생성 프로세스들에서 보틀 넥으로서 동작한다. 요구되는 프로세싱 시간

은 키 생성 프로세스에 의해 생성될 키의 비트 길이의 세제곱(cube)에 비례한다. 예컨대, 2,048개 비트 암호 키 및 3,072개 비트 암호 키를 생성하는 것은, 1,024개 비트 키를 생성하는 것보다 각각 8배 및 27배 더 느릴 수 있다. 전력 및 속도 제약들이 관련되는 모바일 디바이스 애플리케이션들에서, 전력 소모량 및 프로세싱 시간의 이러한 증가들은 악영향이다.

[0003] [0003] 일부 애플리케이션들에 따라, 암호 키들은, 이 암호 키들이 애플리케이션에 의해 실제로 요구되기 이전에 이 암호 키들이 생성된다는 점에서, "오프라인"으로 생성될 수 있다. 이러한 오프라인 방식으로 생성되는 암호 키들을 생성하는데 사용되는 소수들 또는 암호 키들은 통상적으로 메모리에 저장되고, 이후, 요구 시 애플리케이션(들)에 전달된다. 그 경우, 위에서 설명된 키 생성과 연관된 프로세싱 시간에서의 보틀 넥은 사실상 제거된다. 그러나, 이러한 오프라인 키 생성 방식들에 대한 하나의 두드러진 이슈는, 키들 및/또는 키들을 생성하는데 사용되는 소수들이 비교적 커다랄 수 있고(예컨대, 1,024개 비트들을 초과) 그리고 이러한 커다란 키들 및/또는 소수들을 저장하는데 요구되는 필요한 메모리 회로들이 항상 용이하게 이용 가능한 것이 아닐 수 있다는 점이다. 이 문제점을 가라앉히기 위해, 규칙적인 데이터 압축 기법들은 이들 경우들에서 그다지 적용 가능하지 않은데, 그 이유는 암호 키들 및 소수들이 높은 엔트로피를 갖고 그리고 통상적인 압축 알고리즘들에 대해 효율적으로 압축될 수 없기 때문이다.

[0004] [0004] 따라서, 암호 보안 알고리즘들, 예컨대, RSA에서의 사용을 위한 커다란 소수들을 저장하는데 요구되는 메모리의 양을 최소화시키기 위하여 소수 생성 및 저장을 돕는 새로운 방법들 및 장치들이 요구된다.

발명의 내용

[0005] [0005] 하나의 특징은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법을 제공한다. 이 방법은, 생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고, 이 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 −k는 n 미만임−, 그리고 난수 R가 소수인지의 여부를 결정함으로써, 소수를 생성하는 단계를 포함한다. 소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S는 메모리 회로에 저장된다. 일 양상에 따라, 방법은, 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하는 단계, 및 이 난수 씨드 S에 기초하여 소수를 재생성하는 단계를 더 포함한다. 다른 양상에 따라, 방법은 소수에 기초하여 암호 키를 생성하는 단계를 더 포함한다.

[0006] [0006] 일 양상에 따라, 방법은 씨드 S를 저장한 이후에, 메모리 회로로부터 난수 R를 삭제하는 단계를 더 포함한다. 다른 양상에 따라, 난수 R를 생성하는 것은 추가로, 비밀 키 k_S에 기초한다. 또 다른 양상에 따라, 방법은 소수인 것으로 결정된 난수 R를 생성하는데 사용된 비밀 키 k_S를 보안 메모리 회로에 저장하는 단계를 더 포함한다.

[0007] [0007] 일 양상에 따라, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 난수 씨드 S가 저장된다. 다른 양상에 따라, 씨드 S에 기초하여 난수 R를 생성하는 것은, 입력으로서 씨드 S를 수신하고 출력으로서 난수 R를 생성하는 일방향 함수 f를 실행하는 것을 포함하고, 이 일방향 함수 f는 보안 해시 함수 및/또는 블록 암호 중 적어도 하나이다.

[0008] [0008] 다른 특징은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 장치를 제공하고, 이 장치는 메모리 회로, 및 이 메모리 회로에 통신 가능하게 커플링된 프로세싱 회로를 포함하고, 이 프로세싱 회로는, 생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고, 이 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 −k는 n 미만임−, 그리고 난수 R가 소수인지의 여부를 결정함으로써, 소수를 생성하고, 그리고 소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 메모리 회로에 저장하도록 구성된다. 일 양상에 따라, 프로세싱 회로는 추가로, 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하고, 그리고 난수 씨드 S에 기초하여 소수를 재생성하도록 구성된다. 다른 양상에 따라, 프로세싱 회로는 추가로, 소수에 기초하여 암호 키를 생성하도록 구성된다. 또 다른 양상에 따라, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 난수 씨드 S가 저장된다. 다른 양상에 따라, 소수인 것으로 결정된 난수 R를 생성하는 것은 추가로, 비밀 키 k_S에 기초하고, 그리고 프로세싱 회로는 추가로, 비밀 키 k_S를 보안 메모리 회로에 저장하도록 구성된다.

[0009] [0009] 다른 특징은, 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 장치를 제공하고, 이 장치는, 생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고, 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 −k는 n 미만임−, 그리고 난수 R가 소수인지의 여부를 결정함으

로써, 소수를 생성하기 위한 수단, 및 소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 메모리 회로에 저장하기 위한 수단을 포함한다. 일 양상에 따라, 장치는, 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하기 위한 수단, 및 난수 씨드 S에 기초하여 소수를 재생성하기 위한 수단을 더 포함한다. 다른 양상에 따라, 소수인 것으로 결정된 난수 R를 생성하는 것은 추가로, 비밀 키 k_S에 기초하고, 그리고 장치는, 비밀 키 k_S를 보안 메모리 회로에 저장하기 위한 수단을 더 포함한다.

[0010] [0010] 다른 특징은 하나 또는 그 초과의 명령들이 저장되어 있는 컴퓨터-판독가능 저장 매체를 제공하고, 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, 생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고, 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고 -k는 n 미만임-, 그리고 난수 R가 소수인지의 여부를 결정함으로써, 소수를 생성하게 하고, 그리고 소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 메모리 회로에 저장하게 한다. 일 양상에 따라, 명령들은 추가로, 프로세서로 하여금, 메모리 회로로부터 저장된 난수 씨드 S를 리트리빙하게 하고, 그리고 난수 씨드 S에 기초하여 소수를 재생성하게 한다.

[0011] [0011] 다른 특징은, 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법을 제공하고, 이 방법은, k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하는 단계, 각각이 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하는 단계, 각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하는 단계 -n은 k + g 미만이고, 복수의 난수들 R_i 각각은 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함-, 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하는 단계 -난수 R_P는 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 제2 씨드 S_P는 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 난수 씨드 S에 기초함-, 및 난수 씨드 S 및 보충 씨드 T_P를 메모리 회로에 저장하는 단계를 포함한다. 일 양상에 따라, 복수의 난수들 R_i은 추가로, 비밀 키 k_S에 기초하고, 그리고 방법은 비밀 키 k_S를 보안 메모리 회로에 저장하는 단계를 더 포함한다. 다른 양상에 따라, 방법은, 메모리 회로로부터 저장된 난수 씨드 S 및 상기 보충 씨드 T_P를 리트리빙하는 단계, 및 난수 씨드 S 및 보충 씨드 T_P에 기초하여 소수 난수 R_P를 재생성하는 단계를 더 포함한다. 또 다른 양상에 따라, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 난수 씨드 S 및 보충 씨드 T_P가 저장되고, 그리고 방법은, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하는 단계, 소수 난수 R_P에 기초하여 암호 키를 생성하는 단계, 및 암호 키를 암호 키 생성 프로세스에 제공하는 단계를 더 포함한다.

[0012] [0012] 일 양상에 따라, 복수의 제2 씨드들 S_i 중 상이한 제2 씨드들에 기초하여 복수의 난수들 R_i을 생성하는 단계는, 입력들로서 복수의 제2 씨드들 S_i 각각을 수신하고 출력들로서 복수의 난수들 R_i을 생성하는 일방향 함수 f를 실행하는 단계를 포함하고, 일방향 함수 f는 보안 해시 함수 및/또는 블록 암호 중 적어도 하나이다. 다른 양상에 따라, 방법은, 복수의 난수들 R_i 중 적어도 하나의 난수가 소수가 아님을 결정하는 단계, g개 비트들을 갖는 다른 보충 씨드 T_2를 생성하는 단계, 보충 씨드 T_2 및 난수 씨드 S에 기초하여 다른 제2 씨드 S_2를 생성하는 단계, n개 비트들을 갖는 다른 난수 R_2를 생성하는 단계 -난수 R_2는 제2 씨드 S_2에 기초함-, 난수 R_2가 소수임을 결정하는 단계, 및 보충 씨드 T_2를 메모리 회로에 저장하는 단계를 더 포함한다. 또 다른 양상에 따라, 방법은, 메모리 회로로부터 저장된 난수 씨드 S 및 보충 씨드 T_2를 리트리빙하는 단계, 및 난수 씨드 S 및 보충 씨드 T_2에 기초하여 소수 난수 R_2를 재생성하는 단계를 더 포함한다. 다른 양상에 따라, 방법은, 미리 결정된 수의 소수들에 대한 요청을 수신하는 단계, 및 각각이 상이한 소수들과 연관되는 다수의 보충 씨드들이 이 미리결정된 수와 동일한 수로 저장될 때까지, 다른 보충 씨드 T_2를 생성하는 방법 단계, 보충 씨드 T_2 및 난수 씨드 S에 기초하여 다른 제2 씨드 S_2를 생성하는 방법 단계, n개 비트들을 갖는 다른 난수 R_2를 생성하는 방법 단계 -난수 R_2는 제2 씨드 S_2에 기초함-, 난수 R_2가 소수임을 결정하는 방법 단계, 및 보충 씨드 T_2를 메모리 회로에 저장하는 단계를 반복하는 단계를 더 포함한다.

[0013] [0013] 다른 특징은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 장치를 제공하고, 장치는 메모리 회로, 및 메모리 회로에 통신 가능하게 커플링된 프로세싱 회로를 포함하고, 프로세싱 회로는, k개 비트들을 갖는

난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하고, 각각이 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하고, 각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하고 -n은 k + g 미만이고, 복수의 난수들 R_i 각각은 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함-, 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하고 -난수 R_P는 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 제2 씨드 S_P는 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 난수 씨드 S에 기초함-, 그리고 난수 씨드 S 및 보충 씨드 T_P를 메모리 회로에 저장하도록 구성된다. 일 양상에 따라, 복수의 난수들 R_i은 추가로, 비밀 키 k_S에 기초하고, 그리고 프로세싱 회로는 추가로, 비밀 키 k_S를 보안 메모리 회로에 저장하도록 구성된다. 다른 양상에 따라, 프로세싱 회로는 추가로, 메모리 회로로부터 저장된 난수 씨드 S 및 보충 씨드 T_P를 리트리빙하고, 그리고 난수 씨드 S 및 보충 씨드 T_P에 기초하여 소수 난수 R_P를 재생성하도록 구성된다. 또 다른 양상에 따라, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 난수 씨드 S 및 보충 씨드 T_P가 저장되고, 그리고 프로세싱 회로는 추가로, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하고, 소수 난수 R_P에 기초하여 암호 키를 생성하고, 그리고 암호 키를 암호 키 생성 프로세스에 제공하도록 구성된다.

[0014] [0014] 일 양상에 따라, 복수의 제2 씨드들 S_i 중 상이한 제2 씨드들에 기초하여 복수의 난수들 R_i을 생성하는 것은, 프로세싱 회로가 추가로, 입력들로서 복수의 제2 씨드들 S_i 각각을 수신하고 출력들로서 복수의 난수들 R_i을 생성하는 일방향 함수 f를 실행하도록 구성되는 것을 포함하고, 일방향 함수 f는 보안 해시 함수 및/또는 블록 암호 중 적어도 하나이다. 다른 양상에 따라, 프로세싱 회로는 추가로, 복수의 난수들 R_i 중 적어도 하나의 난수가 소수가 아님을 결정하고, g개 비트들을 갖는 다른 보충 씨드 T_2를 생성하고, 보충 씨드 T_2 및 난수 씨드 S에 기초하여 다른 제2 씨드 S_2를 생성하고, n개 비트들을 갖는 다른 난수 R_2를 생성하고 -난수 R_2는 제2 씨드 S_2에 기초함-, 난수 R_2가 소수임을 결정하고, 그리고 보충 씨드 T_2를 메모리 회로에 저장하도록 구성된다. 또 다른 양상에 따라, 프로세싱 회로는 추가로, 메모리 회로로부터 저장된 난수 씨드 S 및 보충 씨드 T_2를 리트리빙하고, 그리고 난수 씨드 S 및 보충 씨드 T_2에 기초하여 소수 난수 R_2를 재생성하도록 구성된다.

[0015] [0015] 다른 특징은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 장치를 제공하고, 장치는, k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하기 위한 수단, 각각이 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하기 위한 수단, 각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하기 위한 수단 -n은 k + g 미만이고, 복수의 난수들 R_i 각각은 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함-, 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하기 위한 수단 -난수 R_P는 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 제2 씨드 S_P는 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 난수 씨드 S에 기초함-, 및 난수 씨드 S 및 보충 씨드 T_P를 메모리 회로에 저장하기 위한 수단을 포함한다. 일 양상에 따라, 장치는, 메모리 회로로부터 저장된 난수 씨드 S 및 보충 씨드 T_P를 리트리빙하기 위한 수단, 및 난수 씨드 S 및 보충 씨드 T_P에 기초하여 소수 난수 R_P를 재생성하기 위한 수단을 더 포함한다.

[0016] [0016] 다른 특징은 하나 또는 그 초과의 명령들이 저장되어 있는 컴퓨터-판독가능 저장 매체를 제공하고, 명령들은, 적어도 하나의 프로세서에 의해 실행될 때, 프로세서로 하여금, k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i을 생성하게 하고, 각각이 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i을 생성하게 하고, 각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하게 하고 -n은 k + g 미만이고, 복수의 난수들 R_i 각각은 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초함-, 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임을 결정하게 하고 -난수 R_P는 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 제2 씨드 S_P는 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 난수 씨드 S에 기초함-, 그리고 난수 씨드 S 및 보충 씨드 T_P를 메모리 회로에 저장하게 한다. 일 양상에 따라, 명령들은 추가로, 프로세서로 하여금, 메모리 회로로부터 저장된 난수 씨드 S 및 보충 씨드 T_P를 리트리빙하게 하고, 그리

고 난수 씨드 S 및 보충 씨드 T_p에 기초하여 소수 난수 R_p를 재생성하게 한다.

도면의 간단한 설명

[0017] [0017] 도 1은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도의 제1 예를 예시한다.

[0018] [0018] 도 2는 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도의 제2 예를 예시한다.

[0019] [0019] 도 3은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름 차트의 제1 예를 예시한다.

[0020] [0020] 도 4는 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도의 제3 예를 예시한다.

[0021] [0021] 도 5는 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도의 제4 예를 예시한다.

[0022] [0022] 도 6은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름 차트의 제2 예를 예시한다.

[0023] [0023] 도 7a 및 도 7b는 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도의 제5 예를 예시한다.

[0024] [0024] 도 8은 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도(800)를 예시한다.

[0025] [0025] 도 9는 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름 차트(900)를 예시한다.

[0026] [0026] 도 10은 본원에 설명되는 암호 보안을 위한 방법들 중 임의의 방법을 실행하는 전자 디바이스(1000)에 대한 하드웨어 구현이 예시적이고 개략적인 블록도를 예시한다.

[0027] [0027] 도 11은 프로세싱 회로의 개략적인 블록도를 예시한다.

[0028] [0028] 도 12는 프로세싱 회로의 개략적인 블록도를 예시한다.

발명을 실시하기 위한 구체적인 내용

[0018] [0029] 하기의 설명에서는, 본 개시물의 다양한 양상들의 완전한 이해를 제공하기 위해 특정 세부사항들이 제공된다. 그러나, 이러한 특정 세부사항들 없이, 양상들이 실시될 수 있음이 당업자에 의해 이해될 것이다. 예컨대, 양상들을 불필요한 세부사항으로 모호하게 하는 것을 회피하기 위하여, 회로들은 블록도들로 도시될 수 있다. 다른 실례들에서, 본 개시물의 양상들을 모호하게 하지 않기 위하여, 잘 알려진 회로들, 구조들 및 기법들은 상세히 도시되지 않을 수 있다.

[0019] [0030] 본원에서 단어 "예시적"은 "예, 실례, 또는 예시로서의 역할을 하는"을 의미하는데 사용된다. 본원에서 "예시적"으로서 설명되는 임의의 구현 또는 양상이 반드시 본 개시물의 다른 양상들보다 바람직하거나 또는 유리한 것으로서 이해되어야 하는 것은 아니다. 마찬가지로, 용어 "양상들"은 본 개시물의 양상들 전부가 개시되는 특징, 장점, 또는 동작 모드를 포함함을 요구하지는 않는다. 본원에 사용되는 바와 같이, "소수 테스트(primality test)들" 및 "합성수 테스트(composite number test)들"은 상호 교환 가능하게 사용될 수 있고, 그리고 일반적으로 "소수 테스트들"로 지칭된다. 예컨대, Miller-Rabin 테스트와 같은 테스트들은 수(number)가 합성수임을 증명할 수 있다. 그렇게 함으로써, 테스트는 수가 소수가 아님을 또한 증명한다. 따라서, 본원에 사용된 바와 같이, 수에 대해 소수 테스트를 실행하는 것은 수가 합성수임을 증명하거나 또는 증명하려고 시도하는 그러한 테스트들을 포함한다. 본원에 사용된 바와 같이, "난수"는 참으로 랜덤할 수 있거나(예컨대, 그것은 진정한 난수 발생기(RNG:random number generator)에 의해 생성되었음) 또는 난수는 의사 랜덤할 수 있다(예컨대, 그것은 의사 난수 발생기(PRNG:pseudo random number generator)를 사용하여 생성되었음).

[0020] **개요**

[0021] [0031] 본원에서는 값들, 예컨대, 소수들을 생성하는데 사용되는 씨드 값들을 저장하는데 요구되는 메모리 회로 스토리지 공간의 양을 감소시키는 방법들 및 디바이스들이 설명되고, 이어서, 이 소수들은 보안 알고리즘들을 위한 암호 키들을 생성하는데 사용될 수 있다. 구체적으로, 비교적 많은 비트 수의 소수들 대신에, 하나 또는 그 초과의 비교적 작은 비트 수의 씨드 값들이 미리-컴퓨팅 및 저장된다. 이 씨드들 값들이, 요구 시 소수들을 생성하는데 추후 시점에 사용될 수 있다. 이러한 방법들 및 디바이스들은, 스토리지 공간이 제한되는 암호 가속기(crypto-accelerator) 하드웨어 모듈들을 갖는 모바일 디바이스들에 특히 유용하다. 또한, 다른 디바이스들은 암호 키 프로비저닝 비용들을 낮추기 위해 본원에 설명되는 방법들 및 장치들로부터 이득을 얻을 수 있다.

[0022] **소수 생성을 위해 사용되는 씨드 값들의 생성 및 저장을 위한 예시적 방법들**

[0023] [0032] 도 1은 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도(100)를 예시한다. 먼저, k-비트 난수 씨드 S가 생성된다(102). 난수 씨드 S는, 예컨대, 난수 발생기 또는 의사 난수 발생기를 사용하여 생성될 수 있다. 값 k는 2와 동일하거나 또는 그 초과의 임의의 정수일 수 있다. 이후, 난수 씨드 S는 n-비트 난수 R를 생성하는데 사용될 수 있고(104), 여기서 n > k이다. 구체적으로, 방정식 (1)에 따라 난수 씨드 S에 기초하여 난수 R를 생성하기 위해, 일방향 함수 f가 실행될 수 있다:

[0024] R = f(S) (1).

[0025] 일 예에 따라, 함수 f는 암호 해시 함수, 예컨대, 보안 해시 함수(예컨대, SHA-1, SHA-2, etc.) 또는 블록 암호, 예컨대, 비밀 키를 갖는 AES(advanced encryption standard)일 수 있다.

[0026] [0033] 다음 차례로, 난수 R가 소수인지의 여부를 결정하기 위해 소수 테스트가 수행된다(106). 단지 일 예로서, 수행되는 소수 테스트는 Miller-Rabin 소수 테스트를 포함할 수 있다. 난수 R가 소수인 것으로 결정되면, 난수 씨드 S는 메모리에 저장된다(108). 그렇지 않으면, 방법 단계들(102, 104, 106)이 반복되어, 새로운 난수 씨드 S가 생성되고(102), (예컨대, 함수 f를 사용하여) 난수 씨드 S에 기초하여 새로운 난수 R가 생성되며(104), 그리고 새롭게 생성된 난수 R가 소수인지의 여부를 결정하기 위해 소수 테스트가 실행된다(106). 난수 R가 소수인 것으로 결정될 때까지, 이들 단계들(102, 104, 106)이 계속해서 반복되고, 난수 R가 소수인 것으로 결정된 이후, 난수 R를 생성했던 난수 씨드 S가 저장된다(108). 일 예에 따라, 난수 씨드 S의 후속하는 반복들은 소수인 것으로 결정되지 않았던, 앞서 생성된 난수 R의 k개 비트들을 사용할 수 있다. 예컨대, 난수 씨드 S의 후속하는 반복은 이전 반복으로부터의 난수 R의 첫 번째 k개 비트들과 동일할 수 있다.

[0027] [0034] 난수 씨드 S의 비트들의 수(k)가 소수 난수 R의 비트들의 수(n) 미만이기 때문에, 난수 R 대신에 씨드 S를 저장함으로써 메모리 공간이 절약되며, 이 난수 R는 폐기/삭제될 수 있다. 추후에, 난수 씨드 S는 (예컨대, 자신이 저장된 메모리 회로로부터) 리트리빙될 수 있고, 그리고 일방향 함수 f를 사용하여 소수 난수 R를 재생성하는데 사용될 수 있다. 예컨대, 키 생성 프로세스는 하나 또는 그 초과의 소수들을 요청할 수 있고, 이 하나 또는 그 초과의 소수들은 위에서 설명된 방법(100)을 사용하여 공급될 수 있다. 단지 일 예에 따라, 이로써 생성된 키들은 암호 보안 알고리즘, 예컨대, RSA에 의해 사용될 수 있다.

[0028] [0035] 따라서, 도 1에 예시된 방법에 따라, 소수인 난수 R가 생성될 수 있고, 그리고 이후, 키 생성 알고리즘, 예컨대, RSA에 대해 사용되어, 암호 보안 키가 생성될 수 있다. 도 1에 예시된 방법은, 암호 보안 알고리즘(예컨대, 키들을 생성하기 위해 소수(들)를 요청하는 RSA 알고리즘)으로부터 소수에 대한 요청을 수신하기 이전에, 소수 난수 R를 생성하는 것으로 알려진 난수 씨드 S가 생성 및 저장된다는 점에서, "오프라인"으로 수행될 수 있다.

[0029] [0036] 도 2는 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도(200)를 예시한다. 먼저, k-비트 난수 씨드 S가 프로세싱 회로(202)(예컨대, 프로세서)에서 생성된다(208). (일 양상에 따라, 프로세싱 회로(202)에 의해 수행되는 단계들이 소프트웨어로 구현될 수 있음을 주목하라.) 이후, (예컨대, 도 1에 대해 위에서 설명된 함수 f를 사용하여) 씨드 S에 기초하여 n-비트 난수 R가 생성된다(210). 다음 차례로, 생성된 난수 R가 소수인지의 여부가 결정된다(212). 적어도 하나의 난수 R가 소수인 것으로 결정될 때까지, 단계들(208, 210, 212)이 반복된다(214). 이후, 일단 난수 R가 소수인 것으로 결정되면, 소수 난수 R를 생성하는데 사용된 씨드 S가 메모리 회로(204)(예컨대, 메모리)에 저장된다(216). 이 지점에서 소수 난수 R는 폐기 또는 삭제될 수 있는데, 그 이유는 씨드 S가 저장되었기 때문이다. 다음 차례로, 암호 보안 알고리즘(예컨대, RSA)을 구현하는 애플리케이션(206)으로부터 하나 또는 그 초과의 소수들에 대한 요청이 수신된다(218). 이 요청에 응답하여, 메모리로부터 씨드 S가 리트리빙되고(220), 그리고 이 씨드 S를 사용하여 n-비트 소수 난수 R가 재생성된다(222). 마지막으로, 이 소수 난수 R가 키 생성을 위해 소수(들)를 요청하는 애플리케이션에 송신/제공된다(224).

[0030] [0037] 도 3은 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름 차트(300)를 예시한다. 먼저, 생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고(304), 이 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고(306) -k는 n 미만임-, 그리고 난수 R가 소수인지의 여부를 결정함으로써(308), 소수 난수가 생성된다(302). 다음 차례로, 소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S가 저장된다(310).

[0031] [0038] 도 4는 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도(400)를 예시한다. 먼저, k-비트 난수 씨드 S가 생성된다(402). 난수 씨드 S는 예컨대, 난수 발생기 또는 의사 난수 발

생기를 사용하여 생성될 수 있다. 값 k는 2와 동일하거나 또는 그 초과의 임의의 정수일 수 있다. 이후, 난수 씨드 S는 비밀 키 k_S와 함께 n-비트 난수 R를 생성하는데 사용될 수 있고(404), 여기서 n > k이다. 구체적으로, 방정식 (2)에 따라 난수 씨드 S 및 비밀 키 k_S에 기초하여 난수 R를 생성하기 위해, 일방향 함수 f가 실행될 수 있다:

[0032] $$R = f(S, k_S) \qquad (2).$$

[0033] 일 예에서, 비밀 키 k_S는 방법(400)을 수행하는 장치에만 알려질 수 있다. 일 양상에 따라, 비밀 키 k_S는 방법(400)을 수행하는 장치에서 보안 메모리(예컨대, 판독 전용 메모리, 암호화될 수 있거나 또는 암호화되지 않을 수 있는 OTP(one-time programmable) 메모리)로부터 리트리빙될 수 있다. 이러한 경우, 비밀 키 k_S는, 키 k_S의 허가되지 않은 액세스/발견을 막기 위해, 사전에 보안 메모리에 저장될 수 있다. 다른 양상에 따라, 비밀 키 k_S가 반드시 장치에서 보안 메모리에 저장되는 것이 아닐 수 있으며, 대신에, 장치에서 즉석에서(on the fly) 생성된다.

[0034] [0039] 일 예에 따라, 일방향 함수 f는, 암호 메시지 인증 코드(MAC:message authentication code), 예컨대, 해시-기반 메시지 인증 코드(HMAC:hash-based message authentication code), 또는 블록 암호, 예컨대, AES(advanced encryption standard)일 수 있다. 양쪽 경우들 모두에서, MAC 또는 블록 암호는 비밀 키 k_S를 사용한다.

[0035] [0040] 다음 차례로, 난수 R가 소수인지의 여부를 결정하기 위해, 소수 테스트가 수행된다(406). 난수 R가 소수인 것으로 결정되면, 난수 씨드 S가 메모리에 저장된다(408). 선택적으로, 비밀 키 k_S가 이미 보안 메모리에 저장된 것이 아닌 경우들(예컨대, 비밀 키 k_S가 위에서 설명된 바와 같이 생성되는 경우들)에서, 그러면 비밀 키 k_S는 난수 R가 소수임이 결정된 이후에 메모리에 저장된다. 난수 R가 소수가 아닌 것으로 결정되면, 방법 단계들(402, 404, 406)이 반복되어, 새로운 난수 씨드 S가 생성되고(402), (예컨대, 함수 f를 사용하여) 난수 씨드 S 및 비밀 키 k_S에 기초하여 새로운 난수 R가 생성되며(404), 그리고 새롭게 생성된 난수 R가 소수인지의 여부를 결정하기 위해 소수 테스트가 실행된다(406). 난수 R가 소수인 것으로 결정될 때까지, 이들 단계들(402, 404, 406)이 계속해서 반복되고, 난수 R가 소수인 것으로 결정된 이후, 난수 R를 생성했던 난수 씨드 S 및 비밀 키 k_S가 저장된다(408). 일 예에 따라, 비밀 키 k_S는 (예컨대, 암호화된 OTP 메모리에) 안전하게 저장되고, 그리고 다른 예에 따라 비밀 키 k_S는 표준 메모리(예컨대, 보통의 RAM(random access memory))에 저장된다.

[0036] [0041] 함수 f를 사용하여 소수 난수 R를 재생성하기 위해, 난수 씨드 S 및 비밀 키 k_S는 추후에 미래 시점에 리트리빙 및 사용될 수 있다. 예컨대, 키 생성 프로세스는 하나 또는 그 초과의 소수들을 요청할 수 있고, 이 하나 또는 그 초과의 소수들은 위에서 설명된 방법(400)을 사용하여 공급될 수 있다. 단지 일 예에 따라, 이로써 생성된 키들은 암호 보안 알고리즘, 예컨대, RSA에 의해 사용될 수 있다.

[0037] [0042] 따라서, 도 4에 예시된 방법에 따라, 소수인 난수 R가 생성될 수 있고, 이어서, 이 소수인 난수 R는 암호 보안 알고리즘, 예컨대, RSA에 대한 암호 보안 키를 생성하는데 사용된다. 도 4에 예시된 방법은, 키 생성 프로세스로부터 소수에 대한 요청을 수신하기 이전에, 소수 난수 R를 생성하는 것으로 알려진 난수 씨드 S 및 비밀 키 k_S가 생성 및 저장된다는 점에서, "오프라인"으로 수행될 수 있다.

[0038] [0043] 도 5는 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도(500)를 예시한다. 먼저, k-비트 난수 씨드 S가 프로세싱 회로(502)(예컨대, 프로세서)에서 생성된다(508). (일 양상에 따라, 프로세싱 회로(502)에 의해 수행되는 단계들이 소프트웨어로 구현될 수 있음을 주목하라.) 이후, 비밀 키 k_S가 생성되거나 또는 메모리 회로(504)(예컨대, 메모리)의 보안 메모리로부터 리트리빙되고(509), 그리고 (예컨대, 도 4에 대해 위에서 설명된 함수 f를 사용하여) 씨드 S 및 비밀 키 k_S에 기초하여 n-비트 난수 R가 생성된다(510). 다음 차례로, 생성된 난수 R가 소수인지의 여부가 결정된다(512). 적어도 하나의 난수 R가 소수인 것으로 결정될 때까지, 단계들(508, 509, 510, 512)이 반복된다(514). 이후, 일단 난수 R가 소수인 것으로 결정되면, 소수 난수 R를 생성하는데 사용된 씨드 S가 메모리 회로(예컨대, RAM과 같은 표준 메모리)에 저장된다(516). 소수 난수 R는 이 지점에서 폐기 또는 삭제될 수 있는데, 그 이유는 씨드 S가 저장되었기 때문이다. 다음 차례로, 암호 키 생성 함수/프로세스를 구현하는 애플리케이션(506)으로부터 하나 또는 그 초과의 소수들

에 대한 요청이 수신된다(518). 이 요청에 응답하여, 씨드 S 및 비밀 키 k_S가 메모리로부터 리트리빙되고(520)(예컨대, 씨드 S는 표준 메모리, 예컨대, RAM으로부터 리트리빙되고, 그리고 비밀 키 k_S는 보안 메모리로부터 리트리빙됨), 그리고 씨드 S 및 비밀 키 k_S를 사용하여 n-비트 소수 난수 R가 재생성된다(522). 마지막으로, 소수 난수 R는, 키 생성을 위한 소수(들)를 요청하는 애플리케이션에 송신/제공된다(524).

[0039] [0044] 도 6은 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름 차트(600)를 예시한다. 먼저, 생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고(604), 이 씨드 S 및 비밀 키 k_S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고(606) -k는 n 미만임-, 그리고 난수 R가 소수인지의 여부를 결정함으로써(608), 소수 난수가 생성된다(602). 다음 차례로, 소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S 및 비밀 키 k_S가 저장된다(610). 난수 씨드 S가 표준 메모리, 예컨대, RAM에 저장될 수 있는 반면에, 비밀 키 k_S는 보안 메모리, 예컨대, OTP 메모리에 저장될 수 있다.

[0040] [0045] 도 7a 및 도 7b는 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도(700)를 예시한다. 도 7a를 참조하면, 먼저, k-비트 난수 씨드 S 및 복수의 g-비트 보충 씨드들 T_i이 생성되고(702), 여기서 정수 $i = \{1, 2, \ldots m\}$이고, 그리고 $m > 1$이다. 난수 씨드 S 및 복수의 보충 씨드들 T_i은 예컨대, 난수 발생기 또는 의사 난수 발생기를 사용하여 생성될 수 있다. 값 k는 2와 동일하거나 또는 그 초과의 임의의 정수일 수 있고, 그리고 값 g는 1과 동일하거나 또는 그 초과의 임의의 정수일 수 있다. 일 양상에 따라, g-비트 보충 씨드들 T_i 각각은 k-비트 난수 씨드 S보다 더 적은 수의 비트들을 갖는다(즉, $g < k$이다).

[0041] [0046] 다음 차례로, 난수 씨드 S 및 복수의 보충 씨드들 T_i에 기초하여 복수의 제2 씨드들 S_i이 생성된다. 예컨대, 난수 씨드 S를 복수의 보충 씨드들 T_i 각각과 연관시킴으로써, 복수의 제2 씨드들 S_i이 생성될 수 있다(704). 제2 씨드들 S_i의 생성이 복수의 보충 씨드들 T_i과 난수 씨드 S의 연관으로 제한되지 않음을 주목하라. 난수 씨드 S 및 복수의 보충 씨드들 T_i에 기초하여 제2 씨드들 S_i을 생성하기 위해 임의의 논리 동작(들)이 수행될 수 있다.

[0042] [0047] 이후, 제2 씨드들 S_i에 기초하여 복수의 n-비트 난수들 R_i이 생성되고(706), 여기서 $n > k + g$이다. 일 양상에 따라, 방정식 (3)에 따라 제2 씨드들 S_i에 기초하여 난수들 R_i을 생성하기 위해 일방향 함수 f가 실행될 수 있다:

[0043] $R_i = f(S_i)$ 정수 값들 $i \geq 1$의 경우 (3).

[0044] [0048] 다른 양상에 따라, 방정식 (4)에 따라 제2 씨드들 S_i 및 비밀 키 k_S(708)에 기초하여 난수들 R_i을 생성하기 위해 일방향 함수 f가 실행될 수 있다:

[0045] $R_i = f(S_i, k_S)$ 정수 값들 $i \geq 1$의 경우 (4).

[0046] 일 예에서, 비밀 키 k_S는 방법(700)을 수행하는 장치에만 알려질 수 있다. 일 양상에 따라, 비밀 키 k_S는 방법(700)을 수행하는 장치에서 보안 메모리(예컨대, 판독 전용 메모리, 암호화될 수 있거나 또는 암호화되지 않을 수 있는 OTP(one-time programmable) 메모리)로부터 리트리빙될 수 있다.

[0047] [0049] 다음 차례로, 난수들 중 임의의 난수가 소수인지의 여부를 결정하기 위해 난수들 R_i 각각에 대해 소수 테스트가 수행된다(710). 난수들 R_i 중 임의의 난수가 소수인 것으로 결정되면, 소수인 것으로 결정된 하나 또는 그 초과의 난수들 R_i을 생성하는데 사용된 난수 씨드 S 및 하나 또는 그 초과의 보충 씨드들 T_i이 메모리에 저장된다(712). 선택적으로, 일방향 함수 f에 의해 비밀 키 k_S가 사용되었다면, 비밀 키 k_S가 보안 메모리에 저장된다(714). 난수들 R_i 중 아무 것도 소수가 아니라면, 적어도 하나의 난수 R_i가 소수인 것으로 결정될 때까지, 단계들(702, 704, 706, 710)이 반복된다.

[0048] [0050] 도 7b를 참조하면, 적어도 하나의 난수 R_i가 소수인 것으로 결정되지만, 난수들 R_i 전부가 소수인 것은 아닌 것으로 결정된 이후, R_i가 소수가 아닌 것으로 결정되었던 모든 i에 대해, 하나 또는 그 초과의 g-비트 보

충 씨드들 T_i이 재생성된다(716). 다음 차례로, R_i가 소수가 아닌 것으로 결정되었던 모든 i에 대해, 난수 씨드 S 및 재생성된 보충 씨드들 T_i에 기초하여 하나 또는 그 초과의 제2 씨드들 S_i이 재생성된다(718). 예컨대, 씨드 S를 보충 씨드들 T_i과 연관시킴으로써, 제2 씨드들 S_i이 생성될 수 있다. 이후, R_i가 소수가 아닌 것으로 결정되었던 모든 i에 대해, 일방향 함수 f를 사용하여 제2 씨드들 S_i에 기초하여 하나 또는 그 초과의 난수들 R_i이 재생성된다(720). 일 예에 따라, 일방향 함수 f는 입력으로서 비밀 키 k_S를 수신할 수 있다(예컨대, 단계(708) 참조).

[0049] [0051] 다음 차례로, 재생성된 난수들 R_i에 대해 소수 테스트가 수행된다(722). 제공된 난수 R_i가 소수인 것으로 결정되면, 난수 R_i를 재생성하는데 부분적으로 사용되었던, 이 난수 R_i에 대응하는 보충 씨드 T_i가 저장된다(724). 그렇지 않으면, 난수 R_i가 소수가 아닌 것으로 결정되면, 재생성되는 난수들 R_i 전부가 소수일 때까지, 프로세스 단계들(716, 718, 720, 및 722)이 반복되고, 그리고 이에 따라, 그러한 난수들 R_i을 생성하는데 사용된 대응하는 보충 씨드들 T_i이 또한 저장된다(724). 일 양상에 따라, 임계치 수의 반복들 이후에, 난수 씨드 S를 포함하는 수 공간(number space)에서 어떠한 소수들도 남지 않았을 경우, 단계들(716, 718, 720, 722)이 반복적으로 수행되는 것이 중지될 수 있다.

[0050] [0052] 도 7a 및 도 7b에 도시된 방법(700)을 더욱 잘 예시하기 위한 예가 하기에서 제공된다. 먼저, 제공된 키 생성 프로세스에 의해 스무 개의 소수들이 원해짐을 가정하라. 이후, 단일의 k-비트 랜덤 씨드 S 및 스무 개의 g-비트 랜덤 보충 씨드들 T_1, T_2, ... T_{20}이 생성된다(702). 다음 차례로, 보충 씨드들 T_1, T_2, ... T_{20}에 기초하여 스무 개의 제2 씨드들 S_1, S_2, ... S_{20}이 생성되고(704), 그리고 이어서, 함수 f를 사용하여 제2 씨드들 S_1, S_2, ... S_{20}에 기초하여 스무 개의 난수들 R_1, R_2, ... R_{20}이 생성된다(706). 이후, 난수들 R_2, R_7, 및 R_{17}이 소수인 것으로 결정되고 그리고 나머지 난수들 R_1, R_3 ... R_6, R_8 ... R_{16}, R_{18}, R_{19}, R_{20}이 소수가 아닌 것으로 결정됨을 가정하라(710). 결과적으로, 난수 씨드 S 및 보충 씨드들 T_2, T_7, 및 T_{17}이 메모리(예컨대, 표준 메모리 RAM)에 저장된다(712).

[0051] [0053] 다음 차례로, 난수들 R_1, R_3 ... R_6, R_8 ... R_{16}, R_{18}, R_{19}, R_{20}이 소수가 아닌 것으로 결정되었기 때문에, 보충 씨드들 T_1, T_3 ... T_6, T_8 ... T_{16}, T_{18}, T_{19}, T_{20}이 재생성된다(예컨대, 랜덤한 새로운 값들)(716). 이후, 새롭게 재생성된 보충 씨드들 T_1, T_3 ... T_6, T_8 ... T_{16}, T_{18}, T_{19}, T_{20}에 기초하여 새로운 제2 씨드들 S_1, S_3 ... S_6, S_8 ... S_{16}, S_{18}, S_{19}, S_{20}이 재생성되고(718), 그리고 이어서, 새롭게 재생성된 제2 씨드들 S_1, S_3 ... S_6, S_8 ... S_{16}, S_{18}, S_{19}, S_{20}에 기초하여 새로운 난수들 R_1, R_3 ... R_6, R_8 ... R_{16}, R_{18}, R_{19}, R_{20}이 재생성된다(720). 다음 차례로, 새롭게 재생성된 난수들 R_1, R_3 ... R_6, R_8 ... R_{16}, R_{18}, R_{19}, R_{20}에 대해, 이들이 소수인지를 결정하기 위해, 소수 테스트가 다시 실행된다(722). 이번에는, 난수들 R_1, R_6, R_{16}, 및 R_{18}이 이제 소수임이 결정되고, 그리고 이에 따라 대응하는 보충 씨드들 T_1, T_6, T_{16}, 및 T_{18}이 메모리에 저장됨(724)을 가정하라. 이후, 스무 개의 난수들 R_1, R_2, ... R_{20} 전부가 소수인 것으로 결정될 때까지, 여전히 소수가 아닌 나머지 난수들에 대해, 단계들(716, 718, 720, 722)이 다시 반복된다.

[0052] [0054] 난수 씨드 S의 비트들의 수(k) 더하기 보충 씨드(들) T_i의 비트들의 수(g)가 소수 난수(들) R_i의 비트들의 수(n) 미만이기 때문에, 난수(들) R_i 대신에 씨드 S 및 보충 씨드(들) T_i를 저장함으로써 메모리 공간이 절약되고, 이 난수(들) R_i는 폐기/삭제될 수 있다. 추후에, 일방향 함수 f를 사용하여 소수 난수(들) R_i를 재생성하기 위해 난수 씨드 S 및 보충 씨드(들) T_i가 메모리로부터 리트리빙되어 사용될 수 있다. 소수 난수(들) R_i를 생성하기 위해 함수 f에 의해 비밀 키 k_S가 또한 사용되었던 경우들에서, 함수 f를 사용하여 소수 난수 R_i를 재생성하기 위해 (보충 씨드들 T_i 및 난수 씨드 S에 부가하여) 비밀 키 k_S가 또한 보안 메모리로부터 리트리빙되어 사용된다.

[0053] [0055] 따라서, 도 7a 및 도 7b에 예시된 방법에 따라, 복수의 소수인 난수들 R_i이 생성될 수 있고, 이후, 복수의 암호 보안 키들을 생성하기 위해, 암호 보안 알고리즘, 예컨대, RSA에 대해 사용될 수 있다. 도 7a 및 도

7b에 예시된 방법은, 키 생성 함수로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 난수 씨드 S 및 복수의 보충 씨드들 T_i -소수 난수들 R_i을 생성하는 것으로 알려짐/증명됨- 이 생성 및 저장된다는 점에서, "오프라인"으로 수행될 수 있다.

[0054] [0056] 도 8a 및 도 8b는 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름도(800)를 예시한다. 도 8a를 참조하면, 먼저, k-비트 난수 씨드 S 및 복수의 g-비트 보충 씨드들 T_i이 프로세싱 회로(802)(예컨대, 프로세서)에서 생성되고(808), 여기서 정수 i = {1, 2, ... m}이고, 그리고 m > 1이다. (일 양상에 따라, 프로세싱 회로(802)에 의해 수행되는 단계들이 소프트웨어로 구현될 수 있음을 주목하라.) 이후, 복수의 (k+g)-비트 제2 씨드들 S_i이 씨드 S 및 복수의 보충 씨드들 T_i에 기초하여(예컨대, 복수의 보충 씨드들 T_i과 씨드 S를 연관시킴) 생성된다(810). 다음 차례로, (예컨대, 도 7a 및 도 7b에 대해 위에서 설명된 일방향 함수 f를 사용하여) 제2 씨드들 S_i에 기초하여 복수의 n-비트 난수들 R_i이 생성되고(812), 여기서 n > g + k이다. 이후, 생성된 난수들 R_i 중 임의의 난수가 소수인지의 여부가 결정된다(814). 적어도 하나의 난수 R_i가 소수인 것으로 결정될 때까지, 단계들(808, 810, 812, 814)이 반복된다. 적어도 하나 또는 그 초과의 난수들 R_i이 소수인 것으로 결정됨을 가정하면, 소수 난수(들) R_i를 생성하는데 사용된 씨드 S 및 보충 씨드(들) T_i가 메모리 회로(804)(예컨대, 메모리)에 저장된다(816).

[0055] [0057] 다음 차례로, 소수가 아닌 것으로 결정되었던 그러한 난수들 R_i과 연관된 보충 씨드들 T_i이 재생성된다(818). 이후, 재생성된 보충 씨드들 T_i에 기초하여 새로운 제2 씨드들 S_i이 재생성되고(820), 그리고 이어서, 재생성된 제2 씨드들 S_i에 기초하여 새로운 난수들 R_i이 재생성된다(822). 다음 차례로, 재생성된 난수들 R_i에 대해 이들이 소수인지를 결정하기 위해 소수 테스트들이 실행된다(824). 소수인 것으로 결정된 난수들 R_i과 연관된 보충 씨드들 T_i이 메모리 회로(804)에 저장된다(826). 도 8b를 참조하면, 재생성된 난수들 R_i 전부가 소수인 것으로 결정될 때까지, 프로세스 단계들(818, 820, 822, 824, 826)이 반복되고(828), 그리고 이에 따라, 그들과 연관된 보충 씨드들 T_i이 또한 메모리 회로(804)에 저장된다. 소수인 것으로 결정된 난수들 R_i이 이 지점에서 폐기 또는 삭제될 수 있는데, 그 이유는 씨드들 S 및 연관된 보충 씨드들 T_i이 저장되었고 그리고 소수들 R_i을 재생성하는데 사용될 수 있기 때문이다.

[0056] [0058] 다음 차례로, 암호 키 생성 함수를 구현하는 애플리케이션(806)으로부터 하나 또는 그 초과의 소수들에 대한 요청이 수신된다(830). 이 요청에 응답하여, 씨드 S 및 보충 씨드들 T_i이 메모리(804)로부터 리트리빙되고(832), 그리고 씨드 S 및 보충 씨드들 T_i을 사용하여 n-비트 소수 난수들 R_i이 재생성된다(834). 제2 씨드들 S_i에 기초하여 난수들 R_i을 생성했던 일방향 함수 f에 의해 비밀 키 k_S가 사용되었다면, 소수 난수들 R_i을 재생성하기 위하여, 메모리(예컨대, 보안 메모리)로부터 비밀 키 k_S가 또한 리트리빙된다. 마지막으로, 소수 난수들 R_i은 키 생성을 위한 소수(들)를 요청하는 애플리케이션(806)에 송신/제공된다(836).

[0057] [0059] 도 9는 일 양상에 따라 소수 생성을 위한 씨드 값들을 생성 및 저장하기 위한 방법의 흐름 차트(900)를 예시한다. 먼저, k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 T_i이 생성된다(902). 다음 차례로, 각각이 복수의 보충 씨드들 T_i 중 상이한 보충 씨드 및 난수 씨드 S에 기초하는 복수의 제2 씨드들 S_i이 생성된다(904). 이후, 각각이 n개 비트들을 갖는 복수의 난수들 R_i -n은 k + g 미만임- 이 생성되고, 그리고 복수의 난수들 R_i 각각은 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초한다(906). 다음 차례로, 복수의 난수들 R_i 중 적어도 하나의 난수 R_P가 소수임이 결정되고, 여기서 난수 R_P는 복수의 제2 씨드들 S_i 중 제2 씨드 S_P에 기초하고, 제2 씨드 S_P는 복수의 보충 씨드들 T_i 중 보충 씨드 T_P 및 난수 씨드 S에 기초한다(908). 이후, 난수 씨드 S 및 보충 씨드 T_P는 메모리 회로에 저장된다(910).

[0058] [0060] 본 개시물의 일 양상에 따라, 저장된 난수 씨드 S 및 보충 씨드 T_P는 메모리 회로로부터 리트리빙될 수 있고, 그리고 소수 난수 R_P는 난수 씨드 S 및 보충 씨드 T_P에 기초하여 재생성될 수 있다. 다른 양상에 따라, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신하기 이전에, 난수 씨드 S 및 보충 씨드 T_P가 저장될 수 있다. 이후, 암호 키 생성 프로세스로부터 하나 또는 그 초과의 소수들에 대한 요청이

수신될 수 있다. 응답하여, 암호 키가 소수 난수 R_P에 기초하여 생성될 수 있다. 이후, 암호 키가 암호 키 생성 프로세스에 제공될 수 있다.

[0059] [0061] 일 양상에 따라, 복수의 제2 씨드들 S_i 중 상이한 제2 씨드들에 기초하여 복수의 난수들 R_i을 생성하는 단계는, 입력들로서 복수의 제2 씨드들 S_i 각각을 수신하고 출력들로서 복수의 난수들 R_i을 생성하는 일방향 함수 f를 실행하는 단계를 포함할 수 있고, 일방향 함수 f는 보안 해시 함수 및/또는 블록 암호 중 적어도 하나이다. 다른 양상에 따라, 복수의 난수들 R_i 중 적어도 하나의 난수가 소수가 아님이 결정될 수 있다. 이후, g개 비트들을 갖는 다른 보충 씨드 T_2가 생성될 수 있고, 보충 씨드 T_2 및 난수 씨드 S에 기초하여 다른 제2 씨드 S_2가 생성될 수 있으며, 그리고 n개 비트들을 갖는 다른 난수 R_2가 제2 씨드 S_2에 기초하여 생성될 수 있다. 다음 차례로, 난수 R_2가 소수임이 결정될 수 있고, 결과적으로, 보충 씨드 T_2는 메모리 회로에 저장될 수 있다.

[0060] [0062] 일 양상에 따라, 저장된 난수 씨드 S 및 보충 씨드 T_2는 메모리 회로로부터 리트리빙될 수 있고, 그리고 소수 난수 R_2는 난수 씨드 S 및 보충 씨드 T_2에 기초하여 재생성될 수 있다. 다른 양상에 따라, 미리결정된 수의 소수들에 대한 요청이 수신될 수 있다. 응답하여, 각각이 상이한 소수들과 연관되는 다수의 보충 씨드들이 미리결정된 수와 동일한 수로 저장될 때까지, 하기의 단계들은 반복될 수 있다: 다른 보충 씨드 T_2를 생성하는 단계; 보충 씨드 T_2 및 난수 씨드 S에 기초하여 다른 제2 씨드 S_2를 생성하는 단계; 제2 씨드 S_2에 기초하여 n개 비트들을 갖는 다른 난수 R_2를 생성하는 단계; 난수 R_2가 소수임을 결정하는 단계; 및 보충 씨드 T_2를 메모리 회로에 저장하는 단계.

[0061] **예시적 전자 디바이스**

[0062] [0063] 도 10은 본원에 설명된 암호 보안을 위한 방법들 중 임의의 방법을 실행하는 전자 디바이스(1000)에 대한 하드웨어 구현의 예시적이고 개략적인 블록도를 예시한다. 전자 디바이스(1000)는 모바일폰, 스마트폰, 태블릿, 휴대용 컴퓨터, 및/또는 회로를 갖는 임의의 다른 전자 디바이스일 수 있다. 전자 디바이스(1000)는 통신 인터페이스(1010), 사용자 인터페이스(1012), 및 프로세싱 시스템(1014)을 포함할 수 있다. 프로세싱 시스템(1014)은 프로세싱 회로(예컨대, 프로세서)(1004), 메모리 회로(예컨대, 메모리)(1005), 컴퓨터-판독가능 저장 매체(1006), 버스 인터페이스(1008), 및 버스(1002)를 포함할 수 있다. 프로세싱 시스템(1014) 및/또는 프로세싱 회로(1004)는 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 및/또는 도 9에 대해 설명된 단계들, 기능들, 및/또는 프로세스들 중 임의의 것을 수행하도록 구성될 수 있다.

[0063] [0064] 프로세싱 회로(1004)는 전자 디바이스(1000)에 대한 데이터를 프로세싱하도록 적응되는 하나 또는 그 초과의 프로세서들(예컨대, 제1 프로세서 등)일 수 있다. 예컨대, 프로세싱 회로(1004)는 전문화된 프로세서, 예컨대, 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 및/또는 도 9에 대해 설명된 단계들 중 임의의 단계를 수행하기 위한 수단으로서의 역할을 하는 ASIC(application specific integrated circuit)일 수 있다.

[0064] [0065] 프로세싱 회로들(1004)의 예들은 마이크로프로세서들, 마이크로제어기들, DSP(digital signal processor)들, FPGA(field programmable gate array)들, PLD(programmable logic device)들, 상태 머신들, 게이티드 논리(gated logic), 이산 하드웨어 회로들, 및 본 개시물 전체에 걸쳐 설명된 다양한 기능을 수행하도록 구성된 다른 적절한 하드웨어를 포함한다. 프로세싱 회로(1004)는 또한, 버스(1002)를 관리하는 것, 그리고 컴퓨터-판독가능 저장 매체(1006) 및/또는 메모리(1005) 상에 저장된 소프트웨어를 실행하는 것을 담당한다. 소프트웨어는, 프로세싱 회로(1004)에 의해 실행될 때, 프로세싱 시스템(1014)으로 하여금, 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 및/또는 도 9에 대해 위에서 설명된 다양한 기능들, 단계들, 및/또는 프로세스들을 수행하게 한다. 컴퓨터-판독가능 저장 매체(1006)는 소프트웨어를 실행할 때 프로세싱 회로(1004)에 의해 조작되는 데이터를 저장하는데 사용될 수 있다.

[0065] [0066] 메모리 회로(1005)는 비-휘발성 메모리, 예컨대, 이에 제한되지는 않지만, FLASH 메모리, 자기 또는 광학 하드 디스크 드라이브들 등일 수 있다. 일부 양상들에서, 섹터 정보 및/또는 오버헤드 메시지들(구성 시퀀스 번호를 포함함)을 저장하는 메모리는 무기한으로 정보를 저장하기 위하여 계속해서 전력을 공급받을 수 있는 휘발성 메모리, 예컨대, DRAM(예컨대, DDR SDRAM), SRAM 등일 수 있다. 메모리 회로(1005)는 난수 씨드 S를 저장하기 위한 수단, 보충 씨드들 T_i을 저장하기 위한 수단, 및 보안이 이루어질 때 비밀 키 k_S를 저장하기 위한

수단의 일 예로서의 역할을 한다.

[0066] [0067] 소프트웨어는, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 하드웨어 기술어로 지칭되든지 또는 다른 방식으로 지칭되든지 간에, 명령들, 명령 세트들, 코드, 코드 세그먼트들, 프로그램 코드, 프로그램들, 서브프로그램들, 소프트웨어 모듈들, 애플리케이션들, 소프트웨어 애플리케이션들, 소프트웨어 패키지들, 루틴들, 서브루틴들, 오브젝트들, 실행 가능들, 실행 스레드들, 프로시저들, 함수들 등을 의미하도록 폭넓게 해석될 것이다. 소프트웨어는 컴퓨터-판독가능 저장 매체(1006) 상에 상주할 수 있다. 컴퓨터-판독가능 저장 매체(1006)는 비-일시적 컴퓨터-판독가능 저장 매체일 수 있다. 비-일시적 컴퓨터-판독가능 저장 매체는, 예로서, 자기 스토리지 디바이스(예컨대, 하드 디스크, 플로피 디스크, 자기 스트립), 광학 디스크(예컨대, CD(compact disc) 또는 DVD(digital versatile disc)), 스마트 카드, 플래시 메모리 디바이스(예컨대, 카드, 스틱, 또는 키 드라이브), RAM(random access memory), ROM(read only memory), PROM(programmable ROM), EPROM(erasable PROM), EEPROM(electrically erasable PROM), 레지스터, 탈착 가능 디스크, 그리고 컴퓨터에 의해 액세스 및 판독될 수 있는 소프트웨어 및/또는 명령들을 저장하기 위한 임의의 다른 적절한 매체를 포함한다. 컴퓨터-판독가능 저장 매체는 또한, 예로서, 반송파, 송신선, 그리고 컴퓨터에 의해 액세스 및 판독될 수 있는 소프트웨어 및/또는 명령들을 송신하기 위한 임의의 다른 적절한 매체를 포함할 수 있다. 컴퓨터-판독가능 저장 매체(1006)는 프로세싱 시스템(1014)에 상주할 수 있거나, 프로세싱 시스템(1014)의 외부에 있을 수 있거나, 또는 프로세싱 시스템(1014)을 포함하는 다수의 엔티티들에 걸쳐 분산될 수 있다. 컴퓨터-판독가능 저장 매체(1006)는 컴퓨터 프로그램 물건으로 구현될 수 있다.

[0067] [0068] 본 예에서, 프로세싱 시스템(1014)은 버스(1002)로 일반적으로 표현되는 버스 아키텍처를 이용하여 구현될 수 있다. 버스(1002)는 프로세싱 시스템(1014)의 특정 애플리케이션 및 전체 설계 제약들에 따라 임의의 수의 상호연결 버스들 및 브릿지들을 포함할 수 있다. 버스(1002)는 하나 또는 그 초과의 프로세서들(프로세서(1004)로 일반적으로 표현됨), 메모리(1005), 및 컴퓨터-판독가능 미디어(컴퓨터-판독가능 저장 매체(1006)로 일반적으로 표현됨)를 포함하는 다양한 회로들을 서로 연결시킨다. 버스(1002)는 또한, 다양한 다른 회로들, 예컨대, 타이밍 소스들, 주변장치들, 전압 조정기들, 및 전력 관리 회로들을 연결시킬 수 있고, 이들은 기술분야에서 잘 알려져 있고 이에 따라 더 이상 추가로 설명되지 않을 것이다. 버스 인터페이스(1008)는 버스(1002)와 통신 인터페이스(1010)(존재한다면) 사이에 인터페이스를 제공한다. 통신 인터페이스(1010)는 송신 매체를 통해 다른 장치와 통신하기 위한 수단을 제공한다. 장치의 성질에 따라, 사용자 인터페이스(1012)(예컨대, 키패드, 디스플레이, 스피커, 마이크로폰, 터치스크린 디스플레이 등)가 또한 전자 디바이스(1000)에 제공될 수 있다.

[0068] [0069] 도 11은 일 양상에 따라 프로세싱 회로(1004)의 개략적인 블록도를 예시한다. 프로세싱 회로(1004)는 소수 발생기 회로(1102), 난수 씨드 S 리트리버 회로(1103), 소수 재발생기 회로(1105), 및 함수 f 실행 회로(1107)를 포함할 수 있다. 소수 발생기 회로(1102)는 난수 씨드 S 발생기 회로(1104), 난수 R 발생기 회로(1106), 및 소수 테스트 회로(1108)를 포함할 수 있다.

[0069] [0070] 소수 발생기 회로(1102)는, 반복적으로, k개 비트들을 갖는 난수 씨드 S를 생성하고, 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하고, 그리고 난수 R가 소수인지의 여부를 결정함으로써, 소수를 생성하기 위한 수단의 일 예로서의 역할을 한다. 구체적으로, 난수 씨드 S 발생기 회로(1104)는 난수 씨드 S를 생성하기 위한 수단의 일 예로서의 역할을 하고, 난수 R 발생기 회로(1106)는 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성하기 위한 수단의 일 예로서의 역할을 하고, 그리고 소수 테스트 회로(1108)는 난수 R가 소수인지의 여부를 결정하기 위한 수단의 일 예로서의 역할을 한다.

[0070] [0071] 난수 씨드 S 리트리버 회로(1103)는 메모리 회로(1005)로부터 난수 씨드 S를 리트리빙하기 위한 수단의 일 예로서의 역할을 한다. 소수 재발생기 회로(1105)는 난수 씨드 S에 기초하여 소수를 재생성하기 위한 수단의 일 예로서의 역할을 한다. 함수 f 실행 회로(1107)는 입력으로서 씨드 S를 수신하고 출력으로서 난수 R를 생성하는 일방향 함수 f를 실행하기 위한 수단의 일 예로서의 역할을 한다.

[0071] [0072] 도 12는 일 양상에 따라 프로세싱 회로(1004)의 개략적인 블록도를 예시한다. 프로세싱 회로(1004)는 씨드 S 및 보충 씨드 T_i 발생기 회로(1202), 제2 씨드 S_i 발생기 회로(1204), 난수 R_i 발생기 회로(1206), 소수 테스트 회로(1208), 씨드 리트리벌 회로(1210), 및 소수 난수 재발생기 회로(1212)를 포함할 수 있다.

[0072] [0073] 씨드 S 및 보충 씨드 T_i 발생기 회로(1202)는 난수 씨드 S 및 보충 씨드들 T_i을 생성하기 위한 수단의 일 예로서의 역할을 한다. 제2 씨드 S_i 발생기 회로(1204)는 각각이 복수의 보충 씨드들 T_i 중 상이한 보충 씨

드 및 난수 씨드 S에 기초하는 제2 씨드들 S_i을 생성하기 위한 수단의 일 예로서의 역할을 한다. 난수 R_i 발생기 회로(1206)는 각각이 n개 비트들을 갖는 복수의 난수들 R_i을 생성하기 위한 수단의 일 예로서의 역할을 하고, 이 난수들 R_i은 각각이 복수의 제2 씨드들 S_i 중 상이한 제2 씨드에 기초한다. 소수 테스트 회로(1208)는 난수 R_P가 소수인지의 여부를 결정하기 위한 수단의 일 예로서의 역할을 한다. 씨드 리트리벌 회로(1210)는 난수 씨드 S 및 복수의 보충 씨드들 T_i(예컨대, 씨드 T_P)을 리트리빙하기 위한 수단의 일 예로서의 역할을 한다. 소수 난수 재발생기 회로(1212)는 난수 씨드 S 및 보충 씨드들 T_i(예컨대, 보충 씨드 T_P)에 기초하여 소수 난수(예컨대, 소수 난수 R_P)를 재생성하기 위한 수단의 일 예로서의 역할을 한다.

[0073] [0074] 본원에 설명된 방법들 및 디바이스들은, 암호 보안 및/또는 암호 키 생성으로 제한되지 않는 임의의 사용을 위해, 소수 생성을 위한 씨드 값들을 생성 및 저장하는데 사용될 수 있다.

[0074] [0075] 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 도 9, 도 10, 도 11, 및/또는 도 12에서 예시된 컴포넌트들, 단계들, 특징들, 및/또는 기능들 중 하나 또는 그 초과는 재배열될 수 있고 그리고/또는 단일의 컴포넌트, 단계, 특징 또는 기능으로 결합될 수 있거나 또는 여러 컴포넌트들, 단계들, 또는 기능들로 구현될 수 있다. 또한, 본 발명으로부터 벗어남 없이, 부가의 엘리먼트들, 컴포넌트들, 단계들, 및/또는 기능들이 부가될 수 있다. 도 10, 도 11, 및/또는 도 12에서 예시된 장치, 디바이스들, 및/또는 컴포넌트들은 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 및/또는 도 9에 설명된 방법들, 특징들, 또는 단계들 중 하나 또는 그 초과를 수행하도록 구성될 수 있다. 본원에 설명된 알고리즘들은 또한, 효율적으로 소프트웨어로 구현될 수 있고 그리고/또는 하드웨어에 임베딩될 수 있다.

[0075] [0076] 또한, 본 개시물의 일 양상에서, 도 10, 도 11, 및/또는 도 12에서 예시된 프로세싱 회로(1004)는 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 및/또는 도 9에 설명된 알고리즘들, 방법들, 및/또는 단계들을 수행하도록 특정하게 설계되고 그리고/또는 하드-와이어링된 전문화된 프로세서(예컨대, 애플리케이션 특정 집적 회로(예컨대, ASIC)일 수 있다. 따라서, 이러한 전문화된 프로세서(예컨대, ASIC)는 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 및/또는 도 9에 설명된 알고리즘들, 방법들, 및/또는 단계들을 실행하기 위한 수단의 일 예일 수 있다. 또한, 컴퓨터-판독가능 저장 매체(1006)는 프로세서(1004) 판독가능 명령들을 저장할 수 있고, 이 명령들은, 전문화된 프로세서(예컨대, ASIC)에 의해 실행될 때, 이 전문화된 프로세서로 하여금, 도 1, 도 2, 도 3, 도 4, 도 5, 도 6, 도 7a, 도 7b, 도 8a, 도 8b, 및/또는 도 9에 설명된 알고리즘들, 방법들, 및/또는 단계들을 수행하게 한다.

[0076] [0077] 또한, 본 개시물의 양상들이 흐름차트, 흐름도, 구조도, 또는 블록도로서 묘사되는 프로세스로서 설명될 수 있음이 주목된다. 흐름차트가 순차적 프로세스로서 동작들을 설명할 수 있지만, 동작들 중 많은 동작들이 병렬로 또는 동시에 수행될 수 있다. 부가하여, 동작들의 순서는 재배열될 수 있다. 프로세스는 자신의 동작들이 완료될 때 종료된다. 프로세스는 방법, 함수, 프로시저, 서브루틴, 서브프로그램 등에 대응할 수 있다. 프로세스가 함수에 대응할 때, 프로세스의 종료는 호출 함수 또는 메인 함수로의 함수의 리턴에 대응한다.

[0077] [0078] 또한, 저장 매체는, ROM(read-only memory), RAM(random access memory), 자기 디스크 저장 매체들, 광학 저장 매체들, 플래시 메모리 디바이스들 및/또는 정보를 저장하기 위한 다른 머신-판독가능 매체들 및 프로세서-판독가능 매체들, 및/또는 컴퓨터-판독가능 매체들을 비롯해, 데이터를 저장하기 위한 하나 또는 그 초과의 디바이스들을 표현할 수 있다. 용어들 "머신-판독가능 매체", "컴퓨터-판독가능 매체", 및/또는 "프로세서-판독가능 매체"는, 이에 제한되지는 않지만, 비-일시적 매체들, 예컨대, 휴대용 또는 고정 스토리지 디바이스들, 광학 스토리지 디바이스들, 및 명령(들) 및/또는 데이터를 저장, 포함 또는 운반할 수 있는 다양한 다른 매체들을 포함할 수 있다. 따라서, 본원에 설명된 다양한 방법들은 "머신-판독가능 매체", "컴퓨터-판독가능 매체", 및/또는 "프로세서-판독가능 매체"에 저장될 수 있는 명령들 및/또는 데이터에 의해 완전히 또는 부분적으로 구현될 수 있고, 그리고 하나 또는 그 초과의 프로세서들, 머신들 및/또는 디바이스들에 의해 실행될 수 있다.

[0078] [0079] 또한, 본 개시물의 양상들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 또는 이들의 임의의 결합에 의해 구현될 수 있다. 소프트웨어, 펌웨어, 미들웨어 또는 마이크로코드로 구현될 때, 필요한 태스크들을 수행하는 프로그램 코드 또는 코드 세그먼트들은 머신-판독가능 매체, 예컨대, 저장 매체 또는 다른 스토리지(들)에 저장될 수 있다. 프로세서가 필요한 태스크들을 수행할 수 있다. 코드 세그먼트는 프로시저, 함수, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들, 데이터 구조들,

또는 프로그램문들의 임의의 결합을 표현할 수 있다. 코드 세그먼트는, 정보, 데이터, 인수들, 파라미터들, 또는 메모리 콘텐츠들을 전달 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수 있다. 정보, 인수들, 파라미터들, 데이터 등은, 메모리 공유, 메시지 전달, 토큰 전달, 네트워크 송신 등을 비롯한 임의의 적절한 수단을 통해 전달, 포워딩, 또는 송신될 수 있다.

[0079] [0080] 본원에 개시된 예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 엘리먼트들, 및/또는 컴포넌트들은 범용 프로세서, DSP(digital signal processor), ASIC(application specific integrated circuit), FPGA(field programmable gate array) 또는 다른 프로그래밍 가능한 논리 컴포넌트, 이산 게이트 또는 트랜지스터 논리, 이산 하드웨어 컴포넌트들, 또는 본원에 설명된 기능들을 수행하도록 설계된, 이들의 임의의 결합을 이용하여 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 통상적인 프로세서, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 또한, 프로세서는 컴퓨팅 컴포넌트들의 결합, 예컨대, DSP 및 마이크로프로세서의 결합, 다수의 마이크로프로세서들, DSP 코어와 공조된 하나 또는 그 초과의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

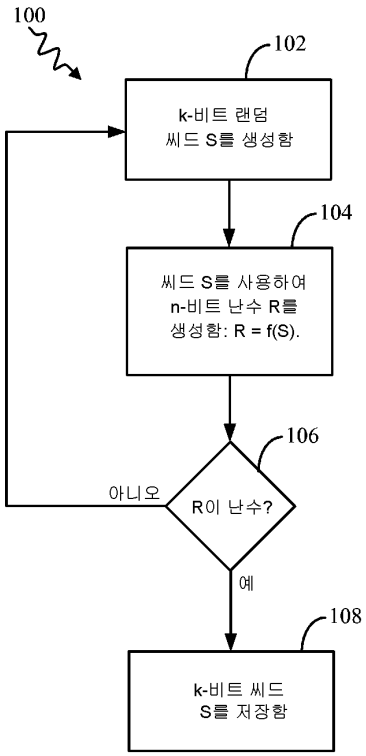
[0080] [0081] 본원에 개시된 예들과 관련하여 설명된 방법들 또는 알고리즘들은 직접적으로 하드웨어로, 프로세서에 의해 실행 가능한 소프트웨어 모듈로, 또는 프로세싱 유닛, 프로그래밍 명령들, 또는 다른 디렉션들의 형태의 양쪽의 결합으로 구현될 수 있고, 그리고 단일의 디바이스에 포함될 수 있거나 또는 다수의 디바이스들에 걸쳐 분산될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 탈착 가능 디스크, CD-ROM, 또는 기술분야에서 알려진 임의의 다른 형태의 저장 매체에 상주할 수 있다. 저장 매체가 프로세서에 커플링될 수 있어, 프로세서는 저장 매체로부터 정보를 판독할 수 있고 저장 매체에 정보를 기록할 수 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다.

[0081] [0082] 당업자들은 추가로, 본원에 개시된 양상들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양쪽의 결합들로서 구현될 수 있음을 인식할 것이다. 하드웨어와 소프트웨어의 이러한 상호 교환 가능성을 명확하게 예시하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들은 위에서 일반적으로 그들의 기능 면에서 설명되었다. 이러한 기능이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지는 특정 애플리케이션, 및 전체 시스템에 부과되는 설계 제약들에 따라 좌우된다.

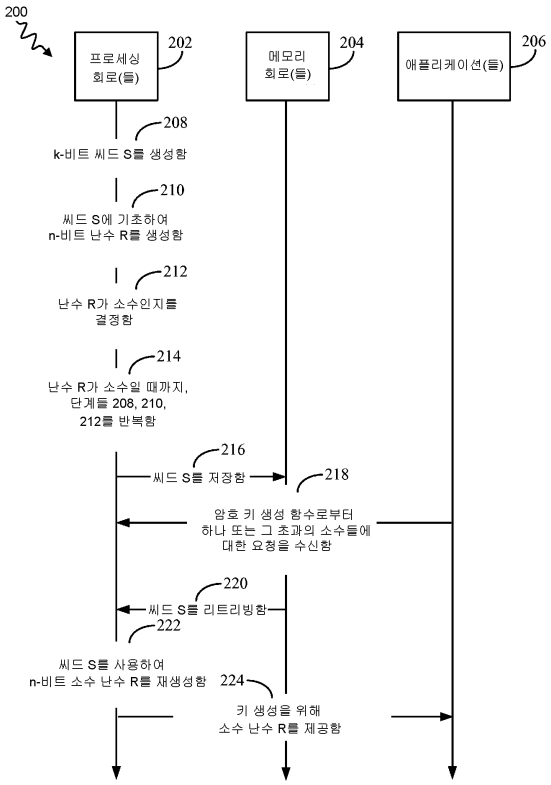
[0082] [0083] 본 발명으로부터 벗어남 없이, 본원에 설명된 본 발명의 다양한 특징들이 상이한 시스템들에서 구현될 수 있다. 본 개시물의 전술된 양상들이 단지 예들이고, 그리고 본 발명을 제한하는 것으로서 이해되지 않아야 함이 주목되어야 한다. 본 개시물의 양상들의 설명은 예시적인 것으로 의도되고, 그리고 청구항들의 범위를 제한하는 것으로 의도되지 않는다. 이와 같이, 본 교시들은 다른 타입들의 장치들에 쉽게 적용될 수 있고, 그리고 많은 대안들, 수정들, 및 변형들이 당업자에게 명백할 것이다.

도면

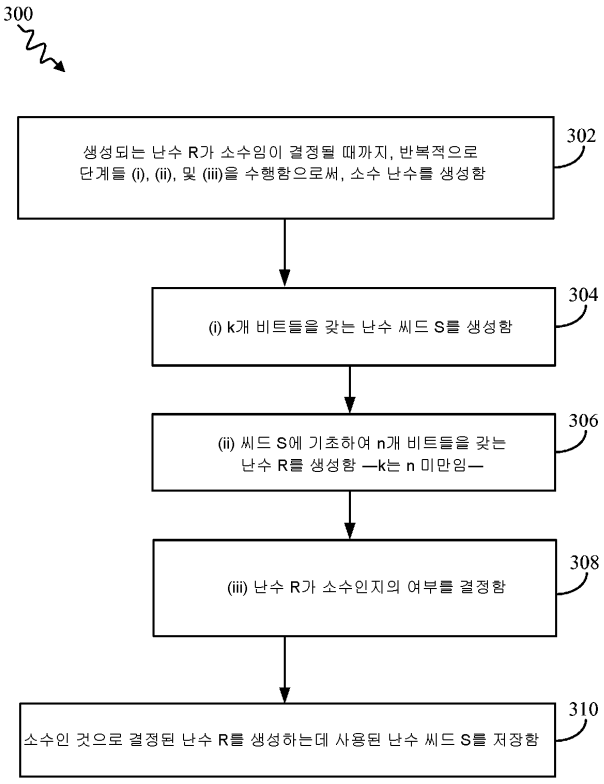
도면1


100
102
k-비트 랜덤
씨드 S를 생성함
104
씨드 S를 사용하여
n-비트 난수 R를
생성함: R = f(S).
106
R이 난수?
아니오
예
108
k-비트 씨드
S를 저장함

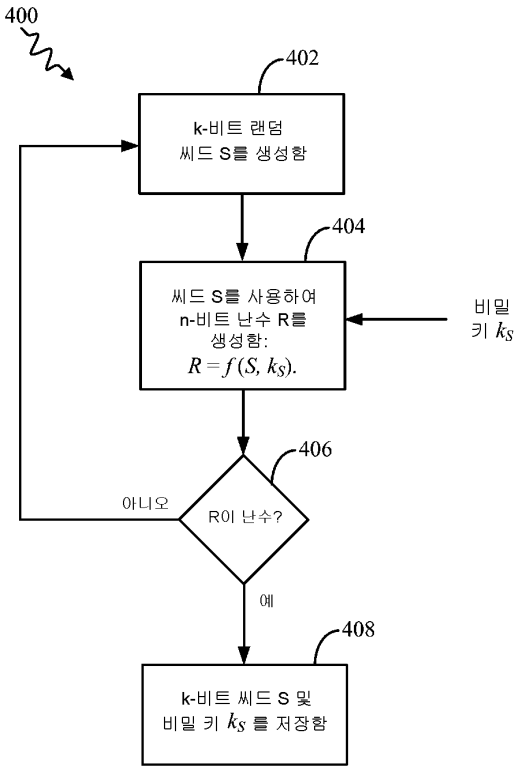
도면2


200
프로세싱 회로(들)
202
메모리 회로(들)
204
애플리케이션(들)
206
208
k-비트 씨드 S를 생성함
210
씨드 S에 기초하여 n-비트 난수 R를 생성함
212
난수 R가 소수인지를 결정함
214
난수 R가 소수일 때까지, 단계들 208, 210, 212를 반복함
216
씨드 S를 저장함
218
암호 키 생성 함수로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신함
220
씨드 S를 리트리빙함
222
씨드 S를 사용하여 n-비트 소수 난수 R를 재생성함
224
키 생성을 위해 소수 난수 R를 제공함

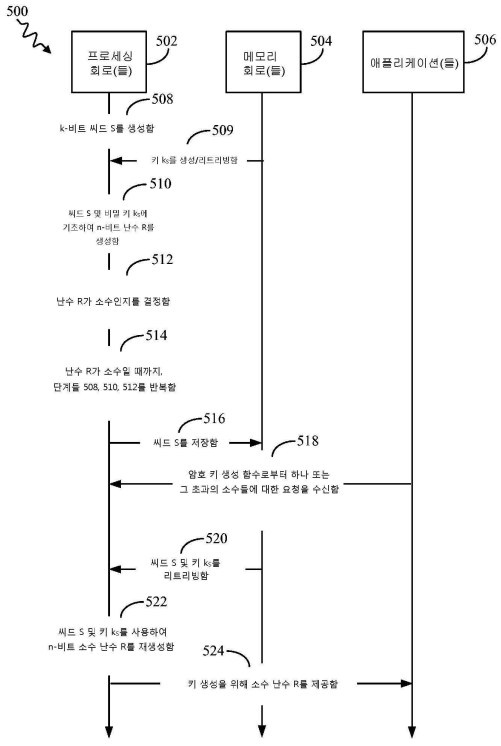
도면3


300
생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로 단계들 (i), (ii), 및 (iii)을 수행함으로써, 소수 난수를 생성함
302
(i) k개 비트들을 갖는 난수 씨드 S를 생성함
304
(ii) 씨드 S에 기초하여 n개 비트들을 갖는 난수 R를 생성함 —k는 n 미만임—
306
(iii) 난수 R가 소수인지의 여부를 결정함
308
소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S를 저장함
310

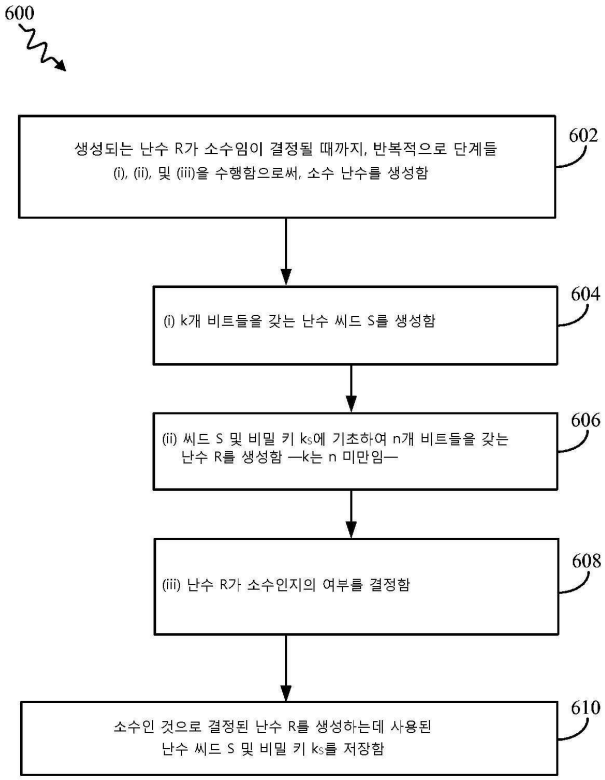
도면4


400
402
k-비트 랜덤
씨드 S를 생성함
404
씨드 S를 사용하여
n-비트 난수 R를
생성함:
$R = f(S, k_S)$.
비밀
키 k_S
406
아니오
R이 난수?
예
408
k-비트 씨드 S 및
비밀 키 k_S 를 저장함

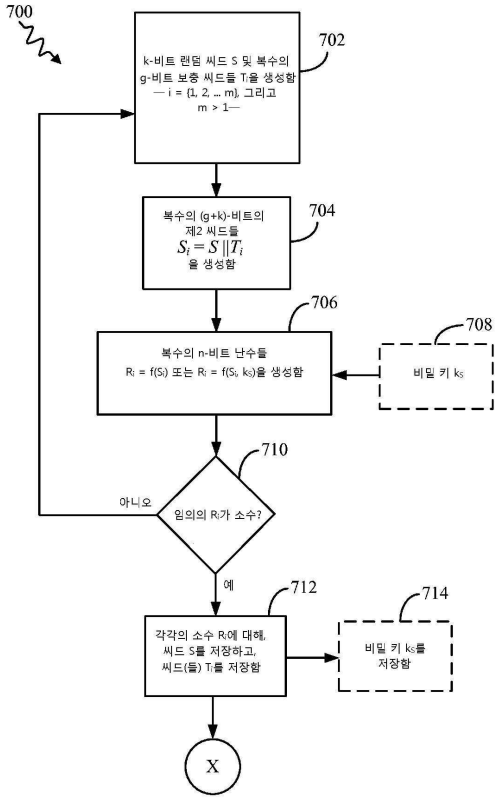
도면5


500
프로세싱
회로(들)
502
메모리
회로(들)
504
애플리케이션(들)
506
508
k-비트 씨드 S를 생성함
509
키 k_S를 생성/리트리빙함
510
씨드 S 및 비밀 키 k_S에
기초하여 n-비트 난수 R를
생성함
512
난수 R가 소수인지를 결정함
514
난수 R가 소수일 때까지,
단계들 508, 510, 512를 반복함
516
씨드 S를 저장함
518
암호 키 생성 함수로부터 하나 또는
그 초과의 소수들에 대한 요청을 수신함
520
씨드 S 및 키 k_S를
리트리빙함
522
씨드 S 및 키 k_S를 사용하여
n-비트 소수 난수 R를 재생성함
524
키 생성을 위해 소수 난수 R를 제공함

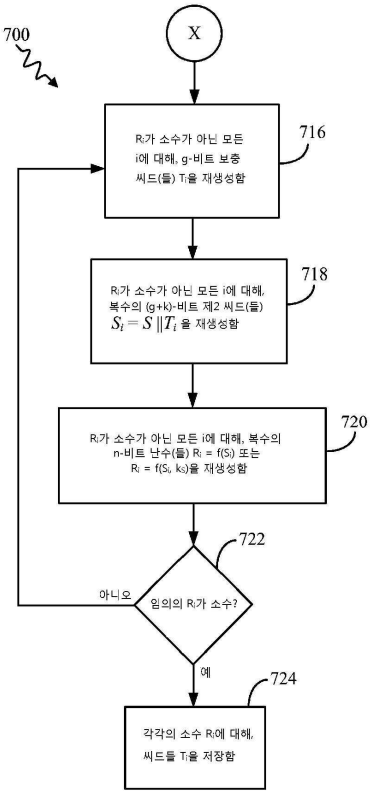
도면6


600
생성되는 난수 R가 소수임이 결정될 때까지, 반복적으로 단계들 (i), (ii), 및 (iii)을 수행함으로써, 소수 난수를 생성함
602
(i) k개 비트들을 갖는 난수 씨드 S를 생성함
604
(ii) 씨드 S 및 비밀 키 kS에 기초하여 n개 비트들을 갖는 난수 R를 생성함 —k는 n 미만임—
606
(iii) 난수 R가 소수인지의 여부를 결정함
608
소수인 것으로 결정된 난수 R를 생성하는데 사용된 난수 씨드 S 및 비밀 키 kS를 저장함
610

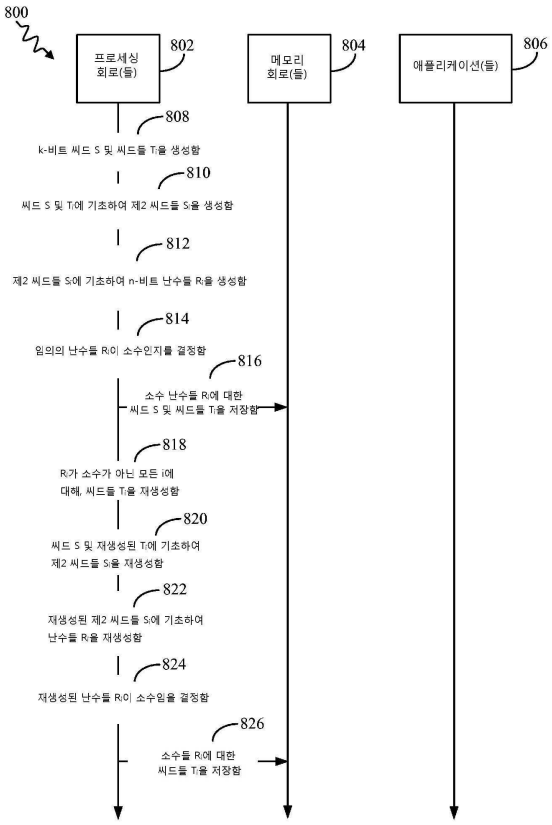
도면7a


700
k-비트 랜덤 씨드 S 및 복수의 g-비트 보충 씨드들 Ti을 생성함 — i = {1, 2, .. m}, 그리고 m > 1—
702
복수의 (g+k)-비트의 제2 씨드들 $S_i = S \| T_i$ 을 생성함
704
복수의 n-비트 난수들 Ri = f(Si) 또는 Ri = f(Si, kS)을 생성함
706
비밀 키 kS
708
임의의 Ri가 소수?
710
아니오
예
각각의 소수 Ri에 대해, 씨드 S를 저장하고, 씨드(들) Ti를 저장함
712
비밀 키 kS를 저장함
714
X

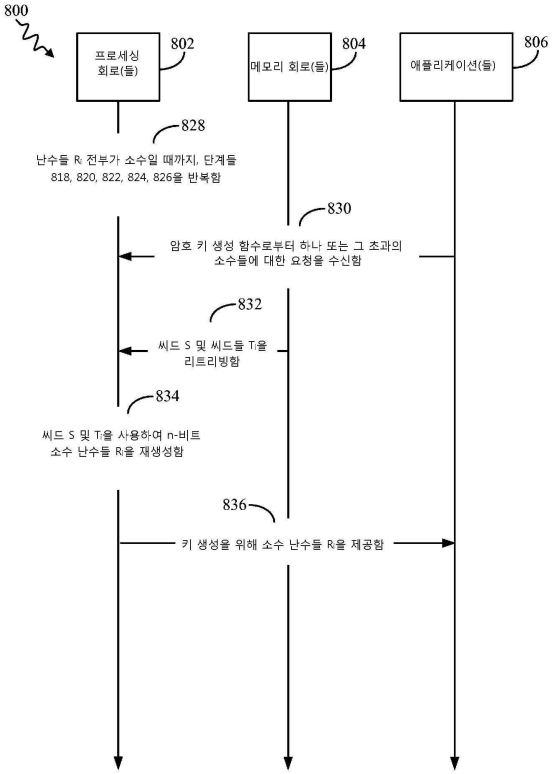
도면7b


700
X
716
Ri가 소수가 아닌 모든 i에 대해, g-비트 보충 씨드(들) Ti을 재생성함
718
Ri가 소수가 아닌 모든 i에 대해, 복수의 (g+k)-비트 제2 씨드(들) $S_i = S \| T_i$ 을 재생성함
720
Ri가 소수가 아닌 모든 i에 대해, 복수의 n-비트 난수(들) Ri = f(Si) 또는 Ri = f(Si, ki)을 재생성함
722
아니오
임의의 Ri가 소수?
예
724
각각의 소수 Ri에 대해, 씨드들 Ti을 저장함

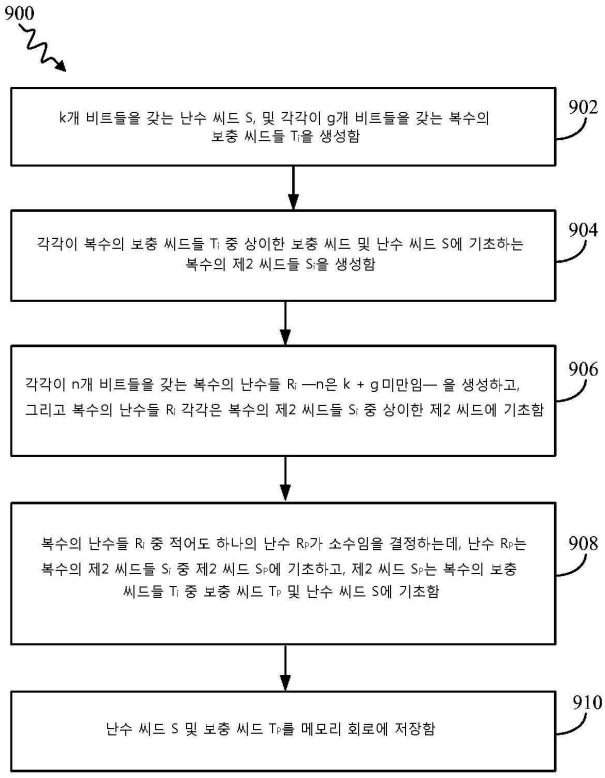
도면8a


800
프로세싱 회로(들)
802
메모리 회로(들)
804
애플리케이션(들)
806
808
k-비트 씨드 S 및 씨드들 Ti을 생성함
810
씨드 S 및 Ti에 기초하여 제2 씨드들 Si을 생성함
812
제2 씨드들 Si에 기초하여 n-비트 난수들 Ri을 생성함
814
임의의 난수들 Ri이 소수인지를 결정함
816
소수 난수들 Ri에 대한 씨드 S 및 씨드들 Ti을 저장함
818
Ri가 소수가 아닌 모든 i에 대해, 씨드들 Ti을 재생성함
820
씨드 S 및 재생성된 Ti에 기초하여 제2 씨드들 Si을 재생성함
822
재생성된 제2 씨드들 Si에 기초하여 난수들 Ri을 재생성함
824
재생성된 난수들 Ri이 소수임을 결정함
826
소수들 Ri에 대한 씨드들 Ti을 저장함

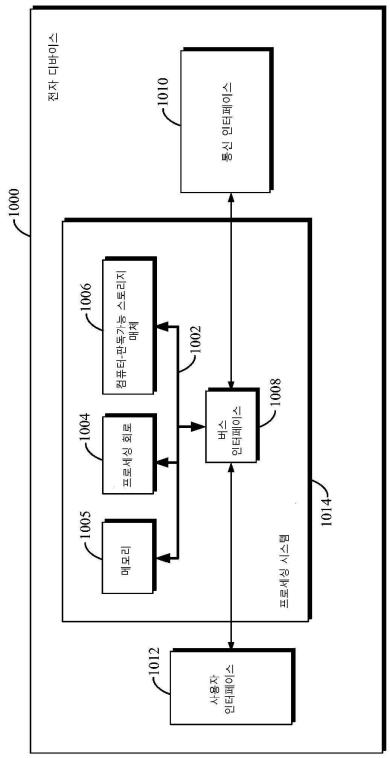
도면8b


800
프로세싱 회로(들)
802
메모리 회로(들)
804
애플리케이션(들)
806
828
난수들 Ri 전부가 소수일 때까지, 단계들 818, 820, 822, 824, 826을 반복함
830
암호 키 생성 함수로부터 하나 또는 그 초과의 소수들에 대한 요청을 수신함
832
씨드 S 및 씨드들 Ti을 리트리빙함
834
씨드 S 및 Ti을 사용하여 n-비트 소수 난수들 Ri을 재생성함
836
키 생성을 위해 소수 난수들 Ri을 제공함

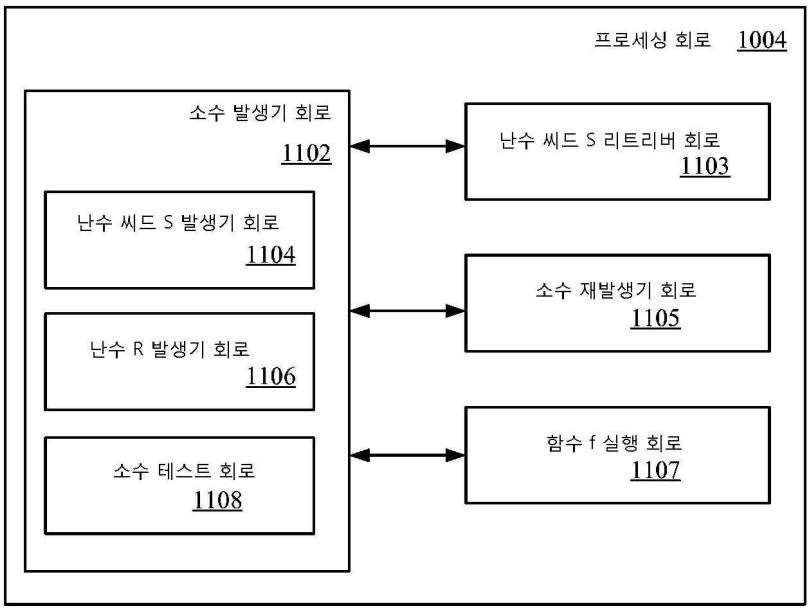
도면9


900
k개 비트들을 갖는 난수 씨드 S, 및 각각이 g개 비트들을 갖는 복수의 보충 씨드들 Ti을 생성함
902
각각이 복수의 보충 씨드들 Ti 중 상이한 보충 씨드 및 난수 씨드 S에 기초하는 복수의 제2 씨드들 Si을 생성함
904
각각이 n개 비트들을 갖는 복수의 난수들 Ri —n은 k + g 미만임— 을 생성하고, 그리고 복수의 난수들 Ri 각각은 복수의 제2 씨드들 Si 중 상이한 제2 씨드에 기초함
906
복수의 난수들 Ri 중 적어도 하나의 난수 Rp가 소수임을 결정하는데, 난수 Rp는 복수의 제2 씨드들 Si 중 제2 씨드 Sp에 기초하고, 제2 씨드 Sp는 복수의 보충 씨드들 Ti 중 보충 씨드 Tp 및 난수 씨드 S에 기초함
908
난수 씨드 S 및 보충 씨드 Tp를 메모리 회로에 저장함
910

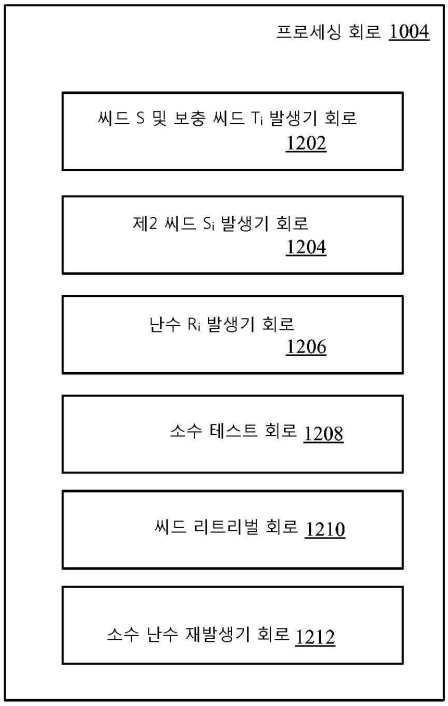
도면10


전자 디바이스
1000
1010
통신 인터페이스
1006
컴퓨터-판독가능 스토리지 매체
1002
1004
프로세싱 회로
1008
버스 인터페이스
1005
메모리
1014
프로세싱 시스템
1012
사용자 인터페이스

도면11


프로세싱 회로 1004
소수 발생기 회로
1102
난수 씨드 S 발생기 회로
1104
난수 R 발생기 회로
1106
소수 테스트 회로
1108
난수 씨드 S 리트리버 회로
1103
소수 재발생기 회로
1105
함수 f 실행 회로
1107

도면12


프로세싱 회로 1004
씨드 S 및 보충 씨드 T_i 발생기 회로 1202
제2 씨드 S_i 발생기 회로 1204
난수 R_i 발생기 회로 1206
소수 테스트 회로 1208
씨드 리트리벌 회로 1210
소수 난수 재발생기 회로 1212