(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0013878
(43) 공개일자 2017년02월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/002 (2013.01)
H04L 63/061 (2013.01)
(21) 출원번호 10-2016-7033318
(22) 출원일자(국제) 2015년06월01일
심사청구일자 없음
(85) 번역문제출일자 2016년11월28일
(86) 국제출원번호 PCT/US2015/033608
(87) 국제공개번호 WO 2015/187591
국제공개일자 2015년12월10일
(30) 우선권주장
14/294,015 2014년06월02일 미국(US)

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

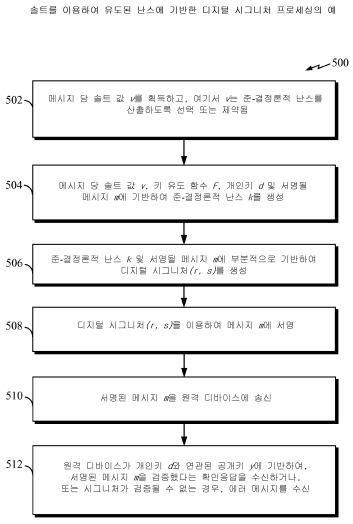
전체 청구항 수 : 총 32 항

(54) 발명의 명칭 **준-결정론적 디지털 시그니처 생성**

(57) 요 약

다양한 특징들은 메시지들을 서명하는데 사용하기 위한 디지털 시그니처들과 관련된다. 일 양상에서, 디지털 시그니처는 메시지 당 솔트 값, 특히, 준-결정론적 난스(즉, 완전히 결정론적이지도 않고 완전히 무작위적이지도 않은 난스)를 제공하기 위해 선택된 솔트를 사용하여 유도된 난스에 기반하여 생성된다. 일 예에서, 난스는 솔트 값을 장기적 개인키와 연접함으로써 그리고 그 다음으로 그 결과를 서명될 메시지의 해시와 함께 키 유도 함수에 적용함으로써 생성된다. 솔트 값은 예컨대, 카운터, 콘텍스트-특정 메시지일 수 있거나 또는 (난스로부터 디지털 시그니처를 생성하기 위해 사용되는 특정 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해) 값들의 제한된 범위 내에서 무작위로 생성될 수 있다.

대 표 도 - 도5



(52) CPC특허분류
H04L 63/0876 (2013.01)
H04L 9/3247 (2013.01)

명 세 서

청구범위

청구항 1

디지털 시그니처(digital signature)를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법으로서,

준-결정론적 난스(semi-deterministic nonce)를 획득하도록 상기 전자 디지털 시그니처 생성 디바이스의 준-결정론적 난스 생성 컴포넌트를 제어하는 단계 - 상기 준-결정론적 난스는 완전히 무작위적인 난스와 완전히 결정론적인 난스 사이의 부분적 양의 결정론(determinism)을 갖는 것을 특징으로 함 -; 및

상기 준-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하도록 상기 전자 디지털 시그니처 생성 디바이스의 디지털 시그니처 생성 컴포넌트를 제어하는 단계를 포함하는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 2

제 1 항에 있어서,

상기 준-결정론적 난스는, 상기 디지털 시그니처를 생성하기 위해 사용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위 내에서 무작위로(randomly) 또는 의사 무작위로(pseudorandomly) 획득된 완전히 무작위적인 난스보다 더 결정론적이도록, 그리고 서명될 동일한 메시지가 항상 동일한 난스를 초래할 경우, 메시지와 함께 사용하기 위해 획득된 완전히 결정론적인 난스보다 덜 결정론적이도록, 상기 준-결정론적 난스 생성 컴포넌트에 의해 획득되는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 3

제 2 항에 있어서,

상기 준-결정론적 난스는, 상기 준-결정론적 난스를 산출하기 위해 선택된 키 유도 함수, 개인키, 메시지, 및 메시지 당 값(per-message value)을 사용하여 상기 준-결정론적 난스 생성 컴포넌트에 의해 획득되는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 4

제 3 항에 있어서,

상기 준-결정론적 난스 생성 컴포넌트에 의해 사용되는 상기 메시지 당 값은 비밀 난스(secret nonce), 공개 난스(public nonce), 카운터(counter) 및 콘텍스트-특정 메시지(context-specific message) 중 하나 또는 그 초과인,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 5

제 3 항에 있어서,

상기 준-결정론적 난스 생성 컴포넌트에 의해 획득된 상기 메시지 당 값은, 결과적인 난스가 완전히 무작위적이지 않도록, 상기 메시지로부터 상기 디지털 시그니처를 생성하기 위해 사용되는 상기 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해 값들의 제한된 범위 내에서 무작위로 또는 의사 무작위로 획득되는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 6

제 5 항에 있어서,

상기 난스로부터 상기 디지털 시그니처를 생성하기 위해 상기 디지털 시그니처 생성 컴포넌트에 의해 사용되는 상기 디지털 시그니처 생성 프로토콜은, DSA(Digital Signature Algorithm), ECDSA(Elliptic Curve DSA), 엘 가말(El Gamal), 슈노르(Schnorr), 나이베르그-루펠(Nyberg-Rueppel), 러시아 표준 GOST R 34.10-2001 디지털 시그니처 알고리즘(Russian standard GOST R 34.10-2001 Digital Signature Algorithm) 및 KCDSA(Korean Certificate-based DSA) 프로토콜들 중 하나 또는 그 초과를 포함하는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 7

제 3 항에 있어서,

상기 준-결정론적 난스는, 상기 메시지 당 값, 상기 키 유도 함수, 상기 개인키 및 상기 메시지에 기반하여,

연접된 값(concatenated value)을 획득하기 위해 상기 개인키를 상기 디지털 시그니처 생성 디바이스의 메모리 내의 상기 메시지 당 값과 연접하고,

해싱된 메시지를 획득하기 위해 해시 함수를 상기 메시지에 적용하고, 그리고

상기 준-결정론적 난스를 획득하기 위해 상기 키 유도 함수를 상기 연접된 값 및 상기 해싱된 메시지에 적용함으로써, 획득되는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 8

제 1 항에 있어서,

상기 준-결정론적 난스에 부분적으로 기반하여 생성된 상기 디지털 시그니처를 이용하여 메시지에 서명하도록 상기 디지털 시그니처 생성 디바이스의 메시지 서명 컴포넌트를 제어하는 단계를 더 포함하는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 9

디바이스로서,

프로세싱 회로를 포함하고,

상기 프로세싱 회로는,

상기 프로세싱 회로의 준-결정론적 난스 생성 컴포넌트를 사용하여 준-결정론적 난스를 획득하도록 - 상기 준-결정론적 난스는 완전히 무작위적인 난스와 완전히 결정론적인 난스 사이의 부분적 양의 결정론을 갖는 것을 특징으로 함 -, 그리고

상기 프로세싱 회로의 디지털 시그니처 생성 컴포넌트를 사용하여 상기 준-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하도록 구성되는,

디바이스.

청구항 10

제 9 항에 있어서,

상기 준-결정론적 난스는, 상기 디지털 시그니처를 생성하기 위해 사용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위 내에서 무작위로 또는 의사 무작위로 획득된 완전히 무작위적인 난스보다 더 결정론적이도록, 그리고 서명될 동일한 메시지가 항상 동일한 난스를 초래할 경우, 메시지와 함께 사용하기 위해 획득된 완전히 결정론적인 난스보다 덜 결정론적이도록, 상기 프로세싱 회로의 상기 준-결정론적 난스 생성 컴포넌트에 의해 획득되는,

디바이스.

청구항 11

제 10 항에 있어서,

상기 프로세싱 회로의 상기 준-결정론적 난스 생성 컴포넌트는, 상기 준-결정론적 난스를 산출하기 위해 선택된 키 유도 함수, 개인키, 메시지, 및 메시지 당 값을 사용하여 상기 준-결정론적 난스를 획득하도록 구성되는,

디바이스.

청구항 12

제 11 항에 있어서,

상기 준-결정론적 난스 생성 컴포넌트에 의해 사용되는 상기 메시지 당 값은 비밀 난스, 공개 난스, 카운터 및 콘텍스트-특정 메시지 중 하나 또는 그 초과인,

디바이스.

청구항 13

제 11 항에 있어서,

상기 프로세싱 회로의 상기 준-결정론적 난스 생성 컴포넌트는, 결과적인 난스가 완전히 무작위적이지 않도록, 상기 메시지로부터 상기 디지털 시그니처를 생성하기 위해 사용되는 상기 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해 값들의 제한된 범위 내에서 무작위로 또는 의사 무작위로 상기 메시지 당 값을 획득하도록 구성되는,

디바이스.

청구항 14

제 13 항에 있어서,

상기 난스로부터 상기 디지털 시그니처를 생성하기 위해 상기 프로세싱 회로의 상기 디지털 시그니처 생성 컴포넌트에 의해 사용되는 상기 디지털 시그니처 생성 프로토콜은, DSA(Digital Signature Algorithm), ECDSA(Elliptic Curve DSA), 엘 가말, 슈노르, 나이베르그-루펠, 러시아 표준 GOST R 34.10-2001 디지털 시그니처 알고리즘 및 KCDSA(Korean Certificate-based DSA) 프로토콜들 중 하나 또는 그 초과를 포함하는,

디바이스.

청구항 15

제 11 항에 있어서,

상기 프로세싱 회로는, 상기 메시지 당 값, 상기 키 유도 함수, 상기 개인키 및 상기 메시지에 기반하여,

연접된 값을 획득하기 위해 상기 개인키를 상기 디지털 시그니처 생성 디바이스의 메모리 내의 상기 메시지 당 값과 연접하고,

해싱된 메시지를 획득하기 위해 해시 함수를 상기 메시지에 적용하고, 그리고

상기 준-결정론적 난스를 획득하기 위해 상기 키 유도 함수를 상기 연접된 값 및 상기 해싱된 메시지에 적용함으로써, 상기 준-결정론적 난스를 획득하도록 구성되는,

디바이스.

청구항 16

제 9 항에 있어서,

상기 프로세싱 회로는, 상기 준-결정론적 난스에 부분적으로 기반하여 생성된 상기 디지털 시그니처를 사용하여 메시지에 서명하도록 구성된 메시지 서명 컴포넌트를 더 포함하는,

디바이스.

청구항 17

전자 디지털 시그니처 생성 디바이스로서,

준-결정론적 난스를 획득하기 위한 준-결정론적 난스 생성 수단 – 상기 준-결정론적 난스는 완전히 무작위적인 난스와 완전히 결정론적인 난스 사이의 부분적 양의 결정론을 갖는 것을 특징으로 함 –; 및

상기 준-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하기 위한 디지털 시그니처 생성 수단을 포함하는,

전자 디지털 시그니처 생성 디바이스.

청구항 18

제 17 항에 있어서,

상기 준-결정론적 난스는, 상기 디지털 시그니처를 생성하기 위해 사용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위 내에서 무작위로 또는 의사 무작위로 획득된 완전히 무작위적인 난스보다 더 결정론적이도록, 그리고 서명될 동일한 메시지가 항상 동일한 난스를 초래할 경우, 메시지와 함께 사용하기 위해 획득된 완전히 결정론적인 난스보다 덜 결정론적이도록, 상기 준-결정론적 난스 생성 수단에 의해 획득되는,

전자 디지털 시그니처 생성 디바이스.

청구항 19

디지털 시그니처를 획득하기 위해 전자 디지털 시그니처 생성 디바이스의 적어도 하나의 프로세싱 회로의 동작들을 제어하기 위한 비-일시적 기계-판독가능 저장 매체로서,

상기 기계-판독가능 저장 매체는 하나 또는 그 초과의 명령들을 갖고,

상기 하나 또는 그 초과의 명령들은, 상기 적어도 하나의 프로세싱 회로에 의해 실행될 때, 상기 적어도 하나의 프로세싱 회로로 하여금,

준-결정론적 난스를 획득하도록 상기 전자 디지털 시그니처 생성 디바이스의 준-결정론적 난스 생성 컴포넌트를 제어하게 하고 – 상기 준-결정론적 난스는 완전히 무작위적인 난스와 완전히 결정론적인 난스 사이의 부분적 양의 결정론을 갖는 것을 특징으로 함 –, 그리고

상기 준-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하도록 상기 전자 디지털 시그니처 생성 디바이스의 디지털 시그니처 생성 컴포넌트를 제어하게 하는,

비-일시적 기계-판독가능 저장 매체.

청구항 20

제 19 항에 있어서,

상기 준-결정론적 난스를 산출하기 위해 선택된 키 유도 함수, 개인키, 메시지, 및 메시지 당 값을 사용하여 상기 준-결정론적 난스를 획득하도록 상기 준-결정론적 난스 생성 컴포넌트를 제어하기 위한 명령들을 더 포함하는,

비-일시적 기계-판독가능 저장 매체.

청구항 21

제 20 항에 있어서,

연접된 값을 획득하기 위해 상기 개인키를 상기 디지털 시그니처 생성 디바이스의 메모리 내의 상기 메시지 당 값과 연접하고,

해싱된 메시지를 획득하기 위해 해시 함수를 상기 메시지에 적용하고, 그리고

상기 준-결정론적 난스를 획득하기 위해 상기 키 유도 함수를 상기 연접된 값 및 상기 해싱된 메시지에 적용하도록 상기 준-결정론적 난스 생성 컴포넌트를 제어하기 위한 명령들을 더 포함하는,

비-일시적 기계-판독가능 저장 매체.

청구항 22

제 19 항에 있어서,

상기 준-결정론적 난스에 부분적으로 기반하여 생성된 상기 디지털 시그니처를 사용하여 메시지에 서명하도록 상기 디지털 시그니처 생성 디바이스를 제어하기 위한 명령들을 더 포함하는,

비-일시적 기계-판독가능 저장 매체.

청구항 23

제 19 항에 있어서,

상기 준-결정론적 난스는, 상기 디지털 시그니처를 생성하기 위해 사용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위 내에서 무작위로 또는 의사 무작위로 획득된 완전히 무작위적인 난스보다 더 결정론적이도록, 그리고 서명될 동일한 메시지가 항상 동일한 난스를 초래할 경우, 메시지와 함께 사용하기 위해 획득된 완전히 결정론적인 난스보다 덜 결정론적이도록, 상기 준-결정론적 난스 생성 컴포넌트에 의해 획득되는,

비-일시적 기계-판독가능 저장 매체.

청구항 24

제 20 항에 있어서,

상기 명령들은, 결과적인 난스가 완전히 무작위적이지 않도록, 상기 메시지로부터 상기 디지털 시그니처를 생성하기 위해 사용되는 상기 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해 값들의 제한된 범위 내에서 무작위로 또는 의사 무작위로 상기 메시지 당 값을 획득하게 상기 준-결정론적 난스 생성 컴포넌트를 제어하도록 동작가능한,

비-일시적 기계-판독가능 저장 매체.

청구항 25

제 1 항에 있어서,

상기 준-결정론적 난스는, 상기 디지털 시그니처 생성 컴포넌트에 의해 사용되는 곱셈 팩터(multiplicative factor)(q)와 연관된 값들의 전체 범위에 비해 값들의 제한된 범위 내에서 무작위로 또는 의사 무작위로 선택된 메시지 당 값을 사용하여 상기 준-결정론적 난스 생성 컴포넌트에 의해 획득되는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 26

제 9 항에 있어서,

상기 준-결정론적 난스는, 상기 디지털 시그니처 생성 컴포넌트에 의해 사용되는 곱셈 팩터(q)와 연관된 값들의 전체 범위에 비해 값들의 제한된 범위 내에서 무작위로 또는 의사 무작위로 선택된 메시지 당 값을 사용하여 상기 준-결정론적 난스 생성 컴포넌트에 의해 획득되는,

디바이스.

청구항 27

제 17 항에 있어서,

상기 준-결정론적 난스는, 상기 디지털 시그니처 생성 컴포넌트에 의해 사용되는 곱셈 팩터(q)와 연관된 값들의 전체 범위에 비해 값들의 제한된 범위 내에서 무작위로 또는 의사 무작위로 선택된 메시지 당 값을 사용하여 상기 준-결정론적 난스 생성 수단에 의해 획득되는,

전자 디지털 시그니처 생성 디바이스.

청구항 28

제 19 항에 있어서,

상기 디지털 시그니처 생성 컴포넌트에 의해 사용되는 곱셈 팩터(q)와 연관된 값들의 전체 범위에 비해 값들의 제한된 범위 내에서 무작위로 또는 의사 무작위로 선택된 메시지 당 값을 사용하여 상기 준-결정론적 난스를 획득하기 위한 명령들을 더 포함하는,

비-일시적 기계-판독가능 저장 매체.

청구항 29

제 8 항에 있어서,

서명된 메시지를 다른 디바이스에 송신하도록 송신기를 제어하는 단계를 더 포함하는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 30

제 1 항에 있어서,

준-결정론적 난스를 사용하여 획득된 디지털 시그니처에 기반하여 다른 디바이스에 의해 서명되었던 서명된 메시지를 수신하는 단계; 및

수신된 서명된 메시지를 검증하는 단계를 더 포함하는,

디지털 시그니처를 획득하기 위한 전자 디지털 시그니처 생성 디바이스에서 동작가능한 방법.

청구항 31

제 16 항에 있어서,

서명된 메시지를 다른 디바이스에 송신하기 위해 구비된 송신기를 더 포함하는,

디바이스.

청구항 32

제 9 항에 있어서,

준-결정론적 난스를 사용하여 획득된 디지털 시그니처에 기반하여 다른 디바이스에 의해 서명되었던 서명된 메시지를 수신하기 위해 구비된 수신기를 더 포함하고, 그리고

상기 디지털 시그니처를 검증하게 상기 디바이스의 검증 컴포넌트를 제어하도록 프로세서가 추가로 구성되는,

디바이스.

발명의 설명

기 술 분 야

[0001] 관련 출원들에 대한 상호 참조

[0002] [0001] 본 출원은, 2014년 6월 2일 미국 특허청에 출원된 미국 정규 특허 출원 번호 제 14/294,015호를 우선권으로 주장하고 그 권익을 청구하며, 그 미국 정규 특허 출원의 전체 내용은 인용에 의해 본원에 포함된다.

[0003] 본 개시내용의 분야

[0004] [0002] 다양한 특징들은 디지털 시그니처 생성, 특히, 난스-기반 디지털 시그니처 생성(nonce-based digital signature generation)에 관한 것이다.

배 경 기 술

[0005] [0003] 상이한 메시지들을 위해 난스들(즉, 이러한 프로시저들에 의해 사용되는 메시지 당 비밀 번호(per-

message secret number)들)이 재사용되는 경우, 디지털 시그니처 방식들, 이를테면, DSA(Digital Signature Algorithm) 및 ECDSA(Elliptic Curve DSA)는 실패할 수 있다. 즉, 디지털 시그니처와 함께 사용되는 장기적 비밀키(long-term secret key)를 해커 또는 악의적 엔티티(malicious entity)가 결정할 수 있고, 이에 의해, 악의적 엔티티가 그렇지 않으면 유효한 것으로 보이는 거짓 시그니처들을 생성하도록 허용될 수 있다. 이러한 문제를 처리하기 위해, 난스들의 결정론적 생성(deterministic generation)이 제안되었으며, 여기서 난스 k는 $k = \mathrm{HMAC}(d, h(m))$에 따라 개략적으로 생성되며, 여기서 d는 장기적 개인키(long-term private key)이고, h는 해시 함수이고, m은 서명될 메시지이고, HMAC는 해시-기반 메시지 인증 코드 함수이다. 이에 의해, 각각의 메시지는 주어진 키 d에 대한 단일 k 값을 결정론적으로 초래한다. 결정론적 접근방식은 예컨대, T. Pornin에 의한 2013년 8월의 "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)"에 설명되어 있다. 결정론적 접근방식에 따른 하나의 문제는, 결정론적 접근방식이 잠재적으로 개인키를 특정 사이드-채널 공격(side-channel attack)들, 예컨대, DPA(differential power analysis)에 노출시키는 것인데, 그 이유는, 공격자가 측정들을 반복하여, 그렇지 않으면 공격을 방지할 노이즈를 감소시킬 수 있기 때문이다.

[0006] [0004] 전술한 문헌에 대한 RFC(Request for Comments)(즉, RFC 6979, ISSN: 2070-1721)에 따르면, 서명 동작을 수행하는데 걸리는 시간의 길이 또는 서명 동작의 각각의 포인트에서 소비되는 전력과 같은 구현의 양상들을 공격자가 정확하게 측정할 수 있을 때마다, 사이드-채널 공격들이 고려된다. 따라서, 이러한 알고리즘들의 결정론(determinism)은 일부 형태들의 사이드-채널 공격들에서 공격자에게 유용할 수 있고, 그러므로, 구현들은, 사이드 채널을 통한 개인키의 유출을 회피하기 위해 방어적인 수단들을 사용해야 한다. 시그니처를 생성하기 위해 사용되는 시그니처 생성 연산들의 지수화(exponentiation) 또는 포인트 곱셈(point multiplication) 부분에서, 난스가 시그니처 오라클(signature oracle)에 대한 각각의 호출에 대해 상이하기 때문에, DSA(또는 유사한 기법들)는, 전력, 전자기 방사 또는 타이밍과 같은 사이드-채널들을 활용하는 DPA-스타일의 사이드-채널 분석 공격들에 대한 타겟이 거의 되지 않는다는 것을 주목한다. 대신에, 공격자들은, 공격자 능력들에 대해 훨씬 더 제한적인 SPA(simple power analysis) 기법들을 이용하는데, 예컨대, 사이드-채널에서 노이즈를 감소시키기 위해 측정들이 반복될 수 없다. 난스들의 결정론적 생성은 이러한 자연적 사이드-채널 저항을 제거 또는 방해하는 것을 도울 수 있다. 다시 말해, 난스들의 결정론적 생성이 디지털 시그니처 기법들에서 특정 취약성들을 감소시키는 것을 도울 수 있지만, 다른 취약성들이 발생할 수 있다.

[0007] [0005] 그러므로, 예컨대, 디지털 시그니처들을 생성하는데 사용하기 위한 개선된 난스-기반 프로시저들을 제공하는 것이 도움이 될 것이다.

발명의 내용

[0008] [0006] 디지털 시그니처를 획득하기 위해 디지털 시그니처 생성 디바이스에서 동작가능한 방법은: 디지털 시그니처 생성 디바이스를 사용하여 비-무작위적(non-random) 및 비-결정론적(non-deterministic) 난스를 획득하는 단계; 및 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 디지털 시그니처 생성 디바이스를 사용하여 디지털 시그니처를 획득하는 단계를 포함한다.

[0009] [0007] 다른 양상에서, 디바이스는, 비-무작위적 및 비-결정론적 난스를 획득하고 그리고 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하도록 구성된 프로세싱 회로를 포함한다.

[0010] [0008] 또 다른 양상에서, 디바이스는: 비-무작위적 및 비-결정론적 난스를 획득하기 위한 수단; 및 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하기 위한 수단을 포함한다.

[0011] [0009] 또 다른 양상에서, 디지털 시그니처를 획득하기 위한 기계-판독가능 저장 매체가 제공되며, 기계-판독가능 저장 매체는, 적어도 하나의 프로세싱 회로에 의해 실행될 때, 적어도 하나의 프로세싱 회로로 하여금, 비-무작위적 및 비-결정론적 난스를 획득하게 하고, 그리고 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하게 하는 하나 또는 그 초과의 명령들을 포함한다.

도면의 간단한 설명

[0012] [0010] 도 1은 사이드-채널 공격을 받는 DSA/ECDSA 시스템을 예시한다.

[0011] 도 2는 사이드-채널 공격을 받는 다른 예시적 DSA/ECDSA 시스템을 예시하며, 여기서 시스템은 스마트 카드 판독기를 포함한다.

[0012] 도 3은 예시적 암호화 서명 디바이스(cryptographic signing device), 시그니처 검증 디바이스 및 그들 사이에서 교환되는 정보를 예시한다.

[0013] 도 4는 모바일 디바이스의 예시적 SoC(system-on-a-chip)를 예시하며, 여기서 SoC는 암호화 서명 디바이스 및 시그니처 검증 디바이스를 갖는 디지털 시그니처 프로세서를 포함한다.

[0014] 도 5는 메시지 당 값(per-message value)(즉, 솔트(salt))을 사용하여 유도된 난스에 기반한 디지털 시그니처 생성을 위한 예시적 프로시저의 개요를 제공한다.

[0015] 도 6은 메시지 당 값(즉, 솔트)을 사용하여 유도된 난스에 기반하여 디지털 시그니처를 생성하기 위한 예시적 프로시저를 예시한다.

[0016] 도 7은 도 1 내지 도 6의 시스템들, 방법들 및 장치를 활용할 수 있는 프로세싱 시스템을 이용하는 장치를 위한 하드웨어 구현의 예를 예시하는 블록도이다.

[0017] 도 8은 도 7의 프로세싱 회로의 예시적 컴포넌트들을 예시하는 블록도이다.

[0018] 도 9는 도 7의 기계-판독가능 매체의 예시적 명령 컴포넌트들을 예시하는 블록도이다.

[0019] 도 10은 디지털 시그니처 생성과 함께 사용하기 위한 예시적 프로시저들의 다른 개요를 제공하며, 여기서 난스는 메시지 당 값(즉, 솔트)으로부터 유도된다.

[0020] 도 11은 디지털 시그니처 생성과 함께 사용하기 위한 예시적 프로시저들의 개요를 제공하며, 여기서 난스는 준-결정론적으로(semi-deterministically) 생성된다.

[0021] 도 12는 디지털 시그니처 생성과 함께 사용하기 위한 추가의 예시적 프로시저들을 제공한다.

발명을 실시하기 위한 구체적인 내용

[0013] [0022] 이하의 설명에서, 본 개시내용의 다양한 양상들의 완전한 이해를 제공하기 위해 특정 세부사항들이 주어진다. 그러나, 양상들이 이러한 특정 세부사항들 없이도 실시될 수 있다는 것이 당업자에 의해 이해될 것이다. 예컨대, 양상들을 불필요한 세부사항으로 모호하게 하는 것을 회피하기 위해, 회로들은 블록도들로 도시될 수 있다. 다른 경우들에서, 본 개시내용의 양상들을 모호하게 하지 않기 위해, 잘-알려진 회로들, 구조들 및 기법들은 상세하게 도시되지 않을 수 있다.

[0014] [0023] 단어 "예시적인"은 본원에서 "예, 예시 또는 예증으로서 기능"하는 것을 의미하기 위해 사용된다. "예시적인" 것으로서 본원에서 설명된 임의의 구현 또는 양상은 반드시 본 개시내용의 다른 양상들에 비해 반드시 바람직하거나 유리한 것으로서 해석되지는 않을 것이다. 마찬가지로, "양상들"이라는 용어는, 본 개시내용의 모든 양상들이 논의된 특징, 이점 또는 동작 모드를 포함하는 것을 요구하지는 않는다.

[0015] **개요**

[0016] [0024] 몇몇 신규한 특징들은 난스-기반 디지털 시그니처 생성과 함께 사용하기 위한 디바이스들 및 방법들과 관련된다. 난스-기반 디지털 시그니처 방식의 예는 전술한 DSA이며, DSA는 1991년 8월 NIST(National Institute of Standards and Technology)에 의해 최초로 제안된, 디지털 시그니처들에 대한 미국 연방 정보 프로세싱 표준이다. 통상의 DSA는 아래와 같이 설명될 수 있다. 소수(prime)들 p 및 q를 취하며, 여기서 $g \in \boldsymbol{F}_{\boldsymbol{p}}^{*}$ 는 차수 q에 대한 것이다. d를 장기적 개인키로 하고, d는 무작위로 선택되고 $1 \le d < q$ 를 충족한다. $y = g^{d} \bmod p$ 를 공개키로 한다. h는 암호화 해시 함수(cryptographic hash function)를 지시한다. 메시지 m에 서명하기 위해, 시스템은 범위 $1 \le k \le q$ 에서 무작위로 난스 k(즉, 메시지 당 비밀 번호)를 균일하게 선택하고, 아래의 수학식을 이용하여 시그니처 (r, s)를 컴퓨팅하며:

[0017] $$r = g^{k} \bmod p \bmod q \qquad (1)$$

[0018] $$s = k^{-1}(h(m) + rd) \bmod q \qquad (2)$$

[0019] 여기서, 이를테면 (적어도 DSA 예들에서) SHA(Secure Hash Algorithm)-1 또는 SHA-2를 이용함으로써, h(m)는 m의 해시이다.

[0020] [0025] ECDSA는 유사하지만, F_p^* 의 타원 곡선들에 대해 작용한다. 난스들을 이용하는 다른 이러한 시그니처 방식들은, 엘 가말(El Gamal), 슈노르(Schnorr), 나이베르그-루펠(Nyberg-Rueppel), 러시아 표준 GOST R 34.10-2001 디지털 시그니처 알고리즘(Russian standard GOST R 34.10-2001 Digital Signature Algorithm)(여기서 GOST는 사실상 "국가 표준"을 의미하는 러시아 약어임), 및 KCDSA(Korean Certificate-based DSA)를 포함한다. 이러한 기법들을 이용시, k가 2개의 상이한 메시지들에 대해 재사용되는 경우, 방식은 즉시 깨진다. 즉, 난스 k 및 비밀 개인키 d를 결정하기 위해 가우스 소거를 이용하여 풀릴 수 있는 2개의 미지수들이 있는 2개의 수학식들이 획득된다:

[0021] $$s_1 = k^{-1}(h(m_1) + rd) \bmod q \qquad (3)$$

[0022] $$s_2 = k^{-1}(h(m_2) + rd) \bmod q \qquad (4)$$

[0023] 이는 예컨대, 서명시, 불충분한 암호화 공학(cryptographic engineering) 또는 엔트로피의 부족으로 인해 실제로 발생할 수 있다. 이와 관련하여, DSA 및 ECDSA(그리고 다른 유사한 난스-기반 시그니처 방식들)는 난스의 고품질의 메시지 당 무작위성 요건(high-quality per-message randomness requirement) 때문에, 실제로 깨질 수 있다. 위에서 언급된 바와 같이, k가 결정론적으로 생성되는, 본질적으로는 아래와 같이 k를 컴퓨팅하는 솔루션이 제안되었다:

[0024] $$k = \mathrm{HMAC}(d, h(m)) \qquad (5)$$

[0025] 즉, 각각의 메시지는 결정론적으로, 비밀키 d에 대해 특정 값이 주어진, 단일 k 값으로 이어진다. 여기서, HMAC가 장기적 개인키 d에 적용되어, 메시지 m의 중첩된 해시 함수(nested hash function) h와 함께 k가 생성된다. 그러므로, 어떠한 메시지 당 무작위성도 요구되지 않는다. 그러나, 위에서 설명된 바와 같이, 결정론적 난스들로 인해 사이드-채널 취약성들이 발생할 수 있다.

[0026] [0026] 용어에 대한 주석: 편의성 및 간결함을 위해, ("메시지 당 비밀 번호" 또는 "세션 시그니처 키"인) 값 k는 본원에서 "난스(nonce)"로 지칭된다. 그러나, 값 k가 비밀성, 유일성 및 예측불가능성(즉, 엔트로피)을 제공하는 반면, 더 통상적인 난스들은 이러한 속성들 각각을 제공하지 않거나 또는 필요로 하지 않기 때문에, 값 k의 특징들은 더 통상적인 난스들과 상이하다. 그러므로, 그 용어가 본원에서 사용되는 바와 같이, "난스"는 적어도 어느 정도의 비밀성, 유일성 및 예측 불가능성을 제공하는, 디지털 시그니처 생성에서 사용하기 위한 메시지 당 비밀 번호이다.

[0027] [0027] 도 1은 사이드-채널 공격을 받는 예시적 디지털 시그니처 시스템(100)을 예시한다. 간략하게, 메시지(102)는 암호화 서명 디바이스(106)에 의해 프로세싱되고, 암호화 서명 디바이스(106)는 메시지에 서명하기 위해 개인키(104)를 사용하여 디지털 시그니처를 생성하기 위해 DSA 또는 ECDSA 프로시저들을 이용할 수 있다. 그 다음으로, 서명된 메시지(108)는 일반적으로 보안되지 않은 채널(109)을 통해 전달되고, 서명된 메시지(108)는, 예/아니오 검증(114)을 산출하기 위해 공개키(110)를 사용하여 DSA 또는 ECDSA 시그니처 검증 디바이스(112)에 의해 프로세싱된다. 서명 디바이스(106)에 의해 사용된 난스가 결정론적인 경우, 디지털 시그니처 프로시저는 사이드-채널 공격 디바이스 또는 시스템(116)에 취약할 수 있으며, 사이드-채널 공격 디바이스 또는 시스템(116)은, 이를테면, 잠재적으로 개인키를 공격자 또는 다른 악의적 엔티티(예컨대, 해커)에게 노출시키는 전력 시그니처들 및 타이밍 정보를 획득하기 위해 전력원(122)에 의해 제공되는 전력 신호들(120)을 모니터링함으로써, 서명 디바이스(106)와 연관된 전력 및 타이밍 정보(118)를 모니터링한다. 역으로, 서명 디바이스(106)에 의해 사용되는 난스가 무작위로 할당되는 경우(즉, 난스가 완전히 비결정론적임), 디지털 시그니처 프로시저는, 난스가 한번이라도 반복된다면, 전술한 가우스 소거 프로시저에 취약하다. 언급된 바와 같이, 상이한 메시지들에 대해 동일한 난스가 재사용된다면, 프로시저의 보안이 즉시 실패하여, 해커가 개인키를 획득하도록 허용된다.

[0028] [0028] 도 2는 사이드-채널 공격을 받는 다른 예시적 디지털 시그니처 시스템(200)을 예시하며, 여기서 공격 하의 시스템은 하나 또는 그 초과의 스마트 카드들(204)을 수용하는 스마트 카드 판독기(206)이다. 또한, 스마트

카드에 의해 이용되는 디지털 시그니처를 생성하기 위해 사용되는 난스가 결정론적인 경우, 개인키는 잠재적으로, 전력원(222)에 의해 제공된 전력 신호들(220)로부터 획득된 전력 및 타이밍 정보(218)에 기반하여 사이드-채널 공격 시스템(이 예에서 사이드-채널 공격 시스템은 전력 측정 오실로스코프(216) 및 사이드-채널 컴퓨터/분석기(217)를 포함함)에 의해 유도될 수 있다. 또한, 이 예에서, EMI(electromagnetic induction) 신호들, 음향 신호들 등(219)이 컴퓨터/분석기(217)에 의한 분석을 위해 적절한 센서 또는 검출기(221)에 의해 획득될 수 있다. 결정론적 난스가 사용되는 경우, 개인키를 유도하기 위해, USB(universal serial bus) 디바이스들, 스마트폰들 등에 대해 유사한 공격들이 가해질 수 있다.

[0029] [0029] 따라서, 일 양상에서, 메시지 당 값(즉, 솔트) v, 특히, 준-결정론적 난스(즉, 완전히 결정론적이지도 않고 완전히 무작위적이지도 않은 난스)를 산출하기 위해 선택된 솔트에 기반하여 난스 k를 생성하기 위한 기법들이 본원에서 설명된다. 통상적으로, "솔트(salt)"는 보통, 패스워드 또는 패스프레이즈(passphrase)를 해싱하는 일방함수(one-way function)에 대한 추가의 입력으로서 사용되는 무작위 데이터 값으로 간주된다는 것을 주목한다. 그러나, 본원에서, 솔트라는 용어는, 완전히 무작위적인, 완전히 결정론적인 또는 완전히 무작위적이지도 않고 완전히 결정론적이지도 않은 값으로 설정될 수 있는 메시지 당 값(per-message value)을 지칭한다. 본원에서 설명된 다양한 예들에서, 솔트 값은, 준-결정론적 난스를 생성하기 위해 설정되며, 여기서 "준-결정론적"은 본원에서 완전히 무작위적인 것과 완전히 결정론적인 것 사이의 부분적 양의 결정론을 갖는 것을 특징으로 하는 것으로 정의된다. 그러나, 다른 예들에서, 솔트는 완전히 무작위적인 난스를 산출하기 위해 완전히 무작위적인 값으로 설정될 수 있다. 솔트는 또한, 완전히 결정론적인 난스를 산출하기 위해 빈 문자열(empty string)로 설정될 수 있다. 준-결정론적(semi-deterministic)은 또한 준-무작위적(semi-random)으로 지칭될 수 있다.

[0030] [0030] 게다가, 솔트 v는 값들의 제한된 또는 제약된 범위 내에서 무작위로 획득될 수 있다는 것을 주목한다. 이러한 솔트는 완전히 무작위적이지 않다. 그러므로, (난스로부터 디지털 시그니처를 생성하기 위해 사용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해) 값들의 제한된 범위 내에서 무작위로 획득되는 솔트 값을 사용하여 획득된 난스는 본원에서 준-결정론적인 난스로 간주되는데, 그 이유는 그 난스는 완전히 결정론적이지도 않고 완전히 무작위적이지도 않을 것이기 때문이다. 본원에서 설명되는 예들은 솔트들로부터 유도된 난스들을 포함하고, 여기서 솔트는 훨씬 더 많은 수의 허용가능한 값들 중에서보다는 단지 32-비트 값들 중에서 "무작위로" 선택된다. 또한, 본원에서 비-무작위적 난스의 "비-무작위성(non-randomness)"은 적어도 부분적으로 결정론적이고 완전히 무작위적이지 않은 것을 특징으로 한다는 것을 주목한다. 비-결정론적 난스의 "비-결정론(non-determinism)"은 적어도 부분적으로 무작위적이고 완전히 결정론적이지 않은 것을 특징으로 한다.

[0031] [0031] 일 특정 예에서, 난스 k는 아래와 같이 생성되며(여기서 $\|$ 는 연접(concatenation)을 지시함):

[0032] $$k = \mathrm{HMAC}(d \,\|\, v, h(m)) \qquad (6)$$

[0033] 여기서 h(m)는 메시지 m의 해시이고, d는 장기적 키이고, v는 솔트이다. 솔트는 예컨대, 비밀 난스(secret nonce), 공개 난스(public nonce), 카운터(counter), 콘텍스트-특정 메시지(context-specific message) 또는 심지어 빈 문자열(empty string) 중 하나 또는 그 초과일 수 있다(여기서, 비밀 난스 및 공개 난스는, k에 대해 전술한 고려사항들에 반드시 종속되는 것이 아니라 통상의 난스들일 수 있음). 메시지 당 솔트 값 v가 빈 문자열인 경우, 공식은 수학식(5)의 결정론적 접근방식으로 되돌아간다는 것을 주목한다. 이와 같이, 시그니처 방식은 난스 재사용에 대해 보안이 유지될 것이지만, 잠재적으로는 사이드-채널 보안성을 잃는다. v가 허용가능한 값들의 전체 범위로부터 무작위로 그리고 균일하게 선택되는 경우, 방식은 완전히 비결정론적이고 그러므로 (난스 재사용에 취약한) DSA와 같은 다른 통상의 비결정론적 디지털 시그니처 기법들의 특성들을 유지한다. 메시지 당 솔트 값 v가 비-무작위적이고 비-결정론적인 경우들에서, 이를테면, 솔트가 카운터 또는 콘텍스트-특정 메시지인 경우, 수학식(6)의 공식은 준-결정론적 난스 k를 제공하며, 이는 일반적으로, 도입된 비-결정론으로 인해 사이드-채널 공격들을 극히 어렵게 만든다(그러면서 또한 난스 재사용을 회피함). 이와 관련하여, 카운터는 준-결정론적인데, 그 이유는 (a) 서명될 주어진 메시지 m이 결정론적으로, 카운터가 이용될 때와 동일한 난스로 이어지지 않고, 그리고 또한 (b) 카운터가 무작위적이지 않고 그러므로 완전히 비-결정론적이지 않기 때문이다. 마찬가지로, 콘텍스트-특정 메시지는 준-결정론적인데, 그 이유는 (a) 콘텍스트-특정 메시지가 콘텍스트에 기반하여 변화되기 때문에, 주어진 메시지 m이 결정론적으로, 동일한 난스 k로 이어지지 않고, 그리고 또한 (b) 콘텍스트 특정 메시지는 무작위적인 값이 아니고 그러므로 완전히 비-결정론적이지 않기 때문이다. (메시

지 당 솔트 값 v로서 사용되는) 비밀 난스 또는 공개 난스는 마찬가지로, 이러한 값들이 완전히 무작위적이지도 않고 완전히 결정론적이지 않은 한 준-결정론적이다. 공개 난스는, 프로토콜 메시지, 예컨대, "클라이언트 헬로우(client hello)" TLS(Transport Layer Security) 메시지에서 이미 제공되었을 수 있다.

[0034] [0032] 메시지 당 솔트 값 v에 기반하여 난스 k를 생성하는 것은, 난스 재사용이 문제가 아닌 상황들에서(이를테면, 난스가 무작위로 획득되는 값들의 범위가 너무 커서 난스 재사용이 실질적인 문제가 아닌 경우), 디지털 시그니처 생성 시스템이 편리하게 무작위적 난스를 이용하도록 허용한다는 것을 또한 주목한다. 마찬가지로, 메시지 당 솔트 값 v에 기반하여 난스 k를 생성하는 것은, 사이드-채널 공격들이 문제가 아닌 상황들에서 디지털 시그니처 생성 시스템이 편리하게 완전히 결정론적인 난스를 이용하도록 허용한다. 즉, 메시지 당 솔트 값 v의 사용은, 단일 디지털 시그니처 생성 시스템이 전체적인 보안 필요성들에 따른 v의 선택에 기반하여, 결정론적인, 준-결정론적인 또는 완전히 비결정론적인 속성들을 편리하게 활용하도록 허용한다. 범용성을 위해 본원에서, 함수 $v = \mathrm{s}(x)$ 는, 준-결정론적 난스 k를 생성하는데 사용하기 위해 (일부 입력 문자열, 값 또는 다른 함수 x로부터) 준-결정론적 메시지 당 솔트 값 v를 생성하거나 또는 다른 방식으로 획득하기 위한 임의의 함수, 프로시저 또는 알고리즘을 나타내기 위해 사용될 수 있다. 당업자들이 이해할 수 있는 바와 같이, 본원의 일반적 교시들에 따라, 매우 다양한 준-결정론적 함수들 $s(x)$ 가 제공될 수 있다. 본원에서, "획득하는"이라는 용어는 예컨대, 계산하는 것, 컴퓨팅하는 것, 생성하는 것, 포착하는 것, 수신하는 것, 리트리브하는 것, 입력하는 것 또는 임의의 다른 적절한 대응하는 동작들을 수행하는 것을 광범위하게 커버한다는 것을 또한 주목한다.

[0035] [0033] 도 3은 암호화 서명 디바이스(302) 및 시그니처 검증 디바이스(304)의 예시적 동작들을 예시하는 타이밍도(300)를 제공한다. 프로세싱은 305에서 시작되며, 암호화 서명 디바이스(302)는 (이미 확립된 공개키/개인키 쌍 y, d의) 개인키 d를 입력하고, 그리고 예컨대, 비밀 난스, 공개 난스, 카운터, 콘텍스트-특정 메시지 또는 빈 문자열로서 메시지 당 솔트 값 v, 즉, 비-무작위적이고 비-결정론적인 솔트를 획득한다. 개인키 d는 예컨대, (일부 예들에서, 신뢰된 기관 디바이스 또는 인증 기관 디바이스(도시되지 않음)와 함께) 시그니처 검증 디바이스(304)와의 초기 공개키/개인키 생성 및 교환 프로시저(도시되지 않음) 다음에 개인키 d가 저장되었던 암호화 서명 디바이스(302)의 저장 디바이스로부터 입력될 수 있다. DSA-기반 예에서, p, q 및 g를 포함하는 특정 글로벌 파라미터들이 이용되며, 여기서 p는 소수이고, g는 그룹 생성원(group generator)이고, q는 그룹 차수(group order)이다(그리고 g의 곱셈 차수(multiplicative order)임). 예시적 DSA 예에서, p는 소수이고, 여기서 $512 \leq \mathrm{L} \leq 1024$ 에 대해 $2^{\mathrm{L1}} < p < 2^{\mathrm{L}}$ 이고, L은 64의 배수이다(즉, 512 내지 1024 비트의 비트 길이가 64 비트의 증분들(N)에서 사용됨). 그러나, L은 더 길 수 있는데, 이를테면, 예컨대, 256의 증분(N)에 따라 최대 3072 또는 그 초과일 수 있다. 예시적 DSA 예에서, L은 $512 \leq \mathrm{L} \leq 1024$ 의 범위이고, q는 $p - 1$ 의 소인수(prime divisor)이고, 여기서 $2^{159} < q < 2^{160}$ 이다(즉, 160 비트의 비트 길이가 사용됨). 그 예시적 예에서, $g = \mathrm{h}^{(p-1)/\mathrm{q}} \bmod p$ 이고, 여기서 h는 $1 < \mathrm{h} < (p-1)$ 인 임의의 정수여서, $\mathrm{h}^{(p-1)/\mathrm{q}} \bmod p > 1$ 이다. 개인키 d는 $0 < d < q$ 인 무작위(random) 또는 의사 무작위(pseudorandom) 정수이다. 공개키 y는 $g^d \bmod p$ 이다. 이는 일부 배경 정보를 제공하기 위한 DSA 파라미터들의 일 예시적 예일 뿐이다. 실제로, 다양한 값들이 상이하게 선택될 수 있다. 당업자들은 p, q의 비트-길이들, 그리고 그 다음으로 특정 애플리케이션들에 대한 해시 함수를 선택하는데 익숙하다. 또한, ECDSA에 대한 파라미터들의 선택은 상당히 상이하다는 것을 주목한다.

[0036] [0034] 306에서, 암호화 서명 디바이스(302)는 예컨대, 아래의 수학식을 이용하여, 메시지 당 솔트 값 v, 개인키 d, 및 메시지 m으로부터 난스 k를 생성한다:

$$k = \mathrm{HMAC}(d \,||\, v, h(m)) \qquad (7)$$

또는

$$k = \mathrm{HMAC}(v \,||\, d, h(m)) \qquad (8)$$

[0037]

[0038] HMAC 외에 다른 키 유도 함수들이 사용될 수 있지만 HMAC가 편리하다는 것을 주목한다. 솔트 v를 개인키와 연접하는 것은, HMAC 함수가 수정될 필요가 없도록, 연접된 결과가 (메시지 m의 해시와 함께) HMAC의 2개의 입력 파라미터들 중 하나로서 적용되도록 허용한다. 더욱이, HMAC는 임의적인 길이의 파라미터들을 수용할 수 있고, 그러므로 연접은 솔트와 개인키를 조합하기에 특히 편리한데, 그 이유는 HMAC가 이에 의해 길이와 무관하게 그 결과를 수용할 수 있기 때문이다. 더욱이, 연접된 솔트/개인키와 함께 HMAC를 사용하는 것은, 일반적으로 상호 운용가능한 방식을 제공하며, 이에 의해, 디지털 시그니처 생성, 서명 및 후속 검증의 전체적인 계산들이 일반적으로, 다른 통상의 난스-기반 기법들과 동일하다. 선택된 함수가, 악의적 엔티티가 활용할 수 있는 정보의 유출을 초래하지 않는 한, 솔트와 개인키를 조합하기 위해 연접 외에 다른 함수들이 대신 사용될 수 있다는 것을 또한 주목한다. 예로서, 솔트와 개인키를 XOR화(XORing)하는 것은 사이드-채널 정보를 유출할 수 있고, 그러므로 권고되지 않는다.

[0039] [0035] 308에서, 암호화 서명 디바이스(302)는 난스 k에 부분적으로 기반하여 디지털 시그니처 (r, s)를 생성하고, 예컨대, 아래의 수학식들을 이용하여, 메시지 m에 서명하며:

$$r = g^k \bmod p \bmod q \qquad (9)$$

및

$$s = k^{-1}(h(m) + rd) \bmod q \qquad (10)$$

[0040]

[0041] 위에서 논의된 바와 같이, 여기서 p는 소수이고, q는 그룹 차수이고, g는 그룹 생성원이다.

[0042] [0036] 310에서, 암호화 서명 디바이스(302)는 디지털 시그니처 (r, s)로 서명된 메시지 m을 시그니처 검증 디바이스(304)를 갖는 원격 또는 외부 시스템에 송신한다. 많은 경우들에서, 메시지 m은 또한 암호화(encrypt)될 것이지만, 이러한 암호화(encryption)는 본원에서 논의된 디지털 시그니처 생성 프로시저들과는 분리되고 그리고 별개일 수 있다는 것을 주목한다. 312에서, 시그니처 검증 디바이스(304)는 공개키 y를 획득하고, 314에서, 공개키 y를 이용하여 메시지 m의 시그니처 (r, s)를 검증한다. 공개키는, 예컨대, 암호화 서명 디바이스(302)와의 초기 키 교환 프로시저 다음에 시그니처 검증 디바이스(304)의 저장 디바이스에 저장된 경우, 시그니처 검증 디바이스(304)의 저장 디바이스로부터 획득될 수 있다(또는 예컨대, 인증 기관 서버로부터 획득될 수 있음). 그 다음으로, 316에서, 시그니처 검증 디바이스(304)는, 시그니처 (r, s)가 검증된 경우, 메시지 m을 출력하거나 또는 다른 방식으로 프로세싱한다. DSA-기반 예에서, 검증은 다음의 수학식들: $w = (s')^{-1} \bmod q$; $\mathrm{u1} = [\, h(m')\, w \,] \bmod q$; $u2 = (r')\, w \bmod q$; 및 $v = [(\, g^{u1}\, y^{u2}\,) \bmod p\,] \bmod q$ 로서 값들 w, u1, u2를 계산함으로써 수행될 수 있고, 여기서 s', r' 및 m'은 r, s 및 m의 수신된 버전들을 나타낸다. 그 다음으로, 시그니처 검증 디바이스는 v = r'라는 것을 검증한다.

[0043] **예시적 SoC(System-on-a-Chip) 하드웨어 환경**

[0044] [0037] 본원에서 설명된 디지털 시그니처 서명 및 검증 시스템들 및 프로시저들은 광범위한 디바이스들에서 그리고 광범위한 애플리케이션들에 대해 활용될 수 있다. 구체적인 예를 제공하기 위해, 예시적 하드웨어 환경이 이제 설명될 것이며, 모바일 통신 디바이스 또는 다른 액세스 단말에서 사용하기 위해, 서명 컴포넌트 및 검증 컴포넌트 둘 모두를 갖는 디지털 시그니처 프로세서가 SoC 프로세싱 회로 상에 제공된다. 이와 관련하여, 모바일 디바이스들은 통상적으로, 비대칭 키 암호기법(asymmetric key cryptography)(즉, 공개키 암호기법)을 위한 충분한 계산 자원들이 부족한 것으로 간주되어 왔지만, 모바일 디바이스들에는 훨씬 더 강력한 프로세서들 및 더 큰 양의 메모리가 제공된다. 충분한 자원들을 이용시, 비대칭 키 생성, 서명 및 검증이 이러한 디바이스들 내에서 제공될 수 있다. 디지털 시그니처 서명 및 검증 시스템들 및 프로시저들이 구현될 수 있는 다른 예시적 하드웨어 환경들은, 다른 통신 디바이스들 및 컴포넌트들 및 그들과 함께 사용하기 위한 주변 디바이스들 등뿐

만 아니라, (제품들 또는 서비스들의 온라인 구매들을 용이하게 하기 위해 인터넷-기반 상업적 벤더들에 의해 이용될 수 있는 바와 같은) 인터넷에 연결된 통상의 데스크톱 컴퓨터들 및 트랜잭션 서버들을 포함한다. 전체적인 프로시저의 양상들은 또한, 예컨대, 키 교환을 용이하게 하기 위해 신뢰된 기관 서버를 활용할 수 있다.

[0045] [0038] 도 4는 다양한 신규한 특징들이 활용될 수 있는 일 예에 따른 모바일 통신 디바이스의 SoC 프로세싱 회로(400)를 예시한다. SoC 프로세싱 회로는 퀄컴사의 Snapdragon™ 프로세싱 회로일 수 있다. SoC 프로세싱 회로(400)는 애플리케이션 프로세싱 회로(410)를 포함하고, 애플리케이션 프로세싱 회로(410)는, 디지털 시그니처 서명 디바이스(415) 및 디지털 시그니처 검증 디바이스(417)를 갖는 디지털 시그니처 프로세서(413)와 함께 동작하도록 구비된 멀티-코어 CPU(412)를 포함한다. 디지털 시그니처 서명 디바이스(415)는 온라인 상업적 트랜잭션 서버(도시되지 않음)와 같은 원격 시스템에 전송될 메시지들을 디지털로 서명하기 위해 사용될 수 있다. 시그니처 검증 디바이스(417)는 원격 디바이스로부터 수신된 디지털 시그니처들을 검증하기 위해 사용될 수 있다(이를테면, 모바일 통신 디바이스가, 수신된 메시지들의 시그니처들을 검증할 필요가 있는 애플리케이션, 즉, "앱(app)"을 실행하는 경우에 필요할 수 있음). 다른 예들에서, 디지털 시그니처 프로세서(413)는 디지털 시그니처 서명 디바이스(415)만을 포함하거나 또는 일부 경우들에서는 디지털 시그니처 검증 디바이스(417)만을 포함할 수 있다. 즉, 컴포넌트들 둘 모두가 요구되지는 않는다.

[0046] [0039] 애플리케이션 프로세싱 회로(410)는 통상적으로 모바일 통신 디바이스의 모든 컴포넌트들의 동작을 제어한다. 일 양상에서, 애플리케이션 프로세싱 회로(410)는, 내부 공유 HW(hardware) 자원들(430)의 부분을 형성하는 내부 공유 저장 디바이스(432)의 키 저장 엘리먼트(433)에서의 공개키 및 개인키의 저장을 비롯하여 데이터의 저장을 제어하기 위한 호스트 저장 제어기(450)에 커플링된다. 애플리케이션 프로세싱 회로(410)는 또한, SoC 프로세싱 회로(400)의 다양한 컴포넌트들에 대한 부트 시퀀스 명령들을 저장하는 부트 ROM(418)을 포함할 수 있다. SoC 프로세싱 회로(400)는 애플리케이션 프로세싱 회로(410)에 의해 제어되는 하나 또는 그 초과의 주변 서브시스템들(420)을 더 포함한다. 주변 서브시스템들(420)은 저장 서브시스템(예컨대, ROM(read-only memory), RAM(random access memory)), 비디오/그래픽스 서브시스템(예컨대, DSP(digital signal processing circuit), GPU(graphics processing circuit unit)), 오디오 서브시스템(예컨대, DSP, ADC(analog-to-digital converter), DAC(digital-to-analog converter)), 전력 관리 서브시스템, 보안 서브시스템(예컨대, 다른 암호화(encryption) 컴포넌트들 및 DRM(digital rights management) 컴포넌트들), I/O(input/output) 서브시스템(예컨대, 키보드, 터치스크린) 및 유선 및 무선 연결 서브시스템들(예컨대, USB(universal serial bus), GPS(Global Positioning System), Wi-Fi, GSM(Global System Mobile), CDMA(Code Division Multiple Access), 4G LTE(Long Term Evolution) 모뎀들)(그러나, 이에 제한되지 않음)을 포함할 수 있다. 모뎀 서브시스템인 예시적 주변 서브시스템(420)은 DSP(422), 다양한 다른 HW(hardware) 및 SW(software) 컴포넌트들(424), 및 다양한 RF(radio-frequency) 컴포넌트들(426)을 포함한다. 일 양상에서, 각각의 주변 서브시스템(420)은 또한, 연관된 주변 서브시스템들(420)의 1차 부트 이미지(도시되지 않음)를 저장하는 부트 ROM(428)을 포함한다.

[0047] [0040] 언급된 바와 같이, SoC 프로세싱 회로(400)는, 다양한 런타임 데이터 또는 다른 파라미터들을 저장하고 그리고 호스트 메모리를 제공하기 위해 애플리케이션 프로세싱 회로(410) 및 다양한 주변 서브시스템들(420)에 의해 공유되는 다양한 내부 공유 HW 자원들(430), 이를테면, 내부 공유 저장소(432)(예컨대, SRAM(static RAM), 플래시 메모리 등)를 더 포함한다. 도 4의 예에서, 내부 공유 저장소(432)는 공개키 및 개인키를 저장하기 위해 사용될 수 있는 전술한 키 저장 엘리먼트, 부분 또는 컴포넌트(433)를 포함한다. 다른 예들에서, 키들은 모바일 디바이스 내의 다른 곳에 저장된다.

[0048] [0041] 일 양상에서, SoC(400)의 컴포넌트들(410, 418, 420, 428 및 430)은 단일-칩 기판 상에 통합된다. SoC 프로세싱 회로(400)는, 상이한 칩 기판 상에 로케이팅될 수 있고 그리고 하나 또는 그 초과의 버스들을 통해 SoC 프로세싱 회로(400)와 통신할 수 있는 다양한 외부 공유 HW 자원들(440)을 더 포함한다. 외부 공유 HW 자원들(440)은 예컨대, 다양한 타입들의 데이터, 이를테면, OS(operating system) 정보, 시스템 파일들, 프로그램들, 애플리케이션들, 사용자 데이터, 오디오/비디오 파일들 등을 저장하기 위해 애플리케이션 프로세싱 회로(410) 및 다양한 주변 서브시스템들(420)에 의해 공유될 수 있는 외부 공유 저장소(442)(예컨대, DDR(double-data rate) 동적 RAM) 및/또는 영구적 또는 반-영구적 데이터 저장소(444)(예컨대, SD(secure digital) 카드, HDD(hard disk drive), 내장형 멀티미디어 카드, UFS(universal flash device) 등)를 포함할 수 있다. SoC 프로세싱 회로(400)를 포함하는 모바일 통신 디바이스가 활성화될 때, SoC 프로세싱 회로는 시스템 부트 업 프로세스를 시작하며, 시스템 부트 업 프로세스에서, 애플리케이션 프로세싱 회로(410)는 다양한 주변 서브시스템들(420)에 대한 부트 시퀀스 명령들을 비롯한 SoC 프로세싱 회로(400)에 대한 부트 명령들을 리트리브하기 위해 부트 ROM(418)에 액세스할 수 있다. 주변 서브시스템들(420)은 또한 추가의 주변 부트 RAM(428)을 가질 수 있

다.

[0049] **예시적 디지털 시그니처 서명 및 검증 프로시저들**

[0050] [0042] 도 5는 도 4의 애플리케이션 프로세싱 회로의 디지털 시그니처 프로세서 또는 다른 적절하게 구비된 컴포넌트들, 디바이스들, 시스템들 또는 프로세싱 회로들에 의해 이용될 수 있는 디지털 시그니처 서명 및 검증 동작들(500)의 개요를 제공한다. 502에서, 디지털 시그니처 프로세서는 메시지 당 솔트 값 v를 획득하고, 여기서 v는 준-결정론적 난스를 산출하도록 선택 또는 제약된다. 504에서, 디지털 시그니처 프로세서는 메시지 당 솔트 값 v, 키 유도 함수 F, 개인키 d 및 서명될 메시지 m에 기반하여 준-결정론적 난스 k를 생성한다. 506에서, 디지털 시그니처 프로세서는 준-결정론적 난스 k 및 서명될 메시지 m에 기반하여 디지털 시그니처 (r, s)를 생성한다. 508에서, 디지털 시그니처 프로세서는 디지털 시그니처 (r, s)를 첨부함으로써 메시지 m에 서명한다. 510에서, 디지털 시그니처 프로세서는 서명된 메시지 m을 온라인 상업적 트랜잭션 서버와 같은 원격 디바이스에 송신하고, 원격 디바이스는 그 다음으로, 개인키 d와 연관된 공개키 y에 기반하여, 서명된 메시지의 시그니처를 검증하려고 시도할 것이다(공개키는 이전에 원격 디바이스와 교환되었음). 이미 언급된 바와 같이, 많은 경우들에서, 메시지 m은 또한 암호화(encrypt)될 것이고, 이러한 암호화(encryption)는 본원에서 논의된 디지털 시그니처 생성 프로시저들과는 분리되고 그리고 별개일 수 있다. 512에서, 디지털 시그니처 프로세서는, 원격 디바이스가 서명된 메시지 m을 공개키 y에 기반하여 검증했다는 확인응답을 수신하거나, 또는 시그니처가 검증될 수 없는 경우에는 에러 메시지를 수신한다. 도 5의 프로시저는 일반적으로, 솔트를 사용하여 유도된 난스를 활용하도록 수정된 DSA/ECDSA 또는 다른 난스-기반 디지털 시그니처 표준들 및 프로토콜들에 따라 수행될 수 있다.

[0051] [0043] 도 6은 솔트로부터 유도된 난스에 기반하여 디지털 시그니처를 생성하기 위한 예시적 프로시저(600)를 예시하며, 추가의 예시적 상세들이 제공된다. 602에서, 디지털 시그니처 프로세서는 비-무작위적 및 비-결정론적 난스(즉, 준-결정론적 난스)를 산출하기에 충분한 메시지 당 솔트 값 v를 획득하며, 여기서 예컨대, 솔트 v는 비밀 난스, 공개 난스, 카운터, 콘텍스트-특정 메시지, 빈 문자열 또는 임의의 적절한 준-결정론적 함수 $s(x)$의 결과이거나, 또는 솔트는 결과적인 난스가 완전히 무작위적이지 않도록, (난스로부터 디지털 시그니처를 생성하기 위해 사용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해) 값들의 제한된 범위 내에서 무작위로 획득된다. 이와 관련하여, 디지털 시그니처 프로세서는 예컨대, 결과적인 난스 k에 더 많은 양의 비-결정론을 주기 위해, 단순한 카운터보다는 콘텍스트-특정 메시지를 이용할 수 있다. 또한 더 많은 양의 비-결정론을 획득하기 위해, 디지털 시그니처 프로세서는 예컨대, 콘텍스트-특정 메시지보다는 비밀 난스를 이용할 수 있고, 여기서 비밀 난스는 콘텍스트-특정 메시지에 비해 더 큰 정도의 비-결정론을 제공한다. 언급된 바와 같이, 디지털 시그니처 프로세서는 값들의 제한된 범위 내에서 무작위로 솔트를 획득할 수 있다. 이와 관련하여, DSA는 통상적으로 1 내지 q-1로부터 균일하게 그리고 무작위로 k를 취하도록 동작하며, 여기서 q는 생성원(generator)의 곱셈 차수(multiplicative order)이다(대략 256 비트). 그러므로, 602에서, 메시지 당 솔트 값 v는 값들의 훨씬 더 작은 세트 내에서 무작위로 선택될 수 있다(예컨대, 메시지 당 솔트 값 v는 단지 32 비트 값들 중에서 균일하게 그리고 무작위로 선택될 수 있음). 일반적으로, 준-결정론적 함수 $s(x)$는, 결과적인 메시지 당 솔트 값 v의 비-결정론의 정도를 설정, 조정 또는 제어하고, 이에 의해, 결과적인 난스 k의 비-결정론의 정도를 설정, 조정 또는 제어하기 위해 선택되거나 선정될 수 있다.

[0052] [0044] 604에서, 디지털 시그니처 프로세서는, 예컨대, 연접된 값을 산출하기 위해 개인키 d를 메시지 당 솔트 값 v와 연접시키고; 해싱된 메시지 h(m)를 산출하기 위해 해시 함수 h를 메시지 m에 적용하고; 그리고 예컨대, 아래의 난스 k를 산출하기 위해 HMAC 함수를 연접된 값 및 해싱된 메시지에 적용함으로써, 메시지 당 솔트 값 v, HMAC 키 유도 함수, 개인키 d 및 서명될 메시지 m에 기반하여 난스 k를 생성한다:

$$k = \mathrm{HMAC}(d \,\|\, v, h(m)) \qquad (11)$$

또는

$$k = \mathrm{HMAC}(v \,\|\, d, h(m)) \qquad (12)$$

[0053]

[0054] [0045] 606에서, 디지털 시그니처 프로세서는, 난스 k에 부분적으로 기반하여 디지털 시그니처 (r, s)를 생성하

고, 예컨대, 아래의 DSA 프로시저들을 사용하여,

$$r = g^k \bmod p \bmod q \qquad (13)$$

및

$$s = k^{-1}(h(m) + rd) \bmod q \qquad (14)$$

[0055]

[0056] (위에서 논의된 바와 같이, 여기서 p는 소수이고, q는 그룹 차수이고, g는 그룹 생성원임), 또는 다른 난스-기반 프로시저들, 이를테면, ECDSA, 엘 가말, 슈노르, 나이베르그-루펠, 러시아 표준 GOST R 34.10-2001 디지털 시그니처 알고리즘 또는 KCDSA(Korean Certificate-based DSA)를 이용하여, 메시지 m에 서명한다.

[0057] **예시적 시스템들 및 방법들**

[0058] [0046] 도 7은 도 1 내지 도 6의 시스템들, 방법들 및 장치가 구현될 수 있는 전체적인 시스템 또는 장치(700)를 예시한다. 본 개시내용의 다양한 양상들에 따르면, 엘리먼트, 또는 엘리먼트의 임의의 부분, 또는 엘리먼트들의 임의의 조합은, 도 4의 SoC 프로세싱 회로와 같은 하나 또는 그 초과의 프로세싱 회로들(704)을 포함하는 프로세싱 시스템(714)을 이용하여 구현될 수 있다. 예컨대, 장치(700)는 모바일 통신 시스템의 UE(user equipment)일 수 있다. 장치(700)는 RNC(radio network controller)와 함께 사용될 수 있다. SoC에 추가하여, 프로세싱 회로들(704)의 예들은 마이크로프로세싱 회로들, 마이크로제어기들, DSP(digital signal processing circuit)들, FPGA(field programmable gate array)들, PLD(programmable logic device)들, 상태 머신들, 게이트 로직(gated logic), 이산 하드웨어 회로들, 및 본 개시내용 전반에 걸쳐 설명된 다양한 기능을 수행하도록 구성된 다른 적절한 하드웨어를 포함한다. 즉, 장치(700)에서 활용되는 바와 같은 프로세싱 회로(704)는, 디지털 시그니처 생성, 서명 및 검증을 수행하기 위한 프로세스들과 같은, 위에서 설명되고 도 3, 도 5 및 도 6에서 예시된 프로세스들(그리고 아래에서 논의되는 도 10 내지 도 12에서 예시되는 프로세스들) 중 임의의 하나 또는 그 초과를 구현하기 위해 사용될 수 있다.

[0059] [0047] 도 7의 예에서, 프로세싱 시스템(714)은, 버스(702)에 의해 일반적으로 표현되는 버스 아키텍처를 이용하여 구현될 수 있다. 버스(702)는 프로세싱 시스템(714)의 특정 애플리케이션 및 전체적인 설계 제약들에 따라, 임의의 개수의 상호연결 버스들 및 브리지들을 포함할 수 있다. 버스(702)는, 하나 또는 그 초과의 프로세싱 회로들(프로세싱 회로(704)에 의해 일반적으로 표현됨), 저장 디바이스(705), 및 기계-판독가능, 프로세서-판독가능, 프로세싱 회로-판독가능 또는 컴퓨터-판독가능 매체(비-일시적 기계-판독가능 매체(706)에 의해 일반적으로 표현됨)를 포함하는 다양한 회로들을 링크한다. 버스(702)는 또한 타이밍 소스들, 주변장치들, 전압 레귤레이터들 및 전력 관리 회로들과 같은 다양한 다른 회로들을 링크시킬 수 있으며, 이들은 당해 기술분야에 잘 알려져 있으므로 더 이상 설명되지 않을 것이다. 버스 인터페이스(708)는 버스(702)와 트랜시버(710) 사이에 인터페이스를 제공한다. 트랜시버(710)는, 송신 매체를 통해 다양한 다른 장치와 통신하기 위한 수단을 제공한다. 장치의 속성에 따라, 사용자 인터페이스(712)(예컨대, 키패드, 디스플레이, 스피커, 마이크로폰, 조이스틱)가 또한 제공될 수 있다.

[0060] [0048] 프로세싱 회로(704)는, 기계-판독가능 매체(706) 상에 저장된 소프트웨어의 실행을 포함하는 일반적인 프로세싱 및 버스(702)를 관리하는 것을 담당한다. 소프트웨어는, 프로세싱 회로(704)에 의해 실행될 때, 프로세싱 시스템(714)으로 하여금, 임의의 특정 장치에 대해 본원에서 설명된 다양한 기능들을 수행하게 한다. 기계-판독가능 매체(706)는 또한, 소프트웨어를 실행할 때 프로세싱 회로(704)에 의해 조작되는 데이터를 저장하기 위해 사용될 수 있다.

[0061] [0049] 프로세싱 시스템의 하나 또는 그 초과의 프로세싱 회로들(704)은 소프트웨어 또는 소프트웨어 컴포넌트들을 실행할 수 있다. 소프트웨어는, 소프트웨어로 지칭되든, 펌웨어로 지칭되든, 미들웨어로 지칭되든, 마이크로코드로 지칭되든, 하드웨어 디스크립션 언어로 지칭되든, 또는 다르게 지칭되든, 명령들, 명령 세트들, 코드, 코드 세그먼트들, 프로그램 코드, 프로그램들, 서브프로그램들, 소프트웨어 모듈들, 애플리케이션들, 소프트웨어 애플리케이션들, 소프트웨어 패키지들, 루틴들, 서브루틴들, 오브젝트들, 실행가능한 것들(exeutables), 실행 스레드들, 프로시저들, 함수들 등을 의미하는 것으로 광범위하게 해석될 것이다. 프로세싱 회로는 태스크들을 수행할 수 있다. 코드 세그먼트는 프로시저, 함수, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들, 데이터 구조들, 또는 프로그램 스테이트먼트들의 임의의 조합을 나타낼

수 있다. 코드 세그먼트는, 정보, 데이터, 아규먼트들, 파라미터들 또는 메모리 또는 저장 콘텐츠를 전달 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수 있다. 정보, 아규먼트들, 파라미터들, 데이터 등은, 메모리 공유, 메시지 전달, 토큰(token) 전달, 네트워크 송신 등을 포함하는 임의의 적절한 수단을 통해 전달, 포워딩 또는 송신될 수 있다.

[0062] [0050] 소프트웨어는 기계-판독가능 매체(706) 상에 상주할 수 있다. 기계-판독가능 매체(706)는 비-일시적 기계-판독가능 매체일 수 있다. 비-일시적 프로세싱 회로-판독가능, 기계-판독가능 또는 컴퓨터-판독가능 매체는 예로서, 자기 저장 디바이스(예컨대, 하드 디스크, 플로피 디스크, 자기 스트립), 광 디스크(예컨대, CD(compact disc) 또는 DVD(digital versatile disc)), 스마트 카드, 플래시 메모리 디바이스(예컨대, 카드, 스틱 또는 키 드라이브), RAM, ROM, PROM(programmable ROM), EPROM(erasable PROM), EEPROM(electrically erasable PROM), 레지스터, 착탈식 디스크, 하드 디스크, CD-ROM, 및 기계 또는 컴퓨터에 의해 액세스 및 판독될 수 있는 소프트웨어 및/또는 명령들을 저장하기 위한 임의의 다른 적절한 매체를 포함한다. "기계-판독가능 매체", "컴퓨터-판독가능 매체", "프로세싱 회로-판독가능 매체" 및/또는 "프로세서-판독가능 매체"라는 용어들은 비-일시적 매체, 이를테면, 휴대용 또는 고정형 저장 디바이스들, 광학 저장 디바이스들, 및 명령(들) 및/또는 데이터를 저장, 포함 또는 반송할 수 있는 다양한 다른 매체(그러나, 이에 제한되지 않음)를 포함할 수 있다. 따라서, 본원에서 설명되는 다양한 방법들은 완전히 또는 부분적으로, "기계-판독가능 매체", "컴퓨터-판독가능 매체", "프로세싱 회로-판독가능 매체" 및/또는 "프로세서-판독가능 매체"에 저장될 수 있고 그리고 하나 또는 그 초과의 프로세싱 회로들, 기계들 및/또는 디바이스들에 의해 실행되는 명령들 및/또는 데이터에 의해 구현될 수 있다. 기계-판독가능 매체는 또한 예로서, 반송파, 송신선, 및 컴퓨터에 의해 액세스 및 판독될 수 있는 소프트웨어 및/또는 명령들을 송신하기 위한 임의의 다른 적절한 매체를 포함할 수 있다.

[0063] [0051] 기계-판독가능 매체(706)는 프로세싱 시스템(714) 내에, 프로세싱 시스템(714) 외부에 상주할 수 있거나, 또는 프로세싱 시스템(714)을 포함하는 다수의 엔티티들에 걸쳐 분배될 수 있다. 기계-판독가능 매체(706)는 컴퓨터 프로그램 제품으로 구현될 수 있다. 예로서, 컴퓨터 프로그램 제품은 패키징 재료들에 기계-판독가능 매체를 포함할 수 있다. 당업자들은 특정 애플리케이션 및 전체 시스템에 부과된 전체 설계 제약들에 따라 본 개시내용 전반에 걸쳐 제시되는 설명된 기능을 어떻게 최상으로 구현할지를 인식할 것이다. 예컨대, 기계-판독가능 저장 매체(706)는, 프로세싱 회로(704)에 의해 실행될 때, 프로세싱 회로로 하여금, 비-무작위적 및 비-결정론적 난스를 획득하게 하고; 그리고 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득하게 하는 하나 또는 그 초과의 명령들을 가질 수 있다.

[0064] [0052] 도면들에서 예시된 컴포넌트들, 단계들, 피처들, 및/또는 기능들 중 하나 또는 그 초과는, 단일 컴포넌트, 블록, 피처 또는 기능으로 재배열 및/또는 결합되거나, 또는 여러 개의 컴포넌트들, 단계들, 또는 기능들로 구현될 수 있다. 본 개시내용으로부터 벗어남이 없이, 추가의 엘리먼트들, 컴포넌트들, 단계들, 및/또는 기능들이 또한 추가될 수 있다. 도면들에서 예시된 장치, 디바이스들, 및/또는 컴포넌트들은 도면들에서 설명된 방법들, 피처들, 또는 단계들 중 하나 또는 그 초과를 수행하도록 구성될 수 있다. 본원에서 설명된 알고리즘들은 또한, 효율적으로 소프트웨어로 구현되고 그리고/또는 하드웨어에 임베딩될 수 있다.

[0065] [0053] 본원에서 개시된 예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들, 엘리먼트들, 및/또는 컴포넌트들은 범용 프로세싱 회로, DSP(digital signal processing circuit), ASIC(application specific integrated circuit), FPGA(field programmable gate array) 또는 다른 프로그램가능 논리 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에서 설명된 기능들을 수행하도록 설계된 이들의 임의의 결합으로 구현되거나 이들에 의해 수행될 수 있다. 범용 프로세싱 회로는 마이크로프로세싱 회로일 수 있지만, 대안적으로, 프로세싱 회로는 임의의 통상의 프로세싱 회로, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 프로세싱 회로는 또한, 컴퓨팅 컴포넌트들의 결합, 예컨대, DSP 및 마이크로프로세싱 회로의 결합, 다수의 마이크로프로세싱 회로들, DSP 코어와 공조하는 하나 또는 그 초과의 마이크로프로세싱 회로들, 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0066] [0054] 그러므로, 본 개시내용의 일 양상에서, 도 4 및 도 7에서 예시된 프로세싱 회로(413 및/또는 704)는, 도 3, 도 5 및/또는 도 6(그리고/또는 아래에서 논의되는 도 10, 도 11 및/또는 도 12)에서 설명되는 알고리즘들, 방법들, 및/또는 블록들을 수행하도록 특정하게 설계된 그리고/또는 하드-와이어링된 특화된 프로세싱 회로(예컨대, ASIC)일 수 있다. 따라서, 이러한 특화된 프로세싱 회로(예컨대, ASIC)는 도 3, 도 5 및/또는 도 6(그리고/또는 아래에서 논의되는 도 10, 도 11 및/또는 도 12)에서 설명되는 알고리즘들, 방법들, 및/또는 블록들을 실행하기 위한 수단의 일 예일 수 있다. 기계-판독가능 저장 매체는 특화된 프로세싱 회로(예컨대, ASIC)에 의해 실행될 때, 특화된 프로세싱 회로로 하여금, 본원에서 설명되는 알고리즘들, 방법들, 및/또는 블록들을 수행

하게 하는 명령들을 저장할 수 있다.

[0067] [0055] 도 8은 디지털 시그니처 생성기(804) 및 디지털 시그니처 검증기(806)를 가진 디지털 시그니처 프로세서(802)를 갖는 프로세싱 회로(704)의 선택된 그리고 예시적인 컴포넌트들을 예시한다. 특히, 도 8의 디지털 시그니처 생성기(804)는, 준-결정론적 난스를 생성하는데 사용하기 위한 메시지 당 솔트 값 v를 획득 또는 생성하도록 동작가능한 솔트 생성 모듈/회로(808)를 포함한다. 디지털 시그니처 생성기(804)는 또한, 디지털 시그니처를 생성하는데 사용하기 위한 준-결정론적 난스 k를 획득 또는 생성하도록 또는 이러한 동작들을 달성하기 위해 다른 모듈들/회로들을 제어하도록 동작가능한 비-무작위적 및 비-결정론적 난스 생성 모듈/회로(810)를 포함한다. 예컨대, 연접 모듈/회로(812)는, 연접된 값을 산출하기 위해 개인키를 솔트와 연접하도록 동작가능하며, 여기서 개인키는 개인키 입력 모듈/회로(814)(개인키 입력 모듈/회로(814)는 의사 난수 생성기(PRNG; pseudorandom number generator)를 포함할 수 있음)에 의해 획득될 수 있다. 해시 함수 모듈/회로(816)는 해싱된 메시지를 산출하기 위해, 해시 함수를 서명될 메시지에 적용하도록 동작가능하다. 키 유도 함수(HMAC) 모듈/회로(816)는, 난스 생성 모듈/회로(810)의 제어 하에 난스를 산출하기 위해 HMAC와 같은 키 유도 함수를 연접된 값 및 해싱된 메시지에 적용하도록 동작가능하다. 디지털 시그니처 생성 모듈/회로(820)는 난스 생성 모듈/회로(810)에 의해 (또는 난스 생성 모듈/회로(810)의 제어 하에) 생성된 난스에 부분적으로 기반하여 디지털 시그니처를 생성하도록 동작가능하다. 그 다음으로, 메시지 서명 모듈/회로(822)는, 예컨대, 도 7의 트랜시버(710)에 연결될 수 있는 시그니처/메시지 송신/수신 모듈/회로(828)를 이용하여 원격 디바이스로의 송신을 위해 디지털 시그니처를 이용하여 메시지에 서명하도록 동작가능하다.

[0068] [0056] 디지털 시그니처를 이용하여 메시지에 서명하는 것은, 단지 시그니처를 메시지에 첨부하는 단순한 문제일 수 있고, 그러므로, 실제 구현들에서, 개별 메시지 서명 모듈/회로가 제공되지 않을 수 있다는 것을 주목한다. 더욱이, 실제 구현들에서, 전체 디지털 시그니처 생성기가 디지털 시그니처들을 이용하여 메시지에 서명하는 역할을 하기 때문에, 전체 디지털 시그니처 생성기는 메시지 서명 모듈로 지칭될 수 있다. 개별 시그니처 생성 및 메시지 서명 컴포넌트들은 필요하지 않을 수 있지만, 완전성 및 범용성을 위해 개별적으로 도시된다. 디지털 신호 프로세서(802)가 원격 디바이스로부터 수신된 시그니처를 검증할 필요가 있는 경우, 공개키 입력 모듈/회로(824)가 공개키를 입력하거나 또는 (도 7의 트랜시버(710)를 통해) 다른 방식으로 획득한다. 그 다음으로, 시그니처 검증 모듈/회로(826)는 공개키를 이용하여, 원격 디바이스로부터 수신된 서명된 메시지의 시그니처를 검증하도록 동작가능하다.

[0069] [0057] 도 9는 디지털 시그니처들을 생성 또는 검증하는데 사용하기 위한 기계- 또는 컴퓨터-판독가능 매체(706)의 선택된 그리고 예시적인 명령들을 예시한다. 간략하게, 도 9의 기계-판독가능 매체(706)는, 도 7의 프로세싱 회로(704)에 의해 실행될 때, 프로세싱 회로로 하여금, 디지털 시그니처 생성 및 검증 동작들을 제어 또는 수행하게 하는 다양한 명령들을 포함한다. 특히, 도 9의 디지털 시그니처 생성 명령들(904)은 난스를 생성하는데 사용하기 위한 메시지 당 솔트 값 v를 획득 또는 생성하도록 동작가능한 솔트 생성 명령들(908)을 포함한다. 비-무작위적 및 비-결정론적 난스 생성 명령들(910)은 디지털 시그니처를 생성하는데 사용하기 위해 준-결정론적 난스 k를 획득 또는 생성하도록 동작가능하다. 연접 명령들(912)은 연접된 값을 산출하기 위해 개인키를 솔트와 연접하도록 동작가능하고, 여기서 개인키는 개인키 입력 명령들(914)에 의해 획득될 수 있다. 해시 함수 명령들(916)은 해싱된 메시지를 산출하기 위해, 해시 함수를 서명될 메시지에 적용하도록 동작가능하다. 키 유도 함수(HMAC) 명령들(916)은 난스를 산출하기 위해 HMAC와 같은 키 유도 함수를 연접된 값 및 해싱된 메시지에 적용하도록 동작가능하다. 디지털 시그니처 생성 명령들(920)은 난스 생성 명령들(910)에 의해 (또는 난스 생성 명령들(910)의 제어 하에) 생성된 난스에 부분적으로 기반하여 디지털 시그니처를 생성하도록 동작가능하다. 그 다음으로, 메시지 서명 명령들(922)은 예컨대, 시그니처/메시지 송신/수신 명령들(928)을 이용한 원격 디바이스로의 송신을 위해 디지털 시그니처를 이용하여 메시지에 서명하도록 동작가능하다. 도 8의 모듈(822)을 참조하여 위에서 언급된 설명들이 여기에 또한 적용가능하다. 디지털 신호 프로세서가 원격 디바이스로부터 수신된 시그니처를 검증할 필요가 있는 경우, 공개키 입력 명령들(924)은 공개키를 입력하거나 또는 (도 7의 트랜시버(710)를 통해) 원격 디바이스로부터 공개키를 다른 방식으로 획득한다. 그 다음으로, 시그니처 검증 명령들(926)은 공개키를 이용하여, 원격 디바이스로부터 수신된 서명된 메시지의 시그니처를 검증하도록 동작가능하다.

[0070] [0058] 도 10은 도 8의 디지털 시그니처 생성기(804) 또는 디지털 시그니처들을 생성하기 위한 또는 다른 방식으로 획득하기 위한 다른 적절하게 구비된 디지털 시그니처 생성 디바이스들, 이를테면 도 4의 애플리케이션 프로세싱 회로(410)에 의해 수행될 수 있는 방법들 또는 프로시저들(1000)을 폭넓게 예시 및 요약한다. 1002에서, 디지털 시그니처 생성기는 비-무작위적 및 비-결정론적 난스를 획득하고, 1004에서, 디지털 시그니처

생성기는, 예컨대, 위에서 설명된 기법들을 사용하여 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 획득한다.

[0071] [0059] 도 11은 도 8의 디지털 시그니처 프로세서(802) 또는 다른 적절하게 구비된 디바이스들에 의해 수행될 수 있는 예시적인 방법들 또는 프로시저들(1100)을 예시한다. 1102에서, 디지털 시그니처 프로세서(802)는 준-결정론적 난스를 산출하기에 충분한 메시지 당 값을 생성하거나 또는 다른 방식으로 획득하고, 메시지 당 값은 비밀 난스, 공개 난스, 카운터 및 콘텍스트-특정 메시지 중 하나 또는 그 초과이거나, 또는 메시지 당 값은 결과적인 난스가 완전히 무작위적이지 않도록, (난스로부터 디지털 시그니처를 생성하기 위해 사용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해) 값들의 제한된 범위 내에서 무작위로 획득된다. 1104에서, 디지털 시그니처 프로세서(802)는, 완전히 무작위적인 난스와 완전히 결정론적인 난스 사이의 부분적 양의 결정론을 갖는 것을 특징으로 하는 준-결정론적 난스를 산출하기 위해 선택된 키 유도 함수, 개인키, 메시지 및 메시지 당 값을 사용하여 비-무작위적 및 비-결정론적 난스를 생성하거나 또는 다른 방식으로 획득하며, 여기서 난스의 비-무작위성은 적어도 부분적으로 결정론적이고 완전히 무작위적이지 않은 것으로서 특징지어지며, 여기서 난스의 비-결정론은 적어도 부분적으로 무작위적이고 완전히 결정론적이지 않은 것으로서 특징지어진다. 1106에서, 디지털 시그니처 프로세서(802)는 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 디지털 시그니처를 생성하거나 또는 다른 방식으로 획득한다. 1108에서, 디지털 시그니처 프로세서(802)는 비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 획득된 디지털 시그니처를 사용하여 메시지에 서명한다. 이미 언급된 바와 같이, 메시지에 서명하는 것은 단순히 디지털 시그니처를 메시지에 첨부하는 것을 수반할 수 있고, 그러므로 개별 시그니처 생성 및 메시지 서명 컴포넌트들은 필요하지 않을 수 있지만, 완전성 및 범용성을 위해 개별적으로 도시된다.

[0072] [0060] 도 12는 도 8의 디지털 시그니처 프로세서(802) 또는 키 유도 함수, 개인키, 메시지 및 메시지 당 값을 사용하여 난스를 획득하거나 또는 다른 방식으로 생성하기 위해 도 11의 블록(1104)에서 사용하기 위한 다른 적절하게 구비된 디지털 시그니처 생성 디바이스들에 의해 수행될 수 있는 예시적 방법들 또는 프로시저들을 예시한다. 1202에서, 디지털 시그니처 프로세서(802)는 연접된 값을 획득하기 위해 개인키를 메시지 당 값과 연접한다. 1204에서, 디지털 시그니처 프로세서(802)는 해싱된 메시지를 획득하기 위해 해시 함수를 메시지에 적용한다. 1206에서, 디지털 시그니처 프로세서(802)는 준-결정론적 난스를 획득하기 위해 키 유도 함수를 연접된 값 및 해싱된 메시지에 적용하며, 여기서 키 유도 함수는 HMAC 함수일 수 있다.

[0073] [0061] 본 개시내용의 양상들이 플로차트, 흐름도, 구조도, 또는 블록도로 도시된 프로세스로서 본원에서 설명될 수 있다는 것을 주목한다. 플로차트가 동작들을 순차적인 프로세스로서 설명할 수 있지만, 동작들 중 다수의 동작들은 병렬로 또는 동시에 수행될 수 있다. 추가로, 동작들의 순서는 재배열될 수 있다. 프로세스는, 자신의 동작들이 완료될 때 종결된다. 프로세스는 방법, 함수, 프로시저, 서브루틴, 서브프로그램 등에 대응할 수 있다. 프로세스가 함수에 대응하는 경우, 프로세스의 종결은 호출 함수 또는 메인 함수로의 함수의 리턴에 대응한다.

[0074] [0062] 당업자들은 본원에서 개시된 양상들과 관련하여 설명되는 다양한 예시적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이 둘의 결합들로서 구현될 수 있음을 추가로 이해할 것이다. 하드웨어와 소프트웨어의 이러한 상호교환가능성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들은 일반적으로 이들의 기능의 관점에서 전술되었다. 이러한 기능이 하드웨어로서 구현되는지 또는 소프트웨어로서 구현되는지는 특정 애플리케이션 및 전체 시스템에 부과된 설계 제약들에 종속된다.

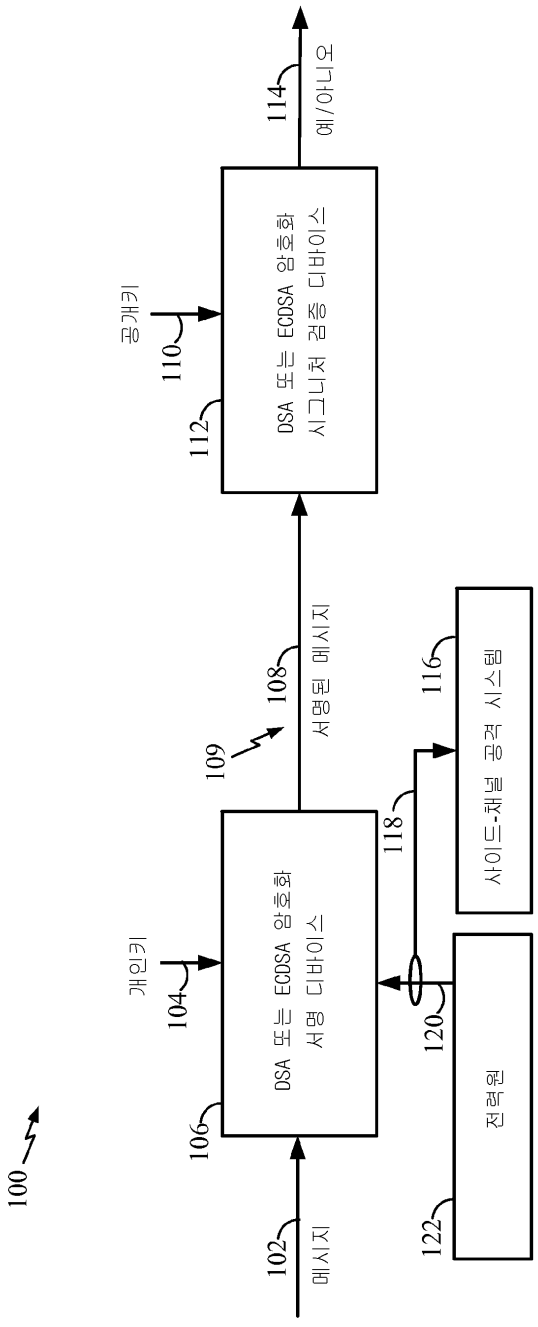
[0075] [0063] 본원에서 개시된 예들과 관련하여 설명된 방법들 또는 알고리즘들은 직접 하드웨어로, 프로세서에 의해 실행되는 소프트웨어 모듈로 또는 이들 둘의 결합으로, 프로세싱 유닛, 프로그래밍 명령들, 또는 다른 지시들의 형태로 구현될 수 있으며, 단일 디바이스에 포함되거나 또는 다수의 디바이스들에 걸쳐 분산될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드디스크, 착탈식 디스크, CD-ROM, 또는 당해 기술분야에 알려진 임의의 다른 형태의 저장 매체에 상주할 수 있다. 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있도록 프로세서에 커플링될 수 있다. 대안적으로, 저장 매체는 프로세서와 일체화될 수 있다.

[0076] [0064] 본원에서 설명된 본 발명의 다양한 특징들은, 본 발명으로부터 벗어남이 없이 상이한 시스템들로 구현될 수 있다. 전술한 실시예들은 단지 예시들이며 본 발명을 제한하는 것으로서 해석되지 않아야 한다는 것을 주목해야 한다. 실시예들의 설명은 청구항들의 범위를 제한하는 것이 아니라 예시하도록 의도된다. 이와 같이, 본

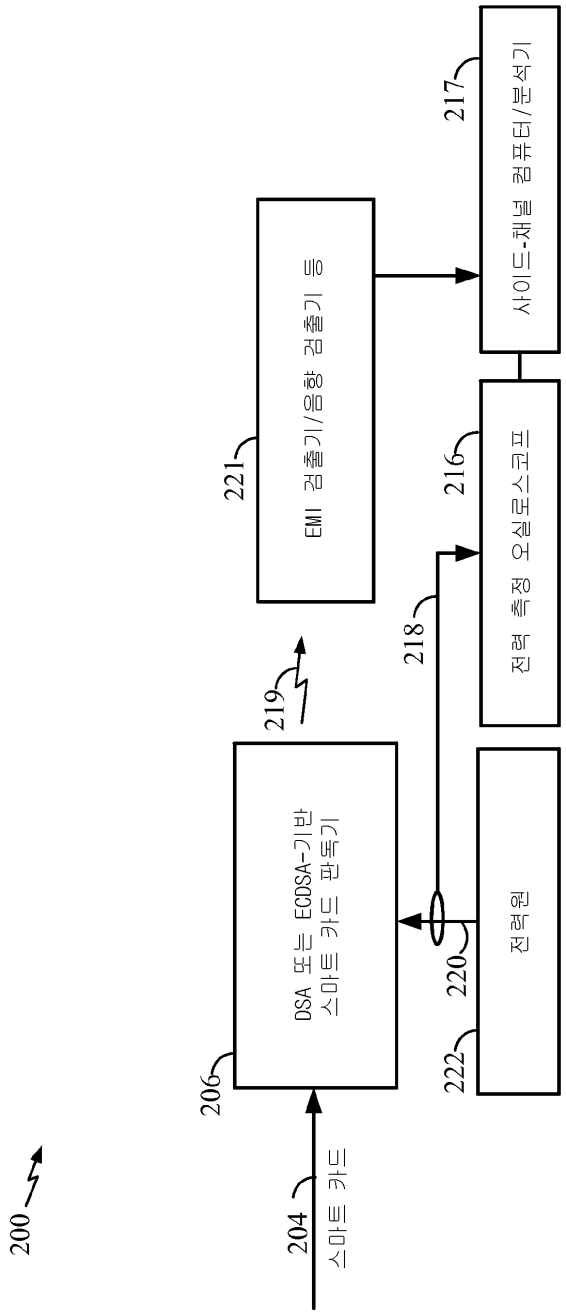
교시들은 다른 타입들의 장치들에 쉽게 적용될 수 있으며, 수많은 대안들, 변형들, 및 변화들이 당업자들에게 명백해질 것이다.

도면

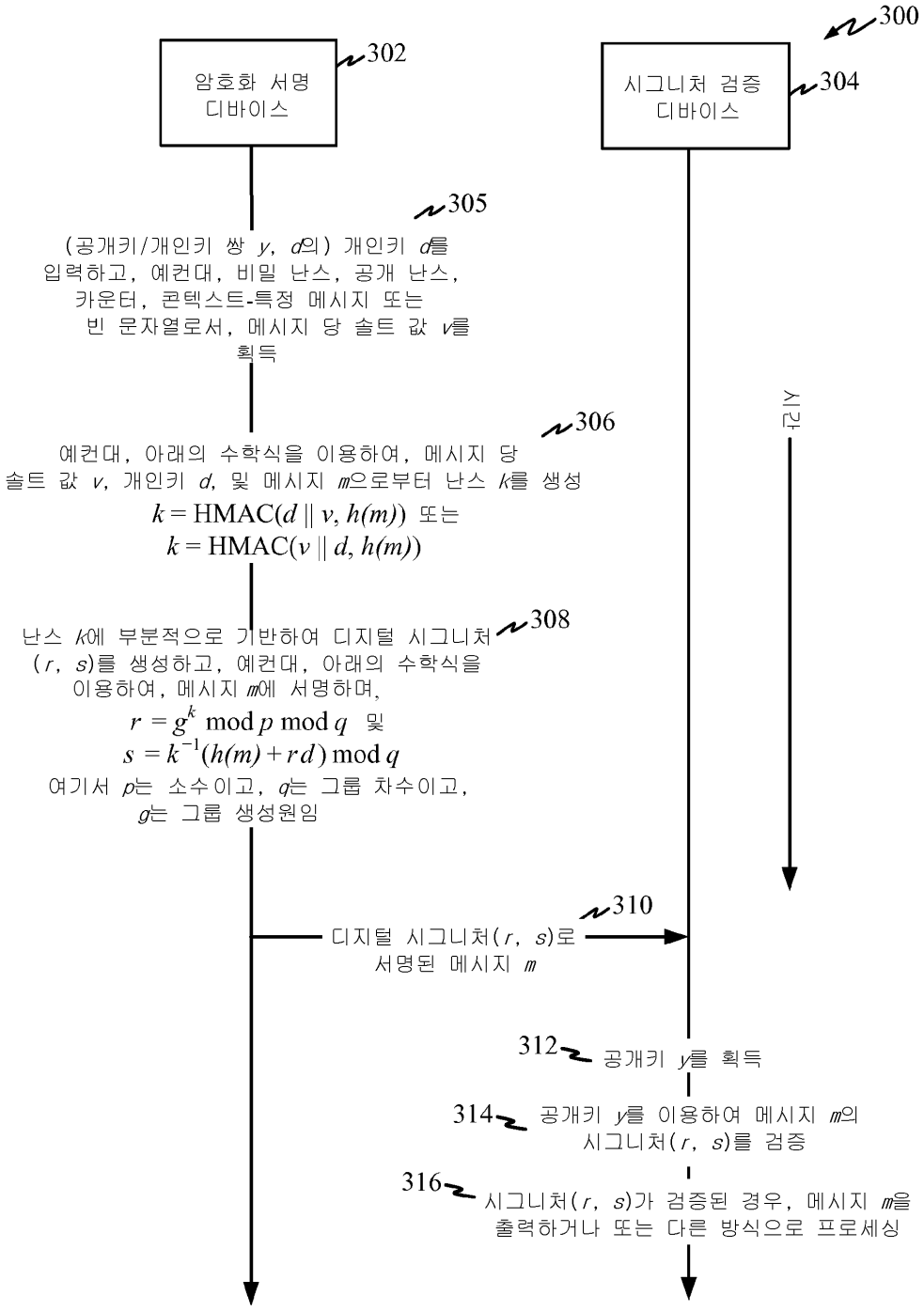
도면1



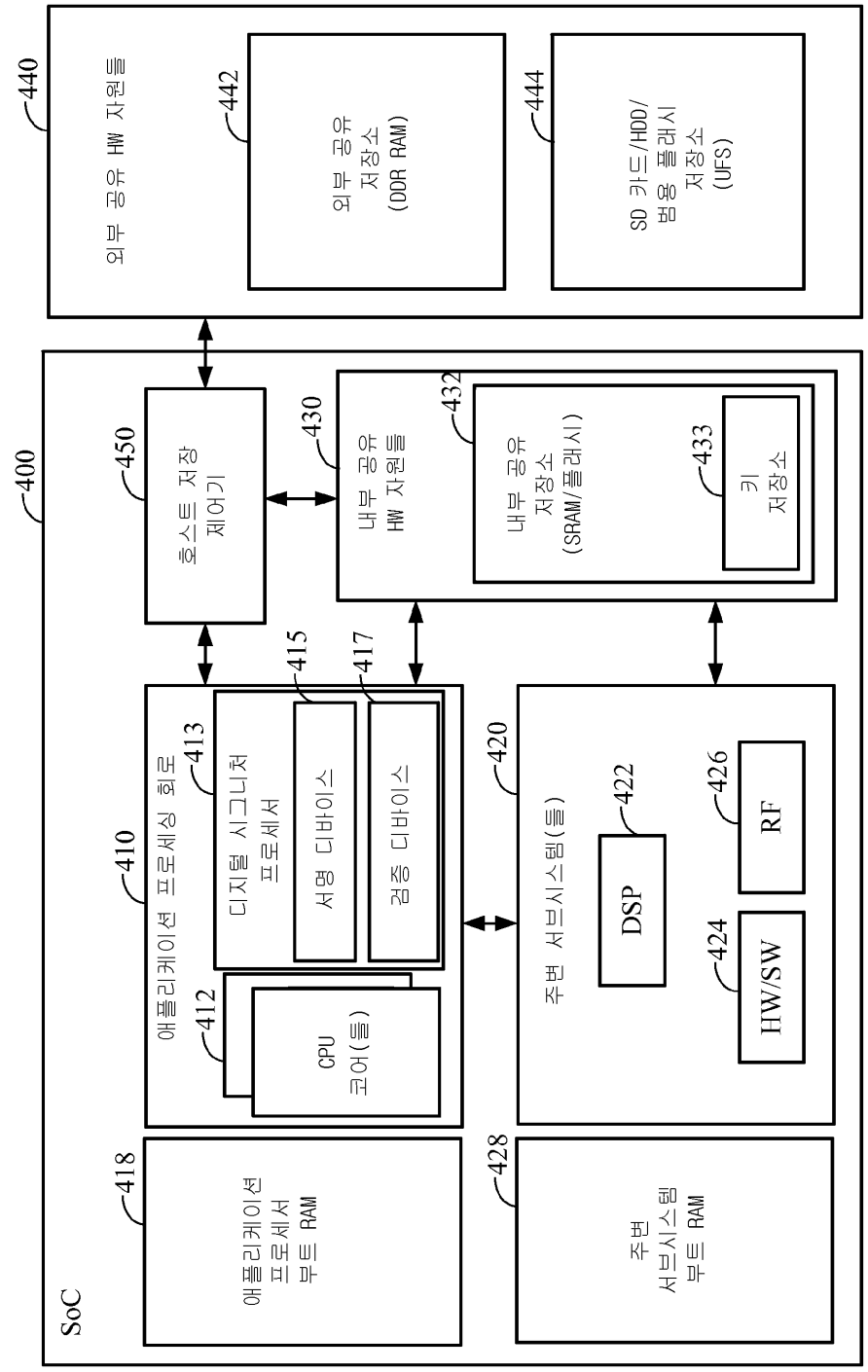
도면2


200
204
스마트 카드
206
DSA 또는 ECDSA-기반
스마트 카드 판독기
219
221
EMI 검출기/음향 검출기 등
217
사이드-채널 컴퓨터/분석기
216
전력 측정 오실로스코프
218
220
전력원
222

도면3

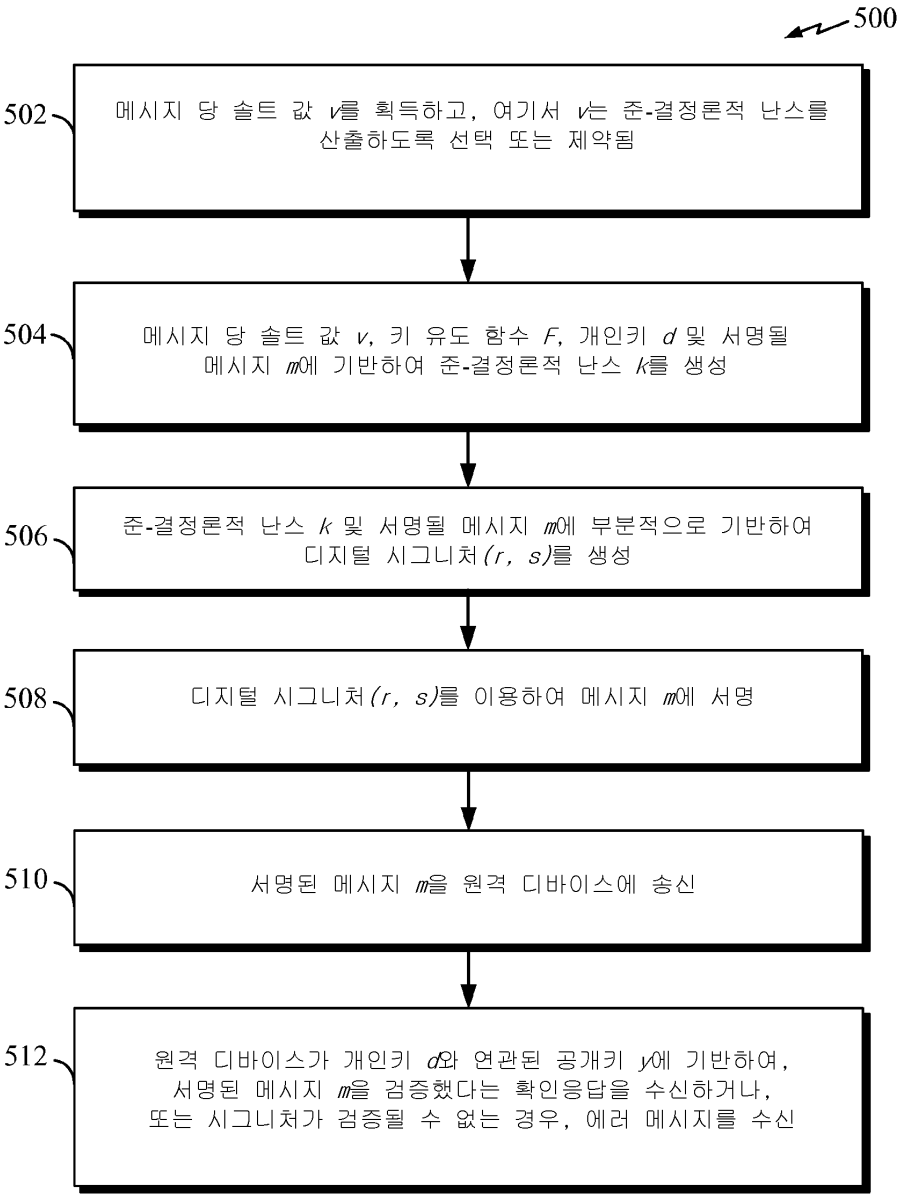

300
암호화 서명 디바이스
302
시그니처 검증 디바이스
304
305
(공개키/개인키 쌍 y, d의) 개인키 d를 입력하고, 예컨대, 비밀 난스, 공개 난스, 카운터, 콘텍스트-특정 메시지 또는 빈 문자열로서, 메시지 당 솔트 값 v를 획득
306
예컨대, 아래의 수학식을 이용하여, 메시지 당 솔트 값 v, 개인키 d, 및 메시지 m으로부터 난스 k를 생성
$k = \mathrm{HMAC}(d \,||\, v, h(m))$ 또는
$k = \mathrm{HMAC}(v \,||\, d, h(m))$
308
난스 k에 부분적으로 기반하여 디지털 시그니처 (r, s)를 생성하고, 예컨대, 아래의 수학식을 이용하여, 메시지 m에 서명하며,
$r = g^k \bmod p \bmod q$ 및
$s = k^{-1}(h(m) + rd) \bmod q$
여기서 p는 소수이고, q는 그룹 차수이고, g는 그룹 생성원임
시간
310
디지털 시그니처(r, s)로 서명된 메시지 m
312
공개키 y를 획득
314
공개키 y를 이용하여 메시지 m의 시그니처(r, s)를 검증
316
시그니처(r, s)가 검증된 경우, 메시지 m을 출력하거나 또는 다른 방식으로 프로세싱

도면4

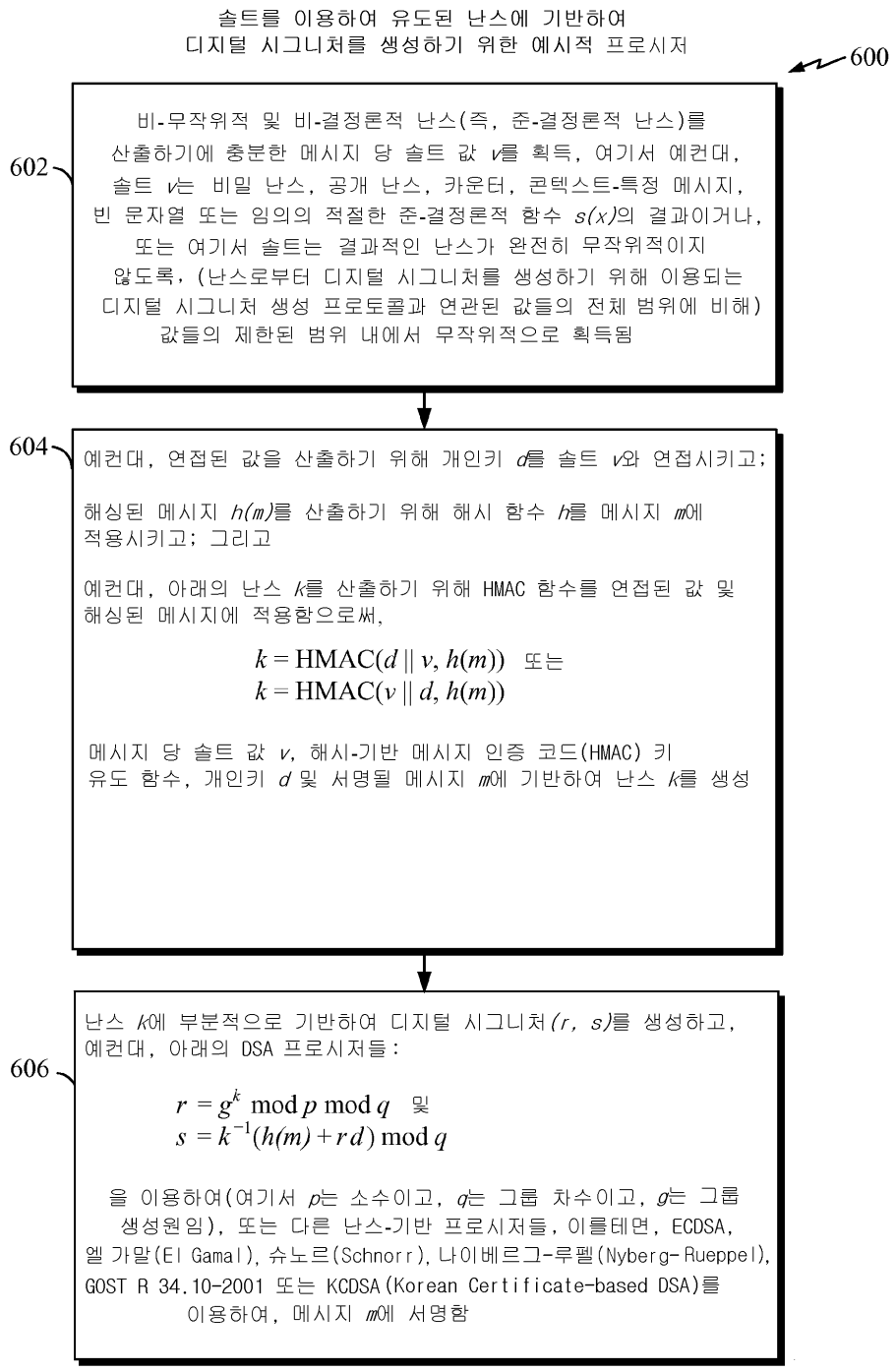

440
외부 공유 HW 자원들
442
외부 공유
저장소
(DDR RAM)
444
SD 카드/HDD/
범용 플래시
저장소
(UFS)
400
450
호스트 저장
제어기
430
내부 공유
HW 자원들
432
내부 공유
저장소
(SRAM/플래시)
433
키
저장소
415
417
410
애플리케이션 프로세싱 회로
413
디지털 시그니처
프로세서
서명 디바이스
검증 디바이스
412
CPU
코어(들)
420
주변 서브시스템(들)
422
DSP
426
RF
424
HW/SW
418
애플리케이션
프로세서
부트 RAM
428
주변
서브시스템
부트 RAM
SoC

도면5

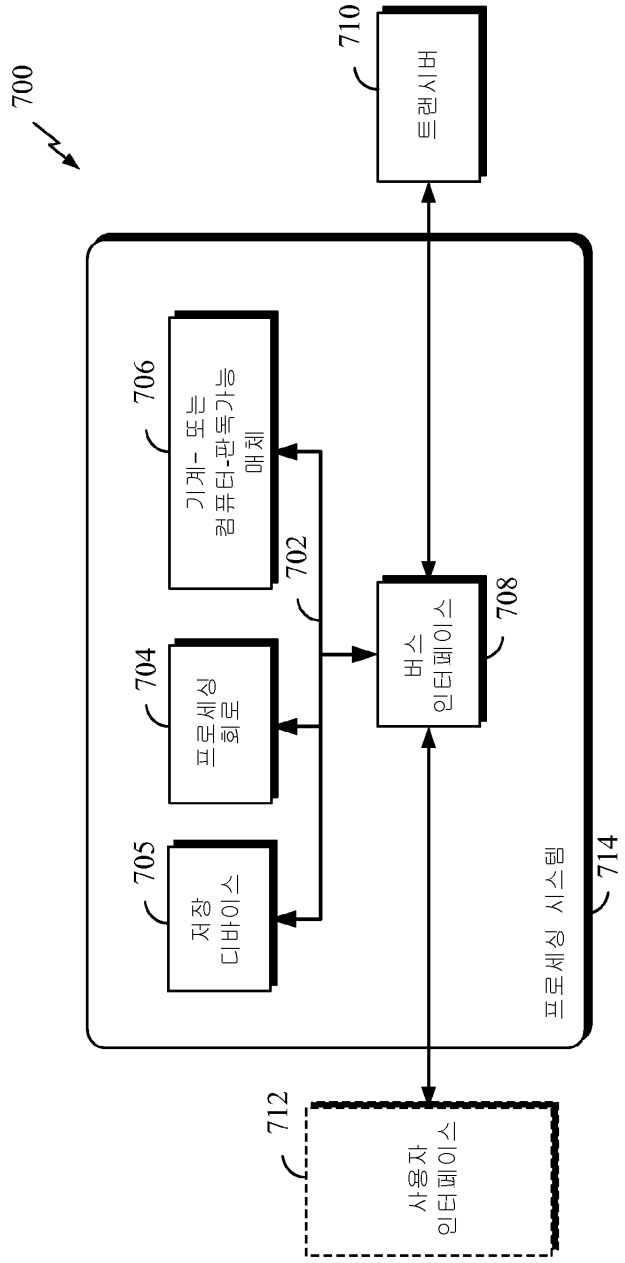
솔트를 이용하여 유도된 난스에 기반한 디지털 시그니처 프로세싱의 예



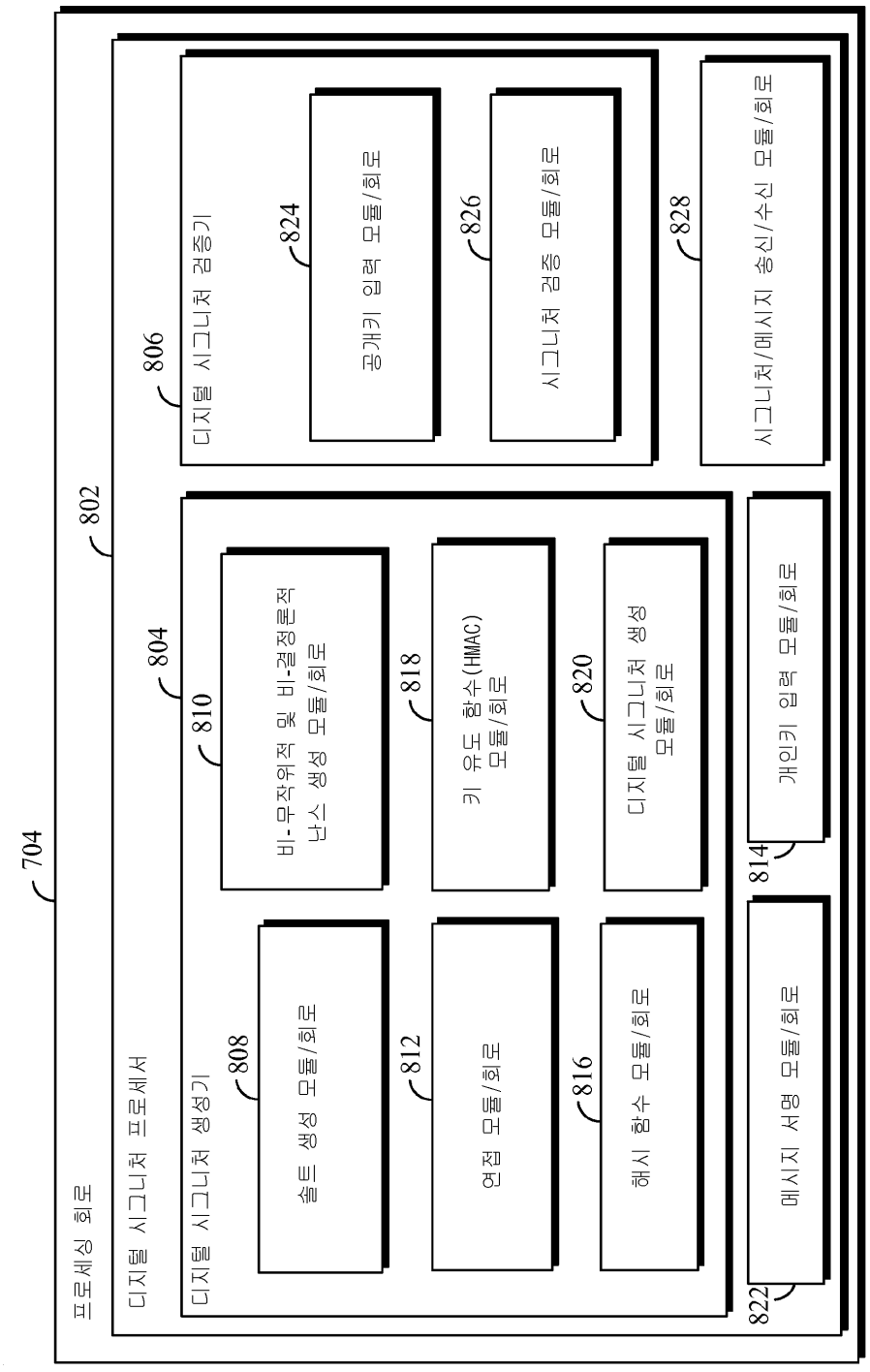
도면6


솔트를 이용하여 유도된 난스에 기반하여
디지털 시그니처를 생성하기 위한 예시적 프로시저
600
602
비-무작위적 및 비-결정론적 난스(즉, 준-결정론적 난스)를 산출하기에 충분한 메시지 당 솔트 값 v를 획득, 여기서 예컨대, 솔트 v는 비밀 난스, 공개 난스, 카운터, 콘텍스트-특정 메시지, 빈 문자열 또는 임의의 적절한 준-결정론적 함수 s(x)의 결과이거나, 또는 여기서 솔트는 결과적인 난스가 완전히 무작위적이지 않도록, (난스로부터 디지털 시그니처를 생성하기 위해 이용되는 디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해) 값들의 제한된 범위 내에서 무작위적으로 획득됨
604
예컨대, 연접된 값을 산출하기 위해 개인키 d를 솔트 v와 연접시키고;
해싱된 메시지 h(m)를 산출하기 위해 해시 함수 h를 메시지 m에 적용시키고; 그리고
예컨대, 아래의 난스 k를 산출하기 위해 HMAC 함수를 연접된 값 및 해싱된 메시지에 적용함으로써,
$k = \mathrm{HMAC}(d \,||\, v, h(m))$ 또는
$k = \mathrm{HMAC}(v \,||\, d, h(m))$
메시지 당 솔트 값 v, 해시-기반 메시지 인증 코드(HMAC) 키 유도 함수, 개인키 d 및 서명될 메시지 m에 기반하여 난스 k를 생성
606
난스 k에 부분적으로 기반하여 디지털 시그니처(r, s)를 생성하고, 예컨대, 아래의 DSA 프로시저들:
$r = g^k \bmod p \bmod q$ 및
$s = k^{-1}(h(m) + rd) \bmod q$
을 이용하여(여기서 p는 소수이고, q는 그룹 차수이고, g는 그룹 생성원임), 또는 다른 난스-기반 프로시저들, 이를테면, ECDSA, 엘 가말(El Gamal), 슈노르(Schnorr), 나이베르그-루펠(Nyberg-Rueppel), GOST R 34.10-2001 또는 KCDSA(Korean Certificate-based DSA)를 이용하여, 메시지 m에 서명함

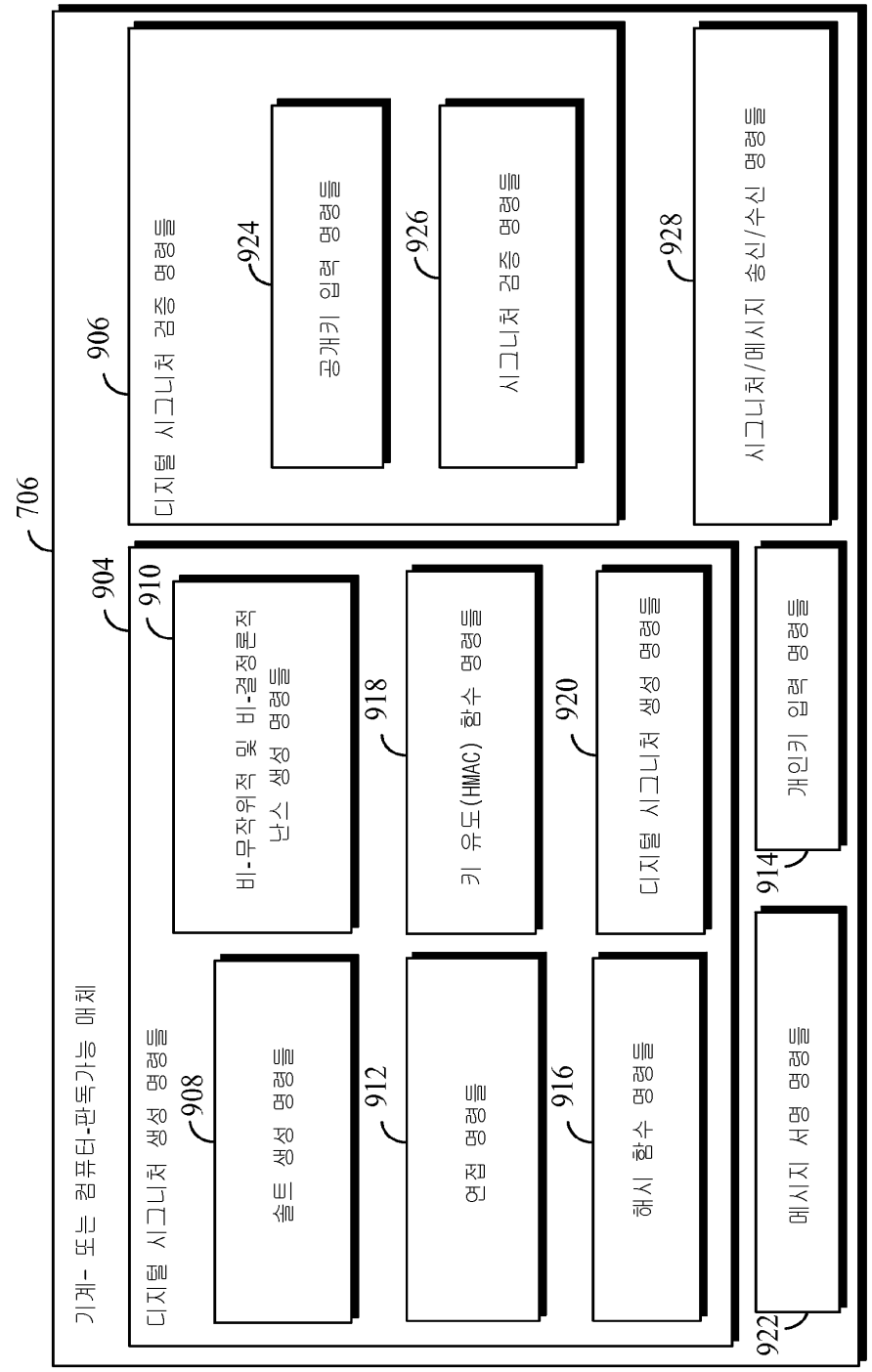
도면7


700
710
트랜시버
706
기계- 또는
컴퓨터-판독가능
매체
702
704
프로세싱
회로
708
버스
인터페이스
705
저장
디바이스
714
프로세싱 시스템
712
사용자
인터페이스

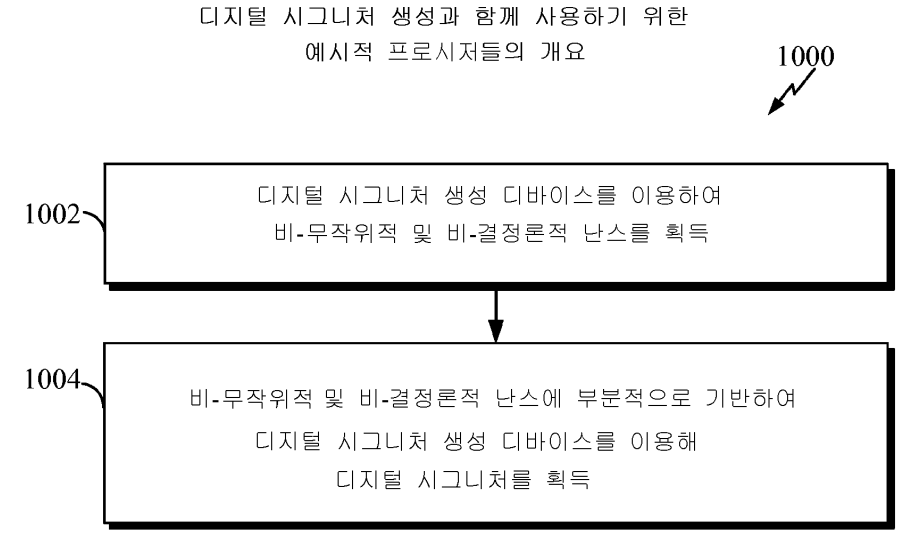
도면8


704
프로세싱 회로
802
디지털 시그니처 프로세서
804
디지털 시그니처 생성기
808
솔트 생성 모듈/회로
810
비-무작위적 및 비-결정론적 난스 생성 모듈/회로
812
연접 모듈/회로
816
해시 함수 모듈/회로
818
키 유도 함수(HMAC) 모듈/회로
820
디지털 시그니처 생성 모듈/회로
814
개인키 입력 모듈/회로
822
메시지 서명 모듈/회로
806
디지털 시그니처 검증기
824
공개키 입력 모듈/회로
826
시그니처 검증 모듈/회로
828
시그니처/메시지 송신/수신 모듈/회로

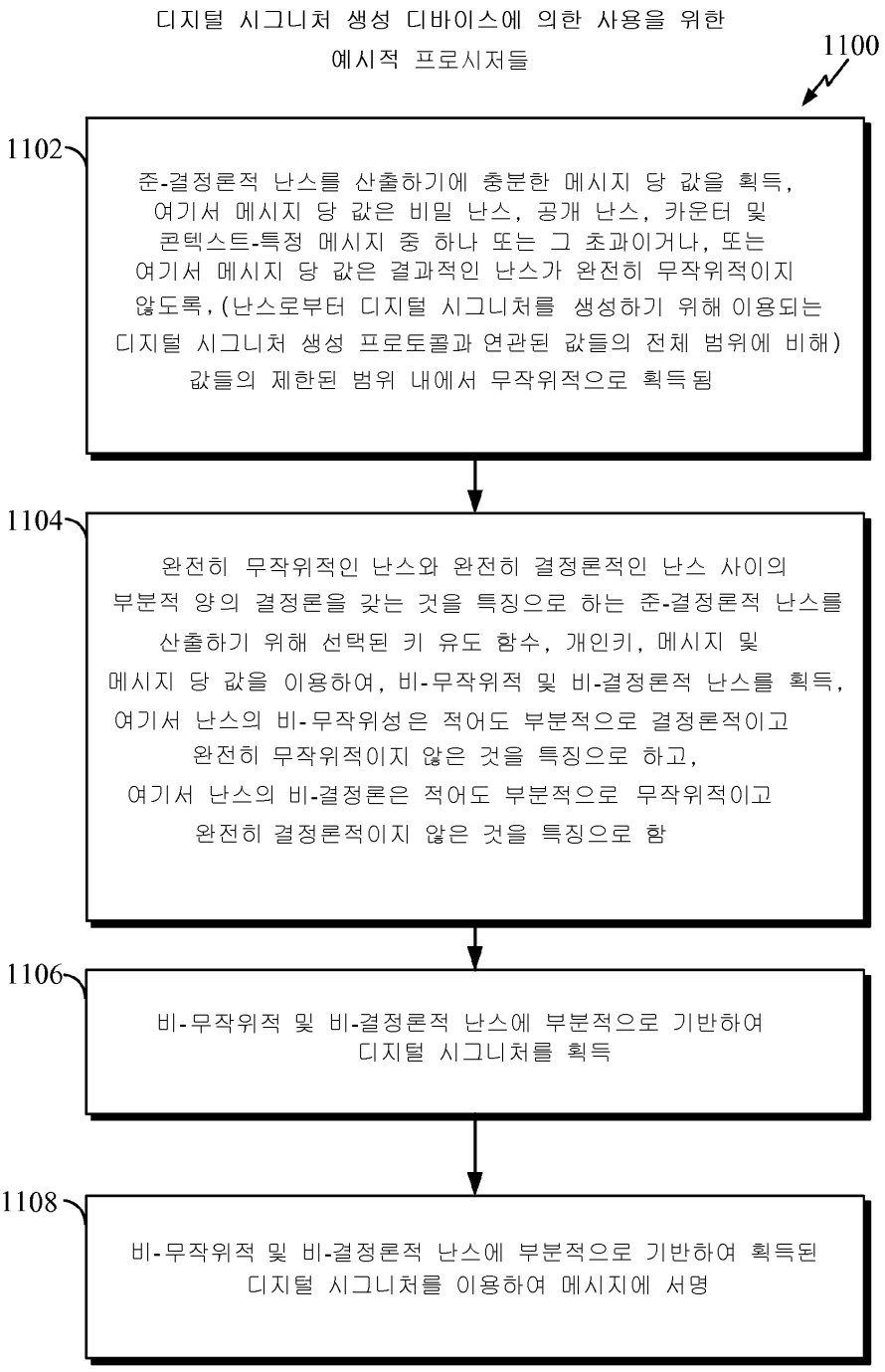
도면9


706
기계- 또는 컴퓨터-판독가능 매체
904
디지털 시그니처 생성 명령들
908
솔트 생성 명령들
910
비-무작위적 및 비-결정론적 난스 생성 명령들
912
연접 명령들
916
해시 함수 명령들
918
키 유도(HMAC) 함수 명령들
920
디지털 시그니처 생성 명령들
922
메시지 서명 명령들
914
개인키 입력 명령들
906
디지털 시그니처 검증 명령들
924
공개키 입력 명령들
926
시그니처 검증 명령들
928
시그니처/메시지 송신/수신 명령들

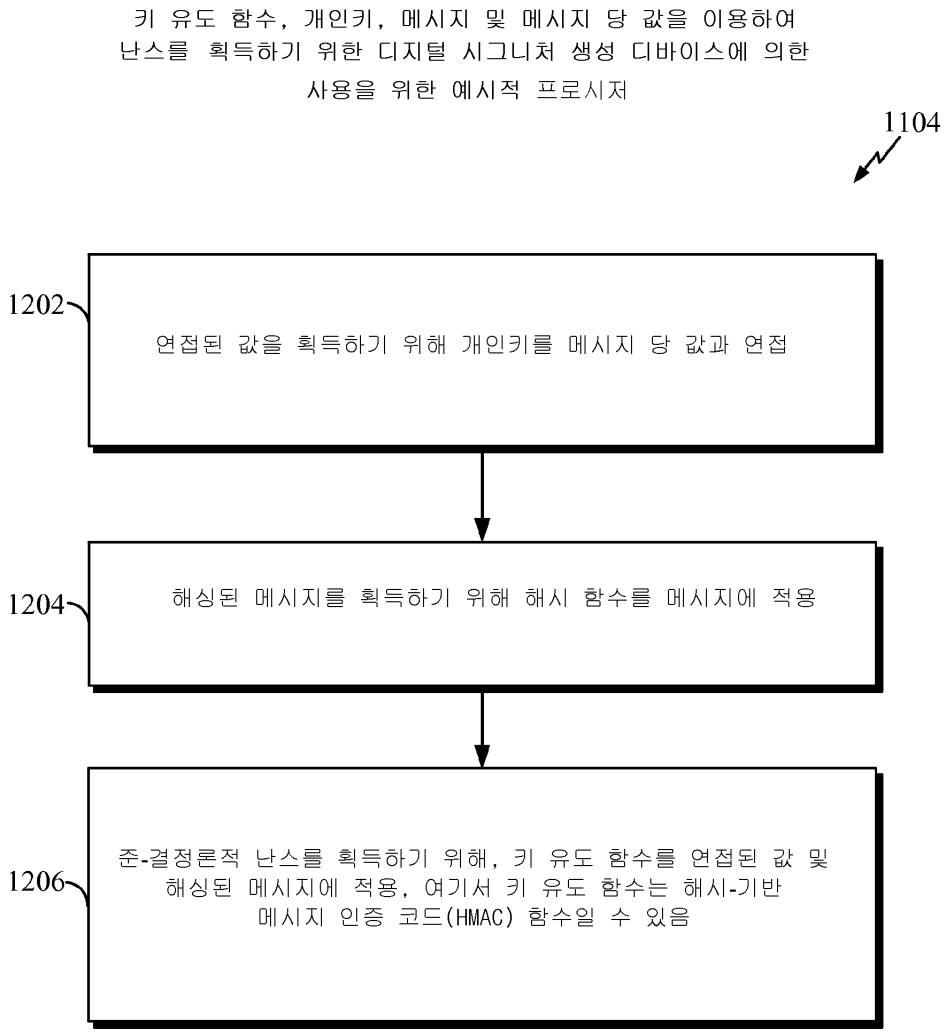
도면10


디지털 시그니처 생성과 함께 사용하기 위한
예시적 프로시저들의 개요
1000
1002
디지털 시그니처 생성 디바이스를 이용하여
비-무작위적 및 비-결정론적 난스를 획득
1004
비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여
디지털 시그니처 생성 디바이스를 이용해
디지털 시그니처를 획득

도면11


디지털 시그니처 생성 디바이스에 의한 사용을 위한
예시적 프로시저들
1100
1102
준-결정론적 난스를 산출하기에 충분한 메시지 당 값을 획득,
여기서 메시지 당 값은 비밀 난스, 공개 난스, 카운터 및
콘텍스트-특정 메시지 중 하나 또는 그 초과이거나, 또는
여기서 메시지 당 값은 결과적인 난스가 완전히 무작위적이지
않도록,(난스로부터 디지털 시그니처를 생성하기 위해 이용되는
디지털 시그니처 생성 프로토콜과 연관된 값들의 전체 범위에 비해)
값들의 제한된 범위 내에서 무작위적으로 획득됨
1104
완전히 무작위적인 난스와 완전히 결정론적인 난스 사이의
부분적 양의 결정론을 갖는 것을 특징으로 하는 준-결정론적 난스를
산출하기 위해 선택된 키 유도 함수, 개인키, 메시지 및
메시지 당 값을 이용하여, 비-무작위적 및 비-결정론적 난스를 획득,
여기서 난스의 비-무작위성은 적어도 부분적으로 결정론적이고
완전히 무작위적이지 않은 것을 특징으로 하고,
여기서 난스의 비-결정론은 적어도 부분적으로 무작위적이고
완전히 결정론적이지 않은 것을 특징으로 함
1106
비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여
디지털 시그니처를 획득
1108
비-무작위적 및 비-결정론적 난스에 부분적으로 기반하여 획득된
디지털 시그니처를 이용하여 메시지에 서명

도면12


키 유도 함수, 개인키, 메시지 및 메시지 당 값을 이용하여 난스를 획득하기 위한 디지털 시그니처 생성 디바이스에 의한 사용을 위한 예시적 프로시저
1104
1202
연접된 값을 획득하기 위해 개인키를 메시지 당 값과 연접
1204
해싱된 메시지를 획득하기 위해 해시 함수를 메시지에 적용
1206
준-결정론적 난스를 획득하기 위해, 키 유도 함수를 연접된 값 및 해싱된 메시지에 적용, 여기서 키 유도 함수는 해시-기반 메시지 인증 코드(HMAC) 함수일 수 있음