

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0142689

(43) 공개일자 2020년12월23일

(51) 국제특허분류(Int. Cl.)

H04L 25/03 (2006.01) H04L 1/00 (2006.01)

H04L 25/497 (2006.01) H04L 9/32 (2006.01)

(52) CPC특허분류

H04L 25/03343 (2013.01)

H04L 1/0042 (2013.01)

(21) 출원번호 10-2019-0069772

(22) 출원일자 2019년06월13일

심사청구일자 2019년06월13일

(71) 출원인

조선대학교산학협력단

광주광역시 동구 필문대로 309 (서석동)

(72) 발명자

김영식

광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호

(74) 대리인

김효성

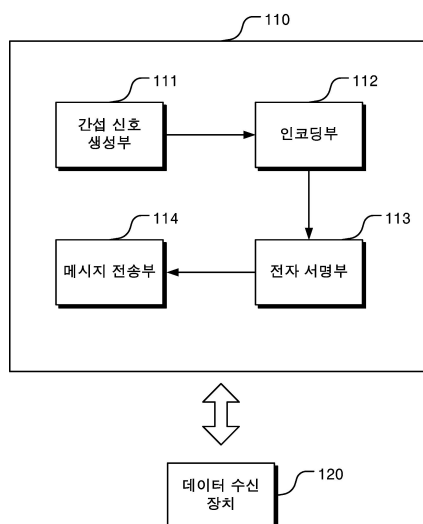
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치 및 그 동작 방법

(57) 요약

더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치 및 그 동작 방법이 개시된다. 본 발명은 데이터 수신 장치로 전송할 원본 메시지에 대한 전자 서명 값으로 소정의 더티 페이퍼 코딩(Dirty Paper Coding: DPC) 메시지를 의도적으로 생성하는 기법을 제시함으로써, 기존의 비대칭키 기반의 전자 서명 기법과 전혀 다른 알고리즘을 가지면서 보안성이 강화된 전자 서명 기법을 제공할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 1/0047 (2013.01)

H04L 25/4975 (2013.01)

H04L 9/3247 (2013.01)

H04L 9/3263 (2013.01)

H04L 2209/34 (2013.01)

H04L 2209/56 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711083493

부처명 과학기술정보통신부

과제관리(전문)기관명 정보통신기획평가원

연구사업명 정보보호핵심원천기술개발(R&D)

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

구

기 여 율 1/1

과제수행기관명 서울대학교 산학협력단

연구기간 2019.01.01 ~ 2019.12.31

명세서

청구범위

청구항 1

데이터 수신 장치로 전송할 원본 메시지와 기설정된(predetermined) 개인키를 기초로 더티 페이퍼 코딩(Dirty Paper Coding: DPC)에 사용될 간섭 신호를 생성하는 간섭 신호 생성부;

랜덤 값을 랜덤하게 생성하고, $(-1, 1]$ 사이에서 균일한 값을 가지는 디터(dither) 신호를 생성하기 위한 기설정된 제1 해시 함수에 상기 원본 메시지와 상기 랜덤 값을 입력으로 인가하여 제1 디터 신호를 생성한 후 상기 랜덤 값을 DPC에서의 전송 신호로 취급하여, 기설정된 최소 평균제곱오차(Minimum Mean Square Error: MMSE)와 상기 간섭 신호 및 상기 제1 디터 신호를 기초로 상기 랜덤 값에 대해 인코딩을 수행함으로써, 인코딩 메시지를 생성하는 인코딩부;

가우시안 분포에 따른 잡음 신호를 랜덤하게 생성하고, 상기 인코딩 메시지에 상기 간섭 신호와 상기 잡음 신호를 추가하여 DPC 메시지를 생성한 후 상기 DPC 메시지와 상기 제1 디터 신호를 전자 서명 값으로 결정하는 전자 서명부; 및

상기 원본 메시지를 상기 데이터 수신 장치로 전송하면서, 상기 전자 서명 값으로 결정된 상기 DPC 메시지와 상기 제1 디터 신호를 상기 데이터 수신 장치로 전송하는 메시지 전송부

를 포함하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치.

청구항 2

제1항에 있어서,

상기 간섭 신호 생성부는

상기 원본 메시지를 기설정된 제2 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 개인키와 상기 해시 값을 기설정된 난수 생성 함수에 입력으로 인가하여 상기 간섭 신호를 생성하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치.

청구항 3

제1항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 MMSE를 상기 개인키에 대응하는 공개키로 저장하고 있음과 동시에 상기 제1 해시 함수를 저장하고 있고, 상기 데이터 전송 장치로부터 상기 원본 메시지와 상기 전자 서명 값으로 결정된 상기 DPC 메시지 및 상기 제1 디터 신호가 수신되면, 상기 수신된 제1 디터 신호와 상기 메모리 상에 저장되어 있는 상기 MMSE를 기초로 상기 수신된 DPC 메시지에 대해 DPC 기반의 디코딩을 수행하여 상기 랜덤 값을 복원한 후 상기 메모리 상에 저장되어 있는 상기 제1 해시 함수에 상기 수신된 원본 메시지와 상기 복원된 랜덤 값을 입력으로 인가하여 검증용 디터 신호를 생성하고, 상기 검증용 디터 신호가 상기 수신된 제1 디터 신호와 일치하는지 여부를 확인함으로써, 상기 전자 서명 값에 대한 검증을 수행하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치.

청구항 4

제3항에 있어서,

상기 인코딩부는

하기의 수학식 1의 연산에 기초하여 상기 인코딩 메시지를 생성하고,

상기 전자 서명부는

하기의 수학식 2의 연산에 기초하여 상기 DPC 메시지를 생성하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한

데이터 전송 장치.

[수학식 1]

$$X = (R - \alpha S - U) \bmod 2Z$$

상기 수학식 1에서, X 는 상기 인코딩 메시지로, R 은 상기 랜덤 값, α 는 상기 MMSE, S 는 상기 간섭 신호, U 는 상기 제1 디터 신호를 의미하며, Z 는 가우시안 분포를 갖는 정수 집합을 의미함.

[수학식 2]

$$Y = X + S + Z$$

상기 수학식 2에서, Y 는 상기 DPC 메시지로, X 는 상기 인코딩 메시지, S 는 상기 간섭 신호, Z 는 상기 잡음 신호를 의미함.

청구항 5

제4항에 있어서,

상기 데이터 수신 장치는

상기 DPC 기반의 디코딩을 수행하기 위해, 하기의 수학식 3의 연산에 기초하여 디코딩 메시지를 생성한 후 상기 디코딩 메시지로부터 상기 랜덤 값을 복원하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치.

[수학식 3]

$$Y' = (\alpha Y + U) \bmod 2Z$$

상기 수학식 3에서, Y' 는 상기 디코딩 메시지, α 는 상기 메모리 상에 저장되어 있는 상기 MMSE, Y 는 상기 수신된 DPC 메시지, U 는 상기 수신된 제1 디터 신호를 의미하며, Z 는 가우시안 분포를 갖는 정수 집합을 의미함.

청구항 6

데이터 수신 장치로 전송할 원본 메시지와 기설정된(predetermined) 개인키를 기초로 더티 페이퍼 코딩(Dirty Paper Coding: DPC)에 사용될 간섭 신호를 생성하는 단계;

랜덤 값을 랜덤하게 생성하고, $(-1, 1]$ 사이에서 균일한 값을 가지는 디터(dither) 신호를 생성하기 위한 기설정된 제1 해시 함수에 상기 원본 메시지와 상기 랜덤 값을 입력으로 인가하여 제1 디터 신호를 생성한 후 상기 랜덤 값을 DPC에서의 전송 신호로 취급하여, 기설정된 최소 평균제곱오차(Minimum Mean Square Error: MMSE)와 상기 간섭 신호 및 상기 제1 디터 신호를 기초로 상기 랜덤 값에 대해 인코딩을 수행함으로써, 인코딩 메시지를 생성하는 단계;

가우시안 분포에 따른 잡음 신호를 랜덤하게 생성하고, 상기 인코딩 메시지에 상기 간섭 신호와 상기 잡음 신호를 부가하여 DPC 메시지를 생성한 후 상기 DPC 메시지와 상기 제1 디터 신호를 전자 서명 값으로 결정하는 단계; 및

상기 원본 메시지를 상기 데이터 수신 장치로 전송하면서, 상기 전자 서명 값으로 결정된 상기 DPC 메시지와 상기 제1 디터 신호를 상기 데이터 수신 장치로 전송하는 단계

를 포함하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법.

청구항 7

제6항에 있어서,

상기 간섭 신호를 생성하는 단계는

상기 원본 메시지를 기설정된 제2 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 개인키와 상기 해시 값을 기설정된 난수 생성 함수에 입력으로 인가하여 상기 간섭 신호를 생성하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법.

청구항 8

제6항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 MMSE를 상기 개인키에 대응하는 공개키로 저장하고 있음과 동시에 상기 제1 해시 함수를 저장하고 있고, 상기 데이터 전송 장치로부터 상기 원본 메시지와 상기 전자 서명 값으로 결정된 상기 DPC 메시지 및 상기 제1 디터 신호가 수신되면, 상기 수신된 제1 디터 신호와 상기 메모리 상에 저장되어 있는 상기 MMSE를 기초로 상기 수신된 DPC 메시지에 대해 DPC 기반의 디코딩을 수행하여 상기 랜덤 값을 복원한 후 상기 메모리 상에 저장되어 있는 상기 제1 해시 함수에 상기 수신된 원본 메시지와 상기 복원된 랜덤 값을 입력으로 인가하여 검증용 디터 신호를 생성하고, 상기 검증용 디터 신호가 상기 수신된 제1 디터 신호와 일치하는지 여부를 확인함으로써, 상기 전자 서명 값에 대한 검증을 수행하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법.

청구항 9

제8항에 있어서,

상기 인코딩 메시지를 생성하는 단계는

하기의 수학식 1의 연산에 기초하여 상기 인코딩 메시지를 생성하고,

상기 전자 서명 값으로 결정하는 단계는

하기의 수학식 2의 연산에 기초하여 상기 DPC 메시지를 생성하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법.

[수학식 1]

$$X = (R - \alpha S - U) \bmod 2Z$$

상기 수학식 1에서, X 는 상기 인코딩 메시지로, R 은 상기 랜덤 값, α 는 상기 MMSE, S 는 상기 간섭 신호, U 는 상기 제1 디터 신호를 의미하며, Z 는 가우시안 분포를 갖는 정수 집합을 의미함.

[수학식 2]

$$Y = X + S + Z$$

상기 수학식 2에서, Y 는 상기 DPC 메시지로, X 는 상기 인코딩 메시지, S 는 상기 간섭 신호, Z 는 상기 잡음 신호를 의미함.

청구항 10

제9항에 있어서,

상기 데이터 수신 장치는

상기 DPC 기반의 디코딩을 수행하기 위해, 하기의 수학식 3의 연산에 기초하여 디코딩 메시지를 생성한 후 상기 디코딩 메시지로부터 상기 랜덤 값을 복원하는 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법.

[수학식 3]

$$Y' = (\alpha Y + U) \bmod 2Z$$

상기 수학식 3에서, Y' 는 상기 디코딩 메시지, α 는 상기 메모리 상에 저장되어 있는 상기 MMSE, Y 는 상기 수신된 DPC 메시지, U 는 상기 수신된 제1 디터 신호를 의미하며, Z 는 가우시안 분포를 갖는 정수 집합을 의미함.

청구항 11

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 더티 페이퍼 코딩(Dirty Paper Coding: DPC)을 이용한 새로운 방식의 전자 서명 기술에 대한 것이다.

배경 기술

[0002] 최근, 인터넷이 널리 보급됨에 따라, 온라인을 이용한 बैंक 서비스나 결제 시스템의 도입이 활발하게 이루어지고 있다.

[0003] 이러한 온라인 बैंक 서비스나 결제 시스템에서는 계좌 이체나 전자 결제를 하고자 하는 진정한 사람으로부터 계좌 이체 또는 전자 결제 요청이 있는지 여부를 정확하게 판단해야 할 필요가 있다.

[0004] 예컨대, A라는 사용자가 온라인 बैंक 서비스를 통해서 B라는 사용자에게 계좌 이체를 한다고 했을 때, 온라인 बैंक 서비스를 제공하는 시스템에서는 해당 계좌 이체 요청이 A라는 사용자에게 의해서 정말로 이루어진 것인지를 확인해야 할 필요가 있다.

[0005] 보통, 일반적인 온라인 बैंक 서비스나 결제 시스템에서 도입하고 있는 사용자 확인 서비스는 공개키 기반의 암호화 방식(Public Key Infrastructure: PKI)을 이용한 전자 서명 시스템이 주를 이루고 있다.

[0006] 공개키 기반의 암호화 방식의 전자 서명 시스템이란 메시지를 전달하는 측에서 해당 메시지에 대한 해시 값에 대해 자신의 개인키로 암호화를 수행하여 전자 서명 값을 생성한 후 해당 메시지와 상기 전자 서명 값을 메시지 수신측에 전달하면, 메시지 수신측에서 상기 개인키에 대응하는 공개키로 상기 전자 서명 값을 복호화하고, 메시지 전송측으로부터 수신한 상기 메시지에 대한 해시 값을 연산한 후 상기 공개키로 복호화한 값과 상기 메시지에 대한 해시 값을 비교하여 두 값이 서로 동일한 것으로 판단되면, 메시지 전송측으로부터 수신된 상기 전자 서명 값이 상기 메시지 전송측의 개인키에 의해서 정말로 암호화된 값임이 입증됨에 따라, 상기 메시지가 진정한 메시지 전송측으로부터 전달된 메시지임을 확인하는 시스템이다.

[0007] 이러한 공개키 기반의 암호화 방식의 전자 서명 시스템은 개인키와 이에 대응하는 공개키를 생성한 후 상기 개인키로 전자 서명 값을 생성하고, 상기 공개키로 상기 전자 서명 값을 검증하는 형태로 운영되고 있다.

[0008] 기존의 전자 서명 생성 및 검증 알고리즘은 이미 관련 업계에서 널리 사용되고 있다는 점에서 전자 서명의 위변조 가능성이 높아 보안상 취약성을 가지고 있다.

[0009] 따라서, 기존의 전자 서명 생성 및 검증 알고리즘과 다른 새로운 방식의 전자 서명 생성 및 검증 알고리즘에 대한 연구가 필요한 상황이다.

[0010] 관련해서, 새로운 전자 서명 생성 및 검증 알고리즘으로, 통신에서 사용되고 있는 더티 페이퍼 코딩(Dirty Paper Coding: DPC)을 활용하는 방식을 고려해 볼 수 있다.

[0011] DPC는 1983년 Costa에 의해서 처음으로 제안된 것으로, 전송단과 수신단 사이의 채널에 간섭 신호가 존재하는 경우, 만일 전송단에서 간섭 신호를 미리 알고 있다면, 수신단에서 간섭 신호를 전혀 몰라도 간섭 신호의 영향을 제거할 수 있도록 지원하는 코딩 기법을 의미한다.

[0012] 관련해서, DPC에 대해 간단히 설명하면 다음과 같다.

[0013] 우선, 전송단에서 수신단으로 송신하는 원본 메시지를 W 라고 하고, 채널의 간섭 신호를 S 라고 하는 경우, 전송단에서는 W 에 대해 하기의 수학식 1의 연산에 따라 인코딩을 수행함으로써, 수신단으로 전송할 인코딩 메시지 X 를 생성할 수 있다.

수학식 1

[0015]
$$X = (W - \alpha S - U) \bmod 2Z$$

[0017] 상기 수학식 1에서 α 는 최소 평균제곱오차(Minimum Mean Square Error: MMSE)이고, U 는 $(-1, 1]$ 사이에서 균일한 값을 가지는 랜덤 디더(dither) 신호로 전송단과 수신단이 서로 공유하고 있는 값이며, Z 는 가우시안 분포를 갖는 정수 집합을 의미한다.

[0018] 전송단이 상기 인코딩 메시지 X 를 생성하여 수신단으로 전송하게 되면, 수신단에서 수신하는 수신 메시지 Y 는 상기 채널의 간섭 신호 S 와 소정의 잡음 신호 Z 가 상기 인코딩 메시지 X 에 부가되어 하기의 수학식 2와 같이 나타낼 수 있게 된다.

수학식 2

[0020]
$$Y = X + S + Z$$

[0022] 수신단이 상기 수학식 2에서 나타낸 바와 같은 수신 메시지 Y 를 수신하게 되면, 수신단은 하기의 수학식 3의 연산에 기초하여 디코딩을 수행함으로써, 디코딩 메시지 Y' 을 생성할 수 있다.

수학식 3

[0024]
$$\begin{aligned} Y' &= (\alpha Y + U) \bmod 2Z \\ &= [W - (1 - \alpha)U + \alpha Z] \bmod 2Z \end{aligned}$$

[0026] 상기 수학식 3에서 $-(1 - \alpha)U + \alpha Z$ 로 나타낸 부분이 노이즈 성분이며, 수신단은 상기 디코딩 메시지 Y' 로부터 원본 메시지를 W 를 복원할 수 있게 된다.

[0027] 이때, $-(1-\alpha)U + \alpha Z$ 로 나타낸 노이즈 성분이 최소화되어야 하기 때문에, 전송단과 수신단이 사용하는 상기 MMSE 값인 α 는 하기의 수학식 4의 연산을 만족하는 상수 값으로 선정되어야 한다.

수학식 4

[0029]

$$\alpha = \frac{P_X}{P_X + P_Z} = \frac{SNR}{1 + SNR}$$

[0031] 여기서, P_X 는 송신 신호의 파워, P_Z 는 잡음 신호의 파워를 의미한다.

[0032] 참고로, 상기 수학식 3에서 $(\alpha Y + U) \bmod 2Z$ 가 $[W - (1-\alpha)U + \alpha Z] \bmod 2Z$ 로 연산되는 과정은 하기의 수학식 5와 같은 연산에 따라 증명될 수 있다.

수학식 5

[0034]

$$\begin{aligned} Y' &= [\alpha Y + U] \bmod \Lambda \\ &= [w - w + \alpha X + \alpha S + \alpha Z + U] \bmod \Lambda \\ &= [w + \alpha X + (\alpha S + U - w) + \alpha Z] \bmod \Lambda \\ &= [w + \alpha X + (\alpha S + U - w) \bmod \Lambda + \alpha Z] \bmod \Lambda \\ &= [w + \alpha X + (-X) + \alpha Z] \bmod \Lambda \\ &= [w - (1-\alpha)X + \alpha Z] \bmod \Lambda \\ &= [w - (1-\alpha)U + \alpha Z] \bmod \Lambda \\ &= [w + Z'] \bmod \Lambda \end{aligned}$$

[0036] 상기 수학식 5에서 네 번째 등호의 연산은 임의의 a, b에 대해서 $(a + b) \bmod \Lambda = (a \bmod \Lambda + b) \bmod \Lambda$ 을 만족하는 성질을 이용한 것이고, 다섯 번째 등호의 연산은 상기 수학식 1에 따라 $-X = (\alpha S + U - w) \bmod \Lambda$ 로 표현될 수 있는 관계식을 이용해서 단순화시킨 것이며, 일곱 번째 등호의 연산은 전송단에서 디더 신호 U 가 사용되었기 때문에 인코딩 메시지 X 의 분포가 격자

Λ 의 기본 보로노이 영역에서 균일하다는 특성 및 인코딩 메시지 X 와 간섭 신호 S 가 독립적이라는 특성을 이용하여 등가 노이즈 Z' 를 계산함에 있어 X 를 U 로 대체한 것이다.

- [0037] 이렇게, DPC 방식의 데이터 전송 기법이 존재한다는 점에서, 본 발명에서는 이러한 DPC 방식의 알고리즘을 활용하여 보안성이 강화된 새로운 전자 서명 기법을 제시하고자 한다.

선행기술문헌

비특허문헌

- [0038] (비특허문헌 0001) 이영승, 정세영, "더티 페이퍼 코딩 기법에 대한 소개", Telecommunications Review, 제16권 5호, 2006년 10월, pp. 760-770 (11 pages)

발명의 내용

해결하려는 과제

- [0039] 본 발명은 데이터 수신 장치로 전송할 원본 메시지에 대한 전자 서명 값으로 소정의 더티 페이퍼 코딩(Dirty Paper Coding: DPC) 메시지를 의도적으로 생성하는 기법을 제시함으로써, 기존의 비대칭키 기반의 전자 서명 기법과 전혀 다른 알고리즘을 갖는 전자 서명 기법의 제안을 통해 전자 서명 과정에서 보안성을 강화할 수 있도록 한다.

과제의 해결 수단

- [0040] 본 발명의 일실시예에 따른 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치는 데이터 수신 장치로 전송할 원본 메시지와 기설정된(predetermined) 개인키를 기초로 더티 페이퍼 코딩(Dirty Paper Coding: DPC)에 사용될 간섭 신호를 생성하는 간섭 신호 생성부, 랜덤 값을 랜덤하게 생성하고, $(-1, 1]$ 사이에서 균일한 값을 가지는 디더(dither) 신호를 생성하기 위한 기설정된 제1 해시 함수에 상기 원본 메시지와 상기 랜덤 값을 입력으로 인가하여 제1 디더 신호를 생성한 후 상기 랜덤 값을 DPC에서의 전송 신호로 취급하여, 기설정된 최소 평균제곱오차(Minimum Mean Square Error: MMSE)와 상기 간섭 신호 및 상기 제1 디더 신호를 기초로 상기 랜덤 값에 대해 인코딩을 수행함으로써, 인코딩 메시지를 생성하는 인코딩부, 가우시안 분포에 따른 잡음 신호를 랜덤하게 생성하고, 상기 인코딩 메시지에 상기 간섭 신호와 상기 잡음 신호를 부가하여 DPC 메시지를 생성한 후 상기 DPC 메시지와 상기 제1 디더 신호를 전자 서명 값으로 결정하는 전자 서명부 및 상기 원본 메시지를 상기 데이터 수신 장치로 전송하면서, 상기 전자 서명 값으로 결정된 상기 DPC 메시지와 상기 제1 디더 신호를 상기 데이터 수신 장치로 전송하는 메시지 전송부를 포함한다.

- [0041] 또한, 본 발명의 일실시예에 따른 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법은 데이터 수신 장치로 전송할 원본 메시지와 기설정된 개인키를 기초로 DPC에 사용될 간섭 신호를 생성하는 단계, 랜덤 값을 랜덤하게 생성하고, $(-1, 1]$ 사이에서 균일한 값을 가지는 디더 신호를 생성하기 위한 기설정된 제1 해시 함수에 상기 원본 메시지와 상기 랜덤 값을 입력으로 인가하여 제1 디더 신호를 생성한 후 상기 랜덤 값을 DPC에서의 전송 신호로 취급하여, 기설정된 MMSE와 상기 간섭 신호 및 상기 제1 디더 신호를 기초로 상기 랜덤 값에 대해 인코딩을 수행함으로써, 인코딩 메시지를 생성하는 단계, 가우시안 분포에 따른 잡음 신호를 랜덤하게 생성하고, 상기 인코딩 메시지에 상기 간섭 신호와 상기 잡음 신호를 부가하여 DPC 메시지를 생성한 후 상기 DPC 메시지와 상기 제1 디더 신호를 전자 서명 값으로 결정하는 단계 및 상기 원본 메시지를 상기 데이터 수신 장치로 전송하면서, 상기 전자 서명 값으로 결정된 상기 DPC 메시지와 상기 제1 디더 신호를 상기 데이터 수신 장치로 전송하는 단계를 포함한다.

발명의 효과

- [0042] 본 발명은 데이터 수신 장치로 전송할 원본 메시지에 대한 전자 서명 값으로 소정의 더티 페이퍼 코딩(Dirty Paper Coding: DPC) 메시지를 의도적으로 생성하는 기법을 제시함으로써, 기존의 비대칭키 기반의 전자 서명 기법과 전혀 다른 알고리즘을 가지면서 보안성이 강화된 전자 서명 기법을 제공할 수 있다.

도면의 간단한 설명

[0043] 도 1은 본 발명의 일실시예에 따른 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0044] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0045] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0046] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0047] 도 1은 본 발명의 일실시예에 따른 더티 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 구조를 도시한 도면이다.

[0048] 도 1을 참조하면, 본 발명에 따른 데이터 전송 장치(110)는 간섭 신호 생성부(111), 인코딩부(112), 전자 서명부(113) 및 메시지 전송부(114)를 포함한다.

[0049] 간섭 신호 생성부(111)는 데이터 수신 장치(120)로 전송할 원본 메시지와 기설정된(predetermined) 개인키를 기초로 더티 페이퍼 코딩(Dirty Paper Coding: DPC)에 사용될 간섭 신호를 생성한다.

[0050] 이때, 본 발명의 일실시예에 따르면, 간섭 신호 생성부(111)는 상기 원본 메시지를 기설정된 제2 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 개인키와 상기 해시 값을 기설정된 난수 생성 함수에 입력으로 인가하여 상기 간섭 신호를 생성할 수 있다.

[0051] 인코딩부(112)는 랜덤 값을 랜덤하게 생성하고, $(-1, 1]$ 사이에서 균일한 값을 가지는 디더(dither) 신호를 생성하기 위한 기설정된 제1 해시 함수에 상기 원본 메시지와 상기 랜덤 값을 입력으로 인가하여 제1 디더 신호를 생성한 후 상기 랜덤 값을 DPC에서의 전송 신호로 취급하여, 기설정된 최소 평균제곱오차(Minimum Mean Square Error: MMSE)와 상기 간섭 신호 및 상기 제1 디더 신호를 기초로 상기 랜덤 값에 대해 인코딩을 수행함으로써, 인코딩 메시지를 생성한다.

[0052] 이때, 본 발명의 일실시예에 따르면, 인코딩부(112)는 하기의 수학식 6의 연산에 기초하여 상기 인코딩 메시지를 생성할 수 있다.

수학식 6

$$X = (R - \alpha S - U) \bmod 2Z$$

[0054]

[0056]

상기 수학식 6에서, X 는 상기 인코딩 메시지로, R 은 상기 랜덤 값, α 는 상기 MMSE, S 는 상기 간섭 신호, U 는 상기 제1 디터 신호를 의미하며, Z 는 가우시안 분포를 갖는 정수 집합을 의미한다.

[0057]

전자 서명부(113)는 가우시안 분포에 따른 잡음 신호를 랜덤하게 생성하고, 상기 인코딩 메시지에 상기 간섭 신호와 상기 잡음 신호를 부가하여 DPC 메시지를 생성한 후 상기 DPC 메시지와 상기 제1 디터 신호를 전자 서명 값으로 결정한다.

[0058]

이때, 본 발명의 일실시예에 따르면, 전자 서명부(113)는 하기의 수학식 7의 연산에 기초하여 상기 DPC 메시지를 생성할 수 있다.

수학식 7

$$Y = X + S + Z$$

[0060]

[0062]

상기 수학식 7에서, Y 는 상기 DPC 메시지로, X 는 상기 인코딩 메시지, S 는 상기 간섭 신호, Z 는 상기 잡음 신호를 의미한다.

[0063]

메시지 전송부(114)는 상기 전자 서명 값의 결정이 완료되면, 상기 원본 메시지를 데이터 수신 장치(120)로 전송하면서, 상기 전자 서명 값으로 결정된 상기 DPC 메시지와 상기 제1 디터 신호를 데이터 수신 장치(120)로 전송한다.

[0064]

즉, 본 발명에 따른 데이터 전송 장치(110)는 상기 원본 메시지를 데이터 수신 장치(120)로 전송할 때, 상기 원본 메시지에 대한 전자 서명 값으로 소정의 DPC 메시지를 의도적으로 생성하여 데이터 수신 장치(120)로 전송할 수 있다.

[0065]

관련해서, 데이터 전송 장치(110)는 소정의 개인키를 기초로 간섭 신호를 의도적으로 생성하고, 소정의 랜덤 값을 생성하며, 상기 랜덤 값과 상기 원본 메시지를 기초로 제1 디터 신호를 생성한 후 상기 랜덤 값을 DPC에서의 전송 신호로 취급해서 소정의 미리 정해져 있는 MMSE와 상기 간섭 신호 및 상기 제1 디터 신호를 기초로 DPC 기반의 인코딩을 수행하여 소정의 인코딩 메시지를 생성할 수 있고, 그 이후 소정의 잡음 신호를 의도적으로 생성하여 상기 인코딩 메시지에 상기 간섭 신호와 상기 잡음 신호를 노이즈로 부가함으로써, DPC 메시지를 생성한 후 상기 DPC 메시지와 상기 제1 디터 신호를 상기 원본 메시지에 대한 전자 서명 값으로 결정해서 데이터 수신 장치(120)로 전송할 수 있다.

[0066]

이때, 본 발명의 일실시예에 따르면, 데이터 수신 장치(120)는 메모리 상에 상기 MMSE를 상기 개인키에 대응하는 공개키로 저장하고 있음과 동시에 상기 제1 해시 함수를 저장하고 있을 수 있다.

[0067]

이때, 데이터 수신 장치(120)는 데이터 전송 장치(110)로부터 상기 원본 메시지와 상기 전자 서명 값으로 결정된 상기 DPC 메시지 및 상기 제1 디터 신호가 수신되면, 상기 수신된 제1 디터 신호와 상기 메모리 상에 저장되어 있는 상기 MMSE를 기초로 상기 수신된 DPC 메시지에 대해 DPC 기반의 디코딩을 수행하여 상기 랜덤 값을 복원할 수 있다.

[0068]

이때, 본 발명의 일실시예에 따르면, 데이터 수신 장치(110)는 상기 DPC 기반의 디코딩을 수행하기 위해, 하기

의 수학적 식 8의 연산에 기초하여 디코딩 메시지를 생성한 후 상기 디코딩 메시지로부터 상기 랜덤 값을 복원할 수 있다.

수학적 식 8

$$Y' = (\alpha Y + U) \bmod 2Z$$

상기 수학적 식 8에서, Y' 는 상기 디코딩 메시지, α 는 상기 메모리 상에 저장되어 있는 상기 MMSE, Y 는 상기 수신된 DPC 메시지, U 는 상기 수신된 제1 디더 신호를 의미하며, Z 는 가우시안 분포를 갖는 정수 집합을 의미한다.

그러고 나서, 데이터 수신 장치(120)는 상기 메모리 상에 저장되어 있는 상기 제1 해시 함수에 상기 수신된 원본 메시지와 상기 복원된 랜덤 값을 입력으로 인가하여 검증용 디더 신호를 생성하고, 상기 검증용 디더 신호가 상기 수신된 제1 디더 신호와 일치하는지 여부를 확인함으로써, 상기 전자 서명 값에 대한 검증을 수행할 수 있다.

즉, 데이터 수신 장치(120)는 데이터 전송 장치(110)로부터 상기 원본 메시지와 상기 전자 서명 값으로 결정된 상기 DPC 메시지 및 상기 제1 디더 신호가 수신되면, 메모리 상에 공개키로 저장되어 있는 MMSE를 기초로 상기 DPC 메시지에 대해 상기 수학적 식 8에 따른 디코딩을 수행하여 랜덤 값을 복원한 후 메모리 상에 저장되어 있는 상기 제1 해시 함수에 상기 랜덤 값과 상기 원본 메시지를 입력으로 인가해서 검증용 디더 신호를 생성한 후 상기 검증용 디더 신호가 상기 수신된 제1 디더 신호와 일치하는 것으로 확인되면, 상기 원본 메시지가 데이터 전송 장치(110)로부터 진정으로 전송된 메시지임을 확인할 수 있다.

도 2는 본 발명의 일실시예에 따른 디더 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법을 도시한 순서도이다.

단계(S210)에서는 데이터 수신 장치로 전송할 원본 메시지와 기설정된 개인키를 기초로 DPC에 사용될 간섭 신호를 생성한다.

단계(S220)에서는 랜덤 값을 랜덤하게 생성하고, $(-1, 1]$ 사이에서 균일한 값을 가지는 디더 신호를 생성하기 위한 기설정된 제1 해시 함수에 상기 원본 메시지와 상기 랜덤 값을 입력으로 인가하여 제1 디더 신호를 생성한 후 상기 랜덤 값을 DPC에서의 전송 신호로 취급하여, 기설정된 MMSE와 상기 간섭 신호 및 상기 제1 디더 신호를 기초로 상기 랜덤 값에 대해 인코딩을 수행함으로써, 인코딩 메시지를 생성한다.

단계(S230)에서는 가우시안 분포에 따른 잡음 신호를 랜덤하게 생성하고, 상기 인코딩 메시지에 상기 간섭 신호와 상기 잡음 신호를 부가하여 DPC 메시지를 생성한 후 상기 DPC 메시지와 상기 제1 디더 신호를 전자 서명 값으로 결정한다.

단계(S240)에서는 상기 원본 메시지를 상기 데이터 수신 장치로 전송하면서, 상기 전자 서명 값으로 결정된 상기 DPC 메시지와 상기 제1 디더 신호를 상기 데이터 수신 장치로 전송한다.

이때, 본 발명의 일실시예에 따르면, 단계(S210)에서는 상기 원본 메시지를 기설정된 제2 해시 함수에 입력으로 인가하여 해시 값을 생성하고, 상기 개인키와 상기 해시 값을 기설정된 난수 생성 함수에 입력으로 인가하여 상기 간섭 신호를 생성할 수 있다.

또한, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 메모리 상에 상기 MMSE를 상기 개인키에 대응하는 공개키로 저장하고 있음과 동시에 상기 제1 해시 함수를 저장하고 있고, 상기 데이터 전송 장치로부터 상기 원본 메시지와 상기 전자 서명 값으로 결정된 상기 DPC 메시지 및 상기 제1 디더 신호가 수신되면, 상기 수신된 제1 디더 신호와 상기 메모리 상에 저장되어 있는 상기 MMSE를 기초로 상기 수신된 DPC 메시지에 대해 DPC 기반의 디코딩을 수행하여 상기 랜덤 값을 복원한 후 상기 메모리 상에 저장되어 있는 상기 제1 해시 함수에 상기 수신된 원본 메시지와 상기 복원된 랜덤 값을 입력으로 인가하여 검증용 디더 신호를 생성하고, 상기 검증용 디

더 신호가 상기 수신된 제1 디터 신호와 일치하는지 여부를 확인함으로써, 상기 전자 서명 값에 대한 검증을 수행할 수 있다.

[0082] 이때, 본 발명의 일실시예에 따르면, 단계(S220)에서는 상기 수학적 식 6의 연산에 기초하여 상기 인코딩 메시지를 생성할 수 있고, 단계(S230)에서는 상기 수학적 식 7의 연산에 기초하여 상기 DPC 메시지를 생성할 수 있다.

[0083] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 상기 DPC 기반의 디코딩을 수행하기 위해, 상기 수학적 식 8의 연산에 기초하여 디코딩 메시지를 생성한 후 상기 디코딩 메시지로부터 상기 랜덤 값을 복원할 수 있다.

[0084] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 디터 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 디터 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법은 도 1을 이용하여 설명한 디터 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0085] 본 발명의 일실시예에 따른 디터 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0086] 또한, 본 발명의 일실시예에 따른 디터 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치의 동작 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광 기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0087] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0088] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0089] 110: 디터 페이퍼 코딩을 통한 전자 서명이 가능한 데이터 전송 장치

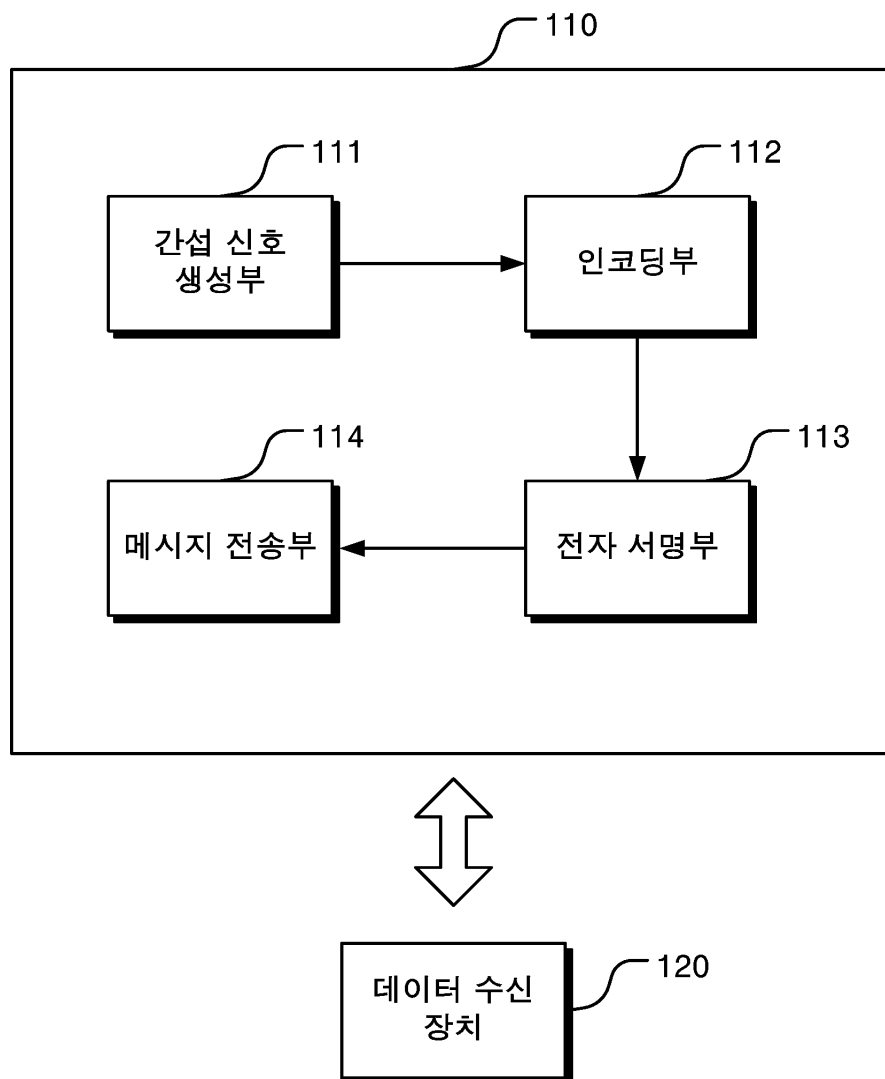
111: 간섭 신호 생성부 112: 인코딩부

113: 전자 서명부 114: 메시지 전송부

120: 데이터 수신 장치

도면

도면1



도면2

