



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0082222
(43) 공개일자 2017년07월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) H04L 12/58 (2006.01)
H04L 9/14 (2006.01)
(52) CPC특허분류
H04L 9/0656 (2013.01)
H04L 51/30 (2013.01)
(21) 출원번호 10-2016-0001362
(22) 출원일자 2016년01월06일
심사청구일자 2016년01월06일

(71) 출원인
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
김영식
광주광역시 서구 풍암2로 62 금호2차아파트 201동
1005호
(74) 대리인
김효성

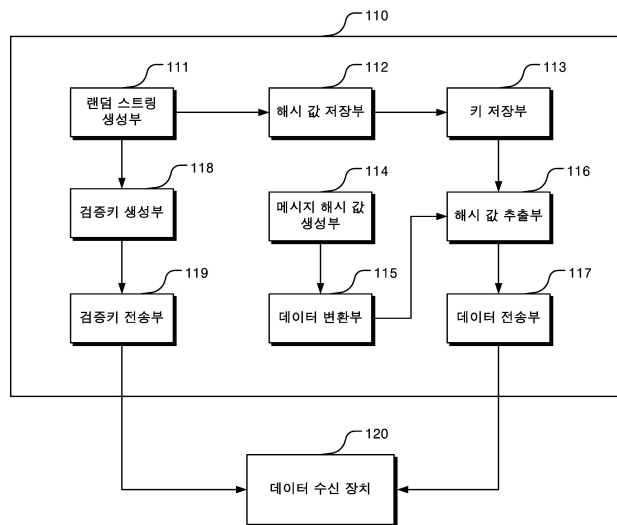
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치 및 방법

(57) 요약

전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치 및 방법이 개시된다. 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치 및 방법은 소정의 랜덤 스트링(string)들을 생성하고, 상기 랜덤 스트링들에 대해 연쇄(chain) 해시 값 연산 과정을 수행하여 생성된 해시 값들을 키 저장부 상에 저장해 놓고, 상기 랜덤 스트링들에 대해 상기 연쇄 해시 값 연산 과정을 추가적으로 수행함으로써, 검증키를 생성하여 상기 검증키를 데이터 수신 장치로 전송한 후 상기 데이터 수신 장치로 전송할 메시지를 상기 키 저장부에 저장되어 있는 해시 값들을 기초로 전자서명하여 상기 데이터 수신 장치로 전송하면, 상기 데이터 수신 장치가 상기 검증키를 기초로 전자서명 값을 검증할 수 있도록 유도함으로써, 상기 전송 메시지에 대한 부인 방지 기능을 제공할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/0643 (2013.01)

H04L 9/14 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711024287

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 중견연구자지원

연구과제명 포스트 양자 암호의 설계 및 효율적 구현에 관한 연구

기 여 율 1/1

주관기관 조선대학교

연구기간 2015.05.01 ~ 2016.04.30

명세서

청구범위

청구항 1

t (t 는 자연수)개의 랜덤 스트링(string)들을 생성한 후 상기 t 개의 랜덤 스트링들 각각에 대해 상기 t 개의 랜덤 스트링들 각각을 지시하는 순번 정보를 할당하는 랜덤 스트링 생성부;

상기 t 개의 랜덤 스트링들 각각에 대해서, 선정된(predetermined) 제1 해시 함수에 기초한 연쇄(chain) 해시 값 연산 과정을 k (k 는 자연수)회 수행하여 상기 k 회의 연쇄 해시 값 연산 과정에서 생성되는 각각의 해시 값들과 상기 각각의 해시 값들을 생성하기 위해서 수행된 연쇄 해시 값 연산 횟수를 키 저장부 상에 서로 대응되도록 저장함으로써, 상기 키 저장부 상에 상기 t 개의 랜덤 스트링들 각각에 대한 k 개의 해시 값들과 상기 k 개의 해시 값들 각각에 대응하는 연쇄 해시 값 연산 횟수를 저장하는 해시 값 저장부;

데이터 수신 장치로 전송할 메시지를 선정된 제2 해시 함수에 입력으로 인가하여 메시지 해시 값을 생성하는 메시지 해시 값 생성부;

상기 메시지 해시 값을 n 개(n 은 자연수)의 데이터 그룹들로 분할하고, 각 그룹내에 포함되어 있는 데이터를 i (i 는 자연수)진수의 숫자로 변환하여 n 개의 숫자들을 생성하는 데이터 변환부;

상기 t 개의 랜덤 스트링들 중 상기 n 개의 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n 개의 랜덤 스트링들을 선택하고, 상기 n 개의 랜덤 스트링들 별로 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 n 개의 선정된 연산 횟수들을 참조하여 상기 키 저장부로부터 상기 n 개의 랜덤 스트링들 별로, 상기 n 개의 선정된 연산 횟수들 중 각 랜덤 스트링에 대응하는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수가 대응되어 저장되어 있는 하나의 해시 값을 추출함으로써, 총 n 개의 해시 값들을 추출하는 해시 값 추출부; 및

상기 데이터 수신 장치에 대해 상기 메시지와 상기 n 개의 해시 값들을 전송하는 데이터 전송부

를 포함하는 전송 메시지에 대한 부인 방식이 가능한 데이터 전송 장치.

청구항 2

제1항에 있어서,

상기 해시 값 저장부는

상기 t 개의 랜덤 스트링들 각각에 대해서, 상기 t 개의 랜덤 스트링들을 상기 선정된 제1 해시 함수에 입력으로 인가하여 해시 값을 연산하고, 상기 연산된 해시 값을 상기 선정된 제1 해시 함수에 다시 입력으로 인가하여 추가 해시 값을 연산하는 방식의 상기 연쇄 해시 값 연산 과정을 상기 k 회 수행하는 전송 메시지에 대한 부인 방식이 가능한 데이터 전송 장치.

청구항 3

제1항에 있어서,

상기 t 개의 랜덤 스트링들 각각에 대해서 상기 연쇄 해시 값 연산 과정을 $k+1$ 회 수행하여 $k+1$ 번째 연쇄 해시 값을 연산하고, 상기 t 개의 랜덤 스트링들 각각에 대해서 연산된 상기 $k+1$ 번째 연쇄 해시 값을 상기 t 개의 랜덤 스트링들 각각에 대한 검증키로 결정함과 동시에 상기 t 개의 랜덤 스트링들 각각에 대한 검증키에 대해 상기 t 개의 랜덤 스트링들 각각에 할당되어 있는 순번 정보와 동일한 순번 정보를 할당하는 검증키 생성부; 및

상기 t 개의 랜덤 스트링들 각각에 대한 검증키를 상기 데이터 수신 장치로 전송하는 검증키 전송부

를 더 포함하는 전송 메시지에 대한 부인 방식이 가능한 데이터 전송 장치.

청구항 4

제3항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 선정된 제1 해시 함수, 상기 선정된 제2 해시 함수, 상기 n개의 선정된 연산 횟수들 및 상기 t개의 랜덤 스트링들 각각에 대한 검증키를 저장하고 있고,

상기 메시지와 상기 n개의 해시 값들이 수신되면, 상기 메시지를 상기 선정된 제2 해시 함수에 입력으로 인가하여 상기 메시지 해시 값을 생성하고, 상기 메시지 해시 값을 n개의 데이터 그룹들로 분할한 후 각 그룹내에 포함되어 있는 데이터를 상기 i진수의 숫자로 변환하여 n개의 검증 숫자들을 생성하며, 상기 t개의 랜덤 스트링들 각각에 대한 검증키 중에서 상기 n개의 검증 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n개의 검증키들을 선택한 후 상기 n개의 선정된 연산 횟수들을 참조하여 상기 n개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 확인하고, 상기 n개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 기초로 상기 k+1번째 연쇄 해시 값이 연산될 때까지 상기 n개의 해시 값들 각각에 대해 상기 선정된 제1 해시 함수에 기초한 상기 연쇄 해시 값 연산 과정을 수행하여 상기 n개의 해시 값들 각각에 대한 상기 k+1번째 연쇄 해시 값을 연산한 후 상기 n개의 해시 값들 각각에 대한 상기 k+1번째 연쇄 해시 값이 상기 n개의 검증키들과 모두 일치하는 것으로 확인되면, 상기 메시지에 대한 인증을 완료하는 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치.

청구항 5

t(t는 자연수)개의 랜덤 스트링(string)들을 생성한 후 상기 t개의 랜덤 스트링들 각각에 대해 상기 t개의 랜덤 스트링들 각각을 지시하는 순번 정보를 할당하는 단계;

상기 t개의 랜덤 스트링들 각각에 대해서, 선정된(predetermined) 제1 해시 함수에 기초한 연쇄(chain) 해시 값 연산 과정을 k(k는 자연수)회 수행하여 상기 k회의 연쇄 해시 값 연산 과정에서 생성되는 각각의 해시 값들과 상기 각각의 해시 값들을 생성하기 위해서 수행된 연쇄 해시 값 연산 횟수를 키 저장부 상에 서로 대응되도록 저장함으로써, 상기 키 저장부 상에 상기 t개의 랜덤 스트링들 각각에 대한 k개의 해시 값들과 상기 k개의 해시 값들 각각에 대응하는 연쇄 해시 값 연산 횟수를 저장하는 단계;

데이터 수신 장치로 전송할 메시지를 선정된 제2 해시 함수에 입력으로 인가하여 메시지 해시 값을 생성하는 단계;

상기 메시지 해시 값을 n개(n은 자연수)의 데이터 그룹들로 분할하고, 각 그룹내에 포함되어 있는 데이터를 i(i는 자연수)진수의 숫자로 변환하여 n개의 숫자들을 생성하는 단계;

상기 t개의 랜덤 스트링들 중 상기 n개의 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n개의 랜덤 스트링들을 선택하고, 상기 n개의 랜덤 스트링들 별로 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 n개의 선정된 연산 횟수들을 참조하여 상기 키 저장부로부터 상기 n개의 랜덤 스트링들 별로, 상기 n개의 선정된 연산 횟수들 중 각 랜덤 스트링에 대응하는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수가 대응되어 저장되어 있는 하나의 해시 값을 추출함으로써, 총 n개의 해시 값들을 추출하는 단계; 및

상기 데이터 수신 장치에 대해 상기 메시지와 상기 n개의 해시 값들을 전송하는 단계

를 포함하는 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법.

청구항 6

제5항에 있어서,

상기 연쇄 해시 값 연산 횟수를 저장하는 단계는

상기 t개의 랜덤 스트링들 각각에 대해서, 상기 t개의 랜덤 스트링들을 상기 선정된 제1 해시 함수에 입력으로 인가하여 해시 값을 연산하고, 상기 연산된 해시 값을 상기 선정된 제1 해시 함수에 다시 입력으로 인가하여 추가 해시 값을 연산하는 방식의 상기 연쇄 해시 값 연산 과정을 상기 k회 수행하는 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법.

청구항 7

제5항에 있어서,

상기 t개의 랜덤 스트링들 각각에 대해서 상기 연쇄 해시 값 연산 과정을 k+1회 수행하여 k+1번째 연쇄 해시 값을 연산하고, 상기 t개의 랜덤 스트링들 각각에 대해서 연산된 상기 k+1번째 연쇄 해시 값을 상기 t개의 랜덤

스트링들 각각에 대한 검증키로 결정함과 동시에 상기 t개의 랜덤 스트링들 각각에 대한 검증키에 대해 상기 t개의 랜덤 스트링들 각각에 할당되어 있는 순번 정보와 동일한 순번 정보를 할당하는 단계; 및

상기 t개의 랜덤 스트링들 각각에 대한 검증키를 상기 데이터 수신 장치로 전송하는 단계

를 더 포함하는 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법.

청구항 8

제7항에 있어서,

상기 데이터 수신 장치는

메모리 상에 상기 선정된 제1 해시 함수, 상기 선정된 제2 해시 함수, 상기 n개의 선정된 연산 횟수들 및 상기 t개의 랜덤 스트링들 각각에 대한 검증키를 저장하고 있고,

상기 메시지와 상기 n개의 해시 값들이 수신되면, 상기 메시지를 상기 선정된 제2 해시 함수에 입력으로 인가하여 상기 메시지 해시 값을 생성하고, 상기 메시지 해시 값을 n개의 데이터 그룹들로 분할한 후 각 그룹내에 포함되어 있는 데이터를 상기 i진수의 숫자로 변환하여 n개의 검증 숫자들을 생성하며, 상기 t개의 랜덤 스트링들 각각에 대한 검증키 중에서 상기 n개의 검증 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n개의 검증키들을 선택한 후 상기 n개의 선정된 연산 횟수들을 참조하여 상기 n개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 확인하고, 상기 n개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 기초로 상기 k+1번째 연쇄 해시 값이 연산될 때까지 상기 n개의 해시 값들 각각에 대해 상기 선정된 제1 해시 함수에 기초한 상기 연쇄 해시 값 연산 과정을 수행하여 상기 n개의 해시 값들 각각에 대한 상기 k+1번째 연쇄 해시 값을 연산한 후 상기 n개의 해시 값들 각각에 대한 상기 k+1번째 연쇄 해시 값이 상기 n개의 검증키들과 모두 일치하는 것으로 확인되면, 상기 메시지에 대한 인증을 완료하는 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법.

청구항 9

제5항 내지 제8항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 10

제5항 내지 제8항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 네트워크 시스템에서 데이터 전송 장치가 데이터 수신 장치로 전송하는 전송 메시지에 대한 부인 방지 기능을 제공하기 위한 보안 기술과 관련된다.

배경 기술

[0002] 최근, 인터넷 기술이 발전함에 따라, 다양한 인터넷 가능 단말 간에 데이터를 송수신할 수 있는 환경이 구축되고 있다. 이러한 인터넷 기술의 발달로 인해 사물인터넷 기술이나 스마트 그리드(smart grid) 관련 기술들이 등장하고 있다.

[0003] 네트워크 시스템에서 단말 간에 메시지를 주고받을 때에는 메시지에 대한 무결성을 검증하거나 메시지에 대한 암호화 등을 수행하는 것과 같은 보안 환경이 구축될 필요가 있다. 특히, 특정 사용자로부터 전달되는 메시지가 진정한 사용자에게 의해서 전달되는 것인지 여부를 확인하기 위한 보안 서비스를 부인 방지 서비스라고 칭한다.

[0004] 보통, 일반적인 온라인 뱅킹 서비스나 네트워크 시스템에서 도입하고 있는 부인 방지 서비스는 공개키 암호화 방식을 이용한 전자서명 시스템이 주를 이루고 있다.

[0005] 공개키 암호화 방식의 전자서명 시스템이란 메시지를 전달하는 측에서 해당 메시지에 대한 해시 값에 대해 자신의 개인키로 암호화를 수행한 후 해당 메시지와 상기 개인키로 암호화한 값을 메시지 수신측에 전달하면, 메시지 수신측에서 상기 개인키에 대응하는 공개키로 상기 암호화한 값을 복호화하고, 메시지 전송측으로부터 수신

한 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 암호화된 값이 상기 메시지 전송측의 개인키에 의해서 정말로 암호화된 값임이 입증됨에 따라, 상기 메시지가 진정한 메시지 전송측으로부터 전달된 메시지임을 확인하는 시스템이다.

[0006] 이러한 공개키 암호화 방식의 전자서명 시스템은 메시지 전송측의 부인 방식을 구현하는데 매우 용이하게 사용될 수 있지만, 매우 많은 연산량을 요구하기 때문에 연산에 사용할 수 있는 하드웨어 또는 소프트웨어 자원이 매우 부족한 환경에서는 공개키 암호화 방식을 사용할 수 없는 단점이 있다.

[0007] 특히, 최근에는 일반 컴퓨터와 같은 장치들뿐만 아니라, 수많은 사물들이 인터넷에 연결되는 사물 인터넷 시스템이나 네트워크 기반의 전력 시스템인 스마트 그리드 시스템이 도입되고 있는 추세이지만, 이러한 환경에서 사용되는 대부분의 단말 장치들은 연산 자원이 부족하다는 점에서, 기존의 공개키 암호화 기반의 부인 방지 기능을 사용하기 어려울 것으로 예상된다.

[0008] 따라서, 기존의 공개키 암호화 기반의 부인 방지 기능이 아닌 새로운 형태의 방식을 통해서 부인 방지 기능을 제공할 수 있는 시스템에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0009] 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치 및 방법은 소정의 랜덤 스트링(string)들을 생성하고, 상기 랜덤 스트링들에 대해 연쇄(chain) 해시 값 연산 과정을 수행하여 생성된 해시 값들을 키 저장부 상에 저장해 놓고, 상기 랜덤 스트링들에 대해 상기 연쇄 해시 값 연산 과정을 추가적으로 수행함으로써, 검증키를 생성하여 상기 검증키를 데이터 수신 장치로 전송한 후 상기 데이터 수신 장치로 전송할 메시지를 상기 키 저장부에 저장되어 있는 해시 값들을 기초로 전자서명하여 상기 데이터 수신 장치로 전송하면, 상기 데이터 수신 장치가 상기 검증키를 기초로 전자서명 값을 검증할 수 있도록 유도함으로써, 상기 전송 메시지에 대한 부인 방지 기능을 제공할 수 있도록 한다.

과제의 해결 수단

[0010] 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치는 t (t 는 자연수)개의 랜덤 스트링(string)들을 생성한 후 상기 t 개의 랜덤 스트링들 각각에 대해 상기 t 개의 랜덤 스트링들 각각을 지시하는 순번 정보를 할당하는 랜덤 스트링 생성부, 상기 t 개의 랜덤 스트링들 각각에 대해서, 선정된(predetermined) 제1 해시 함수에 기초한 연쇄(chain) 해시 값 연산 과정을 k (k 는 자연수)회 수행하여 상기 k 회의 연쇄 해시 값 연산 과정에서 생성되는 각각의 해시 값들과 상기 각각의 해시 값들을 생성하기 위해서 수행된 연쇄 해시 값 연산 횟수를 키 저장부 상에 서로 대응되도록 저장함으로써, 상기 키 저장부 상에 상기 t 개의 랜덤 스트링들 각각에 대한 k 개의 해시 값들과 상기 k 개의 해시 값들 각각에 대응하는 연쇄 해시 값 연산 횟수를 저장하는 해시 값 저장부, 데이터 수신 장치로 전송할 메시지를 선정된 제2 해시 함수에 입력으로 인가하여 메시지 해시 값을 생성하는 메시지 해시 값 생성부, 상기 메시지 해시 값을 n 개(n 은 자연수)의 데이터 그룹들로 분할하고, 각 그룹내에 포함되어 있는 데이터를 i (i 는 자연수)진수의 숫자로 변환하여 n 개의 숫자들을 생성하는 데이터 변환부, 상기 t 개의 랜덤 스트링들 중 상기 n 개의 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n 개의 랜덤 스트링들을 선택하고, 상기 n 개의 랜덤 스트링들 별로 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 n 개의 선정된 연산 횟수들을 참조하여 상기 키 저장부로부터 상기 n 개의 랜덤 스트링들 별로, 상기 n 개의 선정된 연산 횟수들 중 각 랜덤 스트링에 대응하는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수가 대응되어 저장되어 있는 하나의 해시 값을 추출함으로써, 총 n 개의 해시 값들을 추출하는 해시 값 추출부 및 상기 데이터 수신 장치에 대해 상기 메시지와 상기 n 개의 해시 값들을 전송하는 데이터 전송부를 포함한다.

[0011] 또한, 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법은 t (t 는 자연수)개의 랜덤 스트링들을 생성한 후 상기 t 개의 랜덤 스트링들 각각에 대해 상기 t 개의 랜덤 스트링들 각각을 지시하는 순번 정보를 할당하는 단계, 상기 t 개의 랜덤 스트링들 각각에 대해서, 선정된 제1 해시 함수에 기초한 연쇄 해시 값 연산 과정을 k (k 는 자연수)회 수행하여 상기 k 회의 연쇄 해시 값 연산 과정에서 생성되는 각각의 해시 값들과 상기 각각의 해시 값들을 생성하기 위해서 수행된 연쇄 해시 값 연산 횟수를 키 저장부 상에 서로 대응되도록 저장함으로써, 상기 키 저장부 상에 상기 t 개의 랜덤 스트링들 각각에 대한 k 개의 해시 값들과 상기 k 개의 해시 값들 각각에 대응하는 연쇄 해시 값 연산 횟수를 저장하는 단계, 데이터 수신 장치로 전송할 메시지를

선정된 제2 해시 함수에 입력으로 인가하여 메시지 해시 값을 생성하는 단계, 상기 메시지 해시 값을 n 개(n 은 자연수)의 데이터 그룹들로 분할하고, 각 그룹내에 포함되어 있는 데이터를 i (i 는 자연수)진수의 숫자로 변환하여 n 개의 숫자들을 생성하는 단계, 상기 t 개의 랜덤 스트링들 중 상기 n 개의 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n 개의 랜덤 스트링들을 선택하고, 상기 n 개의 랜덤 스트링들 별로 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 n 개의 선정된 연산 횟수들을 참조하여 상기 키 저장부로부터 상기 n 개의 랜덤 스트링들 별로, 상기 n 개의 선정된 연산 횟수들 중 각 랜덤 스트링에 대응하는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수가 대응되어 저장되어 있는 하나의 해시 값을 추출함으로써, 총 n 개의 해시 값들을 추출하는 단계 및 상기 데이터 수신 장치에 대해 상기 메시지와 상기 n 개의 해시 값들을 전송하는 단계를 포함한다.

발명의 효과

[0012] 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치 및 방법은 소정의 랜덤 스트링(string)들을 생성하고, 상기 랜덤 스트링들에 대해 연쇄(chain) 해시 값 연산 과정을 수행하여 생성된 해시 값들을 키 저장부 상에 저장해 놓고, 상기 랜덤 스트링들에 대해 상기 연쇄 해시 값 연산 과정을 추가적으로 수행함으로써, 검증키를 생성하여 상기 검증키를 데이터 수신 장치로 전송한 후 상기 데이터 수신 장치로 전송할 메시지를 상기 키 저장부에 저장되어 있는 해시 값들을 기초로 전자서명하여 상기 데이터 수신 장치로 전송하면, 상기 데이터 수신 장치가 상기 검증키를 기초로 전자서명 값을 검증할 수 있도록 유도함으로써, 상기 전송 메시지에 대한 부인 방지 기능을 제공할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치의 구조를 도시한 도면이다

도 2는 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 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 사용하였다.

[0015] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0016] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0017] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0018] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0019] 도 1은 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치의 구조를 도시한 도면이다

[0020] 도 1을 참조하면, 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지 가능한 데이터 전송 장치(110)는

랜덤 스트링(string) 생성부(111), 해시 값 저장부(112), 메시지 해시 값 생성부(114), 데이터 변환부(115), 해시 값 추출부(116) 및 데이터 전송부(117)를 포함한다.

- [0021] 랜덤 스트링 생성부(111)는 t (t 는 자연수)개의 랜덤 스트링(string)들을 생성한 후 상기 t 개의 랜덤 스트링들 각각에 대해 상기 t 개의 랜덤 스트링들 각각을 지시하는 순번 정보를 할당한다.
- [0022] 해시 값 저장부(112)는 상기 t 개의 랜덤 스트링들 각각에 대해서, 선정된(predetermined) 제1 해시 함수에 기초한 연쇄(chain) 해시 값 연산 과정을 k (k 는 자연수)회 수행하여 상기 k 회의 연쇄 해시 값 연산 과정에서 생성되는 각각의 해시 값들과 상기 각각의 해시 값들을 생성하기 위해서 수행된 연쇄 해시 값 연산 횟수를 키 저장부(113) 상에 서로 대응되도록 저장함으로써, 키 저장부(113) 상에 상기 t 개의 랜덤 스트링들 각각에 대한 k 개의 해시 값들과 상기 k 개의 해시 값들 각각에 대응하는 연쇄 해시 값 연산 횟수를 저장한다.
- [0023] 이때, 본 발명의 일실시예에 따르면, 해시 값 저장부(112)는 상기 t 개의 랜덤 스트링들 각각에 대해서, 상기 t 개의 랜덤 스트링들을 상기 선정된 제1 해시 함수에 입력으로 인가하여 해시 값을 연산하고, 상기 연산된 해시 값을 상기 선정된 제1 해시 함수에 다시 입력으로 인가하여 추가 해시 값을 연산하는 방식의 상기 연쇄 해시 값 연산 과정을 상기 k 회 수행할 수 있다.
- [0024] 메시지 해시 값 생성부(114)는 데이터 수신 장치(120)로 전송할 메시지를 선정된 제2 해시 함수에 입력으로 인가하여 메시지 해시 값을 생성한다.
- [0025] 데이터 변환부(115)는 상기 메시지 해시 값을 n 개(n 은 자연수)의 데이터 그룹들로 분할하고, 각 그룹내에 포함되어 있는 데이터를 i (i 는 자연수)진수의 숫자로 변환하여 n 개의 숫자들을 생성한다.
- [0026] 해시 값 추출부(116)는 상기 t 개의 랜덤 스트링들 중 상기 n 개의 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n 개의 랜덤 스트링들을 선택하고, 상기 n 개의 랜덤 스트링들 별로 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 n 개의 선정된 연산 횟수들을 참조하여 키 저장부(113)로부터 상기 n 개의 랜덤 스트링들 별로, 상기 n 개의 선정된 연산 횟수들 중 각 랜덤 스트링에 대응하는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수가 대응되어 저장되어 있는 하나의 해시 값을 추출함으로써, 총 n 개의 해시 값들을 추출한다.
- [0027] 데이터 전송부(117)는 데이터 수신 장치(120)에 대해 상기 메시지와 상기 n 개의 해시 값들을 전송한다.
- [0028] 이때, 본 발명의 일실시예에 따르면, 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치(110)는 검증키 생성부(118) 및 검증키 전송부(119)를 더 포함할 수 있다.
- [0029] 검증키 생성부(118)는 상기 t 개의 랜덤 스트링들 각각에 대해서 상기 연쇄 해시 값 연산 과정을 $k+1$ 회 수행하여 $k+1$ 번째 연쇄 해시 값을 연산하고, 상기 t 개의 랜덤 스트링들 각각에 대해서 연산된 상기 $k+1$ 번째 연쇄 해시 값을 상기 t 개의 랜덤 스트링들 각각에 대한 검증키로 결정함과 동시에 상기 t 개의 랜덤 스트링들 각각에 대한 검증키에 대해 상기 t 개의 랜덤 스트링들 각각에 할당되어 있는 순번 정보와 동일한 순번 정보를 할당한다.
- [0030] 검증키 전송부(119)는 상기 t 개의 랜덤 스트링들 각각에 대한 검증키를 데이터 수신 장치(120)로 전송한다.
- [0031] 이때, 본 발명의 일실시예에 따르면, 데이터 수신 장치(120)는 메모리 상에 상기 선정된 제1 해시 함수, 상기 선정된 제2 해시 함수, 상기 n 개의 선정된 연산 횟수들 및 상기 t 개의 랜덤 스트링들 각각에 대한 검증키를 저장하고 있고, 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치(110)로부터 상기 메시지와 상기 n 개의 해시 값들이 수신되면, 상기 메시지를 상기 선정된 제2 해시 함수에 입력으로 인가하여 상기 메시지 해시 값을 생성하고, 상기 메시지 해시 값을 n 개의 데이터 그룹들로 분할한 후 각 그룹내에 포함되어 있는 데이터를 상기 i 진수의 숫자로 변환하여 n 개의 검증 숫자들을 생성하며, 상기 t 개의 랜덤 스트링들 각각에 대한 검증키 중에서 상기 n 개의 검증 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n 개의 검증키들을 선택한 후 상기 n 개의 선정된 연산 횟수들을 참조하여 상기 n 개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 확인하고, 상기 n 개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 기초로 상기 $k+1$ 번째 연쇄 해시 값이 연산될 때까지 상기 n 개의 해시 값들 각각에 대해 상기 선정된 제1 해시 함수에 기초한 상기 연쇄 해시 값 연산 과정을 수행하여 상기 n 개의 해시 값들 각각에 대한 상기 $k+1$ 번째 연쇄 해시 값을 연산한 후 상기 n 개의 해시 값들 각각에 대한 상기 $k+1$ 번째 연쇄 해시 값이 상기 n 개의 검증키들과 모두 일치하는 것으로 확인되면, 상기 메시지에 대한 인증을 완료할 수 있다.
- [0032] 이하에서는 본 발명에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치(110)의 동작에 대해 예를 들어 상세히 설명하기로 한다.

[0033] 우선, 랜덤 스트링 생성부(111)는 t (t 는 자연수)개의 랜덤 스트링들을 생성한 후 상기 t 개의 랜덤 스트링들 각각에 대해 상기 t 개의 랜덤 스트링들 각각을 지시하는 순번 정보를 할당할 수 있는데, 상기 t 를 1024라고 가정하면, 랜덤 스트링 생성부(111)는 1024개의 랜덤 스트링들인 " $s_1, s_2, \dots, s_{1024}$ "를 생성할 수 있고, 상기 1024개의 랜덤 스트링들에 대해 각각 "1"부터 "1024"라는 순번 정보를 할당할 수 있다.

[0034] 그리고, 해시 값 저장부(112)는 상기 1024개의 랜덤 스트링들 각각에 대해서, 상기 1024개의 랜덤 스트링들을 선정된 제1 해시 함수인 " $f(x)$ "에 입력으로 인가하여 상기 1024개의 랜덤 스트링들 각각에 대한 해시 값인 " $f^1(s_1), f^1(s_2), \dots, f^1(s_{1024})$ "를 생성할 수 있다.

[0035] 그리고 나서, 해시 값 저장부(112)는 상기 해시 값 " $f^1(s_1), f^1(s_2), \dots, f^1(s_{1024})$ "를 다시 상기 선정된 제1 해시 함수인 " $f(x)$ "에 입력으로 인가하여 두 번째 해시 값들인 " $f^2(s_1), f^2(s_2), \dots, f^2(s_{1024})$ "를 생성할 수 있다. 이러한 방식으로 해시 값 저장부(112)는 상기 1024개의 랜덤 스트링들 각각에 대해서, 상기 선정된 제1 해시 함수에 기초한 연쇄 해시 값 연산 과정을 k (k 는 자연수)회 수행하여 상기 k 회의 연쇄 해시 값 연산 과정에서 생성되는 각각의 해시 값들을 생성할 수 있는데, 상기 k 를 "8"로 가정하면, 해시 값 저장부(112)는 상기 1024개의 랜덤 스트링들 각각에 대해서, 상기 선정된 제1 해시 함수에 기초한 연쇄 해시 값 연산 과정을 8회 수행하여 상기 8회의 연쇄 해시 값 연산 과정에서 생성되는 해시 값들과 상기 각각의 해시 값들을 생성하기 위해서 수행된 연쇄 해시 값 연산 횟수를 k 저장부(113) 상에 서로 대응되도록 저장할 수 있다.

[0036] 관련해서, k 저장부(113) 상에는 하기의 표 1과 같이 정보가 저장되어 있을 수 있다.

표 1

랜덤 스트링들	1회 연산 해시 값	2회 연산 해시 값	3회 연산 해시 값	4회 연산 해시 값	5회 연산 해시 값	6회 연산 해시 값	7회 연산 해시 값	8회 연산 해시 값
s_1	$f^1(s_1)$	$f^2(s_1)$	$f^3(s_1)$	$f^4(s_1)$	$f^5(s_1)$	$f^6(s_1)$	$f^7(s_1)$	$f^8(s_1)$
s_2	$f^1(s_2)$	$f^2(s_2)$	$f^3(s_2)$	$f^4(s_2)$	$f^5(s_2)$	$f^6(s_2)$	$f^7(s_2)$	$f^8(s_2)$
...	...	...	...	...	...	...	...	...
s_{1024}	$f^1(s_{1024})$	$f^2(s_{1024})$	$f^3(s_{1024})$	$f^4(s_{1024})$	$f^5(s_{1024})$	$f^6(s_{1024})$	$f^7(s_{1024})$	$f^8(s_{1024})$

[0040] 상기 표 1에서 해시 값의 위 첨자로 표기된 숫자가 연쇄 해시 값 연산 횟수를 의미하고, 랜덤 스트링의 아래 첨자로 표기된 숫자가 각 랜덤 스트링을 지시하는 순번 정보를 의미한다.

[0041] 예컨대, " $f^3(s_2)$ "의 경우에는 2번째 랜덤 스트링에 대해서 3회 연쇄 해시 값 연산이 수행되어 생성된 해시 값을 의미한다.

[0042] 이러한 방식으로 해시 값 저장부(112)는 상기 1024개의 랜덤 스트링들 각각에 대해서 상기 선정된 제1 해시 함수에 기초한 연쇄 해시 값 연산 과정을 총 8회 수행함으로써, 각 연산 과정에서 생성되는 해시 값들과 각 해시 값들에 대한 연쇄 해시 값 연산 횟수를 k 저장부(113) 상에 저장할 수 있다.

[0043] 이때, 검증키 생성부(118)는 상기 1024개의 랜덤 스트링들 각각에 대해서 상기 연쇄 해시 값 연산 과정을 9회 수행하여 9번째 연쇄 해시 값을 연산하고, 상기 1024개의 랜덤 스트링들 각각에 대해서 연산된 상기 9번째 연쇄 해시 값을 상기 1024개의 랜덤 스트링들 각각에 대한 검증키로 결정함과 동시에 상기 1024개의 랜덤 스트링들 각각에 대한 검증키에 대해 상기 1024개의 랜덤 스트링들 각각에 할당되어 있는 순번 정보와 동일한 순번 정보를 할당할 수 있다.

[0044] 즉, 검증키 생성부(118)는 하기의 표 2와 같이, 상기 1024개의 랜덤 스트링들 각각에 대해서 상기 연쇄 해시 값 연산 과정을 9회 수행하여 상기 1024개의 랜덤 스트링들 각각에 대한 9번째 연쇄 해시 값을 생성할 수 있다.

표 2

랜덤 스트링들	9회 연산된 해시 값
s_1	$f^9(s_1)$
s_2	$f^9(s_2)$
...	...
s_{1024}	$f^9(s_{1024})$

[0046]

[0048]

그리고 나서, 검증키 생성부(118)는 상기 1024개의 랜덤 스트링들 각각에 대해서 연산된 상기 9번째 연쇄 해시 값을 상기 1024개의 랜덤 스트링들 각각에 대한 검증키로 결정함과 동시에 상기 1024개의 랜덤 스트링들 각각에 대한 검증키에 대해 상기 1024개의 랜덤 스트링들 각각에 할당되어 있는 순번 정보와 동일한 순번 정보를 할당할 수 있다.

[0049]

즉, 랜덤 스트링 " s_1 "에 대한 9번째 연쇄 해시 값은 " $f^9(s_1)$ "이므로, 검증키 생성부(118)는 " $f^9(s_1)$ "에 대해서 랜덤 스트링 " s_1 "과 동일한 순번 정보인 1번 순번 정보를 할당할 수 있다.

[0050]

이렇게, 검증키 생성부(118)에서 상기 1024개의 랜덤 스트링들 각각에 대한 검증키의 생성이 완료되면, 검증키 전송부(119)는 상기 1024개의 랜덤 스트링들 각각에 대한 검증키인 " $f^9(s_1)$, $f^9(s_2)$, ..., $f^9(s_{1024})$ "를 데이터 수신 장치(120)로 전송할 수 있다.

[0051]

이때, 데이터 수신 장치(120)는 상기 1024개의 랜덤 스트링들 각각에 대한 검증키인 " $f^9(s_1)$, $f^9(s_2)$, ..., $f^9(s_{1024})$ "을 수신하여 메모리 상에 저장해 둘 수 있다.

[0052]

이렇게, 상기 표 1에 나타난 바와 같은 상기 1024개의 랜덤 스트링들 각각에 대한 해시 값들과 상기 표 2에 나타난 바와 같은 상기 1024개의 랜덤 스트링들 각각에 대한 검증키의 생성이 완료되면, 상기 표 1에 나타난 바와 같은 상기 1024개의 랜덤 스트링들 각각에 대한 해시 값들은 데이터 전송 장치(110)가 데이터 수신 장치(120)로 전송할 메시지에 대한 전자서명 값을 생성하기 위한 키 값으로 활용되고, 상기 표 2에 나타난 바와 같은 상기 1024개의 랜덤 스트링들 각각에 대한 검증키는 데이터 수신 장치(120)가 상기 전자서명 값을 검증하기 위한 검증키 값으로 활용된다.

[0053]

관련해서, 데이터 전송 장치(110)가 데이터 수신 장치(120)로 메시지 " m "을 전송하는 경우, 메시지 해시 값 생성부(114)는 상기 메시지 " m "을 선정된 제2 해시 함수인 " $h(x)$ "에 입력으로 인가하여 메시지 해시 값인 " $h(m)$ "을 생성할 수 있다.

[0054]

그리고 나서, 데이터 변환부(115)는 상기 메시지 해시 값인 " $h(m)$ "을 n 개(n 은 자연수)의 데이터 그룹들로 분할하고, 각 그룹내에 포함되어 있는 데이터를 i (i 는 자연수)진수의 숫자로 변환하여 n 개의 숫자들을 생성할 수 있다.

[0055]

관련해서, 상기 n 을 "8"이라고 하고, 상기 i 진수를 "10진수"라고 하면, 데이터 변환부(115)는 상기 메시지 해시 값 " $h(m)$ "을 8개의 데이터 그룹들로 분할하고, 상기 8개의 데이터 그룹들 각각에 포함되어 있는 데이터를 10진수의 숫자로 변환하여 총 8개의 숫자들을 생성할 수 있다.

[0056]

예컨대, 상기 메시지 해시 값 " $h(m)$ "이 8바이트의 크기를 갖는 데이터라고 하는 경우, 데이터 변환부(115)는 상기 메시지 해시 값 " $h(m)$ "을 1바이트씩 8개의 데이터 그룹들로 분할한 후 각 데이터 그룹에 포함되어 있는 1바이트의 데이터를 10진수의 숫자로 변환함으로써, 총 8개의 숫자들을 생성할 수 있다.

[0057]

그 이후, 해시 값 추출부(116)는 상기 1024개의 랜덤 스트링들 중 상기 8개의 숫자들 각각과 동일한 순번 정보가 할당되어 있는 8개의 랜덤 스트링들을 선택할 수 있다.

[0058]

관련해서, 데이터 변환부(115)에 의해서 생성된 상기 8개의 숫자가 "32, 592, 164, 7, 985, 223, 327, 814"라

고 가정하면, 해시 값 추출부(116)는 상기 1024개의 랜덤 스트링들 중 "32, 592, 164, 7, 985, 223, 327, 814"라는 순번이 할당되어 있는 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"를 선택할 수 있다.

[0059] 그리고 나서, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"들 각각에 대해 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 8개의 선정된 연산 횟수들을 참조하여 키 저장부(113)로부터 상기 8개의 랜덤 스트링들 별로, 상기 8개의 선정된 연산 횟수들 중 각 랜덤 스트링에 대응하는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수가 대응되어 저장되어 있는 하나의 해시 값을 추출함으로써, 총 8개의 해시 값들을 추출할 수 있다.

[0060] 관련해서, 상기 8개의 랜덤 스트링들 별로 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 상기 8개의 선정된 연산 횟수들을 "8회, 7회, 6회, 5회, 4회, 3회, 2회, 1회"라고 가정하자.

[0061] 이때, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"들 중 "s₃₂"에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 "s₃₂"라는 랜덤 스트링에 대응하여 생성된 8개의 해시 값들인 "f¹(s₃₂), f²(s₃₂), f³(s₃₂), f⁴(s₃₂), f⁵(s₃₂), f⁶(s₃₂), f⁷(s₃₂), f⁸(s₃₂))" 중에서 "8회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "8회"가 대응되어 저장되어 있는 "f⁸(s₃₂))"를 추출할 수 있다.

[0062] 그리고, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"들 중 "s₅₉₂"에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 "s₅₉₂"라는 랜덤 스트링에 대응하여 생성된 8개의 해시 값들인 "f¹(s₅₉₂), f²(s₅₉₂), f³(s₅₉₂), f⁴(s₅₉₂), f⁵(s₅₉₂), f⁶(s₅₉₂), f⁷(s₅₉₂), f⁸(s₅₉₂))" 중에서 "7회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "7회"가 대응되어 저장되어 있는 "f⁷(s₅₉₂))"를 추출할 수 있다.

[0063] 그리고, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"들 중 "s₁₆₄"에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 "s₁₆₄"라는 랜덤 스트링에 대응하여 생성된 8개의 해시 값들인 "f¹(s₁₆₄), f²(s₁₆₄), f³(s₁₆₄), f⁴(s₁₆₄), f⁵(s₁₆₄), f⁶(s₁₆₄), f⁷(s₁₆₄), f⁸(s₁₆₄))" 중에서 "6회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "6회"가 대응되어 저장되어 있는 "f⁶(s₁₆₄))"를 추출할 수 있다.

[0064] 그리고, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"들 중 "s₇"에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 "s₇"이라는 랜덤 스트링에 대응하여 생성된 8개의 해시 값들인 "f¹(s₇), f²(s₇), f³(s₇), f⁴(s₇), f⁵(s₇), f⁶(s₇), f⁷(s₇), f⁸(s₇))" 중에서 "5회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "5회"가 대응되어 저장되어 있는 "f⁵(s₇))"를 추출할 수 있다.

[0065] 그리고, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"들 중 "s₉₈₅"에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 "s₉₈₅"라는 랜덤 스트링에 대응하여 생성된 8개의 해시 값들인 "f¹(s₉₈₅), f²(s₉₈₅), f³(s₉₈₅), f⁴(s₉₈₅), f⁵(s₉₈₅), f⁶(s₉₈₅), f⁷(s₉₈₅), f⁸(s₉₈₅))" 중에서 "4회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "4회"가 대응되어 저장되어 있는 "f⁴(s₉₈₅))"를 추출할 수 있다.

[0066] 그리고, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 "s₃₂, s₅₉₂, s₁₆₄, s₇, s₉₈₅, s₂₂₃, s₃₂₇, s₈₁₄"들 중 "s₂₂₃"에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 "s₂₂₃"이라는 랜덤 스트링에 대

응하여 생성된 8개의 해시 값들인 " $f^1(s_{223})$, $f^2(s_{223})$, $f^3(s_{223})$, $f^4(s_{223})$, $f^5(s_{223})$, $f^6(s_{223})$, $f^7(s_{223})$, $f^8(s_{223})$ " 중에서 "3회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "3회"가 대응되어 저장되어 있는 " $f^3(s_{223})$ "를 추출할 수 있다.

[0067] 그리고, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 " s_{32} , s_{592} , s_{164} , s_7 , s_{985} , s_{223} , s_{327} , s_{814} "들 중 " s_{327} "에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 " s_{327} "이라는 랜덤 스트링에 대응하여 생성된 8개의 해시 값들인 " $f^1(s_{327})$, $f^2(s_{327})$, $f^3(s_{327})$, $f^4(s_{327})$, $f^5(s_{327})$, $f^6(s_{327})$, $f^7(s_{327})$, $f^8(s_{327})$ " 중에서 "2회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "2회"가 대응되어 저장되어 있는 " $f^2(s_{327})$ "를 추출할 수 있다.

[0068] 마지막으로, 해시 값 추출부(116)는 상기 8개의 랜덤 스트링들인 " s_{32} , s_{592} , s_{164} , s_7 , s_{985} , s_{223} , s_{327} , s_{814} "들 중 " s_{814} "에 대해서는 상기 표 1과 같은 정보가 저장되어 있는 키 저장부(113)로부터 " s_{814} "이라는 랜덤 스트링에 대응하여 생성된 8개의 해시 값들인 " $f^1(s_{814})$, $f^2(s_{814})$, $f^3(s_{814})$, $f^4(s_{814})$, $f^5(s_{814})$, $f^6(s_{814})$, $f^7(s_{814})$, $f^8(s_{814})$ " 중에서 "1회"라는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수인 "1회"가 대응되어 저장되어 있는 " $f^1(s_{814})$ "를 추출할 수 있다.

[0069] 이러한 방식으로 결국, 해시 값 추출부(116)는 키 저장부(113)로부터 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ "라는 8개의 해시 값들을 추출할 수 있다.

[0070] 그리고 나서, 데이터 전송부(117)는 데이터 수신 장치(120)에 대해 상기 메시지 "m"을 전송하면서 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ "을 상기 메시지 "m"에 대한 부인 방지를 위한 전자서명 값으로 전송할 수 있다.

[0071] 이때, 데이터 수신 장치(120)는 데이터 전송 장치(110)로부터 상기 메시지 "m"과 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ "이 수신되면, 데이터 전송 장치(110)로부터 미리 수신하여 상기 메모리 상에 이미 저장해 둔 상기 표 2에서 나타난 상기 1024개의 랜덤 스트링들 각각에 대한 검증키를 기초로 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ "에 대한 검증을 수행함으로써, 상기 메시지 "m"이 진정으로 데이터 전송 장치(110)로부터 전송된 메시지가 맞는지 여부를 확인할 수 있다.

[0072] 관련해서, 데이터 수신 장치(120)의 상기 메모리에는 상기 표 2에서 나타난 상기 1024개의 랜덤 스트링들 각각에 대한 검증키뿐만 아니라, 상기 선정된 제1 해시 함수 " $f(x)$ ", 상기 선정된 제2 해시 함수 " $h(x)$ "와 해시 값 추출부(116)에서 상기 8개의 랜덤 스트링들 " s_{32} , s_{592} , s_{164} , s_7 , s_{985} , s_{223} , s_{327} , s_{814} " 각각에 대한 해시 값을 추출하는데 사용하였던 상기 8개의 선정된 연산 횟수들인 "8회, 7회, 6회, 5회, 4회, 3회, 2회, 1회"가 미리 저장되어 있다.

[0073] 이러한 상황하에서 데이터 수신 장치(120)는 상기 메시지 "m"과 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ "가 수신되면, 상기 메시지 "m"을 상기 선정된 제2 해시 함수인 " $h(x)$ "에 입력으로 인가하여 메시지 해시 값 " $h(m)$ "을 생성할 수 있다.

[0074] 그리고 나서, 데이터 수신 장치(120)는 상기 메시지 해시 값 " $h(m)$ "을 8개의 데이터 그룹들로 분할한 후 각 그룹내에 포함되어 있는 데이터를 10진수의 숫자로 변환하여 8개의 검증 숫자들을 생성할 수 있다.

[0075] 상기 메시지 "m"이 위조되거나 변조되지 않았다고 가정하면, 상기 8개의 검증 숫자들은 앞서, 데이터 변환부(115)에서 생성된 숫자들과 동일한 "32, 592, 164, 7, 985, 223, 327, 814"가 될 것이다.

- [0076] 이때, 데이터 수신 장치(120)는 상기 표 2에서 나타난 상기 1024개의 랜덤 스트링들 각각에 대한 검증키 중에서 상기 8개의 검증 숫자들인 "32, 592, 164, 7, 985, 223, 327, 814"와 동일한 순번 정보가 할당되어 있는 8개의 검증키들을 선택할 수 있다.
- [0077] 관련해서, 데이터 수신 장치(120)는 상기 표 2에서 나타난 상기 1024개의 랜덤 스트링들 각각에 대한 검증키 중에서 상기 8개의 검증키들로 " $f^9(s_{32})$, $f^9(s_{592})$, $f^9(s_{164})$, $f^9(s_7)$, $f^9(s_{985})$, $f^9(s_{223})$, $f^9(s_{327})$, $f^9(s_{814})$ "를 선택할 수 있다.
- [0078] 그리고 나서, 데이터 수신 장치(120)는 상기 8개의 선정된 연산 횟수들인 "8회, 7회, 6회, 5회, 4회, 3회, 2회, 1회"를 참조하여 상기 8개의 해시 값들 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 각각에 대한 연쇄 해시 값 연산 횟수를 확인하고, 상기 8개의 해시 값들 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 각각에 대한 연쇄 해시 값 연산 횟수를 기초로 9번째 연쇄 해시 값 이 연산될 때까지 상기 8개의 해시 값들 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 각각에 대해 상기 선정된 제1 해시 함수인 " $f(x)$ "에 기초한 연쇄 해시 값 연산 과정을 수행하여 상기 8개의 해시 값들 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 각각에 대한 9번째 연쇄 해시 값을 연산할 수 있다.
- [0079] 관련해서, 상기 8개의 선정된 연산 횟수들이 "8회, 7회, 6회, 5회, 4회, 3회, 2회, 1회"이기 때문에 데이터 수신 장치(120)는 상기 8개의 해시 값들 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ "가 각각 "8회, 7회, 6회, 5회, 4회, 3회, 2회, 1회"에 해당하는 연쇄 해시 값 연산 과정을 수행했음을 확인할 수 있다.
- [0080] 이를 기초로, 데이터 수신 장치(120)는 상기 8개의 해시 값들 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ "에 대해서 상기 선정된 제1 해시 함수인 " $f(x)$ "에 기초한 연쇄 해시 값 연산 과정을 추가로 수행함으로써, 상기 8개의 해시 값들 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 각각에 대한 9번째 해시 값을 연산할 수 있다.
- [0081] 이와 관련하여, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^8(s_{32})$ "가 총 "8회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값임을 확인할 수 있기 때문에 " $f^8(s_{32})$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 1회만 더 수행함으로써, " $f^9(s_{32})$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.
- [0082] 그리고, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^7(s_{592})$ "가 총 "7회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값임을 확인할 수 있기 때문에 " $f^7(s_{592})$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 2회만 더 수행함으로써, " $f^9(s_{592})$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.
- [0083] 그리고, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^6(s_{164})$ "가 총 "6회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값임을 확인할 수 있기 때문에 " $f^6(s_{164})$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 3회만 더 수행함으로써, " $f^9(s_{164})$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.

4)"라는 9번째 연쇄 해시 값을 연산할 수 있다.

[0084] 그리고, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^5(s_7)$ "가 총 "5회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값을 확인할 수 있기 때문에 " $f^5(s_7)$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 4회만 더 수행함으로써, " $f^9(s_7)$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.

[0085] 그리고, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^4(s_{985})$ "가 총 "4회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값을 확인할 수 있기 때문에 " $f^4(s_{985})$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 5회만 더 수행함으로써, " $f^9(s_{985})$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.

[0086] 그리고, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^3(s_{223})$ "이 총 "3회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값을 확인할 수 있기 때문에 " $f^3(s_{223})$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 6회만 더 수행함으로써, " $f^9(s_{223})$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.

[0087] 그리고, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^2(s_{327})$ "이 총 "2회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값을 확인할 수 있기 때문에 " $f^2(s_{327})$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 7회만 더 수행함으로써, " $f^9(s_{327})$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.

[0088] 마지막으로, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 중 " $f^1(s_{814})$ "가 총 "1회" 연쇄 해시 값 연산 과정이 수행되어 생성된 해시 값을 확인할 수 있기 때문에 " $f^1(s_{814})$ "에 대해서는 상기 연쇄 해시 값 연산 과정을 8회만 더 수행함으로써, " $f^9(s_{814})$ "라는 9번째 연쇄 해시 값을 연산할 수 있다.

[0089] 이러한 방식으로 결국, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 각각에 대한 9번째 연쇄 해시 값들로 " $f^9(s_{32})$, $f^9(s_{592})$, $f^9(s_{164})$, $f^9(s_7)$, $f^9(s_{985})$, $f^9(s_{223})$, $f^9(s_{327})$, $f^9(s_{814})$ "를 연산할 수 있다.

[0090] 그 이후, 데이터 수신 장치(120)는 상기 8개의 해시 값들인 " $f^8(s_{32})$, $f^7(s_{592})$, $f^6(s_{164})$, $f^5(s_7)$, $f^4(s_{985})$, $f^3(s_{223})$, $f^2(s_{327})$, $f^1(s_{814})$ " 각각에 대해서 연산된 9번째 연쇄 해시 값들인 " $f^9(s_{32})$, $f^9(s_{592})$, $f^9(s_{164})$, $f^9(s_7)$, $f^9(s_{985})$, $f^9(s_{223})$, $f^9(s_{327})$, $f^9(s_{814})$ "와 상기 표 2에서 나타난 상기 1024개의 랜덤 스트링들 각각에 대한 검증키 중에서 선택된 상기 8개의 검증키들인 " $f^9(s_{32})$, $f^9(s_{592})$, $f^9(s_{164})$, $f^9(s_7)$, $f^9(s_{985})$, $f^9(s_{223})$, $f^9(s_{327})$, $f^9(s_{814})$ "를 서로 비교하여 양 값이 모두 일치하는 것으로 확인되면, 상기 메시지 "m"이 데이터 전송 장치(110)에 저장되어 있는 키 저장부(113) 상에 정말로 저장되어 있는 해시 값들을 기초로 전자서명되었음을 확인할 수 있어, 최종적으로 상기 메시지 "m"에 대한 인증을 완료할 수 있다.

[0091] 결국, 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치(110)는 소정의 랜

덤 스트링들을 생성하고, 상기 랜덤 스트링들에 대해 연쇄 해시 값 연산 과정을 수행하여 생성된 해시 값들을 키 저장부(113) 상에 저장해 놓고, 상기 랜덤 스트링들에 대해 상기 연쇄 해시 값 연산 과정을 추가적으로 수행함으로써, 검증키를 생성하여 상기 검증키를 데이터 수신 장치(120)로 전송한 후 데이터 수신 장치(120)로 전송할 메시지를 키 저장부(113)에 저장되어 있는 해시 값들을 기초로 전자서명하여 데이터 수신 장치(120)로 전송하면, 데이터 수신 장치(120)가 상기 검증키를 기초로 전자서명 값을 검증할 수 있도록 유도함으로써, 상기 전송 메시지에 대한 부인 방지 기능을 제공할 수 있다.

[0092] 도 2는 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법을 도시한 순서도이다.

[0093] 단계(S210)에서는 t (t 는 자연수)개의 랜덤 스트링들을 생성한 후 상기 t 개의 랜덤 스트링들 각각에 대해 상기 t 개의 랜덤 스트링들 각각을 지시하는 순번 정보를 할당한다.

[0094] 단계(S220)에서는 상기 t 개의 랜덤 스트링들 각각에 대해서, 선정된 제1 해시 함수에 기초한 연쇄 해시 값 연산 과정을 k (k 는 자연수)회 수행하여 상기 k 회의 연쇄 해시 값 연산 과정에서 생성되는 각각의 해시 값들과 상기 각각의 해시 값들을 생성하기 위해서 수행된 연쇄 해시 값 연산 횟수를 키 저장부 상에 서로 대응되도록 저장함으로써, 상기 키 저장부 상에 상기 t 개의 랜덤 스트링들 각각에 대한 k 개의 해시 값들과 상기 k 개의 해시 값들 각각에 대응하는 연쇄 해시 값 연산 횟수를 저장한다.

[0095] 이때, 본 발명의 일실시예에 따르면, 단계(S220)에서는 상기 t 개의 랜덤 스트링들 각각에 대해서, 상기 t 개의 랜덤 스트링들을 상기 선정된 제1 해시 함수에 입력으로 인가하여 해시 값을 연산하고, 상기 연산된 해시 값을 상기 선정된 제1 해시 함수에 다시 입력으로 인가하여 추가 해시 값을 연산하는 방식의 상기 연쇄 해시 값 연산 과정을 상기 k 회 수행할 수 있다.

[0096] 단계(S230)에서는 데이터 수신 장치로 전송할 메시지를 선정된 제2 해시 함수에 입력으로 인가하여 메시지 해시 값을 생성한다.

[0097] 단계(S240)에서는 상기 메시지 해시 값을 n 개 (n 은 자연수)의 데이터 그룹들로 분할하고, 각 그룹내에 포함되어 있는 데이터를 i (i 는 자연수)진수의 숫자로 변환하여 n 개의 숫자들을 생성한다.

[0098] 단계(S250)에서는 상기 t 개의 랜덤 스트링들 중 상기 n 개의 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n 개의 랜덤 스트링들을 선택하고, 상기 n 개의 랜덤 스트링들 별로 하나의 해시 값을 추출하기 위해서 미리 설정되어 있는 n 개의 선정된 연산 횟수들을 참조하여 상기 키 저장부로부터 상기 n 개의 랜덤 스트링들 별로, 상기 n 개의 선정된 연산 횟수들 중 각 랜덤 스트링에 대응하는 선정된 연산 횟수와 일치하는 연쇄 해시 값 연산 횟수가 대응되어 저장되어 있는 하나의 해시 값을 추출함으로써, 총 n 개의 해시 값들을 추출한다.

[0099] 단계(S260)에서는 상기 데이터 수신 장치에 대해 상기 메시지와 상기 n 개의 해시 값들을 전송한다.

[0100] 이때, 본 발명의 일실시예에 따르면, 상기 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법은 단계(S230) 이전에 상기 t 개의 랜덤 스트링들 각각에 대해서 상기 연쇄 해시 값 연산 과정을 $k+1$ 회 수행하여 $k+1$ 번째 연쇄 해시 값을 연산하고, 상기 t 개의 랜덤 스트링들 각각에 대해서 연산된 상기 $k+1$ 번째 연쇄 해시 값을 상기 t 개의 랜덤 스트링들 각각에 대한 검증키로 결정함과 동시에 상기 t 개의 랜덤 스트링들 각각에 대한 검증키에 대해 상기 t 개의 랜덤 스트링들 각각에 할당되어 있는 순번 정보와 동일한 순번 정보를 할당하는 단계 및 상기 t 개의 랜덤 스트링들 각각에 대한 검증키를 상기 데이터 수신 장치로 전송하는 단계를 더 포함할 수 있다.

[0101] 이때, 본 발명의 일실시예에 따르면, 상기 데이터 수신 장치는 메모리 상에 상기 선정된 제1 해시 함수, 상기 선정된 제2 해시 함수, 상기 n 개의 선정된 연산 횟수들 및 상기 t 개의 랜덤 스트링들 각각에 대한 검증키를 저장하고 있을 수 있다.

[0102] 이때, 상기 데이터 수신 장치는 상기 메시지와 상기 n 개의 해시 값들이 수신되면, 상기 메시지를 상기 선정된 제2 해시 함수에 입력으로 인가하여 상기 메시지 해시 값을 생성하고, 상기 메시지 해시 값을 n 개의 데이터 그룹들로 분할한 후 각 그룹내에 포함되어 있는 데이터를 상기 i 진수의 숫자로 변환하여 n 개의 검증 숫자들을 생성하며, 상기 t 개의 랜덤 스트링들 각각에 대한 검증키 중에서 상기 n 개의 검증 숫자들 각각과 동일한 순번 정보가 할당되어 있는 n 개의 검증키들을 선택한 후 상기 n 개의 선정된 연산 횟수들을 참조하여 상기 n 개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 확인하고, 상기 n 개의 해시 값들 각각에 대한 연쇄 해시 값 연산 횟수를 기초로 상기 $k+1$ 번째 연쇄 해시 값이 연산될 때까지 상기 n 개의 해시 값들 각각에 대해 상기 선정된 제1 해시 함수에 기초한 상기 연쇄 해시 값 연산 과정을 수행하여 상기 n 개의 해시 값들 각각에 대한 상기 $k+1$ 번째

연쇄 해시 값을 연산한 후 상기 n개의 해시 값들 각각에 대한 상기 k+1번째 연쇄 해시 값이 상기 n개의 검증키들과 모두 일치하는 것으로 확인되면, 상기 메시지에 대한 인증을 완료할 수 있다.

[0103] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법은 도 1을 이용하여 설명한 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0104] 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0105] 또한, 본 발명의 일실시예에 따른 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 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 광기록 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. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0106] 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.

[0107] 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

[0108] 110: 전송 메시지에 대한 부인 방지가 가능한 데이터 전송 장치

111: 랜덤 스트링(string) 생성부 112: 해시 값 저장부

113: 키 저장부 114: 메시지 해시 값 생성부

115: 데이터 변환부 116: 해시 값 추출부

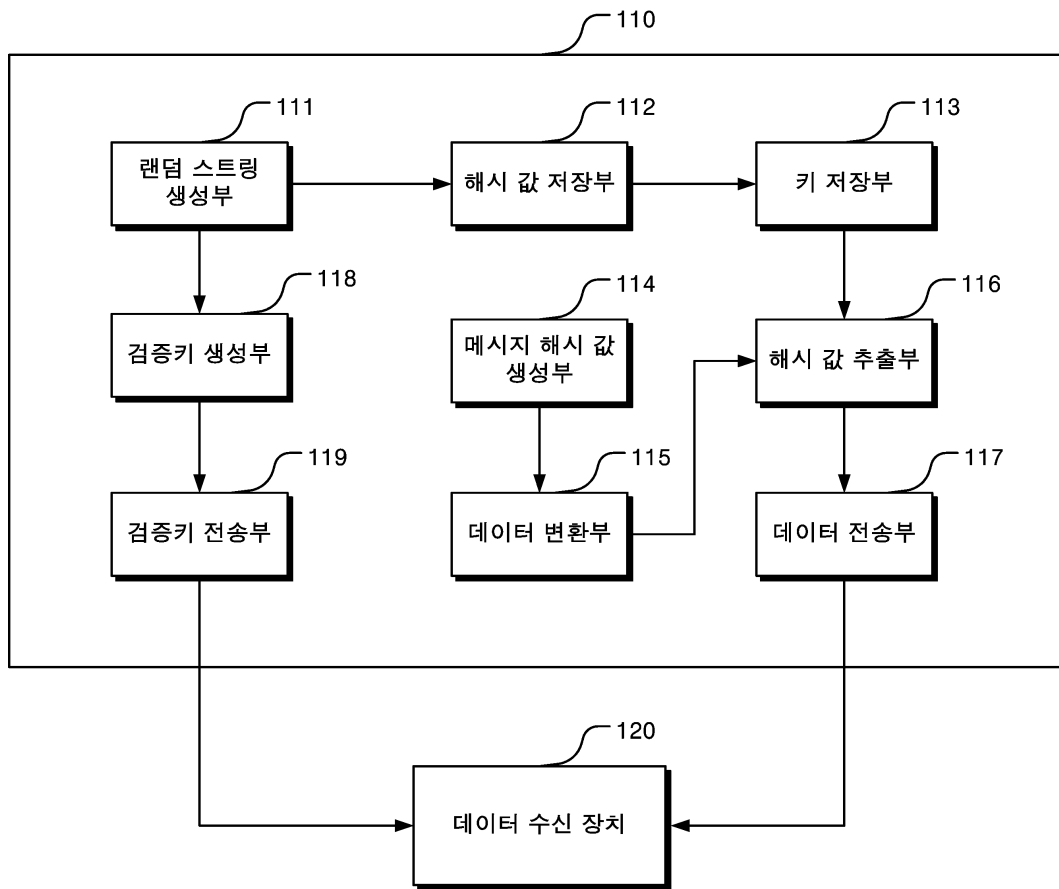
117: 데이터 전송부 118: 검증키 생성부

119: 검증키 전송부

120: 데이터 수신 장치

도면

도면1



도면2

