(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0085926
(43) 공개일자 2017년07월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06Q 20/06* (2012.01)
G06Q 20/38 (2012.01) *G06Q 40/02* (2012.01)
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0838 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2016-0035563
(22) 출원일자 2016년03월24일
심사청구일자 2016년03월24일
(30) 우선권주장
1020160005635 2016년01월15일 대한민국(KR)

(71) 출원인
단국대학교 산학협력단
경기 용인시 수지구 죽전로 152, 내 (죽전동, 단국대학교)
(72) 발명자
김준모
경기도 용인시 기흥구 구성로39번길 13, 102동 908호(마북동, 우림필유아파트)
(74) 대리인
제일특허법인

전체 청구항 수 : 총 14 항

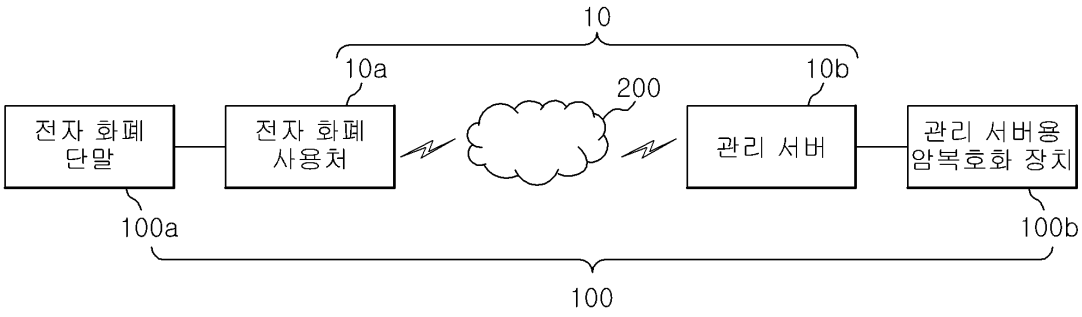
(54) 발명의 명칭 **전자 화폐 단말 및 이를 이용하여 전자 화폐를 제공하는 방법**

(57) 요 약

본 발명의 일 실시예에 따른 전자 화폐 단말은 상기 전자 화폐 단말의 잔액을 저장하는 금액 저장부와, 상기 전자 화폐 단말을 관리하는 관리 서버에 대해서, 상기 관리 서버와 송수신하는 데이터가 입출력되는 데이터 포트부와, 기 설정된 복수 개의 키를 저장하는 키 저장부와, 상기 복수 개의 키 중 어느 하나인 제1 키를 기초로 상기

(뒷면에 계속)

대 표 도 - 도1



관리 서버로부터 상기 잔액을 갱신하는 잔액 관련 데이터가 암호화된 상태로 수신되면 이를 복호화하고, 상기 복호화된 잔액 관련 데이터를 기초로 상기 금액 저장부에 저장된 잔액이 갱신되도록 처리하는 처리부와, 상기 관리 서버가 송신할 데이터를 암호화하거나 상기 관리 서버가 수신한 암호화된 데이터를 복호화하는 관리 서버용 암복호화 장치가 상기 관리 서버와 연결될 때, 상기 전자 화폐 단말을 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결시키는 연결부를 포함하며, 상기 복수 개의 키는 상기 전자 화폐 단말에 포함된 연결부가 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결되면 생성되어 상기 키 저장부에 저장된다.

(52) CPC특허분류
G06Q 20/382 (2013.01)
G06Q 40/02 (2013.01)
H04L 9/0869 (2013.01)
H04L 9/14 (2013.01)
H04L 9/3263 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 IITP-2016-R0992-16-1012
부처명 미래창조과학부
연구관리전문기관 정보통신산업징흥원
연구사업명 대학ICT 연구센터 육성지원사업
연구과제명 세이프 웰빙을 위한 IoT 기반 스마트 웨어러블 SW 기술개발
기 여 율 1/1
주관기관 단국대학교 산학협력단
연구기간 2016.01.01 ~ 2016.12.31

명 세 서

청구범위

청구항 1

전자 화폐 단말로서,

상기 전자 화폐 단말의 잔액을 저장하는 금액 저장부와,

상기 전자 화폐 단말을 관리하는 관리 서버에 대해서, 상기 관리 서버와 송수신하는 데이터가 입출력되는 데이터 포트부와,

기 설정된 복수 개의 키를 저장하는 키 저장부와,

상기 복수 개의 키 중 어느 하나인 제1 키를 기초로 상기 관리 서버로부터 상기 잔액을 갱신하는 잔액 관련 데이터가 암호화된 상태로 수신되면 이를 복호화하고, 상기 복호화된 잔액 관련 데이터를 기초로 상기 금액 저장부에 저장된 잔액이 갱신되도록 처리하는 처리부와,

상기 관리 서버가 송신할 데이터를 암호화하거나 상기 관리 서버가 수신한 암호화된 데이터를 복호화하는 관리 서버용 암복호화 장치가 상기 관리 서버와 연결될 때, 상기 전자 화폐 단말을 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결시키는 연결부를 포함하며,

상기 복수 개의 키는,

상기 전자 화폐 단말에 포함된 연결부가 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결되면 생성되어 상기 키 저장부에 저장되는

전자 화폐 단말.

청구항 2

제 1 항에 있어서,

상기 금액 저장부는,

상기 금액을 저장하는 공간이 1개인 것을 특징으로 하는

전자 화폐 단말.

청구항 3

제 1 항에 있어서,

상기 처리부는 상기 제1 키를 기초로 상기 잔액을 암호화하고,

상기 데이터 포트부는 상기 암호화된 잔액을 출력하여 상기 관리 서버로 송신되도록 하는

전자 화폐 단말.

청구항 4

제 1 항에 있어서,

상기 처리부에 의하여 상기 금액 저장부에 저장된 잔액이 갱신될 때마다 그 값이 기 정의된 규칙에 따라 변화하는 변수를 갖는 위조 방지부를 더 포함하며,

상기 처리부는,

상기 제1 키를 기초로 상기 잔액 및 상기 변수를 암호화하며,

상기 데이터 포트부는 상기 암호화된 잔액 및 상기 변수를 출력하여 상기 관리 서버로 송신되도록 하는

전자 화폐 단말.

청구항 5

제 1 항에 있어서,

상기 키 저장부는,

상기 제1 키가 상기 처리부로 전달되는 경로인 키 버스(key bus)를 통해서 상기 처리부와 연결되지만, 상기 키 버스를 통해서 상기 데이터 포트부와는 연결되지 않는

전자 화폐 단말.

청구항 6

제 1 항에 있어서,

상기 키 저장부와 상기 관리 서버용 암복호화 장치에 포함된 키 저장부는,

동일한 값의 복수 개의 키를 저장하는

전자 화폐 단말.

청구항 7

제 1 항에 있어서,

난수를 생성하는 난수 생성부를 더 포함하며,

상기 복수 개의 키는,

상기 난수 생성부에 의하여 생성된 난수를 기초로 생성되는

전자 화폐 단말.

청구항 8

제 1 항에 있어서,

상기 처리부는,

상기 잔액을, 상기 전자 화폐 단말과 상기 관리 서버용 암복호화 장치가 모두 알고 있는 식별자와 결합시켜서 결합 데이터를 생성한 뒤, 상기 결합 데이터를 상기 제1 키를 기초로 암호화하고,

상기 데이터 포트부는,

상기 결합 데이터를 출력하여 상기 관리 서버로 송신되도록 하는

전자 화폐 단말.

청구항 9

제 8 항에 있어서,

상기 처리부는,

상기 복수 개의 키 중 상기 전자 화폐 단말과 상기 관리 서버용 암복호화 장치가 모두 알고 있는 기 설정된 적어도 두 개 이상의 키를 기초로 상기 식별자를 생성하는

전자 화폐 단말.

청구항 10

제 8 항에 있어서,

난수를 생성하는 난수 생성부를 더 포함하고,

상기 식별자는,

기 설정된 개수의 복수 개의 비트로 구성되며, 상기 복수 개의 비트 중 일부의 비트는 적어도 두 개 이상의 키에 의하여 값이 정해지고, 상기 복수 개의 비트 중 나머지 비트는 상기 난수 생성부에 의하여 생성된 난수에 의하여 값이 정해지는

전자 화폐 단말.

청구항 11

제 1 항에 있어서,

상기 전자 화폐 단말에 비정상적인 것으로 정의된 행위가 가해지는 것을 인식하며, 상기 행위가 가해지는 것이 인식되면 상기 키 저장부에 저장된 상기 복수 개의 키를 삭제하는 보호부를 더 포함하는

전자 화폐 단말.

청구항 12

제 1 항에 있어서,

상기 복수 개의 키는 새로운 복수 개의 키로 변경 가능한

전자 화폐 단말.

청구항 13

제 12 항에 있어서,

상기 복수 개의 키가 상기 새로운 복수 개의 키로 변경될 때,

상기 전자 화폐 단말과 상기 관리 서버용 암복호화 장치가 서로 알고 있는 기 설정된 값을 기초로 상기 새로운 복수 개의 키가 생성되어 변경되는

전자 화폐 단말.

청구항 14

전자 화폐 단말에 의하여 전자 화폐를 제공하는 방법으로서,

상기 전자 화폐 단말을 관리하는 관리 서버로부터, 상기 전자 화폐 단말에 저장된 잔액을 갱신하는 잔액 관련

데이터를 암호화된 상태로 수신하는 단계와,

기 저장된 복수 개의 키 중 어느 하나인 제1 키를 기초로 상기 암호화된 잔액 관련 데이터를 복호화하는 단계와,

상기 복호화된 잔액 관련 데이터를 기초로 상기 잔액을 갱신시키는 단계를 포함하며,

상기 복수 개의 키는,

상기 관리 서버가 송신할 데이터를 암호화하거나 상기 관리 서버가 수신한 암호화된 데이터를 복호화하는 관리 서버용 암복호화 장치가 상기 관리 서버와 연결될 때, 상기 전자 화폐 단말에 포함된 연결부가 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결되면 생성되어 저장되는

전자 화폐를 제공하는 방법

발명의 설명

기 술 분 야

[0001] 본 발명은 전자 화폐 단말 및 이를 이용하여 전자 화폐를 제공하는 방법에 관한 것이다. 보다 자세하게는 전자 화폐 단말을 관리하는 관리 서버와 전자 화폐 단말 사이에서 전자 화폐의 금액과 같은 데이터가 송수신될 때, 이러한 데이터의 암복호화에 사용되는 키는 상기 관리 서버와 연결되는 관리 서버용 암복호화 장치가 전자 화폐 단말과 서로 간에 물리적으로 오프라인 상에서 연결되었을 때 생성 및 공유되도록 하고, 이러한 키를 이용하여 데이터를 암복호화한 뒤 송수신되도록 함으로써, 전자 화폐에 대한 해킹 가능성을 원천적으로 차단하는 기술에 관한 것이다.

배 경 기 술

[0002] 기존의 암복호화 시스템의 경우 비대칭키 시스템인 RSA를 이용한 대칭키 전송과, 이와 같이 전송된 대칭키에 의한 데이터의 암복호화에 의하여 이루어진다. 참고로, RSA는 두 개의 큰 소수 (p,q)를 곱하여 만든 수를 기반으로 공개키와 비밀키를 생성하며, 이와 같이 생성된 공개키와 비밀키를 이용하여 데이터를 암호화하는 방법이다.

[0003] 이러한 기존의 암복호화 시스템은 전자 화폐 분야에도 사용될 수 있다. 그런데, 앞서 설명한 RSA를 이용할 경우 데이터는 공개키로 암호화되어 공유 통신망을 통해 전달되며, 공개키는 인터넷 상에서 공개 및 공유된다. 여기서, 공개키를 기반으로 비밀키가 찾아내어 진다면, 암호화된 데이터는 해킹될 수 있다. 물론, 공개키를 기반으로 비밀키를 찾아내는 것은 매우 어려운 작업으로 알려져 있다. 그러나, 공개키를 기반으로 비밀키를 찾아내는 것이 불가능하다고 수학적으로 증명된 것은 아니다. 아울러, 비밀키를 수리적인 방법으로 찾아내는 경우도 종종 발생하고 있다. 또한, 해커와 같은 악성 행위자가 특정 방법으로 적절한 응답시간 내에 구할 수 있는 소수 (p,q)를 구해놓았다면, 비밀키는 훨씬 수월하게 찾을 수 있다.

[0004] 따라서, 전자 화폐와 같이 그 보안성이 고도로 중요한 분야에서는 데이터, 특히 전자 화폐의 금액과 같은 데이터에 대한 해킹 가능성을 보다 효과적으로 차단할 수 있는 방법에 대한 요구가 있다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국특허공개공보 2005-0017493 , 공개일자 2005년 02월 22일

발명의 내용

해결하려는 과제

[0006] 본 발명의 해결하고자 하는 과제는 데이터의 암복호화에 사용되는 키를 분배하여 공유시키는 과정에서, 이러한 키에 대한 해킹 가능성을 보다 근본적으로 차단하는 기술을 제공하는 것이다.

[0007] 또한, 이러한 기술을 전자 화폐에 적용하여 전자 화폐에 대한 해킹 가능성을 차단하는 것이다.

[0008] 다만, 본 발명의 해결하고자 하는 과제는 이상에서 언급한 것으로 제한되지 않으며, 언급되지 않은 또 다른 해결하고자 하는 과제는 아래의 기재로부터 본 발명이 속하는 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0009] 본 발명의 일 실시예에 따른 전자 화폐 단말은 상기 전자 화폐 단말의 잔액을 저장하는 금액 저장부와, 상기 전자 화폐 단말을 관리하는 관리 서버에 대해서, 상기 관리 서버와 송수신하는 데이터가 입출력되는 데이터 포트부와, 기 설정된 복수 개의 키를 저장하는 키 저장부와, 상기 복수 개의 키 중 어느 하나인 제1 키를 기초로 상기 관리 서버로부터 상기 잔액을 갱신하는 잔액 관련 데이터가 암호화된 상태로 수신되면 이를 복호화하고, 상기 복호화된 잔액 관련 데이터를 기초로 상기 금액 저장부에 저장된 잔액이 갱신되도록 처리하는 처리부와, 상기 관리 서버가 송신할 데이터를 암호화하거나 상기 관리 서버가 수신한 암호화된 데이터를 복호화하는 관리 서버용 암복호화 장치가 상기 관리 서버와 연결될 때, 상기 전자 화폐 단말을 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결시키는 연결부를 포함하며, 상기 복수 개의 키는 상기 전자 화폐 단말에 포함된 연결부가 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결되면 생성되어 상기 키 저장부에 저장된다.

[0010] 또한, 상기 금액 저장부는 상기 금액을 저장하는 공간이 1개인 것을 특징으로 할 수 있다.

[0011] 또한, 상기 처리부는 상기 제1 키를 기초로 상기 잔액을 암호화하고, 상기 데이터본 발명의 일 실시예에 따른 전자 화폐 단말은 상기 전자 화폐 단말의 잔액을 저장하는 금액 저장부와, 상기 전자 화폐 단말을 관리하는 관리 서버에 대해서, 상기 관리 서버와 송수신하는 데이터가 입출력되는 데이터 포트부와, 기 설정된 복수 개의 키를 저장하는 키 저장부와, 상기 복수 개의 키 중 어느 하나인 제1 키를 기초로 상기 관리 서버로부터 상기 잔액을 갱신하는 잔액 관련 데이터가 암호화된 상태로 수신되면 이를 복호화하고, 상기 복호화된 잔액 관련 데이터를 기초로 상기 금액 저장부에 저장된 잔액이 갱신되도록 처리하는 처리부와, 상기 관리 서버가 송신할 데이터를 암호화하거나 상기 관리 서버가 수신한 암호화된 데이터를 복호화하는 관리 서버용 암복호화 장치가 상기 관리 서버와 연결될 때, 상기 전자 화폐 단말을 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결시키는 연결부를 포함하며, 상기 복수 개의 키는 상기 전자 화폐 단말에 포함된 연결부가 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결되면 생성되어 상기 키 저장부에 저장된다.

[0012] 또한, 상기 금액 저장부는 상기 금액을 저장하는 공간이 1개인 것을 특징으로 할 수 있다.

[0013] 또한, 상기 처리부는 상기 제1 키를 기초로 상기 잔액을 암호화하고, 상기 데이터 포트부는 상기 암호화된 잔액을 출력하여 상기 관리 서버로 송신되도록 할 수 있다.

[0014] 또한, 상기 처리부에 의하여 상기 금액 저장부에 저장된 잔액이 갱신될 때마다 그 값이 증가하는 변수를 갖는 위조 방지부를 더 포함하며, 상기 처리부는 상기 제1 키를 기초로 상기 잔액 및 상기 변수를 암호화하며, 상기 데이터 포트부는 상기 암호화된 잔액 및 상기 변수를 출력하여 상기 관리 서버로 송신되도록 할 수 있다.

[0015] 또한, 상기 키 저장부는 상기 제1 키가 상기 처리부로 전달되는 경로인 키 버스(key bus)를 통해서 상기 처리부와 연결되지만, 상기 키 버스를 통해서 상기 데이터 포트부와는 연결되지 않을 수 있다.

[0016] 또한, 상기 키 저장부와 상기 관리 서버용 암복호화 장치에 포함된 키 저장부는 동일한 값의 복수 개의 키를 저장할 수 있다.

[0017] 또한, 난수를 생성하는 난수 생성부를 더 포함하며, 상기 복수 개의 키는 상기 난수 생성부에 의하여 생성된 난수를 기초로 생성될 수 있다.

[0018] 상기 처리부는 상기 잔액을, 상기 전자 화폐 단말과 상기 관리 서버용 암복호화 장치가 모두 알고 있는 식별자와 결합시켜서 결합 데이터를 생성한 뒤, 상기 결합 데이터를 상기 제1 키를 기초로 암호화하고, 상기 데이터 포트부는 상기 결합 데이터를 출력하여 상기 관리 서버로 송신되도록 할 수 있다.

[0019] 또한, 상기 처리부는 상기 복수 개의 키 중 상기 전자 화폐 단말과 상기 관리 서버용 암복호화 장치가 모두 알고 있는 기 설정된 적어도 두 개 이상의 키를 기초로 상기 식별자를 생성할 수 있다.

[0020] 또한, 난수를 생성하는 난수 생성부를 더 포함하고, 상기 식별자는 기 설정된 개수의 복수 개의 비트로 구성되며, 상기 복수 개의 비트 중 일부의 비트는 상기 적어도 두 개 이상의 키에 의하여 값이 정해지고, 상기 복수 개의 비트 중 나머지 비트는 상기 난수 생성부에 의하여 생성된 난수에 의하여 값이 정해질 수 있다.

[0021] 또한, 상기 전자 화폐 단말에 비정상적인 것으로 정의된 행위가 가해지는 것을 인식하며, 상기 행위가 가해지는 것이 인식되면 상기 키 저장부에 저장된 상기 복수 개의 키를 삭제하는 보호부를 더 포함할 수 있다.

[0022] 또한, 상기 복수 개의 키는 새로운 복수 개의 키로 변경 가능할 수 있다.

[0023] 또한, 상기 복수 개의 키가 상기 새로운 복수 개의 키로 변경될 때, 상기 전자 화폐 단말과 상기 관리 서버용 암복호화 장치가 서로 알고 있는 기 설정된 값을 기초로 상기 새로운 복수 개의 키가 생성되어 변경될 수 있다.

[0024] 본 발명의 일 실시예에 따른 전자 화폐 제공 방법은 전자 화폐 단말에 의하여 수행되며, 상기 전자 화폐 단말을 관리하는 관리 서버로부터, 상기 전자 화폐 단말에 저장된 잔액을 갱신하는 잔액 관련 데이터를 암호화된 상태로 수신하는 단계와, 기 저장된 복수 개의 키 중 어느 하나인 제1 키를 기초로 상기 암호화된 잔액 관련 데이터를 복호화하는 단계와, 상기 복호화된 잔액 관련 데이터를 기초로 상기 잔액을 갱신시키는 단계를 포함하며, 상기 복수 개의 키는 상기 관리 서버가 송신할 데이터를 암호화하거나 상기 관리 서버가 수신한 암호화된 데이터를 복호화하는 관리 서버용 암복호화 장치가 상기 관리 서버와 연결될 때, 상기 전자 화폐 단말에 포함된 연결부가 상기 관리 서버용 암복호화 장치에 포함된 연결부와 물리적으로 연결되면 생성되어 저장된다.

발명의 효과

[0025] 본 발명의 실시예에 따르면, 데이터의 암복호화에 사용되는 키를 생성, 분배 및 공유시키는 과정에서 이러한 키가 해킹될 가능성이 보다 근본적으로 차단된다. 따라서, 이를 이용하여 전자 화폐에 대한 해킹 가능성을 원천적으로 차단시킬 수 있다.

도면의 간단한 설명

[0026] 도 1은 본 발명의 일 실시예에 따른 전자 화폐 단말이 사용되는 시스템을 예시적으로 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 전자 화폐 단말의 구성을 도시한 도면이다.

도 3a는 도 2에 도시된 금액 저장부 및 위조 방지부를 도시한 도면이다.

도 3b는 도 2에 도시된 금액 저장부 및 위조 방지부가 전자 화폐 단말에서 이용되는 것을 예시적으로 도시한 도면이다.

도 4은 본 발명의 일 실시예에 따른 전자 화폐 단말과 관리 서버용 암복호화 장치가 서로 간에 연결된 것을 개념적으로 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따른 전자 화폐 단말에서 키 저장부와 처리부 및 데이터 포트부가 연결된 것을 개념적으로 도시한 도면이다.

도 6a 및 6b는 본 발명의 일 실시예에 따른 식별자를 개념적으로 도시한 도면이다.

도 7은 본 발명의 일 실시예에 따른 전자 화폐를 제공하는 방법의 절차를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0027] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0028] 본 발명의 실시예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명의 실시예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0029] 설명에 앞서, 일 실시예에 따른 전자 화폐 단말에 의하여 데이터가 암호화되면 이와 같이 암호화된 데이터는 관리 서버용 암복호화 장치에 의하여 복호화될 수 있으며, 그 반대도 가능한 것으로 정의하기로 한다.

[0030] 도 1은 본 발명의 일 실시예에 따른 전자 화폐 단말이 사용되는 시스템을 예시적으로 도시한 도면이다.

[0031] 도 1을 참조하면, 시스템은 전자 화폐 단말(100a), 전자 화폐 사용처(10a), 관리 서버(10b) 및 관리 서버용 암복호화 장치(100b)에 의하여 구성된다. 여기서, 도 1에 도시된 시스템은 일 실시예에 따른 전자 화폐 단말(100a)이 적용되는 예를 도시한 것에 불과하다.

[0032] 전자 화폐 사용처(10a)와 관리 서버(10b)는 네트워크(200)에 의하여 연결된다. 네트워크(200)는 CDMA, 3G, 4G, LTE-A, 블루투스, 와이파이, NFC 또는 IR과 같은 무선 통신 네트워크이거나 이와 달리 LAN과 같은 유선 통신 네트워크일 수 있다.

[0033] 전자 화폐 사용처(10a)는 전자 화폐 단말(100a)이 연결되어 사용되는 곳이다. 이를 위하여 전자 화폐 단말(100a) 및 전자 화폐 사용처(10a)는 서로를 연결시키기 위한 구성(미도시)을 각각 포함할 수 있다. 전자 화폐 사용처(10a)는 현금 입출금기(ATM) 또는 상점 등에 설치되어 전자 화폐 단말(100a)를 읽고 그로부터 금액을 출금하는 결제 단말기 등일 수 있으나 이에 한정되는 것은 아니다.

[0034] 관리 서버(10b)는 전자 화폐 단말(100a) 자체를 관리한다. 이를 위하여, 전자 화폐 단말(100a)이 복수 개일 때 이들 각각에는 고유 번호가 할당될 수 있는데, 관리 서버(10b)는 이러한 고유 번호 및 고유 번호에 대응되는 전자 화폐 단말(100a)의 특성 등을 미리 저장한다. 관리 서버(10b)는 이러한 고유 번호를 기초로 전자 화폐 단말(100a)을 관리한다.

[0035] 관리 서버(10b)는 전자 화폐 단말(100a)에 저장된 잔액을 관리한다. 예컨데, 관리 서버(10b)는 고유 번호가 i인 전자 화폐 단말에는 잔액이 얼마인지 등을 저장 및 관리할 수 있다. 관리 서버(10a)는 일반적인 은행에 설치된 서버 또는 전자 화폐를 전문적으로 취급하는 은행에 설치된 서버일 수 있다.

[0036] 관리 서버용 암복호화 장치(100b)는 관리 서버(10b)와 연결된다. 이를 위하여 관리 서버용 암복호화 장치(100b)와 관리 서버(10b)는 서로 간을 연결시키기 위한 구성을 각각 포함(미도시)할 수 있다.

[0037] 관리 서버용 암복호화 장치(100b)는 관리 서버(10b)가 전자 화폐 단말(100a) 또는 전자 화폐 사용처(10a)로 송신하고자 하는 데이터를 암호화한다. 또한 관리 서버용 암복호화 장치(100a)는 전자 화폐 단말(100a)이나 전자 화폐 사용처(10a)로부터 수신된 데이터가 암호화되어 있으면 이를 복호화한다. 이 때 암호화되는 데이터는 전자 화폐 단말(100a)의 잔액(잔액 관련 데이터) 등일 수 있는데 이에 대해서는 후술하기로 한다. 또한, 관리 서버용 암복호화 장치(100b)가 데이터를 암호화하고 복호화하는 것은 전자 화폐 단말(100a)이 데이터를 암호화하고 복호화하는 것과 동일하므로, 관리 서버용 암복호화 장치(100b)가 데이터를 암호화하고 복호화하는 것에 대한 설명은 전자 화폐 단말(100a)이 데이터를 암복호화하는 부분의 설명으로 대체하기로 한다.

[0038] 전자 화폐 단말(100a)은 전자 화폐 사용처(10a)에서 사용되는 전자 화폐다. 이러한 전자 화폐 단말(100a)은 후술할 전자 화폐의 기능을 수행하도록 프로그램된 명령어를 저장하는 메모리 및 이러한 명령어를 수행하는 프로세서에 의하여 구현 가능하다.

[0039] 보다 구체적으로 살펴보면, 전자 화폐 단말(100a)은 잔액을 저장한다. 전자 화폐 단말(100a)의 잔액이나 기타 정보 등은 암호화된 뒤, 전자 화폐 사용처(10a)를 거쳐서 관리 서버(10b)로 전달되거나 또는 전자 화폐 단말(100a)로부터 직접 관리 서버(10b)로 전달될 수 있다.

[0040] 아울러, 전자 화폐 단말(100a)이 전자 화폐 사용처(10a)에서 사용되면, 전자 화폐 단말(100a)은 사용된 금액을 제외한 잔액 등을 암호화한다. 암호화된 잔액이나 기타 정보는 전자 화폐 사용처(10a)를 거쳐서 관리 서버(10b)로 전달되거나 또는 전자 화폐 단말(100a)로부터 직접 관리 서버(10b)로 전달될 수 있다.

[0041] 또한, 전자 화폐 단말(100a)은 관리 서버(10b)로부터, 관리 서버(10b)가 관리하는 잔액 등을 수신할 수 있다. 이 때 수신된 잔액은 암호화된 상태일 수 있다. 이 경우 전자 화폐 단말(100a)은 암호화된 잔액을 복호화한 뒤, 현재의 잔액을 수신된 잔액으로 갱신할 수 있다.

[0042] 이하에서는, 전술한 기능을 수행하는 전자 화폐 단말(100a)의 구체적인 구성에 대하여 보다 자세하게 살펴보기로 한다. 이 때, 전자 화폐 단말(100a)의 구성은 관리 서버용 암복호화 장치(100b)와 동일하며, 전자 화폐 단말(100a)과 관리 서버용 암복호화 장치(100b)는 통칭하여 암복호화 장치(100)로 지칭될 수 있다.

[0043] 도 2는 본 발명의 일 실시예에 따른 전자 화폐 단말(100a)의 구성에 대하여 도시한 도면이다.

[0044] 도 2를 참조하면, 전자 화폐 단말(100a)은 금액 저장부(101), 키 저장부(110), 처리부(120), 데이터 포트부(130) 및 연결부(140)를 포함한다. 또한, 전자 화폐 단말(100)은 추가적으로 위조 방지부(103), 난수 생성부(150), 보호부(160), 리셋부(170), 알고리즘 저장부(180) 및 접속부(190)를 포함할 수 있다. 이 중에서, 처리부(120)와 난수 생성부(150)는 이들의 기능을 수행하도록 프로그램된 명령어를 저장하는 메모리 및 이러한 명령어를 수행하는 마이크로프로세서에 의하여 구현될 수 있다.

[0045] 연결부(140)에 대하여 먼저 살펴보면, 연결부(140)는 전자 화폐 단말(100a)이 관리 서버용 암복호화 장치(100b)와 연결되어야 하는 경우, 이들을 서로 간에 연결시키는 구성이다. 예컨데, 연결부(140)는 하드웨어적으로 구현된 커넥터일 수 있다. 도 4를 참조하여 보다 자세하게 살펴보면, 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)은 서로 간에 연결부(140)를 통하여 물리적으로, 그리고 이들이 각각 복수 개이면 링 형태로 연결될 수 있다. 즉, 연결부(140)는 암복호화 장치(100) 복수 개를 서로 간에 물리적으로, 오프라인 상에서 연결시킨다.

[0046] 다시 도 2를 참조하면, 금액 저장부(101)는 전자 화폐 단말(100a)의 잔액을 저장한다. 이를 위하여 금액 저장부(101)는 데이터를 저장하는 메모리로 구현 가능하다. 이 때의 금액 저장부(101)는 금액을 저장하는 공간이 1개인 것으로 구현될 수 있다. 금액을 저장하는 공간이 1개인 경우, 악의적 목적을 가진 자가 서로 다른 금액을 각각의 공간에 저장시킴으로써 전자 화폐를 해킹하는 것을 차단시킬 수 있다.

[0047] 데이터 포트부(130)는 전자 화폐 단말(100a)이 관리 서버(10b)와 송수신하는 데이터가 입출력되는 구성이다. 예컨데, 데이터 포트부(130)는 잔액과 같은 데이터가 처리부(120)에 의하여 암호화되면, 암호화된 데이터가 전자 화폐 사용처(10a)를 통해서 관리 서버(10b)로 송신될 수 있도록, 암호화된 데이터를 전자 화폐 사용처(10a)로 출력한다. 또한, 관리 서버(10b)가 전자 화폐 사용처(10a)로 잔액과 같은 데이터를 송신하면, 데이터 포트부(130)는 전자 화폐 사용처(10a)로부터 이러한 데이터를 입력받는다. 전술한 데이터 포트부(130)는 데이터를 입출력하는 하드웨어적인 포트일 수 있다.

[0048] 키 저장부(110)는 기 설정된 복수 개의 키를 저장한다. 복수 개의 키 각각은 데이터를 암호화하는데 사용되며, 각각 복수 개의 비트로 구성될 수 있다.

[0049] 키 저장부(110)는 난수 생성부(150)에 의하여 생성된 임의의 개수, 예를 들면 1000개의 난수의 값을 기초로 복수 개의 키를 생성할 수 있다. 이 때, 임의의 개수의 난수의 값 그 자체가 복수 개의 키가 되거나, 이와 달리 상기 임의의 개수의 난수를 키 저장부(110)가 가공하여 생성된 값이 복수 개의 키가 될 수도 있다.

[0050] 이 때, 전자 화폐 단말(100a)에 포함된 리셋부(170)는 시드(seed) – 난수를 생성할 때 사용되는 값 – 를 생성하여 난수 생성부(150)에 제공한다. 아울러, 이러한 시드는 연결부(140)를 통하여 다른 전자 화폐 단말(100a) 또는 관리 서버용 암복호화 장치(100b)에 포함된 난수 생성부(150)에도 전달 및 제공된다. 시드를 전달 및 제공받은 난수 생성부(150)는 동일한 시드를 이용하여 난수를 생성한다. 따라서, 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 서로 간에 연결될 경우, 각각에서는 동일한 난수가 생성되며, 따라서 이들은 각각 동일한 값을 갖는 복수 개의 키를 가질 수 있다.

[0051] 여기서, 리셋부(170)에 대하여 보다 자세하게 살펴보면, 리셋부(170)는 사용자에 의한 입력을 받아들이는 버튼 등을 포함할 수 있다. 또한, 리셋부(170)는 난수 생성부(150)와 연결된다. 전자 화폐 단말(100a)이 관리 서버용 암복호화 장치(100b)와 서로 간에 연결되고 리셋부(170)가 버튼이나 터치 등을 통하여 사용자의 입력을 받아들이면, 리셋부(170)는 시드를 생성하여 난수 생성부(150)로 제공한다.

[0052] 이상에서 살펴본 바와 같이, 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)는 서로 간에 물리적으로 오프라인 상에서 연결되었을 때 복수 개의 키를 생성하여 공유한다. 즉, 복수 개의 키가, 유선이든 무선이든 통신망을 통해서 이들 간에 전달되는 일이 발생하지 않는다. 따라서, 기존의 RSA와는 달리 키를 분배하여 공유시키는 과정에서 키가 유출되거나 해킹될 위험이 전혀 없다.

[0053] 키 저장부(110)에 저장된 복수 개의 키는 갱신(업데이트)될 수 있다. 갱신 시점은 주기적으로 또는 필요한 때에 임의로 이루어질 수 있는데, 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)는 이러한 갱신 시점

에 대하여 서로 약속한 규칙을 가지고 있을 수 있으며, 따라서 동일한 시점에 복수 개의 키를 갱신할 수 있다.

[0054] 아울러, 키를 갱신하는 것은 새로운 복수 개의 키를 생성하는 것이므로, 이 경우에도 난수 생성부(150)에 의하여 생성된 난수를 기초로 복수 개의 키를 생성할 수 있다. 키를 갱신할 때 난수 생성부(150)에 전달되는 시드는 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 서로 간에 알고 있는 기 설정된 값, 예를 들면 갱신 전 1번째 또는 마지막 번째의 키일 수 있다. 즉, 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)는 갱신을 위하여 동일한 시드를 가지고 복수 개의 키를 생성하며, 이와 같이 생성된 복수 개의 키를 갱신에 사용한다. 따라서, 복수 개의 키가 갱신이 되더라도 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)는 동일한 값의 복수 개의 키를 공유할 수 있다.

[0055] 처리부(120)는 전자 화폐 단말(100a)이 관리 서버용 암복호화 장치(100b)로 송신할 데이터를 암호화한다. 보다 자세하게 살펴보면, 키 저장부(110)에 저장된 복수 개의 키 중 어느 하나인 제1 키가 선택된다. 제1 키를 선택하는 주체는 키 저장부(110) 또는 처리부(120)일 수 있다. 처리부(120)는 제1 키를 기초로 암호화 대상인 데이터를 암호화한다. 여기서, 제1 키를 기초로 데이터를 암호화하는 암호화 알고리즘은 기존에 공지된 것을 사용할 수 있으며, 알고리즘 저장부(180)에 저장될 수 있다. 알고리즘 저장부(180)는 ROM의 형태일 수 있다. 이때, 제1 키를 기초로 암호화된 데이터는 제1 키에 의해서만 복호화가 가능하다.

[0056] 처리부(120)는 관리 서버용 암복호화 장치(100b)에 의하여 암호화된 데이터가 전자 화폐 사용처(10a)를 통해서 수신되면 이를 복호화하는데, 복호화하는 알고리즘은 전술한 알고리즘 저장부(180)에 저장될 수 있다. 보다 자세하게 살펴보면, 처리부(120)는 암호화된 데이터를 키 저장부(110)에 저장된 복수 개의 키 중 어느 하나인 키를 이용하여 복호화한다. 여기서, 키를 이용하여 암호화된 데이터를 복호화하는 알고리즘은 기존에 공지된 것을 사용할 수 있다.

[0057] 처리부(120)가 복호화한 데이터는 잔액일 수 있다. 이 경우, 처리부(120)는 복호화한 데이터에 포함된 잔액으로 금액 저장부(101)에 저장되어 있던 기존의 잔액을 갱신할 수 있다.

[0058] 여기서, 처리부(120)가 암호화된 데이터를 복호화하기 위해서는, 암호화된 데이터가 복수의 키 중 어떠한 키를 기초로 암호화되었는지 여부를 알아야 한다. 이하에서는 이에 대하여 자세히 설명하기로 하되, 데이터를 암호화하는 처리부를 제1 처리부로 그리고 이러한 제1 처리부를 포함하는 암복호화 장치를 제1 암복호화 장치로, 데이터를 복호화하는 처리부를 제2 처리부로 그리고 이러한 제2 처리부를 포함하는 암복호화 장치를 제2 암복호화 장치로 지칭하기로 한다. 제1 암복호화 장치, 그리고 제2 암복호화 장치는 각각 전자 화폐 단말(100a) 또는 관리 서버용 암복호화 장치(100b)일 수 있다.

[0059] 제1 처리부는 암호화 대상인 데이터에 식별자(또는 control block이라고 지칭될 수도 있음)를 결합시킨 결합 데이터를 생성한다. 식별자는 제1 암복호화 장치와 제2 암복호화 장치가 서로 간에 모두 알고 있는 값이다. 제1 처리부는 키 저장부(110)로부터 제1 키를 전달받으며, 제1 키를 기초로 결합 데이터를 암호화한다. 암호화된 결합 데이터는 제1 암복호화 장치가 제2 암복호화 장치로 송신한다.

[0060] 제2 암복호화 장치는 암호화된 결합 데이터를 수신한다. 제2 처리부는 암호화된 결합 데이터를 다음과 같은 과정을 통하여 복호화하되, 이는 예시적인 것이므로 본 발명의 사상이 이에 한정되는 것은 아니다. 먼저, 키 저장부(110)로부터 복수 개의 키를 하나씩 전달받는다. 전달받은 키를 기초로 암호화된 결합 데이터에 대하여 복호화를 시도한다. 복호화한 결과로부터 식별자를 분리한다. 분리된 식별자가 제2 암복호화 장치가 알고 있는 값인지 여부를 판별한다. 만약 분리된 식별자가 제2 암복호화 장치가 알고 있는 값인 경우에는 전달받은 키가 암호화에 사용된 키인 것으로 간주하며, 복호화된 결합 데이터 중에서 식별자가 분리된 나머지 데이터를 복호화된 데이터로 취급한다. 그러나, 알고 있는 값이 아닌 경우에는 알고 있는 값이 나올 때까지 키 저장부(110)로부터 새로운 키를 전달받아서 복호화 과정을 반복한다.

[0061] 이를 통해 살펴보면, 해커가 암호화된 결합 데이터를 복호화하기 위해서는, 복수 개의 키를 모두 알아야 하며, 추가적으로 식별자가 무엇인지도 알아야 한다. 그러나, 복수 개의 키는 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 물리적으로 오프라인 상에서 서로 연결되었을 때 공유되기 때문에 유출될 우려가 없으며, 식별자 또한 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)의 초기 제작 과정에서 ROM과 같은 곳에 심어지기 때문에 해커가 이를 알아낼 수 없다. 따라서, 일 실시예에 따른 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)를 사용하면 해킹의 위험을 원천적으로 차단시킬 수 있다.

[0062] 한편, 이하에서는 식별자에 대하여 보다 자세하게 살펴보기로 한다. 전술한 바와 같이 식별자는 전자 화폐 단

말(100a) 및 관리 서버용 암복호화 장치(100b)가 서로 간에 모두 알고 있는 값이다. 도 6a는 식별자(122)가 데이터(121)와 결합된, 결합 데이터를 개념적으로 도시한 도면이다. 도 6a를 참조하면, 식별자(122)는 기 설정된 개수, 예를 들면 n개의 비트로 구성될 수 있다.

[0063] 이러한 n개의 비트는 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 서로 알고 있는 약속된 규칙에 의하여 그 값이 채워질 수 있다. 도 6b는 식별자를 구성하는 n개의 비트가 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 서로 알고 있는 약속된 규칙에 의하여 그 값이 채워지는 것을 개념적으로 도시한 도면이다. 이하에서는 이러한 약속된 규칙에 대하여 보다 자세하게 살펴보기로 한다.

[0064] 먼저, 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 서로 알고 있는 기 설정된 적어도 두 개 이상의 키를 이용하여, n개의 비트의 특정 위치에 특정 값을 할당한다. 예를 들면, 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 50개의 키, 즉 제1 키부터 제50 키까지 서로 알고 있다고 가정하자. 그리고 제1 키를 n으로 모듈러 연산을 한 값을 제1 값이라고 하고 제2 키를 2로 모듈러 연산을 한 값을 제2 값이라고 하면, n개의 비트 중 제1 값이 나타내는 번째의 비트에 제2 값을 할당한다. 다음으로, 제3 키를 n으로 모듈러 연산을 한 값을 제3 값이라고 하고 제4 키를 2로 모듈러 연산을 한 값을 제4 값이라고 하면, n개의 비트 중 제3 값이 나타내는 번째의 비트에 제4 값을 할당한다. 이와 같은 방식으로 50개의 키를 이용하여 n개의 비트의 특정 위치에 특정 값을 할당한다. 이 때, 이미 값이 할당된 위치에 또 값을 할당해야 한다면, 뒤에 할당된 값을 해당 위치에 할당한다. 이 후, n개의 비트 중 값이 할당되지 않은 비트가 있을 수 있다. 값이 할당되지 않은 비트에는 난수 생성부(150)에서 생성한 비트를 할당한다. 도 6b는 전술한 과정에 의하여 식별자를 생성한 것을 개념적으로 도시한 도면이다. 도 6b를 참조하면, n개의 비트 중 적어도 두 개 이상의 키를 이용하여 값이 할당되는 비트는 b로 표시되고, 난수 생성부(150)가 생성한 난수가 할당되는 비트는 a로 표시된다.

[0065] 이와 같이 제1 처리부에 의하여 생성된 식별자는, 제2 처리부에 의해서도 동일한 알고리즘으로 도출할 수 있다. 즉, 제2 암복호화 장치는 제1 암복호화 장치와 동일한 알고리즘으로 식별자를 생성한다. 이 후, 제1 암복호화 장치로부터 암호화된 결합 데이터를 수신하면, 제2 처리부는 암호화된 결합 데이터를 복수 개의 키를 이용하여 복호화를 시도한다. 복호화를 시도한 결과 제2 처리부는 결합 데이터로부터 식별자를 분리한다. 이 후, 분리된 식별자 중에서 값이 할당되는 비트 위치인 b에 대해서만 자신이 생성한 식별자와 비교를 한다. 비교 결과 값이 할당되는 비트 위치인 b에 대해서 같은 값이 나오면, 해당 키가 암호화에 사용된 키인 것으로 간주한다.

[0066] 이와 같이 생성된 식별자를 이용할 경우, 해커는 복수 개의 키 전부, 그리고 식별자 생성에 사용되는 적어도 두 개 이상의 키 및 식별자를 생성할 때 사용되는 알고리즘을 모두 알아야만이 데이터를 해킹할 수 있다. 그러나, 전술한 바와 같이 키는 전자 화폐 단말(100a) 및 관리 서버용 암복호화 장치(100b)가 하드웨어적으로 오프라인 상에서 연결될 때 공유되기 때문에 유출될 우려가 없으며, 식별자 또한 암복호화 장치(100)의 초기 제작 과정에서 ROM과 같은 곳에 심어지기 때문에 해커가 이를 알아낼 수 없다. 따라서, 일 실시예에 따르면 해킹의 위험을 원천적으로 차단할 수 있다.

[0067] 한편, 도 5를 참조하면, 데이터 포트부(130)는 데이터 버스(125)를 통해서 처리부(125)와 연결된다. 데이터 버스(125)란 데이터가 송수신되는 경로를 의미한다. 키 저장부(110)는 처리부(120)와 키 버스(115)를 통해서 연결된다. 키 버스(115)란 키 저장부(110)에 저장된 키가 처리부(120)로 전달되는 경로를 의미한다.

[0068] 이 때, 키 저장부(110)는 키 버스(115)를 통해서 처리부(120)와는 연결되지만, 데이터 포트부(130)와는 직접적으로 연결되지 않는다. 따라서, 외부에서는 데이터 포트부(130)를 통해서 키 저장부(110)에 직접 접근할 수 없으며, 그 결과 외부에서는 키 저장부(110)에 저장된 복수 개의 키에 접근할 수 없다.

[0069] 다시 도 2를 참조하면, 위조 방지부(103)는 전자 화폐 단말(100a)의 잔액이 위조되는 것을 방지하기 위한 구성이다. 이를 위하여, 예컨데 위조 방지부(103)는 처리부(120)에 의하여 금액 저장부(101)에 저장된 잔액이 갱신될 때마다 그 값을 정해진 규칙에 따라 증가시키는 변수를 갖는다. 변수는 잔액이 갱신될 때마다 그 값이 예컨데 1씩 증가할 수 있다. 도 3a는 금액 저장부(101)에 저장된 잔액이 ₩50,000이면서 위조 방지부(103)를 구성하는 변수의 값이 k인 것을 예시적으로 도시한 도면이다.

[0070] 위조 방지부(103)에 의하여 전자 화폐 단말(100a)의 잔액이 위조되지 않도록 하는 것은 도 3b를 참조하여 보다 자세하게 살펴보기로 한다. 도 3b를 참조하면, 전자 화폐 단말(100a)의 현재 잔액은 제1 잔액(S10)이다. 전자 화폐 단말(100a)이 전자 화폐 사용처(10a)에서 일정 금액만큼 사용되는 경우, 현재 잔액인 제1 잔액(S10)은 관리 서버(10b)로 송신(S11)되며, 이와 함께 도 3b에는 도시되지 않았지만 전자 화폐 사용처(10a)에서 일정 금액이 사용되었다는 정보 또한 관리 서버(10b)로 송신된다.

[0071] 관리 서버(10b)는 제1 잔액(S10) 및 전자 화폐 사용처(10a)에서 사용된 일정 금액을 기초로 전자 화폐 단말(100a)의 제2 잔액을 산출한다(S12). 그리고 관리 서버(10b)는 이러한 제2 잔액에 변수 k를 부가한 뒤 암호화한다. 제2 잔액과 변수 k는 암호화되어 전자 화폐 단말(100a)로 송신된다(S13).

[0072] 전자 화폐 단말(100a)은 암호화된 데이터를 복호화한다. 이 후, 복호화된 데이터에 포함된 잔액을 기초로 금액 저장부(101)에 저장된 현재의 잔액을 제1 잔액에서 제2 잔액으로 갱신한다(S14). 또한, 복호화된 데이터에 포함된 변수 k를 기초로, 이러한 변수 k에 1을 더한 k+1을 위조 방지부(103)에 저장한다(S14).

[0073] 전자 화폐 단말(100a)은 제2 잔액 및 변수 k+1을 암호화하여 관리 서버(10b)로 송신한다(S15).

[0074] 관리 서버(10b)는 관리 서버용 암복호화 장치(100b)를 통해 암호화된 데이터를 복호화한다. 이 후, 복호화된 데이터에서 전자 화폐 단말(100a)의 잔액이 제2 잔액이 맞는지를 확인하며, 변수 k가 값이 +1만큼 증가한 k+1인지를 확인한다.

[0075] 이를 통해 살펴보면, 잔액이 갱신될 때마다 위조 방지부(103)의 변수 k의 값이 정해진 규칙에 따라 증가되어야 한다. 아울러, 금액 저장부(101)는 금액을 저장하는 1개의 공간만을 갖는다. 따라서, 갱신되어야 하는 잔액을 관리 서버(10b)가 전자 화폐 단말(100a)로 송신하였을 때, 전자 화폐 단말(100a)이 잔액을 갱신하지 않은 채로 관리 서버(10b)가 송신한 잔액을 그대로 관리 서버(10b)로 송신(반사)만함으로써 악의적으로 잔액을 조작하는 행위가 차단될 수 있다.

[0076] 보호부(160)는 전자 화폐 단말(100a)에 비정상적인 것으로 정의된 행위가 가해지는 것을 인식하며, 이러한 행위가 가해지는 것이 인식되면 키 저장부(110)에 저장된 복수 개의 키를 삭제한다. 비정상적인 것으로 정의된 행위에는, 예를 들면 키 저장부(110)에 저장된 복수 개의 키를 전자기적으로 복제하기 위한 시도, 진동이나 열 등을 감지하는 시도 등일 수 있으나 이에 한정되는 것은 아니다.

[0077] 접속부(190)는 전자 화폐 단말(100a)와 전자 화폐 사용처(10a)를 연결시킨다. 이러한 접속부(190)는 하드웨어적인 커넥터이거나 이와 달리 무선 통신(블루투스, NFC, 와이파이 등) 모듈일 수도 있으나 이에 한정되는 것은 아니다.

[0078] 도 7은 본 발명의 일 실시예에 따른 전자 화폐를 제공하는 방법의 절차를 도시한 도면으로, 전자 화폐를 제공하는 방법은 전술한 전자 화폐 단말(100a)에 의하여 수행될 수 있다. 아울러, 이하에서 설명할 전자 화폐를 제공하는 방법은 실시예에 따라서 이하에서 설명할 적어도 하나 이상의 단계가 수행되지 않거나 언급되지 않은 새로운 단계가 추가로 수행될 수도 있으며, 그 순서가 변경될 수도 있다.

[0079] 도 7을 참조하면, 전자 화폐를 제공하는 방법은 전자 화폐 단말(100a)을 관리하는 관리 서버(100b)로부터, 전자 화폐 단말(100a)에 저장된 잔액을 갱신하는 잔액 관련 데이터를 암호화된 상태로 수신하는 단계(S100)와, 기 저장된 복수 개의 키 중 어느 하나인 제1 키를 기초로 암호화된 잔액 관련 데이터를 복호화하는 단계(S110)와, 복호화된 잔액 관련 데이터를 기초로 잔액을 갱신시키는 단계(S120)를 포함한다. 여기서, 복수 개의 키는 관리 서버(100b)가 송신할 데이터를 암호화하거나 관리 서버(100b)가 수신한 암호화된 데이터를 복호화하는 관리 서버용 암복호화 장치(10b)가 관리 서버(100b)와 연결될 때, 전자 화폐 단말(100a)에 포함된 연결부(140)가 관리 서버용 암복호화 장치(10b)에 포함된 연결부와 물리적으로 연결되면 생성되어 저장되는 것을 특징으로 한다.

[0080] 한편, 전자 화폐를 제공하는 방법의 구체적인 내용은 전자 화폐 단말(100a)을 설명하면서 이미 상세하게 설명하였는바, 이에 대해서는 설명을 생략하기로 한다.

[0081] 이상에서 살펴본 바와 같이, 본 발명의 실시예에 따르면 데이터의 암복호화에 사용되는 키를 분배하여 공유시키는 과정에서, 이러한 키가 해킹될 가능성이 원천적으로 차단된다. 따라서, 이를 이용하여 전자 화폐에 대한 해킹 가능성을 원천적으로 차단시킬 수 있다.

[0082] 본 발명에 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는

제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0083] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들 또는 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0084] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0085] 10a: 전자 화폐 사용처

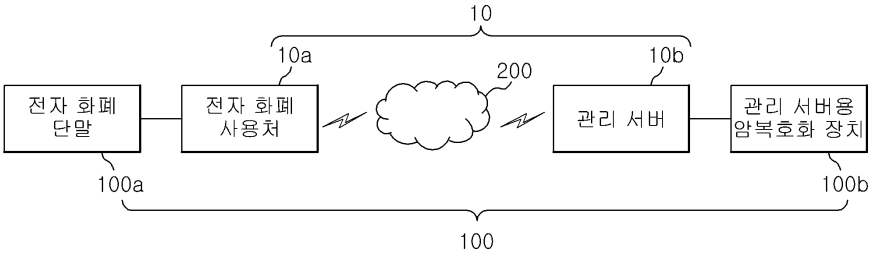
100a: 전자 화폐 단말

10b: 관리 서버

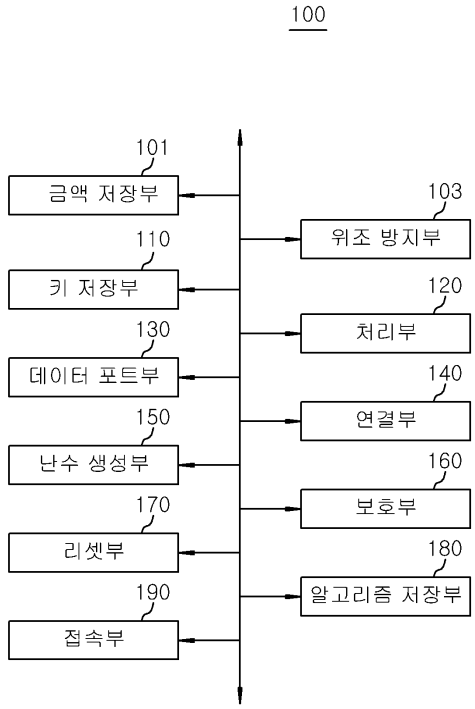
100b: 관리 서버용 암복호화 장치

도면

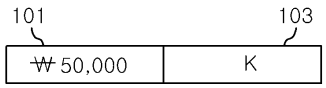
도면1



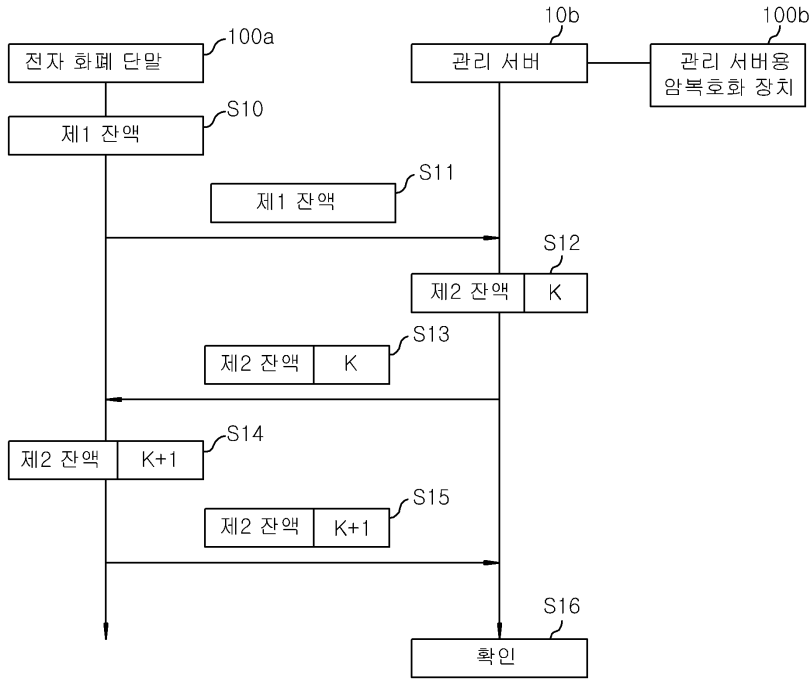
도면2



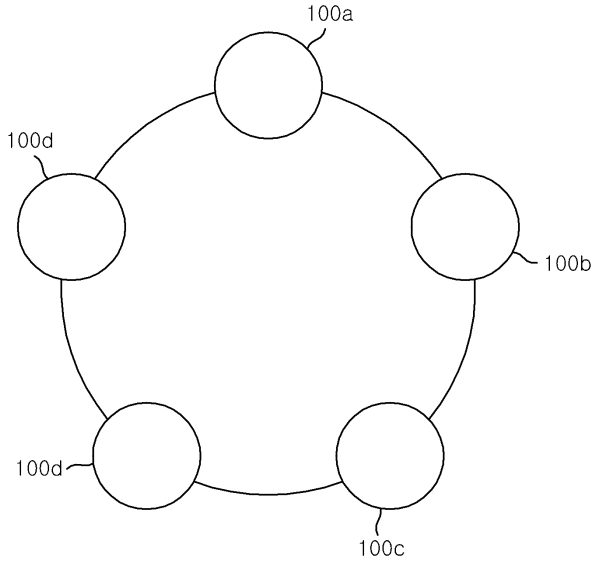
도면3a



도면3b

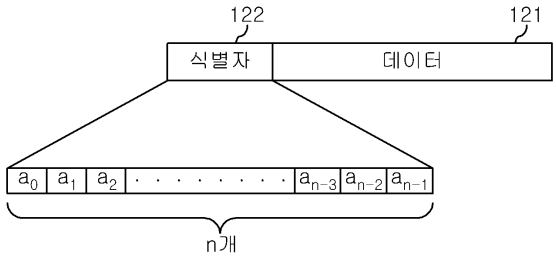


도면4

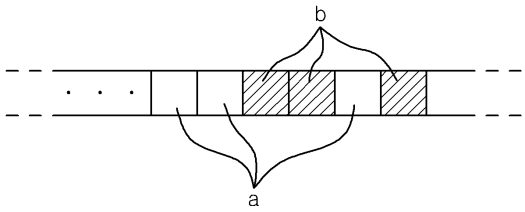


도면5

도면6a



도면6b



도면7