(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0035443
(43) 공개일자 2020년04월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G09C 1/00* (2006.01)
(52) CPC특허분류
H04L 9/085 (2013.01)
G09C 1/00 (2013.01)
(21) 출원번호 10-2020-7006354
(22) 출원일자(국제) 2018년03월29일
심사청구일자 2020년03월03일
(85) 번역문제출일자 2020년03월03일
(86) 국제출원번호 PCT/JP2018/013207
(87) 국제공개번호 WO 2019/049408
국제공개일자 2019년03월14일
(30) 우선권주장
JP-P-2017-173060 2017년09월08일 일본(JP)

(71) 출원인
헬스미디어 가부시끼가이샤
일본국 141-0022 도쿄도 시나가와쿠 히가시고탄다 1쵸메 10방 7고
(72) 발명자
노다 케이이치
일본 141-0022 도쿄도 시나가와쿠 히가시고탄다 1쵸메 10방 7고 헬스미디어 가부시끼가이샤 내
요네모토 쿠미코
일본 272-0026 지바켄 이치카와시 히가시오와다 1쵸메 14방 14고
(74) 대리인
특허법인(유한)케이비케이

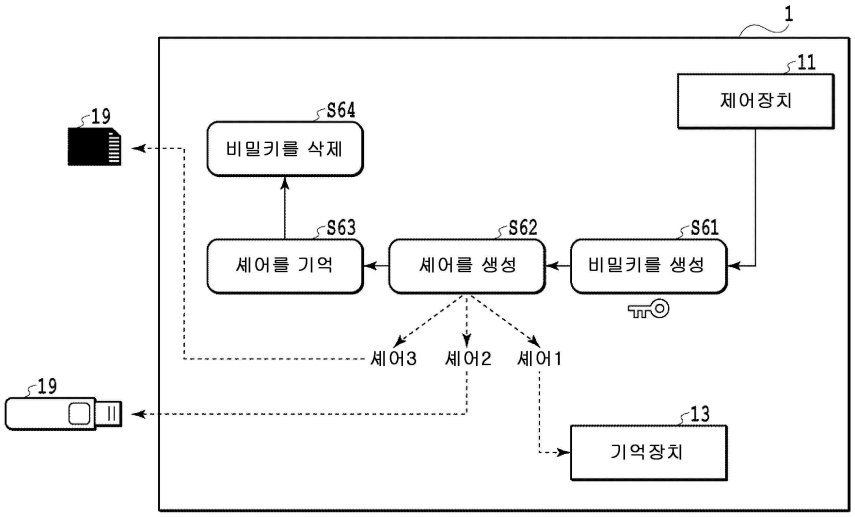
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **비밀정보 복원가능값 분산시스템 및 방법**

(57) 요 약

본 발명은, 비밀정보 복원가능값 분산시스템을 제공하는 것이다. 컴퓨터에 의하여 실행되는 방법으로서, 소정 정보의 처리에 사용하는 비밀정보에 근거하여, n개의 비밀정보 복원가능값을 생성하는 스텝이며, 비밀정보는, 생성한 n개의 셰어 중 적어도 k개의 비밀정보 복원가능값을 사용하여 복원가능하고, n>=k>=2인 스텝과, 생성한 n개의 비밀정보 복원가능값을, 대응하는 n개의 물리적 기억장치에 기억하는 스텝과, 생성한 비밀정보를 삭제하는 스텝을 구비한다.

대 표 도 - 도6



(52) CPC특허분류
H04L 9/0877 (2013.01)
H04L 9/0894 (2013.01)

명 세 서

청구범위

청구항 1

컴퓨터에 의하여 실행되는 방법으로서,

교환되는 정보의 처리에 사용하는 비밀정보에 근거하여, n개의 비밀정보 복원가능값을 생성하는 스텝이며, 상기 비밀정보는, 상기 생성한 n개의 셰어 중 적어도 k개의 비밀정보 복원가능값을 사용하여 복원가능하고, n>=k>=2인 스텝과,

상기 생성한 n개의 비밀정보 복원가능값을, 대응하는 n개의 물리적 기억장치에 기억하는 스텝과,

상기 생성한 비밀정보를 삭제하는 스텝을 구비한 것을 특징으로 하는 방법.

청구항 2

제 1 항에 있어서,

상기 n개의 물리적 기억장치 중 k개의 물리적 기억장치로부터, 대응하는 k개의 비밀정보 복원가능값을 판독하는 스텝과,

상기 판독한 k개의 비밀정보 복원가능값을 사용하여, 상기 비밀정보를 복원하는 스텝과,

상기 k개의 비밀정보 복원가능값을 삭제하는 스텝을 더 구비한 것을 특징으로 하는 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 n개의 물리적 기억장치 중 적어도 n-(k-1)개는, 탈착가능 기억장치이고,

상기 방법은, 상기 탈착가능 기억장치가 상기 컴퓨터에 접속되어 있는지 아닌지를 판정하는 스텝을 더 구비한 것을 특징으로 하는 방법.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 n개의 물리적 기억장치 중 적어도 1개는, 제1 탈착가능 기억장치이고,

상기 n개의 물리적 기억장치 중 적어도 또 다른 1개는, 제2 탈착가능 기억장치이며, 상기 제1 탈착가능 기억장치 및 상기 제2 탈착가능 기억장치는, 동일 종별의 탈착가능 기억장치이고,

상기 생성한 n개의 비밀정보 복원가능값을, 상기 대응하는 n개의 물리적 기억장치에 기억하는 스텝은,

상기 생성한 n개의 비밀정보 복원가능값 중 제1 비밀정보 복원가능값을 상기 제1 탈착가능 기억장치에 기억하는 스텝과,

상기 제2 탈착가능 기억장치가 상기 컴퓨터에 접속되어 있는지 아닌지를 판정하는 스텝과,

상기 제2 탈착가능 기억장치가 상기 제1 탈착가능 기억장치와 물리적으로 다른 탈착가능 기억장치인지를 판정하는 스텝과,

상기 제2 탈착가능 기억장치가 상기 제1 탈착가능 기억장치와 물리적으로 다른 탈착가능 기억장치라고 판정한 것에 응답하여, 상기 생성한 n개의 비밀정보 복원가능값 중 제2 비밀정보 복원가능값을 상기 제2 탈착가능 기억장치에 기억하는 스텝을 포함하는 것을 특징으로 하는 방법.

청구항 5

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

상기 비밀정보를 생성하고, 또는 상기 비밀정보를 수신하는 스텝을 더 구비한 것을 특징으로 하는 방법.

청구항 6

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

복수의 어플리케이션 프로그램을 실행함으로써, 상기 비밀정보를 생성하는 스텝을 더 구비하고,

상기 n개의 물리적 기억장치 중 적어도 1개는, 상기 컴퓨터에 내장된 기억장치이며, 상기 기억장치는, 상기 복수의 어플리케이션 프로그램의 각각에 대하여 독립된 복수의 논리적 기억영역을 포함하고,

상기 생성한 n개의 비밀정보 복원가능값을, 상기 대응하는 n개의 물리적 기억장치에 기억하는 스텝은, 상기 생성한 n개의 비밀정보 복원가능값 중 1개를, 상기 복수의 논리적 기억영역 중 어느 1개에 기억하는 스텝을 포함하는 것을 특징으로 하는 방법.

청구항 7

제 1 항 내지 제 6 항 중 어느 한 항에 있어서,

상기 n개의 비밀정보 복원가능값을 생성하는 스텝은, (k, n) 임계치법을 사용하여 실행되는 것을 특징으로 하는 방법.

청구항 8

제 1 항 내지 제 7 항 중 어느 한 항에 있어서,

상기 비밀정보는, 비밀키인 것을 특징으로 하는 방법.

청구항 9

제 1 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 처리는, 서명인 것을 특징으로 하는 방법.

청구항 10

제 1 항 내지 제 9 항 중 어느 한 항에 있어서,

상기 교환되는 정보는, 가상통화의 트랜잭션 이력정보인 것을 특징으로 하는 방법.

청구항 11

컴퓨터 디바이스로서,

제어장치와,

상기 제어장치에 결합되어, 컴퓨터 실행가능명령을 기억한 메모리를 구비하고,

상기 컴퓨터 실행가능명령은, 상기 제어장치에 의하여 실행되면, 상기 컴퓨터 디바이스에, 제 1 항 내지 제 10 항 중 어느 한 항에 기재된 방법을 실행시키는 것을 특징으로 하는 컴퓨터 디바이스.

청구항 12

컴퓨터 실행가능명령을 포함하는 컴퓨터 프로그램으로서, 상기 컴퓨터 실행가능명령은, 컴퓨터에 의하여 실행되면, 상기 컴퓨터에 제 1 항 내지 제 10 항 중 어느 한 항에 기재된 방법을 실행시키는 것을 특징으로 하는 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은, 비밀정보 복원가능값 분산시스템 및 방법에 관한 것이다. 특히, 본 발명은, 비밀정보를 복원하기 위한 비밀정보 복원가능값(셰어)을 물리적인 기억매체에 분산하여 기억함으로써, 시큐리티를 확보하는 비밀정보

복원가능값 분산시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷 등의 공중네트워크를 통하여 온라인 상에서 거래를 행하는 컴퓨터 시스템이 이용되고 있다. 상기 컴퓨터 시스템의 예는, 피어 투 피어(P2P)형 결제망인 비트코인(Bitcoin)으로 불리는 가상통화 관리시스템 등을 포함한다. 비트코인에 있어서는, 쌍을 이루는 2개의 키를 이용하여 데이터의 암호화 및 복호를 행하는 공개키 암호방식이 이용된다.

[0003] 이하에서는, 비트코인에서의 가상통화의 송금처리의 흐름을 간단하게 설명한다. (1) 우선, 가상통화를 지불하는 측(송금원)이 공개키 및 비밀키의 페어를 생성한다. (2) 송금원이 공개키로부터 어드레스(계좌번호)를 생성한다(이러한 어드레스의 집합이 '월렛(지갑)이 됨'). (3) 송금원이 송금정보(송신하는 비트코인, 어드레스 등의 트랜잭션 이력정보)에 자신의 비밀키를 사용하여 서명한다. (4) 송금원이 P2P 네트워크에 송금정보를 브로드캐스트한다. (5) 가상통화를 수취하는 측(송금처)이 거래 내에 포함되는 공개키 및 서명이 완료된 송금정보를 대조하여 거래가 정상인 것을 검증한다.

[0004] 비트코인에서는, 송금원만이 알 수 있는 비밀키를 사용하여 송금정보가 서명되므로, 그 비밀키는 고도의 레벨로 비밀스럽게 관리될 필요가 있다. 이러한 것으로부터, 비트코인의 구조에서는, 비밀키를 어떻게 관리해야 하는가라는 과제가 존재한다. 비밀키는, 시큐리티면을 고려하여 일반적으로는 임의의 영숫자에 의한 64자리의 비밀키가 사용되고 있다. 따라서, 그 비밀키를 잊어버리면, 그 어드레스에 대응하는 비트코인은 두번 다시 사용할 수 없게 된다. 이와 같은 배경으로부터, 다양한 디바이스나 서비스를 사용하여 비밀키를 관리하는 이용자가 존재한다. 예를 들어, 비트코인의 사용용도에 맞추어 복수의 계좌를 소유하고, 편의성이나 시큐리티성 등을 고려하여 각각 다른 방법으로 관리하고 있는 이용자가 존재한다.

선행기술문헌

비특허문헌

[0005] (비특허문헌 0001) 비특허문헌 1: 도이 히로시, '비밀분산법과 그 응용에 대하여', 정보시큐리티종합과학, 제4권, [online], 2012년 11월, 정보시큐리티대학원대학, [평성29년 8월 30일 검색], 인터넷 <URL: https://www.iisec.ac.jp/proc/vol0004/doi.pdf>

(비특허문헌 0002) 비특허문헌 2: G.R.Blakley, Safeguarding cryptographic keys, Proc. of the National Computer Conference, Vol.48, pp.313-317, 1979, <URL: https://www.computer.org/csdl/prodeedings/afips/1979/5087/00/50870313.pdf>

발명의 내용

해결하려는 과제

[0006] 비트코인을 이용하기 위하여, 이용자는, P2P 네트워크에 접속된 컴퓨터 단말(스마트폰, 태블릿 컴퓨터 및 퍼스널 컴퓨터 등)을 사용할 필요가 있다. 그러한 단말이 네트워크에 접속되는 이상, 악의가 있는 제삼자가 컴퓨터 단말에 부정 액세스할 우려가 있다. 따라서, 비밀키가 제삼자에게 누설될 위험성을 완전히 배제할 수 없다.

[0007] 비특허문헌 1은, Shamir의 임계치법을 개시하고 있다. Shamir의 임계치법에서는, 비밀정보에 근거하여 n개의 일의적 셰어가 생성되고, 그러한 일의적 셰어가 n명의 공유자에게 주어진다. 그리고, n개 중 k개(k<n)의 셰어를 사용함으로써, 원래의 비밀정보를 복원할 수 있다. 즉, n-k의 수만큼 일의적 셰어가 손실되어도, 나머지 k개의 일의적 셰어를 사용하여 비밀정보를 복원할 수 있다. 이것은, k-1의 셰어를 사용하여도 정보를 복원할 수 없는 것을 의미한다. 이러한 기술을 사용함으로써, 비밀정보를 복원하기 위한 셰어를 분산시킬 수 있다.

[0008] 하지만, 셰어를 분산시켜도, 예를 들어 그러한 셰어를 네트워크에 접속된 기억장치에 기억한 경우, 제삼자가 그 기억장치에 부정 액세스함으로써 k개의 셰어가 누설될 위험성이 있다. 이러한 것으로부터, 비특허문헌 1에 개시된 기술을 사용하여도, 비밀정보를 적절히 보호할 수 없는 경우가 있다. 특히, k개의 셰어를 동일한 LAN에 위치하는 기억장치에 기억한 경우, 제삼자가 그 LAN의 입구가 되는 Gateway(Firewall)를 통과함으로써, k개의 모든 셰어가 쉽게 그 제삼자에게 누설될 가능성이 있다.

[0009] 비밀정보를 적절히 보호하기 위한 궁극적인 방법으로서, 예를 들어 특허문헌 1에 개시된 기술을 사용하여, 적어도 k개의 셰어값을 종이 등에 적어 두고, 그 종이를 금고 등에 보관하는 방법을 생각할 수 있다. 종이 매체를 사용하여 셰어를 보존하게 되므로, 셰어 정보가 네트워크를 통하여 액세스되는 경우가 없어져, k개의 셰어가 제삼자에게 누설될 가능성을 저감시킬 수 있다. 하지만, 이러한 방법은, 이용자의 정보 관리 부하를 증대시키게 된다.

[0010] 본 발명에 따르면, 이용자의 정보 관리 부하를 경감시키는 것이 가능한, 및/또는 비밀정보를 적절히 보호하는 것이 가능한, 컴퓨터에 의하여 실행되는 방법이 제공된다. 또한, 본 발명에 따르면, 이용자의 정보 관리 부하를 경감시키는 것이 가능한, 및/또는 비밀정보를 적절히 보호하는 것이 가능한, 컴퓨터 디바이스가 제공된다.

과제의 해결 수단

[0011] 본 발명의 일 실시형태에 따른 컴퓨터에 의하여 실행되는 방법은, 소정의 정보 처리에 사용하는 비밀정보에 근거하여, n개의 비밀정보 복원가능값을 생성하는 스텝이며, 상기 비밀정보는, 상기 생성한 n개의 셰어 중 적어도 k개의 비밀정보 복원가능값을 사용하여 복원 가능하고, n>=k>=2인 스텝과, 상기 생성한 n개의 비밀정보 복원가능값을 대응하는 n개의 물리적 기억장치에 기억하는 스텝과, 상기 생성한 비밀정보를 삭제하는 스텝을 구비한다.

[0012] 또한, 본 발명의 다른 실시형태에 따른 컴퓨터 디바이스는, 제어장치와, 상기 제어장치에 결합되고, 컴퓨터 실행가능명령을 기억한 메모리를 구비하며, 상기 컴퓨터 실행가능명령은, 상기 제어장치에 의하여 실행되면, 상기 컴퓨터 디바이스에, 소정의 정보 처리에 사용하는 비밀정보에 근거하여, n개의 비밀정보 복원가능값을 생성하는 스텝으로서, 상기 비밀정보는, 상기 생성한 n개의 셰어 중 적어도 k개의 비밀정보 복원가능값을 사용하여 복원가능하고, n>=k>=2인 스텝과, 상기 생성한 n개의 비밀정보 복원가능값을, 대응하는 n개의 물리적 기억장치에 기억하는 스텝과, 상기 생성한 비밀정보를 삭제하는 스텝을 포함하는 방법을 실행시키도록 구성되어 있다.

발명의 효과

[0013] 본 발명의 일 실시형태에 따른 컴퓨터에 의하여 실행되는 방법 또는 컴퓨터 디바이스에 의하면, 이용자는 막대한 부하가 걸리는 정보처리의 필요성 없이, 적절하게 비밀정보를 보호할 수 있다. 특히, 복수의 물리적 기억장치에 분산하여 셰어를 기억하므로, 만일 분산하여 기억한 셰어 중 1개가 누설되어도, k개의 셰어 모두가 누설되지 않는 한 비밀정보를 보호할 수 있다.

도면의 간단한 설명

[0014] 도 1은, 종래기술에 따른 (k, n) 임계치법에 따라서 산출한 비밀키 값에 대응하는 좌표를 통과하는 그래프를 나타낸다.

도 2는, 종래기술에 따른 (k, n) 임계치법에 따라서 산출한 비밀키 값에 대응하는 좌표를 통과하는 그래프를 나타낸다.

도 3은, 종래기술에 따른 (k, n) 임계치법에 따라서 산출한 비밀키 값에 대응하는 좌표를 통과하는 그래프를 나타낸다.

도 4는, 본 발명의 실시형태에 따른 비밀정보 복원가능값 분산시스템을 구성하는 컴퓨터 시스템 전체 구성의 예를 나타내는 도면이다.

도 5는, 본 발명의 실시형태에 따른 비밀정보 복원가능값 분산시스템을 구성하는 컴퓨터 단말의 상세한 구성의 예를 나타내는 도면이다.

도 6은, 본 발명의 실시형태에 따른 비밀정보 복원가능값 분산시스템을 실행하는 셰어생성처리의 예를 나타내는 도면이다.

도 7은, 본 발명의 실시형태에 따른 비밀정보 복원가능값 분산시스템을 실행하는 비밀정보 복원처리의 예를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하, 첨부도면을 참조하여, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템을 상세하게 설명한

다. 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 종래기술에 따른 Shamir의 임계치법(비밀분산법)을 이용함으로써, 비밀정보 복원가능값(셰어)을 분산하고 있다. 여기에서, Shamir의 임계치법은, 비밀정보를 복원할 수 있는 셰어의 수인 k(임계치), 및 그 셰어를 분산하는 수인 n(셰어수)을 정하고 있다. 상기와 더불어, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 정보를 복원할 수 있는/할 수 없는 집합을 임의로 정할 수 있는 어떤 다른 비밀분산법을 이용하여도 좋다(비특허문헌 2를 참조).

[0016] 우선, 종래기술에 따른 Shamir의 임계치법의 개요를, 도 1 내지 도 3을 참조하여 설명한다. Shamir의 임계치법(이하, '(k, n) 임계치법'이라고 함)에서는, 비밀정보인 S에 대하여, 그 비밀정보 S를 n명이 공유하는 것을 전제로 한다. 그 n명 각각에게는, 소정의 다항식을 사용하여 생성된 n개의 셰어가 각각 주어진다. 그 중 k개의 셰어에 의하여 비밀정보 S를 복원할 수 있다. 즉, 생성된 n개의 셰어를 n명 사이에서 공유하고, 그 중 k명이 가지는 k개의 셰어를 사용함으로써 비밀정보 S를 복원할 수 있다. 본 명세서에서는, 이러한 n의 수를 셰어수라고 하고, k의 수를 임계치라고 한다.

[0017] 셰어를 생성할 때에는, 정수항을 S로 하는 임의의 k-1차 다항식을 사용한다. 여기에서, k를 3으로 하고, n을 4로 하며(즉, 4개의 셰어를 생성하고, 그 중 3개의 셰어를 사용함으로써, 비밀정보 S를 복원할 수 있음), 비밀정보를 9로 한다. 따라서, k-1차 다항식, 즉 정수항을 9로 하는 임의의 2차 다항식을 사용하게 된다. 예를 들어, 제1 항의 계수에 2, 제2 항에 계수 7을 사용하여, 식 (1)

[0018] $f(x)=2x^2-7x+9$ 식 (1)

[0019] 로 한다.

[0020] n=4개의 셰어를 생성할 때, 셰어번호로서 {1, 2, 3, 4}를 할당한다. f(1), f(2), f(3) 및 f(4)로 하여서 식 (1)에 적용하면, n개의 셰어값의 집합, n={(1, 4), (2, 3), (3, 6), (4, 13)}이 산출된다.

[0021] 도 1은, 상술한 바와 같이 산출된 셰어값을 좌표로 하고, 각 좌표를 통과하는 곡선을 그린 그래프를 나타내고 있다. 도 1에 나타내는 곡선은, 4개의 셰어값에 대응하는 4곳의 좌표를 통과하고 있다. 이러한 곡선이, 식 (1)의 2차 다항식을 나타내고 있다. (k, n) 임계치법에서는, n=4개 중 k=3개의 셰어를 사용함으로써 비밀정보를 복원할 수 있다. 즉, 도 1에 나타내는 4곳의 좌표 중, 임의의 3곳의 좌표를 통과하는 것에 의하여도, 마찬가지의 곡선을 그릴 수 있다. 한편으로, k-1개의 셰어를 사용하는 것에 의하여는, 비밀정보를 복원할 수 없다. 즉, 도 1에 나타내는 4곳의 좌표 중 임의의 2곳의 좌표를 통과하는 것에 의하여는, 마찬가지의 곡선을 그릴 수 없다.

[0022] 도 2는, k=3개의 셰어값을 좌표로 하고, 각 좌표를 통과하는 곡선을 그린 그래프를 나타내고 있다. 도 2로부터 이해할 수 있는 바와 같이, 임계치인 k=3곳의 좌표를 알면, 도 1에 나타내는 곡선과 동일한 곡선을 그릴 수 있다. 도 3은, k-1=2개의 셰어값을 좌표로 하고, 각 좌표를 통과하는 곡선을 그린 그래프를 나타내고 있다. 도 2로부터 이해할 수 있는 바와 같이, 임계치 k-1=2 부분의 좌표만에서는, 파선으로 나타내는 곡선 등도 그릴 수 있어, 반드시 도 1에 나타내는 곡선과 동일한 곡선을 그릴 수 없다. 즉, k-1(2)개의 셰어를 사용하는 것에 의하여는, 식 (1)에 나타낸 2차 다항식을 도출할 수 없고, 나아가서는 비밀정보 S를 복원할 수 없다.

[0023] k개의 셰어값으로부터는, 다항식 보간을 사용하는 것에 의하여 비밀정보를 복원할 수 있는데, 그 구체적인 산출식을 이하에 나타낸다. 우선, 임계치 k=3인 것으로부터, 셰어를 생성하는 다항식이 $y=x^2+x+$정수항인 2차 다항식인 것을 알 수 있다. 그리고, 각 항의 계수를 a, b 및 c로 치환하고, $y=a^2+b+c$로 하며, k=3개의 셰어값의 집합, k={(1, 4), (2, 3), (3, 6)}을 대입한다. 이에 따라, 이하와 같이 식 (2) 내지 식 (4)를 산출할 수 있다.

[0024] $c=-a-b+4$ 식 (2)

[0025] $c=-4a-2b+3$ 식 (3)

[0026] $c=-9a-3b+6$ 식 (4)

[0027] 다음으로, 식 (2)를 식 (3) 및 식 (4)에 각각 대입한다. 이에 따라, 이하와 같이 식 (5) 및 식 (6)을 통하여 a (즉, 식 (1)에 나타낸 2차 다항식의 제1 항의 계수)를 도출할 수 있다.

[0028] $3a=-b-1$ 식 (5)

[0029] $8a=-2b+2$ 식 (6)

[0030] $a=2$

[0031] 상기 식으로부터 계수 a의 값을 도출할 수 있었으므로, 도출한 a의 값을 식 (2) 및 식 (3)에 대입한다. 이에 따라, 이하와 같이 식 (7) 및 식 (8)을 통하여 b(즉, 식 (1)에 나타낸 2차 다항식의 제2 항의 계수)를 도출할 수 있다.

[0032] c=-b+2 식 (7)

[0033] c=-2b-5 식 (8)

[0034] b=-7

[0035] 마지막으로, 도출한 계수 a의 값 및 계수 b의 값을 식 (2)에 대입한다. 이에 따라, c=9(즉, 식 (1)에 나타낸 2차 다항식의 정수항의 값)를 도출할 수 있다.

[0036] 이상과 같이 하여서 도출한 계수의 값을 2차 다항식에 대입하면, 식 (1)에 나타낸 2차 다항식, 즉 비밀정보 S를 복원할 수 있는 것을 알 수 있다. 이러한 비밀정보 S를 복원하는 구체적인 식은, 예를 들어 비특허문헌 1에 개시되어 있는 바와 같이 공지이므로, 본 명세서에서는 구체적인 설명은 하지 않는다.

[0037] 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 상술한 (k, n) 임계치법을 포함하는 어느 비밀분산법을 사용하여 n개의 셰어를 생성하고, k개의 셰어를 사용하여, 비밀정보를 복원한다. (k, n) 임계치값법에서는, n>k인데, 사용하는 비밀분산법에 따라서는, n=k의 경우도 있고, 그와 같은 경우에도 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템을 적용할 수 있다는 것에 유의하길 바란다.

[0038] 이하, 본 명세서에서는, 비밀분산법을 사용하여 n개의 셰어를 생성할 때에 사용하는 산출식을, 비밀정보 복원가능값(셰어) 생성식이라고 한다. 또한, 생성한 n개의 셰어 중 k개의 셰어를 사용하여 비밀정보를 복원할 때에 사용하는 산출식을 비밀정보 복원식이라고 한다. 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템이 (k, n) 임계치법을 이용하는 경우, 셰어 생성식 및 비밀정보 복원식은 각각, 비특허문헌 1에 나타내는 산출식이 사용된다. (k, n) 임계치법에 더하여, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템이 다른 비밀분산법을 이용하는 경우, 그 비밀분산법에 대응하는 셰어 생성식 및 비밀정보 복원식이 각각 사용된다.

[0039] 다음으로, 도 4를 참조하여, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템을 구성하는 컴퓨터 시스템 전체의 구성예를 나타내고 있다. 본 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 단독으로 사용되지 않고, 비밀정보 복원가능값 분산시스템을 이용하는 서비스(컴퓨터 시스템)가 존재하는 것이 전제가 된다. 하지만, 상술한 컴퓨터 시스템 자체가 본 실시형태에 따른 비밀정보 복원가능값 분산시스템을 실장하여도 좋다.

[0040] 이하의 실시형태에서는, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템이, 비트코인 등의 가상통화를 사용한 결제서비스를 제공하는 컴퓨터 시스템(이하, 결제시스템)과 연동하는 예를 설명한다. 이 예에서는, 가상통화를 사용하여 결제(송금)를 행하는 경우, 이용자(송금원)가 비밀키를 생성하고, 생성한 비밀키를 사용하여 가상통화의 트랜잭션 이력정보의 서명을 행한다. 이러한 것으로부터, 결제시스템에 있어서 생성된 비밀키에 근거하여, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템이 n개의 셰어를 생성하고, k개의 셰어에 근거하여 비밀키를 복원한다.

[0041] 도 4에 나타내는 바와 같이, 본 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 컴퓨터 단말(1) 및 서버 컴퓨터(2)를 포함하고, 그들이 네트워크(3)(인터넷 등의 공중네트워크, 본 실시형태에서는 P2P 네트워크)를 통하여 접속되어 있다.

[0042] 컴퓨터 단말(1)은, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템을 실장하는 컴퓨터 디바이스이다. 컴퓨터 단말(1)은, 예를 들어 스마트폰, 태블릿 컴퓨터 및 퍼스널 컴퓨터 등에 실장되어도 좋다. 이용자는, 컴퓨터 단말(1)을 사용하여 소정의 정보를 입력하는 것에 의하여, n개의 셰어를 생성하고, 그 중 k개의 셰어를 사용하여 비밀정보를 복원한다.

[0043] 서버 컴퓨터(2)는, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산방법을 이용하여 결제서비스 등을 제공하는 기능을 실행하는 컴퓨터 디바이스이다. 본 실시형태에서는, 컴퓨터 단말(1)이 단독으로 n개의 셰어를 생성하고, 비밀정보를 복원하는 처리를 실행한다. 하지만, 컴퓨터 단말(1)과 서버 컴퓨터(2)가 연동하여, 비밀정보 복원가능값 분산시스템을 실장하여도 좋다. 이 경우, 컴퓨터 단말(1)로부터의 요구에 따라서, 서버 컴퓨터(2)가 n개의 셰어를 생성한다.

[0044] 다음으로, 도 5를 참조하여, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템을 구성하는 컴퓨터

단말(1)의 상세한 구성의 예를 설명한다. 컴퓨터 단말(1)은, 제어장치(11), 메모리(12), 기억장치(13), 통신장치(14), 입력 디바이스(15), 입력 드라이버(16), 출력 디바이스(17), 및 출력 드라이버(18)를 포함한다.

[0045] 제어장치(11)는, 프로세서 등에 실장되고, 중앙처리장치(CPU), 그래픽 프로세싱유닛(GPU), 및 1개 또는 복수의 제어장치코어를 포함하여도 좋다. 제어장치(11)는, 소정의 프로그램(OS 및 어플리케이션 프로그램)을 실행한다. 메모리(12)는, 휘발성 또는 비휘발성 메모리, 예를 들어 랜덤 액세스 메모리(RAM), 다이나믹 RAM, 또는 캐시메모리를 포함하여도 좋다. 메모리(12)는, 제어장치(11)가 실행하는 프로그램 데이터를 일시적으로 기억한다.

[0046] 기억장치(13)는, 컴퓨터 단말(1)에 내장된 기억장치이고, 예를 들어 하드디스크 드라이브, 솔리드 스테이트 드라이브, 광디스크, 및 플래시 드라이브를 포함하여도 좋다. 기억장치(13)는, 생성된 n개 중 1개의 셰어를 기억한다. 통신장치(14)는, 네트워크 인터페이스 카드(예를 들어, LAN 카드) 등에 실장되고, 네트워크(3)를 통하여 데이터를 송수신한다.

[0047] 입력 디바이스(15)는, 키보드, 키패드, 터치스크린, 터치패드, 마이크로폰, 가속도계, 자이로스코프, 및 생체스캐너 등을 포함하여도 좋다. 입력 디바이스(15)는, 입력 드라이버(16)를 통하여, 이용자에 의한 입력을 수신하고, 그것을 제어장치(11)와 통신한다.

[0048] 출력 디바이스(17)는, 디스플레이, 스피커, 및 프린터 등을 포함하여도 좋다. 출력 디바이스(17)는, 출력 드라이버(18)를 통하여 제어장치(11)로부터의 출력을 수신하고, 그것을 출력한다(디스플레이를 통한 시각적 출력, 스피커를 통한 음성출력 등).

[0049] 컴퓨터 단말(1)에는, 탈착가능 기억장치(19)가 접속된다. 탈착가능 기억장치(19)가 접속되면, 입력 드라이버(16)를 통하여 탈착가능 기억장치(19)로부터의 정보가 제어장치(11)와 통신된다. 또한, 제어장치(11)로부터의 출력이 출력 드라이버(18)를 통하여 탈착가능 기억장치(19)에 출력(기억)된다. 탈착가능 기억장치(19)는, 예를 들어 USB 메모리 및 SD 카드 등의 플래시메모리, CD-ROM 및 DVD 등의 광학기억매체, 플로피디스크 등의 자기기억매체 등 어떠한 착탈 가능, 및 비휘발성의 기억장치를 포함한다.

[0050] 본 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 소정의 컴퓨터 시스템과 연동하는 것은 상술한 바와 같다. 즉, 컴퓨터 단말(1) 상에서, 그 소정의 컴퓨터 시스템이 제공하는 어플리케이션 프로그램이 실행된다. 본 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 컴퓨터 단말(1) 상에서 실행되는 어플리케이션 프로그램에 대응하는 서비스마다 독립적으로 실행되는 것이 바람직하다.

[0051] 예를 들어, 컴퓨터 단말(1)이 Apple(등록상표)사 제품의 오퍼레이팅 시스템 'iOS(등록상표)'를 실행하는 경우(iPhone(등록상표) 등), 기억장치(13)가 서비스마다 논리적으로 독립된 기억영역을 구성하게 된다. 이 경우, 예를 들어 컴퓨터 단말(1)이 복수의 어플리케이션 프로그램을 실행하고, 각 어플리케이션 프로그램이 비밀정보 복원가능값 분산시스템과 연동한다. 따라서, 어플리케이션 프로그램에 대응하는 서비스마다 논리적으로 독립된 기억영역이 사용된다. 이것은, 후술하는 셰어를 기억장치(13)에 기억할 때, 실행하는 어플리케이션 프로그램마다 논리적으로 독립된 영역에 기억할 수 있다는 것을 의미하여, 시큐리티가 보다 높아지게 된다.

[0052] 컴퓨터 단말(1)이 iOS 이외의 오퍼레이팅 시스템을 실행하는 경우(Windows(등록상표) 및 Android(등록상표) 등), 예를 들어 컨테이너형 가상화 기술을 사용함으로써, 서비스마다, 또는 유저마다 기억영역을 독립시킬 수 있다. 이와 같이, 복수의 어플리케이션 프로그램을 실행하고, 각 어플리케이션 프로그램이 비밀정보 복원가능값 분산시스템과 연동하는 경우, 독립된 기억영역을 실장함으로써, 시큐리티를 더욱 확보할 수 있다.

[0053] 다음으로, 도 6을 참조하여, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템이 실행하는 비밀정보 복원가능값(셰어) 생성처리를 설명한다. 본 실시형태에서는, 상술한 결제서비스에 있어서 사용되는 비밀키를 비밀정보로 하고, 그러한 비밀키에 근거하여 셰어를 생성하여, 셰어를 분산하여서 기억하는 예를 설명한다. 이 경우, 그 결제서비스를 제공하는 어플리케이션 프로그램과 비밀정보 복원가능값 분산시스템이 연동하고, 이하에서는, 결제서비스를 제공하는 어플리케이션 프로그램을 결제어플리케이션이라고 한다. 결제서비스는, 컴퓨터 단말(1)과 서버 컴퓨터(2) 사이에서 정보를 교환하는 것에 의하여 행하여진다.

[0054] 도 6에 나타내는 바와 같이, 컴퓨터 단말(1)의 제어장치(11)가, 소정의 프로그램을 실행하는 것에 의하여, 스텝 S61 내지 스텝 S64를 포함하는 셰어생성처리를 실행한다. 스텝 S61에서는, 제어장치(11)가 결제 어플리케이션을 실행함으로써, 비밀키를 생성한다. 이러한 처리는, 종래기술에 따라서, 결제서비스에 있어서 가상통화를 송금할 때에 사용하는 비밀키의 생성처리를 포함한다. 생성된 비밀키는, 메모리(12) 및/또는 기억장치(13)에 기억된다.

[0055] 스텝 S62에서는, 제어장치(11)가, 스텝 S61에서 생성한 비밀키에 근거하여, 상술한 셰어생성식을 사용하여, 셰

어수 (n)개의 셰어를 생성한다. 본 실시형태에서는, n=3인 것으로 하고, 각각의 셰어를 식별하기 위하여, 셰어 1~셰어 3으로 나타낸다. 또한, 임계치 k=2인 것으로 한다.

[0056] 여기에서, 스텝 S62에서 생성되는 셰어는, 예를 들어 '.t×t'의 확장자를 가지는 파일이고, 파일 중에 비밀분산법에 근거하여 산출된 값이 입력된다. 또한, 파일명은, 예를 들어 'UUID_셰어번호.t×t'로 하여도 좋다. UUID는, 임의의 버전에 따라서 어플리케이션 프로그램마다 일의적으로 생성된다. 즉, 본 실시형태에서는, 비밀정보 복원가능값 분산시스템과 연동하는 어플리케이션마다 일의적인 UUID가 생성된다. UUID는, 생성할 때마다 일의적인 번호가 되므로, 셰어의 파일명이 어플리케이션 프로그램마다, 및 생성할 때마다 일의적인 파일명이 된다. 이와 같이 파일명을 할당함으로써, 어플리케이션 프로그램의 독립성이 더욱 높아진다.

[0057] 한편, 파일명에 UUID를 사용하는 것은 예시적인 것에 불과하고, 이와 같은 형식으로 한정되지 않는다. 본 실시형태에 따른 비밀정보 복원가능값 분산시스템과 연동하는 서비스마다 일의적이 되는 임의의 수치를 생성하고, 그 수치를 파일명에 사용하여도 좋다. 또한, 후술하지만, 생성한 셰어는, 비밀정보를 복원할 때마다 삭제된다. 파일명에 사용하는 UUID 등의 일의적 수치는, 비밀정보를 복원할 때마다, 새로운 수치를 할당하여도 좋고, 또는 셰어를 분실하였을 때 등에만 새로운 수치를 할당하여도 좋다.

[0058] 한편, 본 실시형태에서는, 스텝 S61 및 스텝 S62의 처리를 컴퓨터 단말(1)에서 실행하고 있는데, 그와 같은 형식으로 한정되지 않는다. 스텝 S61 및/또는 스텝 S62의 처리가 서버 컴퓨터(2)에서 실행되어도 좋다. 이 경우, 예를 들어 컴퓨터 단말(1)로부터의 요구에 따라서, 서버 컴퓨터(2)가 비밀키 및/또는 셰어를 생성하고, 그것을 컴퓨터 단말(1)에 송신하게 된다. 서버 컴퓨터(2)에서 비밀키 및/또는 셰어를 생성한 경우, 컴퓨터 단말(1)에 송신한 후, 그들이 서버 컴퓨터(2)의 기억영역으로부터 삭제된다.

[0059] 스텝 S63에서는, 제어장치(11)가 스텝 S62에서 생성한 3개의 셰어를, 소정의 기억영역에 각각 기억한다. 여기에서, 소정의 기억영역이란, 컴퓨터 단말(1)의 기억장치(13)의 소정 영역에 더하여, 상술한 탈착가능 기억장치(19)를 포함한다. 즉, n개의 셰어는, 복수의 독립된 물리적 기억장치(매체)에 각각 개별적으로 기억된다. 탈착가능 기억장치(19)는, 예를 들어 USB 메모리 및 SD 카드를 포함하는 것으로 한다.

[0060] 셰어가 분산되어 기억되는 복수의 물리적 기억장치의 조합은, 상술한 조합으로 한정되지 않는다. 예를 들어, 이하에 나타내는 표 1 내지 표 3에 나타내는 조합을 생각할 수 있다.

표 1

[0061]

셰어번호	물리기억영역
1	기억장치(13)
2	USB 메모리
3	SD 카드

[0062] 표 1 물리적 기억장치의 조합 1

[0063] 표 1에 나타내는 조합은, 셰어 1이 기억장치(13)에 기억되고, 셰어 2가 USB 메모리에 기억되며, 셰어 3이 SD 카드에 기억되는 것을 나타내고 있다. 기억장치(13)는, 네트워크에 접속되는 컴퓨터 단말(1)에 내장된 기억장치이므로, 컴퓨터 단말(1)을 통하여 네트워크(3)에 접속되게 된다. 한편으로, USB 메모리 및 SD 카드는, 그것들을 제거함으로써, 네트워크(3)로부터 차단되게 된다. 이러한 것으로부터, USB 메모리 등의 탈착가능 기억장치(19)에 셰어를 기억하는 편이 보다 시큐리티가 높아진다.

[0064] 상술한 바와 같이, 본 실시형태에 따른 비밀정보 복원가능값 분산시스템에서는, k-1개의 셰어를 사용하여도, 비밀정보를 복원할 수 없다. 즉, n-(k-1)개의 셰어의 누설 등을 방지하는 것에 의하여, 비밀정보의 누설을 방지할 수 있다. 표 1에 나타내는 조합에서는, n-(k-1)(즉, 2)개의 셰어를 각각 네트워크(3)로부터 차단 가능한 탈착가능 기억장치(19)에 기억하고 있으므로, 시큐리티를 확보하는 데에 바람직한 조합이 된다.

[0065] 본 실시형태에서는, n개의 셰어를 복수의 독립된 물리적 기억장치에 기억하는 것을 보증하기 위하여, 스텝 S61 또는 스텝 S62를 실행하기 전에, 탈착가능 기억장치(19)가 컴퓨터 단말(1)에 접속되어 있는지를 판정하여도 좋다. 이러한 처리는, 제어장치(11)가, 예를 들어 Android 오퍼레이팅 시스템에 있어서 표준으로 제공되고 있는 UsbDevice 등의 디바이스 제어 API를 실행하는 것에 의하여, 탈착가능 기억장치(19)가 접속되어 있는지를 인식할 수 있다. 이러한 처리에 의하여, 제어장치(11)가, 컴퓨터 단말(1)에 탈착가능 기억장치(19)가 접속되어 있지 않다고 판정한 경우, 에러 메시지를 이용자에게 통지하여도 좋다(출력 디바이스(17)를 통하여). 한편으로, 제어

장치(11)가, 컴퓨터 단말(1)에 탈착가능 기억장치(19)가 접속되어 있다고 판정한 경우, 그러한 내용의 메시지를 이용자에게 통지하고, 후속하는 스텝 S64의 처리로 천이한다.

[0066] 또한, 디바이스 제어 API를 실행함으로써, 컴퓨터 단말(1)에 접속되어 있는 디바이스의 종별을 판정할 수 있다. 따라서, n-(k-1)개의 셰어를 탈착가능 기억장치(19)에 기억하는 것을 보증하기 위하여, n-(k-1)개의 탈착가능 기억장치(19)가 컴퓨터 단말(1)에 접속되어 있는지를 판정하여도 좋다. 표 1에 나타내는 조합에서는, SD 카드 및 USB 메모리가 각각 접속되어 있는지를 판정한다.

[0067] 표 1에 나타내는 조합에 더하여, 이하와 같은 조합도 마찬가지의 시큐리티를 확보할 수 있다.

표 2

[0068]

셰어번호	물리기억영역
1	기억장치(13)
2	USB 메모리 1
3	USB 메모리 2

[0069] 표 2 물리적 기억장치의 조합 2

[0070] 표 2에 나타내는 조합은, 셰어 2 및 셰어 3이 각각 독립된 2개의 USB 메모리에 기억되는 것을 나타내고 있다. 이와 같이, 복수의 독립된 물리적 기억장치가 동일 종별의 탈착가능 기억장치(19)인 경우, 이용자는 1번째 물리적 기억장치에 셰어를 기억한 후, 그 물리적 기억장치를 제거하고, 2번째 물리적 기억장치를 새롭게 접속할 필요가 있다.

[0071] 이와 같이, 동일 종별의 독립된 개별의 물리적 기억장치에 셰어를 기억하는 것을 보증하기 위하여, 2번째 물리적 기억장치가 접속될 때, 1번째 물리적 기억장치와 다른 물리적 기억장치인지를 판정하여도 좋다. 이러한 처리는, 제어장치(11)가 상술한 디바이스 제어 API를 실행하는 것에 의하여, 물리적 기억장치의 각각을 식별하는(접속되는 장치의 시리얼 번호 등에 의하여) 것에 의하여 행하여진다. 이러한 처리에 의하여, 제어장치(11)가 2번째 물리적 기억장치가 1번째 물리적 기억장치와 동일한 물리적 기억장치라고 판정한 경우, 에러 메시지를 이용자에게 통지하여도 좋다(출력 디바이스(17)를 통하여). 한편으로, 제어장치(11)가 2번째 물리적 기억장치가 1번째 물리적 기억장치와 다른 물리적 기억장치라고 판정한 경우, 그러한 내용의 메시지를 이용자에게 통지하여, 후속하는 스텝 S64의 처리로 천이한다.

[0072] 더욱이, 이하와 같은 조합도 가능하다.

표 3

[0073]

셰어번호	물리기억영역
1	기억장치(13)
2	네트워크 접속되는 외부기억장치
3	USB 메모리

[0074] 표 3 물리적 기억장치의 조합 3

[0075] 표 3에 나타내는 조합은, 셰어 1이 기억장치(13)에 기억되고, 셰어 2가 NAS(Network Attached Storage) 또는 SAN(Storage Area Network) 등의 네트워크 접속되는 외부기억장치에 기억되고, 셰어 3이 USB 메모리에 기억되는 것을 나타내고 있다. 이러한 조합은, k개의 수의 셰어가, 통상적으로는 네트워크로부터 차단되지 않는 기억장치에 기억되게 되므로, 표 1 및 표 2에 나타낸 조합과 비교하여, 시큐리티성이 떨어지게 된다.

[0076] 상술한 셰어가 분산되어 기억되는 기억장치의 조합은, 비밀정보 복원가능값 분산시스템에 있어서 미리 정의되어도 좋고, 또는 이용자가 임의의 타이밍에 그 조합을 설정하여도 좋다. 또한, 셰어수 및 임계치수도 마찬가지로, 비밀정보 복원가능값 분산시스템에 있어서 미리 정의되어도 좋고, 또는 이용자가 임의의 타이밍에 그 수를 설정하여도 좋다.

[0077] 스텝 S64에서는, 스텝 S61에서 생성하고, 메모리(12) 및/또는 기억장치(13)에 기억한 비밀정보를 삭제한다. 이러한 처리에 의하여, 컴퓨터 단말(1)에는, 비밀정보가 존재하지 않게 되며, 또한 n개의 셰어가 분산되어 기억되게 된다. 한편, 셰어를 기억하고나서 일정 기간이 경과하여도 탈착가능 기억장치(19)가 제거되지 않은 경우에,

그러한 내용의 메시지를 이용자에게 통지하여도 좋다. 이에 따라, 탈착가능 기억장치(19)가 컴퓨터 단말(1)로부터 제거되는 것, 즉 기억된 셰어가 네트워크로부터 차단되는 것을 보증할 수 있다.

[0078] 다음으로, 도 7을 참조하여, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템이 실행하는 비밀정보 복원처리를 설명한다. 본 실시형태에서 설명하는 비밀정보 복원처리는, 도 6에서 설명한 셰어생성처리에 있어서 생성된 비밀정보를, 통상의 이용에 있어서 복원하는 처리이다. 즉, 셰어를 1개도 누설 또는 손실하지 않고, 상술한 결제서비스에 있어서의 가상통화의 송금시의 가상통화의 트랜잭션 이력정보의 서명에 사용하는 비밀키 등을 복원하는 예이다.

[0079] 비밀정보 복원처리는 2가지 타입이 존재한다. 1번째가 상술한 통상 이용에 있어서의 복원처리이다. 2번째가 셰어의 누설, 컴퓨터 단말의 분실 혹은 교환 등일 때에 있어서의 복원처리이다. 이러한 2가지 타입의 복원처리는, 컴퓨터 단말(1)의 출력 디바이스(17)(디스플레이 등)에 표시되는 메뉴화면(미도시)에 있어서 선택할 수 있다(전자의 타입을 '통상복원 모드', 후자의 타입을 '리커버리 모드'라고 함). 리커버리 모드에서는, 비밀정보를 복원하는 것을 목적으로 하지 않고, 셰어를 다시 생성하는 것을 목적으로 한 모드이다.

[0080] 도 7에 나타내는 바와 같이, 컴퓨터 단말(1)의 제어장치(11)가, 소정의 프로그램을 실행하는 것에 의하여, 스텝 S71 내지 스텝 S73을 포함하는 비밀정보 복원처리를 실행한다. 스텝 S71에서는, 제어장치(11)가 복수의 물리적 기억장치 중 어느 것으로부터, 임계치 (k)개의 셰어를 판독한다. 본 실시형태에서는, k=2인 것으로 하고, 셰어 1이 기억장치(13)로부터 판독되며, 셰어 2가 USB 메모리로부터 판독된다.

[0081] 스텝 S71의 처리에 있어서, 도 6에서 설명한 셰어생성처리에 있어서의 스텝 S63에서 셰어를 기억하였을 때와 동일한 물리적 기억장치로부터 셰어를 판독하고 있는지를 판정하여도 좋다. 상술한 바와 같이, 제어장치(11)가 디바이스 제어 API를 실행하는 것에 의하여, 물리적 기억장치를 식별할 수 있다. 따라서, 제어장치(11)가 n개의 셰어를 기억한 시점에 각각의 물리적 기억장치의 식별자를 기억해 둠으로써, 이러한 판정을 행할 수 있다. 이러한 처리에 의하여, 기억하였을 때와 다른 물리적 기억장치로부터 셰어를 취득하고 있다고 판정한 경우, 에러 메시지를 이용자에게 통지하여도 좋다(출력 디바이스(17)를 통하여). 이에 따라, 셰어가 누설된 경우에도, 비밀정보가 제삼자에게 복원될 가능성을 더욱 저감시킬 수 있다.

[0082] 스텝 S72에서는, 제어장치(11)가, 스텝 S71에서 취득한 k개의 셰어에 근거하여, 상술한 비밀정보 복원식을 사용하여서 비밀정보를 복원한다. 복원한 비밀정보는, 어플리케이션 1과 연계하여, 결제서비스에 있어서의 가상통화의 트랜잭션 이력정보의 서명에 사용된다.

[0083] 스텝 S73에서는, 제어장치(11)가, 각 물리적 기억장치에 기억한 셰어를 삭제한다. 여기에서, 상술한 리커버리 모드를 선택한 경우, 적어도 스텝 S71에서 취득한 k개의 셰어가 기억된 k개의 물리적 기억장치로부터, 대응하는 셰어를 삭제한다. 한편으로, 통상복원 모드를 선택한 경우, n개의 셰어가 기억된 n개의 물리적 기억장치로부터, 대응하는 셰어를 삭제한다. 이러한 삭제 처리를 실행할 때, 이용자가 선택한 모드에 따라서, 소정 수의 셰어를 삭제하였는지를 판정하여도 좋다.

[0084] 또한, 스텝 S73에서는, 제어장치(11)는, 스텝 S72에서 복원한 비밀키를 삭제한다. 이러한 삭제 처리는, 비밀키를 복원한 타이밍에 타이머를 설정하고, 타이머가 소정 기간을 경과한 것에 응답하여, 비밀키를 삭제하도록 하여도 좋다. 이러한 처리에 의하여, 소정 기간을 경과한 것에 의하여, 복원한 비밀키를 컴퓨터 단말(1)로부터 삭제하므로, 비밀정보가 제삼자에게 누설될 가능성을 더욱 저감시킬 수 있다.

[0085] 이렇게 하여서, 생성 및 복원을 행할 때마다, 셰어를 삭제하고 있으므로, 비밀정보의 시큐리티를 더욱 확보할 수 있다. 한편, 상술한 리커버리 모드를 선택한 경우, 제어장치(11)는, 스텝 S73 후에, 도 6에서 설명한 셰어생성처리를 실행하도록 제어하고, 스텝 S72에서 복원한 비밀정보에 근거하여 셰어를 생성한다. 예를 들어, 식(1)에 나타낸 2차 다항식에 있어서의 제1 항의 계수 및 제2 항의 계수를 변경하는 것에 의하여, 다른 셰어를 생성할 수 있다. 이러한 처리에 의하여, 셰어 중 1개를 분실한 경우 등에서도, 새로운 셰어를 다시 생성할 수 있다.

[0086] 이상과 같이, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템을 설명하였다. 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템에 따르면, 생성한 셰어를 물리적 기억장치에 기억하므로, 예를 들어 결제서비스에서 사용되는 비밀키를 관리하는 부하가 저감된다. 또한, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템을, 예를 들어 ID 및 패스워드를 사용한 인증시스템에 적용하여도 좋다. 패스워드를 비밀정보로 하는 경우, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템에 의하여, 모든 서비스에 있어서 동일 또는 유사한 패스워드를 돌려 사용함으로써 그 패스워드가 누설될 위험성을 회피할 수 있다.

[0087] 한편으로, 셰어를 기억한 기억장치를 탈착가능 기억장치에서 실장하고, 그것을 컴퓨터 단말로부터 제거하는 것에 의하여, 셰어를 네트워크로부터 차단할 수 있다. 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템에서는, k개의 셰어가 모이지 않는 한, 비밀정보를 복원할 수 없다. 따라서, 적어도 n-(k-1)개의 셰어를 탈착가능 기억장치에 기억시키고, 그것들을 컴퓨터 단말로부터 제거하여 보관함으로써, 매우 높은 시큐리티를 확보할 수 있다.

[0088] 상기 실시형태에서 사용한 식 및 하드웨어의 구성요소는 예시적인 것에 불과하고, 그 밖의 구성도 가능한 것에 유의하길 바란다. 또한, 상기 실시형태에서 설명한 처리의 순서는, 반드시 설명한 순서로 실행될 필요가 없으며, 임의의 순서로 실행되어도 좋다. 더욱이, 본 발명의 기본적인 개념으로부터 일탈하지 않고, 추가 스텝이 새롭게 추가되어도 좋다.

[0089] 또한, 본 발명의 일 실시형태에 따른 비밀정보 복원가능값 분산시스템은, 컴퓨터 단말(1)에 의하여 실행되는 프로그램에 의하여 실장되는데, 그 프로그램은, 비일시적 기억매체에 기억되어도 좋다. 비일시적 기억매체의 예는, 리드 온리 메모리(ROM), 랜덤 액세스 메모리(RAM), 레지스터, 캐시메모리, 반도체 메모리 장치, 내장 하드디스크 및 제거가능 디스크 장치 등의 자기매체, 광자기매체, 그리고 CD-ROM 디스크 및 디지털 다용도 디스크(DVD) 등의 광학매체 등을 포함한다.

부호의 설명

[0090] 1: 컴퓨터 단말

2: 서버 컴퓨터

3: 네트워크

11: 제어장치

12: 메모리

13: 기억장치

14: 통신장치

15: 입력 디바이스

16: 입력 드라이버

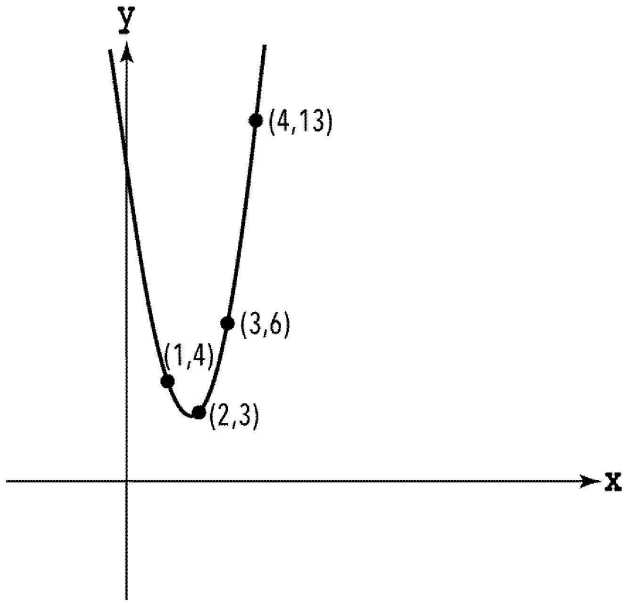
17: 출력 디바이스

18: 출력 드라이버

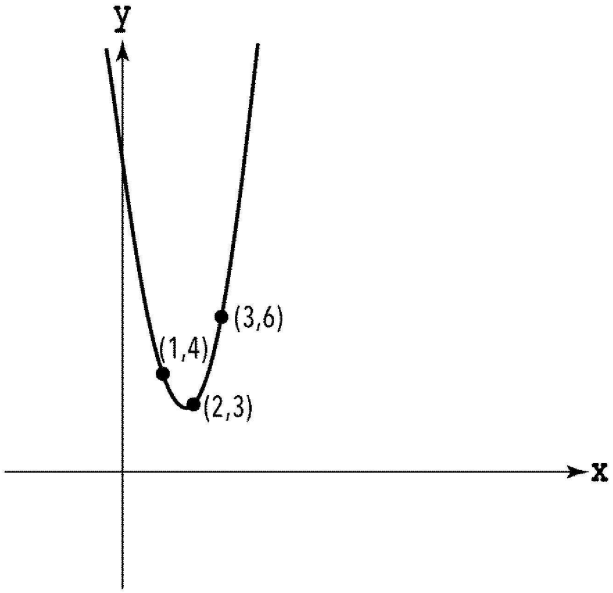
19: 탈착가능 기억장치

도면

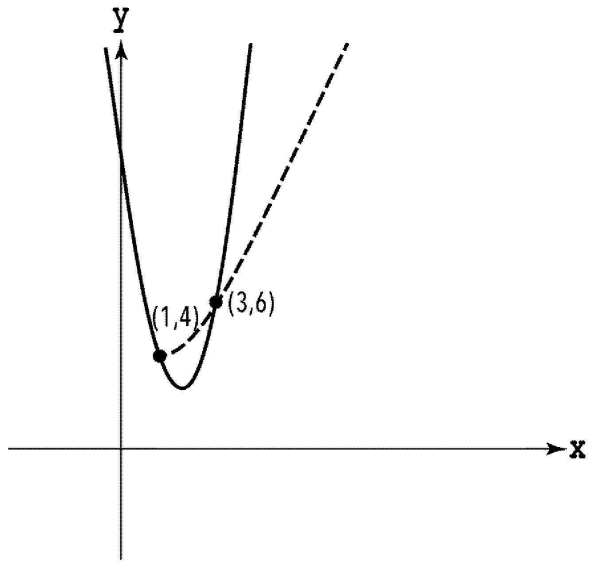
도면1



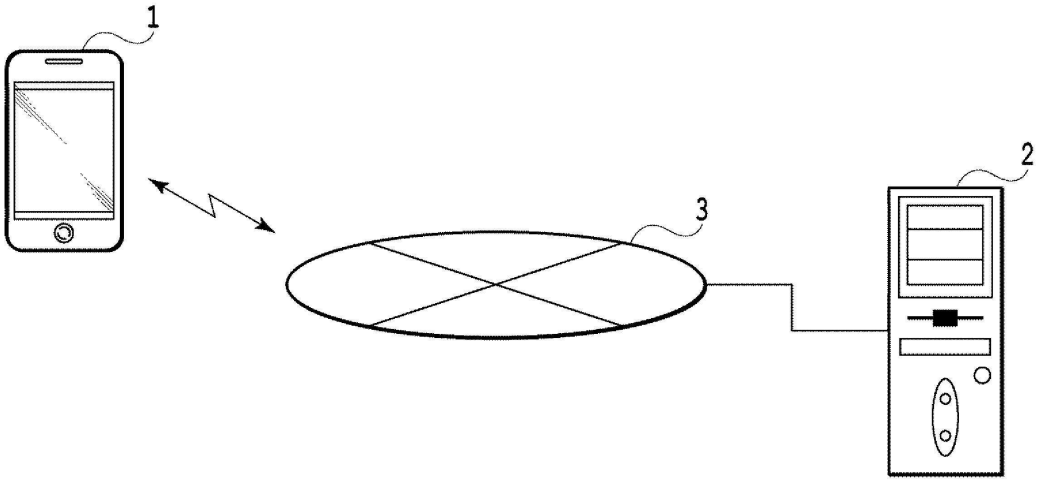
도면2



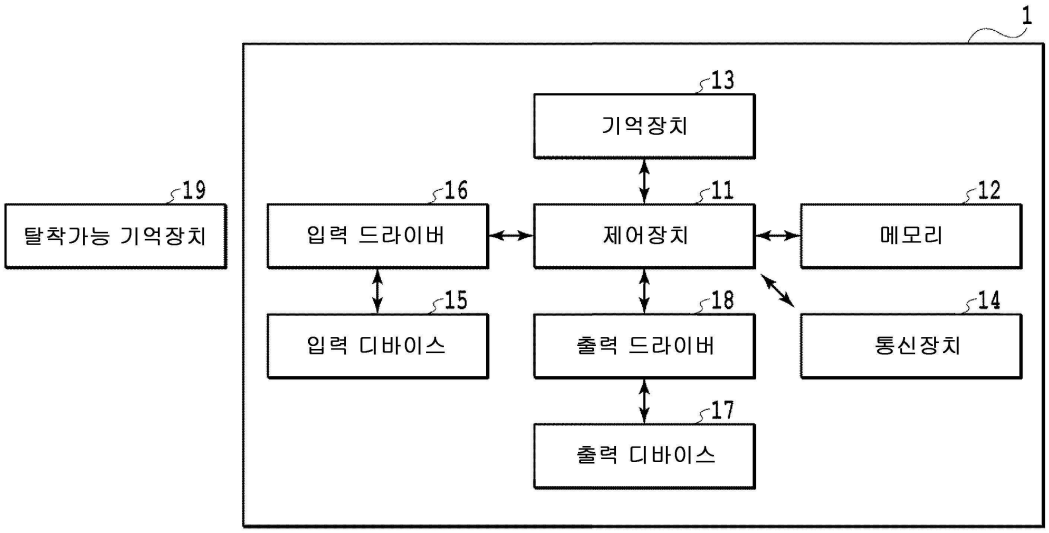
도면3



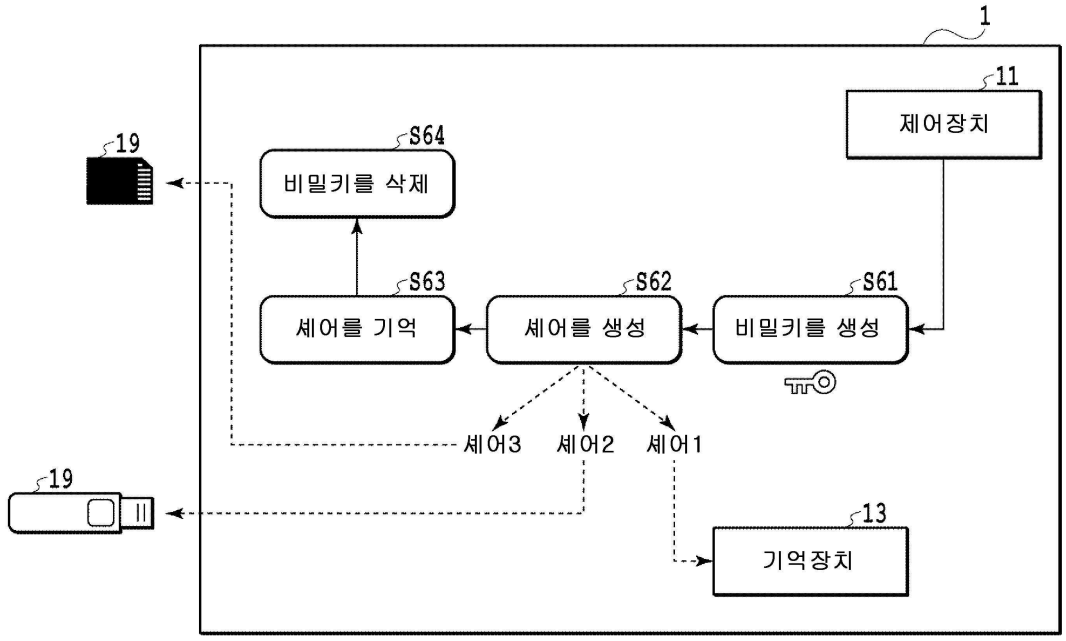
도면4



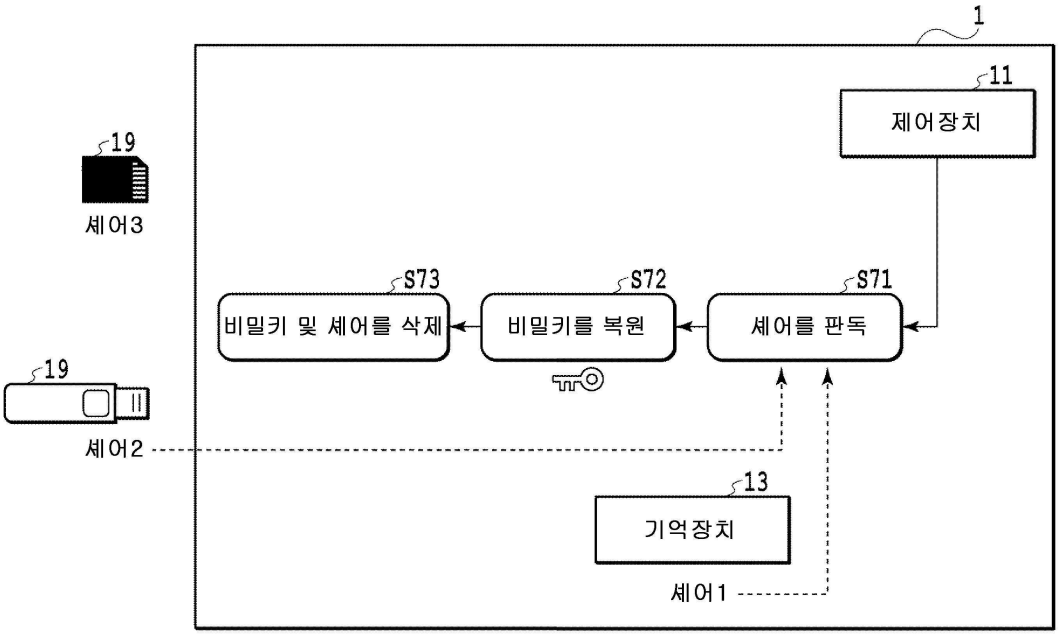
도면5


1
13
기억장치
19
탈착가능 기억장치
16
입력 드라이버
11
제어장치
12
메모리
15
입력 디바이스
18
출력 드라이버
14
통신장치
17
출력 디바이스

도면6


1
11
제어장치
19
S64
비밀키를 삭제
S63
S62
S61
제어를 기억
제어를 생성
비밀키를 생성
제어3
제어2
제어1
19
13
기억장치

도면7


1
11
제어장치
19
제어3
S73
S72
S71
비밀키 및 제어를 삭제
비밀키를 복원
제어를 판독
19
제어2
13
기억장치
제어1