(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0099454
(43) 공개일자 2014년08월12일

(51) 국제특허분류(Int. Cl.)
*H04L 9/32* (2006.01) *H04L 9/28* (2006.01)
(21) 출원번호 10-2014-7013227
(22) 출원일자(국제) 2011년12월28일
심사청구일자 2014년05월16일
(85) 번역문제출일자 2014년05월16일
(86) 국제출원번호 PCT/KR2011/010253
(87) 국제공개번호 WO 2013/100224
국제공개일자 2013년07월04일

(71) 출원인
**인하대학교 산학협력단**
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
**이문규**
경기도 부천시 원미구 계남로 81 진달래신동아베르디 2222-702
(74) 대리인
**김태홍, 김성기**

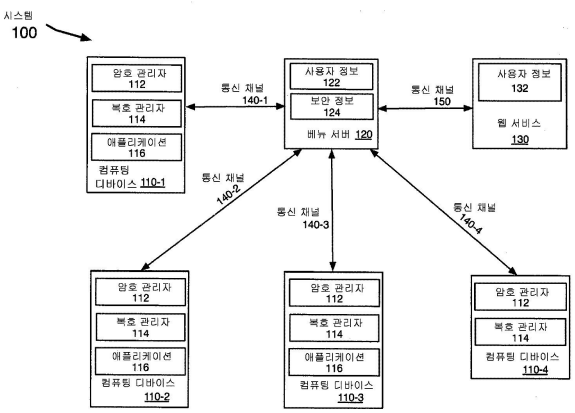
전체 청구항 수 : 총 38 항

(54) 발명의 명칭 **데이터를 안전하게 공유하기 위한 테이스트 기반 인증**

## (57) 요 약

컴퓨팅 장치의 사용자에 대한 관심 지역에 관련된 테이스트에 대한 다차원 속성 값을 변환하고, 변환된 다차원 속성 값을 암호화 또는 복호하여 다른 컴퓨팅 디바이스와 데이터를 안전하게 공유하기 위한 예들이 개시된다.

## 대 표 도



## *특허청구의 범위*

**청구항 1**

방법에 있어서,

관심 지역에 관한 제1 테이스트(taste) - 상기 제1 테이스트는 다차원 속성 값을 가짐 - 를 갖는 제1 사용자와 관련된 제1 컴퓨팅 디바이스를 적어도 일시적으로 식별하도록 제1 필명(pseudonym)을 생성하는 것;

상기 제1 컴퓨팅 디바이스에 유지되는 데이터를 하나 이상의 다른 컴퓨팅 디바이스와 안전하게 공유하도록 상기 필명과 함께 사용될 제1 세션 키를 생성하는 것;

변환 파라미터를 생성하는 것;

상기 변환 파라미터를 사용하여 상기 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 것;

제1 암호문(ciphertext)을 생성하기 위해, 상기 1차원 속성 값을 사용하여 상기 필명 및 상기 세션 키를 암호화(encrypt)하는 것; 및

상기 제1 암호문 및 상기 변환 파라미터를, 상기 제1 컴퓨팅 디바이스와 상기 하나 이상의 다른 컴퓨팅 디바이스 양자 모두에 액세스 가능한 서버에 전송하는 것을 포함하고, 상기 서버는 상기 제1 암호문 및 상기 변환 파라미터를 유지하는 것인, 방법.

**청구항 2**

제1항에 있어서,

상기 하나 이상의 다른 컴퓨팅 디바이스 중에서 제2 컴퓨팅 디바이스로부터 제2 필명 및 제2 세션 키를 수신하는 것; 및

상기 제1 필명과 실질적으로 유사한 제2 필명에 기초하여 그리고 상기 제1 세션 키와 실질적으로 유사한 제2 세션 키에 기초하여, 상기 제2 컴퓨팅 디바이스와의 보안 세션을 설정하는 것을 더 포함하는, 방법.

**청구항 3**

제2항에 있어서, 상기 제2 컴퓨팅 디바이스와의 보안 세션을 설정하는 것은 상기 관심 지역과 관련된 데이터를 공유하는 것을 포함하는 것인, 방법.

**청구항 4**

제1항에 있어서, 상기 다차원 속성 값은 상기 제1 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값에 적어도 부분적으로 기초하는 다차원 속성 값을 포함하는 것인, 방법.

**청구항 5**

제4항에 있어서, 상기 제1 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값은, 제1 축과 관련된 제1 값 및 제2 축과 관련된 제2 값을 포함하며, 상기 제1 축은 상기 제2 축과 직교하는 것인, 방법.

**청구항 6**

제5항에 있어서, 상기 변환 파라미터를 사용하여 상기 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 것은, 미리 정의된 유한 필드에 걸쳐 상기 다차원 값을 1차원 속성 값으로 변환하는 것 및 상기 1차원 속성 값을 단일 축에 매핑하는 것을 포함하는 것인, 방법.

**청구항 7**

제1항에 있어서, 상기 변환 파라미터를 생성하는 것은, 상기 하나 이상의 컴퓨팅 디바이스 중에서 제2 컴퓨팅 디바이스와의 보안 세션을 설정하고 완료하는 것에 응답하여 새로운(fresh) 변환 파라미터를 생성하는 것을 포함하고, 설정되어 완료된 상기 보안 세션은 상기 관심 지역과 관련된 데이터의 공유를 포함하는 것인, 방법.

**청구항 8**

제1항에 있어서, 상기 1차원 속성 값을 사용하여 상기 필명 및 상기 세션 키를 암호화하는 것은, 상기 제1 암호문을 생성하도록 결함 감내 암호 스킴(fault tolerant encryption scheme)의 적어도 일부를 구현하는 것을 포함하는 것인, 방법.

**청구항 9**

제1항에 있어서, 다차원 속성 값을 갖는 상기 제1 테이스트는, 상기 제1 컴퓨팅 디바이스와 상기 하나 이상의 다른 컴퓨팅 디바이스 양자 모두에 액세스 가능한 서버로부터 상기 제1 컴퓨팅 디바이스에 제공되는 다차원 속성 값을 포함하고, 상기 다차원 속성 값은 상기 제1 사용자와 관련된 정보에 적어도 부분적으로 기초하는 것인, 방법.

**청구항 10**

제1항에 있어서, 다차원 속성 값을 갖는 상기 제1 테이스트는, 상기 제1 컴퓨팅 디바이스와 상기 하나 이상의 다른 컴퓨팅 디바이스 양자 모두에 액세스 가능한 서버로부터 상기 제1 컴퓨팅 디바이스에 제공되는 일반적인 질문에 적어도 부분적으로 기초하여 상기 제1 컴퓨팅 디바이스에 의해 결정되는 다차원 속성 값을 포함하고, 상기 일반적인 질문은 상기 관심 지역에서 상기 제1 사용자의 기호(preference)에 관련되는 것인, 방법.

**청구항 11**

제1항에 있어서, 다차원 속성 값을 갖는 상기 제1 테이스트는, 상기 제1 사용자와 관련되는 정보에 적어도 부분적으로 기초하여 상기 제1 컴퓨팅 디바이스에 의해 유지되는 애플리케이션에 의해 결정되는 다차원 속성 값을 포함하는 것인, 방법.

**청구항 12**

방법에 있어서,

제1 컴퓨팅 디바이스에서, 서버로부터 제1 암호문 및 변환 파라미터 - 상기 암호문 및 상기 변환 파라미터는 제2 컴퓨팅 디바이스에 의해 생성됨 - 를 수신하는 것;

상기 제1 컴퓨팅 디바이스의 제1 사용자에 대한 제1 테이스트 - 상기 제1 테이스트는 관심 지역과 관련되고 다차원 속성 값을 가짐 - 를 수신하는 것;

상기 변환 파라미터를 사용하여 상기 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 것;

상기 제2 컴퓨팅 디바이스를 식별하는 필명을 획득하고, 상기 제2 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 상기 필명과 함께 사용될 세션 키를 획득하기 위해, 상기 1차원 속성 값을 사용하여 상기 제1 암호문을 복호하는 것;

상기 복호의 품질을 결정하는 것; 및

임계값을 초과하는 상기 복호의 결정된 품질에 적어도 부분적으로 기초하여 데이터를 공유하도록 상기 제2 컴퓨팅 디바이스와의 보안 세션을 개시하는 것을 포함하는, 방법.

**청구항 13**

제12항에 있어서, 상기 복호의 품질을 결정하는 것은, 상기 제2 컴퓨팅 디바이스의 제2 사용자에 대한 제2 테이스트에 대한 상기 제1 테이스트의 유사성(similarity)에 적어도 부분적으로 기초하고, 상기 제2 테이스트도 또한 상기 관심 지역과 관련되는 것인, 방법.

**청구항 14**

제12항에 있어서, 상기 제1 테이스트를 수신하는 것은, 상기 서버로부터 상기 제1 테이스트를 수신하는 것을 포함하고, 상기 제1 테이스트는 상기 제1 사용자와 관련된 정보에 적어도 부분적으로 기초하는 것인, 방법.

**청구항 15**

제14항에 있어서, 상기 제1 사용자와 관련된 정보는 상기 제1 사용자에 대한 구매 이력, 상기 제1 사용자에 대

한 검색 이력 또는 상기 제1 사용자에 대한 인구 통계학적 특성(demographic characteristics) 중 하나 이상을 포함하는 것인, 방법.

**청구항 16**

제12항에 있어서, 상기 제1 테이스트를 수신하는 것은, 상기 서버로부터 상기 제1 컴퓨팅 디바이스에 제공되는 일반적인 질문에 적어도 부분적으로 기초하여 상기 제1 테이스트를 수신하는 것을 포함하고, 상기 일반적인 질문은 상기 관심 지역에서의 상기 제1 사용자의 기호에 관련되는 것인, 방법.

**청구항 17**

제12항에 있어서, 상기 제1 테이스트를 수신하는 것은, 상기 제1 사용자에 대한 구매 이력, 상기 제1 사용자에 대한 검색 이력 또는 상기 제1 사용자에 대한 인구 통계학적 특성 중 하나 이상을 포함하는, 상기 제1 사용자와 관련된 정보에 적어도 부분적으로 기초하여 상기 제1 컴퓨팅 디바이스에 의해 유지되는 애플리케이션으로부터 상기 제1 테이스트를 수신하는 것을 포함하는 것인, 방법.

**청구항 18**

제12항에 있어서, 상기 다차원 속성 값은 상기 제1 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값에 적어도 부분적으로 기초하는 다차원 속성 값을 포함하는 것인, 방법.

**청구항 19**

제18항에 있어서, 상기 제1 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값은 제1 축과 관련된 제1 값 및 제2 축과 관련된 제2 값을 포함하며, 상기 제1 축은 상기 제2 축과 직교하는 것인, 방법.

**청구항 20**

제19항에 있어서, 상기 변환 파라미터를 사용하여 상기 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 것은, 미리 정의된 유한 필드에 걸쳐 상기 다차원 값을 1차원 속성 값으로 변환하는 것 및 상기 1차원 속성 값을 단일 축에 매핑하는 것을 포함하는 것인, 방법.

**청구항 21**

제12항에 있어서, 상기 필명 및 상기 세션 키를 획득하기 위해, 상기 1차원 속성 값을 사용하여 상기 제1 암호문을 복호하는 것은, 상기 필명 및 상기 세션 키를 획득하도록 결함 감내 복호 스킴의 적어도 일부를 구현하는 것을 포함하는 것인, 방법.

**청구항 22**

장치에 있어서,

로직(logic)을 갖는 암호 관리자를 포함하고, 상기 로직은:

관심 지역에 관한 제1 테이스트 - 상기 제1 테이스트는 다차원 속성 값을 가짐 - 를 갖는 제1 사용자와 관련된 제1 컴퓨팅 디바이스를 적어도 일시적으로 식별하도록 제1 필명을 생성하고;

상기 제1 컴퓨팅 디바이스에 유지되는 데이터를 하나 이상의 다른 컴퓨팅 디바이스와 안전하게 공유하도록 상기 필명과 함께 사용될 제1 세션 키를 생성하고;

변환 파라미터를 생성하고;

상기 변환 파라미터를 사용하여 상기 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하고;

제1 암호문을 생성하기 위해, 상기 1차원 속성 값을 사용하여 상기 필명 및 상기 세션 키를 암호화하고;

상기 제1 암호문 및 상기 변환 파라미터를, 상기 제1 컴퓨팅 디바이스와 상기 하나 이상의 다른 컴퓨팅 디바이스 양자 모두에 액세스 가능한 서버에 전송하도록 구성되며, 상기 서버는 상기 제1 암호문 및 상기 변환 파라미터를 유지하는 것인, 장치.

**청구항 23**

제22항에 있어서, 상기 로직이,

상기 하나 이상의 다른 컴퓨팅 디바이스 중에서 제2 컴퓨팅 디바이스로부터 제2 필명 및 제2 세션 키를 수신하고;

상기 제1 필명과 실질적으로 유사한 제2 필명에 기초하여 그리고 상기 제1 세션 키와 실질적으로 유사한 제2 세션 키에 기초하여, 상기 제2 컴퓨팅 디바이스와의 보안 세션을 설정하도록, 구성되는 것을 더 포함하는 것인, 장치.

**청구항 24**

제23항에 있어서, 상기 제2 컴퓨팅 디바이스와의 보안 세션을 설정하는 것은, 상기 로직이, 상기 관심 지역과 관련된 데이터를 공유하도록 구성되는 것을 포함하는 것인, 장치.

**청구항 25**

제22항에 있어서, 상기 다차원 속성 값은 상기 제1 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값에 적어도 부분적으로 기초하는 다차원 속성 값을 포함하는 것인, 장치.

**청구항 26**

제25항에 있어서, 상기 제1 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값은, 제1 축과 관련된 제1 값 및 제2 축과 관련된 제2 값을 포함하며, 상기 제1 축은 상기 제2 축과 직교하는 것인, 장치.

**청구항 27**

제26항에 있어서, 상기 변환 파라미터를 사용하여 상기 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 것은, 상기 로직이, 미리 정의된 유한 필드에 걸쳐 상기 다차원 값을 1차원 속성 값으로 변환하고, 또한 상기 1차원 속성 값을 단일 축에 매핑하도록 구성되는 것을 포함하는 것인, 장치.

**청구항 28**

제22항에 있어서, 상기 1차원 속성 값을 사용하여 상기 필명 및 상기 세션 키를 암호화하는 것은, 상기 로직이, 상기 제1 암호문을 생성하도록 결함 감내 암호 스킴의 적어도 일부를 구현하도록 구성되는 것을 포함하는 것인, 장치.

**청구항 29**

컴퓨팅 디바이스에 있어서,

컴퓨팅 디바이스의 사용자에 대한 테이스트 - 상기 제1 테이스트는 관심 지역과 관련되고 다차원 속성 값을 가짐 - 를 생성하기 위한 로직을 갖는 애플리케이션; 및

로직을 갖는 복호 관리자를 포함하고,

상기 로직은:

서버로부터 암호문 및 변환 파라미터 - 상기 암호문 및 상기 변환 파라미터는 다른 컴퓨팅 디바이스에 의해 생성됨 - 를 수신하고;

상기 애플리케이션으로부터 상기 다차원 속성 값을 수신하고;

상기 변환 파라미터를 사용하여 상기 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하고;

상기 다른 컴퓨팅 디바이스를 식별하는 필명을 획득하고, 상기 다른 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 상기 필명과 함께 사용될 세션 키를 획득하기 위해, 상기 1차원 속성 값을 사용하여 상기 암호문을 복호하고;

상기 복호의 품질을 결정하고;

임계값을 초과하는 상기 복호의 결정된 품질에 적어도 부분적으로 기초하여 데이터를 공유하도록 상기 다른 컴퓨팅 디바이스와의 보안 세션을 개시하도록 구성되는 것인, 컴퓨팅 디바이스.

**청구항 30**

제29항에 있어서, 상기 복호의 품질을 결정하는 것은, 상기 다른 컴퓨팅 디바이스의 다른 사용자에 대한 또 다른 테이스트와 비교하여 상기 사용자에 대한 테이스트의 유사성에 적어도 부분적으로 기초하고, 상기 또 다른 테이스트도 또한 상기 관심 지역과 관련되는 것인, 시스템.

**청구항 31**

제30항에 있어서, 상기 다차원 속성 값은 상기 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값에 적어도 부분적으로 기초하는 다차원 속성 값을 포함하는 것인, 시스템.

**청구항 32**

제31항에 있어서, 상기 사용자에 대한 상기 테이스트를 특징으로 하는 2 이상의 속성에 대해 개별적으로 할당된 값은, 제1 축과 관련된 제1 값 및 제2 축과 관련된 제2 값을 포함하며, 상기 제1 축은 상기 제2 축과 직교하는 것인, 시스템.

**청구항 33**

제32항에 있어서, 상기 변환 파라미터를 사용하여 상기 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 것은, 상기 로직이, 미리 정의된 유한 필드에 걸쳐 상기 다차원 값을 1차원 속성 값으로 변환하고 상기 1차원 속성 값을 단일 축에 매핑하도록 구성되는 것을 포함하는 것인, 시스템.

**청구항 34**

제29항에 있어서, 상기 필명 및 상기 세션 키를 획득하기 위해 상기 1차원 속성 값을 사용하여 상기 암호문을 복호하는 것은, 상기 로직이, 상기 필명 및 상기 세션 키를 획득하기 위해 결함 감내 복호 스킴의 적어도 일부를 구현하도록 구성되는 것을 포함하는 것인, 시스템.

**청구항 35**

제1 컴퓨팅 디바이스에서 구현될 명령어를 갖는 비일시적 매체를 포함하는 컴퓨터 프로그램 제품에 있어서,

상기 명령어는, 로직에 의해 실행될 때, 상기 로직으로 하여금:

서버로부터 제1 암호문 및 변환 파라미터 - 상기 제1 암호문 및 변환 파라미터는 제2 컴퓨팅 디바이스에 의해 생성됨 - 를 수신하고;

상기 제1 컴퓨팅 디바이스의 제1 사용자에 대한 제1 테이스트 - 상기 제1 테이스트는 관심 지역과 관련되고 다차원 속성 값을 가짐 - 를 수신하고;

상기 변환 파라미터를 사용하여 상기 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하고;

상기 제2 컴퓨팅 디바이스를 식별하는 필명을 획득하고, 상기 제2 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 상기 필명과 함께 사용될 세션 키를 획득하기 위해, 상기 1차원 속성 값을 사용하여 상기 제1 암호문을 복호하고;

상기 복호의 품질을 결정하고;

임계값을 초과하는 상기 복호의 결정된 품질에 적어도 부분적으로 기초하여 데이터를 공유하도록 상기 제2 컴퓨팅 디바이스와의 보안 세션을 개시하도록 하는 것인, 컴퓨터 프로그램 제품.

**청구항 36**

제35항에 있어서, 상기 복호의 품질을 결정하는 것은, 상기 제2 컴퓨팅 디바이스의 제2 사용자에 대한 제2 테이스트에 대한 상기 제1 테이스트의 유사성에 적어도 부분적으로 기초하고, 상기 제2 테이스트도 또한 상기 관심 지역과 관련되는 것인, 컴퓨터 프로그램 제품.

**청구항 37**

제35항에 있어서, 상기 제1 테이스트를 수신하는 것은 상기 서버로부터 상기 제1 테이스트를 수신하는 것을 포

함하며, 상기 제1 테이스트는 상기 제1 사용자에 대한 구매 이력, 상기 제1 사용자에 대한 검색 이력 또는 상기 제1 사용자에 대한 인구 통계학적 특성 중 하나 이상을 포함하는 상기 제1 사용자와 관련된 정보에 적어도 부분적으로 기초하는 것인, 컴퓨터 프로그램 제품.

**청구항 38**

제35항에 있어서, 상기 제1 테이스트를 수신하는 것은, 상기 로직으로 하여금, 상기 제1 사용자에 대한 구매 이력, 상기 제1 사용자에 대한 검색 이력 또는 상기 제1 사용자에 대한 인구 통계학적 특성 중 하나 이상을 포함하는 상기 제1 사용자와 관련된 정보에 적어도 부분적으로 기초하여 상기 제1 컴퓨팅 디바이스에 의해 유지되는 애플리케이션으로부터 상기 제1 테이스트를 수신하도록 하기 위한 명령어를 포함하는 것인, 컴퓨터 프로그램 제품.

# 명 세 서

## 기 술 분 야

[0001] 본 발명은 데이터를 안전하게 공유하기 위한 테이스트(taste) 기반 인증 방법 및 장치에 관한 것이다.

## 배 경 기 술

[0002] 본 명세서에서 달리 나타내는 바가 없으면, 이 섹션에서 기재되는 접근법은 이 출원의 청구범위에 대한 종래 기술이 아니고, 이 섹션에 포함하여 종래 기술이라고 인정되는 것도 아니다.

[0003] 컴퓨팅 장치들 사이에서의 데이터의 안전한 공유는 컴퓨팅 장치의 사용자의 바람직한 목표일 수 있다. 또한, 사용자는 관심 지역에 대한 유사한 기호(preference) 또는 테이스트에 기초하여 다른 사용자와 데이터를 공유하기를 원할 수 있다. 이들 사용자는 또한, 데이터를 공유하면서 다른 엔티티로부터 사적 권리 및/또는 보안성의 허용 가능 레벨을 유지하기를 원할 수 있다. 이들 다른 엔티티는 원하지 않는 광고주, 스패머(spammer) 또는 악의적인 액터(actor)를 포함할 수 있다.

## 발명의 내용

[0004] 다양한 실시예에서, 본 개시내용은 암호문을 암호화하여 암호문을 서버에 전송하는 방법의 예들을 기술한다. 그 방법은 관심 지역에 관한 제1 테이스트를 갖는 제1 사용자와 관련된 제1 컴퓨팅 디바이스를 적어도 일시적으로 식별하도록 제1 필명(pseudonym)을 생성하는 것을 포함할 수 있다. 제1 테이스트는 다차원 속성 값을 가질 수 있다. 제1 세션 키는 그 후, 제1 컴퓨팅 디바이스 상에 유지되는 데이터를 하나 이상의 다른 컴퓨팅 디바이스와 안전하게 공유하기 위해 필명과 함께 사용되도록 생성될 수 있다. 변환 파라미터가 또한 생성된 후, 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 데 사용될 수 있다. 필명 및 세션 키는 그 후, 제1 암호문을 생성하기 위해 1차원 속성 값을 사용하여 암호화될 수 있다. 몇몇 예들에서는, 제1 암호문 및 변환 파라미터가 제1 컴퓨팅 디바이스와 하나 이상의 다른 컴퓨팅 디바이스의 양자 모두에 액세스 가능한 서버에 전송될 수 있다. 이들 예에서는, 서버는 제1 암호문 및 변환 파라미터를 유지할 수 있다.

[0005] 다양한 실시예에서, 본 개시내용은 또한 암호문을 복호하고 보안 세션을 개시하는 방법의 예를 기술한다. 그 방법은 서버로부터 제1 암호문 및 변환 파라미터를 수신하는 제1 컴퓨팅 디바이스를 포함할 수 있다. 제2 컴퓨팅 디바이스가 암호문 및 변환 파라미터를 생성했을 수 있다. 제1 컴퓨팅 디바이스의 제1 사용자에 대한 제1 테이스트가 또한 수신될 수 있다. 제1 테이스트에 대한 다차원 속성 값이 그 후, 1차원 속성 값으로 변환될 수 있다. 또한, 제1 암호문은, 제2 컴퓨팅 디바이스를 식별하는 필명을 획득하기 위해 및 제2 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 필명과 함께 사용될 세션 키를 획득하기 위해 1차원 속성 값을 사용하여 복호될 수 있다. 몇몇 예들에서는, 복호의 품질이 그 후, 판정될 수 있다. 이들 예에서는, 데이터를 공유하도록 제2 컴퓨팅 디바이스와의 보안 세션이 임계값을 초과하는 복호의 판정된 품질을 적어도 부분적으로 기초로 하여 개시될 수 있다.

[0006] 다양한 실시예에서, 본 개시내용은 암호문을 암호화하여 암호문을 서버에 전송하는 디바이스의 예들을 기술한다. 그 디바이스의 예는 로직을 갖는 암호 관리자를 가질 수 있다. 로직은 관심 지역에 관한 제1 테이스트를 갖는 제1 사용자와 관련된 제1 컴퓨팅 디바이스를 적어도 일시적으로 식별하도록 제1 필명을 생성하도록 구성될 수 있다. 제1 테이스트는 다차원 속성 값을 가질 수 있다. 로직은 또한, 제1 세션 키를 생성하도록 구성될 수 있다. 제1 세션 키는 제1 컴퓨팅 디바이스 상에 유지되는 데이터를 하나 이상의 다른 컴퓨팅 디바이스

와 안전하게 공유하기 위해 필명과 함께 사용될 수 있다. 로직은 또한 그 후, 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하는 데 사용될 수 있는 변환 파라미터를 생성하도록 구성될 수 있다. 로직은 또한, 제1 암호문을 생성하기 위해 1차원 속성 값을 사용하여 필명 및 세션 키를 암호화할 수 있다. 몇몇 예들에서는, 로직이 제1 암호문 및 변환 파라미터를 제1 컴퓨팅 디바이스와 하나 이상의 다른 컴퓨팅 디바이스의 양자 모두에 액세스 가능한 서버에 전송하도록 구성될 수 있다. 이들 예에서는, 서버는 제1 암호문 및 변환 파라미터를 유지할 수 있다.

[0007] 다양한 실시예에서, 본 개시내용은 또한, 암호문을 복호하고 보안 세션을 개시하기 위한 컴퓨팅 디바이스의 일례를 기술한다. 그 컴퓨팅 디바이스의 예는 애플리케이션 및 복호 관리자를 포함할 수 있다. 애플리케이션은 컴퓨팅 디바이스의 사용자에 대한 테이스트를 생성하도록 로직을 포함할 수 있다. 제1 테이스트는 관심 지역과 관련될 수 있고, 다차원 속성 값을 가질 수 있다. 암호 관리자는 서버로부터 암호문 및 변환 파라미터를 수신하도록 구성되는 로직을 가질 수 있고, 암호문 및 변환 파라미터는 다른 컴퓨팅 디바이스에 의해 생성되었을 수 있다. 암호 관리자는 또한, 애플리케이션으로부터 다차원 속성 값을 수신하고, 변환 파라미터를 사용하여 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하도록 구성되는 로직을 가질 수 있다. 암호 관리자는 또한, 다른 컴퓨팅 디바이스를 식별하는 필명을 획득하기 위해 및 다른 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 필명과 함께 사용될 세션 키를 획득하기 위해 1차원 속성 값을 사용하여 암호문을 복호하도록 구성되는 로직을 가질 수 있다. 몇몇 예들에서는, 암호 관리자는 복호의 품질을 판정하고, 임계값을 초과하는 복호의 판정된 품질을 적어도 부분적으로 기초로 하여 데이터를 공유하도록 다른 컴퓨팅 디바이스와의 보안 세션을 개시하도록 구성되는 로직을 가질 수 있다.

[0008] 다양한 실시예에서, 본 개시내용은 또한, 컴퓨터 프로그램 제품의 예를 기술한다. 몇몇 예들에서는, 컴퓨터 프로그램 제품은 제1 컴퓨팅 디바이스에서 구현되는 명령을 갖는 신호 베어링(bearing) 매체를 포함할 수 있다. 명령은, 로직에 의해 실행될 때, 로직이 서버로부터 암호문 및 변환 파라미터를 수신하게 할 수 있다. 제2 컴퓨팅 디바이스가 암호문 및 변환 파라미터를 생성했을 수 있다. 명령은 또한, 로직이 제1 컴퓨팅 디바이스의 제1 사용자에 대한 제1 테이스트를 수신하게 할 수 있다. 제1 테이스트는 관심 지역과 관련될 수 있고 다차원 속성 값을 가질 수 있다. 명령은 또한, 로직이 변환 파라미터를 사용하여 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하게 할 수 있다. 명령은 또한, 로직이 제2 컴퓨팅 디바이스를 식별하는 필명을 획득하기 위해 및 제2 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 필명과 함께 사용될 세션 키를 획득하기 위해 1차원 속성 값을 사용하여 제1 암호문을 복호하게 할 수 있다. 몇몇 예들에서는, 명령은 또한, 로직이 복호의 품질을 판정하게 하고, 임계값을 초과하는 복호의 판정된 품질을 적어도 부분적으로 기초로 하여 데이터를 공유하도록 제2 컴퓨팅 디바이스와의 보안 세션을 개시하게 할 수 있다.

[0009] 이상의 요약은 예시적인 것일 뿐 어떠한 방식으로 제한하고자 하는 것은 아니다. 상술한 예시적인 양태, 실시예 및 특징에 덧붙여, 추가의 양태, 실시예 및 특징이 도면 및 아래의 상세한 설명을 참조하여 명백해질 것이다.

## 도면의 간단한 설명

[0010] 본 개시내용의 이상의 및 다른 특징들은 첨부하는 도면과 관련하여 취해진 이하의 설명 및 첨부하는 청구항들로부터 더욱 완전하게 명백해질 것이다. 이들 도면은 개시내용에 따라서 여러 가지 실시예들만 도시하며, 그에 따라 그 범위를 제한하는 것으로 간주되지 않음을 이해하면, 개시내용은 첨부하는 도면의 사용을 통해 부가적인 특이성 및 세부사항과 함께 기재된다.

도 1은 컴퓨팅 디바이스 간에 데이터를 공유하는 시스템의 일례를 예시하는 도면;

도 2는 암호 관리자의 아키텍처(architecture)의 일례를 예시하는 블록도;

도 3은 복호 관리자의 아키텍처의 일례를 예시하는 블록도;

도 4는 다차원 속성 값의 예를 예시하는 도면;

도 5는 결함 감내 암호 스킴(fault-tolerant encryption scheme)의 일례를 예시하는 도면;

도 6은 암호문을 암호화하여 암호문을 서버에 전송하는 방법의 예를 예시하는 플로우차트;

도 7은 결함 감내 복호 스킴의 일례를 예시하는 도면;

도 8은 암호문을 복호하고 보안 세션을 개시하는 방법의 예를 예시하는 플로우차트;

도 9는 컴퓨터 프로그램 제품의 일례를 예시하는 블록도;

도 10은 컴퓨팅 디바이스의 일례를 예시하는 도면;

모두 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된다.

## *발명을 실시하기 위한 구체적인 내용*

[0011] 이하의 상세한 설명에서는, 그 일부를 형성하는 첨부하는 도면에 대한 참조가 이루어진다. 도면에서는, 유사한 기호는 일반적으로 상황정보가 그렇지 않음을 지시하지 않으면, 유사한 구성요소를 식별한다. 상세한 설명, 도면 및 청구항들에 기재된 예시적인 예들 또는 실시예들은 제한되는 것을 의미하는 것은 아니다. 다른 예들 또는 실시예들이 이용될 수 있고, 여기에 제시된 주제의 사상 또는 범위를 벗어남 없이 다른 변경이 이루어질 수 있다. 본 명세서에 전체적으로 기재되고 도면에서 예시되는 바와 같이, 본 개시내용의 양태들이 배열, 치환, 결합 및 설계될 수 있고, 그들 모두는 명확하게 예상되고 본 개시내용의 일부를 생성한다.

[0012] 본 개시내용은 그 중에서도, 컴퓨팅 디바이스 간에 데이터를 안전하게 공유하기 위해 테이스트 기반 인증을 위한 방법, 장치, 시스템 및 프로그램 제품으로 정해진다.

[0013] 본 개시내용에서 고안되는 바와 같이, 컴퓨팅 디바이스 사용자가 관심 지역에 대한 유사한 기호 또는 테이스트에 기초하여 다른 컴퓨팅 디바이스 사용자와 데이터를 사적으로 및/또는 안전하게 공유하기를 원할 수도 있다. 또한, 이들 사용자는 원하지 않는 광고주, 스패머 또는 악의적인 액터와 같은 다른 엔티티가 또한 데이터를 공유할 수 있게 함 없이 관심 지역에서 유사한 테이스트를 갖는 다른 사용자를 찾기를 원할 수도 있다. 그 결과, 원하지 않는 광고주, 스패머 또는 악의적인 액터를 제외하면서 유사한 기호 또는 테이스트를 갖는 사용자를 찾은 후 그 사용자와 데이터를 안전하게 공유하는 것이 문제가 될 수도 있다.

[0014] 몇몇 예들에서는, 관심 지역에 관련하여 제1 테이스트를 갖는 제1 사용자와 관련된 제1 컴퓨팅 디바이스를 적어도 일시적으로 식별하기 위해 제1 필명(pseudonym)을 생성하는 방법이 구현된다. 제1 테이스트는 다차원 속성 값을 가지거나 다차원 속성 값에 의해 표현될 수도 있다. 제1 세션 키가 그 후, 제1 컴퓨팅 디바이스 상에 유지되는 데이터를 하나 이상의 다른 컴퓨팅 디바이스와 안전하게 공유하기 위해 필명으로 사용되도록 생성될 수도 있다. 변환 파라미터가 또한 생성된 후 제1 테이스트에 대한 다차원 속성 값을 1차원 속성 값으로 변환하기 위해 사용될 수도 있다. 필명 및 세션 키는 그 후, 제1 암호문을 생성하기 위해 1차원 속성 값을 사용하여 암호화될 수도 있다. 몇몇 예들에서는, 제1 암호문과 변환 파라미터가 제1 컴퓨팅 디바이스와 하나 이상의 다른 컴퓨팅 디바이스의 양자 모두에 액세스 가능한 서버에 전송될 수도 있다. 이들 예에 있어서는, 서버는 제1 암호문 및 변환 파라미터를 유지할 수도 있다. 하나 이상의 다른 컴퓨팅 디바이스는 그 후, 제1 암호문과 변환 파라미터의 양자 모두를 수신할 수도 있다. 하나 이상의 다른 컴퓨팅 디바이스는 그 후, 제1 암호문을 복호하고, 변환 파라미터를 사용하여 제1 암호문의 복호의 품질을 판정할 수도 있다. 적어도 부분적으로 제1 암호문의 복호의 판정된 품질에 기초하여, 하나 이상의 다른 컴퓨팅 디바이스는 데이터를 안전하게 공유하도록 제1 컴퓨팅 디바이스와 보안 세션을 개시할 수도 있다.

[0015] 도 1은 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된 컴퓨팅 장치들 간에 데이터를 공유하는 시스템(100)의 일례를 예시한다. 도 1에 도시된 바와 같이, 시스템(100)은 컴퓨팅 디바이스(110-1 내지 110-4), 베뉴(venue) 서버(120) 및 웹 서비스(130)를 포함한다. 몇몇 예들에서는, 도 1에 도시된 바와 같이, 통신 채널(140-1 내지 140-4)이 컴퓨팅 디바이스(110-1 내지 110-4)를 각각 베뉴 서비스(120)에 통신 가능하게 결합할 수도 있다. 도 1에는 4개의 컴퓨팅 디바이스가 도시되어 있지만, 본 개시내용은 4개의 컴퓨팅 디바이스로 제한되는 것이 아니라 베뉴 서버(120)에 통신 가능하게 결합되는 임의의 수의 컴퓨팅 디바이스를 포함할 수도 있다. 또한, 도 1에 도시된 바와 같이, 통신 채널(150)이 베뉴 서버(120)를 웹 서비스(130)에 통신 가능하게 결합할 수도 있다.

[0016] 몇몇 예들에 따르면, 도 1에 도시된 바와 같이, 컴퓨팅 디바이스(110-1 내지 110-4)는 암호 관리자(112) 및 복호 관리자(114)를 별개로 포함할 수도 있다. 이하 더욱 상세히 기술되는 바와 같이, 암호 관리자(112) 및 복호 관리자(114)는 적어도 부분적으로 테이스트 기반 인증에 기초하여 데이터를 안전하게 공유하도록 구성되는 로직(logic) 및/또는 특징부(feature)들을 포함할 수도 있다. 테이스트 기반 인증은 컴퓨팅 디바이스(예컨대, 컴퓨팅 디바이스(110-1))의 정해진 사용자에 대한 관심 지역에 관한 테이스트를 통합할 수도 있다. 또한, 도 1에 도시된 바와 같이, 컴퓨팅 디바이스의 적어도 일부는 애플리케이션(116)을 별개로 포함한다. 몇몇 예들에서는, 애플리케이션(116)은 컴퓨팅 디바이스의 정해진 사용자에 대한 테이스트를 생성하도록 구성되는 로직 및/또는

특징부들을 포함할 수도 있다.

[0017] 몇몇 예들에서는, 도 1에 도시된 바와 같이, 베뉴 서버(120)가 사용자 정보(122) 및 보안 정보(124)를 포함할 수도 있다. 사용자 정보(122)는 베뉴 서버(120)에 의해 유지되는 베뉴 특정(venue-specific) 사용자 정보를 포함할 수도 있다. 예를 들면, 베뉴는 상거래 사이트(물리적 또는 가상의)일 수 있으며, 이를 통해 컴퓨팅 장치의 사용자가 아이템(예컨대, 도서, 영화, 앨범, 음악, 의류, 음료 등)을 구매할 수 있도록 방문할 수 있다. 베뉴 특정 사용자 정보는 컴퓨팅 디바이스의 사용자가 베뉴를 방문하는 동안 수집되는 정보(예컨대, 구매 이력, 검색 이력, 사용자 인구 통계학적 특성(user demographic characteristics) 등)을 포함할 수 있고, 사용자의 관심 지역에 관한 테이스트를 생성 또는 판정하는 데 사용될 수도 있다. 보안 정보(124)는 더욱 이후에 기술되는 바와 같이, 베뉴 서버(120)에 또는 베뉴 서버(120)와 유지되는 정보를 포함할 수 있고, 컴퓨팅 디바이스(110-1 내지 110-4)가 데이터를 안전하게 공유할 수 있게 하는 데 사용될 수도 있다.

[0018] 몇몇 예들에 따르면, 도 1에 도시된 바와 같이, 웹 서비스(130)는 사용자 정보(132)를 포함할 수도 있다. 사용자 정보(132)는 컴퓨팅 디바이스의 사용자와 관련된 사용자 특정 정보를 포함할 수도 있다. 사용자 정보(132)에 포함되는 사용자 특정 정보는 증가하거나, 베뉴 서버(120)에 의해 유지되는 사용자 정보(122)에 포함되는 베뉴 특정 정보 대신에 사용될 수도 있다. 예를 들면, 정해진 컴퓨팅 디바이스의 사용자에 대한 사용자 특정 정보가 사용자 정보(132)에 포함될 수도 있다. 정해진 컴퓨팅 디바이스의 사용자는 베뉴 서버(120)와 관련된 베뉴에 의한 선매나 검색 이력이 부족할 수도 있다. 베뉴 서버(120)는 사용자 정보(122) 내에 유지되는 임의의 베뉴 특정 사용자 정보를 증가시키도록 웹 서비스(130)로부터 사용자에 대한 사용자 특정 정보를 획득하거나 수신하도록 구성될 수도 있다.

[0019] 몇몇 예들에 따르면, 컴퓨팅 디바이스(110-1)의 사용자는 컴퓨팅 디바이스(110-1)가 베뉴 서버(120)와 관련된 베뉴에 물리적으로나 가상적으로 들어가게 할 수도 있다. 예를 들면, 베뉴는 서점일 수도 있고, 컴퓨팅 디바이스(110-1)가 통신 채널(140-1)을 통해 베뉴 서버(120)와 통신 가능하게 결합하면, 컴퓨팅 디바이스(110-1)가 서점에 들어가는 것으로 간주될 수도 있다. 이하 더욱 상세히 기술되는 바와 같이, 암호 관리자(112), 복호 관리자(114) 또는 애플리케이션(116)은 베뉴 서버(120)와 또한 통신 가능하게 결합되는 다른 컴퓨팅 디바이스(예컨대, 컴퓨팅 디바이스(110-4))와 컴퓨팅 디바이스(110-1)에 또는 컴퓨팅 디바이스(110-1)에 의해 유지되는 데이터를 안전하게 공유하도록 구성될 수도 있다. 또한, 이하 더욱 상세히 기술되는 바와 같이, 컴퓨팅 디바이스(110-1)의 사용자는 특정 장르의 서적과 같은 관심 지역에 관련된 테이스트를 가질 수도 있다. 이들 테이스트는 관심 지역의 유사한 테이스트를 갖는 다른 컴퓨팅 디바이스의 사용자와 데이터를 선택적으로 및 안전하게 공유하도록 사용될 수도 있다.

[0020] 몇몇 예들에 따르면, 통신 채널(140-1 내지 140-4) 또는 통신 채널(150)은 컴퓨팅 디바이스(110-1 내지 110-4), 베뉴 서버(120) 또는 웹 서비스(130)가 통신 가능하게 결합할 수 있게 하는 하나 이상의 유선 또는 무선 표준에 따라 동작할 수도 있다. 이들 유선 또는 무선 표준은 IEEE 802.1, IEEE 802.11, IEEE 802.16, GSM, GPRS, EDGE, W-CDMA, HSPA, CDMA-2000, EV-DO, LTE 또는 TD-LTE와 관련된 것들과 같은 하나 또는 하나 이상의 산업 표준에서 기술될 수 있으며, 본 개시내용은 상술한 유선 또는 무선 표준에만 제한되는 것은 아니다.

[0021] 도 1에 도시되지는 않지만, 컴퓨팅 디바이스(110-1 내지 110-4)는 또한 서로 간에 직접 또는 베뉴 서버(120)를 통해 별개의 통신 채널들을 설정한다. 몇몇 예들에서는, 별개의 통신 채널들이 유사한 관심 지역에 관련된 데이터를 안전하게 공유하기 위해 보안 세션을 셋업 또는 설정할 때 설정될 수도 있다. 이들 별개의 통신 채널들은 상술한 유선 또는 무선 표준에 따라서 동작할 수도 있다.

[0022] 도 2는 본 개시내용의 적어도 몇몇 실시예에 따라서 배열되는 암호 관리자(112)에 대한 아키텍처의 일례의 블록도를 예시한다. 도 1에서 시스템(100)에 대해 상술한 바와 같이, 컴퓨팅 디바이스(110-1 내지 110-4)는 암호 관리자(112)를 포함할 수도 있다. 몇몇 예들에서는, 암호 관리자(112)는 컴퓨팅 디바이스가 베뉴 서버(120)에 통신 가능하게 결합할 수 있게 하고, 베뉴 서버(120)에 또한 통신 가능하게 결합되는 다른 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 구성되거나 배열되는 특징부 및/또는 로직을 포함한다.

[0023] 도 2의 암호 관리자(112)의 예는 암호 로직(210), 제어 로직(220), 메모리(230), 입/출력(I/O) 인터페이스(240) 및 선택적으로 하나 이상의 애플리케이션(250)을 포함한다. 도 2에 예시되는 바와 같이, 암호 로직(210)은 제어 로직(220), 메모리(230) 및 I/O 인터페이스(240)에 결합될 수도 있다. 또한, 도 2에 예시되는 바와 같이, 선택적인 애플리케이션(250)이 제어 로직(220)과 통신하여 배열될 수도 있다. 암호 로직(210)은 테이스트 특징부(211), 생성 특징부(213), 변환 특징부(215), 암호 특징부(217), 또는 전송 특징부(219) 중 하나 이상, 또는 이들의 임의의 적정 조합을 더 포함할 수도 있다.

[0024] 몇몇 예들에서는, 도 2의 블록도에 나타내는 소자들은 이 개시내용에 기술되는 바와 같이 암호 관리자(112)를 지원하거나 인에이블(enable)시키도록 구성된다. 정해진 암호 관리자(112)는 도 2에 도시된 소자의 일부, 전부 또는 그보다 더 많은 소자를 포함할 수도 있다. 예를 들면, 암호 로직(210) 및 제어 로직(220)은 암호 관리자(112)의 특징을 구현하기 위해 매우 다양한 로직 디바이스(들)을 개별적으로 또는 집합적으로 나타낼 수도 있다. 로직 디바이스의 일례는 컴퓨터, 마이크로프로세서, 마이크로컨트롤러, 필드 프로그램 가능한 게이트 어레이(FPGA), 애플리케이션 특정 집적 회로(ASIC: Application specific integrated circuit), 멀티 코어/멀티 쓰레드(multi-core/multi-threaded) 마이크로프로세서의 격리된 쓰레드 또는 코어 중 하나 이상, 또는 이들의 조합을 포함할 수도 있다.

[0025] 몇몇 예들에서는, 도 2에 도시된 바와 같이, 암호 로직(210)이 테이스트 특징부(211), 생성 특징부(213), 변환 특징부(215), 암호 특징부(217), 또는 전송 특징부(219)를 포함한다. 암호 로직(210)은 이들 특징부의 하나 이상을 사용하여 동작을 실행하도록 구성될 수도 있다. 이하 더욱 상세히 기술되는 바와 같이, 동작의 예들은 암호문을 생성하기 위해 관심 지역에 관련된 컴퓨팅 디바이스 사용자의 테이스트(들)를 사용하는 것을 포함할 수도 있다. 동작들은 서버에 액세스 가능하게 될 수도 있는 다른 컴퓨팅 디바이스와 데이터를 안전하게 공유하기 위해 컴퓨팅 디바이스에 액세스 가능한 서버(예컨대, 베뉴 서버(120))에 암호문을 전송하는 것을 또한 포함할 수도 있다.

[0026] 몇몇 실시예들에서는, 제어 로직(220)은 암호 관리자(112)의 전체 동작을 제어하도록 구성될 수도 있다. 상술한 바와 같이, 제어 로직(220)은 암호 관리자(112)의 제어를 구현하기 위해 실행 가능한 컨텐츠 또는 명령과 관련하여 동작하도록 구성되는 매우 다양한 로직 디바이스(들) 중 어느 하나를 나타낼 수도 있다. 몇몇 대체 예들에서는, 제어 로직(220)의 특징 및 기능성이 암호 로직(210)에 의해 구현될 수도 있다.

[0027] 몇몇 예들에 따르면, 메모리(230)가 실행 가능한 컨텐츠 또는 명령을 저장하도록 배열된다. 실행 가능한 컨텐츠 또는 명령은 암호 관리자(112)의 특징부 또는 소자를 구현 또는 활성화시키기 위해 제어 로직(220) 및/또는 암호 로직(210)에 의해 사용될 수도 있다. 이하 더욱 상세히 기술되는 바와 같이, 메모리(230)는 또한, 관심 지역에 관련된 컴퓨팅 디바이스의 사용자의 테이스트를 사용하여 암호문을 생성하는 것과 관련된 정보를 일시적으로 유지하도록 배열될 수도 있다.

[0028] 메모리(230)는 휘발성 메모리, 비휘발성 메모리, 플래시 메모리, 프로그램 가능한 변수 또는 상태, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 또는 다른 정적 또는 동적 저장 매체에 제한되지는 않지만, 이들을 포함하는 매우 다양한 메모리 매체를 포함할 수도 있다.

[0029] 몇몇 예들에서는, I/O 인터페이스(240)는 도 1에 도시된 컴퓨팅 디바이스(110-1 내지 110-4)와 같은 컴퓨팅 디바이스 상에 상주하거나 컴퓨팅 디바이스와 함께 위치하는 소자들과 암호 관리자(112) 사이의 로컬 유선 및/또는 무선 통신 매체 또는 링크를 통해 인터페이스를 제공할 수도 있다. I/O 인터페이스(240)는 유선 또는 무선 통신 매체 또는 링크(예컨대, I2C, SMBus, SPI, PCI-Express, USB 등) 상으로 통신하도록 여러 가지 통신 프로토콜에 따라서 동작하는 인터페이스를 포함할 수도 있다. I/O 인터페이스(240)는 또한, 컴퓨팅 디바이스에 원격으로 위치하는 소자들과 암호 관리자(112) 사이의 인터페이스를 제공할 수도 있다. 예를 들면, 도 1에 대해 상술한 바와 같이, 암호 관리자(112)를 갖는 컴퓨팅 디바이스(110-1)는 통신 채널(140-1)을 통해 베뉴 서버(120)에 통신 가능하게 결합할 수도 있다. 또한, 암호 관리자(112)를 갖는 컴퓨팅 디바이스(110-1)는 베뉴 서버(120)를 통해서 및 통신 채널(140-2 내지 140-4)을 통해 또는 별개로 설정된 통신 채널을 통해서 컴퓨팅 디바이스(110-2 내지 110-4)에 통신 가능하게 결합할 수도 있다. I/O 인터페이스(240)는 예를 들면, 암호 관리자(112)가 이들 통신 채널을 통해 통신할 수 있게 하기 위해 여러 가지 유선 또는 무선 통신 프로토콜에 따라서 동작하도록 구성되는 인터페이스를 포함한다. 이들 유선 또는 무선 통신 프로토콜은 IEEE 802.1, IEEE 802.11, IEEE 802.16, GSM, GPRS, EDGE, W-CDMA, HSPA, CDMA-2000, EV-DO, LTE, TD-LTE에 제한되는 것은 아니지만, 이들을 포함할 수도 있다.

[0030] 몇몇 예들에서는, 암호 관리자(112)는 제어 로직(220) 및/또는 암호 로직(210)에 명령을 제공하도록 하나 이상의 애플리케이션(250)을 포함한다. 이들 명령은 예를 들면, 테이스트 특징부(211), 생성 특징부(213), 변환 특징부(215), 암호 특징부(217), 또는 전송 특징부(219) 중 하나 이상을 구현하거나 사용하기 위한 암호 관리자(112)용의 명령을 포함할 수도 있다.

[0031] 도 3은 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열되는 복호 관리자(114)에 대한 아키텍처의 일례의 블록도를 예시한다. 도 1에서 시스템(100)에 대해 상술한 바와 같이, 컴퓨팅 디바이스(110-1 내지 110-4)는 암호 관리자(112)를 포함할 수도 있다. 몇몇 예들에서는, 복호 관리자(114)는 컴퓨팅 디바이스가 베뉴 서버(120)에

통신 가능하게 결합하여, 데이터를 안전하게 공유하도록 베뉴 서버(120)에 통신 가능하게 결합된 다른 컴퓨팅 디바이스와의 보안 세션을 개시하는 것을 가능하게 하기 위해 구성되거나 배열되는 특징부 및/또는 로직을 포함한다.

[0032] 도 3의 복호 관리자(114)의 예는 복호 로직(310), 제어 로직(320), 메모리(330), 입/출력(I/O) 인터페이스(340) 및 선택적으로 하나 이상의 애플리케이션(350)을 포함한다. 도 3에 예시된 바와 같이, 복호 로직(310)은 제어 로직(320), 메모리(330) 및 I/O 인터페이스(340)에 결합될 수도 있다. 또한, 도 3에 예시된 바와 같이, 선택적인 애플리케이션(350)은 제어 로직(320)과 협력하여 배열될 수도 있다. 복호 로직(310)은 수신 특징부(311), 테이스트 특징부(313), 변환 특징부(315), 복호 특징부(317), 또는 개시 특징부(319)의 하나 이상 또는 이들의 임의의 적정 조합을 더 포함할 수도 있다.

[0033] 몇몇 예들에서는, 도 3의 블록도에 나타내는 소자들은 이 개시내용에 기술되는 바와 같이 복호 관리자(114)를 지원하거나 인에이블시키도록 구성된다. 정해진 복호 관리자(114)는 도 3에 도시된 소자의 일부, 전부 또는 그보다 더 많은 소자를 포함할 수도 있다. 예를 들면, 복호 로직(310) 및 제어 로직(320)은 복호 관리자(114)의 특징부를 구현하기 위해 매우 다양한 로직 디바이스(들)을 개별적으로 또는 집합적으로 나타낼 수도 있다. 로직 디바이스의 일례는 컴퓨터, 마이크로프로세서, 마이크로컨트롤러, 필드 프로그램 가능한 게이트 어레이(FPGA), 애플리케이션 특정 집적 회로(ASIC), 멀티 코어/멀티 쓰레드 마이크로프로세서의 격리된 쓰레드 또는 코어 중 하나 이상, 또는 이들의 조합을 포함할 수도 있다.

[0034] 몇몇 예들에서는, 도 3에 도시된 바와 같이, 복호 로직(310)은 수신 특징부(311), 테이스트 특징부(313), 변환 특징부(315), 복호 특징부(317), 또는 개시 특징부(319)를 포함한다. 복호 로직(310)은 이들 특징부의 하나 이상을 사용하여 동작을 실행하도록 구성될 수도 있다. 이하 더욱 상세히 기술되는 바와 같이, 동작들의 예는 서버(예컨대, 베뉴 서버(120))로부터 수신되는 암호문을 복호하는 것 및 복호된 암호문의 판정된 품질에 기초하여 컴퓨팅 디바이스들 간에 데이터를 공유하기 위해 보안 세션을 개시하는 것을 포함할 수도 있다.

[0035] 몇몇 예들에서는, 제어 로직(320)이 복호 관리자(114)의 전체 동작을 제어하도록 구성될 수도 있다. 상술한 바와 같이, 제어 로직(320)은 복호 관리자(1140의 제어를 구현하기 위해 실행 가능한 컨텐츠 또는 명령과 관련하여 동작하도록 구성되는 매우 다양한 로직 디바이스(들) 중 어느 하나를 나타낼 수도 있다. 몇몇 대체 예들에서는, 제어 로직(320)의 특징부 및 기능성이 복호 로직(310) 내에서 구현될 수도 있다.

[0036] 몇몇 예들에 따르면, 메모리(330)가 실행 가능한 컨텐츠 또는 명령을 저장하도록 배열된다. 실행 가능한 컨텐츠 또는 명령은 복호 관리자(114)의 특징부 또는 소자를 구현 또는 활성화시키기 위해 제어 로직(320) 및/또는 복호 로직(310)에 의해 사용될 수도 있다. 이하 더욱 상세히 기술되는 바와 같이, 메모리(330)는 또한, 컴퓨팅 디바이스들 간에 데이터를 공유하도록 보안 세션을 개시하기 위하여 암호문을 복호하는 것과 관련된 정보를 일시적으로 유지하도록 배열될 수도 있다. 이 정보는 예를 들면, 복호 관리자(114)를 포함하는 컴퓨팅 디바이스의 사용자에 대한 관심 지역에 관한 사용자 테이스트 정보를 포함할 수도 있다.

[0037] 메모리(330)는 휘발성 메모리, 비휘발성 메모리, 플래시 메모리, 프로그램 가능한 변수 또는 상태, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 또는 다른 정적 또는 동적 저장 매체에 제한되지는 않지만, 이들을 포함하는 매우 다양한 메모리 매체를 포함할 수도 있다.

[0038] 몇몇 예들에서는, I/O 인터페이스(340)는 도 1에 도시된 컴퓨팅 디바이스(110-1 내지 110-4)와 같은 컴퓨팅 디바이스 상에 상주하거나 컴퓨팅 디바이스와 함께 위치하는 소자들과 복호 관리자(114) 사이의 로컬 유선 및/또는 무선 통신 매체 또는 링크를 통해 인터페이스를 제공할 수도 있다. I/O 인터페이스(340)는 유선 또는 무선 통신 매체 또는 링크(예컨대, I2C, SMBus, SPI, PCI-Express, USB 등) 상으로 통신하도록 여러 가지 통신 프로토콜에 따라서 동작하는 인터페이스를 포함할 수도 있다. I/O 인터페이스(340)는 또한, 컴퓨팅 디바이스에 원격으로 위치하는 소자들과 복호 관리자(114) 사이의 인터페이스를 제공할 수도 있다. 예를 들면, 도 1에 대해 상술한 바와 같이, 복호 관리자(114)를 갖는 컴퓨팅 디바이스(110-1)는 통신 채널(140-1)을 통해 베뉴 서버(120)에 통신 가능하게 결합할 수도 있다. 또한, 복호 관리자(114)를 갖는 컴퓨팅 디바이스(110-1)는 베뉴 서버(120)를 통해서 및 통신 채널(140-2 내지 140-4)을 통해 또는 별개로 설정된 통신 채널을 통해서 컴퓨팅 디바이스(110-2 내지 110-4)에 통신 가능하게 결합할 수도 있다. I/O 인터페이스(340)는 예를 들면, 복호 관리자(114)가 이들 통신 채널을 통해 통신할 수 있게 하기 위해 여러 가지 유선 또는 무선 통신 프로토콜에 따라서 동작하도록 구성되는 인터페이스를 포함한다. 이들 유선 또는 무선 통신 프로토콜은 IEEE 802.1, IEEE 802.11, IEEE 802.16, GSM, GPRS, EDGE, W-CDMA, HSPA, CDMA-2000, EV-DO, LTE, TD-LTE에 제한되는 것은 아니지만, 이들을 포함할 수도 있다.

[0039] 몇몇 예들에서는, 복호 관리자(114)는 제어 로직(320) 및/또는 복호 로직(310)에 명령을 제공하도록 하나 이상의 애플리케이션(350)을 포함한다. 이들 명령은 예를 들면, 수신 특징부(311), 테이스트 특징부(313), 변환 특징부(315), 복호 특징부(317), 또는 개시 특징부(319) 중 하나 이상을 구현하거나 사용하기 위한 복호 관리자(114)용의 명령을 포함할 수도 있다.

[0040] 도 4는 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된 다차원 속성 값들의 예를 예시하는 도면이다. 도 4에 도시되는 바와 같이, 다차원 속성 값들이 맵(400) 상에 다차원 속성 값(405, 415 및 425)으로서 도시되어 있다. 몇몇 예들에 따르면, 이들 3개의 다차원 속성 값은 각각 컴퓨팅 플랫폼의 사용자에 대한 개별 테이스트를 특징으로 할 수 있다. 개별 테이스트는 예를 들면, 베뉴에서 사용자에 의해 구매되는 서적에 대한 것일 수도 있다. 이들 예에서, 도 4에 도시된 바와 같이, 다차원 속성 값(405, 415 및 425)을 특징으로 하는 개별 테이스트는 2개의 값을 포함할 수도 있다. 제1의 값은 정해진 구매 서적의 평균 구독률을 기초로 할 수 있고, 제2의 값은 정해진 구매 서적의 장르를 기초로 할 수도 있다. 또한, 도 4에 도시된 바와 같이, 평균 구독률을 기초로 하는 제1의 값은 축(410) 또는 (x)와 관련될 수 있고, 장르를 기초로 하는 제2의 값은 축(420) 또는 (y)와 관련될 수도 있다. 도 4에 도시된 바와 같이, 몇몇 예들에서는, 축(410) 및 축(420)은 서로 직교할 수도 있다. 도 4에 도시되지는 않았지만, 부가적인 속성이 양 축(410) 및 축(420)에 또한 직교할 수 있는 다른 축(예컨대, (z) 축) 상에 표시될 수도 있다.

[0041] 몇몇 예들에서는, 평균 구독률을 기초로 하는 제1의 값이 축(410) 상의 전체 숫자들의 표시를 허용하도록 크기 변경될 수도 있다. 다차원 속성(415)에 대해 구매된 서적은 예를 들면, 1 대 5의 비율에 기초하여 평균 구독률을 가질 수도 있다. 이 예에서는, 다차원 속성(415)에 대해 구매된 서적은 3.9의 평균 구독률을 가질 수 있다. 3.9의 평균 구독률은 39의 값으로 크기 변경될 수도 있다. 또한, 장르를 기초로 하는 제2의 값은 구매된 서적에 대한 장르에 할당한 수치를 기초로 할 수도 있다. 예를 들면, 모험 장르는 1의 할당 값을 가질 수도 있고, 코믹, 판타지, 역사, 미스터리 및 로맨스의 장르는 각각 2, 3, 4, 5 및 6의 할당 값을 가질 수도 있다. 이 예에서는, 다차원 속성(415)에 대해 구매된 서적은 코믹 장르일 수도 있다. 따라서, 다차원 속성(415)은 2차원 값을 가질 수도 있으며, 이는 도 4에 도시되는 바와 같이 맵(400) 상에 좌표 (39,2로 표시되거나 매핑될 수 있다. 또한, 다차원 속성(405 및 425)에 대해 구매된 서적은 각각 판타지(3의 할당 값) 및 모험(1의 할당 값)의 장르를 가질 수 있다. 이들 구매된 서적은 또한, 10 및 40으로 크기 변경된 1 및 4의 평균 구독률을 가질 수도 있고, 도 4에 도시된 바와 같이 표시되거나 매핑될 수 있다.

[0042] 도 5는 본 개시내용의 적어도 몇몇 실시예에 따라서 배열된 결함 감내 암호(FTE) 스킴(500)의 일례를 예시한다. 몇몇 예들에서는, 도 1에 도시된 바와 같이 또는 도 2에 기술되는 바와 같이 컴퓨팅 디바이스와 함께 위치하는 암호 관리자(112)는 FTE 스킴(500)의 적어도 부분들을 구현하기 위해 로직 및/또는 특징부를 포함할 수도 있다. 그렇지만, FTE 스킴(500)은 암호 관리자(112)의 로직 및/또는 특징부에 의한 구현에 한정되는 것은 아니다. 컴퓨팅 디바이스 상에 상주하거나 그에 포함되는 다른 로직 및/또는 특징부가 또한, FTE 스킴(500)의 적어도 일부를 구현할 수도 있다.

[0043] 단계 5.1의 예(테이스트(T)를 제공하고; 변환 파라미터(P)를 제공)에서 시작하며, 테이스트 특징부(211)가 컴퓨팅 플랫폼(예컨대, 컴퓨팅 플랫폼(110-1))의 사용자에 대한 관심 지역에 관한 테이스트(T)를 제공할 수도 있고, 생성 특징부(213)는 변환 파라미터(P)를 제공할 수도 있다. 몇몇 예들에서는, T 및 P가 각각 변환 특징부(215)에 제공될 수도 있다. T에 관련된 관심 지역은 예를 들면, 컴퓨팅 플랫폼의 사용자에 의해 구매되는 구매된 서적일 수도 있다. 몇몇 예들에서는, T는 도 4에 도시되는 다차원 속성 값(예컨대, (39,2))과 유사한 다차원 속성 값일 수도 있다. 또한, 이들 예에서는, P는 생성 특징부(213)에 의해 갓 생성되어, 그 후 변환 특징부(214)에 제공되었을 수도 있다.

[0044] 단계 5.2의 예(변환된 테이스트(T')를 제공)로 이동하며, 변환 특징부(215)는 변환된 테이스트(T')를 암호 특징부(217)에 제공할 수도 있다. 몇몇 예들에 따르면, 변환 특징부(215)는 T의 다차원 속성 값을 미리 정의된 유한 필드(F)에 걸쳐 T'의 1차원 속성 값으로 변환시킬 수도 있다. 바꿔 말하면, T는 P에 의해 정의되는 비가역 변환을 사용하여 1차원 이산 집합 T' ? F로 변환될 수도 있다. 이러한 T'로의 변환의 결과는 그 후 1차원 데이터로 매핑될 수도 있다.

[0045] 단계 5.3의 예(평문(X)으로서 필명 및 세션 키를 제공)로 이어지며, 생성 특징부(213)는 평문(X)을 암호 특징부(217)에 제공할 수도 있다. 몇몇 예들에서는, 생성 특징부(213)는 컴퓨팅 플랫폼(예컨대, 컴퓨팅 플랫폼(110-1))에 대한 고유 식별자로서의 역할을 하도록 필명을 생성할 수도 있다. 이들 예에 있어서, 필명은 랜덤하게 생성될 수도 있다. 또한, 생성 특징부(213)는 세션 키를 또한 생성할 수도 있다. 세션 키는 또한 랜덤하게 생

성될 수도 있다. 생성 특징부(213)는 필명 및 세션 키를 결합 또는 연관시켜 X를 형성할 수도 있다.

[0046] 단계 5.4의 예(암호문(Y)을 제공)로 이동하며, 암호 특징부(217)는 암호문(Y)을 전송 특징부(219)에 제공할 수도 있다. 몇몇 예들에서는, 암호 특징부(217)는 F 상에서 아래의 파라미터: k, r(k? r)을 기초로 하여 Y를 생성하여 제공하도록 구성될 수도 있다. 이들 예에 있어서, X는 k 섹션으로 분할되어, 각 섹션이 F 내의 소자를 나타내도록 할 수도 있으며, 여기에서 F는 유한 필드를 나타낸다. 차수 k-1을 갖는 F 상에서의 다항식(f)이 정의될 수도 있고, f가 이들 k 값에 의해 정의되는 계수를 가질 수도 있다. 암호 특징부(217)는 또한, 집합 (S)={(x, f(x)): x는 T' 내에 있음}를 획득하기 위하여 f를 사용하여 T' 내의 각 소자를 평가하도록 구성될 수도 있다. 또한, 이들 예에 있어서, 암호 특징부(217)는 r-|T'| 소자를 갖는 노이즈 집합 (N)={(x,y): x는 T' 내에 있지 않음, y!=f(x)}를 생성하도록 구성될 수도 있다. 암호 특징부(217)는 그 후, Y로서 (S ?N)을 작성 또는 생성한 후 Y를 전송 특징부(219)에 제공할 수도 있다. 몇몇 예들에 따르면, 전송 특징부(219)는 그 후 Y를 컴퓨팅 플랫폼에 통신 가능하게 결합된 서버(예컨대, 베뉴 서버(120))에 전송할 수도 있다.

[0047] 도 6은 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된, 암호문을 암호화하여 암호문을 서버에 전송하는 방법의 예의 플로우차트를 예시한다. 몇몇 예들에서는, 시스템(100)의 소자들이 도 6에 도시된 플로우차트와 관련된 방법의 예를 예시하는 데 사용될 수도 있다. 도 2에 도시된 바와 같은 암호 관리자(112)가 또한, 방법들의 예를 예시하는 데 사용될 수도 있다. 그렇지만, 기술된 방법들은 시스템(100) 상에서의 구현 또는 도 2에 도시된 암호 관리자(112)에 제한되는 것은 아니다. 방법들의 예는 도 1 또는 도 2에 도시된 소자들 중의 하나 이상을 갖는 다른 시스템 상에서 구현될 수도 있다.

[0048] 시작에서 블록 605(베뉴에 들어감)로 이동하며, 컴퓨팅 디바이스(110-1)와 같은 컴퓨팅 디바이스가 베뉴에 들어갈 수도 있다. 몇몇 예들에서는, 컴퓨팅 디바이스(110-1)는 베뉴에 들어갈 때 통신 채널(140-1)을 통해 베뉴 서버(120)와 통신 가능하게 결합할 수도 있다.

[0049] 블록 605에서 블록 610(테이스트를 수신)으로 진행하며, 컴퓨팅 디바이스(110-1)와 함께 위치하는 암호 관리자(112)가 (예컨대, 테이스트 특징부(211)를 통해) 관심 영역에 관련된 테이스트를 수신하거나 획득하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 테이스트는 컴퓨팅 디바이스(110-1)의 사용자의 관심 지역에 관련될 수도 있다. 또한, 테이스트는 도 4에 대해 상술한 다차원 속성 값과 같은 다차원 속성 값으로 나타낼 수도 있다. 컴퓨팅 디바이스(110-1)의 사용자가 베뉴 서버(120)에 대해 필명을 유지하기를 원하는 경우, 테이스트에 대한 다차원 속성 값은 컴퓨팅 디바이스(110-1)에 또는 와 함께 상주하는 애플리케이션(116)으로부터 수신될 수도 있다. 그렇지 않은 경우, 테이스트에 대한 다차원 속성 값은 베뉴 서버(120)로부터 또는 베뉴 서버(120)를 통해서 수신될 수도 있다.

[0050] 블록 610에서 블록 615(제1 필명, 제1 세션 키 및 변환 파라미터를 생성)로 진행하며, 암호 관리자(112)는 컴퓨팅 디바이스(110-1)를 적어도 일시적으로 식별하기 위해 그리고 또한 제1 세션 키 및 변환 파라미터를 생성하기 위해 (예를 들면, 생성 특징부(213)를 통해) 제1 필명을 생성하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 이들 예에 있어서, 제1 세션 키는 베뉴 서버(120)와 통신 가능하게 결합되는 다른 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 제1 필명과 함께 사용될 수도 있다.

[0051] 블록 615에서 블록 620(테이스트를 변환)으로 진행하며, 암호 관리자(112)는 (예를 들면, 변환 특징부(215)를 통해) 수신된 테이스트에 대한 다차원 속성 값을 변환하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에 따르면, 다차원 속성 값은 FTE 스킴(500)에 대해 상술한 바와 같이 변환될 수도 있다. 이들 예에 있어서 다차원 속성 값은 생성된 변환 파라미터를 사용하여 1차원 속성 값으로 변환될 수도 있다.

[0052] 블록 620에서 블록 625(암호문을 생성)로 진행하며, 암호 관리자(112)는 (예를 들면, 암호 특징부(217)를 통해) 암호문을 생성하도록 구성된 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에 따르면, 암호문은 FTE 스킴(500)에 대해 상술한 바와 같이 생성될 수도 있다. 예를 들면, 변환된 다차원 속성 값이 암호문을 생성하는 데 사용될 수도 있다.

[0053] 블록 625에서 블록 630(암호문을 서버로 전송)으로 진행하며, 암호 관리자(112)는 생성된 암호문을 베뉴 서버(120)에 (예를 들면, 전송 특징부(219)를 통해) 전송하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 생성된 변환 파라미터가 또한 베뉴 서버(120)에 전송될 수도 있다. 이들 예에 있어서, 베뉴 서버(120)는 보안 정보(124)에 또는 보안 정보(124)와 함께 컴퓨팅 디바이스(110-1)용의 암호문 및 변환 파라미터를 유지하도록 로직 및/또는 특징부를 포함할 수도 있다. 컴퓨팅 디바이스(110-2 내지 110-4) 중에서 다른 컴퓨팅 디바이스가 베뉴 서버(120)로부터의 암호문 및 변환 파라미터에 액세스 가능하게 될 수도 있다.

[0054] 블록 630에서 판정 블록 635(암호문 복호 적절?)로 진행하며, 암호 관리자(112)는 데이터를 안전하게 공유하라는 요구가 (예를 들면, 암호 특징부(217)를 통해) 베뉴 서버(120)에 전송된 암호문이 적절히 복호되었는지의 여부를 나타내는지의 여부를 판정하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 이하 더욱 상세히 기술되는 바와 같이, 다른 컴퓨팅 디바이스가 베뉴 서버(120)를 통해 암호문 및 변환 파라미터에 액세스하고, 암호문을 복호하여 복호의 품질을 판정하고자 시도하기 위해 변환 파라미터를 사용할 수도 있다. 몇몇 예들에서는, 암호문이 적절히 복호된 경우에는, 다른 컴퓨팅 디바이스(예컨대, 컴퓨팅 디바이스(110-2))가 컴퓨팅 디바이스(110-1)에 의해 최초로 생성된 제1 필명 및 제1 세션 키와 실질적으로 유사할 수도 있는 제2 필명 및 제2 세션 키를 컴퓨팅 디바이스(110-1)에 중계할 수도 있다. 제2 필명 및 세션 키는 또한, 어떻게 유사한 그 사용자의 테이스트가 컴퓨팅 디바이스(110-1) 사용자의 테이스트의 것과 함께 일 수도 있는지의 다른 컴퓨터의 평가를 나타내기 위해 품질 값을 포함할 수도 있다. 암호문이 적절히 복호된 경우에는(예를 들면, 높은 품질 값을 갖고 및/또는 필명 및 세션 키가 정확한 경우에는), 프로세스는 블록 640으로 이동한다. 그렇지 않은 경우에는, 프로세스는 블록 64로 이동한다.

[0055] 판정 블록 635로부터 블록 640(데이터를 안전하게 공유)으로 이동하며, 암호 관리자(112)는 (예를 들면, 테이스트 특징부(211)를 통해) 다른 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 공유된 데이터가 컴퓨팅 디바이스(110-1)의 사용을 위한 관심 지역과 관련될 수도 있다. 예를 들면, 관심 지역은 사용자가 구매했던 서적, 영화, 음악 등의 타입일 수도 있다. 이들 예에 있어서, 데이터는 컴퓨팅 디바이스(110-1)에 유지되는 메모리에 저장될 수 있거나, 컴퓨팅 디바이스(110-1)를 통해서 액세스 가능한 메모리(예를 들면, 클라우드(cloud) 또는 네트워크된 메모리)에 저장될 수도 있다. 또한, 몇몇 예들에 있어서, 데이터는 2개의 컴퓨팅 디바이스 사이에 별개로 설정된 통신 채널을 통해 안전하게 공유될 수도 있다. 이와 달리, 데이터는 이미 설정된 통신 채널(예컨대, 통신 채널(140-1 내지 140-4))을 통해 베뉴 서버(120)를 통해서 안전하게 공유될 수도 있다.

[0056] 블록 635에서 블록 645(데이터를 공유하지 않음)로 이동하며, 암호 관리자(112)는 부정확한 필명 또는 세션 키로 인해 (예를 들면, 테이스트 특징부(211)를 통해) 다른 컴퓨팅 디바이스와 데이터를 공유하는 것을 거부하도록 로직 및/또는 특징부를 포함할 수도 있다. 또한, 부가적인 컴퓨팅 디바이스들로부터 수신된 다른 품질 값들과 비교하여 낮은 품질 값이 다른 컴퓨팅 디바이스와 데이터를 공유하는 것을 거부하도록 유도할 수도 있다. 몇몇 예들에서는, 데이터를 공유하라는 요구가 간단히 무시될 수도 있다. 다른 예들에서는, 거절 메시지가 다른 컴퓨팅 디바이스에 중계될 수도 있다.

[0057] 블록 640이나 블록 645 중 어느 하나로부터 블록 650(여전히 베뉴 내?)으로 진행하며, 암호 관리자(112)는 컴퓨팅 디바이스(110-1)가 베뉴 서버(120)와 관련된 베뉴 내에 여전히 있는지의 여부를 판정하도록 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 컴퓨팅 디바이스(110-1)의 사용자가 컴퓨팅 디바이스(110-1)을 전원 차단했을 수도 있다. 다른 예들에서는, 사용자는 베뉴 서버(120)와의 통신 채널(140-1)을 종료했을 수도 있다. 다른 예들에 있어서, 종료된 통신 채널은 사용자가 베뉴 서버(120)(예컨대, 웹사이트)와 관련된 가상 베뉴를 떠나거나 물리적인 베뉴(예를 들면, 일반 서점(brick and mortar book store))를 물리적으로 떠나는 것으로부터 초래될 수도 있다. 컴퓨팅 디바이스(110-1)가 여전히 베뉴 내에 있는 경우, 프로세스는 판정 블록 635로 이동한다. 그렇지 않은 경우, 프로세스는 종료된다.

[0058] 도 7은 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된 결함 감내 복호(FTD) 스킴(700)의 일례를 예시한다. 몇몇 예들에서는, 도 1에 도시된 바와 같은 또는 도 3에 기술된 바와 같은 컴퓨팅 디바이스와 함께 위치하는 복호 관리자(114)가 FTD 스킴(700)의 적어도 부분들을 구현하도록 로직 및/또는 특징부를 포함할 수도 있다. 그렇지만, FTD 스킴(700)은 복호 관리자(114)의 로직 및/또는 특징부에 의한 구현에 제한되는 것은 아니다. 컴퓨팅 디바이스 상에 상주하거나 컴퓨팅 디바이스에 포함되는 다른 로직 및/또는 특징부가 FTD 스킴(700)의 적어도 일부를 또한 구현할 수도 있다.

[0059] 단계 7.1의 예(암호문(Y) 및 변환 파라미터(P)를 제공; 테이스트(S)를 제공)에서 시작하며, 수신 특징부(311)는 암호문(Y) 및 변환 파라미터(P)를 제공할 수도 있고, 테이스트 특징부(313)는 컴퓨팅 플랫폼(예컨대, 컴퓨팅 플랫폼(110-4)의 사용자의 관심 지역에 관련된 테이스트(S)를 제공할 수도 있다. 몇몇 예들에서는, Y 및 P는 각각 베뉴 서버(120)로부터 수신 특징부(311)에 의해 수신된 후 변환 특징부(315)에 제공되었을 수도 있다. Y 및 P는 예를 들면, 베뉴 서버(120)에 또한 통신 가능하게 결합되는 다른 컴퓨팅 디바이스에서 로직 및/또는 특징부에 의해 최초로 생성되었을 수도 있다. 다른 컴퓨팅 디바이스는 도 5 및 도 6에 대해 상술한 단계들/프로세스들과 유사한 Y 및 P를 생성했을 수도 있다. 다른 컴퓨팅 디바이스는 그 후, 베뉴 서버(120)에 유지되도록 Y 및 P를 전송했을 수도 있다. 또한, 이들 예에 있어서, S가 변환 특징부(315)에 제공될 수도 있다. S에 관한 관심

지역은 예를 들면, 컴퓨팅 디바이스의 사용자에 의해 구매된 서적일 수도 있다. 몇몇 예들에서는, 도 4에 도시된 다차원 속성 값(예를 들면, (39,2))과 유사한 다차원 속성 값일 수도 있다.

[0060] 단계 7.2의 예(변환된 테이스트(S')를 제공)로 이동하며, 변환 특징부(315)는 변환된 테이스트(S')를 복호 특징부(317)에 제공할 수도 있다. 몇몇 예들에 따르면, 변환 특징부(315)는 S의 다차원 속성 값을 미리 정의된 유한 필드(F)에 걸쳐 S'의 1차원 속성 값으로 변환할 수도 있다. 바꿔 말하면, S는 P에 의해 정의되는 비가역 변환을 사용하여 1차원 이산 집합 S' ? F로 변환될 수도 있다. 이러한 S'로의 변환의 결과는 그 후 1차원 데이터로 매핑될 수도 있다.

[0061] 단계 7.3의 예(복호의 품질을 기초로 하여 필명 및 세션 키를 제공)로 이어지며, 복호 특징부(317)는 복호의 품질의 평가에 기초하여 복호된 필명 및 복호된 세션 키를 개시 특징부(319)에 제공할 수도 있다. 몇몇 예들에서는, 필명 및 세션 키가 상술한 바와 같이, 수신 특징부(311)에 의해 제공되는 Y로부터 획득된다. 이들 예에 있어서, 필명은 다른 컴퓨팅 디바이스를 식별할 수도 있고, 세션 키는 다른 컴퓨팅 디바이스와의 보안 세션을 개시하는 데 사용될 수도 있다. 복호 특징부(217)는 F 상에서 이하의 파라미터: k, r(k? r)에 기초하여 Y의 복호 품질을 판정하도록 구성될 수도 있다.

[0062] 몇몇 예들에서는, 컴퓨팅 플랫폼의 사용자에 대한 S가 Y를 최초로 생성했던 컴퓨팅 플랫폼에 대한 테이스트(T)와 유사한 경우, 동일한 P를 S 및 T에 적용한 변환의 결과, 즉, S' 및 T'는 거의 동일하게 된다. 이들 예에 있어서, 품질 판정 프로세스가 아래의 2개의 단계 프로세스를 포함할 수도 있다:

[0063] 단계 1: Y 내의 각 (x,y)에 대해 행함

[0064] x가 S' 내에 있지 않으면, Y로부터 (x,y)를 소거한다.

[0065] 단계 2: 가능하면

[0066] 차수 k-1을 갖는 F 상에서의 다항식 g를 구성하여

[0067] g가 감소된 Y의 포인트의 최대 수를 커버할 수도 있게 한다.

[0068] 그 후 g의 k 계수를 수집하고 비트 스트링 Z를 구성한다.

[0069] 실재로 g 내에 있는 감소된 Y 내의 쌍(x,y)의 수 Q를 카운트한다.

[0070] (Z, Q)를 출력한다.

[0071] 이것이 가능하지 않으면, "복호 실패"를 출력한다.

[0072] 몇몇 예들에서는, 품질 판정 프로세스가 Y로부터 x 좌표가 S' 내에 있지 않은 포인트들을 소거하는 것을 포함할 수도 있다. 이들 예에 있어서, Y는 처음에 x 값으로서 집합 T' 내의 모든 소자들을 사용하여 평가되었던 포인트 (x,f(x))뿐만 아니라 랜덤한 노이즈 포인트를 함유할 수도 있다. 또한, S' 및 T'의 다수의 중첩된 값들이 존재하는 경우, 이들 노이즈 포인트의 대부분이 품질 판정 프로세스의 제1 단계에서 제거될 수도 있다. 또한, 다수의 최초의 함수 값 (x,f(x))는 남아 있어야 한다. 품질 판정 프로세스의 단계 2는 라그랑제 보간(Lagrange interpolation)을 통해서 이들 순서 쌍 (x,y)를 결합함으로써 곡선을 재구성하도록 프로세스를 포함할 수도 있다. 그러나, S' 및 T'가 정확히 매치하지 않고 그들 사이에 작은 차이가 있을 수도 있는 경우에는, 이들 에러는 정확한 보간을 위해 제거될 수도 있다. 에러를 제거하기 위해, 리드 솔로몬 알고리즘(Reed-Solomon algorithm)과 같은 코딩 원리에 널리 사용되는 디코딩 알고리즘이 사용될 수도 있다.

[0073] 디코딩이 성공적이거나 적절한 품질일 때, 다항식 g가 재구성될 수 있다. 다항식 g는 도 5에 대해 상술한 바와 같이 암호문의 생성을 위한 상술한 다항식 f와 실질적으로 유사할 수도 있다. S가 T와 매우 상이할 때, S' 및 T'에서 큰 차이가 있을 수도 있다. S' 및 T'에서의 큰 차이의 결과로서, 품질 판정 프로세스의 단계 2를 구현하는 것은 다항식 g 상에서 다수의 포인트를 소거할 수도 있고 다수의 랜덤한 노이즈는 남아 있어야 한다. 다수의 랜덤한 노이즈의 존재는 디코딩의 실패 또는 부적절한 품질을 야기할 수도 있다.

[0074] 몇몇 예들에서는, 복호가 적절했거나 수용 가능했던 경우에는, 출력 (Z,Q)가 품질 판정 프로세스로부터 초래될 수도 있다. 이들 예에 있어서 Z는 다른 컴퓨팅 디바이스를 식별하도록 평문 세션 키 및 필명을 포함할 수도 있고, Q는 복호와 관련된 품질 값을 포함할 수도 있다. Q의 값은 단계 2를 구현한 후에 여전히 남아 있는 랜덤한 노이즈의 크기에 기초할 수도 있다. 예를 들면, 랜덤한 노이즈의 큰 크기가 Q의 더 낮은 값과 같고 랜덤한 노이즈의 작은 크기는 Q의 더 높은 값과 같다. 상술한 바와 같이, 랜덤한 노이즈의 더 작은 크기는 S 및 T가 실

질적으로 유사한 것을 의미할 수도 있다.

[0075] 도 8은 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된 암호문을 복호하고 보안 세션을 개시하는 방법의 예의 플로우차트를 예시한다. 몇몇 예들에서는, 시스템(100)의 소자들이 도 8에 도시된 플로우차트와 관련된 방법의 예를 예시하는 데 사용될 수도 있다. 도 3에 도시된 바와 같은 복호 관리자(114)가 방법의 예를 예시하는 데 사용될 수도 있다. 그렇지만, 기술된 방법은 도 3에 도시된 시스템(100) 상에서 또는 복호 관리자(114)에 대한 구현에 제한되는 것은 아니다. 방법의 예는 도 1 또는 도 3에 도시된 소자들 중의 하나 이상을 갖는 다른 시스템 상에서 구현될 수도 있다.

[0076] 시작으로부터 블록 810(베뉴로 들어감)으로 이동하며, 컴퓨팅 디바이스(110-4)와 같은 컴퓨팅 디바이스가 베뉴에 들어갈 수도 있다. 몇몇 예들에서는, 컴퓨팅 디바이스(110-4)는 베뉴에 들어갈 때 통신 채널(140-4)을 통해 베뉴 서버(120)와 통신 가능하게 결합할 수도 있다.

[0077] 블록 810으로부터 블록 820(암호문 및 변환 파라미터를 수신)으로 진행하며, 컴퓨팅 디바이스(110-4)와 함께 위치하는 복호 관리자(114)는 (예를 들면, 수신 특징부(311)를 통해) 암호문 및 변환 파라미터를 수신하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 암호문 및 변환 파라미터가 통신 채널(140-1)을 통해 베뉴 서버(120)로부터 수신될 수도 있다. 이들 예에 있어서, 암호문 및 변환 파라미터는 베뉴 서버(120)에 또한 통신 가능하게 결합되는 다른 컴퓨팅 디바이스(예컨대, 컴퓨팅 디바이스(110-1))로부터 베뉴 서버(120)에 전송된 후 (예를 들면, 보안 정보(124)와 함께) 베뉴 서버(120)에 유지되었을 수도 있다.

[0078] 블록 820으로부터 블록 830(테이스트를 수신)으로 진행하며, 복호 관리자(114)는 (예를 들면, 테이스트 특징부(311)를 통해) 관심 지역에 관련된 테이스트를 수신하거나 획득하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 테이스트가 컴퓨팅 디바이스(110-4)의 사용자의 관심 지역에 관련될 수도 있다. 또한, 테이스트는 도 4에 대해 상술한 다차원 속성 값과 같은 다차원 속성 값으로 나타낼 수도 있다. 이들 예에 있어서, 컴퓨팅 디바이스(110-4)는 애플리케이션(116)을 포함하지 않으며, 따라서 테이스트에 대한 다차원 속성 값을 제공하도록 베뉴 서버(120)에 의존할 수도 있다.

[0079] 블록 830으로부터 블록 840(테이스트를 변환)으로 진행하며, 복호 관리자(114)는 (예를 들면, 변환 특징부(315)를 통해) 수신된 테이스트에 대한 다차원 속성 값을 변환하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에 따르면, 다차원 속성 값이 FTD 스킴(700)에 대해 상술한 바와 같이 변환될 수도 있다. 이들 예에 있어서, 다차원 속성 값은 생성된 변환 파라미터를 사용하여 1차원 속성 값으로 변환될 수도 있다.

[0080] 블록 840으로부터 블록 850(암호문을 복호)으로 진행하며, 복호 관리자(114)는 (예를 들면, 복호 특징부(317)를 통해) 수신된 암호문을 복호하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에 따르면, 암호문은 FTD 스킴(700)에 대해 상술한 바와 같이 복호될 수도 있다. 예를 들면, 변환된 다차원 속성 값은 1차원 속성 값을 사용하여 수신된 암호문으로부터 필명 및 세션 키를 복호하는 데 사용될 수도 있다.

[0081] 블록 840으로부터 블록 850(품질 적절?)으로 진행하며, 복호 관리자(114)는 (예를 들면, 복호 특징부(317)를 통해) 복호된 암호문의 품질이 적절한지의 여부를 판정하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 2 단계 품질 판정 프로세서가 복호의 품질이 적절한지의 여부를 판정하기 위해 FTD 스킴(700)에 대해 상술한 바와 같이 구현될 수도 있다. 품질이 적절한 경우에는(예를 들면, 랜덤한 노이즈가 거의 남아 있지 않음), 프로세스는 블록 870으로 이동한다. 그렇지 않은 경우에는, 프로세스는 판정 블록 880으로 이동한다.

[0082] 판정 블록 860으로부터 블록 870(보안 세션을 개시)으로 이동하며, 복호 관리자(114)는 다른 컴퓨팅 디바이스(예컨대, 컴퓨팅 디바이스(110-1))와의 보안 세션을 개시하도록 구성되는 로직 및/또는 특징부(예를 들면, 개시 특징부(319))를 포함할 수도 있다. 몇몇 예들에서는, 보안 세션은 다른 컴퓨팅 디바이스에 복호된 세션 키 및 복호된 필명을 전송하는 것을 통해서 개시될 수도 있다. 이들 예 중 몇몇에 있어서, 베뉴 서버(120)와 미리 설정된 통신 채널(예컨대, 통신 채널(140-1 내지 140-4))이 다른 컴퓨팅 디바이스와의 보안 세션을 개시하도록 사용될 수도 있다. 다른 예들에서는, 별개로 설정된 통신 채널이 다른 컴퓨팅 디바이스와의 보안 세션을 개시하도록 사용될 수도 있다.

[0083] 몇몇 예들에 따르면, 다른 컴퓨팅 디바이스는 최초로 암호화된 필명 및 세션 키에 실질적으로 매칭하는 필명 및 세션 키에 적어도 부분적으로 기초하여 보안 세션을 설정할 수도 있다. 보안 세션이 설정되었다면, 컴퓨팅 디바이스(110-4)는 다른 컴퓨팅 디바이스와 관심 지역과 관련된 데이터를 안전하게 공유할 수도 있다. 데이터는 2개의 컴퓨팅 디바이스 사이에 별개로 설정된 통신 채널을 통해 또는 미리 설정된 통신 채널(예컨대, 통신 채널

(140-1 내지 140-4))을 통해 베뉴 서버(120)를 통해서 안전하게 공유될 수도 있다.

[0084] 블록 879으로부터 판정 블록 880(여전히 베뉴 내에 있음)으로 진행하며, 복호 관리자(114)는 컴퓨팅 디바이스(110-4)가 베뉴 서버(120)와 관련된 베뉴 내에 여전히 있는지의 여부를 판정하도록 구성되는 로직 및/또는 특징부를 포함할 수도 있다. 몇몇 예들에서는, 컴퓨팅 디바이스(110-4)의 사용자가 컴퓨팅 디바이스(110-4)를 전원 차단했을 수도 있다. 다른 예들에서는, 사용자는 베뉴 서버(120)와의 통신 채널(140-4)을 종료했을 수도 있다. 다른 예들에 있어서, 종료된 통신 채널은 사용자가 베뉴 서버(120)와 관련된 가상 베뉴(예컨대, 웹사이트)를 떠나거나 물리적인 베뉴(예를 들면, 일반 서점)를 물리적으로 떠나는 것으로부터 초래될 수도 있다. 컴퓨팅 디바이스(110-4)가 여전히 베뉴 내에 있는 경우, 프로세스는 블록 820으로 이동한다. 그렇지 않은 경우, 프로세스는 종료된다.

[0085] 도 9는 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된 컴퓨터 프로그램 제품(900)의 일례의 블록도를 예시한다. 몇몇 예들에서는, 도 9에 도시된 바와 같이, 컴퓨터 프로그램 제품(900)은 제1 컴퓨팅 디바이스에서 구현되도록 명령(904)을 포함할 수도 있는 신호 베어링 매체(902)를 포함한다. 로직(예컨대, 암호 로직(210))에 의해 실행될 때 명령(904)은 로직이 서버로부터 제1 암호문 및 변환 파라미터를 수신하게 할 수도 있다. 제2 컴퓨팅 디바이스는 암호문 및 변환 파라미터를 생성했을 수도 있다. 명령(904)은 또한 로직이 제1 컴퓨팅 디바이스의 제1 사용자에 대한 제1 테이스트를 수신하게 할 수도 있다. 제1 테이스트는 관심 지역과 관련될 수도 있고, 다차원 속성 값을 가질 수도 있다. 명령(904)은 또한, 로직이 제1 테이스트에 대한 다차원 속성 값을 변환 파라미터를 사용하여 1차원 속성 값으로 변환하게 할 수도 있다. 명령(904)은 또한, 로직이 제2 컴퓨팅 디바이스를 식별하는 필명을 획득하기 위해 및 제2 컴퓨팅 디바이스와 데이터를 안전하게 공유하도록 필명과 함께 사용될 세션 키를 획득하기 위해 1차원 속성 값을 사용하여 제1 암호문을 복호하게 할 수도 있다. 몇몇 실시예들에서는, 명령(904)은 로직이 복호의 품질을 판정하고, 임계값을 초과하는 복호의 판정된 품질에 적어도 부분적으로 기초하여 데이터를 공유하도록 다른 컴퓨팅 디바이스와의 보안 세션을 개시하게 할 수도 있다.

[0086] 또한 도 9에 도시된, 몇몇 예들에서는, 컴퓨터 제품(900)은 컴퓨터 판독 가능한 매체(906), 기록 가능한 매체(908) 및 통신 매체(910) 중 하나 이상을 포함할 수도 있다. 이들 소자 주위의 점선 박스는 신호 베어링 매체(902)에 제한되는 것은 아니지만 그 내에 포함되는 상이한 타입의 매체를 도시한다. 이들 타입의 매체는 로직(예컨대, 암호 로직(210))에 의해 실행될 명령(904)을 배포할 수도 있다. 컴퓨터 판독 가능한 매체(906) 및 기록 가능한 매체(908)는 플렉시블(flexible) 디스크, 하드 디스크 드라이브(HDD), 컴팩트 디스크(CD), 디지털 다기능 디스크(DVD: Digital Versatile Disk), 디지털 테이프, 컴퓨터 메모리 등에 제한되는 것은 아니지만 이들을 포함할 수도 있다. 통신 매체(910)는 디지털 및/또는 아날로그 통신 매체(예컨대, 섬유 광학 케이블, 도파관, 유선 통신 링크, 무선 통신 링크 등)에 제한되는 것은 아니지만 이것을 포함할 수도 있다.

[0087] 도 10은 본 개시내용의 적어도 몇몇 실시예들에 따라서 배열된 컴퓨팅 디바이스(1000)의 일례를 예시한다. 몇몇 예들에서는, 도 1, 도 2 또는 도 3에 도시된 암호 관리자(112) 또는 복호 관리자(114)가 컴퓨팅 디바이스(1000) 상에서 구현될 수도 있다. 이들 예에서는, 컴퓨팅 디바이스(1000)의 소자들은 컴퓨팅 디바이스들 간에 데이터를 안전하게 공유하기 위해 테이스트 기반 인증을 구현하도록 배열되거나 구성될 수도 있다. 매우 기본적인 구성(1001)에서, 컴퓨팅 디바이스(1000)는 일반적으로 하나 이상의 프로세서(1010) 및 시스템 메모리(1020)를 포함한다. 메모리 버스(1030)는 프로세서(1010)와 시스템 메모리(1020) 사이의 통신을 위해 사용될 수 있다.

[0088] 원하는 구성에 따라서, 프로세서(1010)는 마이크로프로세서(μP), 마이크로컨트롤러(μC), 디지털 신호 프로세서(DSP)에 제한되는 것은 아니지만 이들을 포함하는 어느 타입 또는 이들의 임의의 조합으로 될 수 있다. 프로세서(1010)는 레벨 1 캐시(1011) 및 레벨 2 캐시(1012)와 같은 하나 이상의 레벨의 캐싱(caching), 프로세서 코어(1013) 및 레지스터(1014)를 포함할 수 있다. 프로세서 코어(1013)는 산술 논리 유닛(ALU), 부동 소수점 유닛(FPU), 디지털 신호 처리 코어(DSP Core), 또는 이들의 임의의 조합을 포함할 수 있다. 메모리 제어기(1015)는 또한 프로세서(1010)와 함께 사용될 수 있거나, 몇몇 구현예에서는, 메모리 제어기(1015)는 프로세서(1010)의 내부 부품일 수 있다.

[0089] 원하는 구성에 따라서, 시스템 메모리(1020)는 (RAM과 같은) 휘발성 메모리, (ROM, 플래시 메모리 등과 같은) 비휘발성 메모리로 제한되는 것은 아니지만 이들을 포함하는 어느 타입 또는 이들의 임의의 조합일 수 있다. 시스템 메모리(1020)는 일반적으로 운영 체계(1021), 하나 이상의 애플리케이션(1022) 및 프로그램 데이터(1024)를 포함한다. 애플리케이션(1022)은 도 2 또는 도 3에 도시된 암호 관리자(112) 또는 복호 관리자(114) 아키텍처에 대해 기술된 동작을 포함하는 또는 도 5 내지 도 8에 도시된 스킴 및 플로우차트에 대해 기술된 동

작을 포함하는 본 명세서에 기술된 바와 같은 기능을 실행하도록 배열되는 명령(1023)을 포함한다. 프로그램 데이터(1024)는 명령(1023)을 구현하는 데 유용한 공유 데이터(1025)를 포함한다. 몇몇 예들에서는, 애플리케이션(1022)은 운영 체계(1021) 상에서 프로그램 데이터(1024)로 동작하도록 배열될 수 있어 컴퓨팅 디바이스들 간에 데이터를 안전하게 공유하기 위해 테이스트 기반 인증을 구현하기 위한 명령의 구현예가 본 명세서에 기술된 바와 같이 제공될 수도 있게 된다. 이 기술된 기본 구성은 점선(1001) 내의 그들 구성요소에 의해 도 10에 예시된다.

[0090] 컴퓨팅 디바이스(1000)는 부가적인 특징부 또는 기능성, 및 기본 구성(1001)과 임의의 필요한 디바이스들 및 인터페이스들 사이의 통신을 용이하게 하기 위해 부가적인 인터페이스를 가질 수 있다. 예를 들면, 버스/인터페이스 제어기(1040)가 저장 인터페이스 버스(1041)를 통해 기본 구성(1001)과 하나 이상의 데이터 저장 디바이스(1050) 사이의 통신을 용이하게 하는 데 사용될 수 있다. 데이터 저장 디바이스(1050)는 착탈식 저장 디바이스(1051), 비착탈식 저장 디바이스(1052), 또는 이들의 조합일 수 있다. 착탈식 저장 및 비착탈식 저장 디바이스의 예들은 두서너 가지 예만 들면, 플렉시블 디스크 드라이브 및 하드 디스크 드라이브(HDD)와 같은 자기 디스크 디바이스, 컴팩트 디스크(CD) 드라이브 또는 디지털 다기능 디스크(DVD) 드라이브, 고체 상태 드라이브(SSD) 및 테이프 드라이브와 같은 광학 디스크 드라이브를 포함한다. 컴퓨터 저장 매체의 예는 컴퓨터 판독 가능한 명령, 데이터 구조, 프로그램 모듈, 또는 다른 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술에서 구현되는 휘발성 및 비휘발성, 착탈 가능 및 비착탈식 매체를 포함할 수 있다.

[0091] 시스템 메모리(1020), 착탈식 저장장치(1051) 및 비착탈식 저장장치(1052)는 모두 컴퓨터 저장 매체의 예이다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, 디지털 다기능 디스크(DVD) 또는 다른 광학 저장장치, 자기 카세트, 자기 테이프, 자기 디스크 저장장치 또는 다른 자기 저장 디바이스, 또는 원하는 정보를 저장하는 데 사용될 수 있고 컴퓨팅 장치(1000)에 의해 액세스될 수 있는 임의의 다른 매체(예를 들면, 신호의 기저대역 표시)에 제한되는 것은 아니지만 이들을 포함한다. 그러한 컴퓨터 저장 매체의 어느 하나는 디바이스(1000)의 일부일 수 있다.

[0092] 컴퓨팅 디바이스(1000)는 또한 버스/인터페이스 제어기(1040)를 통해 다양한 인터페이스 디바이스들(예를 들면, 출력 인터페이스, 주변 인터페이스, 및 통신 인터페이스)로부터 기본 구성(1001)으로의 통신을 용이하게 하기 위한 인터페이스 버스(1042)를 포함할 수 있다. 출력 인터페이스(1060)의 예는 그래픽 처리 유닛(1061) 및 오디오 처리 유닛(1062)을 포함하고, 이들은 하나 이상의 A/V 포트(1063)를 통해 디스플레이 또는 스피커와 같은 다양한 외부 디바이스들에 통신하도록 구성될 수 있다. 주변 인터페이스(1070)의 예는 직렬 인터페이스 제어기(1071) 또는 병렬 인터페이스 제어기(1072)를 포함하며, 이들은 하나 이상의 I/O 포트(1073)를 통해 입력 디바이스(예를 들면, 키보드, 마우스, 펜, 보이스 입력 디바이스, 터치 입력 디바이스 등) 또는 다른 주변 디바이스(예를 들면, 프린터, 스캐너 등)와 같은 외부 디바이스들과 통신하도록 구성될 수 있다. 통신 인터페이스(1080)의 예는 하나 이상의 통신 포트(1082)를 통해 네트워크 통신 상으로 하나 이상의 다른 컴퓨팅 디바이스(1090)와의 통신을 용이하게 하도록 배열될 수 있는 네트워크 제어기(1081)를 포함한다. 네트워크 통신 접속은 통신 매체의 일례이다. 통신 매체는 일반적으로 컴퓨터 판독 가능한 명령, 데이터 구조, 프로그램 모듈, 또는 반송파나 다른 전송 메커니즘과 같은 변조된 데이터 신호 내의 다른 데이터에 의해 구현될 수도 있고, 임의의 정보 전달 매체를 포함할 수도 있다. "변조된 데이터 신호"는 신호 내의 정보를 인코드하기 위한 방식으로 설정되거나 변경된 그 특징부 중의 하나 이상을 갖는 신호일 수 있다. 제한되는 것이 아닌 예로서, 통신 매체는 유선 네트워크 또는 직접 유선 접속과 같은 유선 매체, 및 음향, 무선 주파수(RF), 적외선(IR) 및 다른 무선 매체와 같은 무선 매체를 포함할 수 있다. 본 명세서에서 사용된 바와 같은 용어 컴퓨터 판독 가능한 매체는 저장 매체와 통신 매체의 양자 모두를 포함할 수 있다.

[0093] 컴퓨팅 디바이스(1000)는 워크스테이션 또는 서버 구성에서 구현되거나 랩탑 컴퓨터 및 비랩탑(non-laptop) 컴퓨터 구성의 양자 모두를 포함하는 퍼스널 컴퓨터의 일부로서 구현될 수 있다.

[0094] 용어 "응답하는" 또는 "응답하여"에 대해 이 개시내용에서 이루어진 참조는 특별한 특징부 및/또는 구조에 대한 응답성에 제한되는 것은 아니다. 특징부는 또한, 다른 특징부 및/또는 구조에 응답할 수도 있고, 그 특징부 및/또는 구조 내에 위치할 수도 있다. 또한, "결합된" 또는 "응답하는" 또는 "응답하여" 또는 "통신하여" 등과 같은 용어 또는 구가 본 명세서에서 또는 뒤따르는 청구항들에서 사용될 때, 이들 용어는 넓게 해석되어야 한다. 예를 들면, 구 "결합된"은 그 구가 사용되는 전후상황에 적절한 것으로서 통신 가능하게, 전기적으로 및/또는 동작 가능하게 결합되는 것을 지칭할 수도 있다.

[0095] 당업자는 본 명세서에 나타내는 방식으로 디바이스들 및/또는 프로세스들을 기술하고, 그 후 그러한 기술된 디

바이스들(예를 들면, 송신기, 수신기, 무선 디바이스, 컴퓨팅 플랫폼, 컴퓨팅 디바이스 등) 및/또는 방법을 데이터 처리 시스템에 병합하도록 공학적 실무를 사용하는 것이 당업계에서 일반적인 것을 인지할 것이다. 즉, 본 명세서에 기술된 디바이스 및/또는 방법의 적어도 일부는 적정 량의 실험을 통해 데이터 처리 시스템으로 병합될 수 있다. 당업자는 일반적인 데이터 처리 시스템이 통상적으로 시스템 유닛 하우징, 비디오 디스플레이 디바이스, 휘발성 및 비휘발성 메모리와 같은 메모리, 마이크로프로세서 및 디지털 신호 프로세서와 같은 프로세서, 운영 체계와 같은 연산 엔티티(computational entities), 드라이버, 그래픽 유저 인터페이스, 및 애플리케이션 프로그램 중 하나 이상, 터치 패드 또는 스크린과 같은 하나 이상의 대화식(interaction) 디바이스, 및/또는 피드백 루프 및 제어 모터(예를 들면, 위치 및/또는 속도를 감지하기 위한 피드백; 구성요소 및/또는 수량(quantities)을 이동 및/또는 조정하기 위한 제어 모터)를 포함하는 제어 시스템을 포함하는 것을 인지할 것이다. 일반적인 데이터 처리 시스템은 데이터 연산/통신 및/또는 네트워크 연산/통신 시스템에서 일반적으로 발견되는 것과 같은 임의의 적절한 시중에 유통되고 있는 구성요소를 이용하여 구현될 수도 있다.

[0096] 본 명세서에서 기술한 주제는 종종 상이한 다른 구성요소 또는 소자 내에 포함되거나, 그와 접속되는 상이한 구성요소 또는 소자를 예시한다. 그러한 도시된 아키텍처는 단순히 예라는 것과, 다수의 다른 아키텍처가 구현되어 동일한 기능성을 달성할 수 있다는 것을 이해할 것이다. 개념적인 의미에서, 동일한 기능성을 달성하기 위한 구성요소의 임의의 배치는 원하는 기능성이 달성되도록 하기 위해 효과적으로 "관련된다". 따라서, 특별한 기능성을 달성하기 위해 본 명세서에서 결합된 임의의 2개의 구성요소는, 아키텍처나 중간 구성요소에 무관하게 원하는 기능성이 달성되도록 하기 위해 서로 "관련되는" 것으로 보여질 수 있다. 유사하게, 그렇게 관련된 임의의 2개의 구성요소가 원하는 기능성을 달성하기 위해 서로 "동작 가능하게 접속되는" 또는 "동작 가능하게 결합되는" 것으로 보여질 수도 있고, 그렇게 관련된 임의의 2개의 구성요소가 원하는 기능성을 달성하기 위해 서로 "동작 가능하게 결합 가능한" 것으로 보여질 수도 있다. 동작 가능하게 결합 가능한의 특정 예들은 물리적으로 메이트 가능한(mateable) 및/또는 물리적으로 대화식의 구성요소 및/또는 무선으로 대화 가능한 및/또는 무선으로 대화식의 구성요소 및/또는 논리적으로 대화식의 및/또는 논리적으로 대화 가능한 구성요소로 제한되는 것은 아니지만 이들을 포함한다.

[0097] 본 명세서에서의 실질적으로 임의의 복수의 및/또는 단일의 용어의 사용에 대해, 당업자는 전후상황 및/또는 애플리케이션에 적절한 경우에 복수에서 단일로 및/또는 단일에서 복수로 바꿀 수 있다. 다양한 단일의/복수의 순열이 명확하게 하기 위해 본 명세서에서 분명하게 제시될 수도 있다.

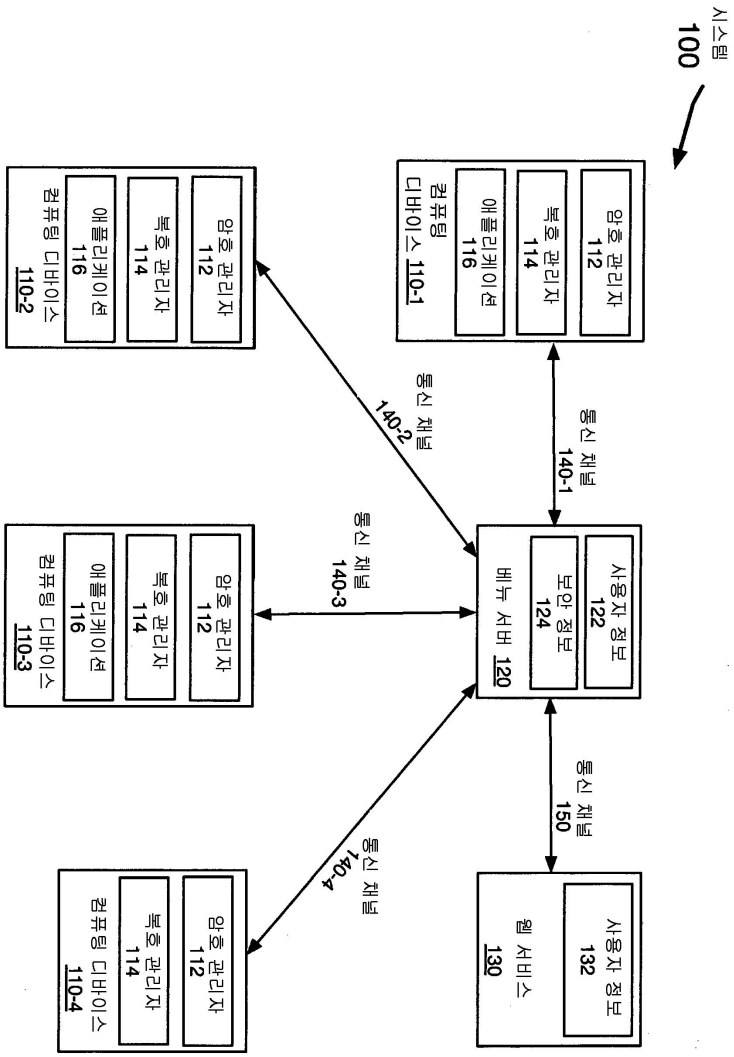
[0098] 일반적으로, 본 명세서에 및 특히 첨부하는 청구항(예를 들면, 첨부하는 청구항들의 본문)에서 사용되는 용어는 통상적으로 "오픈" 용어로서 의도되는 것을 당업자는 이해할 것이다(예를 들면, 용어 "포함하는"은 "그것에 제한되는 것은 아니지만 그것을 포함하는"으로 해석되어야 하고, 용어 "갖는"은 "적어도 갖는"으로 해석되어야 하며, 용어 "포함한다"는 "그것에 제한되는 것은 아니지만 그것을 포함한다"로 해석되어야 한다). 특정 수의 도입되는 청구항 설명이 의도되는 경우, 그러한 의도는 청구항에서 명백하게 인용될 것이고, 그러한 설명의 부재시에 그러한 의도는 존재하지 않는다는 것을 당업자는 이해할 것이다. 예를 들면, 이해에 도움을 주기 위해, 아래의 첨부하는 청구항들은 청구항 설명을 도입하기 위해 도입 구 "적어도 하나의" 및 "하나 이상의"의 사용을 포함할 수도 있다. 그러나, 그러한 구의 사용은 부정 관사 "a" 또는 "an"에 의한 청구항 설명의 도입이 그러한 도입된 청구항 설명을 포함하는 임의의 특정 청구항을 단 하나의 그러한 설명만을 포함하는 발명으로 제한하는 것을 나타내도록 해석되어서는 아니 되며, 동일한 청구항이 도입 구 "하나 이상의" 또는 "적어도 하나의" 및 "a" 또는 "an"과 같은 부정 관사를 포함할 때에도(예를 들면, "a" 및/또는 "an"은 일반적으로 "적어도 하나의" 또는 "하나 이상의"를 의미하도록 해석되어야 한다); 동일한 것이 청구항 설명을 도입하는 데 사용되는 부정 관사의 사용에 대해서도 참을 유지한다. 또한, 특정 수의 도입되는 청구항 설명이 명확하게 인용되더라도, 당업자는 그러한 설명이 적어도 인용된 수를 의미하는 것으로 일반적으로 해석되어야 하는 것을 인지할 것이다(예를 들면, 다른 수식어 없이 "2개의 설명"의 기본 설명은 일반적으로는 적어도 2개의 설명, 또는 2 이상의 설명을 의미한다). 더욱이, "A, B 및 C 중 적어도 하나"와 유사한 형식이 사용되는 경우에는, 일반적으로 그러한 구성은 당업자가 그 형식을 이해할 것이라는 의미로 의도된다(예를 들면, "A, B 및 C 중 적어도 하나를 갖는 시스템"은 A만, B만, C만, A 및 B를 함께, A 및 C를 함께, B 및 C를 함께, 및/또는 A, B, 및 C를 함께 등을 갖는 시스템에 제한되는 것은 아니지만 이를 포함할 것이다.). "A, B, 또는 C 등 중 적어도 하나"와 유사한 형식이 사용되는 경우에는, 일반적으로 그러한 구성은 당업자가 그 형식을 이해할 것이라는 의미로 의도된다(예를 들면, "A, B, 또는 C 중 적어도 하나를 갖는 시스템"은 A만, B만, C만, A 및 B를 함께, A 및 C를 함께, B 및 C를 함께, 및/또는 A, B, 및 C를 함께 등을 갖는 시스템에 제한되는 것은 아니지만 이를 포함할 것이다.). 상기 설명, 청구항, 또는 도면의 어느 것에서 2 이상의 대체 용어를 나타내는 가상적으로 임의의 이접적인 단어 및/또는 구가 용어 중 하나, 용어 중 어느 하나, 또는 용어의 양자를 포함할 가능성을 고려하는 것으로 이해되어야

하는 것을 당업계의 당업자는 또한 이해할 것이다. 예를 들면, 구 "A 또는 B"가 "A" 또는 "B" 또는 "A 및 B"의 가능성을 포함하는 것으로 이해될 것이다.

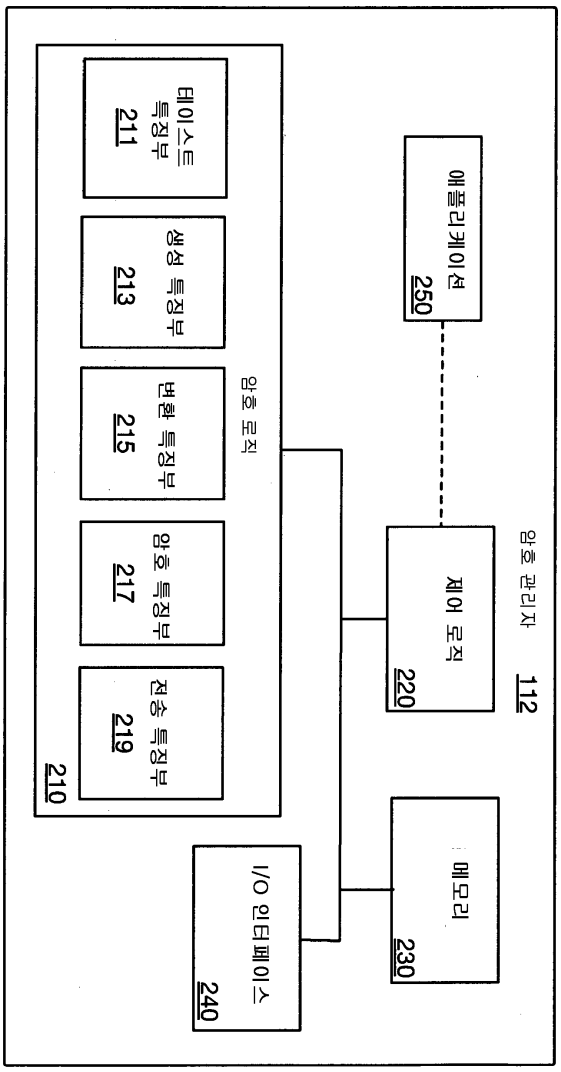
[0099] 본 명세서에서는 다양한 양태 및 실시예들이 개시되어 있지만, 다른 양태 및 실시예가 당업자에게는 명백해질 것이다. 본 명세서에 개시된 다양한 양태 및 실시예는 예시할 목적이지, 제한하고자 하는 의도는 아니며, 진정한 범위 및 사상은 아래의 청구항들에 의해 나타난다.

## 도면

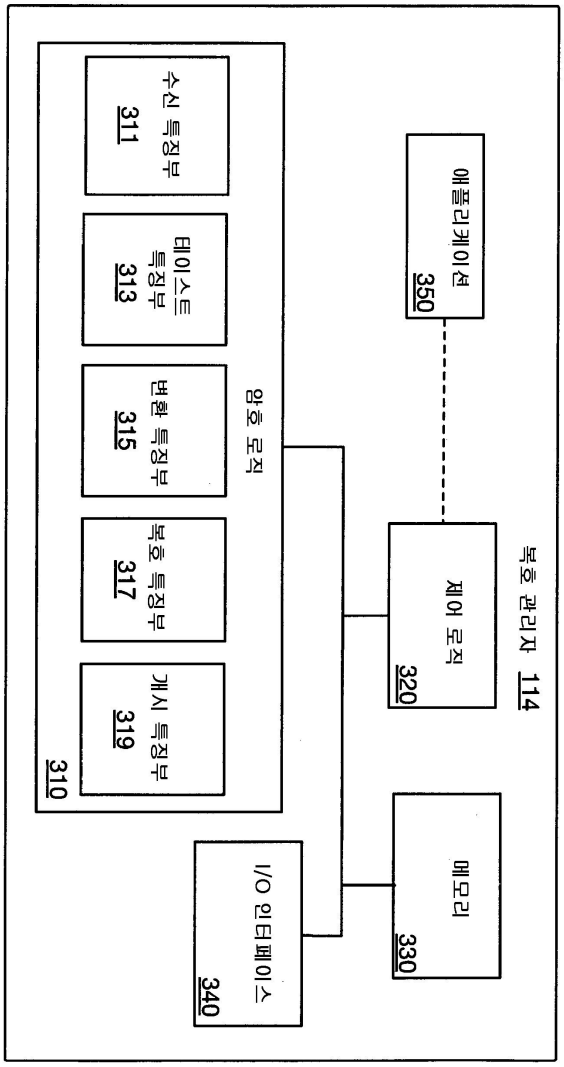
### 도면1



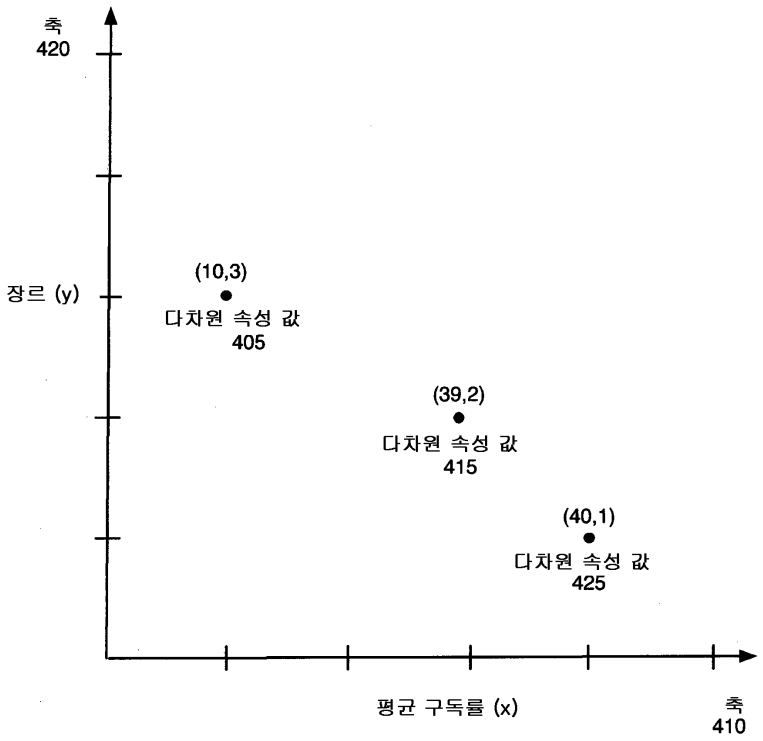
도면2


암호 관리자 112
애플리케이션 250
제어 로직 220
메모리 230
I/O 인터페이스 240
암호 로직 210
테이스트 특정부 211
생성 특정부 213
변환 특정부 215
암호 특정부 217
전송 특정부 219

도면3

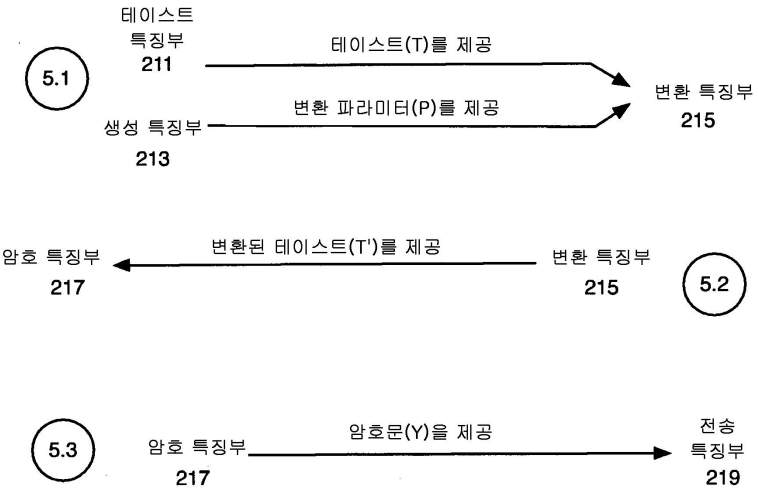

복호 관리자 114
애플리케이션 350
제어 로직 320
메모리 330
I/O 인터페이스 340
암호 로직 310
수신 특징부 311
테이스트 특징부 313
변환 특징부 315
복호 특징부 317
개시 특징부 319

도면4



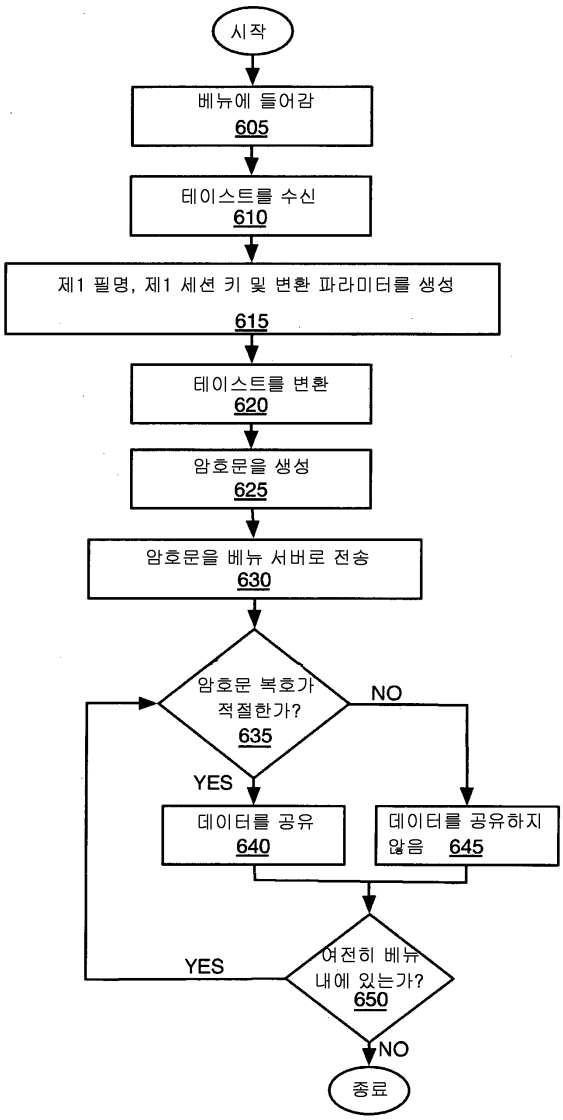

Map 400

도면5

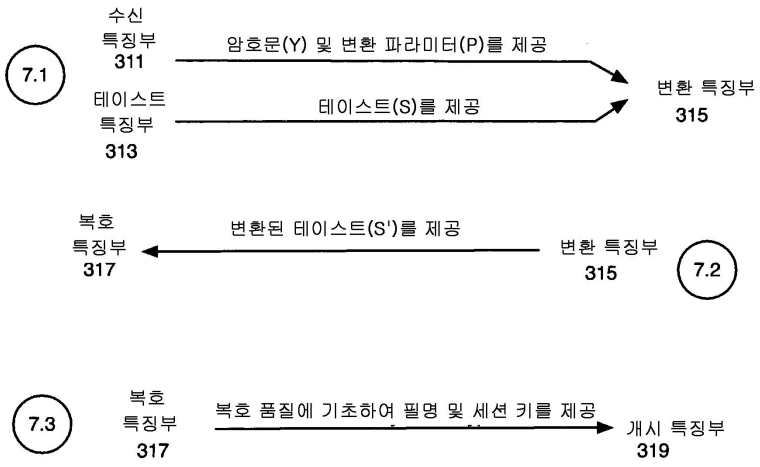



결함 감내 암호(FTE) 스킴 500

도면6

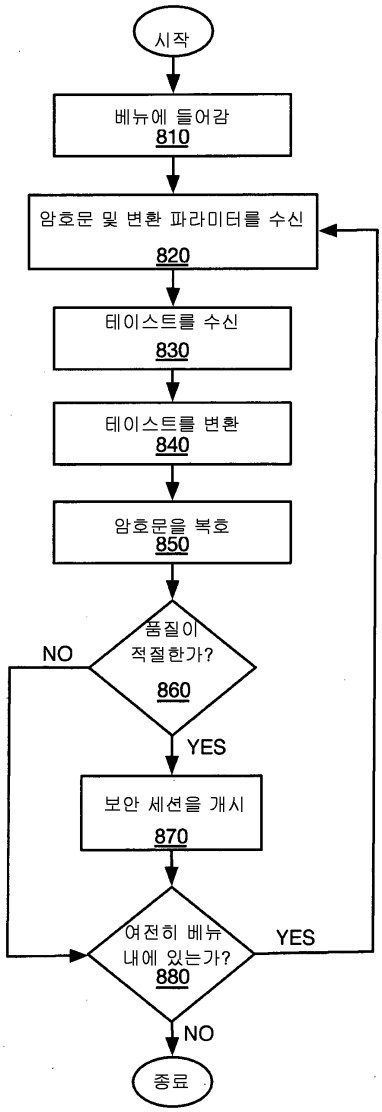



도면7

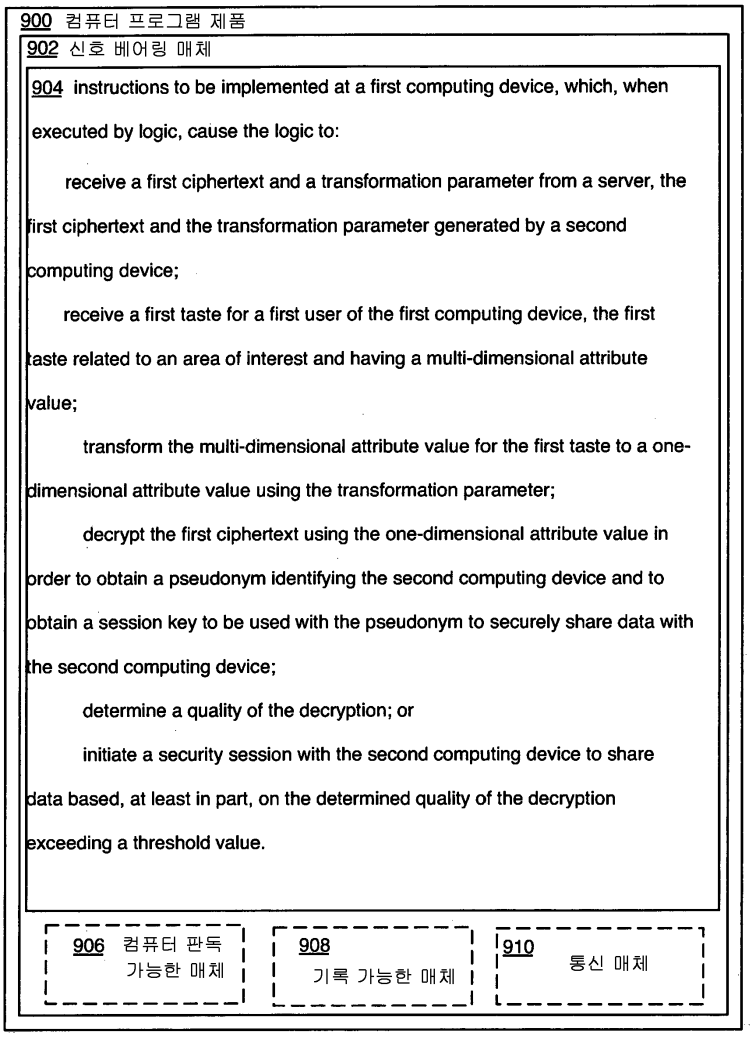



결함 감내 복호(FTD) 스킴 700

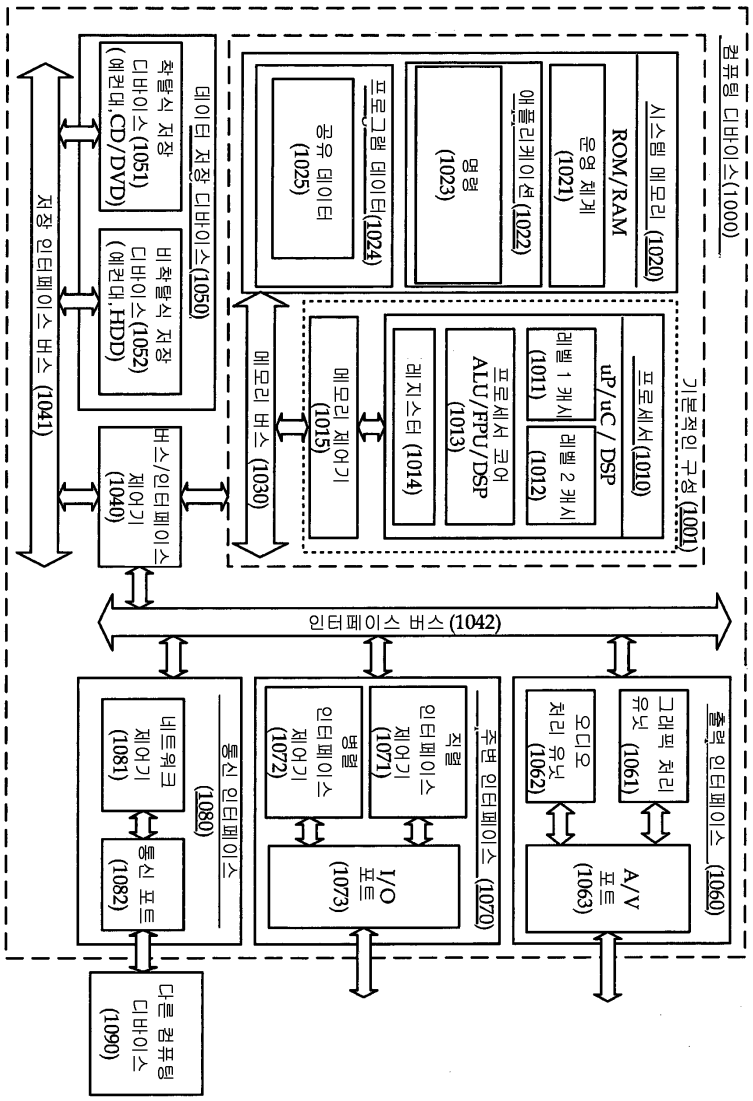
도면8


시작
베뉴에 들어감
810
암호문 및 변환 파라미터를 수신
820
테이스트를 수신
830
테이스트를 변환
840
암호문을 복호
850
품질이
적절한가?
860
NO
YES
보안 세션을 개시
870
여전히 베뉴
내에 있는가?
880
YES
NO
종료

도면9


900 컴퓨터 프로그램 제품
902 신호 베어링 매체
904 instructions to be implemented at a first computing device, which, when executed by logic, cause the logic to:
receive a first ciphertext and a transformation parameter from a server, the first ciphertext and the transformation parameter generated by a second computing device;
receive a first taste for a first user of the first computing device, the first taste related to an area of interest and having a multi-dimensional attribute value;
transform the multi-dimensional attribute value for the first taste to a one-dimensional attribute value using the transformation parameter;
decrypt the first ciphertext using the one-dimensional attribute value in order to obtain a pseudonym identifying the second computing device and to obtain a session key to be used with the pseudonym to securely share data with the second computing device;
determine a quality of the decryption; or
initiate a security session with the second computing device to share data based, at least in part, on the determined quality of the decryption exceeding a threshold value.
906 컴퓨터 판독 가능한 매체
908 기록 가능한 매체
910 통신 매체

도면10


컴퓨팅 디바이스(1000)
시스템 메모리 (1020)
ROM/RAM
운영 체계 (1021)
애플리케이션 (1022)
명령 (1023)
프로그램 데이터(1024)
공유 데이터 (1025)
기본적인 구성 (1001)
프로세서(1010)
uP/uC / DSP
레벨 1 캐시 (1011)
레벨 2 캐시 (1012)
프로세서 코어 ALU/FPU/DSP (1013)
레지스터 (1014)
메모리 제어기 (1015)
메모리 버스 (1030)
데이터 저장 디바이스(1050)
착탈식 저장 디바이스 (1051) (예컨대,CD/DVD)
비 착탈식 저장 디바이스(1052) (예컨대,HDD)
저장 인터페이스 버스 (1041)
버스/인터페이스 제어기 (1040)
인터페이스 버스 (1042)
출력 인터페이스 (1060)
그래픽 처리 유닛 (1061)
오디오 처리 유닛 (1062)
A/V 포트 (1063)
주변 인터페이스 (1070)
직렬 인터페이스 제어기 (1071)
병렬 인터페이스 제어기 (1072)
I/O 포트 (1073)
통신 인터페이스 (1080)
네트워크 제어기 (1081)
통신 포트 (1082)
다른 컴퓨팅 디바이스 (1090)