(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0024498
(43) 공개일자 2013년03월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/28 (2006.01)
(21) 출원번호 10-2011-0087982
(22) 출원일자 2011년08월31일
심사청구일자 2011년08월31일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
정익래
서울특별시 노원구 공릉동 81번지 태강아파트 1014동 1303호
이동훈
서울특별시 종로구 사직로8길 34, 경의궁의아침 3단지아파트 1404호 (내수동)
(뒷면에 계속)
(74) 대리인
특허법인엠에이피에스

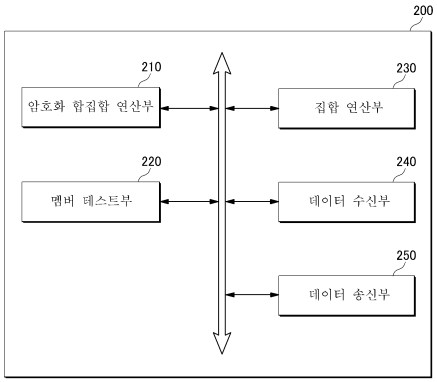
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **분산된 집합에서 프라이버시를 보호하는 집합 연산 제공 방법 및 시스템**

(57) 요 약

집합 연산 시스템이 분산된 집합의 프라이버시를 보호하는 집합 연산을 제공하는 방법은, 복수의 참여자의 협력을 통해, 상기 복수의 참여자가 소유한 각각의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합을 생성하는 단계, 상기 복수의 참여자가 소유한 각각의 집합에 속하는 원소가 상기 암호화된 합집합에 속하는지 여부를 판단하는 단계 및 상기 집합 연산의 연산식 및 상기 각각의 집합에 속한 원소의 상기 암호화된 합집합에 속하는 지 여부에 기초하여, 상기 집합 연산을 수행하는 단계를 포함한다.

대 표 도 - 도2



(72) 발명자

천지영

서울특별시 성북구 오패산로 46, 두산위브 아파트 118동 104호 (하월곡동)

노건태

서울특별시 강남구 개포로 516, 주공아파트 707동 1304호 (개포동)

이 발명을 지원한 국가연구개발사업

과제고유번호	KI002113201103100110013918KI002113201103
부처명	연구지원부
연구사업명	산업원천기술개발사업
연구과제명	Car-헬스케어 보안 기술개발
주관기관	고려대학교 산학협력단
연구기간	2011.03.01 ~ 2012.02.29

특허청구의 범위

청구항 1

집합 연산 시스템이 분산된 집합의 프라이버시를 보호하는 집합 연산을 제공하는 방법에 있어서,

(a) 복수의 참여자의 협력을 통해, 상기 복수의 참여자가 소유한 각각의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합을 생성하는 단계;

(b) 상기 복수의 참여자가 소유한 각각의 집합에 속하는 원소가 상기 암호화된 합집합에 속하는지 여부를 판단하는 단계; 및

(c) 상기 집합 연산의 연산식 및 상기 각각의 집합에 속한 원소의 상기 암호화된 합집합에 속하는 지 여부에 기초하여, 상기 집합 연산을 수행하는 단계를 포함하는

집합 연산 제공 방법.

청구항 2

제 1 항에 있어서,

상기 복수의 집합에 포함되는 각각의 집합은 다항식의 형태로 표현되는 것인

집합 연산 제공 방법.

청구항 3

제 2 항에 있어서,

상기 (a) 단계는,

(a-1) 제 1 참여자를 제외한 복수의 참여자가 각각 소유한 집합을 다항식의 형태로 표현하고, 랜덤 데이터를 선택하는 단계;

(a-2) 상기 제 1 참여자를 제외한 복수의 참여자가 상기 다항식, 상기 랜덤 데이터 및 상기 복수의 참여자가 각각 소유한 집합에 대하여 암호화된 데이터를 상기 제 1 참여자에게 전달하는 단계; 및

(a-3) 상기 제 1 참여자가 자신의 소유한 집합 및 상기 제 1 참여자를 제외한 복수의 참여자로부터 수신한 암호화된 데이터에 기초하여, 암호화된 합집합을 생성하는 단계를 포함하는

집합 연산 제공 방법.

청구항 4

제 1 항에 있어서,

(d) 상기 집합 연산의 수행을 통해 획득한 상기 연산식의 결과 데이터를 상기 복수의 참여자에게 제공하는 단계를

더 포함하는 집합 연산 제공 방법.

청구항 5

제 4 항에 있어서,

(e) 상기 복수의 참여자의 협력을 통해, 상기 연산식의 결과 데이터를 복호화하는 단계를 더 포함하는

집합 연산 제공 방법.

청구항 6

제 1 항에 있어서,

상기 (a) 단계는,

복수의 참여자의 단말로부터 참여자의 집합 데이터를 수신하는 단계를 포함하는

집합 연산 제공 방법.

청구항 7

제 1 항에 있어서,

상기 집합 연산은 상기 복수의 참여자가 소유한 각각의 집합에 대한 DNF(Disjunctive normal form) 연산인 것인

집합 연산 제공 방법.

청구항 8

분산된 집합의 프라이버시를 보호하는 집합 연산을 제공하는 집합 연산 제공 시스템에 있어서,

복수의 참여자의 협력을 통해, 상기 복수의 참여자가 소유한 각각의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합을 생성하는 암호화 합집합 연산부;

상기 복수의 참여자가 소유한 각각의 집합에 속하는 원소가 상기 암호화된 합집합에 속하는지 여부를 판단하는 멤버 테스트부; 및

상기 집합 연산의 연산식 및 상기 각각의 집합에 속한 원소가 상기 암호화된 합집합에 속하는 지 여부에 기초하여, 상기 집합 연산을 수행하는 집합 연산부를 포함하는

집합 연산 제공 시스템.

청구항 9

제 8 항에 있어서,

상기 집합 연산의 수행을 통해 획득한 상기 연산식의 결과 데이터를 상기 복수의 참여자에게 제공하는 데이터 제공부를 더 포함하는

집합 연산 제공 시스템.

청구항 10

제 8 항에 있어서,

복수의 참여자의 단말로부터 참여자의 집합 데이터를 수신하는 데이터 수신부를 더 포함하는

집합 연산 제공 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 분산된 집합에서 프라이버시를 보호하는 집합 연산 제공 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 프라이버시를 보호하는 집합 연산들에 대한 연구가 다양하고 활발하게 진행되고 있으며, 특히 자신이 가지고 있는 비밀 입력 집합에 대한 어떠한 정보의 노출 없이도 합집합이나 교집합 연산이 가능한 기법들이 연구되고 있다.

[0003] 프라이버시를 보호하는 다양한 집합 연산들은 프라이버시 보존 데이터 마이닝(PPDM, Privacy Preserving Data Mining) 기술에서 유용하게 사용될 수 있지만, 현재까지는 기존 집합 연산에서 가능한 다양한 연산들에 대해서 프라이버시를 보호하는 연구가 부족한 실정이다.

[0004] 프라이버시를 보호하는 다양한 집합 연산들은 프라이버시 보존 데이터 마이닝 기술에서 유용하게 사용될 수 있다. 기존에 제안되었던 프라이버시를 보호하는 집합 연산은 합집합, 교집합, 부분집합 등 일부 연산 집합에 국한된다.

[0005] 이에, 기존 집합 연산에서 가능한 연산들을 모두 포괄하며, 임의의 집합 형태도 프라이버시를 보호하며 얻어낼 수 있는 집합 연산이 필요한 실정이다.

[0006] 이와 관련하여, 한국공개특허 1(출원번호: 2007-0112469, 발명의 명칭: 프라이버시를 보장하는 암호화와 복호화를 이용한 파일공유 방법 및 시스템)은 프라이버시를 보장하는 암호화와 복호화를 이용한 파일공유 방법 및 시스템에 관한 것으로서, 파일 또는 데이터를 공유하는 데 있어서, 사용자의 프라이버시를 보호하기 위해 데이터를 암호화하고 암호화된 데이터를 복호화하는 방법을 제공하고 있다. 하지만, 분산된 집합에서 집합에 속한 데이터에 대한 임의의 집합 연산에 대해서는 개시하고 있지 않다.

[0007] 한편, 한국공개특허 2(출원번호: 2009-0125220, 발명의 명칭: 연관규칙 마이닝에서의 프라이버시 보호 장치 및 방법)는 연관규칙 마이닝에서의 프라이버시 보호 장치 및 방법에 관한 것으로서, 데이터 집합을 알고리즘을 통해서 가상 데이터 집합으로 변환시키는 방법을 제공하고 있다. 하지만, 한국공개특허 2 또한, 집합에 속한 데이터에 대한 임의의 집합 연산에 대해서는 개시하고 있지 않다.

발명의 내용

해결하려는 과제

[0008] 본 발명의 일부 실시예는, 복수의 참여자들의 분산된 비밀 입력 집합들에 대해 복수의 참여자들 간의 프라이버시를 보호할 수 있는 집합 연산을 제공하는 방법을 제공하는 데에 목적이 있다.

[0009] 또한, 본 발명의 일부 실시예는, 복수의 참여자들의 분산된 비밀 입력 집합들에 대해 복수의 참여자들 간의 프라이버시를 보호할 수 있는 집합 연산을 제공하는 시스템을 제공하는 데에 목적이 있다.

과제의 해결 수단

[0010] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따른 집합 연산 시스템이 분산된 집합의 프라이버시를 보호하는 집합 연산을 제공하는 방법은, 복수의 참여자의 협력을 통해, 상기 복수의 참여자가 소유한 각각의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합을 생성하는 단계, 상기 복수의 참여자가 소유한 각각의 집합에 속하는 원소가 상기 암호화된 합집합에 속하는지 여부를 판단하는 단계 및 상기 집합 연산의 연산식 및 상기 각각의 집합에 속한 원소의 상기 암호화된 합집합에 속하는 지 여부에 기초하여, 상기 집합 연산을 수행하는 단계를 포함한다.

[0011] 본 발명의 제 2 측면에 따른 분산된 집합의 프라이버시를 보호하는 집합 연산을 제공하는 집합 연산 제공 시스템은, 복수의 참여자의 협력을 통해, 상기 복수의 참여자가 소유한 각각의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합을 생성하는 암호화 합집합 연산부, 상기 복수의 참여자가 소유한 각각의 집합에 속하는 원소가 상기 암호화된 합집합에 속하는지 여부를 판단하는 멤버 테스트부 및 상기 집합 연산의 연산식 및 상기 각각의 집합에 속한 원소가 상기 암호화된 합집합에 속하는 지 여부에 기초하여, 상기 집합 연산을 수행하는 집합 연산부를 포함한다.

발명의 효과

[0012] 전술한 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 복수의 참여자들의 분산된 비밀 입력 집합들에 대해 복수의 참여자들 간의 프라이버시를 보호할 수 있는 집합 연산을 제공하는 방법을 제공할 수 있다.

[0013] 또한, 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 복수의 참여자들의 분산된 비밀 입력 집합들에 대해 복수의 참여자들 간의 프라이버시를 보호할 수 있는 집합 연산을 제공하는 시스템을 제공할 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 일실시예에 따른 집합 연산 제공 시스템을 설명하기 위한 구성도이다.

도 2는 본 발명의 일실시예에 따른 집합 연산 제공 방법에 있어서, 집합 연산 서버를 도시한 블록도이다.

도 3은 본 발명의 일실시예에 따른 집합 연산 제공 방법을 설명하기 위하여, 집합의 예시를 도시한 도면이다.

도 4는 본 발명의 일실시예에 따른 집합 연산 제공 시스템을 통하여 집합 연산을 제공하는 방법을 설명하기 위한 순서도이다.

도 5는 본 발명의 일실시예에 따른 집합 연산 제공 방법에 있어서, 암호화된 합집합 연산 수행 방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0016] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0017] 이하 첨부된 도면을 참고하여 본 발명을 상세히 설명하기로 한다.

[0018] 도 1은 본 발명의 일실시예에 따른 집합 연산 제공 시스템을 설명하기 위한 구성도이다.

[0019] 본 발명의 일실시예에 따른 집합 연산 제공 시스템은 복수의 참여자의 암호화된 집합에 대한 집합 연산을 수행하기 위하여, 복수의 참여자(100) 및 집합 연산 서버(200)를 포함할 수 있다.

[0020] 복수의 참여자(100)는 자신 및 타 참여자의 프라이버시를 보호할 수 있는 집합 연산을 통하여, 참여자 간에 서로 노출시키고 싶지 않은 데이터에 대한 암호화된 데이터를 타 참여자에게 제공하고, 임의의 집합 연산에 대한 결과를 제공 받을 수 있다. 예를 들어, 복수의 병원 전산 시스템이 복수의 병원에 산재한 질병 데이터를 공유하며, 특정 목적에 의한 가공 데이터를 추출하고자 할 때, 각 병원 전산 시스템은 질병 데이터 또는 환자 데이터가 타 병원에 노출되는 것을 꺼릴 것이다. 이때, 복수의 참여자(병원)는 특정 질병에 걸린 환자들의 프라이버시를 보호하면서, 같은 질병에 걸린 환자 들의 정보를 타 참여자와 공유하기 위해, 본 발명의 일실시예에 따른 집합 연산을 수행할 있다.

[0021] 본 발명의 다른 실시예에 따른 집합 연산 제공 시스템은 네트워크(10)에 연결된 복수의 참여자의 단말(100) 및 집합 연산 서버(200)를 포함할 수 있다.

[0022] 네트워크(10)는 근거리 통신망(Local Area Network; LAN), 광역 통신망(Wide Area Network; WAN) 또는 부가가치 통신망(Value Added Network; VAN) 등과 같은 유선 네트워크나 이동 통신망(mobile radio communication network) 또는 위성 통신망 등과 같은 모든 종류의 무선 네트워크로 구현될 수 있다.

[0023] 복수의 참여자의 단말(100)은 네트워크(10)를 통해 원격지의 서버에 접속할 수 있는 단말로 구현될 수 있다. 상기 단말(100)은 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal

Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말, 스마트폰(smartphone) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다.

[0024] 집합 연산 서버(200)는 참여자의 단말(100)로부터 집합의 원소, 집합을 표현하는 다항식 데이터 및 참여자의 단말(100)에서 선택된 랜덤 데이터 등 집합 연산에 필요한 일체의 데이터를 수신하고, 수신된 데이터에 기초하여 암호화된 합집합 연산, 참여자의 단말(100)로 수신한 집합의 원소가 암호화된 합집합에 속하는지 여부를 판단하는 멤버 테스트 등에 기초하여, 복수의 참여자 단말(100)로부터 제공받은 집합에 대한 다양한 집합 연산을 수행할 수 있다.

[0025] 상술한 바와 같이, 본 발명의 일실시예에 따른 집합 연산 시스템은 네트워크(10)에 연결된 복수의 참여자 단말과의 데이터 송수신을 통해 수행되거나, 또는 단일 시스템으로 구성될 수 있다.

[0026] 도 2는 본 발명의 일실시예에 따른 집합 연산 제공 방법에 있어서, 집합 연산 서버를 도시한 블록도이다.

[0027] 본 발명의 일실시예에 따른 집합 연산 서버(200)는 암호화 합집합 연산부(210), 멤버 테스트부(220), 집합 연산부(230), 데이터 수신부(240) 및 데이터 송신부(250)를 포함할 수 있다.

[0028] 암호화 합집합 연산부(210)는 복수의 참여자의 협력을 통해, 복수의 참여자가 소유한 각각의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합을 생성할 수 있다.

[0029] 암호화 합집합 연산부(210)가 수행하는 작업에 대해 이해를 돕기 위해, 예를 들어, 복수의 참여자에 대해 각각의 참여자를 $P_k(1\leq k\leq n)$라고 하고, 참여자 P_k가 비밀 집합 A_k를 가진다고 하자. A_k는 l_k개의 원소를 가지며, $A_k = \{e_k^1, \ldots, e_k^{\ell_k}\}$와 같이 나타낼 수 있다.

[0030] 또한, $U = A_1 \cup \cdots \cup A_n = \{u_1, \ldots, u_m\}$이고, $\ell' = \ell_1 + \cdots + \ell_n$이라고 가정 하자. 이 때, m은 합집합 U의 원소의 개수이다.

[0031] 상기와 같은 가정하에, 제 1 참여자(P_1)을 제외한 각각의 참여자 P_k $(1\leq k\leq n)$는 다항식 $f_{A_k}(x) = (x - e_k^1)\cdots(x - e_k^{\ell_k})$를 계산하고, $r_k^{\ell}(1 \leqslant \ell \leqslant \ell')$을 랜덤하게 선택하며, $\mathrm{HPE}\cdot \mathrm{enc}_{pk}(f_{A_k}(x))$, $\mathrm{HPE}\cdot \mathrm{enc}_{pk}(r_k^{\ell})(1 \leqslant \ell \leqslant \ell')$와 암호화된 비밀 집합 $\{\mathrm{HPE}\cdot \mathrm{enc}_{pk}(e_k^1), \ldots, \mathrm{HPE}\cdot \mathrm{enc}_{pk}(e_k^{\ell_k})\}$를 제 1 참여자 P_1에게 보낸다.

[0032] 제 1 참여자는 $(\mathrm{HPE}\cdot \mathrm{enc}_{pk}(e_1^i), \mathrm{HPE}\cdot \mathrm{enc}_{pk}(1))(1 \leqslant i \leqslant \ell_1)$을 계산하고, k=2부터 n까지에 대해 아래 [수학식 1]을 계산한다.

수학식 1

[0033] $$\left(\mathrm{HPE}\cdot \mathrm{enc}_{pk}(e_k^j \cdot \left(\prod_{\ell=1}^{k-1} f_{A_\ell}\right)(e_k^j)), \mathrm{HPE}\cdot \mathrm{enc}_{pk}\left(\left(\prod_{\ell=1}^{k-1} f_{A_\ell}\right)(e_k^j)\right)\right)(1 \leqslant j \leqslant \ell_k)$$

[0034] 또한, 제 1 참여자 P_1은 $r_k^{\ell}(1 \leqslant \ell \leqslant \ell')$을 랜덤하게 선택하고, 아래 [수학식 2]의 계산을 수행한다.

수학식 2

[0035] $$(\mathrm{HPE}\cdot \mathrm{enc}_{pk}(a_\ell \cdot \prod_{k=1}^{n} r_k^\ell), \mathrm{HPE}\cdot \mathrm{enc}_{pk}(b_\ell \cdot \prod_{k=1}^{n} r_k^\ell))(1 \leqslant \ell \leqslant \ell')$$

[0036] 여기서 $(\mathrm{HPE}\cdot \mathrm{enc}_{pk}(a_\ell),\ \mathrm{HPE}\cdot \mathrm{enc}_{pk}(b_\ell))$ 은 제 1 참여자 P_1이 계산한 값들을 나타낸 것이다. 즉, $b_l \neq 0$이면, $a_\ell \cdot b_\ell^{-1}$ 은 합집합 원소들 중의 하나이다. 제 1 참여자 P_1은 아래 [수학식 3]을 배포한다.

수학식 3

[0037] $$(X_\ell, Y_\ell) = (\mathrm{HPE}\cdot \mathrm{enc}_{pk}(x_\ell), \mathrm{HPE}\cdot \mathrm{enc}_{pk}(y_\ell))$$

[0038] $$= (\mathrm{HPE}\cdot \mathrm{enc}_{pk}(a_\ell \cdot \prod_{k=1}^{n} r_k^\ell), \mathrm{HPE}\cdot \mathrm{enc}_{pk}(b_\ell \cdot \prod_{k=1}^{n} r_k^\ell))$$

[0039] $$(1 \leqslant \ell \leqslant \ell')$$

[0040] 상기와 같은 과정들을 통해, 모든 참여자 P_k ($1 \leq k \leq n$)는 배포된 값에 대해 셔플 프로토콜(shuffle protocol)을 수행하고, y_l=0인지를 테스트하기 위해 (X_l, Y_l) ($1 \leq l \leq l'$) 중에서 $Y_\ell = \mathrm{HPE}\cdot \mathrm{enc}_{pk}(y_\ell)$ 을 다함께 복호화한다. 만약 $y_l \neq 0$이면, 리스트 Γ에 (X_l, Y_l)를 추가한다.

[0041] 암호화 합집합 연산부(210)는 상기와 같은 과정을 통해, 암호화된 합집합을 생성할 수 있다.

[0042] 멤버 테스트부(220)는 복수의 참여자가 소유한 각각의 집합에 속하는 원소가 암호화된 합집합에 속하는지 여부를 판단할 수 있다.

[0043] 멤버 테스트부(210)가 수행하는 작업에 대해 이해를 돕기 위해 예를 들어, 복수의 참여자에 대해 각각의 참여자를 P_k($1 \leq k \leq n$)라고 하고, 참여자 P_k가 비밀 집합 A_k를 가진다고 하자. A_k는 l_k개의 원소를 가지며, $A_k = \{e_k^1, \ldots, e_k^{\ell_k}\}$와 같이 나타낼 수 있다. 각각의 참여자 P_k($1 \leq k \leq n$)는 $C_k = E(A_i)||(X_j, Y_j)$를 가지며, 여기서 $E(A_i) = \{\mathrm{HPE}\cdot \mathrm{enc}_{pk}(e_i^1), \ldots, \mathrm{HPE}\cdot \mathrm{enc}_{pk}(e_i^{\ell_i})\}$이고, $(X_j, Y_j) = (\mathrm{HPE}\cdot \mathrm{enc}_{pk}(x_j), \mathrm{HPE}\cdot \mathrm{enc}_{pk}(y_j))$이다.

[0044] 참여자 P_i가 x_j/y_j가 A_i의 원소인지 아닌지를 알기 원한다고 가정한다. i번째 참여자 P_i를 제외한 각각의 참여자 P_k ($1 \leq k \leq n$)는 r_k ($1 \leq l \leq l'$)를 랜덤하게 선택하고, i번째 참여자 P_i에게 $\mathrm{HPE}\cdot \mathrm{enc}_{pk}(r_k)$ 를 보낸다. i번째 참여자 P_i는 r_i와 R을 랜덤하게 선택하고, 아래 [수학식 4]에서의 B를 계산하여 배포한다.

수학식 4

[0045] $$B = \mathrm{HPE}\cdot \mathrm{enc}_{pk}\left(\prod_{\ell=1}^{\ell_i}(y_j \cdot e_i^\ell - x_j) \cdot \prod_{k=1}^{n} r_k + R\right)$$

[0046] 그러면 모든 참여자는 아래 [수학식 5]에서의 b를 얻기 위해 B를 다함께 복호화한다.

수학식 5

[0047] $$b = \prod_{\ell=1}^{\ell_i} (y_j \cdot e_i^{\ell} - x_j) \cdot \prod_{k=1}^{n} r_k + R$$

[0048] 만약 b=R이면 i번째 참여자 P_i는 1을 출력하고, 아니면 0을 출력한다. 한편, i번째 참여자 P_i를 제외한 다른 어떤 참여자들은 어떠한 정보도 얻지 못한다.

[0049] 멤버 테스트부(220)는 상기와 같은 과정을 통해, 특정 원소가 암호화된 집합에 속하는 지 여부에 대한 판단을 할 수 있다.

[0050] 집합 연산부(230)는 상기 암호화 합집합 연산부(210)에 의한 암호화된 합집합 및 집합 연산의 연산식에 기초하여 다양한 집합 연산을 수행할 수 있다.

[0051] 데이터 수신부(240)는 복수의 참여자의 단말로부터 참여자의 집합 데이터를 수신할 수 있다.

[0052] 데이터 제공부(250)는 상기 집합 연산의 수행을 통해 획득한 상기 연산식의 결과 데이터를 상기 복수의 참여자에게 제공할 수 있다.

[0053] 도 3은 본 발명의 일실시예에 따른 집합 연산 제공 방법을 설명하기 위하여, 집합의 예시를 도시한 도면이다.

[0054] 본 발명의 일실시예에 따른 집합 연산 제공 방법에 있어서, 복수의 집합에 연산을 설명하기 위해, 아래 [수학식 6]을 만족시키는 집합 SF를 찾는 과정을 예로 들기로 한다.

수학식 6

[0055] $$S_F = (S_{1,1} \cap \cdots \cap S_{1,t_2}) \cup \cdots \cup (S_{t_1,1} \cap \cdots \cap S_{t_1,t_2}) \text{ where } S_{i,j} \in \{A_1, \ldots, A_n, \overline{A_1}, \ldots, \overline{A_n}\}$$

[0056] 상기 [수학식 6]에서 A_k는 참여자 P_k가 소유한 집합을 의미하며, 여집합(complement set) $\overline{A_k}$는 $\overline{A_k} = (A_1 \cup \cdots \cup A_n) - A_k$ 와 같이 정의할 수 있다.

[0057] 본 발명의 일실시예에 따른 집합 연산 제공 방법에서, 복수의 참여자(P_k)는 자신이 소유한 집합(A_k)에 대한 정보만 알 수 있으며, 타 참여자가 소유한 집합($\overline{A_k}$)에 대한 정보는 알 수 없다. 복수의 모든 참여자는 분산된 집합에 대하여, 프라이버시를 보호하는 집합 연산을 수행하기 위해 상호 협력할 수 있다.

[0058] 보다 상세한 설명을 위해, 도 3에 도시된 집합 A1, A2, A3를 예를 들어, 집합 연산 과정에 대해 이하에서 설명한다.

[0059] 도3에서는 예를 들어, 참여자 P1, P2 및 P3가 각각 소유하고 있는 집합 A1, A2 및 A3에 대해서, 하나의 집합에만 속하는 원소를 추출하는 연산을 수행한다.

[0060] 먼저, 참여자 P1, P2 및 P3는 암호화되고, 섞인(suffled) 합집합의 튜플(tuple)을 아래 [수학식 7]과 같이 생성한다.

수학식 7

[0061] $$(X_j, Y_j) = (\text{HPE} \cdot \text{enc}_{pk}(x_j), \text{HPE} \cdot \text{enc}_{pk}(y_j)) \; (1 \leqslant j \leqslant 5)$$

[0062] where, $\frac{x_j}{y_j} \in U$

[0063] 참여자들은 상기 [수학식 7]에서의 (x_j, y_j) 값을 알지 못하며, (x_j, y_j)는 아래 [표 1]과 같다.

표 1

[0064]

x_j	$3 \cdot R_1$	$1 \cdot R_2$	$4 \cdot R_3$	$2 \cdot R_4$	$5 \cdot R_5$
y_j	R_1	R_2	R_3	R_4	R_5

[0065] 이후, 각 참여자 P_k는 집합 $A_k = \{e_k^1, \ldots, e_k^{\ell_k}\}$에 대하여, 멤버 테스트를 수행한다. 만약 참여자 P_k가 $\frac{x_j}{y_j}$와 같은 값인 원소를 갖는다면, b_k^j의 값을 1로 설정하고, 그 결과는 아래 [표 2]와 같다.

표 2

[0066]

$\frac{x_j}{y_j}$	3	1	4	2	5
b_1^j	1	1	0	1	0
b_2^j	0	1	1	1	0
b_3^j	0	0	1	1	1

[0067] 이후, 각 참여자 P_k는 $T_k^{i,j} = \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b_k^{i,j})(1 \leqslant i \leqslant 3, 1 \leqslant j \leqslant 5)$에 대하여 계산을 수행한다. 만약, $1 \leqslant i \leqslant 3$인 i에 대하여, $A_k \in \{S_{i,1}, S_{i,2}, S_{i,3}\}$이라면, P_k는 $T_k^{i,j} = \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b_k^j)(1 \leqslant j \leqslant 5)$로 계산한다. 한편, $\overline{A_k} \in \{S_{i,1}, S_{i,2}, S_{i,3}\}$이라면, $T_k^{i,j} = \mathrm{HPE} \cdot \mathrm{enc}_{pk}(\tilde{b}_k^j)(1 \leqslant j \leqslant 5)$와 같이 계산한다. 그렇지 않을 경우, P_k는 $T_k^{i,j} = \mathrm{HPE} \cdot \mathrm{enc}_{pk}(0)(\ddot{1} \leqslant j \leqslant 5)$와 같이 계산을 수행한다.

[0068] 상기 과정을 통해 계산된 는 아래 [표 3]과 같다.

표 3

[0069]

$b_1^{i,j}$	0	0	1	0	1	0	0	1	0	1	1	1	0	1	0
$b_2^{i,j}$	1	0	0	0	1	0	1	1	1	0	1	0	0	0	1
$b_3^{i,j}$	0	0	1	1	1	1	1	0	0	0	1	1	0	0	0

[0070] 이후, 각 참여자 P_k는 $r_k^j(1 \leqslant j \leqslant 5)$를 랜덤하게 선택하고, $T_k^{i,j}$와 $\mathrm{HPE} \cdot \mathrm{enc}_{pk}(r_k^j)(1 \leqslant i \leqslant 3, 1 \leqslant j \leqslant 5)$ 값을 중계(broadcasting)한다.

[0071] 각 참여자 P_k는 중계된 값을 받은 후, 아래 [수학식 8]과 같은 계산을 수행한다.

수학식 8

[0072] $$T^{i,j} = \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b^{i,j}) = \mathrm{HPE} \cdot \mathrm{mult}(T_1^{i,j}, T_2^{i,j}, T_3^{i,j})$$

[0073] $$= \mathrm{HPE} \cdot \mathrm{mult}(\mathrm{HPE} \cdot \mathrm{enc}_{pk}(b_1^{i,j}), \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b_2^{i,j}), \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b_3^{i,j}))$$

[0074] $$= \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b_1^{i,j} \cdot b_2^{i,j} \cdot b_3^{i,j})$$

[0075] 상기 과정을 통해서 계산된 $\hat{b}^j = b^j \cdot \hat{R}_j \text{ for } 1 \leqslant j \leqslant 5$ 는 아래 [표 4]와 같다.

표 4

[0076]

b^j	1	0	0	0	1

[0077] 이후, 각 참여자 P_k는 아래 [수학식 9]와 같은 계산을 수행한다.

수학식 9

[0078] $$T^j = \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b^j) = \mathrm{HPE} \cdot \mathrm{add} \quad (T^{1,j}, T^{2,j}, T^{3,j})$$

[0079] $$= \mathrm{HPE} \cdot \mathrm{add} \quad (\mathrm{HPE} \cdot \mathrm{enc}_{pk}(b^{1,j}), \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b^{2,j}), \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b^{3,j}))$$

[0080] $$= \mathrm{HPE} \cdot \mathrm{enc}_{pk}(b^{1,j} + b^{2,j} + b^{3,j}) \; (1 \leqslant j \leqslant 5)$$

[0081] 상기 과정을 통해 계산된 는 아래 [표 5]와 같다.

표 5

[0082]

$\hat{b}^j$	$1 \cdot \hat{R}_1$	$0 \cdot \hat{R}_2$	$0 \cdot \hat{R}_3$	$0 \cdot \hat{R}_4$	$1 \cdot \hat{R}_5$

[0083] 이후, 모든 참여자들은 $\hat{T}^j = \mathrm{HPE} \cdot \mathrm{enc}_{pk}(\hat{b}^j)$ 인 $\hat{b}^j$ 를 얻기 위해 $\hat{T}^j (1 \leqslant j \leqslant 5)$ 를 협력적으로 복호화한다. 만약, $\hat{b}^j \neq 0$ 라면, 모든 참여자들은 $\frac{x_j}{y_j}$ 를 계산하기 위해 (X_j, Y_j) 를 복호화하고, $\frac{x_j}{y_j}$ 를 결과 집합인 S_{R_1}에 덧붙인다. 만약, $\hat{b}^j \neq 0$ 라면 모든 참여자들은 (X_j, Y_j) 를 복호화하지 않는다. 결과적으로, 모든 참여자들은 $S_{R_1} = \{3, 5\}$ 를 얻게 된다.

[0084] 도 4은 본 발명의 일실시예에 따른 집합 연산 제공 시스템을 통하여 집합 연산을 제공하는 방법을 설명하기 위한 순서도이고, 도 5는 본 발명의 일실시예에 따른 집합 연산 제공 방법에 있어서, 암호화된 합집합 연산 수행 방법을 설명하기 위한 순서도이다.

[0085] 본 발명의 일실시예에 따른 집합 연산 제공 방법은 복수의 참여자로부터 집합 연산에 필요한 집합, 집합의 다항

식 표현 및 랜덤 데이터 등의 암호화된 데이터를 수집하여, 집합 연산을 수행할 수 있다. 또한, 본 발명의 다른 실시예에 따른 집합 연산 제공 방법은 복수의 참여자의 단말로부터 집합 연산에 필요한 집합, 집합의 다항식 표현 및 랜덤 데이터 등의 암호화된 데이터를 수신하여, 집합 연산을 수행할 수도 있다. 즉, 집합 연산 제공 시스템은 네트워크(10)로 연결된 복수의 참여자 단말, 예를 들어 병원 전산 서버 등에서 환자의 진단 데이터 등을 수신하여, 특정 질병에 대한 데이터를 수집 가공하는 데에 활용될 수 있으며, 또는 집합 연산 시스템과 연결된 입력 수단을 통해 상술한 집합 연산에 필요한 데이터를 입력하고, 입력된 피 연산 데이터에 대한 집합 연산을 수행하는 데에 활용될 수도 있다.

[0086] 먼저, 집합 연산 시스템은 복수의 참여자의 협력을 통해, 복수의 참여자가 소유한 각각의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합을 생성한다(S2100).

[0087] 본 발명의 일실시예에 따른 암호화된 합집합 연산은 복수의 참여자가 자신 및 타 참여자의 프라이버시를 보호하면서, 특정 집합 연산을 수행하기 위하여, 집합 연산에 참여하는 복수의 참여자의 집합 데이터를 통합하는 역할을 수행한다.

[0088] 먼저, 제 1 참여자를 제외한 복수의 참여자가 각각 소유한 집합을 다항식의 형태로 표현하고, 랜덤 데이터를 선택한다(S2110).

[0089] 다음으로, 제 1 참여자를 제외한 복수의 참여자가 상기 다항식, 상기 랜덤 데이터 및 상기 복수의 참여자가 각각 소유한 집합에 대하여 암호화된 데이터를 상기 제 1 참여자에게 전달한다(S2120).

[0090] 다음으로, 상기 제 1 참여자가 자신의 소유한 집합 및 상기 제 1 참여자를 제외한 복수의 참여자로부터 수신한 암호화된 데이터에 기초하여, 암호화된 합집합을 생성한다(S2130).

[0091] 다음으로, 집합 연산 시스템은 복수의 참여자가 소유한 각각의 집합에 속하는 원소가 암호화된 합집합에 속하는지 여부를 판단한다(S2200).

[0092] 다음으로, 집합 연산 시스템은 집합 연산의 연산식 및 각각의 집합에 속한 원소가 암호화된 합집합에 속하는 지 여부에 기초하여, 집합 연산을 수행한다(S2300).

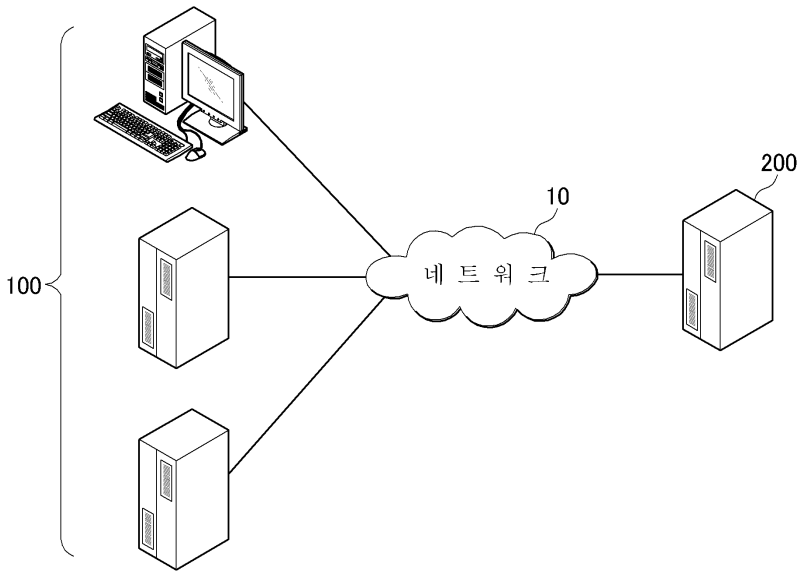
[0093] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0094] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

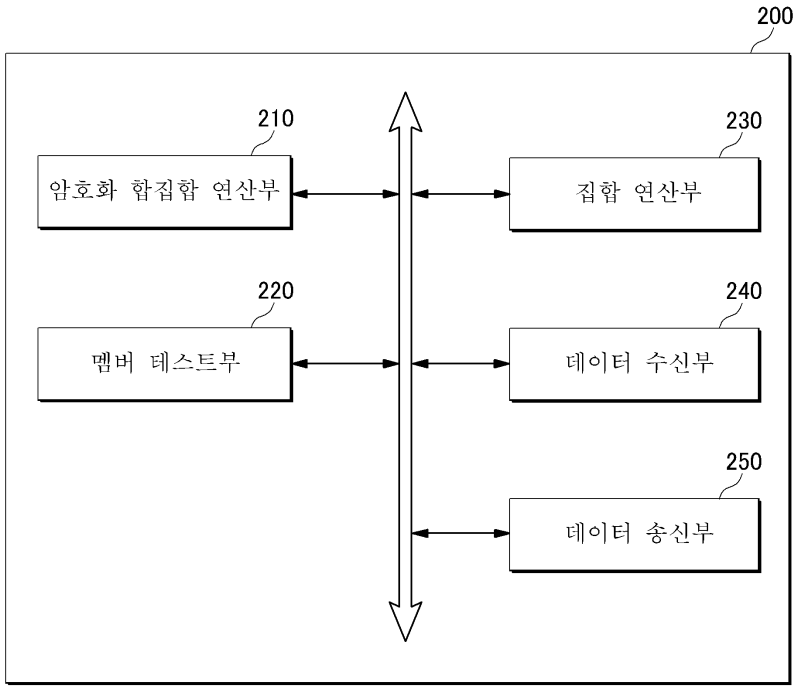
[0095] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

도면

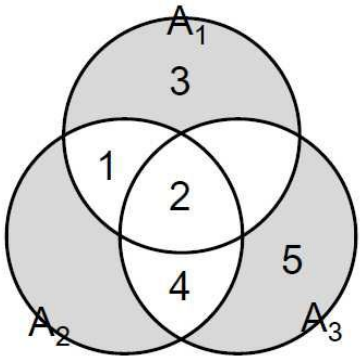
도면1


100
10
네 트 워 크
200

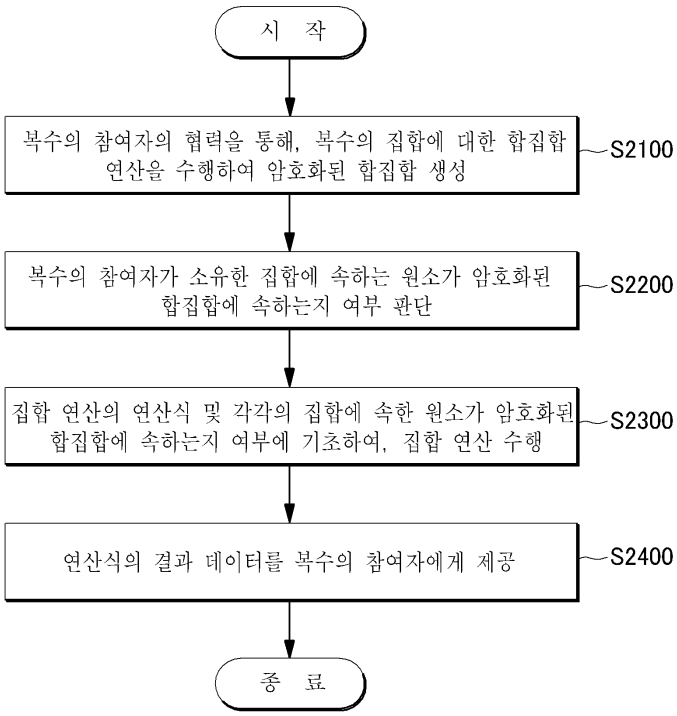
도면2


200
210
암호화 합집합 연산부
230
집합 연산부
220
멤버 테스트부
240
데이터 수신부
250
데이터 송신부

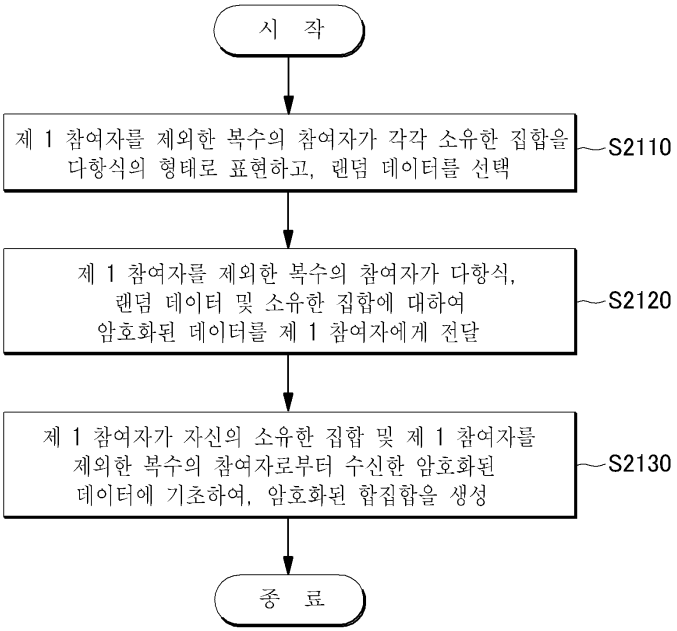
도면3


A1
3
1
2
5
4
A2
A3

도면4


시 작
복수의 참여자의 협력을 통해, 복수의 집합에 대한 합집합 연산을 수행하여 암호화된 합집합 생성
S2100
복수의 참여자가 소유한 집합에 속하는 원소가 암호화된 합집합에 속하는지 여부 판단
S2200
집합 연산의 연산식 및 각각의 집합에 속한 원소가 암호화된 합집합에 속하는지 여부에 기초하여, 집합 연산 수행
S2300
연산식의 결과 데이터를 복수의 참여자에게 제공
S2400
종 료

도면5


시 작
제 1 참여자를 제외한 복수의 참여자가 각각 소유한 집합을 다항식의 형태로 표현하고, 랜덤 데이터를 선택
S2110
제 1 참여자를 제외한 복수의 참여자가 다항식, 랜덤 데이터 및 소유한 집합에 대하여 암호화된 데이터를 제 1 참여자에게 전달
S2120
제 1 참여자가 자신의 소유한 집합 및 제 1 참여자를 제외한 복수의 참여자로부터 수신한 암호화된 데이터에 기초하여, 암호화된 합집합을 생성
S2130
종 료