(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0022818
(43) 공개일자 2023년02월16일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01) *H04L 67/52* (2022.01)
H04L 9/00 (2022.01)
(52) CPC특허분류
H04L 63/107 (2013.01)
H04L 67/52 (2022.05)
(21) 출원번호 10-2022-0098859
(22) 출원일자 2022년08월08일
심사청구일자 2022년08월08일
(30) 우선권주장
1020210104487 2021년08월09일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
윤지원
서울특별시 용산구 한강대로43길 8, 102동 1401호
유준수
서울특별시 송파구 백제고분로36나길 28-1, 3층
홍미연
경기도 성남시 분당구 내정로 152, 130동 901호
(74) 대리인
김등용

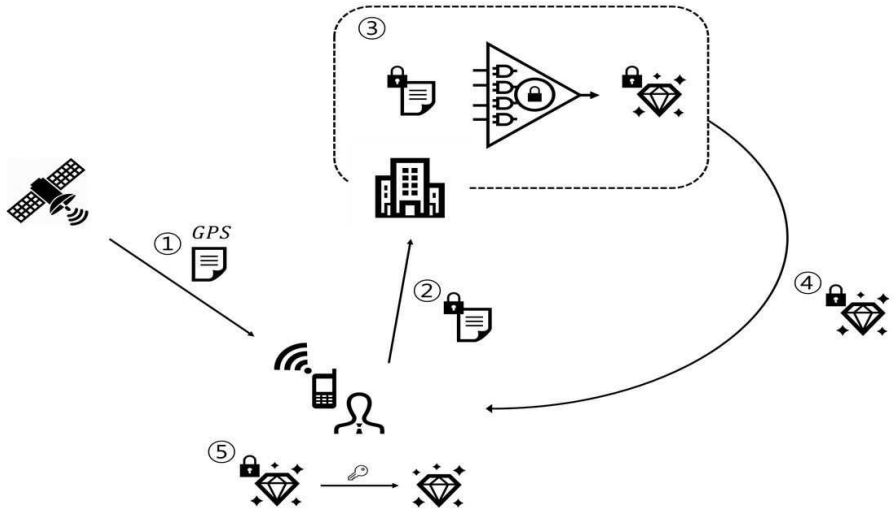
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **암호화된 사용자의 위치 정보를 이용한 위치 기반 서비스 제공 방법**

(57) 요 약

암호화된 사용자의 위치 정보를 이용한 위치 기반 서비스 제공 방법이 개시된다. 상기 위치 기반 서비스 제공 방법은 적어도 프로세서를 포함하는 위치 기반 서비스 제공 장치에 의해 수행되고, 사용자 단말로부터 암호화된 사용자 위치 정보를 수신하는 단계, 상기 암호화된 사용자 위치 정보와 미리 저장된 암호화된 위치 정보들 각각에 대한 동형암호 동치 연산을 수행하는 단계, 동형암호 동치 연산의 결괏값 각각과 미리 저장된 암호화된 위치 기반 서비스들 중 대응되는 암호화된 위치 기반 서비스에 대하여 비트마다 AND 연산을 수행하는 단계, 및 AND 연산의 수행 결과값들에 대하여 비트마다 XOR 연산을 수행하는 단계를 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/008 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711134646
과제번호	2021-0-00558-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D,정보화)
연구과제명	동형암호 기술을 활용한 국가통계 분석 시스템 개발
기 여 율	1/1
과제수행기관명	(주)마크애니
연구기간	2021.04.01 ~ 2021.12.31

명 세 서

청구범위

청구항 1

적어도 프로세서를 포함하는 위치 기반 서비스 제공 장치에 의해 수행되는 위치 기반 서비스 제공 방법에 있어서,

사용자 단말로부터 암호화된 사용자 위치 정보를 수신하는 단계;

상기 암호화된 사용자 위치 정보와 미리 저장된 암호화된 위치 정보들 각각에 대한 동형암호 동치 연산을 수행하는 단계;

동형암호 동치 연산의 결괏값 각각과 미리 저장된 암호화된 위치 기반 서비스들 중 대응되는 암호화된 위치 기반 서비스에 대하여 비트마다 AND 연산을 수행하는 단계; 및

AND 연산의 수행 결과값들에 대하여 비트마다 XOR 연산을 수행하는 단계를 포함하는 위치 기반 서비스 제공 방법.

청구항 2

제1항에 있어서,

상기 XOR 연산의 수행 결괏값을 상기 사용자 단말로 송신하는 단계를 더 포함하는,

위치 기반 서비스 제공 방법.

청구항 3

제1항에 있어서,

상기 암호화된 사용자 위치 정보는 비트 기반의 완전동형암호 기법을 이용하여 암호화된,

위치 기반 서비스 제공 방법.

청구항 4

제3항에 있어서,

상기 암호화된 사용자 위치 정보는 LWE(Learning With Error, LWE) 또는 RLWE(Ring LWE) 기반의 암호문인,

위치 기반 서비스 제공 방법.

청구항 5

제1항에 있어서,

상기 동형암호 동치 연산은 두 입력의 대응되는 비트들에 대한 XNOR 연산의 결과들에 대한 AND 연산을 나타내는,

위치 기반 서비스 제공 방법.

청구항 6

제1항에 있어서,

상기 암호화된 사용자 위치 정보는 위도에 대한 암호문과 경도에 대한 암호문을 포함하는,

위치 기반 서비스 제공 방법.

청구항 7

적어도 프로세서를 포함하는 위치 기반 서비스 제공 장치에 의해 수행되는 위치 기반 서비스 제공 방법에 있어서,

사용자 단말로부터 암호화된 사용자 위치 정보를 수신하는 단계;

상기 암호화된 사용자 위치 정보와 미리 정해진 위치 구간들 각각에 대한 동형암호 비교 연산을 수행하는 단계;

상기 동형암호 비교 연산의 결괏값 각각과 미리 정해진 암호화된 위치 기반 서비스들 중 대응되는 암호화된 위치 기반 서비스에 대하여 비트마다 AND 연산을 수행하는 단계; 및

AND 연산의 결과값들에 대하여 비트마다 XOR 연산을 수행하는 단계를 포함하는 위치 기반 서비스 제공 방법.

청구항 8

제7항에 있어서,

상기 동형암호 비교 연산을 수행하는 단계는,

상기 미리 정해진 위치 구간들 각각에 대하여,

상기 암호화된 사용자 위치 정보와 위치 구간의 하한에 대한 암호문에 대한 '크다' 비교 연산을 수행하는 단계;

상기 암호화된 사용자 위치 정보와 상기 위치 구간의 상한에 대한 암호문에 대한 '작다' 비교 연산을 수행하는 단계; 및

상기 '크다' 비교 연산의 결괏값과 상기 '작다' 비교 연산의 결괏값에 대하여 AND 연산을 수행하는 단계를 포함하는,

위치 기반 서비스 제공 방법.

청구항 9

제7항에 있어서,

상기 XOR 연산의 수행 결괏값을 상기 사용자 단말로 송신하는 단계를 더 포함하는,

위치 기반 서비스 제공 방법.

청구항 10

제7항에 있어서,

상기 암호화된 사용자 위치 정보는 비트 기반의 완전동형암호 기법을 이용하여 암호화된,

위치 기반 서비스 제공 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 암호화된 사용자의 위치 정보를 복호화하지 않고, 암호화된 사용자의 위치 정보를 이용하여 사용자에게 원하는 서비스를 제공할 수 있는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 동형암호(Homomorphic Encryption, HE)는 암호화된 데이터를 복호화하지 않고 암호화된 데이터 간의 연산을 가능하게 하는 암호 기술이다. 동형암호는 크게 정수/실수 기반의 동형암호 기법과 암호화된 게이트 설계를 기반으로 암호화된 회로를 구성하는 방법으로 나뉜다.

[0003] 위치 기반 서비스(Location-Based Service, LBS)를 제공하기 위해서, 각 개인에게 개인정보 제공 동의를 받거나 위치 데이터의 사용에 대한 동의를 받아야 한다. 이와 관련하여, 기존 GPS 시스템의 가장 큰 문제점은 사용자와 클라우드가 동일한 암호키(또는 암호화키)를 공유하면서 클라우드에게 사용자의 개인 위치 정보에 대한 접근을 허용하는 것이다. 클라우드는 수집한 개인 위치 정보를 사용자의 동의 없이 악용하여 금전적인 이득을 얻는 등

불법적으로 사용할 수 있다.

[0004] 도 1은 현재 제공되는 위치 기반 서비스의 제공 방법을 설명하기 위한 개념도이다. 도 1을 참조하면, 위치 기반 서비스를 제공받기 위해서는 다음 단계들이 수행되어야 한다.

[0005] ① 사용자는 인공위성으로부터 GPS 데이터를 수신한다.

[0006] ② 사용자는 원하는 위치 기반 서비스를 제공받기 위해, 키교환 프로토콜을 수행하여 특정 기업(또는 정부)과 암호키를 공유한다.

[0007] ③ 사용자는 클라우드와 공유한 암호키(k)를 이용하여 개인위치정보(D_A)를 암호화하고($Enc_k(D_A)$), 암호화된 개인위치정보($Enc_k(D_A)$)를 클라우드에 전송한다.

[0008] ④ 클라우드는 사용자의 암호키를 이용하여 암호화된 개인위치정보($Enc_k(D_A)$)를 복호화한다. 여기서, 클라우드는 이 정보를 수집하여 사용자의 위치 정보를 악용할 수 있다.

[0009] ⑤ 클라우드는 비식별화되지 않은 사용자의 위치 정보를 이용하여 사용자의 위치에 따른 서비스를 찾는다.

[0010] ⑥ 클라우드는 사용자의 암호키로 서비스를 암호화하고, 암호화된 서비스를 사용자에게 전송한다.

[0011] ⑦ 사용자는 본인의 암호키로 암호화된 서비스를 복호화하여 원하는 서비스를 얻는다.

[0012] 상술한 방법에 의할 경우, 사용자의 위치 정보는 클라우드에 노출되고, 악용될 가능성이 존재한다. 이에, 본 발명에서는 사용자의 개인위치정보를 노출하지 않으면서, 클라우드로부터 원하는 정보(또는 서비스)를 얻을 수 있는 방법을 제안하고자 한다.

발명의 내용

해결하려는 과제

[0013] 본 발명이 이루고자 하는 기술적인 과제는 사용자의 개인위치정보를 노출시키지 않으면서, 사용자의 개인위치정보에 대응하는 위치 기반 서비스를 제공하는 방법 및 장치를 제공하는 것이다.

과제의 해결 수단

[0014] 본 발명의 일 실시예에 따른, 암호화된 사용자의 위치 정보를 이용한 위치 기반 서비스 제공 방법은 적어도 프로세서를 포함하는 위치 기반 서비스 제공 장치에 의해 수행되고, 사용자 단말로부터 암호화된 사용자 위치 정보를 수신하는 단계, 상기 암호화된 사용자 위치 정보와 미리 저장된 암호화된 위치 정보들 각각에 대한 동형암호 동치 연산을 수행하는 단계, 동형암호 동치 연산의 결괏값 각각과 미리 저장된 암호화된 위치 기반 서비스들 중 대응되는 암호화된 위치 기반 서비스에 대하여 비트마다 AND 연산을 수행하는 단계, 및 AND 연산의 수행 결과값들에 대하여 비트마다 XOR 연산을 수행하는 단계를 포함한다.

[0015] 본 발명의 다른 실시예에 따른, 암호화된 사용자의 위치 정보를 이용한 위치 기반 서비스 제공 방법은 적어도 프로세서를 포함하는 위치 기반 서비스 제공 장치에 의해 수행되고, 사용자 단말로부터 암호화된 사용자 위치 정보를 수신하는 단계, 상기 암호화된 사용자 위치 정보와 미리 정해진 위치 구간들 각각에 대한 동형암호 비교 연산을 수행하는 단계, 상기 동형암호 비교 연산의 결괏값 각각과 미리 정해진 암호화된 위치 기반 서비스들 중 대응되는 암호화된 위치 기반 서비스에 대하여 비트마다 AND 연산을 수행하는 단계, 및 AND 연산의 결과값들에 대하여 비트마다 XOR 연산을 수행하는 단계를 포함한다.

발명의 효과

[0016] 본 발명의 일 실시예에 따른, 암호화된 사용자의 위치 정보를 이용한 위치 기반 서비스 제공 방법 및 장치에 의할 경우, 클라우드 사용자에게 데이터 사용에 대한 동의를 구하는 절차를 생략하고, 사용자의 위치 데이터를 이용할 수 있어 효율성을 높일 수 있다.

[0017] 또한, 사용자는 민감한 개인 위치 정보를 노출하지 않고도 원하는 위치 기반 서비스를 얻을 수 있다.

[0018] 또한, 사용자는 오로지 개인의 위치 데이터를 암호화하여 클라우드로 전송하고, 클라우드는 사용자가 원하는 위치 기반 서비스를 암호 회로를 통해 연산하여 사용자에게 돌려주면, 사용자는 이를 복호화하여 원하는 서비스를

얻는 등의 간단한 프로토콜을 이용하여 발명을 구현할 수 있다.

[0019] 또한, 제안하는 암호 회로는 병렬처리가 가능하여, 처리량(throughput)을 높여 처리 속도를 높일 수 있다.

[0020] 또한, 위치 범위를 조절함에 따라, 제공하는 서비스에 대한 속도를 제어할 수 있고 다양한 서비스에 유연하게 대철할 수 있다.

도면의 간단한 설명

[0021] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 현재 제공되는 위치 기반 서비스의 제공 방법을 설명하기 위한 개념도이다.

도 2는 본 발명의 일 실시예에 따른, 암호화된 사용자의 위치 정보를 이용한 서비스 제공 방법을 설명하기 위한 개념도이다.

도 3은 두 암호문 간 동치 연산을 설명하기 위한 도면이다.

도 4는 도 3에 도시된 동치 연산을 이용한 위치 기반 서비스를 설명하기 위한 도면이다.

도 5는 도 3에 도시된 동치 연산을 이용한, 일반적인 동형암호 동치 연산 알고리즘 기반의 위치 기반 서비스를 설명하기 위한 도면이다.

도 6은 동형암호 비교 연산을 설명하기 위한 도면이다.

도 7은 대소 비교 연산을 이용한 위치 기반 서비스를 설명하기 위한 도면이다.

도 8은 일반적인 대소 비교 연산을 이용한 위치 기반 서비스를 설명하기 위한 도면이다.

도 9는 본 발명의 일 실시예에 따른 위치 기반 서비스 제공 시스템을 설명하기 위한 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0022] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시예들에 한정되지 않는다.

[0023] 본 발명의 개념에 따른 실시예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0024] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0025] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0026] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0027] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이

속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0028] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0029] 도 2는 본 발명의 일 실시예에 따른, 암호화된 사용자의 위치 정보를 이용한 서비스 제공 방법을 설명하기 위한 개념도이다.

[0030] 위치 기반 서비스 제공 방법 등으로 명명될 수도 있는 서비스 제공 방법의 대략적인 과정은 다음과 같다.

[0031] ① 사용자 단말은 개인위치정보(D_A)를 인공위성(또는 GPS 시스템)으로부터 수신할 수 있다. 여기서, 사용자 단말은 적어도 프로세서(Processor) 및/또는 메모리(Memory)를 포함하는 컴퓨팅 장치(Computing device)를 의미할 수 있다. 또한, GPS 시스템으로부터 위치 정보를 수신할 수 없는 실내 환경에서는, WIFI 신호가 수신될 수 있고, 사용자 단말은 수신된 WIFI 신호를 이용하여 사용자의 위치 정보를 추출(또는 생성)할 수도 있다.

[0032] ② 사용자 단말은 개인위치정보를 본인의 암호키(k)로 암호화($Enc_k(D_A)$)하고, 정보, 공공기관, 사기업 등과 같이 소정의 서비스(예컨대, 위치 기반 서비스)를 제공하는 기관이 운영하는 서버(예컨대, 클라우드 서버로써, 위치 기반 서비스 제공 서버나 위치 기반 서비스 장치 등으로 명명될 수 있음)로 암호화된 개인위치정보를 전송한다.

[0033] ③ 클라우드 서버는 사용자의 암호화된 비식별 데이터($Enc_k(D_A)$)를 수신하여 암호 회로를 연산한다. 이때, 클라우드 서버는 사용자의 개인위치정보 데이터가 암호화되어 있어 사용자의 위치를 알 수 없다. 여기서, 암호 회로는 사용자의 위치에 따른 서비스(S_A)를 암호화 상태($Enc_k(S_A)$)로 출력한다. 즉, 클라우드 서버는 미리 정해진 연산 동작을 통해 암호화된 위치 기반 서비스($Enc_k(S_A)$)를 도출할 수 있다.

[0034] ④ 클라우드 서버는 암호화 상태에 있는 사용자가 원하는 서비스($Enc_k(S_A)$)를 사용자 단말로 전송한다.

[0035] ⑤ 사용자 단말은 본인이 원했던 서비스(S_A)를 암호키(k)로 복호화(해독)하여 이용할 수 있다.

[0036] 따라서, 본 발명에서 가장 큰 특징은, 정부, 공공기관, 사기업 등과 같은 소정의 서비스를 제공하는 기관(또는 클라우드 서버)은 사용자의 개인위치정보와 개인위치정보에 해당하는 서비스(S_A)에 대해 전혀 알 수 없지만, 사용자가 원하는 서비스를 암호 회로를 이용하여 도출한 후 제공할 수 있다는 것이다.

[0037] 본 발명에서는 1) 동형암호 동치 연산 알고리즘 기반의 위치 기반 서비스 제공 방법과 2) 동형암호 비교 연산 알고리즘 기반의 위치 기반 서비스 제공 방법을 제안한다. 우선, 비트 기반의 완전동형암호 기법을 설명한 후 1) 동형암호 동치 연산 알고리즘 기반의 위치 기반 서비스 제공 방법과 2) 동형암호 비교 연산 알고리즘 기반의 위치 기반 서비스 제공 방법을 설명하기로 한다.

[0038] 본 발명에서는 비트 기반의 완전동형암호(Bitwise Fully Homomorphic Encryption) 기법을 이용한다. 또한, 본 발명에서는 4개의 동형암호 논리 게이트(XOR, AND, XNOR, Mux)를 이용한다. 비트 기반의 완전동형암호 기법에 대하여는 기존에 널리 알려져 있기 때문에, 이에 대한 상세한 설명은 생략하기로 한다.

[0039] 암호문(c)은 $c=(c_{l-1}, c_{l-2}, \cdots, c_0)$와 같이 l-비트로 표현(암호화)된다. 여기서, c_i는 한 개의 비트(x_i)가 암호화된 것을 의미하고, x는 평문을 의미하고, 평문을 바이너리로 표현하면 $x=(x_{l-1}, x_{l-2}, \cdots, x_0)$이 된다. 따라서, 암호문(c)의 비트들 각각은 평문(x)의 비트들 각각에 대응되는 암호문이다.

[0040] 암호문의 각 원소 c_i는 LWE(Learning With Error) 또는 RLWE(Ring LWE) 기반의 암호문이다. 즉, 각각의 랜덤한 LWE 샘플들에 대해 (잡음이 더해져) 암호화되어 있는 암호문이다.

[0041] 암호문 간의 연산(ex. 동형암호 논리 게이트)이 행해지면, 출력되는 암호문은 기존의 암호문보다 잡음이 더해져 출력된다. 예를 들어, 완전동형암호 내에서 동형암호 논리 게이트는 입력 값으로 암호문 c_i, c_i' 를 입력받아서, c*의 암호화된 결괏값을 산출한다. 여기서, c*는 c_i, c_i' 보다 잡음을 더 많이 갖은 채로 출력된다. 암호문이

일정 수준 이상의 잡음을 갖게 되면, 암호문을 복호화해도 정확한 값을 갖을 수 없게 된다. 따라서, 더 많은 연산을 계속 수행하기 위해 암호문을 부트스트랩(bootstrap, 잡음 제거)하게 된다. 위에서 c*에 대해 부트스트랩을 적용하여, 잡음을 어느 정도 제거하고 다시 또 c*에 연산(논리 회로)을 수행한다. 따라서, 본 발명에서는 암호문을 대상으로 하는 연산 결과에 대한 부트스트랩 동작을 포함할 수 있다.

[0042] 1) 동형암호 동치 연산 알고리즘 기반의 위치 기반 서비스 제공 방법

[0043] 도 3은 두 암호문 간 동치 연산을 설명하기 위한 도면이다.

[0044] 도 3을 참조하면, 동치 연산은 도 3과 같이 구성될 수 있다. 즉, 동치 연산은 XNOR 연산과 AND 연산을 포함한다. 구체적으로, 동치 연산은 두 암호문에 포함된 대응 비트에 대한 XNOR 연산의 결과들에 대한 AND 연산을 의미할 수 있다. 도 3에서 ⊙는 XNOR 연산을 의미하고, ∧는 AND 연산을 의미한다.

[0045] XNOR 연산의 특성은 두 암호 비트 c_i, c_i' 에 대해서 두 암호 비트(두 암호문에서 대응되는 비트를 의미함)가 같으면 e(1), 즉 1에 대한 암호문을 출력하고(여기서, e는 암호화했다는 것을 의미), 두 암호 비트가 같지 않으면 e(0), 즉 0에 대한 암호문을 출력한다. 결과적으로, 모든 i에 대해서 c_i와 c_i' 이 같아야만, 이후 AND 연산을 모두 적용한 연산의 결괏값이 e(1)이 된다. 반대로, c_i와 c_i' 의 대응되는 비트가 하나라도 다르면, e(0)이 출력된다.

[0046] 도 4는 도 3에 도시된 동치 연산을 이용한 위치 기반 서비스를 설명하기 위한 도면이다.

[0047] 먼저, GPS 데이터는 다양한 정보를 포함하고 있는데, 본 발명에서 필요한 정보는 사용자의 위치 정보(x,y)인 위도(x)와 경도(y)에 대한 것이다. 또한, 도 4에서, ▲는 동형암호 동치 연산을, $\wedge_{bitw}$는 AND 연산을 비트마다 적용하는 것을, ∑는 XOR 연산을 비트마다 적용하는 것을 의미한다.

[0048] 위도(x)는 -90 부터 90 사이의 값(0 부터 180 사이의 값으로 표현될 수도 있음)을 갖는다. 즉, x는 -90 보다 크거나 같고 90 보다 작거나 같은 값을 갖는 정수일 수 있다. 또한, 위도(x)의 단위를 1씩 변경하면서 수행할 수 있지만, 실시예에 따라 단위는 자유롭게 변경 가능하다.

[0049] 경도(y)만 고려한 서비스를 수행하고 싶다면, 경도의 범위를 원하는 단위마다 나누어 암호 회로를 설계할 수 있다.

[0050] 도 4에 도시된 동치 연산 기반의 위치 기반 서비스는 다음과 같은 과정을 통해 수행될 수 있다.

[0051] ① 클라우드 서버는 181개의 값(0, 1, …, 180)을 도 4와 같이 사용자의 암호키를 이용해서 암호화(e(0), e(1), …, e(180))한 후 저장한다. 또한, 각 위도(x)에 따른 서비스(S_x)를 사용자의 암호키로 암호화(e(S_0)), e(S_1), …, e(S_{180}))한 후 저장한다. 예를 들어, 위도 5에 대응되는 서비스(또는 제공가능한 서비스)는 S_5으로 표현될 수 있다.

[0052] ② 만약, 사용자 단말(또는 사용자)의 위치(위도)가 x=7이라면 사용자 단말은 이를 암호화하여 암호화된 위치 정보(e(7))를 생성하고, 생성된 암호화된 위치 정보(e(7))를 클라우드 서버로 전송한다.

[0053] ③ 클라우드 서버는 암호문 e(7)을 각 위도에 대한 암호문(e(0), e(1), …, e(180)과 동형암호 동치 연산(▲)을 수행한다.

[0054] ④ 만약, 사용자 단말로부터 수신된 암호문 e(7)이 위도 암호문과 같다면 e(1)이 출력되고, 다르면 e(0)의 결괏값을 출력한다. 다시말해, 암호화된 사용자의 위치 정보와 위도 7에 대한 암호문(e(7))의 동치 연산의 결과만이 e(1)이고, 나머지 암호문과의 동치 연산의 결과는 모두 e(0)이 된다.

[0055] ⑤ 위 결괏값(동치 연산의 결괏값)에 대해 암호화된 서비스(e(S_x))와 AND 연산($\wedge_{bitw}$)을 수행하면, 결괏값은 오직 e(1)일때만 e(S_x)이 e(S_x)으로 출력되고, 나머지는 e(0)을 출력한다.

[0056] ⑥ 마지막으로, 출력된 값을 더해주는데(덧셈 연산), 여기서 덧셈 연산(∑)은 XOR 연산을 각각의 비트마다 적용하는 것으로 구현될 수 있다. 이는 XOR 논리 회로가 e(0)과 각각 XOR 연산되면, e(0)이 아닌 값만 남는 결과를 얻을 수 있기 때문이다.

[0057] 도 5는 일반적인 동형암호 동치 연산 알고리즘 기반의 위치 기반 서비스를 설명하기 위한 도면이다.

[0058] 도 4에서는 위도와 경도 중 어느 하나만을 고려했다면, 도 5의 방법은 위도와 경도를 모두 고려하여, 전수(brute force) 비교를 통해 암호화된 서비스를 제공할 수 있다.

[0059] 도 4에 도시된 방법과 비교하여, 도 5의 방법에서 추가된 점은 다음과 같다.

[0060] 위도 x의 구간을 n(n은 임의의 자연수)개로 나누고, 경도 y의 구간을 m(m은 임의의 자연수)개로 분할한다. 임의의 위치 x_i와 y_i는 다음의 식으로 표현될 수 있다.

[0061] $$x_i = x_1 + \frac{x_n - x_1}{n} \cdot i$$

[0062] $$y_j = y_1 + \frac{y_m - y_1}{m} \cdot j$$

[0063] 여기서, i와 j는 각각 $1 \le i \le n$, $1 \le j \le m$의 범위를 갖는 자연수이다.

[0064] 또한, 사용자의 위치(x_a, y_b)에 대해 $e(x_i)$와 $e(y_j)$에 대해 동치 연산한 결괏값들, $e(x_a)$와 $e(x_i)$에 대한 동치 연산 결괏값과 $e(y_b)$와 $e(y_j)$에 대한 동치 연산 결괏값에 AND 연산($\wedge$)을 적용한다.

[0065] 나머지 과정들은 도 4에 도시된 방법과 동일하므로 이에 대한 상세한 설명은 생략하기로 한다.

[0066] 2) 동형암호 비교 연산 알고리즘 기반의 위치 기반 서비스 제공 방법

[0067] 동형암호 동치 연산 알고리즘이 사용자(또는 사용자 단말)이 특정 위치(x)에 있을 때 해당 서비스(S_x)를 출력하는 것이라면, 동형암호 비교 연산을 이용한 위치 기반 서비스는 사용자(또는 사용자 단말)이 특정 범위($x \in A$)에 있을 때, 구간 서비스(S_A)를 출력하는 방법이다.

[0068] 도 6은 동형암호 비교 연산을 설명하기 위한 도면이다.

[0069] 도 6에는 동형암호 비교 연산의 암호 회로를 나타낸다. 두 암호 회로 모두 XNOR 논리회로와 멀티플렉서(Multiplexer, MUX)를 이용한다.

[0070] 도 6의 좌측은 대소 비교 중 '크다'에 해당하는 암호 회로 모델이고, 입력 값(a, b)에 대해 a가 b보다 크면 e(1)을 출력하고, 작으면 e(0)을 출력한다. XNOR 논리회로와 멀티플렉서를 각 비트(a_i, b_i)마다 반복적으로 적용하여 결괏값을 출력한다.

[0071] 구체적으로, 도 6에서 XNOR 논리회로는 두 암호문이 같으면 e(1)을 출력하고, 다르면 e(0)을 출력한다. 만약, a와 b의 i-번째 암호 비트가 서로 같다면 e(1)을 출력하고, 이 결과를 Mux 논리회로가 입력으로 받으면, c의 i-1번째 암호 비트가 출력된다. 즉, i-번째에서는 두 암호문 간에 대소를 비교할 수 없으므로 이전 결과가 대소 비교의 결과값이 된다. 반대로, 만약 a와 b의 i-번째 암호 비트가 서로 다르다면, e(0)이 출력되고 Mux 논리회로는 a의 i-번째 암호 비트를 출력한다. 여기서, a가 b보다 작다면 암호문 a는 e(0)일 것이고, 따라서 Mux 논리회로는 a의 i-번째 암호 비트인 e(0)을 출력한다. 반대로, a가 b보다 크면 암호문 a는 e(1)일 것이고, Mux 논리회로는 e(1)을 출력하고, 이는 대소 결과와 일치한다.

[0072] 마찬가지로, 도 6의 우측은 '작다'를 출력하는 암호 회로 모델이다. 입력 값(a, b)에 대해서 a가 b보다 작으면 e(1)을 출력하고, 크면 e(0)을 출력한다.

[0073] 도 7은 대소 비교 연산을 이용한 위치 기반 서비스를 설명하기 위한 도면으로써, 위도 x와 경도 y 중 어느 하나만을 고려한 예이다.

[0074] 클라우드 서버는 도 7과 같이 비교 연산 기반의 위치 기반 서비스를 다음과 같이 수행할 수 있다.

[0075] ① 사용자의 위치(예컨대, 위도)가 x=13이라면 사용자 단말은 이를 암호화하여 e(13)을 생성하고, 암호화된 위치 정보(e(13)를 클라우드 서버에 전송한다.

[0076] ② 클라우드 서버는 e(13)에 대해 구간마다 동형암호 대소 비교를 진행한다. 예를 들어, 첫번째 구간을 1<x<10이라고 한다면, a) e(13)을 e(1)과 '크다' 비교, b) e(13)을 e(10)과 '작다' 비교를 진행한다. 여기서, 구간의 크기나 개수는 실시예에 따라 가변할 수 있다.

[0077] ③ 대소 비교 결과들에 대해서 AND 연산을 수행한다. 위의 예시에 따르면, 대소 비교 결과 e(1)과 e(0)의 AND

연산 값은 e(0)이다.

[0078] ④ 클라우드 서버는 ③의 결과와 이전에 클라우드 서버가 저장한 구간마다 할당된 서비스(S_A)에 대해 비트마다 AND 연산($\wedge_{bitw}$)을 진행한다. 이를 통해, 위치 정보 x가 속하고 있는 구간의 서비스만 e(0)이 되지 않는다.

[0079] ⑤ 마지막으로, 동치 연산에서와 같이 출력된 값을 더한다(∑은 비트마다 XOR 연산). 최종 결괏값은 사용자 단말로 송신될 수 있다.

[0080] 도 8은 일반적인 대소 비교 연산을 이용한 위치 기반 서비스를 설명하기 위한 도면이다.

[0081] 사용자의 위치(또는 사용자 단말의 위치)를 x_a, y_b라고 한다면, 암호화된 사용자의 위치 $e(x_a)$, $e(y_b)$가 특정 범위 구간과 비교될 수 있다.

[0082] 위도 범위 내에서 비교하고 싶은 각 구간을 (x_i, x_{i+1})이라고 하면, 구간(x_i, x_{i+1})은 다음을 만족한다.

[0083] ① $1 \leq i < n$의 정수 값을 갖는 i

[0084] ② x_i는 위도 x의 범위 안에 있는 값을 갖는다.

[0085] 마찬가지로 경도 범위 내에서 구간 (y_j, y_{j+1})도 정수 값을 갖는 $1 \leq j < m$에 대해 y_j는 경도 범위 안에 있는 값을 갖는다.

[0086] 도 7에서와 같이 사용자의 위치 $e(x_a)$, $e(y_b)$를 각 구간별로 비교 연산 수행하고, 이 결괏값에 대해 AND 연산을 수행한다. 만약 모든 조건을 만족한다면, 즉 $x_s < x_a < x_{s+1}$, $y_t < y_b < y_{t+1}$ 이 두가지 조건을 동시에 만족하는 구간 (x_s, x_{s+1}), (y_t, y_{t+1})에 대해서, AND 연산 결과는 e(1)이 된다.

[0087] 도 7에서 처럼 위 조건을 만족한 암호화된 서비스가 $e(S_{xs,yt})$ 비트 마다 e(1)과 연산되고, 결과적으로 이 값들을 모두 XOR로 더해 원하는 암호화된 서비스 $e(S_{xs,yt})$가 산출된다. 이때, 구간의 개수에 따라, 암호 회로의 속도가 결정된다. 또한, 산출된 암호화된 서비스($e(S_{xs,yt})$)는 사용자 단말로 송신될 수 있다.

[0088] 도 9는 본 발명의 일 실시예에 따른, 암호화된 사용자의 위치 정보를 이용한 위치 기반 서비스 시스템을 도시한다.

[0089] 시스템 등으로 명명될 수도 있는 위치 기반 서비스 시스템은 사용자 단말(USER)과 클라우서 서버(CLOUD)를 포함한다. 사용자 단말 및/또는 클라우드 서버는 적어도 프로세서(processor) 및/또는 메모리(memory)를 포함하는 컴퓨팅 장치로 구현될 수 있다. 컴퓨팅 장치는 PC(Personal Computer), 스마트폰(smart phone), 모바일 폰(mobile phone), HMD(Head Mounted Device), 태플릿 PC(tablet PC), 내비게이션 시스템, 스마트 안경(smart glassed), 스마트 와치(smart watch) 등을 포함할 수 있다. 따라서, 위치 기반 서비스 시스템 상에서 수행되는 방법, 예컨대 위치 기반 서비스 제공 방법은 사용자 단말 및/또는 클라우드 서버에 포함되는 프로세서의 동작으로 이해될 수도 있다.

[0090] 사용자 단말은 GPS 시스템 등으로부터 위치 정보를 수신하고, 수신된 위치 정보를 암호화한 후 암호화된 위치 정보를 클라우드 서버로 송신할 수 있다. 이때, 위치 정보에 대한 암호화는 LWE(Learning With Error) 기법 또는 RLWE(Ring LWE) 기법을 이용하여 수행될 수 있다. 이를 위해, 사용자 단말은 위치 정보를 바이너리로 변환하고 바이너리고 변환된(즉, 이진수로 표현된) 위치 정보를 비트 단위로 암호화할 수 있다.

[0091] 또한, 위치 정보는 복수의 차원을 가질 수 있고, 사용자 단말은 위치 정보의 각 차원 데이터를 바이너리로 변환한 후 비트 단위로 암호화할 수 있다. 위치 정보는 GPS 시스템으로 수신된 위도 정보 및/경도 정보를 의미할 수 있다. 실시예에 따라, 위치 정보는 3차원 이상의 차원을 가질 수도 있다.

[0092] 다른 예로, 실내에서는 GPS 데이터가 수신되지 않기 때문에, WIFI 신호 정보를 통해 추출한 위치 정보가 사용될 수도 있다. WIFI 신호를 이용하면 사용자의 위치 정보를 추출할 수 있기 때문이다.

[0093] 위치 기반 서비스 제공 서버 등으로 명명될 수도 있는 클라우드 서버는 사용자 단말로부터 암호화된 위치 정보를 수신하고, 수신된 위치 정보에 대하여 미리 정의된 동작을 수행하여 도출된 위치 기반 서비스를 도출할 수 있다. 물론, 위치 기반 서비스를 도출하기 위한 과정에서 연산은 암호화된 데이터를 복호화하지 않고 암호화된 데이터를 이용하여 수행될 수 있다. 또한, 도출되는 위치 기반 서비스역시 암호화된 결과물일 수 있다. 마지막

으로, 도출된 위치 기반 서비스는 사용자 단말로 송신될 수 있다.

[0094] 사용자 단말은 클라우드 서버로부터 수신된 위치 기반 서비스를 복호화하여 이를 이용할 수 있다.

[0095] 본 발명이 활용될 수 있는 예시로써 국가 위치 서비스를 들 수 있다. 예를 들어, 국가(또는 정부에서 운용하는 서버)에서 국민의 위치를 알 수는 없지만 본 발명에 의한 방법을 사용하는 국민(사용자)은 특정 위치를 국가에 노출하지 않으면서, 특정 위치와 관련된 서비스를 받을 수 있다. 가령, 사용자가 위험한 지역에 방문할 경우 국가는 해당 사용자가 특정 위치에 있는지 알 수는 없지만, 사용자에게 위험 메시지를 보낼 수 있다(여기서, 국가는 사용자에게 어떤 메시지를 보냈는지 알 수 없다). 따라서, 위치 기반 서비스로서 사용자 단말로 제공되는 암호화된 서비스는 해당 위치(즉, 사용자의 위치)의 상황(기상 상황, 교통 상황, 치안 상황, 범죄 발생 현황 등), 위험도(예컨대, 위험 메시지), 대사관이나 영사관에 관한 정보(전화번호, 주소, 위치, 담당자 등) 등 중 적어도 하나를 포함하는 메시지로써, 암호화된 메시지를 의미할 수 있다.

[0096] 또 다른 예시로, 기업에서 본 발명을 이용해 사용자의 위치에 따른 서비스를 제공할 수 있다. 스마트폰 앱 등에서는 사용자의 위치에 따른 서비스를 제공할 시에 사용자 위치 정보 제공에 대한 동의를 반드시 동반한다. 하지만, 기업에서 본 서비스를 사용할 경우, 사용자의 위치 정보 제공에 대해 동의를 받지 않고도, 암호화된 사용자 위치 데이터를 받아 사용자가 원하는 위치 기반 서비스를 제공할 수 있다.

[0097] 이상에서 설명된 장치는 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 콘트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크로컴퓨터, FPA(Field Programmable array), PLU(Programmable Logic Unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(Processing Element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

[0098] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 구체화(Embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

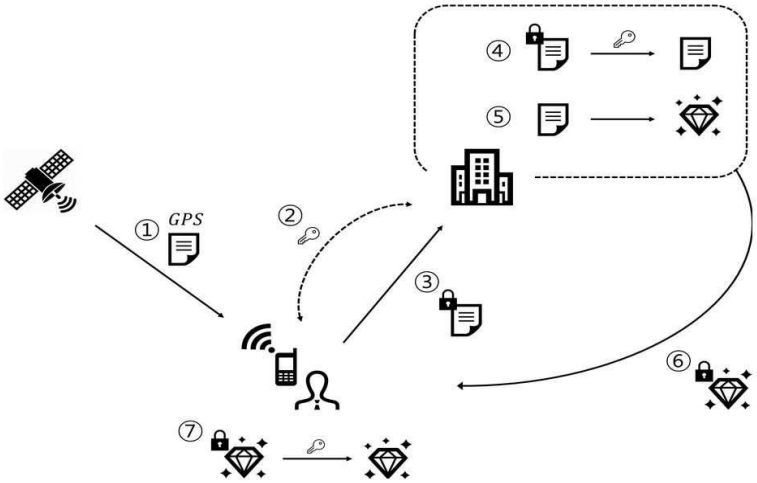
[0099] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0100] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성

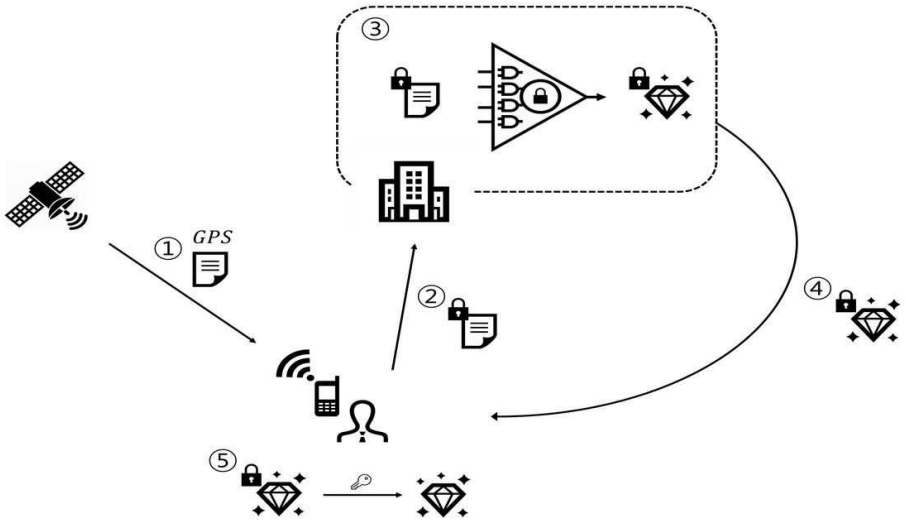
요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

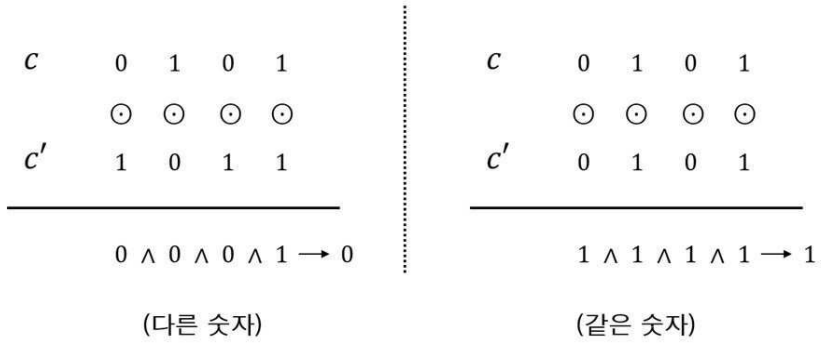
도면1



도면2

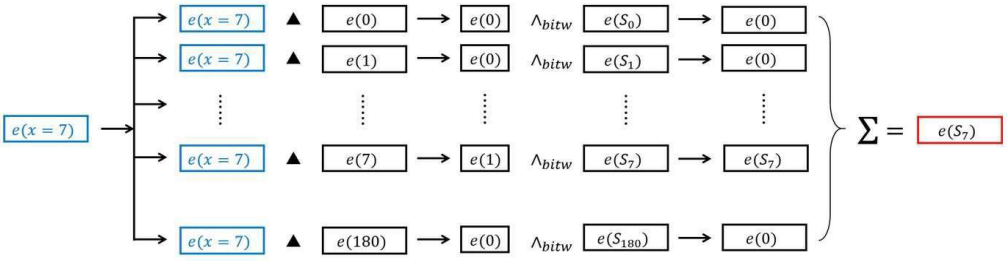


도면3



동형암호 동치 연산(⊙: XNOR 논리회로, ∧: AND 논리회로)

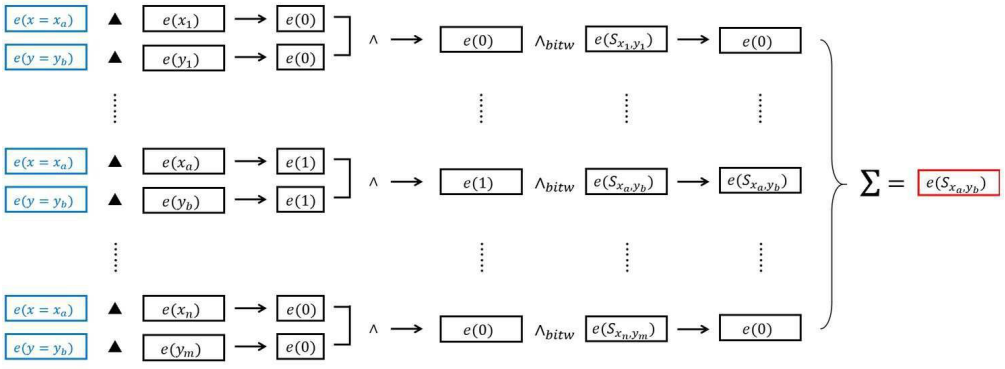
도면4



동치 연산 기반의 위치 기반 서비스 (위치정보 1개)만 고려한 경우

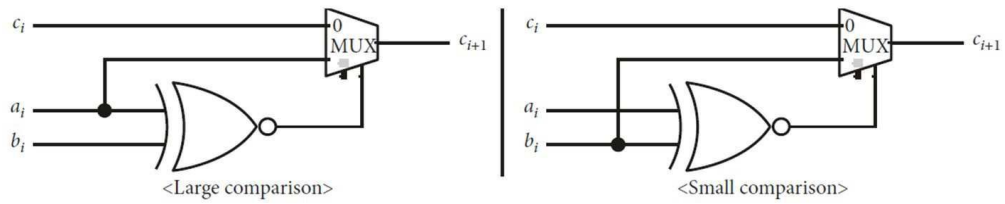
(▲: 동형암호 동치 연산, $\wedge_{bitw}$: AND 연산을 비트마다 적용, ∑: XOR 연산을 비트마다 적용)

도면5



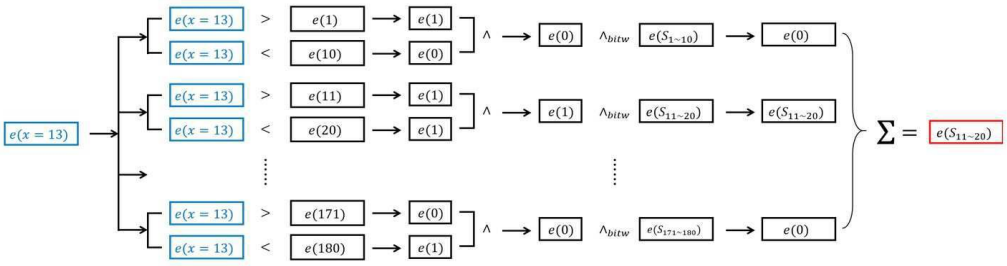
일반적인 동치 연산 기반의 위치 기반 서비스

도면6



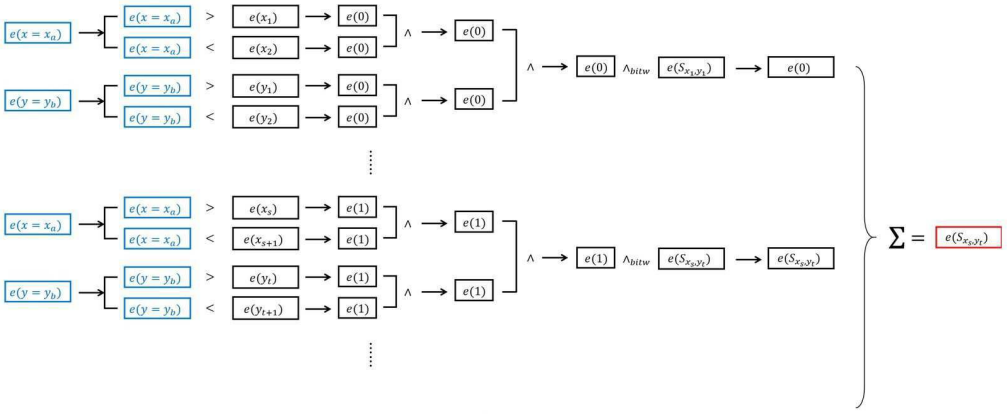
동형암호 비교 연산(대소 비교). 왼쪽은 대소 비교 중 '크다'에 해당하고, 오른쪽은 '작다'에 해당하는 암호 회로이다. XNOR 논리회로와 멀티플렉서 논리회로를 이용한다.

도면7



비교 연산 기반의 위치 기반 서비스 (>, <: 동형암호 대소 비교 연산)
(위치정보 1개)만 고려한 경우

도면8



일반적인 비교 연산 기반의 위치 기반 서비스

도면9

