(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월02일
(11) 등록번호 10-1731628
(24) 등록일자 2017년04월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) *H04L 9/08* (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/008 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2015-0148436
(22) 출원일자 2015년10월26일
심사청구일자 2015년10월26일
(56) 선행기술조사문헌
KR101373577 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
서민혜
서울특별시 양천구 목동중앙남로 21-15 101동 703호 (목동,에이스아파트)
이동훈
서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)
(74) 대리인
김등용, 김홍석

전체 청구항 수 : 총 3 항 심사관 : 전용해

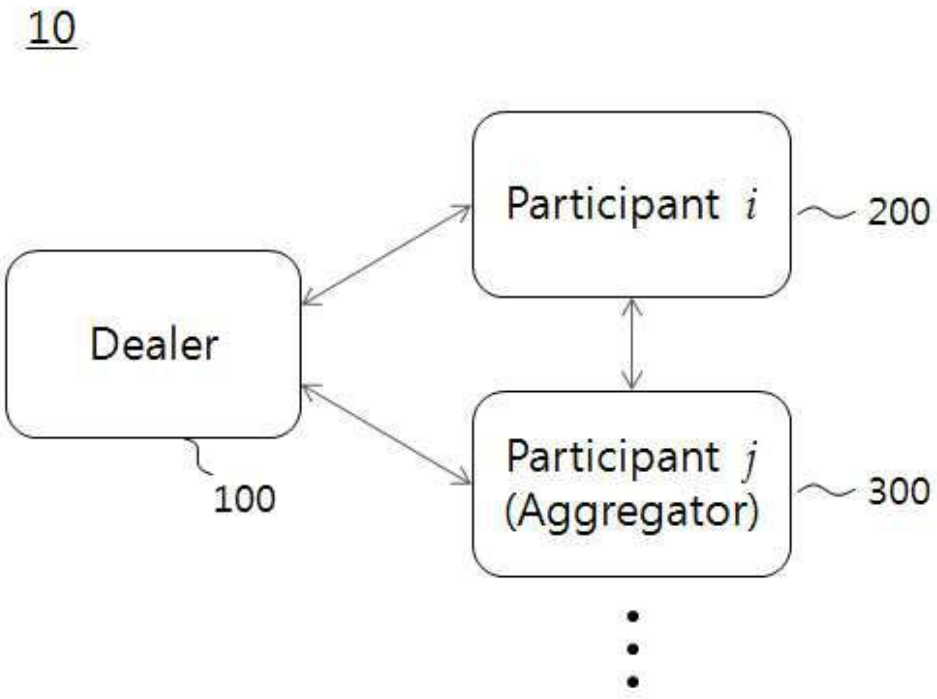
(54) 발명의 명칭 **프라이버시를 보장하는 시계열 데이터의 임계 병합 방법**

(57) 요 약

프라이버시를 보장하는 시계열 데이터의 임계 병합 방법이 개시된다. 시계열 데이터를 병합하는 사용자 장치에 있어서, 상기 시계열 데이터 임계 병합 방법은 상기 사용자 장치가 분배자 장치로부터 공개 파라미터 및 비밀키를 수신하는 단계, 상기 사용자 장치가 상기 공개 파라미터를 이용하여 공개키 및 개인키를 생성하는 단계, 및

(뒷면에 계속)

대 표 도 - 도1



상기 사용자 장치가 취합자 장치가 아닌 경우 상기 취합자 장치의 공개키 및 상기 사용자 장치의 상기 비밀키를 이용하여 암호문을 생성하고 상기 취합자 장치에 송신하고, 상기 사용자 장치가 상기 취합자 장치인 경우 상기 취합자 장치를 제외한 사용자 장치로부터 암호문을 수신하고 상기 취합자 장치의 비밀키를 이용하여 상기 암호문을 병합 및 복호화하는 단계를 포함하고, 상기 사용자 장치가 상기 취합자 장치인 경우 상기 암호문을 전송한 상기 취합자 장치를 제외한 사용자 장치의 개수가 미리 설정된 임계값 이상인 경우 상기 암호문의 병합을 수행하는 것을 특징으로 한다.

(52) CPC특허분류
H04L 9/0861 (2013.01)
H04L 9/3006 (2013.01)

명 세 서

청구범위

청구항 1

취합자 장치를 포함하는 복수의 사용자 장치 및 분배자 장치를 포함하며, 병합에 참여하기 위하여 암호문을 전송하는 사용자 장치의 수가 임계값(t) 이상인 경우 암호문의 병합을 수행하는 시계열 데이터 임계 병합 시스템에서 있어서,

상기 분배자 장치가 공개 파라미터 및 마스터키를 생성하는 단계;

상기 분배자 장치가 '$q(0)=0$'을 만족하는 t차 다항식 $q(x)$를 랜덤하게 선택하는 단계;

상기 분배자 장치가 상기 t차 다항식 $q(x)$를 이용하여 각각의 사용자 장치에 대한 비밀키를 생성하고 전송하는 단계;

상기 각각의 사용자 장치가 상기 공개 파라미터를 이용하여 공개키 및 개인키를 생성하는 단계;

상기 복수의 사용자 장치 중 적어도 하나 이상의 사용자 장치가 생성된 데이터를 암호화하여 암호문(C_i)을 생성하는 단계;

상기 복수의 사용자 장치 중 데이터 취합자로 선정된 취합자 장치가 상기 복수의 사용자 장치 중 적어도 둘 이상의 사용자 장치로부터 상기 암호문(C_i)을 수신하는 단계;

상기 암호문(C_i)을 전송한 사용자 장치의 개수가 상기 임계값(t) 이상인 경우, 상기 취합자 장치가 상기 분배자 장치로부터 수신한 상기 취합자 장치의 비밀키 및 라그랑지 보간법을 이용하여 적어도 둘 이상의 사용자 장치로부터 수신한 상기 암호문(C_i)을 병합하여 병합된 암호문(V)을 생성하는 단계; 및

상기 취합자 장치가 상기 병합된 암호문(V)을 복호화하는 단계;를 포함하되,

상기 사용자 장치가 상기 암호문(C_i)을 생성하는 단계는,

덧셈에 대한 동형 성질을 제공하는 동형 암호 기법을 이용하여 상기 취합자 장치의 공개키에 대한 제1 암호문을 생성하는 과정; 및

상기 제1 암호문, 상기 사용자 장치에서 상기 데이터가 생성된 시간(T), 및 상기 사용자 장치의 비밀키를 이용하여 제2 암호문을 생성하는 과정;을 포함하고,

상기 취합자 장치가 상기 병합된 암호문(V)을 생성하는 단계는,

상기 암호문(C_i)이 각 사용자 장치에서 같은 시간대에 생성된 데이터에 대한 암호문인 경우에만 병합에 대한 정당한 결과값을 도출하는 것을 특징으로 하는,

시계열 데이터 임계 병합 시스템에서의 시계열 데이터 임계 병합 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

병합에 참여하기 위하여 시계열 데이터의 암호문을 전송하는 사용자 장치의 수가 임계값(t) 이상인 경우 암호문의 병합을 수행하는 사용자 장치에 있어서,

상기 사용자 장치가 분배자 장치로부터 공개 파라미터 및 비밀키를 수신하는 단계;

상기 사용자 장치가 상기 공개 파라미터를 이용하여 공개키 및 개인키를 생성하는 단계; 및

상기 사용자 장치가 취합자 장치가 아닌 경우 상기 취합자 장치의 공개키 및 상기 사용자 장치의 상기 비밀키를 이용하여 암호문(C_i)을 생성하여 상기 취합자 장치에 송신하고, 상기 사용자 장치가 상기 취합자 장치인 경우 상기 취합자 장치를 제외한 사용자 장치로부터 암호문(C_i)을 수신하고 상기 취합자 장치의 비밀키를 이용하여 상기 암호문(C_i)을 병합하여 병합된 암호문(V)을 생성하고 상기 병합된 암호문(V)을 복호화하는 단계;를 포함하되,

상기 사용자 장치가 취합자 장치가 아닌 경우 덧셈에 대한 동형 성질을 제공하는 동형 암호 기법을 이용하여 취합자 장치의 공개키에 대한 중간 암호문을 생성하고, 상기 중간 암호문, 상기 사용자 장치에서 상기 데이터가 생성된 시간(T), 및 상기 사용자 장치의 비밀키를 이용하여 최종 암호문을 생성하고,

상기 사용자 장치가 상기 취합자 장치인 경우 상기 암호문을 전송한 상기 취합자 장치를 제외한 사용자 장치의 개수가 상기 임계값(t) 이상인 경우 라그랑지 보간법을 이용하여 상기 암호문(C_i)을 병합하여 상기 병합된 암호문(V)을 생성하는 것을 특징으로 하며,

상기 사용자 장치가 상기 취합자 장치인 경우 상기 암호문(C_i)이 각 사용자 장치에서 같은 시간대에 생성된 데이터에 대한 암호문인 경우에만 병합에 대한 정당한 결과값을 도출하는 것을 특징으로 하는,

사용자 장치의 시계열 데이터 임계 병합 방법.

청구항 5

삭제

청구항 6

삭제

청구항 7

시계열 데이터의 임계 병합을 수행하는 사용자 장치에 있어서,

분배자 장치로부터 비밀키를 수신하고, 다른 사용자 장치로부터 암호문(C_i)을 수신하거나, 다른 사용자 장치에 암호문(C_i)을 전송하는 통신 모듈;

동형 암호 기법의 키생성 알고리즘을 수행하여 상기 사용자 장치의 공개키 및 개인키를 생성하는 키생성 모듈;

취합자 장치의 공개키 및 상기 사용자 장치의 상기 비밀키를 이용하여 암호문(C_i)을 생성하는 암호화 모듈; 및

상기 사용자 장치가 취합자 장치로 선정된 경우, 상기 취합자 장치로 선정된 상기 사용자 장치를 제외한 사용자 장치들 각각으로부터 수신한 암호문(C_i)을 병합하여 병합된 암호문(V)를 생성하고, 상기 병합된 암호문(V)를 복호화하는 병합 및 복호화 모듈;을 포함하되,

상기 병합 및 복호화 모듈은, 상기 암호문(C_i)이 각 사용자 장치에서 같은 시간대에 생성된 데이터에 대한 암호문인 경우에만 병합에 대한 정당한 결과값을 도출하고,

상기 병합 및 복호화 모듈은, 상기 취합자 장치로 선정된 상기 사용자 장치로 상기 암호문(C_i)을 전송한 사용자 장치들의 개수가 미리 설정된 임계값(t) 이상인 경우 라그랑지 보간법을 이용하여 상기 암호문(C_i)의 병합을 수

행하며,

상기 암호화 모듈은, 덧셈에 대한 동형 성질을 제공하는 동형 암호 기법을 이용하여 상기 취합자 장치의 공개키에 대한 제1 암호문을 생성하고, 상기 제1 암호문, 상기 사용자 장치에서 상기 데이터가 생성된 시간(T) 및 상기 사용자 장치의 상기 비밀키를 이용하여 제2 암호문을 생성하는,

시계열 데이터 임계 병합 사용자 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 프라이버시를 보장하는 시계열 데이터의 임계 병합 방법에 관한 것으로, 특히, 분배자가 동형 암호 기법을 이용하여 공개 파라미터 및 임계 기능 제공을 위한 비밀키를 생성하고, 각 사용자는 취합자의 공개키, 사용자의 비밀키 및 데이터 생성 시간 정보를 입력하여 암호문을 생성하고, 취합자는 상기 암호문을 수신하여 임계값 이상인 경우 취합자의 비밀키를 이용하여 상기 암호문을 병합하고 취합자의 개인키를 이용하여 복호화를 수행하는 시계열 데이터의 임계 병합 방법에 관한 것이다.

배 경 기 술

[0002] 본 특허는 프라이버시를 보장하는 시계열 데이터(time series data)의 데이터 병합 기술을 제시하고 있다.

[0003] 데이터 병합 기술은 다수의 사용자들의 데이터를 이용하여 원하는 연산의 결과값을 얻는 기술로 데이터 병합 시스템을 셋팅하는 분배자(Dealer), 데이터를 생성하는 사용자(Participant), 데이터를 병합하는 취합자(Aggregator)로 구성된다.

[0004] 개인정보가 포함된 데이터의 경우 사용자의 민감한 정보를 포함하고 있기 때문에 유출시 각종 범죄에 악용될 가능성이 있다. 따라서, 데이터 취합자는 원본 데이터에 대하여 알 수 없어야 하며 사용자의 프라이버시를 보존하며 데이터를 병합할 수 있는 데이터 병합 방법이 요구된다.

[0005] 또한, 시계열 데이터의 병합 기술은 같은 시간대에 생성된 데이터에 대해서 병합하는 기술로, 다른 시간대의 데이터에 대해서는 병합에 대한 정당한 결과값 도출할 수 없는 데이터 병합 기술이 요구된다.

발명의 내용

해결하려는 과제

[0006] 본 발명이 이루고자 하는 기술적인 과제는 사용자들의 프라이버시를 보장할 수 있는 동형암호를 이용한 데이터 병합 방법을 제공하는 것이다.

[0007] 또한, 시계열 데이터를 병합하는 과정에서 항상 시스템 내의 모든 사용자들의 데이터를 병합하는 것은 아니기 때문에 임계치 이상의 일부 사용자 집합에 대하여 프라이버시를 보장하면서 데이터를 병합하는 방법을 제공하는 것이다.

[0008] 또한, 시스템 내의 임의의 사용자가 취합자가 될 수 있으며, 메시지 공간의 제한 없이 임의의 크기의 데이터에 대해서도 병합 및 복호화가 가능한 데이터 병합 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 실시 예에 따른 시계열 데이터를 병합하는 사용자 장치에 있어서, 프라이버시를 보장하는 시계열 데이터의 임계 병합 방법은 상기 사용자 장치가 분배자 장치로부터 공개 파라미터 및 비밀키를 수신하는 단계, 상기 사용자 장치가 상기 공개 파라미터를 이용하여 공개키 및 개인키를 생성하는 단계, 및 상기 사용자 장치가 취합자 장치가 아닌 경우 상기 취합자 장치의 공개키 및 상기 사용자 장치의 상기 비밀키를 이용하여 암호문을 생성하고 상기 취합자 장치에 송신하고, 상기 사용자 장치가 상기 취합자 장치인 경우 상기 취합자 장치를 제외한 사용자 장치로부터 암호문을 수신하고 상기 취합자 장치의 비밀키를 이용하여 상기 암호문을 병합 및 복호화하는 단계를 포함하되, 상기 사용자 장치가 상기 취합자 장치인 경우 상기 암호문을 전송한 상기 취합자 장치를 제외한 사용자 장치의 개수가 미리 설정된 임계값 이상인 경우 상기 암호문의 병합을 수행하는 것을 특징으로 한다.

발명의 효과

[0010] 본 발명의 실시 예에 따른 시계열 데이터 임계 병합 방법은 사용자들이 개인키를 이용하여 시계열 데이터를 암호화하기 때문에 데이터의 프라이버시를 보장할 수 있으며, 개인키 발급 과정에서 임계기능을 적용함으로써 임계값 이상의 사용자들에 대한 시계열 데이터의 병합이 가능하도록 하는 효과가 있다.

[0011] 또한, 메시지 공간의 크기에 제약 없이 임의의 크기의 데이터에 대해서도 병합 및 복호화할 수 있는 효과가 있다.

도면의 간단한 설명

[0012] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시예에 따른 프라이버시를 보장하는 시계열 데이터의 임계 병합 시스템의 개략도이다.

도 2는 도 1에 도시된 분배자 장치의 기능 블럭도이다.

도 3은 도 1에 도시된 사용자 장치 중 취합자 장치의 기능 블럭도이다.

도 4는 도 1에 도시된 시계열 데이터 임계 병합 시스템을 이용한 시계열 데이터 임계 병합 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0014] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0015] 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.

[0016] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 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.

[0017] 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 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.

[0018] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0019] 우선, 본 발명에서 사용하는 시계열 데이터 병합 기술은 2011년 Shi, Chan, Rieffel, Chow, 그리고 Song이 제안한 기법으로 각 사용자의 데이터에 대한 프라이버시를 보장하는 시계열 데이터 병합 기술이다. G는 소수 p를 위수(Order)로 가지는 순환군(Cyclic group)이고 해쉬 함수 H를 $H : Z \rightarrow G$와 같이 정의하며, 해당 데이터 병합 기술은 시계열 데이터 병합을 위한 셋업 알고리즘(Setup), 노이지 암호화 알고리즘(NoisyEnc) 및 병합 및 복호화 알고리즘(AggrDec)을 포함한다.

[0020] 시계열 데이터 병합을 위한 셋업 알고리즘(Setup)은 보안 상수 k를 입력 받아 공개 파라미터와 각 사용자 및 취합자의 개인키를 생성하는 알고리즘이다. 분배자는 임의의 생성원 $g \in G$를 선택하고, $s_0 + s_1 + \cdots + s_n = 0$ 을 만족하는 (n+1) 개의 임의의 비밀값 $s_0, s_1, \ldots, s_n \in Z_p$ 을 선택한다. 공개 파라미터 ($PP = (g)$)와 취합자의 개인키($sk_0 = s_0$), 각 사용자 i 의 개인키($sk_i = s_i$)를 출력하며, 분배자는 취합자를 포함하는 사용자들에게 각자의 개인키를 전송한다.

[0021] 노이지 암호화 알고리즘(NoisyEnc)은 공개 파라미터, 시간 정보, 각 사용자의 개인키와 데이터를 입력받아 암호문을 생성하는 알고리즘이다. 각 사용자 i 는 시간 정보 t 와 자신의 데이터 $x_i \in Z_n$에 대하여 개인키 sk_i를 이용하여 암호문 $C_i \leftarrow g^{x_i} \cdot H(t)^{sk_i}$ 를 생성한다.

[0022] 병합 및 복호화 알고리즘(AggrDec)은 공개 파라미터, 취합자의 개인키, 시간 정보와 모든 사용자의 암호문들을 입력 받아 병합된 데이터를 생성하는 알고리즘이다. 취합자는 먼저 취합자의 개인키 sk_0, 시간 정보 t와 각 사용자 i 의 암호문 C_i를 이용하여 $V \leftarrow H(t)^{sk_0} \prod_{i=1}^{n} C_i$ 를 계산한다. 취합자는 $V = g^{\sum_{i=1}^{n} x_i}$ 를 복호화하기 위하여 $\log_g V$ 를 계산하고, $\sum_{i=1}^{n} x_i$ 를 출력한다.

[0023] 상기 기법은 복호화를 위해서 로그 연산을 수행해야하기 때문에 메시지 공간(Plaintext space)이 작은 경우에 대해서만 기법이 동작한다. 무작위 대입 검색(Brute-force search)을 통해서 복호화를 수행할 수 있으며, 바람직하게는 Pollard의 람다(Lambda) 방법을 이용하여 복호화를 수행할 수 있다.

[0024] 또한, 본 발명에서는 덧셈에 대한 동형 성질을 갖는 동형 암호 기법을 이용한다. 예를 들어, 2003년 Bresson, Catalano 및 Pointcheval이 제안한 기법(이하, BCP 암호 기법이라 함)일 수 있다. BCP 암호 기법은 Paillier 암호 기법을 기반으로 설계된 것으로서, 사용자의 개인키를 가지고 복호화하거나 마스터키를 가지고 복호화하는 두 개의 복호화 알고리즘이 있는 점을 특징으로 한다.

[0025] 본 발명이 상기 BCP 암호 기법에 제한되는 것은 아니며, 암호 기법의 이름과는 무관하게 상기 BCP 암호 기법과 동일하거나 유사한 알고리즘을 제공하는 암호 기법을 이용할 수도 있다.

[0026] 본 발명에서 이용하는 동형 암호 기법은 2003년 Bresson, Catalano 및 Pointcheval이 제안한 기법(이하, BCP 암호 기법이라 함)으로 덧셈에 대한 동형 성질을 제공한다. 상기 BCP 암호 기법은 Paillier 암호 기법을 기반으로 설계된 것으로써, 사용자의 개인키를 가지고 복호화하거나 마스터키를 가지고 복호화하는 두 개의 복호화 알고리즘이 있는 점을 특징으로 한다.

[0027] 다만 본 발명이 상기 BCP 암호 기법에 제한되는 것은 아니며, 암호 기법의 이름과는 무관하게 상기 BCP 암호 기법과 동일하거나 유사한 알고리즘을 제공하는 암호 기법을 이용할 수도 있다.

[0028] 상기 BCP 암호 기법은 5개의 알고리즘(BCP.Setup, BCP.KeyGen, BCP.Enc, BCP.Dec, BCP.mDec)을 포함한다.

[0029] BCP 암호 기법의 셋업 알고리즘(BCP.Setup)은 보안 상수(k)를 입력받아 공개 파라미터(PP)와 마스터키(MK)를 생성하는 알고리즘이다. 상기 셋업 알고리즘은 안전 소수(safe prime)인 p(p=2p´+1)와 q(q=2q´+1)를 생성한 뒤 상기 p와 상기 q를 곱한 N(N=pq)을 계산한다. 상기 p´과 상기 q´은 소수(prime number)이다.

[0030] 또한, 상기 BCP 암호 기법의 셋업 알고리즘은 k($k \in [1, N-1]$)에 대해 $g^{p'q'} = 1 + kN \bmod N^2$ 를 만족하는 임의의 g($g \in Z^*_{N^2}$)를 선택한다. 이때 메시지 공간은 Z_N 이다. 즉, k는 1보다 크거나 같고 N보다 작은 정수 값을 갖는다. 상기 g는 1보다 크거나 같고 (N^2-1)보다 작거나 같은 정수들의 집합의 원소이다.

[0031] 상기 BCP 암호 기법의 셋업 알고리즘은 최종적으로 공개 파라미터(PP=(N,k,g))와 마스터키(MK=(p´,q´))를 생성하여 출력할 수 있다.

[0032] BCP 암호 기법의 키생성 알고리즘(BCP.KeyGen)은 상기 공개 파라미터(PP)를 이용하여 사용자의 공개키(pk)와 개인키(sk)를 생성하는 알고리즘이다.

[0033] 상기 BCP 암호 기법의 키생성 알고리즘은 임의의 a($a \in Z_{N^2}$)를 선택하여 h($h = g^a \bmod N^2$)를 계산함으로써, 상기 공개키(pk=h)와 상기 개인키(sk=a)를 생성하여 출력한다.

[0034] BCP 암호 기법의 암호화 알고리즘(BCP.Enc)은 상기 사용자의 상기 공개키(pk)를 이용하여 메시지(m)을 암호화하는 알고리즘이다.

[0035] 상기 BCP 암호 기법의 암호화 알고리즘은 상기 공개키(pk=h)와 상기 메시지($m \in Z_N$)에 대해 임의의 난수($r = Z_{N^2}$)을 선택하여 암호문(A,B)을 생성하고, 생성된 암호문(A,B)을 출력한다. 상기 암호문(A,B)는 아래 수식을 이용하여 생성될 수 있다.

[0036] $$A = g^r \bmod N^2$$

[0037] $$B = h^r (1 + mN) \bmod N^2$$

[0038] BCP 암호 기법의 제1 복호화 알고리즘(BCP.Dec)은 상기 사용자의 상기 개인키(sk=a)를 이용하여 상기 암호문(A,B)을 복호화하는 알고리즘이다.

[0039] 상기 BCP 암호 기법의 제1 복호화 알고리즘은 아래 수식을 이용하여 상기 암호문(A,B)을 복호화하고 메시지(m)를 출력한다.

[0040] $$m = \frac{B/(A^a) - 1 \bmod N^2}{N}$$

[0041] BCP 암호 기법의 제2 복호화 알고리즘(BCP.mDec)은 상기 마스터키(MK)를 이용하여 상기 암호문(A,B)을 복호화하는 알고리즘이다.

[0042] 상기 BCP 암호 기법의 제2 복호화 알고리즘은 상기 마스터키(MK=(p´,q´))와 상기 암호문(A,B)에 사용된 공개키(pk=h)에 대해 다음 두 식을 계산하여 상기 개인키(sk=a)와 상기 임의의 난수(r)에 대한 정보를 얻는다.

[0043] $$a \bmod N = \frac{(h^{p'q'} - 1) \bmod N^2}{N} \times k^{-1} \bmod N$$

[0044] $$r \bmod N = \frac{(A^{p'q'} - 1) \bmod N^2}{N} \times k^{-1} \bmod N$$

[0045] 상기 BCP 암호 기법의 제2 복호화 알고리즘은 다음의 식을 이용하여 상기 암호문(A,B)을 복호화 하고 메시지(m)을 출력한다.

[0046] $$m = \frac{((B/(g^{ar \bmod N}))^{p'q'} - 1) \bmod N^2}{N} \times (p'q')^{-1} \bmod N$$

[0047] 상술한 BCP 암호 기법은 덧셈에 대한 동형 성질을 갖기 때문에 메시지의 합에 대한 암호문을 생성할 수 있고, 지수승 연산을 통해 메시지의 상수배에 대한 암호문을 생성할 수 있다.

[0048] 즉, 덧셈에 대한 동형성질을 이용하여 두 암호문 $(A, B) = (g^r \bmod N^2, h^r (1 + mN) \bmod N^2)$ 와 $(A', B') = (g^{r'} \bmod N^2, h^{r'} (1 + m'N) \bmod N^2)$ 에 대해 각 항목의 값을 곱하면 두 암호문의 메시지를 더한 값(m + m´)의 암호문 $(AA', BB') = g^{r+r'} \bmod N^2, h^{r+r'} (1 + (m + m')N) \bmod N^2$ 을 계산할 수 있다.

[0049] 또한, 암호문 $(A,B)=(g^r \bmod N^2, h^r(1+mN) \bmod N^2)$ 의 각 항목에 $\sigma \in Z_N$를 지수승하면 mσ 에 대한 암호문 $(A^\sigma, B^\sigma)=(g^{\sigma r} \bmod N^2, h^{\sigma r}(1+\sigma mN) \bmod N^2)$ 을 생성할 수 있다.

[0050] 또한, 본 발명에서는 임계치 이상의 사용자 데이터가 모였을 때 병합 가능하도록 하기 위하여, Shamir의 비밀 분산 기법(Shamir' s Threshold Secret Sharing) 이용한다. 1979년 Shamir에 의하여 제안된 기법으로 라그랑지 보간법(Largrange interpolation)을 이용하여 임계기능을 제공하는 기법이다. 라그랑지 보간법이란 t개의 순서쌍이 주어졌을 때 이를 만족시키는 $(t-1)$차 다항식 위의 점(순서쌍)을 계산하는 방법이다. 비밀 분산 기법에서 기본적으로 분배자(Dealer)는 수신자들에게 분할된 정보에 대한 비밀을 보장하여야 하며, k명의 수신자 집합에 분할된 정보 중 임의의 t명 이상이 정보를 재구성하였을 때 비밀 정보가 복원되어야 한다. Shamir가 제안한 비밀 분산 기법은 아래와 같다.

[0051] 분배자는 비밀 정보 $s=a_0$를 상수항으로 하는 랜덤한 $(t-1)$차 다항식 $f(x)$를 선택한다. 단, 유한체 $GF(p)$에서 계산이 되고, 비밀 정보 s또한 유한체 $GF(p)$에 속해 있다. 여기서 p는 비밀 정보 s보다 큰 소수이다.

[0052] $$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1} \pmod p$$

[0053] 분배자는 각 수신자(사용자) $i\,(1 \le i \le k)$에게 분할된 정보 $f(i)$를 전송한다.

[0054] k명에게 분할된 정보 중 최소 t명(임계값)이 모였을 때, 라그랑지 보간법에 의해 $f(0)$값인 비밀 정보 $s=a_0$를 구할 수 있다.

[0055] 이하, 도 1 내지 도 3를 참조하여, 본 발명의 일 실시예에 따른 프라이버시를 보장하는 시계열 데이터의 임계 병합 시스템에 대해 상술한다.

[0056] 도 1은 본 발명의 일 실시예에 따른 프라이버시를 보장하는 시계열 데이터의 임계 병합 시스템(10)을 도시한다. 도 1을 참조하면, 시계열 데이터 임계 병합 시스템(10)은 분배자 장치(100), 복수의 사용자 장치(200, 300)를 포함한다.

[0057] 사용자 장치는 네트워크 망을 통하여 분배자 장치(100) 및 다른 사용자 장치들과 통신할 수 있다. 일 실시예에 따른 네트워크 망은, 개방형 인터넷, 폐쇄형 인트라넷을 포함한 유선 인터넷망, 이동 통신망과 연동된 무선 인터넷 통신망 뿐만 아니라, 각종 데이터 통신이 가능한 컴퓨터 네트워크 등의 가능한 통신 수단을 포함하는 넓은 개념이다.

[0058] 도 2는 도 1에 도시된 분배자 장치(100)의 기능 블럭도이다.

[0059] 도 1과 도 2를 참조하면, 상기 시스템을 세팅하는 분배자(Dealer) 장치(100)는 셋업부(110), 비밀키 생성부(120), 통신부(170), 저장부(180), 및 제어부(190)을 포함한다.

[0060] 본 명세서에서 사용되는 '~부' 또는 '모듈'이라 함은 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 '~부' 또는 '모듈'은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나 한 종류의 하드웨어를 의미하는 것은 아니다.

[0061] 분배자 장치(100)는 초기에 시계열 데이터 임계 병합 시스템을 설정하고, 임계 기능 제공을 위한 비밀키를 생성한다.

[0062] 분배자 장치(100)의 셋업부(110)는 제어부(190)의 제어 하에, 덧셈에 대한 동형 성질을 제공하는 암호 기법의 셋업 알고리즘(예를 들어, BCP.Setup)을 이용하여 공개 파라미터(PP=(N,k,g))와 마스터키(MK=(p´,q´))를 생성한다. 이때, 마스터키는 분배자 장치(100)의 저장부(180)에 안전하게 저장하고, 공개 파라미터는 시스템(10)의 사용자 장치에 공개한다.

[0063] 분배자 장치(100)의 비밀키 생성부(120)는 제어부(190)의 제어 하에, $q(0)=0$을 만족하는 t차 다항식 $q(x)$를 랜덤하게 선택한다. 분배자 장치(100)는 각 사용자 장치(i)에 대하여 임계기능 제공을 위한 비밀키($s_i=q(i)$)를 생성하여 각 사용자 장치(i)에게 전송한다. 이때, t는 이후 취합자 장치(300)의 병합 및 복호화을 위한 임계값이다.

[0064] 통신부(170)는 제어부(190)의 제어 하에, 사용자 장치(200, 300)들과 통신을 수행할 수 있다. 즉, 통신부(170)는 각각의 사용자 장치에 공개 파라미터(PP) 또는 비밀키(s_i)를 전송할 수 있다.

[0065] 저장부(180)는 프로그램 메모리와 데이터 메모리를 포함할 수 있다. 상기 프로그램 메모리는 분배자 장치(100)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 메모리에는 상기 프로그램들을 수행하는 과정 중에 발생하는 데이터들이 저장될 수 있다.

[0066] 제어부(190)는 분배자 장치(100)의 전반적인 동작을 제어한다. 즉, 셋업부(110), 비밀키 생성부(120), 통신부(170) 및 저장부(180)의 동작을 제어할 수 있다.

[0067] 도 3는 도 1에 도시된 사용자 장치(200, 300), 특히, 취합자 장치(300)의 기능 블럭도이다. 도 1에는 2개의 사용자 장치가 도시되어 있으나, 시계열 데이터 임계 병합 시스템(10)에 포함된 사용자 장치의 개수는 2 이상일 수 있다. 사용자 장치는 데이터 병합에 필요한 데이터를 생성하는 장치이며, 데이터를 병합하는 취합자 장치(300)는 상기 시스템(10)에 포함된 복수의 사용자 장치 중 하나일 수 있다. 또한, 취합자 장치(300)는 상기 시스템(10)에 포함된 복수의 사용자 장치 중 하나를 임의로 선택할 수 있다.

[0068] 도 1과 도 3를 참조하면, 취합자 장치(300)는 키생성 모듈(310), 암호화 모듈(320), 병합 및 복호화 모듈(330), 통신 모듈(370), 메모리(380), 및 제어 모듈(390)을 포함한다.

[0069] 취합자 장치(300)를 포함하는 사용자 장치의 키생성 모듈(310)은 덧셈에 대한 동형 성질을 제공하는 동형 암호 기법의 키생성 알고리즘(예를 들어, BCP.KeyGen)을 수행하여 데이터 암호화를 위한 각각의 사용자 장치 i의 공개키와 개인키(pk_i, sk_i)를 생성한다. 즉, 취합자 장치(j, 300)의 키생성 모듈(310)은 동형 암호 기법의 키생성 알고리즘을 수행하여 취합자 장치(j, 300)의 공개키(pk_j) 및 개인키(sk_j)를 생성하고, 공개키(pk_j)를 공개한다.

[0070] 취합자 장치(300)를 포함하는 사용자 장치의 암호화 모듈(320)은 데이터($x_i \in Z_p$) 암호화한다. 구체적으로, 먼저, 각각의 사용자 장치의 데이터(x_i)에 대하여, 복수의 사용자 장치 중 데이터 취합자로 결정된 취합자 장치(j, 300)의 상기 공개키(pk_j)를 이용하여 덧셈에 대한 동형 성질을 제공하는 동형 암호 기법의 암호화 알고리즘(예를 들어, BCP.Enc)을 수행하여 취합자 장치(j, 300)의 상기 공개키(pk_j)에 대한 제1 암호문 $Enc_{pk_j}(x_i)$을 생성한다. 다음, 시간 T에 대한 제2 암호문 C_i를 아래와 같이 생성한다.

[0071] $$C_i = \left(Enc_{pk_j}(x_i) H(T)^{s_i \triangle_{i,S\cup j}(0)} \right)$$

[0072] 이때, S는 병합에 참여하는 사용자 장치의 집합을 의미하며, j는 취합자 장치(300)를 의미한다. $\triangle_{i,S}(x) = \prod_{j\in S, j\neq i} \frac{x-j}{i-j}$는 $i \in Z_p$와 집합 S에 대한 라그랑지 계수(Lagrange coefficient)이다.

[0073] 취합자 장치(300)의 병합 및 복호화 모듈(330)은 분배자 장치(100)로부터 수신한 취합자 장치(j, 300)의 비밀키(s_j)를 이용하여 병합 시스템(10)에 포함된 사용자 장치들로부터 수신한 시간 T에 대한 암호문(C_i)들을 병합하여 병합된 암호문(V)을 생성한다.

[0074] $$V \leftarrow H(T)^{s_j \triangle_{j,S\cup j}(0)} \prod_{i \in S} C_i$$

[0075] 이때, 집합 S의 원소의 개수가 t 이상인 경우, 즉, 병합에 참여하는 사용자 장치의 수가 t 이상인 경우, 취합자 장치(300)를 포함하면 총 $(t+1)$개 이상의 분할된 정보를 얻을 수 있기 때문에 라그랑지 보간법에 의하여 t차 다항식 $q(x)$의 상수항인 $q(0)$값을 도출해낼 수 있다. ,

[0076] $$\sum_{i \in S\cup j} s_i \triangle_{i,S\cup j}(0) = q(0) = 0$$

[0077] 따라서, 병합에 참여하는 사용자 장치의 수가 t 이상인 경우, 병합된 암호문(V)는 아래의 등식을 만족한다.

[0078] $$V = Enc_{pk_j}\left(\sum_{i \in S} x_i\right)$$

[0079] 다음, 취합자 장치(300)의 병합 및 복호화 모듈(330)은 취합자 장치(300)의 개인키(sk_j)로 덧셈에 대한 동형 성질을 제공하는 동형 암호 기법의 복호화 알고리즘(예를 들어, DCP.Dec)을 수행하여 최종 연산 결과인 $\sum_{i \in S} x_i$를 얻을 수 있다.

[0080] 취합자 장치(300)는 각 사용자 장치로부터 암호문 C_i를 전송받아도 임계기능 제공을 위한 사용자의 비밀키 s_i를 알 수 없기 때문에 자신의 개인키 sk_j를 이용하더라도 데이터 x_i에 대한 정보를 얻을 수 없다.

[0081] 실시예에 따라, 취합을 수행하지 아니하는 사용자 장치의 경우 병합 및 복호화 모듈(330)의 구성을 생략할 수 있다.

[0082] 통신 모듈(370)은 제어 모듈(390)의 제어 하에, 다른 사용자 장치 또는 분배자 장치(100)와 유선 또는 무선 통신망을 통하여 통신을 수행할 수 있다.

[0083] 메모리(380)는 프로그램 메모리와 데이터 메모리를 포함할 수 있다. 상기 프로그램 메모리에는 사용자 장치(200, 300)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 메모리에는 상기 프로그램들을 수행하는 과정 중에 발생되는 데이터들이 저장될 수 있다.

[0084] 제어 모듈(390)은 취합자 장치(300)를 포함하는 사용자 장치의 전반적인 동작을 제어한다. 즉, 키생성 모듈(310), 암호화 모듈(320), 병합 및 복호화 모듈(330), 통신 모듈(370), 및 메모리(380)의 동작을 제어할 수 있다.

[0085] 도 4는 도 1에 도시된 시계열 데이터 임계 병합 시스템을 이용한 프라이버시를 보장하는 시계열 데이터의 임계 병합 방법을 설명하기 위한 흐름도이다. 이하에서는 상술된 내용과 중복되는 내용에 관한 기재는 생략하기로 한다.

[0086] 먼저, 분배자 장치(100)는 동형 암호 기법의 셋업 알고리즘(BCP.Setup)을 수행하여 공개 파라미터(PP=(N,k,g))와 마스터키(MK=(p´,q´))를 생성한다(S100).

[0087] 다음, 분배자 장치(100)는 $q(0)=0$을 만족하는 t차 다항식 $q(x)$를 랜덤하게 선택한다. 분배자 장치(100)는 각 사용자 장치(i)에 대하여 임계기능 제공을 위한 비밀키($s_i = q(i)$)를 생성(S200)하여 취합자 장치(j)를 포함하는 각 사용자 장치(i)에게 전송한다.

[0088] 다음, 취합자 장치(300, j)를 포함하는 각 사용자 장치(i)는 동형 암호 기법의 키생성 알고리즘(BCP.KeyGen)을 수행하여 데이터 암호화를 위한 공개키 및 개인키 쌍 (pk_i, sk_i)을 생성하고(S300), 공개키를 통신망을 통하여 공개한다.

[0089] 취합자 장치(300, j)를 포함하는 각 사용자 장치(i)는 데이터(x_i)를 암호화하여 암호문 C_i를 생성한다(S400). 암호문 생성 단계는 동형 암호 기법을 이용하여 암호문을 생성하는 단계 및 시간 T에 대한 암호문을 생성하는 단계로 구분할 수 있다.

[0090] 구체적으로, 먼저, 각각의 사용자 장치(i)는 각 사용자 장치(i)에서 생성한 데이터(x_i)에 대하여, 취합자 장치(j, 300)의 공개키(pk_j)를 이용하여 동형 암호 기법의 암호화 알고리즘(BCP.Enc)을 수행하여 상기 취합자 장치의 공개키(pk_j)에 대한 제1 암호문 $Enc_{pk_j}(x_i)$을 생성한다.

[0091] 다음, 시간 T에 대한 제2 암호문 C_i를 아래와 같이 생성한다.

[0092] $$C_i = \left(Enc_{pk_j}(x_i) H(T)^{s_i \triangle_{i,S\cup j}(0)}\right)$$

[0093] 이때, S는 병합에 참여하는 사용자 장치의 집합을 의미한다.

[0094] 다음, 취합자 장치(300)는 각 사용자 장치(i)로부터 제2 암호문 C_i를 수신한다(S500).

[0095] 다음, 취합자 장치(300)는 분배자 장치(100)로부터 수신한 취합자 장치(j, 300)의 비밀키(s_j)를 이용하여 상기 제2 암호문(C_i)들을 병합하여 병합된 암호문(V)을 아래와 같이 생성한다(S600).

[0096] $$V \leftarrow H(T)^{s_j \triangle_{j,S\cup j}(0)} \prod_{i\in S} C_i$$

[0097] 이때, 병합에 참여하는 사용자 장치의 수가 t 이상인 경우, 라그랑지 보간법에 의하여 t차 다항식 $q(x)$의 상수항인 $q(0)$값을 도출해낼 수 있으며, 병합된 암호문(V)는 아래의 등식을 만족한다.

[0098] $$V = Enc_{pk_j}\left(\sum_{i\in S} x_i\right)$$

[0099] 다음, 취합자 장치(300)는 취합자 장치(300)의 개인키(sk_j)로 동형 암호 기법의 복호화 알고리즘(DCP.Dec)을 수행하여 상기 병합된 암호문(V)을 복호화하고(S700), 최종 연산 결과인 $\sum_{i\in S} x_i$를 얻을 수 있다.

[0100] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

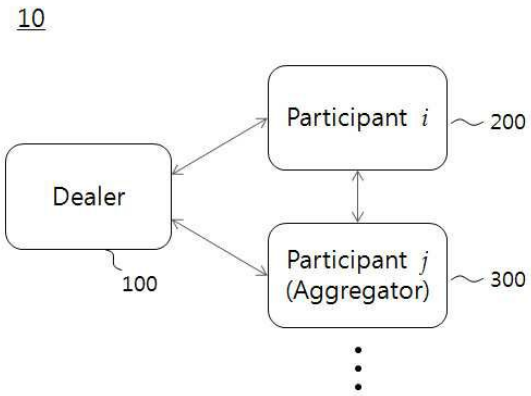
[0101] 10 : 시계열 데이터 임계 병합 시스템

100 : 분배자 장치 200 : 사용자 장치

300 : 취합자 장치

도면

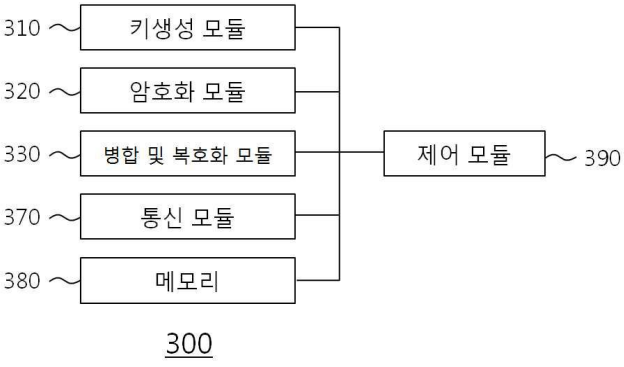
도면1



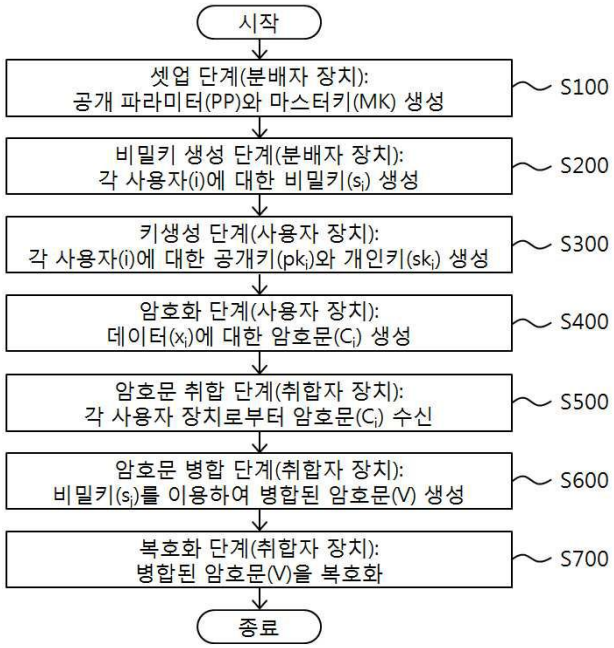
도면2



도면3



도면4


시작
셋업 단계(분배자 장치):
공개 파라미터(PP)와 마스터키(MK) 생성
S100
비밀키 생성 단계(분배자 장치):
각 사용자(i)에 대한 비밀키(s_i) 생성
S200
키생성 단계(사용자 장치):
각 사용자(i)에 대한 공개키(pk_i)와 개인키(sk_i) 생성
S300
암호화 단계(사용자 장치):
데이터(x_i)에 대한 암호문(C_i) 생성
S400
암호문 취합 단계(취합자 장치):
각 사용자 장치로부터 암호문(C_i) 수신
S500
암호문 병합 단계(취합자 장치):
비밀키(s_i)를 이용하여 병합된 암호문(V) 생성
S600
복호화 단계(취합자 장치):
병합된 암호문(V)을 복호화
S700
종료