(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년05월07일
(11) 등록번호 10-1391628
(24) 등록일자 2014년04월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/22 (2006.01)
(21) 출원번호 10-2012-0129495
(22) 출원일자 2012년11월15일
심사청구일자 2012년12월04일
(56) 선행기술조사문헌
Cory Thoma, "Protecting Consumers: The Smart Grid and Your Data", Honors in Information Technology Leadership, Fall 2011
JP2012113670 A
KR1020130036522 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)
박승환
서울 성북구 안암로 145, 정보보호대학원 (안암동5가, 고려대학교)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 8 항 심사관 : 이병수

(54) 발명의 명칭 **스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 방법 및 그 시스템**

(57) 요 약

본 발명은 스마트 그리드(smart grid)에서 전력 소비 정보의 기밀성과 무결성을 보장하는 방법에 관한 것으로, 보다 상세하게는 전력 소비자의 전력 소비 정보(metering data)에 대한 기밀성을 보장하고, 전력 소비 정보와 이에 근거한 전력 사용 가격(billing data)의 무결성을 보장하는 방법에 관한 것이다.

개시되는 방법은 a)스마트 그리드(smart grid)의 각 스마트 미터기 i(i ■ {1,…,n})가 전력 소비 정보(metering data)를 은닉하기 위한 난수값을 생성하는 단계; b)상기 각 스마트 미터기 i가 상기 미터링 데이터 $m_{i,j}$(j ■ {1,…,k})를 은닉한 값과 상기 $m_{i,j}$의 서명을 포함한 미터링 데이터 $\sigma_{i,j}$를 생성하는 단계; 및 c)상기 각 스마트 미터기 i가 상기 $m_{i,j}$에 대한 빌링 데이터(billing data) ψ_i를 생성하는 단계를 포함하고, d)상기 $m_{i,j}$의 서명의 유효성을 검증하는 단계; 및 e)상기 ψ_i의 정확성을 검증하는 단계를 더 포함하여 본 발명의 과제를 해결한다.

대 표 도 - 도3

이 발명을 지원한 국가연구개발사업

과제고유번호	ITAH0301120330070001000100100
부처명	정보통신산업진흥원
연구사업명	대학IT연구센터육성지원사업
연구과제명	스마트 그리드 보안 연구센터(스마트 그리드 보안기술 개발)
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2012.01.01 ~ 2012.12.31

특허청구의 범위

청구항 1

a)스마트 그리드(smart grid)의 각 스마트 미터기 i(i ∈ {1,…,n})가 전력 소비 정보(metering data)를 은닉하기 위한 난수(random number)를 생성하는 단계;

b)상기 각 스마트 미터기 i가 상기 전력 소비 정보 $m_{i,j}$(j ∈ {1,…,k})를 상기 난수를 이용해 은닉한 값과 상기 $m_{i,j}$의 서명을 포함한 전력 소비 정보 $\sigma_{i,j}$를 생성하는 단계; 및

c)상기 각 스마트 미터기 i가 상기 $m_{i,j}$에 대한 빌링 데이터(billing data) ψ_i를 생성하는 단계를 포함하되,

상기 $\sigma_{i,j}$에는 상기 $m_{i,j}$의 서명의 위변조를 방지하기 위한 임의의 값이 더 포함되는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 방법.

여기서, 상기 j는 미터링 총 기간을 여러 시간대로 분할한 경우의 각 시간대를 의미함.

청구항 2

제 1 항에 있어서,

d)상기 스마트 그리드의 미터 정보 관리 시스템(Meter Data Management System: MDMS)이 상기 $m_{i,j}$의 서명의 유효성을 검증하는 단계; 및

e)상기 MDMS가 상기 ψ_i의 정확성을 검증하는 단계를 더 포함하는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 방법.

청구항 3

제 1 항에 있어서,

상기 난수는 상기 $m_{i,j}$에 더해져서 상기 은닉이 이루어지는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 방법.

청구항 4

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 난수를 $x_{i,j}$라고 할 때, 상기 $x_{i,j}$는 다음의 식을 만족하는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 방법.

$$\sum_{i=1}^{n} x_{i,j} = 0 \bmod p \,(\text{for each } j) \quad \text{and} \quad \sum_{j=1}^{k} x_{i,j} = 0 \bmod p \,(\text{for each } i)$$

청구항 5

삭제

청구항 6

스마트 그리드(smart grid)의 각 스마트 미터기 i(i ∈ {1,…,n})에 의해 측정된 전력 소비 정보(metering data)를 은닉하기 위한 난수(random number)를 생성하는 난수 생성부;

상기 전력 소비 정보 $m_{i,j}$(j ∈ {1,…,k})를 상기 난수를 이용해 은닉한 값과 상기 $m_{i,j}$의 서명을 포함한 전력 소비 정보 $\sigma_{i,j}$를 생성하는 은닉부; 및

상기 $m_{i,j}$에 대한 빌링 데이터(billing data) ψ_i를 생성하는 빌링 데이터 생성부를 포함하되,

상기 $\sigma_{i,j}$에는 상기 $m_{i,j}$의 서명의 위변조를 방지하기 위한 임의의 값이 더 포함되는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 시스템.

여기서, 상기 j는 미터링 총 기간을 여러 시간대로 분할한 경우의 각 시간대를 의미함.

청구항 7

제 6 항에 있어서,

상기 $m_{i,j}$의 서명의 유효성을 검증하는 유효성 검증부; 및

상기 ψ_i의 정확성을 검증하는 정확성 검증부를 더 포함하는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 시스템.

청구항 8

제 6 항에 있어서, 상기 은닉부는

상기 난수를 상기 $m_{i,j}$에 더해서 상기 은닉을 하는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 시스템.

청구항 9

제 6 항 내지 제 8 항 중 어느 한 항에 있어서,

상기 난수를 $x_{i,j}$라고 할 때, 상기 $x_{i,j}$는 다음의 식을 만족하는 것을 특징으로 하는 스마트 그리드에서 전력 소비 정보의 기밀성과 무결성을 보장하는 시스템.

$$\sum_{i=1}^{n} x_{i,j} = 0 \bmod p \,(\text{for each } j) \quad \text{and} \quad \sum_{j=1}^{k} x_{i,j} = 0 \bmod p \,(\text{for each } i)$$

청구항 10

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 스마트 그리드(smart grid)에서 전력 소비 정보의 기밀성과 무결성을 보장하는 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 전력 소비자의 전력 소비 정보(metering data)에 대한 기밀성을 보장하고, 전력 소비 정보와 이에 근거한 전력 사용 가격(billing data)의 무결성을 보장하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 스마트 그리드(smart grid)는 '지능형 전력망'을 의미하는 것으로, 기존의 전력망에 정보 기술(IT)을 접목하여, 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환하고 에너지 효율을 최적화하는 차세대 전력망을 말한다. IT 기술이 발전하면서 에너지 부문에서도 양방향 통신 접목이 가능해지고, 태양풍력 등 출력이 불규칙한 신재생 전원의 보급을 확대시킬 수 있다는 점에서 많은 관심을 끌고 있다.

[0003] 스마트 그리드(지능형 전력망)의 가장 큰 장점은 에너지를 효율적으로 사용할 수 있다는 것이다. 예를 들면 집안 세탁기는 가장 싼 전기 요금 시간대에 맞춰 작동하고, 전기 자동차는 주간에 주차해도 심야에 맞춰 싼 요금으로 충전한다. 또 소비자 전력관리 장치를 통해 전기 사용 행태나 전기 요금 등을 실시간으로 살펴볼 수 있어 소비자의 자발적인 에너지절약에도 도움이 된다.

[0004] 스마트 그리드의 가장 큰 목적은 전력 소비가 많아지는 피크(peak) 시간에 실시간으로 가격을 높이거나 이전의 전력 소비 기록들로부터 수요를 예측해서 시간대별 소비 가격을 달리하여 전체적인 에너지 소비를 줄이거나 효율적인 사용을 유도하는 것이다. 이를 위해서는 시간대별 전력 소비 정보(metering data)의 수집이 정확히 이루어져야 한다.

[0005] 스마트 그리드를 형성하는 각 요소에 대해 간단히 살펴보면 다음과 같다.

[0006] AMI(Advanced Metering Infrastructure)는 스마트 그리드에서 스마트 미터기, DCU(Data Collecting Unit)와 서버 간에 전력 소비 정보 및 DR 정보(Demand Response info: 전력 정보의 수요 반응 정보) 등을 주고받기 위한 양방향성 원격 검침 시스템으로 스마트 그리드와 거의 대등한 개념으로 사용된다. AMI에서는 실시간 전체 소비량에 따라 전기 사용료를 달리 하기 위하여 소정의 짧은 시간 간격(time interval, 예를 들어 10~15분)마다 주기적으로 전력 소비 정보가 스마트 미터기에서 서버로 전송된다.

[0007] 스마트 미터기는 댁내에 설치가 되어 있는 전력 검침계로 댁내의 전력 소비 정보를 모아서 상기한 DCU에 전송한다. 스마트 미터기에는 안전한 키 저장과 암호 알고리즘을 수행하기 위한 TPM(Trusted Platform Module)이 설치되어 있다. DCU는 작은 지역별 혹은 아파트 단지별로 설치가 되어 있으며, 하나의 DCU에는 200 내지 300개의 스마트 미터기가 연결되어 있고 스마트 미터기들로부터 전력 소비 정보를 수집하여 미터 정보 관리 시스템(Meter Data Management System: MDMS, 통상 '서버'로 칭하며 이하 MDMS를 '서버'로 약칭함)로 전송한다. 서버는 DCU로부터 수집된 전력 소비 정보(검침 정보)를 받으며, 서버는 검침 정보를 사용자별 요금 청구를 하거나 실시간 요금 정산 및 미래 수요 예측을 하는데 사용한다.

[0008] 한편 스마트 미터기에서 서버까지 전송되는 전력 소비 정보는 하루 동안의 전력 소비자에 대한 전력 사용 패턴을 보여주기 때문에 전력 소비가 큰 세탁기를 돌리는 시간이나 집을 비우는 시간 등 전력 소비자의 프라이버시 노출에 대한 우려가 있다. 전력 소비 정보는 AMI 내의 통신 구간에서 암호화를 통해 외부로의 프라이버시 노출을 막을 수 있지만 정보를 수집하는 서버 측에는 프라이버시 노출의 위험이 여전히 존재한다. 또한, 전력 소비 정보는 소비한 전력량에 따라서 과금이 되어야 하기 때문에 소비된 전력량에 대하여 부인(deny)할 수 없어야 하고, 소비된 전력량이 변경 혹은 조작되어 전송되지 않아야 한다. 이는 전력 소비 정보에 대한 무결성이 보장되어야 한다는 의미이다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 배경을 인식하여 창안된 것으로, 본 발명이 해결하고자 하는 과제는 스마트 그리드에서 전력 사용자의 프라이버시 노출 가능성을 차단하기 위해 전력 소비 정보에 대한 기밀성을 보장하는 방안을 제시하는 것이다.

[0010] 본 발명이 해결하고자 하는 또 다른 과제는 스마트 그리드에서 전력 소비 정보와 전력 소비 정보에 대한 빌링 데이터의 무결성을 보장할 수 있도록 하는 방안을 제시하는 것이다.

과제의 해결 수단

[0011] 상기와 같은 과제를 해결하기 위해 개시되는 방법은 a)스마트 그리드(smart grid)의 각 스마트 미터기 i($i \in \{1,\cdots,n\}$)가 전력 소비 정보(metering data)를 은닉하기 위한 난수값을 생성하는 단계; b)상기 각 스마트 미터기 i가 상기 미터링 데이터 $m_{i,j}$($j \in \{1,\cdots,k\}$)를 은닉한 값과 상기 $m_{i,j}$의 서명을 포함한 미터링 데이터 $\sigma_{i,j}$를 생성하는 단계; 및 c)상기 각 스마트 미터기 i가 상기 $m_{i,j}$에 대한 빌링 데이터(billing data) Ψ_i를 생성하는 단계를 포함하고, d)상기 $m_{i,j}$의 서명의 유효성을 검증하는 단계; 및 e)상기 Ψ_i의 정확성을 검증하는 단계를 더 포함하여 상기한 과제를 해결한다.

[0012] 상기와 같은 과제를 해결하기 위해 개시되는 시스템은 스마트 그리드(smart grid)의 각 스마트 미터기 i($i \in \{1,\cdots,n\}$)에 의해 측정된 전력 소비 정보(metering data)를 은닉하기 위한 난수(random number)를 생성하는 난수 생성부; 상기 미터링 데이터 $m_{i,j}$($j \in \{1,\cdots,k\}$)를 상기 난수를 이용해 은닉한 값과 상기 $m_{i,j}$의 서명을 포함한 미터링 데이터 $\sigma_{i,j}$를 생성하는 미터링 데이터 은닉부; 및 상기 $m_{i,j}$에 대한 빌링 데이터(billing data) Ψ_i를 생성하는 빌링 데이터 생성부를 포함하고, 상기 $m_{i,j}$의 서명의 유효성을 검증하는 유효성 검증부; 및 상기 Ψ_i

의 정확성을 검증하는 정확성 검증부를 더 포함하여 상기한 과제를 해결한다.

발명의 효과

[0013] 본 발명에 의하면 전력 사용자측(스마트 미터기)에서 자신의 전력 사용 정보가 은닉되어 그 사용 정보에 대한 서명과 같이 서버에 전송되므로 전력 사용 정보에 대한 기밀성을 보장할 수 있으며, 전력 사용 정보가 서버에 노출되지 아니하더라도 서명의 유효성 검증을 통해 소비된 전력량이 변경 혹은 조작 가능성을 차단함으로서 전력 소비 정보에 대한 무결성을 보장할 수 있다.

도면의 간단한 설명

[0014] 도 1은 전력 소비 정보를 시간대별(Time) 그리고 사용자별(Customers)로 2차원 그래프로 일례를 제시한 도면이다.

도 2는 본 시스템 발명의 구성을 제시한 도면이다.

도 3은 본 방법 발명의 흐름을 제시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하, 본 발명을 실시하기 위한 구체적인 내용을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0016] 도 1은 전력 소비 정보를 시간대별(Time) 그리고 사용자별(Customers)로 2차원 그래프로 일례를 제시한 도면이다. Time는 분(minute) 단위로 1440분은 24시간(하루)에 해당한다.

[0017] 서버가 전력 소비 정보를 근거로 사용자별 요금 청구를 하거나 실시간 요금을 정산하기 위해 필요한 정보는 사용자별 하루의 총 전력 소비량을 나타내는 열(column)의 합(예를 들어 도 1에서 사용자 C_3의 경우)과 전력 소비 피크 시간대(예를 들어 도 1에서 15분~30분의 15분간)를 나타내는 행(row)의 합이다.

[0018] 도 2는 본 시스템 발명의 구성을, 도 3은 본 방법 발명의 흐름을 제시한 도면이다.

[0019] 본 발명에 의한 전력 소비 정보의 기밀성과 무결성을 보장하기 위해서 각각 소정의 암호화 기법 및 서명 기법이 전력 소비 정보에 적용되는데, 기밀성 보장을 위해 사용자와 서버 간에 안전한 키 길이를 갖는 대칭키 암호화 기법(AES(Advanced Encryption Standard) 등)이 적용되며, 무결성 보장을 위해 ECC(Elliptic Curve Cryptosystem)에서 정의되는 전자 서명 기법(DSA((Digital Signature Algorithm) 등)이 적용될 수 있다.

[0020] 본 발명에 의한 전력 소비 정보의 기밀성과 무결성을 보장하는 구현 방안은 여섯 단계로 이루어지는 다항식 시간 알고리즘(polynomial-time algorithms)으로 구성된다.

[0021] <제1 단계: Init(1^{λ})>

[0022] 서버가 보안 파라미터(security parameter) λ를 입력받아 공개 파라미터 PP를 생성하는 단계이다(s31).

[0023] <제2 단계: Setup(PP)>

[0024] 스마트 미터기가 PP를 입력받아 전력 소비자의 공개키 PK와 전력 소비자의 비밀키 SK를 생성하는 단계이다(s32).

[0025] <제3 단계: Metering(m, PP, PK, SK)>

[0026] 스마트 미터기가 PP, PK, SK, 실제의 전력 소비 정보 m을 입력받아 m을 은닉시킨 미터링 데이터 σ를 생성하는 단계이다(s33). σ에는 소정의 서명 스킴(signature scheme)에 의한 전력 소비 정보에 대한 서명이 포함된다. 이러한 은닉을 통해 제3자 뿐만이 아니라 전력 소비 정보를 수집하는 서버조차도 전력 소비 정보를 상세히 알지 못하게 된다.

[0027] <제4 단계: Verifying metering data(σ, PP, PK)>

[0028] 서버가 σ, PP, PK을 입력받아 미터링 데이터 σ에 포함된 서명이 실제의 전력 소비 정보 m에 대한 유효한 서명(valid signature)인지를 검증(체크)하는 단계이다(s34).

[0029] <제5 단계: Billing(m, tariff)>

[0030] 스마트 미터기가 m과 시간별 전력 사용 요금(tariff)을 입력받아 전력 소비 정보 m에 대한 빌링 데이터(billing data) ψ를 생성하는 단계이다(s35).

[0031] <제6 단계: Verifying billing data(σ, PP, ψ)>

[0032] 서버가 스마트 미터기로부터 ψ를 입력받아 빌링 데이터(billing data) ψ가 올바르게 산출되었는지 검증(체크)하는 단계이다(s36).

[0033] 이하에서는 상기한 각 단계의 구현 방안을 상세히 설명한다.

[0034] <제1 단계: Init(1^k)>

[0035] i가 각 전력 소비자측에 구비된 스마트 미터기(i ∈ {1,…,n}, 각 소비자 i로도 표현 가능)를, j가 미터링 총 기간(예를 들어 도 1에서와 같이 1440분)을 여러 시간대(도 1의 경우에는 15분을 하나의 시간 단위로 하여 96개의 시간대)로 분할한 경우의 각 시간대(j ∈ {1,…,k})를 지정한다고 하자(도 1의 경우에는 k = 96). 우선 서버는 ECC에서 정의되는 전자 서명 알고리즘을 선택하고 이를 구동시켜 서명용 공개키 PP_{sign}을 생성한다. 한편 ECC에서 정의되는 전자 서명 알고리즘은 기존에 제시된 것을 사용할 수 있는데, 예를 들어 상기한 DSA 알고리즘, LW-signature 알고리즘(A. Lewko, B. Waters, New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts, In: TCC 2010, LNCS 5978, pp. 455-479, 2010), BLS-signature 알고리즘(Dan Boneh, Ben Lynn, and Hovav Shacham, Short signatures from the Weil pairing, In: Journal of Cryptology, 17(4):pp. 297-319, 2004. Extended abstract in Proceedings of Asiacrypt 2001, LNCS vol.2248), BB-signature 알고리즘(Dan Boneh and Xavier Boyen, Short signatures without random oracles, In: Advances in Cryptology. EUROCRYPT 2004, vol.3027, pp. 56-73. Springer-Verlag, 2004) 등이다. 이들 서명 알고리즘은 소정의 서명 검증 모듈도 아울러 포함하며 이하에서 언급될 검증은 서버가 선택한 ECC에서 정의되는 전자 서명 알고리즘에 의해 이루어진다.

[0036] 서버는 다음으로 겹선형 함수(bilinear map)와 관련된 순환 군(cyclic group) (G, G_T, e)을 생성한다. 이때 G와 G_T는 소수(prime number) p를 위수(位數)로 가지며, g는 G의 생성원이다. e는 e: $G \times G \rightarrow G_T$를 만족하는 어드미서블 겹선형 함수(admissible bilinear map)이다. 또한 해시 함수(hash function) H: $Z_p \rightarrow Z_p$를 선택한다.

[0037] 서버는 이들을 이용하여 공개 파라미터 PP를 다음과 같이 생성한다.

[0038] $PP = (PP_{sign}, PP_{enc}, p, e, g, H)$.

[0039] PP_{sign}는 전력 소비 정보에 대한 서명용 공개키이고, PP_{enc}는 전력 소비 정보에 대한 암호화용 공개키이다.

[0040] <제2 단계: Setup(PP)>

[0041] 전력 소비자들 사이에는 인증된 채널(authenticated channel)이 있음을 가정한다. 각 스마트 미터기 i는 자신의 공개키(PK_i)와 비밀키(SK_i)를 생성하여 서버에 전송한다. 각 스마트 미터기 i는 아울러 임의의 값 h_i(∈ G)을 선택하고 각 스마트 미터기 i에 구비된 난수 생성부(21)는 아래의 식을 만족하는 난수(random number) $x_{i,j}$(∈ Z_p)를 생성한다. 이 난수는 실제의 미터링 데이터(real metering data) $m_{i,j}$을 은닉(concealment)하여 전력 소비 정보의 기밀성을 보장하기 위해 사용되는 것으로 다음의 식을 만족하도록 선택된다.

[0042] $$\sum_{i=1}^{n} x_{i,j} = 0 \bmod p \,(\text{for each } j) \quad \text{and} \quad \sum_{j=1}^{k} x_{i,j} = 0 \bmod p \,(\text{for each } i)$$

[0043] $x_{i,j}$를 행렬 M으로 표현하면 다음과 같다.

[0044] $$M=\begin{pmatrix} x_{1,1} & \cdots & x_{1,k} \\ \cdots & x_{i,j} & \cdots \\ x_{n,1} & \cdots & x_{n,k} \end{pmatrix}$$. 즉, 서버는 행렬 M의 각 행의 합과 각 열의 합은 0이 되도록 난수 $x_{i,j}$를 선택하는 것이다.

[0045] 난수 $x_{i,j}$를 상기한 식을 만족하도록 선택(생성)하는 이유는 서버에서 얻고자 하는 전력 소비 정보가 도 1에 제시된 그래프의 행의 합과 열의 합이라는 사실에서 기인한다. 전력 소비 정보는 주기적으로 하나씩 서버에 보내지고 그 합은 서버에서 계산한다. 미터링 데이터를 은닉하는 값이 합을 구하는 과정에서 자연스럽게 사라지게 하기 위하여 행의 합과 열의 합이 0이 되게 난수를 선택하는 것이고, 행과 열의 합을 따로 구하지만 데이터 하나가 두 개의 합에 얽혀있기 때문에 마방진(매직 스퀘어)의 성질을 이용하는 것이 효율적이다. 행 따로 열 따로 한다면 하나의 전력 소비 정보에 두 개의 은닉값을 사용하게 되며 이는 두 배의 데이터가 서버에 전송되어 매우 비효율적이 될 것이기 때문이다.

[0046] 한편 각 스마트 미터기 i는 PK_i와 SK_i를 다음과 같이 생성한다.

[0047] $PK_i = (h_i , PK_{signi}, PK_{enci})$. $SK_i = (SK_{signi}, SK_{enci}, x_{i,1},\cdots,x_{i,k})$.

[0048] PK_{signi}는 스마트 미터기 i에 대한 서명용 공개키이고, PK_{enci}는 스마트 미터기 i에 대한 암호화용 공개키이다. 아울러 SK_{signi}는 스마트 미터기 i에 대한 서명용 비밀키이고, SK_{enci}는 스마트 미터기 i에 대한 암호화용 비밀키이다.

[0049] <제3 단계: Metering($m_{i,j}$, PP, PK_i, SK_i)>

[0050] 스마트 미터기 i는 임의로 $r_{i,j}(\in Z_p)$와 $r_i(\in Z_p)$를 선택한다. 스마트 미터기 i에 구비되는 은닉부(22)는 다음과 같이 실제의 미터링 데이터 $m_{i,j}$를 은닉한 값의 암호화한 값과 서명을 포함한 미터링 데이터 $\sigma_{i,j}$를 생성한다.

[0051] $$\sigma_{i,j} = (Enc(m_{i,j}+x_{i,j}), Sign(H(m_{i,j}+x_{i,j}), g^{r_{i,j}}), g^{r_{i,j}}, h_i^{m_{i,j}r_i})$$

$$= (\sigma_{i,j,1}, \sigma_{i,j,2}, \sigma_{i,j,3}, \sigma_{i,j,4})$$.

[0052] $Enc(m_{i,j} + x_{i,j})$는 $m_{i,j}$를 은닉한 값 $[m_{i,j} + x_{i,j}]$을 암호화한 값이고, $H(m_{i,j} + x_{i,j})$은 $[m_{i,j} + x_{i,j}]$에 해시 함수를 적용한 결과값이며, $Sign(H(m_{i,j}+x_{i,j}), g^{r_{i,j}})$은 $H(m_{i,j} + r_{i,j})$의 서명에 해당하며 서버가 선택한 전자서명 알고리즘의 서명 스킴에 의해 생성된다. 그리고 $\sigma_{i,j,3}$과 $\sigma_{i,j,4}$는 서명의 위변조를 방지하기 위해 삽입되는 임의의 값으로 서로 바뀌어도 상관없다. 그리고 임의의 값인 $r_{i,j}$와 r_i는 차후의 빌링(billing)을 위해 안전하게 보관된다.

[0053] 한편 j = k인 경우에는 미터링 데이터 $\sigma_{i,j}$를 나타내는 상기 식 중 $r_{i,j}$ 부분이 $r_{i,k}$로 바뀌며 $r_{i,k}$는 다음과 같다.

[0054] $$r_{i,k} = r_i - \sum_{j=1}^{k-1} r_{i,j}$$.

[0055] 이러한 은닉 처리에 의해 제3자 뿐만이 아니라 데이터를 수집하는 서버조차도 상세한 전력 소비 정보를 알 수 없게 되어 각 전력 소비자의 전력 사용 패턴에 대한 기밀성을 보장하게 된다.

[0056] <제4 단계: Verifying metering data($\sigma_{i,j}$, PP, PK_i)>

[0057] 서버는 자신이 선택한 전자 서명 알고리즘의 검증 모듈(유효성 검증부(24))을 통해 $\sigma_{i,j}$에 포함된 $Sign(H(m_{i,j}+x_{i,j}),g^{r_{i,j}})$ 이 $m_{i,j}$에 대한 유효한 서명인지를 검증하여 전력 소비 정보(미터링 데이터)의 무결성을 보장한다. 검증의 결과값이 1이 나오면 유효한 서명으로 판단하고, 0이 나오면 유효하지 아니한 서명으로 판단한다. 서명의 유효성 판단에 요구되는 값은 전력 소비 정보에 대한 서명용 공개키 PP_{sign}과 $\sigma_{i,j}$ = ($\sigma_{i,j,1}$, $\sigma_{i,j,2}$, $\sigma_{i,j,3}$, $\sigma_{i,j,4}$)에서 $m_{i,j}$의 서명과 관련된 $\sigma_{i,j,1}$, $\sigma_{i,j,2}$, $\sigma_{i,j,3}$이다.

[0058] <제5 단계: Billing($m_{i,j}$, tariff)>

[0059] 각 스마트 미터기 i가 $m_{i,j}$과 시간별 전력 사용 요금(tariff, 즉 각 시간 단위 j에서의 사용 요금)을 입력받아 빌링 데이터(billing data) ψ_i를 생성하는 단계이다. 빌링은 각 시간 단위 j($\in\{1,\cdots,k\}$)마다 이루어진다. tariff가 벡터 V = ($v_1,\cdots,v_k$)로 표현되면, 각 스마트 미터기 i에 구비된 빌링 데이터 생성부(23)는 각 스마트 미터기 i에 대한 빌링 데이터 ψ_i를 다음과 같이 구할 수 있다.

[0060] $$\psi_i = \sum_{j=1}^{k} m_{i,j} v_j$$.

[0061] <제6 단계: Verifying billing data($\sigma_{i,j}$, PP, ψ_i)>

[0062] 서버에 구비되는 정확성 검증부(25)를 통해 빌링 데이터 ψ_i가 올바르게 산출되었는지 검증하려면 다음의 두 식(두 등호 관계)이 만족함을 증명해야 한다.

[0063] $$e(\prod_{j=1}^{k}\sigma_{i,j,3},\prod_{j=1}^{k}h_i^{\sigma_{i,j,1}}) = e(g,\prod_{j=1}^{k}\sigma_{i,j,4}),\ e(g,\prod_{j=1}^{k}\sigma_{i,j,4}^{v_j}) = e(\prod_{j=1}^{k}\sigma_{i,j,3},h_i^{\psi_i})$$.

[0064] [증명]

$$e(\prod_{j=1}^{k}\sigma_{i,j,3},\prod_{j=1}^{k}h_i^{\sigma_{i,j,1}}) = e(g^{r_i},\prod_{j=1}^{k}h_i^{m_{i,j}+x_{i,j}})$$

$$= e(g^{r_i},h_i^{\Sigma_{j=1}^{k}m_{i,j}+x_{i,j}}) = e(g^{r_i},h_i^{\Sigma_{j=1}^{k}m_{i,j}})$$

[0065] $$= e(g,\prod_{j=1}^{k}h_i^{m_{i,j}r_i}) = e(g,\prod_{j=1}^{k}\sigma_{i,j,4})$$.

$$e(g, \Pi_{j=1}^{k}\sigma_{i,j,4}^{v_j}) = e(g, \prod_{j=1}^{k}(h_i^{m_{i,j}r_i})^{v_j})$$

$$= e(g^{r_i}, \prod_{j=1}^{k}(h_i^{m_{i,j}})^{v_j}) = e(g^{r_i}, h_i^{\Sigma_{j=1}^{k} m_{i,j}v_j})$$

$$= e(g^{\Sigma_{j=1}^{k} r_{i,j}}, h_i^{\Sigma_{j=1}^{k} m_{i,j}v_j}) = e(\prod_{j=1}^{k}\sigma_{i,j,3}, h_i^{\psi_i})$$

[0066] .

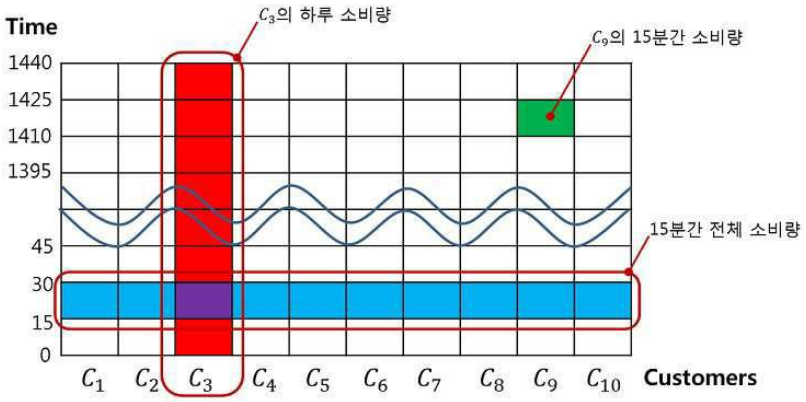
[0067] 따라서 빌링 데이터 ψ_i가 올바르게 산출되었음이 검증되어 빌링 데이터의 무결성이 보장되었음이 증명된다.

[0068] 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

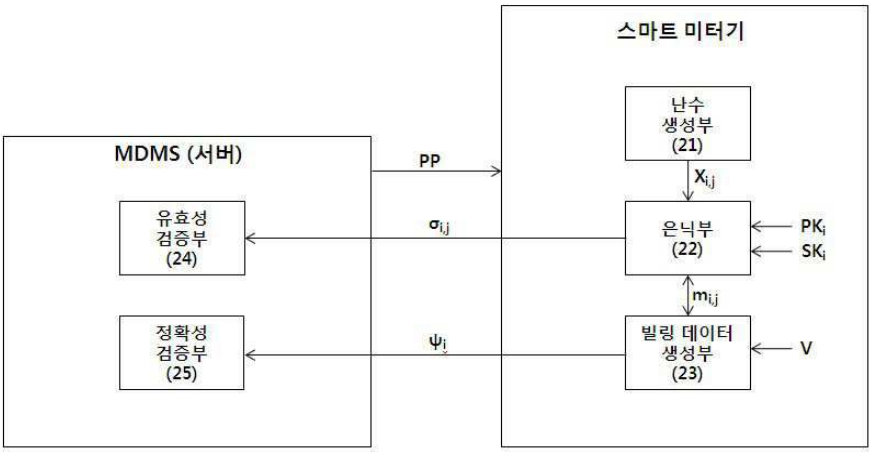
[0069] 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예는 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

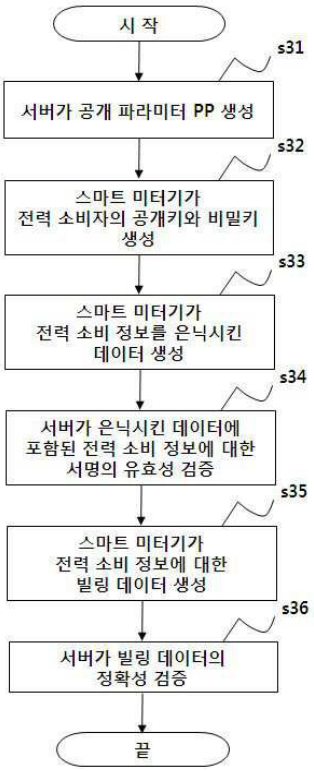
도면1



도면2


스마트 미터기
난수
생성부
(21)
$X_{i,j}$
MDMS (서버)
PP
유효성
검증부
(24)
$\sigma_{i,j}$
은닉부
(22)
PK_i
SK_i
$m_{i,j}$
정확성
검증부
(25)
ψ_i
빌링 데이터
생성부
(23)
V

도면3


시 작
s31
서버가 공개 파라미터 PP 생성
s32
스마트 미터기가
전력 소비자의 공개키와 비밀키
생성
s33
스마트 미터기가
전력 소비 정보를 은닉시킨
데이터 생성
s34
서버가 은닉시킨 데이터에
포함된 전력 소비 정보에 대한
서명의 유효성 검증
s35
스마트 미터기가
전력 소비 정보에 대한
빌링 데이터 생성
s36
서버가 빌링 데이터의
정확성 검증
끝