



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년06월11일
(11) 등록번호 10-1866693
(24) 등록일자 2018년06월04일

(51) 국제특허분류(Int. Cl.)
G06Q 50/06 (2012.01) G06Q 20/14 (2012.01)
G06Q 20/38 (2012.01) H04L 9/08 (2006.01)
(52) CPC특허분류
G06Q 50/06 (2013.01)
G06Q 20/14 (2013.01)
(21) 출원번호 10-2017-0079839
(22) 출원일자 2017년06월23일
심사청구일자 2017년06월23일
(56) 선행기술조사문헌
JP2013219775 A*
JP2014197726 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
이문규
경기도 부천시 계남로 81, 2222동 702호(상동, 진달래마을)
임종혁
경기도 수원시 권선구 서수원로 589, 302동 503호(금곡동, 삼익3차아파트)
윤예진
인천광역시 서구 심곡로 11, 101동 804호(심곡동, 광명아파트)
(74) 대리인
양성보

전체 청구항 수 : 총 6 항

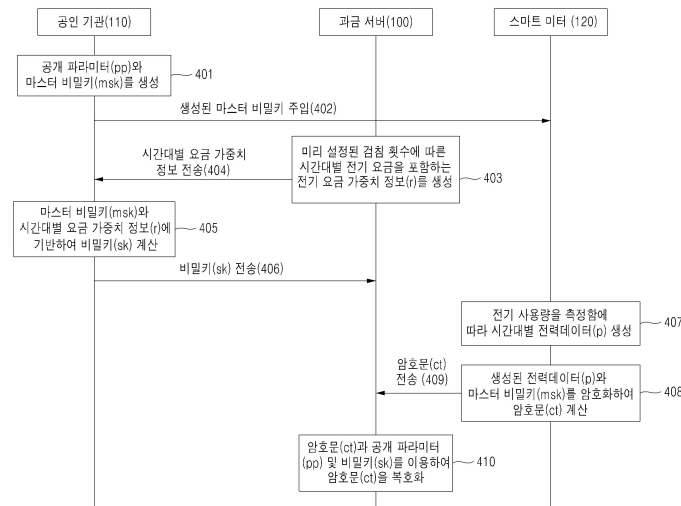
심사관 : 백양규

(54) 발명의 명칭 합수 암호를 이용한 안전한 전기 요금 과금 방법

(57) 요약

일 실시예에 따른 전기 요금 과금 시스템은, 공개 파라미터(pp)와 마스터 비밀키(msk)를 생성하고, 상기 생

대표도



성된 마스터 비밀키(msk)를 스마트 미터에 주입하고, 과금 서버에서 획득된 시간대별 요금 가중치 정보(r)와 상기 생성된 마스터 비밀키(msk)에 기반하여 계산된 비밀키(sk)를 과금 서버로 전송하는 공인 기관; 전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성하고, 상기 생성된 시간대별 전력데이터(p)와 상기 마스터 비밀키(msk)를 이용하여 암호문(ct)을 계산하고, 상기 계산된 암호문(ct)을 과금 서버로 전송하는 스마트 미터; 및 미리 정해진 요금 가중치 정보(r)를 공인 기관으로 전송하고, 상기 스마트 미터로부터 전송받은 암호문(ct)과 상기 공개 파라미터(pp), 상기 비밀키(sk)를 이용하여 상기 암호문을 복호화하는 과금 서버를 포함할 수 있다.

(52) CPC특허분류

G06Q 20/3829 (2013.01)

H04L 9/0816 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 20161210200610

부처명 산업통상자원부

연구관리전문기관 한국에너지기술평가원

연구사업명 에너지기술개발사업

연구과제명 EMS 내장 분산형 서버미터링을 이용한 빅데이터 분석 기반 소규모 공장 및 상업용 빌딩용 에너지 컨설팅 시스템 구축 및 실증

기 여 율 1/1

주관기관 (주)대흥전기

연구기간 2016.12.01 ~ 2017.09.30

공지예외적용 : 있음

명세서

청구범위

청구항 1

전기 요금 과금 시스템에 있어서,

공개 파라미터(pp)와 마스터 비밀키(msk)를 생성하고, 상기 생성된 마스터 비밀키(msk)를 스마트 미터에 주입하고, 과금 서버에서 획득된 미리 정해진 요금 정책에 따른 시간대별 요금 가중치 정보(r)와 상기 생성된 마스터 비밀키(msk)에 기반하여 계산된 비밀키(sk)를 과금 서버로 전송하는 공인 기관;

전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성하고, 상기 생성된 시간대별 전력데이터(p)와 상기 마스터 비밀키(msk)를 이용하여 암호문(ct)을 계산하고, 상기 계산된 암호문(ct)을 과금 서버로 전송하는 스마트 미터; 및

상기 미리 정해진 요금 정책에 따른 시간대별 요금 가중치 정보(r)를 공인 기관으로 전송하고, 상기 스마트 미터로부터 전송받은 암호문(ct)과 상기 공개 파라미터(pp), 상기 비밀키(sk)를 이용하여 상기 암호문을 복호화하는 과금 서버

를 포함하고,

상기 과금 서버는,

상기 스마트 미터로부터 측정된 특정 시간대별 원본 전력 데이터에 대한 값이나 전력 데이터에 대한 사용 패턴의 판단이 불가능한

전기 요금 과금 시스템.

청구항 2

제1항에 있어서,

상기 과금 서버는,

기 설정된 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보(r)를 생성하고, 상기 생성된 시간대별 요금 가중치 정보를 상기 공인 기관으로 전송하는

것을 특징으로 하는 전기 요금 과금 시스템.

청구항 3

제1항에 있어서,

상기 스마트 미터는,

기 설정된 단위 시간동안에 시간마다 전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성하는 것을 포함하고,

상기 시간마다 상기 스마트 미터에 누적된 전기 사용량을 측정하는

것을 특징으로 하는 전기 요금 과금 시스템.

청구항 4

제1항에 있어서,

상기 과금 서버는,

요금 정책 변경으로 시간대별 요금 가중치 정보를 재생성함에 따라 설정된 제2 시간대별 요금 가중치 정보(r')를 상기 공인 기관으로 전송하고, 상기 공인 기관으로부터 상기 제2 시간대별 요금 가중치 정보(r')와 상기 마스터 비밀키(msk)를 이용하여 생성된 제2 비밀키(sk')를 수신하고, 상기 수신된 제2 비밀키(sk')에 기초하여 상기 비밀키(sk)를 상기 제2 비밀키(sk')로 대체하고, 상기 제2 비밀키(sk')에 기초하여 상기 암호문(ct)을 복호화함으로써 상기 스마트 미터에 설정된 요금 체계를 변경하고, 상기 변경된 요금 체계에 대한 과금을 진행하는 것을 특징으로 하는 전기 요금 과금 시스템.

청구항 5

전기 요금 과금 시스템에서 수행되는 전기 요금 과금 방법에 있어서,

공인 기관에서 공개 파라미터(pp)와 마스터 비밀키(msk)를 생성하고, 상기 생성된 마스터 비밀키(msk)를 스마트 미터에 주입하는 단계;

과금 서버에서 미리 정해진 요금 정책에 따른 시간대별 요금 가중치 정보(r)를 상기 공인 기관으로 전송하는 단계;

상기 공인 기관에서, 상기 미리 정해진 요금 정책에 따른 시간대별 요금 가중치 정보(r)와 상기 생성된 마스터 비밀키(msk)에 기반하여 계산된 비밀키(sk)를 상기 과금 서버로 전송하는 단계;

상기 스마트 미터에서, 전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성하는 단계;

상기 스마트 미터에서 생성된 시간대별 전력데이터(p)와 상기 마스터 비밀키(msk)를 이용하여 암호문(ct)을 계산하고, 상기 계산된 암호문(ct)을 상기 과금 서버로 전송하는 단계; 및

상기 과금 서버에서, 상기 스마트 미터로부터 전송받은 암호문(ct)과 상기 공개 파라미터(pp), 상기 비밀키(sk)를 이용하여 상기 암호문을 복호화하는 단계

를 포함하고,

상기 과금 서버는,

상기 스마트 미터로부터 측정된 특정 시간대별 원본 전력 데이터에 대한 값이나 전력 데이터에 대한 사용 패턴의 판단이 불가능한

전기 요금 과금 방법.

청구항 6

과금 서버의 전기 요금 과금 방법에 있어서,

미리 정해진 요금 정책에 따른 시간대별 요금 가중치 정보(r)를 공인 기관으로 전송하는 단계;

상기 공인 기관으로부터 생성된 마스터 비밀키(msk)와 상기 미리 정해진 요금 정책에 따른 시간대별 요금 가중치 정보(r)에 기반하여 계산된 비밀키(sk)를 수신하는 단계;

스마트 미터에서 측정된 전기 사용량으로부터 생성된 시간대별 전력데이터(p)가 생성되고, 상기 스마트 미터로부터 상기 생성된 시간대별 전력데이터(p)와 상기 마스터 비밀키(msk)를 이용하여 계산된 암호문(ct)을 수신하는 단계; 및

상기 공인 기관으로부터 생성된 공개 파라미터(pp) 및 상기 비밀키(sk)를 이용하여 상기 스마트 미터로부터 수신된 암호문(ct)을 복호화하는 단계

를 포함하고,

상기 과금 서버는,

상기 스마트 미터로부터 측정된 특정 시간대별 원본 전력 데이터에 대한 값이나 전력 데이터에 대한 사용 패턴의 판단이 불가능한

과금 서버의 전기 요금 과금 방법.

발명의 설명

기술 분야

[0001] 아래의 설명은 암호 기술에 관한 것으로, 함수 암호를 이용한 전기 요금 과금 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 스마트 그리드란 전기 및 정보통신 기술을 활용하여 전력망을 지능화 고도화함으로써 고품질의 전력서비스를 제공하고 에너지 이용효율을 극대화하는 전력망이다. 스마트 그리드 기술의 발달과 확산은 좁게는 공장이나 가정의 전력 사용 효율을 늘리는 것에서부터, 넓게는 빌딩 또는 도시의 전력 사용 효율을 높이는 데에 기여하고 있다. 또한, 기계 학습이나 딥 러닝 등의 분석 기술을 접목시켜 전기 사용 패턴을 분석하는 방법 등으로 전력 사용 효율성을 고도화시키는 다양한 연구가 진행 중이다. 스마트 그리드 환경에서 각 전력 사용 주체는 스마트 미터를 통해 전력 사용량을 측정하고 해당 정보를 실시간으로 전력회사로 전송한다. 개별 가정의 스마트 미터로부터 전송되는 실시간 전력 소비 데이터를 전력회사에서 분석하면 사용자의 생활 패턴에 대한 다양한 정보를 얻을 수 있어 유용한 동시에, 프라이버시에 심각한 위협이 될 수 있다. 단순히 현재 시간의 전력 사용량으로부터 재택 여부를 알 수 있으며, 실시간 전력 사용 패턴에 신호 분해(Signal Disaggregation) 기법 등 좀 더 정밀한 분석 기법을 적용하면 현재 사용하고 있는 가전 기기의 종류까지도 역추적할 수 있음이 알려져 있다.

[0003] 이러한 문제의 대안으로 스마트 미터 외부로 전송되는 전력데이터를 암호화하는 방법이 있을 수 있다. 그러나 스마트 미터로부터 암호화된 전력데이터는 그 값을 제공받은 전력 사업자 또한 암호화 되기 전의 전력데이터 값을 알 수 없기 때문에 사용한 각 미터가 실시간으로 제공하는 사용 전력량에 대한 요금 과금이 불가능하다는 문제가 있다.

발명의 내용

해결하려는 과제

[0004] 함수 암호 기술을 사용하여 전력 사용량을 암호화함에 따라 획득된 시간대별 전력데이터와 시간대별 요금 가중

치 정보에 기반하여 전기 요금을 과금하는 방법 및 시스템을 제공할 수 있다.

과제의 해결 수단

- [0005] 전기 요금 과금 시스템은, 공개 파라미터(pp)와 마스터 비밀키(msk)를 생성하고, 상기 생성된 마스터 비밀키(msk)를 스마트 미터에 주입하고, 과금 서버에서 획득된 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보(r)와 상기 생성된 마스터 비밀키(msk)에 기반하여 계산된 비밀키(sk)를 과금 서버로 전송하는 공인 기관; 전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성하고, 상기 생성된 시간대별 전력데이터(p)와 상기 마스터 비밀키(msk)를 이용하여 암호문(ct)을 계산하고, 상기 계산된 암호문(ct)을 과금 서버로 전송하는 스마트 미터; 및 상기 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보(r)를 공인 기관으로 전송하고, 상기 스마트 미터로부터 전송받은 암호문(ct)과 상기 공개 파라미터(pp), 상기 비밀키(sk)를 이용하여 상기 암호문을 복호화하여 전기요금을 산출하는 과금 서버를 포함할 수 있다.
- [0006] 상기 과금 서버는, 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보(r)를 생성하고, 상기 생성된 시간대별 요금 가중치 정보를 상기 공인 기관으로 전송할 수 있다.
- [0007] 상기 스마트 미터는, 기 설정된 단위 시간 동안에 기 설정된 시간마다 전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성하는 것을 포함하고, 상기 기 설정된 시간마다 상기 스마트 미터에 누적된 전기 사용량을 측정할 수 있다.
- [0008] 상기 과금 서버는, 요금 정책 변경으로 시간대별 요금 가중치 정보를 재생성함에 따라 설정된 제2 시간대별 요금 가중치 정보(r')를 상기 공인 기관으로 전송하고, 상기 공인 기관으로부터 상기 제2 시간대별 요금 가중치 정보(r')와 상기 마스터 비밀키(msk)를 이용하여 생성된 제2 비밀키(sk')를 수신하고, 상기 수신된 제2 비밀키(sk')에 기초하여 상기 비밀키(sk)를 상기 제2 비밀키(sk')로 대체하고, 상기 제2 비밀키(sk')에 기초하여 상기 암호문(ct)을 복호화함으로써 상기 스마트 미터에 설정된 요금 체계를 변경하고, 상기 변경된 요금 체계에 대한 과금을 진행할 수 있다.
- [0009] 전기 요금 과금 시스템에서 수행되는 전기 요금 과금 방법은, 공인 기관에서 공개 파라미터(pp)와 마스터 비밀키(msk)를 생성하고, 상기 생성된 마스터 비밀키(msk)를 스마트 미터에 주입하는 단계; 과금 서버에서 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보(r)를 상기 공인 기관으로 전송하는 단계; 상기 공인 기관에서, 상기 시간대별 요금 가중치 정보(r)와 상기 생성된 마스터 비밀키(msk)에 기반하여 계산된 비밀키(sk)를 상기 과금 서버로 전송하는 단계; 상기 스마트 미터에서, 전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성하는 단계; 상기 스마트 미터에서 생성된 시간대별 전력데이터

(p)와 상기 마스터 비밀키(msk)를 이용하여 암호문(ct)을 계산하고, 상기 계산된 암호문(ct)을 상기 과금 서버로 전송하는 단계; 및 상기 과금 서버에서, 상기 스마트 미터로부터 전송받은 암호문(ct)과 상기 공개 파라미터(pp), 상기 비밀키(sk)를 이용하여 상기 암호문을 복호화하는 단계를 포함할 수 있다.

[0010] 과금 서버의 전기 요금 과금 방법은, 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보(r)를 공인 기관으로 전송하는 단계; 상기 공인 기관으로부터 생성된 마스터 비밀키(msk)와 상기 시간대별 요금 가중치 정보(r)에 기반하여 계산된 비밀키(sk)를 수신하는 단계; 스마트 미터에서 측정된 전기 사용량으로부터 생성된 시간대별 전력데이터(p)가 생성되고, 상기 스마트 미터로부터 상기 생성된 시간대별 전력데이터(p)와 상기 마스터 비밀키(msk)를 이용하여 계산된 암호문(ct)을 수신하는 단계; 및 상기 공인 기관으로부터 생성된 공개 파라미터(pp) 및 상기 비밀키(sk)를 이용하여 상기 스마트 미터로부터 수신된 암호문(ct)을 복호화하는 단계를 포함할 수 있다.

발명의 효과

[0011] 본 발명은 함수 암호 기술을 사용하여 전력 사용량을 암호화함에 따라 획득된 시간대별 전력데이터와 시간대별 요금 가중치 정보에 기반하여 전기 요금을 과금함으로써 전력 패턴 분석을 통한 분해 공격 자체를 원천적으로 봉쇄하면서도 정상적인 과금이 가능하도록 한다.

[0012] 본 발명은 정상적인 전기 요금 과금 기능을 제공할 수 있다. 더욱 상세하게는, 본 발명은 단순히 전력데이터 누적량을 계산하는 것이 아닌 시간별 계절별 요금표에 따른 적절한 과금이 가능하기 때문에 전력 사업자의 요구 사항에 맞추어 실용적으로 요금 과금이 가능하다.

[0013] 본 발명은 암호화된 전력데이터를 이용하여 요금을 계산하기 때문에 스마트 미터와 관련된 전력데이터 원본의 복원이 불가능하고, 해킹과 같은 공격에도 안전하다.

도면의 간단한 설명

[0014] 도 1은 일 실시예에 따른 전기 요금 과금 시스템의 개괄적인 동작을 설명하기 위한 도면이다.
 도 2는 일 실시예에 따른 전기 요금 과금 시스템에서 과금 서버의 구성을 설명하기 위한 블록도이다.
 도 3은 일 실시예에 따른 과금 서버에서의 과금 방법을 설명하기 위한 흐름도이다.
 도 4는 일 실시예에 따른 전기 요금 과금 시스템에 포함된 공인 기관, 과금 서버 및 스마트 미터들의 동작을 통하여 전기 요금 과금 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[0016] 함수 암호(Functional Encryption)란 평문(Plaintext)(m)에 대한 암호문과 함수(f)에 대한 비밀키가 해독기(Decryptor)에 주어지면, 해독기가 해당 비밀키를 이용해 암호문으로부터 $f(m)$ 을 계산할 수 있는 암호다. 예를 들어, 함수 $f(x) = ax + b$ (a, b 는 정수)에 대한 함수 암호는 평문 m 의 암호문 $E(m)$ 및 f 에 대한

비밀키(K)가 주어질 때 복호화 연산 $D_K(E(m)) = f(m) = a \times m + b$ 를 만족하는 암호이다. 단, 비밀키(K)를 보유한 측은 암호문에 대해 함수(f)에 대한 결과만을 복호화할 뿐, 다른 복호화는 불가능한 특성이 있다. 이에 따라 아래의 실시예들에서는 함수 암호 기술을 이용하여 안전한 전기 요금 과금 방법을 설명하기로 한다.

- [0017] 도 1은 일 실시예에 따른 전기 요금 과금 시스템의 개괄적인 동작을 설명하기 위한 도면이다.
- [0018] 전기 요금 과금 시스템은 과금 서버(100), 공인 기관(110) 및 스마트 미터(120)를 포함할 수 있다. 이와 같은 전기 요금 과금 시스템에 대해 과금 서버(100), 공인 기관(110) 및 스마트 미터(120) 사이의 동작을 통하여 함수 암호(Functional Encryption) 기술을 이용하여 안전한 전기 요금을 과금하는 방법을 설명하기로 한다.
- [0019] 과금 서버(100)는 스마트 미터(120)로부터 시간대별 암호화된 전력데이터를 획득하기 때문에 특정 시간대별 원본 전력 데이터에 대한 값이나 전력 데이터에 대한 사용 패턴을 판단할 수 없다. 또한, 감청을 통해 암호화된 전력 데이터를 획득하는 공격자 또한 분해 공격을 수행할 수 없다.
- [0020] 한편, 과금 서버(100)는 암호화된 전력데이터를 암호문 상에서 처리하여 시간대별 가중치가 적용된 과금을 수행할 수 있다. 이와 같이 암호화된 데이터들은 미리 정해진 함수로 조합하여 함수값에 대한 평문을 계산하는 함수 암호의 특성으로 인하여 과금을 처리할 수 있다. 일반적으로 전기 요금은 요금제별, 시간대별로 다르게 책정될 수 있으며, 청구되는 전기 요금은 시간대별로 정해진 사용 요금 가중치 정보와 해당 시간의 전력 사용량의 곱을 누적한 금액을 의미한다.
- [0021] 공인 기관(110)은 공개 파라미터와 마스터 비밀키를 생성할 수 있다. 공인 기관(110)은 전력 사용량을 측정하는 스마트 미터(120)에 마스터 비밀키를 주입하고, 시간대별 요금 가중치 정보와 마스터 비밀키를 이용하여 생성된 비밀키를 과금 서버(100)로 제공할 수 있다.
- [0022] 스마트 미터(120)는 사용자의 전력 사용량을 지속적으로 측정할 수 있다. 스마트 미터(120)는 원격 검침, 전력 공급자와 수용자 간 양방향 통신, 시간대별 계량이 가능한 전자식 전력량계를 의미할 수 있다. 스마트 미터(120)는 시간대별로 수집된 전력 사용량에 대한 과금 계산에 사용될 수 있으며, 시간대별로 전기 요금이 달라질 수 있다. 스마트 미터(120)는 기 설정된 단위 시간동안(예를 들면, 24시간, 일주일 등) 기 설정된 시간 간격마다(예를 들면, 1시간, 30분 단위) 단위 시간당 누적 사용 전력량을 측정할 수 있다. 예를 들면, 스마트 미터(120)의 누적 전력 사용량의 측정 간격은 1시간으로 설정될 수 있다. 더욱 상세하게는, 스마트 미터(120)는 하루 24시간 동안 총 24회의 전기 사용량을 측정하여 시간대별 전력데이터를 생성할 수 있다. 스마트 미터(120)는 시간대별 전력데이터를 공인 기관(110)으로부터 전달받은 마스터 비밀키를 이용하여 암호화한 암호문을 과금 서버(100)로 전송할 수 있다.
- [0023] 과금 서버(100)는 기 설정된 단위 시간(예를 들면, 24 시간, 일주일 등)에 대한 요금 가중치 정보를 생성할 수 있고, 생성된 시간대별 요금 가중치 정보를 공인 기관(110)으로 전송할 수 있다.
- [0024] 과금 서버(100)는 스마트 미터(120)로부터 전달받은 암호문과 공인 기관(110)의 파라미터, 비밀키를 이용하여 복호화를 수행할 수 있다. 과금 서버(100)는 요금 가중치 정보를 반영하여 생성된 비밀키를 이용하여 복호화를 수행함에 따라 스마트 미터(120)에 대한 전기 사용 요금을 산출할 수 있다. 이에 따라 과금 서버(100)는 암호화된 스마트 미터의 전력 사용량이 포함된 전력데이터에 과금 서버(100)가 미리 설정한 요금 정책에 따른 시간대별 요금 가중치 정보를 적용한 최종 요금을 과금할 수 있게 된다.
- [0025] 도 2는 일 실시예에 따른 전기 요금 과금 시스템에서 과금 서버의 구성을 설명하기 위한 블록도이고, 도 3은 일 실시예에 따른 과금 서버에서 과금 방법을 설명하기 위한 흐름도이다.
- [0026] 과금 서버(100)는 전송부(210), 제1 수신부(220), 제2 수신부(230) 및 복호화부(240)를 포함할 수 있다. 이러한 과금 서버(100)의 구성요소들은 도 3의 과금 방법이 포함하는 단계들(310 내지 340)을 수행하도록 과금 서버(100)를 제어할 수 있다.
- [0027] 우선적으로, 공인 기관에서 공개 파라미터와 마스터 비밀키를 생성할 수 있으며, 생성한 마스터 비밀키는 스마트 미터로 주입될 수 있다.
- [0028] 단계(310)에서 전송부(210)는 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보를 공인 기관으로 전송할 수 있다. 이때, 공인 기관은 마스터 비밀키와 시간대별 전기 요금을 포함하는 요금

가중치 정보에 기반하여 계산된 비밀키를 생성할 수 있고, 생성된 비밀키를 과금 서버로 전송할 수 있다.

- [0029] 단계(320)에서 제1 수신부(220)는 공인 기관으로부터 생성된 마스터 비밀키와 시간대별 요금 가중치 정보에 기반하여 계산된 비밀키를 수신할 수 있다.
- [0030] 단계(330)에서 제2 수신부(230)는 스마트 미터에서 측정된 전기 사용량으로부터 생성된 시간대별 전력데이터가 생성되고, 스마트 미터로부터 생성된 시간대별 전력데이터와 마스터 비밀키를 이용하여 계산된 암호문을 수신할 수 있다.
- [0031] 단계(340)에서 복호화부(240)는 공인 기관으로부터 생성된 공개 파라미터 및 비밀키를 이용하여 스마트 미터로부터 수신된 암호문을 복호화할 수 있다.
- [0032] 도 4는 일 실시예에 따른 전기 요금 과금 시스템에 포함된 공인 기관, 과금 서버 및 스마트 미터들의 동작을 통하여 전기 요금 과금 방법을 설명하기 위한 흐름도이다.
- [0033] 도 4에는 공인 기관(110), 과금 서버(100) 및 스마트 미터(120)의 동작을 통하여 전기 요금이 과금되는 방법을 설명하기로 한다. 또한, 도 4에서는 1일(24시간)동안 스마트 미터의 전력 사용량을 1시간 간격으로 측정하고, 과금 서버의 검침 횟수도 1시간 간격으로 검침한다고 가정하고 설명하기로 한다. 이때, 측정되는 측정 간격 및 스마트 미터가 검침하는 검침 횟수는 사용자 및 관리자에 의하여 변경될 수 있다.
- [0034] 공인 기관(110)은 공개 파라미터(pp)와 마스터 비밀키(msk)를 생성할 수 있다(401). 공인 기관(110)은 마스터 비밀키(msk)를 스마트 미터(120)에 주입할 수 있다(402). 이때, 스마트 미터(120)는 공인 기관(110)으로부터 전송된 마스터 비밀키(msk)를 저장하고 있을 수 있다.
- [0035] 과금 서버(100)는 검침 횟수 $n=24$ (n 은 자연수)로 분할된 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보(r)를 생성할 수 있다(403). 과금 서버(100)는 생성된 시간대별 요금 가중치 정보를 공인 기관(110)으로 전송할 수 있다(404).
- [0036] 공인 기관(110)은 마스터 비밀키와 시간대별 요금 가중치 정보(r)에 기반하여 비밀키(sk)를 생성할 수 있다(405). 공인 기관(110)은 생성된 비밀키(sk)를 과금 서버(100)로 전송할 수 있다. 과금 서버(100)는 공인 기관(110)으로부터 전송된 비밀키(sk)를 수신할 수 있다.
- [0037] 스마트 미터(120)는 전기 사용량을 측정함에 따라 시간대별 전력데이터(p)를 생성할 수 있다(407). 스마트 미터(120)는 생성된 전력데이터(p)와 마스터 비밀키(msk)를 암호화하여 암호문(ct)을 계산할 수 있다(408). 스마트 미터(120)는 암호문(ct)을 과금 서버(100)로 전송할 수 있다(409).
- [0038] 과금 서버(100)는 스마트 미터(120)로부터 전송된 암호문(ct)을 수신할 수 있다. 과금 서버(100)는 암호문(ct)과 공개 파라미터(pp), 비밀키(sk)를 이용하여 암호문(ct)을 복호화할 수 있다(410).
- [0039] 과금 서버(100)는 복호화를 수행함에 따른 복호화 결과에서 미리 정해진 요금 정책에 따른 시간대별 전기 요금을 포함하는 요금 가중치 정보를 반영한 계산 결과인 최종 전기 요금을 도출할 수 있다. 이때, 과금 서버(100)는 암호화된 스마트 미터의 전력 사용량이 포함된 원본 전력데이터(p)의 값을 알 수 없지만 전기 요금 가중치 정보(r)가 반영된 스마트 미터(120) 별 누적 전기 요금 정보를 알 수 있기 때문에 각 스마트 미터(120)에 최종 전기 요금을 과금할 수 있다.
- [0040] 또한, 과금 서버(100)는 요금 체계의 변경을 지원할 수 있다. 과금 서버(100)가 요금 체계를 변경하기 위하여

시간대별 요금 가중치 정보($\mathbf{r}'$)를 재생성할 수 있다. 과금 서버(100)가 재생성한 시간대별 요금 가중치 정보($\mathbf{r}'$)를 공인 기관(110)으로 전송할 수 있다. 공인 기관(110)은 재생성된 시간대별 요금 가중치 정보($\mathbf{r}'$)와 마스터 비밀키(msk)를 이용하여 새로운 비밀키(sk')를 생성할 수 있다. 공인 기관(110)은 새로운 비밀키(sk')를 과금 서버(100)로 전송할 수 있다. 과금 서버(100)는 기존 비밀키(sk)를 새로운 비밀키(sk')로 대체하여 암호문(ct)에 대한 복호화를 수행함으로써 변경된 요금 체계에 대한 과금을 수행할 수 있다.

[0041] 다른 예로서, 함수 암호 방법 중 하나인 내적 암호 방법을 이용하여 전기 요금을 과금하는 방법을 설명하기로 한다. 우선적으로, 안전성 파라미터 $\lambda \in \mathbb{N}$ 를 고정하고, n 을 양의 정수라고 가정하자. 또한, S 를 $\mathbb{Z}_q$ 의 다항식 크기의 부분집합이라고 하자. 이때, 내적 함수 암호(Inner-Product Encryption: IPE) 방법 $\Pi_{ipe} = (IPE.Setup, IPE.KeyGen, IPE.Encrypt, IPE.Decrypt)$ 을 다음과 같이 구성할 수 있다.

[0042] $IPE.Setup(1^\lambda, S)$: 안전성 파라미터 λ 가 주어졌을 때, 설정(Setup) 알고리즘은 비대칭 곱셈형 군 $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e)$ 를 샘플링하고, 생성자 $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ 를 선택한다. 그 후, $B \leftarrow \text{GL}_n(\mathbb{Z}_q)$ 를 샘플링하고, $B^* = \det(B) \cdot (B^{-1})^T$ 를 결정할 수 있다. 마지막으로, 설정 알고리즘은 공개 파라미터 $pp = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, e, S)$ 와 마스터 비밀키 $msk = (pp, g_1, g_2, B, B^*)$ 를 출력할 수 있다.

[0043] $IPE.KeyGen(msk, \mathbf{x})$: 마스터 비밀키(msk)와 벡터($\mathbf{x} \in \mathbb{Z}_q^n$)가 주어지면, 키 생성(Key Generation) 알고리즘은 균일한(Uniformly) 임의의 원소 $\alpha \xleftarrow{R} \mathbb{Z}_q$ 를 선택하고, 쌍 $sk = (K_1, K_2) = (g_1^{\alpha \cdot \det(B)}, g_1^{\alpha \cdot \mathbf{x} \cdot B})$ 을 출력할 수 있다.

[0044] $IPE.Encrypt(msk, \mathbf{y})$: 마스터 비밀키(msk)와 벡터($\mathbf{y} \in \mathbb{Z}_q^n$)가 주어지면, 암호화(Encryption) 알고리즘은 균일한 임의의 원소($\beta \xleftarrow{R} \mathbb{Z}_q$)를 선택하고, 쌍 $ct = (C_1, C_2) = (g_2^\beta, g_2^{\beta \cdot \mathbf{y} \cdot B^*})$ 을 출력할 수 있다.

[0045] $IPE.Decrypt(pp, sk, ct)$: 공개 파라미터(pp), 비밀키($sk = (K_1, K_2)$)와 암호문($ct = (C_1, C_2)$)이 주어지면, 복호화(Decryption) 알고리즘은 $D_1 = e(K_1, C_1)$ 와 $D_2 = e(K_2, C_2)$ 를 계산할 수 있다. 그 후, $(D_1)^z = D_2$ 와 같은 $z \in S$ 가 존재하는지 여부를 확인할 수 있다. 만약, 존재한다면, 복호화 알고리즘은 z 를 출력하고, 존재하지 않는다면, $\perp$ 를 출력할 수 있다.

[0046] 공인 기관(110)은 $IPE.Setup$ 을 통해 공개 파라미터(pp)와 마스터 비밀키(msk)를 생성할 수 있다. 공인 기

관(110)은 마스터 비밀키(msk)를 스마트 미터(120)에 주입할 수 있다.

[0047] 과금 서버(100)는 하루를 스마트 미터(120)가 하루동안 전기 검침을 수행하는 횟수인 $n=24$ 로 분할하고, 분할된 범위 내의 각각의 시간대별 전기 요금 가중치를 원소로 가지는 길이가 n 인 벡터($r \in \mathbb{Z}_q^n$)를 생성할 수 있다.

[0048] 공인 기관(110)은 키 생성 알고리즘 $IPE.KeyGen$ 에 벡터(r)과 마스터 비밀키(msk)를 입력하여 계산한 비밀키(sk)를 과금 서버(100)로 전송할 수 있다.

[0049] 스마트 미터(120)는 하루동안 총 $n=24$ 회 전기 사용량을 측정함에 따라 길이가 $n=24$ 인 벡터($p \in \mathbb{Z}_q^n$)를 생성할 수 있다. 스마트 미터(120)는 벡터(p)와 마스터 비밀키(msk)를 암호화 알고리즘 $IPE.Encrypt$ 에 입력하여 암호문($ct = (C_1, C_2)$)을 계산하고, 계산된 암호문(ct)을 과금 서버(100)로 전송할 수 있다.

[0050] 과금 서버(100)는 복호화 알고리즘 $IPE.Decrypt$ 에 스마트 미터(120)로부터 전송받은 암호문(ct)과 공개 파라미터(pp) 및 비밀키(sk)를 입력하여 $D_1 = e(K_1, C_1)$ 과 $D_2 = e(K_2, C_2)$ 를 계산할 수 있다. 마지막으로, $(D_1)^z = D_2$ 와 같은 $z \in S$ 를 복원할 수 있다.

[0051] 복호화를 수행한 복호화 결과(z)는 벡터(r)과 벡터(p)의 내적 계산 결과인 $z = \langle r, p \rangle$ 로, 과금 서버에 설정된 요금 가중치 정보(r)를 반영하여 스마트 미터(120)가 설치된 장소에 하루 동안 사용한 누적 전기 요금을 계산한 결과가 된다.

[0052] 일 실시예에 따른 전기 요금 과금 시스템은 정상적인 전기 요금 과금 기능을 제공할 수 있다. 전기 요금 과금 시스템은 단순히 전력데이터 누적량을 계산하는 것이 아닌 시간별 계절별 요금표에 따른 적절한 과금이 가능하도록 설계되었기 때문에 전력 사업자의 요구사항에 맞추어 실용적으로 요금 과금이 가능하다.

[0053] 일 실시예에 따른 전기 요금 과금 시스템은 전력 사업자(과금 서버)에 의한 전력데이터의 원본 복원이 불가능하다. 과금 서버는 로컬 시스템(예: 스마트 미터)으로부터 전력데이터 원본을 직접 전송 받아 처리하는 것이 아니라, 전력데이터의 암호문만을 사용하여 요금을 계산하고 있으므로, 전력데이터 원본을 복원할 수 없다. 왜냐하면 전력데이터 원본을 얻어내기 위해서는 함수 암호의 마스터 비밀키(msk)를 정확히 알아야 하는데, 이 마스터 비밀키는 로컬 시스템(예: 스마트 미터)과 공인 기관만이 알고 있기 때문이다. 만약, 로컬 시스템이나 공인 기관을 해킹하여 마스터 비밀키(msk)를 획득한 공격자가 전력 사업자의 서버까지 공격에 성공한다면, 전력데이터 원본을 획득할 수 있으나, 현실적으로 두개 이상의 시스템이 동시에 공격 당하는 상황은 발생하기 어렵다.

[0054] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate 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(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 기술분야에서 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 장치

는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0055] 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, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 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.

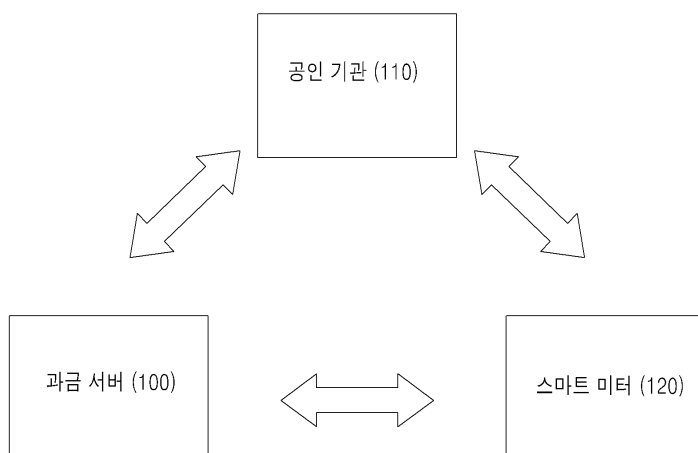
[0056] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 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.

[0057] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

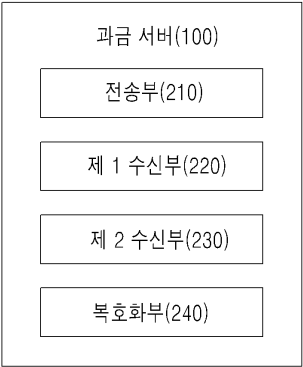
[0058] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

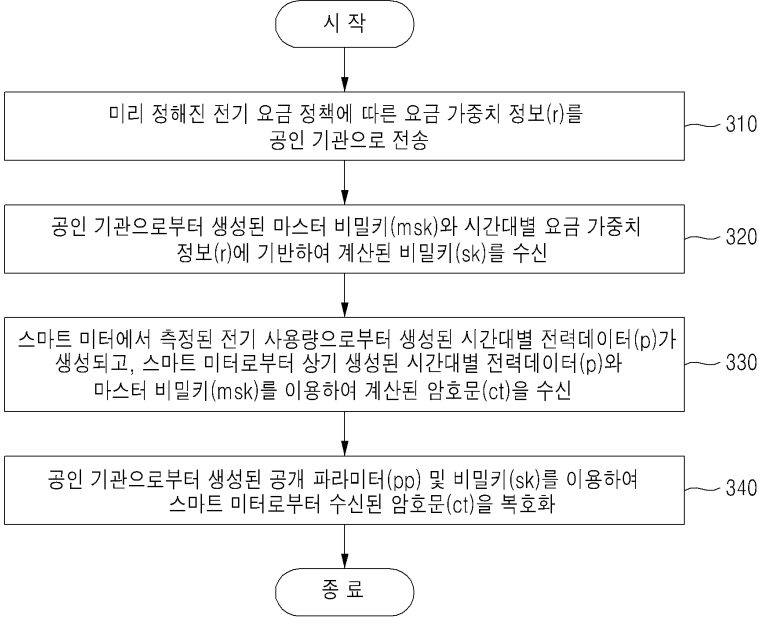
도면1



도면2



도면3



도면4

