Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.3, Jun. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.3.685

동형 암호를 이용한 스마트그리드에서의 효율적 프라이버시 보존 전력량 집계 방법*

구 동 영†‡
한성대학교

Efficient Privacy-Preserving Metering Aggregation in Smart Grids Using Homomorphic Encryption*

Dongyoung Koo†‡
Hansung University

요 약

스마트그리드는 기존의 단방향 전력 전송에서 나아가 양방향 정보 교환이 이루어지는 시스템으로 전력의 이동 및 소요량에 대한 실시간 파악이 가능하다. 전력 생산자는 전력 소모량 집계 결과로부터 향후 전력 생산량 예측이 용이하며, 사용자 또한 다수 전력원으로부터의 단위 사용 비용을 고려한 선택적 전력 사용 및 전력 절약 계획 수립이 용이해져 자원의 효율적 생산 및 사용을 가능하게 한다. 반면 자원의 사용 및 이동에 대한 실시간 정보 수집은 개인의 프라이버시를 침해할 수 있는 위험성을 내포하고 있다. 이러한 스마트그리드에서의 전력량 집계 과정에서 프라이버시 침해를 방지하기 위하여, 본 논문에서는 동형 암호화 기법을 활용함으로써 단순 합계를 포함한 복합 연산을 허용하는 유연하면서도 효율적인 전력량 집계 및 분석 기법을 제시한다.

ABSTRACT

Smart grid enables efficient power management by allowing real-time awareness of electricity flows through two-way communication. Despite its various advantages, threats to user privacy caused by frequent meter reading hinder prosperous deployment of smart grid. In this paper, we propose a privacy-preserving aggregation method exploiting fully homomorphic encryption (FHE). Specifically, it achieves privacy-preserving fine-grained aggregation of electricity usage for smart grid customers in multiple electrical source environments, while further enhancing efficiency through SIMD-style operations simultaneously. Analysis of our scheme demonstrates the suitability in next-generation smart grid environment where the customers select and use a variety of power sources and systematic metering and control are enabled.

Keywords: smart grid, aggregation, privacy, efficiency, homomorphic encryption

I. 서 론

스마트그리드는 기존 전력망과 달리 전력원으로부터 최종 소비자에 이르는 전력이동의 전 과정에 참여하는 주체들 사이에서 양방향 정보 교환이 실시간으로 이루어진다. 이를 통하여 잉여 전력 생산으로 인한 자원 낭비를 사전에 방지하고 시스템 결함 등에 의한 위기상황을 실시간으로 파악하여 능동적으로 대처할 수 있을 뿐만 아니라, 최종 소비자는 실시간 전력 사용량 및 소모 패턴을 인지하고 다양한 전력원으로부터 제공되는 전력의 단위 시간당 비용을 비교하

Received(04. 22. 2019), Modified(06. 03. 2019), Accepted(06. 03. 2019)
* 본 연구는 한성대학교 교내학술연구비 지원과제 임
† 주저자, dykoo@hansung.ac.kr
‡ 교신저자, dykoo@hansung.ac.kr(Corresponding author)

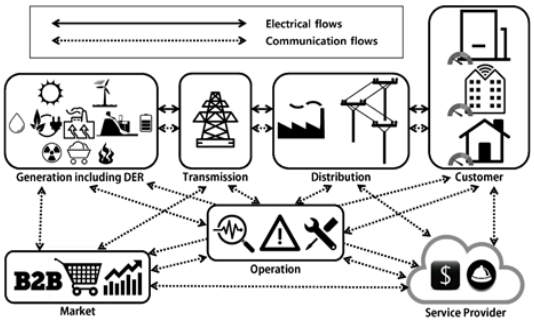

Fig. 1. Smart Grid Architecture

여 선택적으로 사용함으로써 비용 효율적 전력 사용 계획을 세울 수 있다.

이러한 스마트그리드의 다양한 이점에도 불구하고, 사용자 부재 상황 파악을 통한 강도 등 [1] 실시간 전력 사용 정보의 노출은 최종 소비자들의 개별 생활 패턴 파악을 가능하게 하여 개인 프라이버시에 대한 심각한 침해 가능성을 내포하고 있다 [2,3].

스마트그리드에서의 전력 사용량에 대한 프라이버시 보존을 위한 기존 연구 [4-9]에서는 대부분 암호화 기법을 적용하여 정보 유출의 방지를 도모하고 있으며, 특히 누적 전력량 집계를 위하여 암호문에 대한 연산을 허용하는 동형 암호화 기법을 활용하고 있다. 그러나 이는 단순 덧셈 등 제한된 연산만을 허용하는 부분 동형 암호화 (partial homomorphic encryption, partial HE) 기법으로, 전력원별 상이한 요금 및 사용자의 다양한 전력 사용 권한이 부여된 차세대 스마트그리드 시스템에 적용되기 어렵고 소규모 가구 내에서의 전력량 집계를 대상으로 연구가 이루어져 전체 가구수의 증가에 따른 확장성을 충분히 제공하지 못하고 있다.

이에 본 논문에서는 프라이버시가 보존되는 환경에서 덧셈 뿐 아니라 곱셈 등 다양한 연산을 충분히 활용하여 효율적인 자원 관리가 가능하도록 동형 암호 (fully homomorphic encryption, FHE)를 이용한 전력량 집계 및 분석 기법을 제시한다.

II. 스마트그리드 구조 및 프라이버시

선진 검침 기반시설 (advanced metering infrastructure, AMI)이라 불리는 지능형 스마트그리드 시스템은 분산된 다수의 전력원으로부터 전력 생산, 저장, 부하 제어 및 전송이 가능하며 그 구조는 Fig. 1.과 같다. 전력원 (Generation)으로부터 생산된 전력은 전송 (Transmission) 시스템을 통하여 원거리로 이동되며 분산 (Distribution) 시스템을 통하여 해당 지역에 분포되어 있는 다수의 최종 소비자 (Customer)에게 제공된다.

운영 (Operator) 시스템은 전력 공급 상황을 실시간으로 모니터링하여 유지·관리하며, 서비스 제공자 (Service Provider)는 분산 시스템과 최종 소비자 사이에서의 전력 공급 계약 체결 및 전력 공급을 담당하고 전력 시장 (Market)에서는 스마트그리드 참여 기관 사이에서의 거래가 이루어진다. 전력 공급과 함께 스마트그리드에서의 실시간 정보는 시스템을 구성하는 모든 참여자가 유기적으로 연결된 네트워크를 통하여 양방향으로 공유될 수 있다.

이와 같은 정보 교환 구조에서, 최종 소비자의 프라이버시 보존을 위해서는 각 참여자가 필요로 하는 최소한의 정보만 제공될 필요가 있다. 다시 말하면, 서비스 제공자는 개별 사용자의 생활 패턴이 노출되지 않는 범위에서 장기간 (월 또는 연 단위)에 걸친 누적 사용량과 최종 소비자와의 계약으로 합의된 전력원별 비용을 곱하여 사용료를 청구할 수 있으면 충분하며, 전력원에서는 개별 사용자의 전력 소모량이 아닌 단위 시간당 소모된 총 전력량만을 이용하여 향후 생산할 전력량을 예측할 수 있을 것이다.

2.1 프라이버시 보존 전력량 집계

스마트그리드 시스템의 최종 소비자가 보유한 스마트 미터 (smart meter)는 프라이버시 보존을 위하여 전력 소모량 정보를 암호화하여 전달할 필요가 있으며, 이에 대한 다수의 연구가 진행되었다 [4,5].

Garcia와 Jacobs는 자신의 전력 사용량을 자신과 연결된 이웃 스마트 미터에게 Paillier 암호화를 이용하여 전달함으로써 최종 집계 결과를 공유할 수 있는 단위 시간당 누적 전력량 계산 방안을 제시하였다 [6]. Li 등은 구조적 효율성 향상을 위하여 집계 트리 (aggregation tree) 구조를 활용함으로써 말단 노드 (leaf node)에 위치한 스마트 미터로부터 근 노드 (root node)의 집계자에 이르는 경로에 분포된 스마트 미터들의 전력 사용량 집계를 Paillier 암호문을 이용하여 합산할 수 있는 방안을 제시하였다 [7]. Hur 등은 집계 트리를 활용하되, Paillier 암호화 기법의 지수 연산에 따른 연산 복잡도를 개선하기 위하여 모듈로 기반의 동형 암호화 기법을 제시

함으로써 효율성 향상를 도모하였다 [8]. 최근 Rial 등은 단위 시간당 서로 상이한 전력원을 사용하는 환경에서의 비간섭 영지식증명 (non-interactive zero knowledge proof, NIZK), 서명, 커밋 (commit) 등의 암호학적 요소를 결합한 프라이버시 보존을 집계 기법을 제시하였다 [9].

하지만 위 연구들은 단위 시간당 개별 전력량 정보를 숨긴 총 사용량만을 계산하도록 설계되었으며, 비용 청구를 위한 개인의 누적 사용량 집계 및 다수의 전력원을 활용하는 스마트그리드 시스템에 대한 고려는 충분히 이루어지지 않았다. 시스템 전반에서의 프라이버시 보존을 위해서는 참여자들이 유기적으로 결합된 환경에서 스마트 미터에서 암호화된 전력 사용량이 각 주체가 필요로 하는 정보에 대해서만 효과적으로 제공될 수 있는 방안이 마련될 필요가 있다. 따라서 본 연구에서는 별도의 암호화 기법을 중복 적용하지 않고도 스마트 미터에서 암호화된 데이터를 각 주체가 필요로 하는 형태로 변환하여 다수 전력원에 따른 전력 소모량 취합 및 분석이 가능한 방안을 제시한다.

III. 제안 기법

프라이버시 보존 전력량 집계에서의 기능성 및 효율성 향상 방안을 제시하기에 앞서, 본 논문에서 사용된 동형 암호화 기법을 간략히 살펴본다.

3.1 동형 암호화 (fully homomorphic encryption)

동형 암호화는 평문에 대응되는 암호문에서의 연산 결과가 해당 평문에서의 연산 결과로 복호화될 수 있는 특수한 암호화 기법으로, 프라이버시가 보존된 상태에서 덧셈과 곱셈 등의 연산을 가능하게 한다.

Gentry에 의하여 구현된 동형 암호는 연산의 종류 및 횟수의 제한이 없으며 [10], 암호화 알고리즘 E 및 복호화 알고리즘 D에 대하여 동일한 공개키 pk 및 개인키 sk에 대한 평문 p_1, p_2와 암호문 c_1, c_2의 연산이 아래와 같이 수행될 수 있다:

$$c_1 = E_{pk}(p_1),\ c_2 = E_{pk}(p_2),$$
$$D_{sk}(c_1 + c_2) = p_1 + p_2,\ D_{sk}(c_1 \cdot c_2) = p_1 \cdot p_2.$$

또한 Smart와 Vercauteren은 R-LWE (Ring-Learning with Errors) 난제에 기반하여 하나의 암호문에 다수의 평문을 포함하도록 하는 패킹 (packing) 기법을 제시하여 한 쌍의 암호문 연산이 다수 평문에 대한 연산에 대응되는 SIMD (single instruction multiple data) 유형의 동형 연산 방안을 제시하였다. 평문 $p_{11},...p_{1n}$, $p_{21},...,p_{2n}$과 이에 대응되는 암호문 c_1, c_2의 연산은 다음과 같이 표현될 수 있다:

$$c_1 = E_{pk}(p_{11},...,p_{1n}),\ c_2 = E_{pk}(p_{21},...,p_{2n}),$$
$$D_{sk}(c_1 + c_2) = (p_{11} + p_{21},...,p_{1n} + p_{2n}),$$
$$D_{sk}(c_1 \cdot c_2) = (p_{11} \cdot p_{21},...,p_{1n} \cdot p_{2n}).$$

3.2 스마트그리드 구조

스마트그리드 시스템에서 다수 전력원으로부터 공급되는 전력은 사용자가 실시간으로 선택하여 사용할 수 있으며, 주/야, 동/하절기 등 전력 생산 시기에 따라 상이한 전력 요금이 부과되는 환경을 고려한다. 따라서 사용자 요구에 따라 서비스 제공자는 전력원별 단위 시간당 요금을 사전에 공지하고 사용자의 전력원별 소모량과 단가를 이용하여 전력 사용에 따른 요금을 계산하도록 한다.

스마트그리드를 구성하는 모든 참여자는 서로 독립된 기관으로 제안 기법을 따라 암호화된 통신을 수행하되, 개인 프라이버시 침해를 유발할 수 있는 잠재적 (honest-but-curious) 공격자로 가정한다. 다시 말하면, 사용자를 제외한 모든 스마트그리드 참여자와 외부 공격자는 전송되는 데이터로부터 유의미한 사용자 전력 소모량 정보를 획득하려 하며, 서비스 제공자와 분산 시스템 또한 단위 시간별 특정 사용자의 전력 소모량에 대한 정보 획득을 꾀하는 공격자로 볼 수 있다. 하지만 임의 조작을 통한 데이터 변조 및 독립된 서로 다른 기관 사이에서의 공모 공격을 통한 정보 공개는 이루어지지 않는다고 가정한다.

3.3 동형 암호화를 활용한 프라이버시 보존 전력량 집계

제안 기법에서 사용되는 용어는 Table 1.과 같으며, 제안 시스템은 크게 초기 환경 설정, (최종 사용자의) 전력 소모량 보고, (분산 시스템에서의) 전력량 집계, (서비스 제공자의) 요금 취합 및 청구의 네 단계로 나누어 볼 수 있다.

Table 1. Notations

Notation	Description
sm_i	smart meter $(1 \le i \le n)$
es_j	electricity source $(1 \le j \le l)$
$u_{i,j}$	usage amount of sm_i from es_j
u_i	total usage amount of sm_i
$h(\cdot)$	cryptographic hash function
$a \parallel b$	concatenation of a and b
$(x,...,y)$	series of components $x,...,y$
$E_{pk}(m)$	FHE encryption of m with pk
$D_{sk}(c)$	FHE decryption of c with sk

3.3.1 초기 환경 설정

서비스 제공자는 시스템 전반에 사용될 동형 암호화 공개키/개인키 쌍을 생성한다. 최종 사용자는 Fig. 2.와 같이 서비스 제공자로부터 가용 전력원 및 요금, (서비스 제공자의) 공개키, 전력량 보고 주기, 요금 징수 기간 등의 정보를 수신하고 등록 정보를 제공함으로써 해당 지역의 분산 시스템으로부터 사용자 선택에 따른 전력을 공급받는다.

3.3.2 전력 소모량 보고

최종 사용자에 속하는 스마트 미터는 사전 계약된 단위 시간의 짧은 주기 (예, 15분) 마다 전력원에 따른 실시간 전력 소모량을 측정하고, 동형 암호화 패킹 기법을 활용하여 암호화한다. 사용자 i가 전력원 es_j $(1 \le j \le l)$로부터 단위 시간 t_k $(k \ge 0)$ 동안 사용한 전력량 $u_{i,k} = (u_{i,1,k}, u_{i,2,k}, ..., u_{i,l,k})$는 총 전력원 수 l에 대하여 암호화 과정에서 패킹을 수행하여 $c_{i,k} = E_{pk}(u_{i,k}) = E_{pk}(u_{i,1,k}, u_{i,2,k}, ..., u_{i,l,k})$ 형태의 단일 암호문을 생성한다.

암호화된 전력 소모량 $c_{i,k}$는 단위 시간 t_k마다 분산 시스템에 전달된다.

3.3.3 전력량 집계

분산 시스템은 다수 최종 사용자로부터 수신한 암호문 $c_{i,k}(1 \le i \le n)$으로부터 단위 시간 t_k에서의 전력원에 따른 전력 사용량을 집계한다 (Fig. 3.). 다시 말하면, n개의 스마트 미터로부터 수신한 암호문에 동형 덧셈을 수행하여 단위 시간 t_k에서의 전력

Fig. 2. Smart meter deployment and registration

원별 전력량에 대한 단일 암호문

$$C_{\cdot,k} = \sum_{i=1}^{n} c_{i,k} = E_{pk}(\sum_{i=1}^{n} u_{i,1,k}, ..., \sum_{i=1}^{n} u_{i,l,k})$$

을 얻을 수 있다.

분산 시스템은 암호문 $C_{\cdot,k}$을 서비스 제공자에게 전달하고[1], 서비스 제공자는 자신의 개인키로 복호화한 단위 시간 t_k 동안 소요된 전력원별 누적 전력량을 개별 전력 생산자에게 전달함으로써 향후 전력 생산량 예측에 활용되도록 한다.

3.3.4 요금 취합 및 청구

최종 사용자로부터 수집된 전력 소모량은 서비스 제공자의 과금 정보로도 활용될 수 있다. 이 경우, 동일 사용자에 속하는 스마트 미터 sm_i로부터 수신된 전력 소모량을 시간의 경과에 따라 누적함으로써 긴 주기의 과금 기간 (예, 1개월)에 사용된 사용자별 전력 소모량을 파악할 수 있다. 사용자 i가 시간 t_1부터 t_m까지 소모한 누적 전력량에 대한 암호문은

$$C_{i,\cdot} = \sum_{k=1}^{m} c_{i,k} = E_{pk}(\sum_{k=1}^{m} u_{i,1,k}, ..., \sum_{k=1}^{m} u_{i,l,k})$$

와 같이 표현될 수 있다 (Fig. 4.).

전력원에 따른 사용요금 $\cos t = (\cos t_1, ..., \cos t_l)$에 대하여, 분산시스템은 $\cos t$와 암호문 $C_{i,\cdot}$의 동형 곱셈 연산으로부터 전력원에 따른 과금 정보에 대응되는 암호문

$$\begin{aligned} C_i &= \cos t \cdot C_{i,\cdot} \\ &= (\cos t_i, ..., \cos t_l) \cdot E_{pk}(\sum_{k=1}^{m} u_{i,1,k}, ..., \sum_{k=1}^{m} u_{i,l,k}) \\ &= E_{pk}(\cos t_i \sum_{k=1}^{m} u_{i,1,k}, ..., \cos t_l \sum_{k=1}^{m} u_{i,l,k}) \end{aligned}$$

를 계산하여 서비스 제공자에게 전달한다. 서비스 제

1) 최종 사용자로부터 전달받은 암호문은 서비스 제공자의 개인키로만 복호화가 가능하므로 분산 시스템은 개별 사용자에 대한 전력 소모량을 확인할 수 없다.

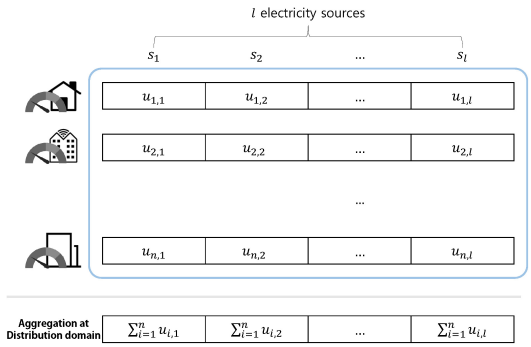

Fig. 3. Meter aggregation per time interval for electricity prediction

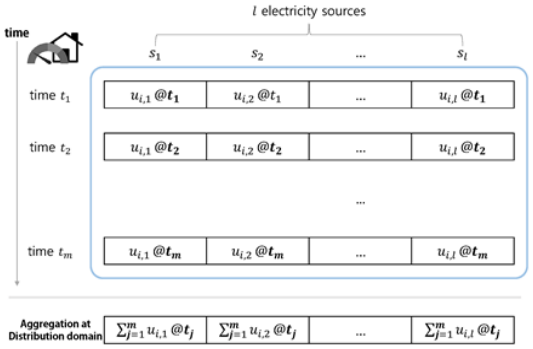

Fig. 4. Meter aggregation for customer charge

공자는 분산 시스템으로부터 전달받은 암호문을 복호화하여 사용자의 단기 전력 사용 패턴 정보를 모르는 상황에서도 전력원에 따른 과금 정보를 취합하고 최종 사용자에게 전력 소모에 따른 비용을 청구한다.

IV. 안전성 및 성능 분석, 제안 기법의 특징

먼저 동형 암호를 활용한 전력 소모량 집계 기법의 특징은 아래와 같이 요약할 수 있다:

1. 선행 연구와 동일하게 단위 시간의 전체 가구에 대한 프라이버시 보존 전력량 집계 기능을 수행한다. 이는 단위 시간당 전체 전력 소모량 집계 결과로부터 근미래의 전력 생산 필요량 예측에 활용될 수 있다.

2. 프라이버시 보존 사용자별 요금 계산 기능을 수행한다. 단위 시간 전력 소모량 집계만을 수행하는 기존 연구에서 나아가 이미 생성된 동형 암호문을 활용하여 별도의 암호화 시스템을 도입하지 않고 전력 소모 패턴이 노출되지 않는 요금 계산이 가능하다.

3. 다수 전력원에 대한 개별 전력량 집계 기능을 수행한다. 상이한 전력 생산자로부터 소모되는 전력량의 개별 분석이 가능하면서도, 하나의 암호문에 대한 연산이 가능하도록 함으로써 단일 전력원에 대한 전력량 집계와 동등한 연산 효율성을 유지한다.

4.1 안전성 분석

제안 기법에서 생성된 암호문의 기밀성 및 동형 연산 과정에서의 무결성은 기반 동형 암호화의 안전성에 기반하므로 [11], 여기서는 전력량 집계 과정에서의 정보 유출 가능성에 따른 안전성을 살펴본다.

단위 시간 당 전력량 집계에 있어, 스마트 미터 sm_i에 의하여 암호화된 내용은 서비스 제공자의 개인키로만 복호화가 가능하다. 따라서 분산 시스템은 동형 덧셈 연산을 수행하더라도 개별 사용자의 전력 소모량에 대한 정보를 수집할 수 없어 사용자 프라이버시가 보장된다. 개별 사용자 요금 청구 과정에 있어서도, 분산 시스템은 복호화 키를 소유하지 않기 때문에 개인 전력 소모량 누적 과정에서 대응되는 평문 내용을 파악하지 못한다. 서비스 제공자는 자신이 생성한 개인키로 암호문에 대한 복호화를 수행할 수 있으나, 분산 시스템에서 취합된 전체 기간의 누적 전력량에 대한 암호문만을 전달받기 때문에 단기 전력 소모 패턴을 파악하기 어렵다.

4.2 성능 분석

제안 기법의 효율성 검증을 위한 구현은 Halevi의 동형 암호화 라이브러리 (HElib) [12]와 Bethencourt의 Paillier 암호화 라이브러리 [13]를 사용하였으며, Ubuntu 16.04 Server에서 C++로 작성되었다. 3.4GHz CPU에서 수행된 실험은 단일 코어상에서 별도의 최적화를 수행하지 않은 결과를 측정하였으며, 100회 반복을 통하여 획득한 평균값을 표기하였다. 가구당 월별 평균 전력 소모량 (867kWh)을 참조 [14]하여 100가구에서 100,000가구에 이르는 누적 전력 소모량을 집계하였으며, 이를 위하여 최대 40비트의 평문 공간을 가지도록 설정하였다. 또한 NIST의 권고안 [15]에 따라, 동일 수준의 안전성 (112비트)을 유지하도록 동형 암호는 하나의 암호문에 168개의 평문 (전력원 종류의 개수)을 포함하도록 하였고, Paillier 암호화의 키 길이는 2,048비트로 설정하였다.

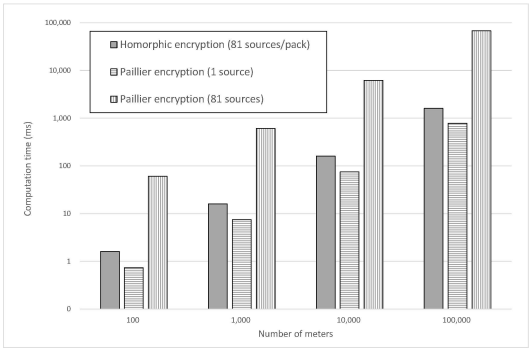

Fig. 5. Comparison of computation cost for aggregation per meters and sources

4.2.1 통신 복잡도

스마트그리드 시스템의 참여자들은 프라이버시에 민감한 정보를 암호화된 형태로 송수신하므로 단위 암호문에 대한 크기 비교를 통하여 암호문 통신에 소요되는 비용을 가늠할 수 있다. Paillier 암호화에서는 하나의 암호문이 512바이트의 공간을 차지하는 반면 동형 암호문 하나의 크기는 163,208바이트로 측정되었다. 하나의 동형 암호문에 168개의 평문이 내포되기 때문에 평문 하나당 971바이트의 암호문에 대응된다고 볼 수 있다. 이는 Paillier 암호화 기법에 대비하여 동형 암호화 기법에서 약 89%의 오버헤드가 발생한 것으로, (leveled FHE에서의) 동형 곱셈 연산의 허용 횟수, 암호문 패킹 수준, 안전성 정도에 따른 매개변수 설정에 따라 달라지는데, 동형 암호문에 포함된 노이즈 및 복호화 과정에서의 노이즈 제거를 위하여 공개키의 크기가 상대적으로 크기 때문에 기존 암호화 시스템에 비하여 암호문의 크기가 커질 수 밖에 없다. 하지만 시스템 설정 과정에서 동형 곱셈 허용 횟수 및 전력원 종류에 따른 단일 암호문 내 평문 개수 조절에 대한 추가 분석을 통하여 동형 암호문의 최적 크기를 파악함으로써 불필요한 저장공간의 낭비를 감소시키고 통신 복잡도를 낮출 수 있을 것이다.

4.2.2 연산 복잡도

서비스 제공자는 시스템 전반에 사용될 암호화를 위한 공개키/개인키 쌍을 생성하는데, Paillier 암호화에서는 236.904ms가 소요된 반면 동형 암호화는 3,413.937ms가 소요되어 14.4배의 시간을 필요로 한다. 하지만 이는 시스템 초기 환경 설정에서 한 번만 수행되므로 그 의미가 크지 않다고 할 수 있다.

Table 2. Comparison of aggregation time (ms) with varying number of houses

Enc* / #.houses**	Homo-morphic	Paillier (1 src.)	Paillier (168 srcs.)
100	1.61	0.74	60.41
1,000	16.02	7.47	607.54
10,000	160.16	74.66	6,196.96
100,000	1,606.09	783.44	67,464.64

* Enc: encryption algorithm
** #.houses: number of houses being aggregated

가장 빈번한 연산이 이루어지는 분산 시스템에서의 집계에 소요되는 시간은 Fig. 5. (Table 2)와 같으며, 가구 (meter) 수에 비례하여 소요시간이 증가하는 경향을 보인다. 제안 기법에서는 10,000가구 기준으로 160.163ms가 소요(좌측 단색)된 반면, Paillier 암호화를 이용한 경우에는 6,195.959ms가 소요(우측 세로줄무늬)되어 약 37배의 성능 향상을 꾀할 수 있었다. 이는 Paillier 암호화를 이용하여 단일 집계 연산을 수행하는데 소요되는 시간(중앙 가로줄무늬)은 상대적으로 짧음에도 불구하고, 동형 암호화에서는 패킹을 이용하여 한 가구에서 사용할 수 있는 168개의 서로 다른 전력원에 대한 집계를 하나의 암호문 연산으로 수행할 수 있는 것과 달리 Paillier 기법을 이용하는 경우에는 논리적 병렬 연산이 불가능하기 때문이다.

V. 결 론

안정적 전력 생산 및 효율적 유지·관리 등 다양한 장점을 지닌 스마트그리드 시스템의 활성화를 위해서는 사용자 프라이버시 문제의 해결이 선행되어야 할 것이다. 본 논문에서는 다양한 전력원으로부터의 선택적 전력 이용이 가능한 환경에서 사용자, 서비스 제공자, 전력원이 필요로 하는 정보를 프라이버시가 보존된 환경에서 효율적으로 집계 및 활용할 수 있는 방안을 동형 암호화 기법을 활용하여 제시하였다. 평문 대비 암호문 크기의 증가는 기존 암호문 기법에 비하여 동형 암호화 기법에서 개선되어야 할 중요한 이슈 중의 하나로 볼 수 있으며, 스마트그리드 시스템의 요구사항 분석을 통하여 최적 매개변수를 설정

함으로써 저장 공간 및 통신 복잡도를 감소시킬 수 있을 것이다. 반면, 성능 분석을 통하여 확인한 바와 같이 패킹 기법을 활용하여 개별 평문에 대한 개별 연산을 수행하지 않고도 다수 평문에 대응되는 암호문 상에서의 연산을 통하여 보다 효율적인 집계 및 분석이 가능함을 확인하였다.

개발 초기의 동형 암호화에서 비롯된 성능 저하 문제가 지속적으로 개선되고 있는 현시점에서, 동형 암호의 전력 사용량 집계에의 활용은 프라이버시가 보존되는 환경에서 다양한 연산 및 분석의 효율적 수행을 가능하게 할 것이다.

References

[1] Xu Li, Xiaohui Liang, Rongxing Lu, Xuemin Shen, Xiaodong Lin, and Haojin Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38-45, Aug. 2012.

[2] Ruilong Deng, Zaiyue Yang, Mo-Yuen Chow, and Jiming Chen, "A Survey on Demand Response in Smart Grids: Mathematical Models and Approaches," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 570-582, 2015.

[3] Ronald Petrlic, "A privacy-preserving Concept for Smart Grids," *Sicherheit in vernetzten Systemen 18 DFN Workshop*, 2010.

[4] Rongxing Lu, Xiaohui, Liang, Xu Li, Xiaodong Lin, and Xuemin Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621-1631, 2012.

[5] Yuwen Chen, J-F. Martinez-Ortega, Pedro Castillejo, and Lourdes Lopez, "A Homomorphic-Based Multiple Data Aggregation Scheme for Smart Grid," *IEEE Sensors Journal*, vol. 19, no. 10, pp. 3921-3929, 2019.

[6] F.D. Garcia and Bart Jacobs, "Privacy-Friendly Energy-Metering via Homomorphic Encryption," *International Workshop on Security and Trust Management*, pp. 226-238, Sep. 2010.

[7] Fengjun Li, Bo Luo, and Peng Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," *IEEE International Conference on Smart Grid Communications*, pp. 327-332, Oct. 2010.

[8] Junbeom Hur, Dongyoung Koo, and Yougjoo Shin, "Privacy-Preserving Smart Metering with Authentication in a Smart Grid," *Applied Sciences*, vol. 5, no. 4, pp. 1503-1527, Dec. 2015.

[9] Alfredo Rial, George Danezis, and Markulf Kohlweiss, "Privacy-preserving smart metering revisited," *International Journal of Information Security*, vol. 17, no. 1, pp. 1-31, Feb. 2018.

[10] Craig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," *ACM Symposium on Theory of Computing*, pp. 169-178, May. 2009.

[11] N.P. Smart and Frederik Vercauteren, "Fully homomorphic SIMD operations," *Designs, Codes and Cryptography*, vol. 71, no. 1, pp. 57-81, Apr. 2014.

[12] Shai Halevi and Victor Shoup, "Algorithms in HElib," *CRYPTO*, pp. 554-571, Aug. 2014 (Available on https://github.com/homenc/HElib).

[13] John Bethencourt, "Advanced Crypto Software Collection: Paillier Library," (Available on http://hms.isi.jhu.edu/acsc/libpaillier/, version: Jan. 2010).

[14] U.S. Energy Information Administra-

tion, "How much electricity does an American hose use?," (Available on https://www.eia.gov/tools/faqs/faq.php?id=97&t=3), Oct. 2018.
[15] Elaine Barker, "Recommendation for Key Management, Part 1: General," *NIST Special Publication 800-57 Part 1, Revision 4*, Jan. 2016.

〈저자소개〉

구 동 영 (Dongyoung Koo) 종신회원
2009년 2월: 연세대학교 컴퓨터.산업공학과 졸업
2012년 2월: 한국과학기술원 전산학과 석사
2016년 2월: 한국과학기술원 전산학부 박사
2016년 3월~2017년 3월: 고려대학교 정보대학 컴퓨터학과 연구교수
2017년 4월~현재: 한성대학교 전자정보공학과 조교수
〈관심분야〉 정보보호, 응용 암호, 네트워크 보안, 클라우드/엣지/포그 컴퓨팅 보안