



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0169930
(43) 공개일자 2022년12월28일

(51) 국제특허분류(Int. Cl.)
G06F 17/14 (2006.01) H04L 9/00 (2022.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
G06F 17/141 (2013.01)
H04L 9/008 (2013.01)
(21) 출원번호 10-2022-0075783
(22) 출원일자 2022년06월21일
심사청구일자 2022년06월21일
(30) 우선권주장
1020210080300 2021년06월21일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암
동5가)
(72) 발명자
이강훈
서울특별시 동작구 동작대로39길 22, 115-301
전영배
경기도 성남시 수정구 위례순환로 211, 위례센트
럴푸르지오 5405호 902호
윤지원
서울특별시 용산구 한강대로43길 8, 102동 1401
호
(74) 대리인
김등용

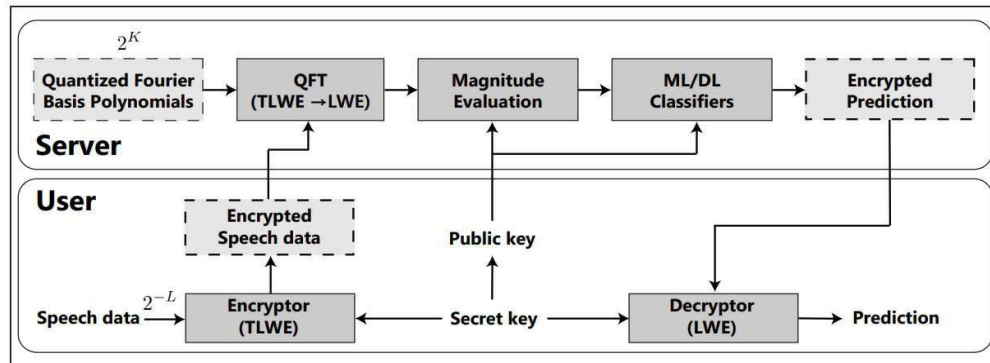
전체 청구항 수 : 총 5 항

(54) 발명의 명칭 동형암호에 기반한 시계열 데이터의 암호화 및 이산 푸리에 변환 방법

(57) 요약

동형암호에 기반한 시계열 데이터의 암호화 및 이산 푸리에 변환 방법이 개시된다. 상기 방법은 단말과 서버를 포함하는 시스템 상에서 수행되는 암호화 및 푸리에 변환 방법으로써, 상기 단말이 음성 데이터에 대한 암호문을 생성하는 단계, 상기 단말이 상기 암호문을 서버로 송신하는 단계, 상기 서버가 상기 암호문에 대한 이산 푸리에 변환을 수행하는 단계, 및 상기 서버가 상기 이산 푸리에 변환의 결과를 상기 단말로 송신하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류
H04L 9/3093 (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

명세서

청구범위

청구항 1

단말과 서버를 포함하는 시스템 상에서 수행되는 암호화 및 푸리에 변환 방법에 있어서,
상기 단말이 음성 데이터에 대한 암호문을 생성하는 단계;
상기 단말이 상기 암호문을 서버로 송신하는 단계;
상기 서버가 상기 암호문에 대한 이산 푸리에 변환을 수행하는 단계; 및
상기 서버가 상기 이산 푸리에 변환의 결과를 상기 단말로 송신하는 단계를 포함하는 암호화 및 푸리에 변환 방법.

청구항 2

제1항에 있어서,
상기 암호문을 생성하는 단계는 상기 음성 데이터에 대한 전처리 단계를 포함하고,
상기 전처리 단계는,
상기 음성 데이터를 미리 정해진 길이를 갖는 복수의 세그먼트들로 분할하는 단계;
상기 세그먼트들 각각에서 DC 바이어스를 제거하는 단계; 및
상기 세그먼트들 각각이 미리 정해진 범위 내의 값을 갖도록 스케일링하는 단계를 포함하는,
암호화 및 푸리에 변환 방법.

청구항 3

제2항에 있어서,
상기 암호문을 생성하는 단계는 동형암호(Homomorphic Encryption, HE) 기법을 이용하여 상기 암호문을 생성하는,
암호화 및 푸리에 변환 방법.

청구항 4

제3항에 있어서,
상기 이산 푸리에 변환을 수행하는 단계는 푸리에 다항식을 생성하는 단계를 포함하고,
상기 푸리에 다항식은 알고리즘 1을 이용하여 생성되는,
암호화 및 푸리에 변환 방법.

[알고리즘 1]

Algorithm 1: Conversion of the Fourier basis polynomial

Input: Fourier basis polynomial $F(X) = \sum_i F_i X^i \in \{C_f(X), S_f(X) \mid f \in [N]\}$, QFT scaling parameter K , Fourier quantization parameter Q .

Output: Quantized Fourier basis polynomial $\bar{F}_K(X) \in \mathbb{Z}_N[X]$ with $(Q+1)$ bits of resolution

- 1 For each $F_i \in \mathbb{R}$, set $\bar{F}_i$ as the closest multiple of $\frac{1}{2^Q}$ to F_i
 - 2 Compute $\bar{F}_{K,i} = \bar{F}_i \cdot 2^K$ where each $\bar{F}_{K,i} \in [-2^K, 2^K]$
 - 3 **return** $\bar{F}_K(X) = \sum_{i=0}^{N-1} \bar{F}_{K,i} X^i$
-

청구항 5

제4항에 있어서,

상기 이산 푸리에 변환을 수행하는 단계는 알고리즘 2를 이용하여 이산 푸리에 변환을 수행하는,

암호화 및 푸리에 변환 방법.

Algorithm 2: Quantized Fourier Transform on TLWE ciphertext

Input: TLWE ciphertext

$\mathbf{C} = (\mathbf{a}, \mathbf{b}) \in \text{TLWE}_{\mathcal{K}}(\mu(X))$, a set of quantized Fourier basis polynomials $\{\bar{C}_{K,f}(X), \bar{S}_{K,f}(X) \mid f \in [N]\}$

Output: $2N$ LWE ciphertexts $(\mathbf{c}_{f,i})_{f \in [N], i \in \{0,1\}}$ encrypting $\bar{X}_C[f]$'s and $\bar{X}_S[f]$'s under the key $\mathcal{K}'$

- 1 **for** $f \in [N], i \in \{0,1\}$ **do**
 - 2 **if** $i = 0$ **then**
 - 3 $\bar{F}_K(X) = \bar{C}_{K,f}(X)$
 - 4 **else**
 - 5 $\bar{F}_K(X) = \bar{S}_{K,f}(X)$
 - 6 $\mathbf{C}_i = (\mathbf{a} \cdot \bar{F}_K(X), \mathbf{b} \cdot \bar{F}_K(X))$
 - 7 $\mathbf{c}_{f,i} = \text{SampleExtract}_{N-1}(\mathbf{C}_i)$
 - 8 **return** $(\mathbf{c}_{f,i})_{f \in [N], i \in \{0,1\}}$
-

발명의 설명

기술 분야

[0001]

본 발명은 동형암호(Homomorphic Encryption)를 이용하여 실수 시계열 데이터를 암호화하고, 암호화된 시계열 데이터에 이산 푸리에 변환(Discrete Fourier Transform, DFT)을 적용하여 암호화된 상태에서도 시계열 데이터를 주파수 대역에서 분석할 수 있는 방법 및 장치에 관한 것이다.

배경 기술

[0002]

최근, Amazon Alexa, Microsoft Cortana, Apple Siri, 및 Google Assistant와 같은 보이스(voice) 또는 스피치(speech) 기반의 인터페이스(interface)가 널리 소개되고 있다. 이러한 스피치 기반의 인터페이스는 스마트 장치의 사용이 증가함에 따라 보다 폭넓게 활용되고 있는 추세이다. 게다가, Microsoft Azure에서의 스피치 서비스(Speech Service)와 Google cloud Speech API와 같이, 스피치 데이터에 특화된 클라우드 컴퓨팅 서비스들이 제공되고 있다. 이러한 스피치 기반의 서비스들은 사용자의 데이터를 처리하기 위하여 사용자의 스피치 데이터를 서버로 전송하는 과정을 필요로 한다. 서버로 전송된 데이터는 음성 인식(speech recognition)과 자연어 처리(natural language processing)를 위하여 처리되고 텍스트로 변환된다. 텍스트 변환은 사용자에게 제공되는 응답을 생성하기 위해 이용된다. 그러나, 스피치 데이터에 대한 레코딩(recordings)과 텍스트로의 변환

(translations)의 결과는 서비스를 제공하는 서버에 저장되어 유지될 수 있다.

[0003] 스피치 데이터는 민감한 생체 데이터(sensitive biometric data)이기 때문에, 이는 심각한 프라이버시 침해의 문제를 야기할 수 있다. 스피치 데이터는 화자(speaker)의 성별(gender), 나이(age), 감정(emotion)에 대한 정보를 포함하고, 심지어 녹취 자체에는 보이스 명령(voice commands), 메시지(messages), 대화(conversations)가 포함될 수 있다.

[0004] 상술한 문제를 해결하기 위한 방법 중 하나는 동형암호(Homomorphic Encryption, HE)에 기반한 접근법이다. 동형암호를 통해 서버로 전송되는 모든 데이터는 암호화될 수 있다. 입력(input) x , 함수(function) f , 및 암호화 함수(encryption function) E 가 주어졌을 때, HE는 $E(x)$ 에 대한 복호화 없이 $E(x)$ 로부터 $E(f(x))$ 를 연산할 수 있다. 사용자의 키를 이용하여 입력 데이터를 암호화하는 것은 보안을 유지시킬 수 있고, 동형 연산(homomorphic operations)은 서버가 복호화되지 않은 데이터를 처리할 수 있도록 한다. 이는 서버가 사용자의 데이터(예컨대, 스피치 기록)가 유출되지 않은 상태에서 처리할 수 있도록 한다.

[0005] 본 발명에서는, (완전) 동형암호 기법((fully) homomorphic encryption scheme)을 이용하여 안전한 엔드투엔드(end-to-end) 스피치 처리와 암호화된 시계열 데이터에 대한 응용을 제안한다. 안전한 시계열 데이터 처리를 위해, 빠른 동형 QFT(fast homomorphic Quantized Fourier Transform)를 제안한다.

선행기술문헌

비특허문헌

[0006] (비특허문헌 0001) Bianchi, T., Piva, A., & Barni, M. (3009). On the implementation of the discrete Fourier transform in the encrypted domain. IEEE Transactions on Information Forensics and Security, 4(1), 86-97.

(비특허문헌 0002) Costache, A., Smart, N. P., & Vivek, S. (2017, April). Faster homomorphic evaluation of discrete fourier transforms. In International Conference on Financial Cryptography and Data Security (pp. 517-529). Springer, Cham.

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적인 과제는 동형암호에 기반한 시계열 데이터의 암호화 및 이산 푸리에 변환 적용 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 일 실시예에 따른, 동형암호에 기반한 시계열 데이터의 암호화 및 이산 푸리에 변환 방법 단말과 서버를 포함하는 시스템 상에서 수행되는 암호화 및 푸리에 변환 방법으로써, 상기 단말이 음성 데이터에 대한 암호문을 생성하는 단계, 상기 단말이 상기 암호문을 서버로 송신하는 단계, 상기 서버가 상기 암호문에 대한 이산 푸리에 변환을 수행하는 단계, 및 상기 서버가 상기 이산 푸리에 변환의 결과를 상기 단말로 송신하는 단계를 포함한다.

발명의 효과

[0009] 본 발명의 실시예에 따른 동형암호 기반의 시계열 데이터의 암호화 및 이산 푸리에 변환 방법에 의할 경우, 기존의 동형암호를 이용한 이산 푸리에 변환 적용 연구들에 비해 한 암호문 내에 다중의 데이터를 암호화함으로써 동형암호의 문제점으로 지적되었던 메모리 사용 문제를 해소할 수 있다.

[0010] 또한, 기존 연구들보다 이산 푸리에 변환에 필요한 연산량을 줄여 속도를 획기적으로 개선하였다. 요컨대, 개인의 시계열 데이터를 효율적으로 암호화하여 사용자가 전송하여야할 데이터 용량을 줄이고, 해당 데이터에 이산 푸리에 변환을 짧은 시간 내에 복호화 없이 계산하여 사용자의 개인 데이터 및 정보를 보호함과 동시에 시계열 데이터의 특성을 추출할 수 있다.

도면의 간단한 설명

- [0011] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.
- 도 1은 본 발명의 일 실시예에 따른 푸리에 변환 방법을 설명하기 위한 개략도이다.
- 도 2는 고정된 K 값에 따른 양자화 결과를 도시한다.
- 도 3은 본 발명의 일 실시예에 따른, 동형암호 기반 (실수) 시계열 데이터의 암호화 및 이산 푸리에 변환 시스템을 도시한다.
- 도 4는 도 3에 도시된 시스템에서 수행되는 동형암호 기반 (실수) 시계열 데이터의 암호화 및 이산 푸리에 변환 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0012] 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.
- [0013] 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.
- [0014] 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.
- [0015] 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.
- [0016] 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.
- [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 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.
- [0018] 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.
- [0019] 우선, 본 발명의 일 실시예에 따른 동형암호 기반의 실수 시계열 데이터의 암호화 및 이산 푸리에 변환 방법 및 장치를 구현하기 위한 기술들을 소개한다.

A. 표기법(Notation)

- [0021] 본 명세서에서는, 집합 $\{0,1\}$ 을 $\mathbb{B}$ 로 나타내고, 실수에 대한 모듈러 1 연산의 결과 집합인 리얼 토러스(real Torus) $\mathbb{R}/\mathbb{Z}$ 를 $\mathbb{T}$ 로 나타낸다(즉, $T = \mathbb{R}/\mathbb{Z} = \mathbb{R} \pmod{1}$). 또한, 반개구간(half open interval) $[-\frac{1}{2}, \frac{1}{2}[= [0, \frac{1}{2}[\cup [-\frac{1}{2}, 0[$ 을 리얼 토러스로 고려한다. 모듈러 1 연산 후의 $\mathbb{T}$ 와 동일하기 때문이다. 다만, 실시예에 따라, 반폐구간, 개구간, 및 폐구간의 리얼 토러스가 적용될 수도 있다.
- [0022] $\mathbb{R}[X]/(X^N + 1)$ 와 $\mathbb{Z}_N[X]/(X^N + 1)$ 를 각각 나타내기 위하여, $\mathbb{R}_N[X]$ 와 $\mathbb{Z}_N[X]$ 를 이용한다. 또한, $\mathbb{T}_N[X]$ 은 $\mathbb{Z}_N[X]$ 에 대한 모듈러 1 연산의 결과를 나타내고, $\mathbb{B}_N[X]$ 는 이진 계수들(binary coefficients)을 갖는 $\mathbb{Z}_N[X]$ 내의 다항식들로 나타낸다.
- [0023] $[n, m]$ for $n, m \in \mathbb{Z}$ 는 정수 집합 $\{x \in \mathbb{Z} \mid n \leq x \leq m\}$ 을 나타내고, $[n]$ for $n \in \mathbb{Z}^+$ 는 $\{x \in \mathbb{Z} \mid 0 \leq x \leq n-1\}$ 를 나타낸다.
- [0024] 집합 $\mathcal{S}$ 에 대해, $x \stackrel{\$}{\leftarrow} \mathcal{S}$ 는 x 가 집합 $\mathcal{S}$ 로부터 균등 샘플링됨(uniformly sampled)을 의미한다. 유사하게, 분포(distribution) $\mathcal{D}$ 에 대해, $x \leftarrow \mathcal{D}$ 는 x 가 $\mathcal{D}$ 로부터 샘플링되었음을 의미한다.
- [0025] **B. TFHE**
- [0026] TFHE는 LWE(Learning With Errors)과 LWE의 Ring 변이(Ring LWE)의 어려움(hardness)에 기반한 완전동형암호 기법(fully homomorphic encryption scheme)이다. 이에 관한 구체적인 내용은 I. Chillotti 등의 논문(I. Chillotti, N. Gama, M. Georgieva, and M. Izabachene. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3-33. Springer, 2016.), I. Chillotti 등의 논문(I. Chillotti, N. Gama, M. Georgieva, and M. Izabachene. Faster packed homomorphic operations and efficient circuit bootstrapping for TFHE. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 377-408. Springer, 2017.) 및 I. Chillotti 등의 논문(I. Chillotti, N. Gama, M. Georgieva, and M. Izabachene. TFHE: fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34?91, 2020.) 등이 참조될 수 있다. 다만, 본 발명이 I. Chillotti 등이 제안한 암호화 기법에만 적용될 수 있는 것은 아니고, (완전) 동형암호 기법이 사용된 다른 암호화 기법에 사용될 수 있음은 자명하다.
- [0027] TFHE는 리얼 토러스 $\mathbb{T}$ 상에서 동작한다. $\mathbb{T}$ 는 환(ring)이 아니기 때문에, $\mathbb{T}$ 상에서의 곱셈은 정의되지 않는다. 차라리, $\mathbb{T}$ 는 이하의 정의 1(Definition1)을 따르는 $\mathbb{Z}$ -module 이고, $\mathbb{Z}$ 와 $\mathbb{T}$ 사이의 프리덕트(product) 연산은 정의된다. 이를 확장하여, $\mathbb{T}_N[X]$ 내의 다항식은 $\mathbb{Z}_N[X]$ -module 이다. 본 발명에서는 이러한 특성(property)을 이용하고자 한다.
- [0028] **Definition 1** : $(R, +, \times)$ 를 가환환(commutative ring)이라 하자. 연산 $\cdot$ 에 대한 덧셈 아벨 군(additive abelian group) A : $R \times A \rightarrow A$ 는 **R-module** if $\forall r, s \in R$ and $a, b \in A$, $r \cdot (a + b) = r \cdot a + r \cdot b$, $(r + s) \cdot a = r \cdot a + s \cdot a$, $(r \times s) \cdot a = r \cdot (s \cdot a)$, $1_R \cdot a = a$.
- [0029] **Sub-Gaussian distribution.** 랜덤 변수(random variable) X over $\mathbb{R}$ 는 파라미터 σ^2 를 갖는 sub-Gaussian이다와 $\mathbb{E}[X] = 0$ 는 필요충분조건이고, 이의 모멘트 생성 함수(moment generating function)는 $\mathbb{E}[\exp(tX)] \leq \exp(\sigma^2 t^2 / 2) \forall t \in \mathbb{R}$ 를 만족한다.
- [0030] 고정된 σ 에 대하여, 표준편차(standard deviation) σ 를 갖는 가우시안 랜덤 변수 또는 $[-\sqrt{3}\sigma, \sqrt{3}\sigma]$ 상에서의 균등 랜덤 변수(uniform random variable)는 모두 파라미터 σ^2 를 갖는 서브-가우시안이다. 또한, 임의의 독립적인(independent) 서브-가우시안 랜덤 변수로써, 파라미터 σ_1^2 와 σ_2^2 를 갖는 X 와 Y 에 대하여, $aX + bY$ 는 임의의 $a, b \in \mathbb{R}$ 에 대하여 파라미터 $(a^2\sigma_1^2 + b^2\sigma_2^2)$ 를 갖는 서브-가우시안이다.

[0031] **LWE(Learning with errors)**. 보안 상수(security parameter) λ 에 대하여, LWE의 차원(dimension) $n \in \mathbb{N}$ 과 $\mathbb{R}$ 상에서의 에러 분포(error distribution) $\mathcal{X}$ 가 결정된다. LWE 비밀값(secret) $\mathbf{K} \in \mathbb{B}^n$ 은 키 분포(key distribution)으로부터 샘플링된다. 메시지 μ 를 이산 메시지 공간(discrete message space) $\mathcal{M} \subset \mathbb{T}$ 의 원소(element)라고 하자. μ 에 대한 LWE 암호화는 튜플(tuple) $(\mathbf{a}, \mathbf{b}) \in \mathbb{T}^n \times \mathbb{T}$ ($\mathbf{a} \xleftarrow{\$} \mathbb{T}^n$, and $\mathbf{b} = \mathbf{a} \cdot \mathbf{K} + \mu + e \in \mathbb{T}$, with $e \leftarrow \mathcal{X}$)이다. 이하에서는, $\mathbf{c}$ 가 키(key) $\mathbf{K}$ 하에서 μ 에 대한 LWE 암호문이면, $\mathbf{c} \in \text{LWE}_{\mathbf{K}}(\mu)$ 로 표기한다.

[0032] $\mathbb{T}^n \times \mathbb{T}$ 로부터 $\mathbb{T}$ 로의 선형 함수(linear function)인 $\mathbf{c}$ 의 상(phase)은 $\varphi_{\mathbf{K}}(\mathbf{c}) = \mathbf{b} - \mathbf{K} \cdot \mathbf{a}$ 으로 정의된다. 복호화를 위해, 상(phase)은 $\mathcal{M}$ 의 가장 가까운 원소(nearest element)로 라운드된다(rounded). 암호문 $\mathbf{c}$ 에 대한 복호화의 결과가 매우 높은 확률로 μ 가 되는 경우, 암호문 $\mathbf{c}$ 는 μ 에 대한 유효한 암호문이라고 말할 수 있다. 상 함수(phase function)의 선형성(linearity)로 인하여, LWE 암호는 덧셈에 대한 동형(additively homomorphic)이다. 이는 LWE 암호문 $\mathbf{c} \in \text{LWE}_{\mathbf{K}}(\mu)$ 에 대한 정수 $r \in \mathbb{Z}$ 의 곱셈을 아래와 같이 가능케 한다($r \geq 0$ 인 경우).

$$r \cdot \mathbf{c} = \underbrace{\mathbf{c} + \mathbf{c} + \cdots + \mathbf{c}}_{r \text{ times}}$$

[0033]

[0034] r 이 0 보다 작은 경우, 대신 $(-\mathbf{c})$ 를 더할 수 있다. 에러 $r \cdot e$ 가 작은 값을 유지한다면, $r \cdot \mathbf{c}$ 는 $r \cdot \mu$ 에 대한 유효한 암호문이다.

[0035]

TLWE. Z. Brakerski 등의 논문(Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3):1-36, 2014.)과 V. Lyubashevsky 등의 논문(V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1-23. Springer, 2010.)에 따라, 토러스 상에서의 LWE와 Ring LWE에 대한 TLWE로의 일반화를 고려한다. 보안 상수 λ 하에서, 파라미터들 $k, N \in \mathbb{N}$ 와 $\mathbb{T}_N[X]$ 상에서의 에러 분포 $\mathcal{X}$ 가 결정된다. N 은 2의 거듭제곱(power)으로 선택되고 $2N$ 번째 원분 다항식(cyclotomic polynomial) $X^N + 1$ 이 주어진다.

[0036]

암호화를 위해, TLWE 비밀값(secret) $\mathbf{K} \in \mathbb{B}_N[X]^k$ 이 키 분포로부터 선택된다. 키 $\mathbf{K}$ 하에서 다항식 $\mu(X) \in \mathbb{T}_N[X]$ 에 대한 TLWE 암호화는 또한 튜플 $(\mathbf{A}, \mathbf{B}) \in \mathbb{T}_N[X]^k \times \mathbb{T}_N[X]$ ($\mathbf{A} \xleftarrow{\$} \mathbb{T}_N[X]^k$ 및 $\mathbf{B} = \mathbf{K} \cdot \mathbf{A} + \mu(X) + e$ with $e \leftarrow \mathcal{X}$)이다. 이하에서는, $k = 1$ 을 사용하였고, 제안하는 TLWE 암호문은 $\mathbb{T}_N[X]$ 내의 두 개의 다항식들로 구성된다.

[0037]

LWE와 같이, TLWE 암호 역시 덧셈에 대한 동형이고, 이는 $\mathbb{Z}$ 에 속하는 정수를 이용한 스칼라 곱을 가능케 한다. 게다가, $\mathbb{T}_N[X]$ 의 $\mathbb{Z}_N[X]$ -module 성질을 이용하면, 상수 다항식(integer polynomial) $r(x) \in \mathbb{Z}_N[X]$ 을 TLWE 암호문에 곱할 수 있다.

$$r(X) \cdot \mathbf{C} = (r(X) \cdot \mathbf{A}, r(X) \cdot \mathbf{B}) \bmod (X^N + 1) \bmod 1 \\ \in \mathbb{T}_N[X] \times \mathbb{T}_N[X].$$

[0038]

[0039] 그러면, 기대값(expectation) $\mathbb{E}[r(X) \cdot e] = 0$ 이기 때문에 $r(X) \cdot \mathbf{C}$ 는 $r(X) \cdot \mu(X)$ 를 암호화한다. 여전히, 에러는 $r(X)$ 에 의존하여 선형적으로 증가하고, 노이즈 증가는 LWE 암호문의 선형 합과 같다.

[0040]

TLWE 암호문 $\mathbf{C} \in \text{TLWE}_{\mathbf{K}}(\mu)$ 의 복호화는 $\mathbf{C}$, $\varphi_{\mathbf{K}}(\mathbf{C}) = \mathbf{B} - \mathbf{K} \cdot \mathbf{A}$ 의 상(phase)으로 정의된다. 복호화

결과는 작은 에러 $e \leftarrow \mathcal{X}$ 를 갖는 μ 의 근사값(approximation)이다. I. Chillotti 등의 논문(I. Chillotti, N. Gama, M. Georgieva, and M. Izabachene. TFHE: fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34-91, 2020.)에 따라, $\mathbb{E}[\mathcal{X}] = 0$ 를 취함에 따라 상(phase)의 기대값은 평문(Plaintext) μ 가 된다. $\text{msg}(\mathbf{C})$ 를 $\varphi_{\mathcal{K}}(\mathbf{C}) \in \mathbb{T}_N[X]$ 의 기대값으로, $\text{Err}(\mathbf{C})$ 를 $\varphi_{\mathcal{K}}(\mathbf{C}) - \text{msg}(\mathbf{C})$ 로 표시한다. 또한, $\text{Var}(\text{Err}(\mathbf{C}))$ 는 $\text{Err}(\mathbf{C})$ 의 분산(variance)으로, $\|\text{Err}(\mathbf{C})\|_{\infty}$ 를 $\text{Err}(\mathbf{C})$ 의 최대 크기(maximum amplitude)로 표시한다.

BlindRotate. 부트스트래핑(bootstrapping)은 BlindRotate가 담당하는 암호문에 대한 동형 복호를 포함한다. $\mathbf{c}$ 를 차원 $n \in \mathbb{N}$ 을 갖는 LWE 암호문 $\mathbf{c} = (\mathbf{a}_1, \dots, \mathbf{a}_n, \mathbf{b}) \in \text{LWE}_{\mathcal{R}}(\mu)$ 이라 하자. BlindRotate는 부트스트래핑 키(Bootstrapping key)를 이용하여 $\mathbf{c}$ 의 상만큼 동형적으로 테스트 다항식(test polynomial)을 회전시킨다. 테스트 다항식 $\nu = \nu_0 + \nu_1 X + \dots + \nu_{N-1} X^{N-1}$ 은 $\mathbb{T}_N[X]$ 에 포함되는 다항식이고, 테스트 다항식을 회전시키기 위해서는 상(phase)을 $\mathbb{Z}/2N\mathbb{Z}$ 로 이산화(discretization)하는 것이 요구된다. 이는 $\mathbf{c}$ 의 모든 계수들을 $\mathbb{Z}/2N\mathbb{Z}$ 로 이산화함으로써 완료된다.

$$\begin{aligned} \hat{\mathbf{a}}_i &= \lfloor 2N \cdot \mathbf{a}_i \rfloor \in \mathbb{Z}/2N\mathbb{Z} \text{ for } i \in \{1, \dots, n\} \text{ and} \\ \hat{\mathbf{b}} &= \lfloor 2N \cdot \mathbf{b} \rfloor \in \mathbb{Z}/2N\mathbb{Z}. \end{aligned}$$

$$\hat{\mu} = \hat{\mathbf{b}} - \sum_{i=1}^n \mathcal{R}_i \hat{\mathbf{a}}_i \pmod{2N}$$

이러한 근사화로 인하여 상은 이 된다.

BlindRotate는 TLWE 키 $\mathcal{K}$ 하에서 $X^{-\hat{\mu}} \cdot \nu$ 의 TLWE 암호문을 출력한다. 출력의 노이즈는 입력 암호문과는 무관하고, 외적(external product)으로부터 발생하는 고정된 분산(fixed variance)을 갖는다. 이는 SampleExtract 알고리즘을 이용하여 상수항(constant term)의 LWE 암호문을 간단하게 추출하는 것을 의미한다.

SampleExtract. 키 $\mathcal{K}$ 하에서 $\mu = \mu_0 + \dots + \mu_{N-1} X^{N-1}$ 의 TLWE 암호문 $\mathbf{C} = (\mathbf{A}, \mathbf{B})$ 를 고려하자. 키 $\mathcal{K} \in \mathbb{B}_N[X]$ 는 동일한 시퀀스의 계수들을 갖는 LWE 키 $\mathcal{K}' \in \mathbb{B}^N$ 로 볼 수도 있고, 그 역도 마찬가지다. 특정 포지션(specific position) $p \in [N]$ 가 주어진 경우, 키 $\mathcal{K}'$ 하에서 $\mu_p \in \mathbb{T}$ 의 LWE 암호문은 아래와 같이 N-항주기성 인덱스들(N-antiperiodic indices)을 갖도록 추출될 수 있다.

$$\begin{aligned} \text{SampleExtract}_p(\mathbf{C}) = \\ (\mathbf{A}_p, \mathbf{A}_{p-1}, \dots, \mathbf{A}_{p-N+1}, \mathbf{B}_p) \in \text{LWE}_{\mathcal{K}'}(\mu_p) \end{aligned}$$

SampleExtract_p는 추가적인 에러를 암호문에 부가하지 않고, 결과적인 암호문은 $\mathbf{C}$ 와 동일한 노이즈 크기 또는 분산을 갖는다.

KeySwitch. LWE 차원 N 을 갖는 $\mathbf{c} \in \text{LWE}_{\mathcal{K}}(\mu)$ 를 가정하자. 그러면, LWE 키 $\mathcal{R} \in \mathbb{B}^n$ 에 대해, 키스위치 키들(Keyswitch keys)은 아래와 같이 정의된다.

$$\text{KS}_{i,j,k} \in \text{LWE}_{\mathcal{R}} \left(\frac{\mathcal{K}_i}{B_{\text{KS}}^j} \cdot k \right)$$

여기서, $1 \leq i \leq N$, $1 \leq j \leq \ell_{\text{KS}}$, and $0 \leq k \leq B_{\text{KS}}$ 를 만족한다. 두 개의 파라미터들 B_{KS} 와 ℓ_{KS} 는 각각 디컴포지션 베이스(decomposition base)와 디컴포지션 렛스(decomposition length)를 정의한다. Keyswitching 알고리즘은 LWE 암호문 $\mathbf{C}$ 를 키 $\mathcal{R}$ 하에서 동일한 메시지를 암호화한 LWE 암호문으로 변환한다.

Bootstrapping. TFHE 내에서의 전체 부트스트래핑 과정은 입력 LWE 암호문에 대한 연속되는 알고리즘들을 실행하는 것을 포함한다.

[0052] **Bootstrap = Keyswitch ◦ SampleExtract ◦ BlindRotate**

[0053] 부트스트래핑 키(Bootstrapping key)와 키스위치 키(Keyswitch key)는 모두 부트스트래핑 과정에서, BlindRotate 알고리즘과 Keyswitch 알고리즘 내에서 각각 사용된다. 출력 LWE 암호문의 노이즈 분산은 사용되는 파라미터들에 의해 고정되고 용이하게 추정될 수 있다.

[0054] **C. Quantized Fourier Transform**

[0055] 길이가 N 인 임의의 이산 시간 신호(discrete time signal) $x[n]$ 에 대하여, DFT(Discrete Fourier Transform)은 $f = 0, \dots, N-1$ 에 대하여 다음과 같이 정의된다.

$$X[f] = \sum_{n=0}^{N-1} x[n] \cdot e^{-\frac{i2\pi}{N}fn}$$

$$= \sum_{n=0}^{N-1} x[n] \cdot \cos\left(\frac{2\pi}{N}fn\right) - i \sum_{n=0}^{N-1} x[n] \cdot \sin\left(\frac{2\pi}{N}fn\right)$$

[0056] 그러면, $X[f]$ 의 크기(amplitude)는 $f \in [0, N/2]$ 에 대하여 $fs \cdot f/N$ (fs 는 샘플링 주파수(sampling frequency)) Hz에서 스펙트럼 밀도(spectral density)를 나타낸다.

[0058] QFT(Quantized Fourier Transform)은 DFT의 변이체(variant)이다. J. Mason 등의 논문(J. Mason. Power spectra from approximate transforms. IEE Proceedings A-Physical Science, Measurement and Instrumentation, Management and Education-Reviews, 127(4):250-251, 1980.)에 따르면, QFT에서 모든 복소 지수 계수들(complex exponential coefficients) $\cos\left(\frac{2\pi}{N}fn\right)$ 와 $\sin\left(\frac{2\pi}{N}fn\right)$ 는 특정 레벨(예컨대, $\{\pm 1, 0\}$)로 양자화된다. 신호 처리 분야에서, 이러한 접근법은 근사 신호 처리(approximate signal processing)으로 알려져 있고, Nawab 등에 의해 소개되었다(S. H. Nawab, A. V. Oppenheim, A. P. Chandrakasan, J. M. Winograd, and J. T. Ludwig. Approximate signal processing. Journal of VLSI signal processing systems for signal, image and video technology, 15(1-2):177-300, 1997.). 근사화는 정확성(precision)과 리소스(resources) 간의 트레이드오프(tradeoff)를 포함한다.

[0059] 본 발명에서는 리소스를 절약하기 보다는 $\mathbb{T}_N[X]$ (i.e. $\mathbb{Z}_N[X]$ -module)의 대수적인 구조를 이용하여 암호화된 메시지에 대하여 DFT를 수행하는 QFT의 대안을 제시한다.

[0060] 이하에서는, 본 발명에 의한 푸리에 변환 기법을 소개한다.

[0061] 암호화된 데이터(시계열 데이터를 의미할 수 있고, 예시적으로 스피치 데이터일 수 있음)에 적용 가능한 동형 QFT(homomorphic QFT) 알고리즘을 소개한다. TFHE에 기초하여, 스피치 데이터에 대한 다항식 기반의 암호화와 다항식 곱셈(polynomial multiplications)을 이용한 동형 QFT를 제안한다. 또한, QFT의 출력 노이즈(output noise)를 처리하고 QFT 계수를 토러스 내로 근사화 시키는 기법을 제안한다. 본 발명에서, 사용자의 스피치 데이터의 요소는 $\mathbb{R}$ 에 속해 있음을 가정한다. 제안하는 기법에 대한 개략적인 모식도는 도 1에 도시되어 있다.

[0062] **A. 암호화(Encryption)**

[0063] 우선, 사용자(사용자의 단말로 이해될 수 있음)는 사용자의 비밀키(secret key)를 이용하여 클라우드 키(cloud key)를 생성한다. 이때, 사용자는 TFHE(TFHE: LWE, TLWE, 및 TGSW(TLWE와 TGSW는 동일한 키를 공유함)) 기법을 이용하기 위한 두 개의 키($\mathcal{R}$, $\mathcal{K}$)를 생성할 수 있다. 생성된 두 개의 키를 이용하여, 사용자는 부트스트래핑 키(Bootstrapping key)와 키스위치 키(Keyswitch key)를 생성한다. 부트스트래핑 키와 키스위치 키는 이후 임의의 시점에서 서버로 송신될 수 있다.

[0064] 다음으로, 사용자는 데이터(예컨대, 스피치 데이터)를 암호화하여 TLWE 암호문(ciphertext)을 생성한다. LWE 암호 대신에 TLWE 암호를 사용하는 주된 이유는, N 데이터를 단일의 TLWE 암호문에 패킹(packing)함으로써 리소스(resources)를 절약할 수 있기 때문이다. 패킹되는 데이터의 갯수 N 은 DFT를 위한 윈도우 사이즈(window size)로 해석될 수 있고, 윈도우 함수(window functions)은 암호화 과정에서 적용될 수 있다. TLWE 기법은 $\mathbb{T}_N[X]$

내의 다항식(polynomial)을 암호화하기 때문에, 스피치 데이터는 단일 스케일링 파라미터 $L \in \mathbb{Z}^+$ 을 갖는 구간(interval) $[-2^{-L}, 2^{-L}]$ 내로 정규화되어야 한다(normalized).

[0065] 스피치 데이터는 길이(length)가 N인 세그먼트들(segments)로 분할(분리, 또는 분절)되고 각 세그먼트들의 평균(mean)이 추출하여 각 세그먼트들로부터 DC 바이어스(DC bias)가 제거될 수 있다. 즉, 각 세그먼트의 값에서 평균을 차감하는 것으로 DC 바이어스는 제거될 수 있다. 각 세그먼트는 다항식 $\mu(X) = \sum_{i=0}^{N-1} \mu_i X^i \in \mathbb{T}_N[X]$ 로 해석될 수 있다. 여기서, 데이터 세그먼트의 각 원소(elements)는 토러스 다항식(torus polynomial)의 계수(coefficients)이다. 분절 이후에, 각 토러스 다항식 $\mu(X)$ 는 단일의 TLWE 암호문으로 암호화된다. N 보다 작은 길이의 데이터에 대한 암호화는 제로 패딩(zero padding)을 통해 가능하다. 즉, N보다 작은 길이의 데이터에는 뒷단에 0를 추가함으로써 길이가 N인 데이터로 변환될 수 있다.

[0066] 사용자는 TLWE 암호문을 공개키(public key)와 함께 서버로 송신할 수 있다. 암호화를 진행하는 동안 가우시안 노이즈(Gaussian noise)가 부가되기 때문에, 암호화된 신호의 SNR(signal-to-noise ratio)은 가우시안 노이즈의 분산과 L에 의존하여 감소할 수 있다.

[0067] B. 양자화(Fourier Basis Quantization)

[0068] 길이가 N인 이산 시간 신호(discrete time signal) $x[n]$ 에 대한 DFT는 다음 수학적 식 1과 같이 정의된다.

[0069] [수학적 식 1]

$$X[f] = \sum_{n=0}^{N-1} x[n] \cdot \cos\left(\frac{2\pi}{N}fn\right) - i \sum_{n=0}^{N-1} x[n] \cdot \sin\left(\frac{2\pi}{N}fn\right)$$

[0071] 상기 수학적 식에서, f는 0, ..., N-1의 값을 갖는다. 이하에서, $C_N(f, n)$ 과 $S_N(f, n)$ 을 각각 $\cos\left(\frac{2\pi}{N}fn\right)$ 과 $\sin\left(\frac{2\pi}{N}fn\right)$ 으로 나타낸다.

[0072] 우선, 수학적 식 1의 각 텀들(terms)은 두 개의 다항식의 곱들로 계산될 수 있다. $\left(\sum_{j=0}^{N-1} x[j]X^j\right) \left(\sum_{j=0}^{N-1} C_N(f, j)X^{N-1-j}\right)$ 과 $i \left(\sum_{j=0}^{N-1} x[j]X^j\right) \left(\sum_{j=0}^{N-1} S_N(f, j)X^{N-1-j}\right)$ 의 X^{N-1} 의 계수가 수학적 식 1의 제1 및 제2 텀임은 용이하게 증명될 수 있다. 다항식들 $\sum_j C_N(f, j)X^{N-1-j}$ 과 $\sum_j S_N(f, j)X^{N-1-j}$ 을 각각 $C_f(X)$ 과 $S_f(X)$ 으로 표시한다.

[0073] 사용자의 TLWE 암호문 $\mathbf{C} = (\mathbf{A}, \mathbf{B}) \in \text{TLWE}_{\mathcal{K}}(\mu(X))$ 에서, 서버는 $C_f(X)$ 과 $S_f(X)$ 에 대한 곱셈 연산을 바로 수행할 수 없다. 이는 $\mathbb{T}_N[X]$ 가 $\mathbb{R}_N[X]$ -module가 아닌 $\mathbb{Z}_N[X]$ -module이기 때문이다. 그러나, $C_f(X)$ 과 $S_f(X)$ 는 $\mathbb{R}_N[X]$ 내의 다항식들이다. 따라서, 계수들을 스케일링한 후 양자화(quantization)함으로써 이 다항식들을 $\mathbb{R}_N[X]$ 에서 $\mathbb{Z}_N[X]$ 로 매핑할 수 있다.

[0074] 따라서, 푸리에 기반 다항식에 대한 변환을 위해, 두 개의 파라미터들(K 및 Q, K와 Q는 모두 음이 아닌 정수)을 도입한다. QFT의 스케일링 파라미터(scaling parameter) K는 변환 후 푸리에 계수들의 범위 $[-2^{\frac{K}{2}}, 2^{\frac{K}{2}}]$ 를 결정한다. 반면에, 푸리에 양자화 파라미터(Fourier quantization parameter) Q는 양자화의 해상도(resolution)를 나타내고, $Q \leq K$ 를 만족하여야 한다. 알고리즘 1은 $(Q+1)$ 비트의 해상도를 갖는 양자화를 이용하여 푸리에 기반 다항식을 $\mathbb{Z}_N[X]$ 로 변환하는 변환 알고리즘을 나타낸다.

[0075] [알고리즘 1]

Algorithm 1: Conversion of the Fourier basis polynomial

Input: Fourier basis polynomial $F(X) = \sum_i F_i X^i \in \{C_f(X), S_f(X) \mid f \in [N]\}$, QFT scaling parameter K , Fourier quantization parameter Q .

Output: Quantized Fourier basis polynomial $\bar{F}_K(X) \in \mathbb{Z}_N[X]$ with $(Q+1)$ bits of resolution

- 1 For each $F_i \in \mathbb{R}$, set $\bar{F}_i$ as the closest multiple of $\frac{1}{2^Q}$ to F_i
 - 2 Compute $\bar{F}_{K,i} = \bar{F}_i \cdot 2^K$ where each $\bar{F}_{K,i} \in [-2^K, 2^K]$
 - 3 **return** $\bar{F}_K(X) = \sum_{i=0}^{N-1} \bar{F}_{K,i} X^i$
-

[0076]

[0077] 고정된 $K(K=5)$ 값에 대하여, $Q(Q=0, 1, 2)$ 의 값에 의존하는 계수들의 양자화는 도 2에 도시되어 있다. 이하에서는, 양자화된 변수들(quantized variables) 또는 양자화된 변수들이 사용되는 알고리즘의 출력을 나타내기 위해 서 바(upper bar)를 사용한다.

[0078] 알고리즘 1에서, 수학식 2는 용이하게 증명될 수 있다.

[0079] [수학식 2]

$$|2^K \cdot F_i - \bar{F}_{K,i}| \leq 2^{K-Q-1} \quad \forall i \in [N]$$

[0081] 예시적으로, 가능한 최대의 해상도(maximal resolution)을 얻기 위하여 K 와 같은 값을 갖는 Q 를 사용하였다.

[0082] C. 양자화된 푸리에 변환(QFT in Encrypted Domain)

[0083] 푸리에 기반 다항식들을 양자화된 정수 다항식들 $\bar{C}_{K,f}(X), \bar{S}_{K,f}(X) \in \mathbb{Z}_N[X]$ 로 변환한 후, 서버는 사용자의 암호화된 데이터 $\mu(X)$ 에 대한 QFT를 수행할 수 있다. $\bar{X}[f] = \bar{X}_C[f] - i\bar{X}_S[f] \approx 2^K \cdot X[f]$ 의 도출은 다항식에 대한 곱셈들을 포함한다. 첫번째로, 서버는 $\bar{C}_{K,f}(X) \cdot \mathbf{C}$ and $\bar{S}_{K,f}(X) \cdot \mathbf{C}$ 를 계산한다. 여기서, 다항식들은 암호문의 모든 다항식 원소들(every polynomial elements)에 곱하여 진다. 그런 다음, 서버는 결과 암호문들 각각에 $\text{SampleExtract}_{N-1}$ 를 적용한다. 이와같이 추출된 LWE 암호문들은 각각 키 $\mathcal{K} \in \mathbb{B}^N$ 하에서 $\bar{X}_C[f]$ 와 $\bar{X}_S[f]$ 에 대한 암호문이다. 알고리즘 2는 모든 QFT 과정을 나타낸다.

[0084] [알고리즘 2]

Algorithm 2: Quantized Fourier Transform on TLWE ciphertext

Input: TLWE ciphertext

$\mathbf{C} = (\mathbf{a}, \mathbf{b}) \in \text{TLWE}_{\mathcal{K}}(\mu(X))$, a set of quantized Fourier basis polynomials $\{\bar{C}_{K,f}(X), \bar{S}_{K,f}(X) \mid f \in [N]\}$

Output: $2N$ LWE ciphertexts $(\mathbf{c}_{f,i})_{f \in [N], i \in \{0,1\}}$ encrypting $\bar{X}_C[f]$'s and $\bar{X}_S[f]$'s under the key $\mathcal{K}'$

- 1 **for** $f \in [N], i \in \{0, 1\}$ **do**
 - 2 **if** $i = 0$ **then**
 - 3 $\bar{F}_K(X) = \bar{C}_{K,f}(X)$
 - 4 **else**
 - 5 $\bar{F}_K(X) = \bar{S}_{K,f}(X)$
 - 6 $\mathbf{C}_i = (\mathbf{a} \cdot \bar{F}_K(X), \mathbf{b} \cdot \bar{F}_K(X))$
 - 7 $\mathbf{c}_{f,i} = \text{SampleExtract}_{N-1}(\mathbf{C}_i)$
 - 8 **return** $(\mathbf{c}_{f,i})_{f \in [N], i \in \{0,1\}}$
-

[0085]

[0086] 도 3은 본 발명의 일 실시예에 따른, 동형암호 기반 (실수) 시계열 데이터의 암호화 및 이산 푸리에 변환 시스템을 도시하고, 도 4는 도 3에 도시된 시스템에서 수행되는 동형암호 기반 (실수) 시계열 데이터의 암호화 및 이산 푸리에 변환 방법을 설명하기 위한 흐름도이다.

- [0087] 도 1을 참조하면, 시스템(10)은 단말(100)과 서버(300)를 포함한다. 단말(100) 및/또는 서버(300)는 적어도 프로세서(processor) 및/또는 메모리(memory)를 포함하는 컴퓨팅 장치로 구현될 수 있다. 따라서, 동형암호 기반(실수) 시계열 데이터의 암호화 및 이산 푸리에 변환 방법은 단말(100)의 프로세서 및/또는 서버(300)의 프로세서에 의해 수행되는 것으로 이해될 수도 있다. 컴퓨팅 장치는 PC(Personal Computer), 랩탑 컴퓨터, 노트북 PC, 모바일 폰(mobile phone), 스마트 폰(smart phone), 두부 장착 장치(Head Mounted Device, HMD), 스마트 글라스(smart glasses), 스마트 watch(smart watch) 등을 포함할 수 있다.
- [0088] 단말(100)은 데이터(예컨대, 음성 데이터)를 수집하고, 수집된 데이터를 암호화하여 암호문을 생성할 수 있다(S110). 또한, 단말(100)은 생성된 암호문을 서버(300)로 송신할 수 있고(S130), 암호문에 대한 처리 결과(예컨대, 이산 푸리에 변환 결과)를 서버(300)로부터 수신할 수 있다(S170).
- [0089] 이를 위해, 단말(100)은 데이터 수집부, 전처리부, 암호화부, 송수신부, 및 저장부 중 적어도 하나를 포함할 수 있다.
- [0090] 데이터 수집부는 사용자의 음성 데이터를 수집할 수 있다. 이를 위해, 단말(100)에는 사용자의 음성 신호를 수신하기 위한 음성 인식 장치(예컨대, 마이크로폰)가 구비될 수 있다. 실시예에 따라, 데이터 수집부는 수집된(또는 수신된) 음성 신호를 디지털 신호로 변환할 수도 있다.
- [0091] 전처리부는 수신된 음성 데이터에 대한 전처리 동작을 수행할 수 있다. 전처리 동작은 음성 데이터를 미리 정해진 크기를 갖는 세그먼트들로 분할하는 과정, 각 세그먼트의 DC 바이어스를 제거하는 과정, 및 각 세그먼트에 포함된 데이터 값이 미리 정해진 범위를 갖도록 스케일링하는 정규화하는 과정 중 적어도 하나를 포함할 수 있다.
- [0092] 암호화부는 전처리부에 의해 전처리된 각 세그먼트를 암호화하여 암호문을 생성할 수 있다. 이때, 암호화부는(완전) 동형암호 기법 중 어느 하나를 이용하여 암호문을 생성할 수 있다.
- [0093] 송수신부는 생성된 암호문을 서버(300)로 송신하고, 이에 대한 응답으로 암호문에 대한 이산 푸리에 변환 결과를 수신할 수 있다.
- [0094] 저장부에는 단말(100)의 동작을 위한 각종 프로그램, 소프트웨어, 소스코드 등이 저장되어 있을 수 있다. 또한, 저장부에는 암호문을 생성하는 과정 중에 일시적으로 또는 비일시적으로 생성되는 데이터가 저장될 수 있다.
- [0095] 서버(300)는 단말(100)로부터 암호문을 수신하고, 수신된 암호문에 대한 이산 푸리에 변환을 수행(S150)한 후 수행 결과(이산 푸리에 변환 결과)를 단말(100)로 송신할 수 있다(S170).
- [0096] 이를 위해, 서버(300)는 데이터 수신부, 양자화부, 푸리에 변환부, 송신부, 및 저장부 중 적어도 하나를 포함할 수 있다.
- [0097] 데이터 수신부는 단말(100)로부터 암호문과 암호문에 대한 이산 푸리에 변환을 수행하는 과정에서 사용되는 데이터들을 수신할 수 있다.
- [0098] 양자화부는 푸리에 기반 다항식을 생성할 수 있다. 이때, 양자화부는 알고리즘 1을 이용하여 다항식을 생성할 수 있다.
- [0099] 푸리에 변환부는 단말(100)로부터 수신된 암호문에 대하여 이산 푸리에 변환을 수행할 수 있다. 이때, 푸리에 변환부는 알고리즘 2를 이용하여 이산 푸리에 변환 동작을 수행할 수 있다.
- [0100] 송신부는 이산 푸리에 변환의 결과를 단말(100)로 송신할 수 있다.
- [0101] 저장부에는 서버(300)의 동작을 위한 프로그램, 소프트웨어, 소스코드 등이 저장될 수 있다. 또한, 저장부에는 이산 푸리에 변환 과정 중에 일시적으로 또는 비일시적으로 생성되는 데이터가 저장될 수 있다.
- [0102] 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, 컨트롤러, 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 응

답하여, 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 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

[0103] 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.

[0104] 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.

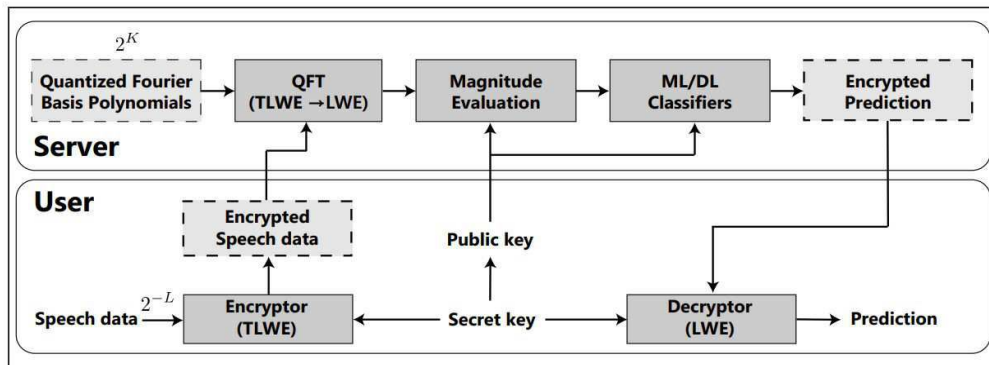
[0105] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성 요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

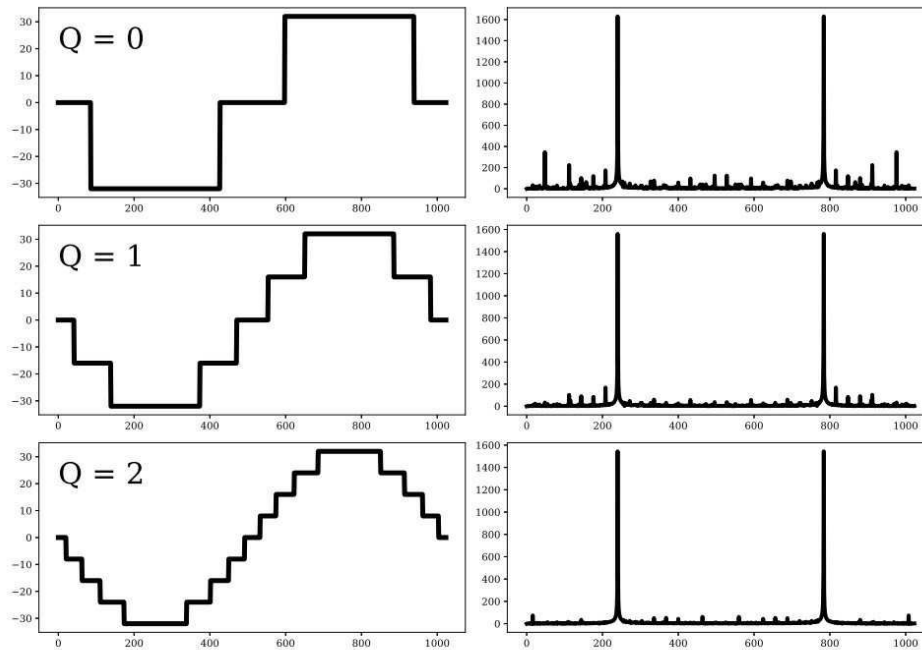
[0106] 10 : 시스템
100 : 단말
300 : 서버

도면

도면1

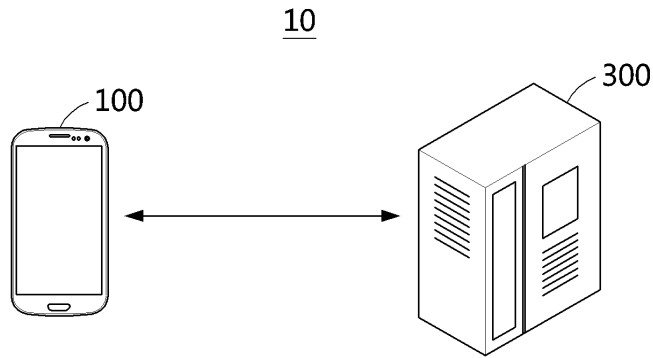


도면2



Quantization of Fourier basis for fixed $K = 5$ (left, $Q = 0, 1, 2$), and corresponding (absolute) results of QFT on a single sinusoidal wave (right)

도면3



도면4

