



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0075135
(43) 공개일자 2022년06월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2022.01) G06F 21/75 (2013.01)
(52) CPC특허분류
H04L 9/003 (2013.01)
G06F 21/755 (2020.05)
(21) 출원번호 10-2020-0163263
(22) 출원일자 2020년11월27일
심사청구일자 2020년11월27일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
윤지원
서울특별시 용산구 한강대로43길 8 102동 1401호
정지혁
서울특별시 광진구 능동로44길 31, 401호 (중곡동)
(뒷면에 계속)
(74) 대리인
제일특허법인(유)

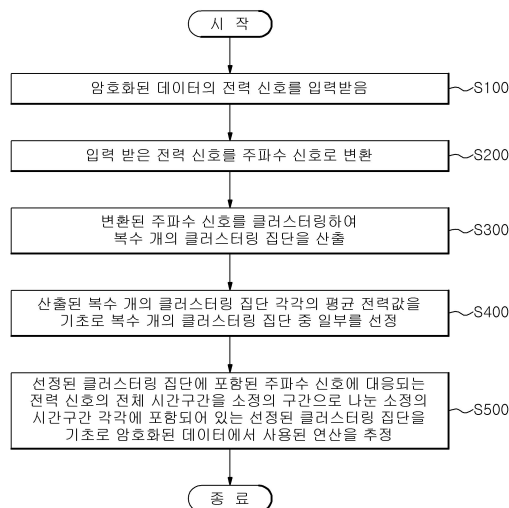
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 전력 분석 장치, 방법, 컴퓨터 판독 가능한 기록매체 및 컴퓨터 프로그램

(57) 요약

일 실시예에 따른 전력 분석 방법은, 전력 분석 장치에 의해 수행되는 암호화된 데이터의 전력 분석 방법에 있어서, 상기 암호화된 데이터의 전력 신호를 입력 받는 단계와, 상기 입력 받은 전력 신호를 주파수 신호로 변환하는 단계와, 상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 단계와, 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 단계와, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계를 포함할 수 있다.

대표도 - 도7



(52) CPC특허분류

H04L 2209/046 (2013.01)

(72) 발명자

한혜경

경기도 김포시 청송로 70 청송마을현대아파트 102
동 1501호

전영배

경기도 성남시 수정구 위례순환로 220 위례센트럴
푸르지오 5405동 902호

김현숙

대전광역시 유성구 북유성대로488번길 160

신임섭

대전광역시 유성구 북유성대로488번길 160

명세서

청구범위

청구항 1

전력 분석 장치에 의해 수행되는 암호화된 데이터의 전력 분석 방법에 있어서,
 상기 암호화된 데이터의 전력 신호를 입력 받는 단계와,
 상기 입력 받은 전력 신호를 주파수 신호로 변환하는 단계와,
 상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 단계와,
 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 단계와,
 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계를 포함하는
 전력 분석 방법.

청구항 2

제 1 항에 있어서,
 상기 주파수 신호로 변환하는 단계는,
 상기 입력 받은 전력 신호에 국소 푸리에 변환(STFT: Short-Time Fourier Transform)을 수행하여 상기 주파수 신호로 변환하는
 전력 분석 방법.

청구항 3

제 1 항에 있어서,
 상기 복수 개의 클러스터링 집단을 산출하는 단계는,
 K-평균 클러스터링(K-means Clustering) 알고리즘을 이용하여 상기 복수 개의 클러스터링 집단을 산출하는
 전력 분석 방법.

청구항 4

제 1 항에 있어서,
 상기 복수개의 클러스터링 집단 중 일부를 선정하는 단계는,
 상기 복수 개의 클러스터링 집단 중, 평균 전력값이 가장 높은 두 개의 클러스터링 집단을 선정하는
 전력 분석 방법.

청구항 5

제 1 항에 있어서,
 상기 암호화된 데이터에서 사용된 연산은,
 제곱(square) 연산 또는 곱셈(multiply) 연산을 포함하는
 전력 분석 방법.

청구항 6

제 5 항에 있어서,

상기 선정된 클러스터링 집단은,

제 1 클러스터링 집단 및 제 2 클러스터링 집단을 포함하고,

상기 암호화된 데이터에서 사용된 연산을 추정하는 단계는,

상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간구간에 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함될 경우 상기 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함될 경우 상기 제 1 클러스터링 집단이 사용되었다고 추정하고, 상기 전력신호의 소정의 시간구간에 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 상기 제 2 클러스터링 집단이 사용되었다고 추정하며,

상기 제 1 임계값은 상기 제 2 임계값보다 큰 값인

전력 분석 방법.

청구항 7

제 6 항에 있어서,

상기 암호화된 데이터에서 사용된 연산을 추정하는 단계는,

상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간구간에 상기 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함되고, 상기 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 상기 제 2 클러스터링 집단이 사용되었다고 추정하는,

전력 분석 방법.

청구항 8

암호화된 데이터의 전력 분석 장치에 있어서,

상기 암호화된 데이터의 전력 신호를 입력 받는 신호 입력부;

상기 입력 받은 전력 신호를 주파수 신호로 변환하는 주파수 신호 변환부;

상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 클러스터링부;

상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 선정부; 및

상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 추정부를 포함하는

전력 분석 장치.

청구항 9

제 8 항에 있어서,

상기 주파수 신호 변환부는,

상기 입력 받은 전력 신호에 국소 푸리에 변환(STFT: Short-Time Fourier Transform)을 수행하여 상기 주파수 신호로 변환하는

전력 분석 장치.

청구항 10

제 8 항에 있어서,

상기 클러스터링부는,

K-평균 클러스터링(K-means Clustering) 알고리즘을 이용하여 상기 복수 개의 클러스터링 집단을 산출하는 전력 분석 장치.

청구항 11

제 8 항에 있어서,

상기 선정부는,

상기 복수 개의 클러스터링 집단 중, 평균 전력값이 가장 높은 두 개의 클러스터링 집단을 선정하는 전력 분석 장치.

청구항 12

제 8 항에 있어서,

상기 암호화된 데이터에서 사용된 연산은,

제곱(square) 연산 또는 곱셈(multiply) 연산을 포함하는 전력 분석 장치.

청구항 13

제 12 항에 있어서,

상기 선정부에서 선정된 클러스터링 집단은,

제 1 클러스터링 집단 및 제 2 클러스터링 집단을 포함하고,

상기 추정부는,

상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간구간에 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함될 경우 상기 제곱 연산이 사용되었다고 추정하고, 상기 전력신호의 소정의 시간구간에 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 상기 곱셈 연산이 사용되었다고 추정하며,

상기 제 1 임계값은 상기 제 2 임계값보다 큰 값인

전력 분석 장치.

청구항 14

제 13 항에 있어서,

상기 추정부는,

상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간구간에 상기 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함되고, 상기 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 상기 제곱 연산이 사용되었다고 추정하는,

전력 분석 장치.

청구항 15

컴퓨터 프로그램을 저장하고 있는 컴퓨터 판독 가능 기록매체로서,

상기 컴퓨터 프로그램은, 프로세서에 의해 실행되면,

암호화된 데이터의 전력 신호를 입력 받는 단계와,

상기 입력 받은 전력 신호를 주파수 신호로 변환하는 단계와,

상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 단계와,
 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 단계와,
 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계를 포함하는 방법을 상기 프로세서가 수행하도록 하기 위한 명령어를 포함하는 컴퓨터 판독 가능한 기록매체.

청구항 16

컴퓨터 판독 가능한 기록매체에 저장되어 있는 컴퓨터 프로그램으로서,
 상기 컴퓨터 프로그램은, 프로세서에 의해 실행되면,
 암호화된 데이터의 전력 신호를 입력 받는 단계와,
 상기 입력 받은 전력 신호를 주파수 신호로 변환하는 단계와,
 상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 단계와,
 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 단계와,
 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계를 포함하는 방법을 상기 프로세서가 수행하도록 하기 위한 명령어를 포함하는 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 암호화 데이터의 전력 분석 장치, 방법, 컴퓨터 판독 가능한 기록매체 및 컴퓨터 프로그램에 관한 것이다.

배경 기술

[0002] 일반적으로 RSA(Rivest-Shamir-Adleman) 암호에서의 부채널 공격 중 SPA(Simple Power Analysis) 공격을 수행할 경우, 육안으로 RSA 암호 데이터에서 산출된 전력 파형의 패턴을 보고 RSA 암호에서 사용된 연산을 추정하고 있으나, 육안으로 암호화된 데이터의 연산을 추정하는 것은 정확도와 신뢰성이 떨어졌다.

[0003] 따라서, RSA(Rivest-Shamir-Adleman) 암호 데이터에서의 SPA(Simple Power Analysis) 공격을 자동화하여 암호 데이터에 사용된 연산 추정 결과의 정확성 및 신뢰성을 높이고, 암호 데이터에서 사용된 연산 추정 결과를 산출하는 속도를 빠르게 할 수 있는 알고리즘 기술을 필요로 하는 실정이다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 한국등록특허공보, 10-1135062호 (2012.04.03. 등록)

발명의 내용

해결하려는 과제

[0005] 본 발명의 해결하고자 하는 과제는, 전력 분석 장치, 방법, 컴퓨터 판독 가능한 기록매체 및 컴퓨터 프로그램을

제공하는 것이다.

[0006] 또한, 이러한 전력 분석 장치, 방법, 컴퓨터 판독 가능한 기록매체 및 컴퓨터 프로그램을 이용하여 자동으로 암호화 데이터의 전력을 분석하여 암호화 데이터에 사용된 연산을 추정하는 것 등이 본 발명의 해결하고자 하는 과제에 포함될 수 있다.

[0007] 다만, 본 발명의 해결하고자 하는 과제는 이상에서 언급한 것으로 제한되지 않으며, 언급되지 않은 또 다른 해결하고자 하는 과제는 아래의 기재로부터 본 발명이 속하는 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0008] 일 실시예에 따른 전력 분석 방법은, 전력 분석 장치에 의해 수행되는 암호화된 데이터의 전력 분석 방법에 있어서, 상기 암호화된 데이터의 전력 신호를 입력 받는 단계와, 상기 입력 받은 전력 신호를 주파수 신호로 변환하는 단계와, 상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 단계와, 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 단계와, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계를 포함할 수 있다.

[0009] 또한, 상기 주파수 신호로 변환하는 단계는, 상기 입력 받은 전력 신호에 국소 푸리에 변환(STFT: Short-Time Fourier Transform)을 수행하여 상기 주파수 신호로 변환할 수 있다.

[0010] 또한, 상기 복수 개의 클러스터링 집단을 산출하는 단계는, K-평균 클러스터링(K-means Clustering) 알고리즘을 이용하여 상기 복수 개의 클러스터링 집단을 산출할 수 있다.

[0011] 또한, 상기 복수개의 클러스터링 집단 중 일부를 선정하는 단계는, 상기 복수 개의 클러스터링 집단 중, 평균 전력값이 가장 높은 두 개의 클러스터링 집단을 선정할 수 있다.

[0012] 또한, 상기 암호화된 데이터에서 사용된 연산은, 제곱(square) 연산 또는 곱셈(multiply) 연산을 포함할 수 있다.

[0013] 또한, 상기 선정된 클러스터링 집단은, 제 1 클러스터링 집단 및 제 2 클러스터링 집단을 포함하고, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간구간에 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함될 경우 상기 제곱 연산이 사용되었다고 추정하고, 상기 전력신호의 소정의 시간구간에 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 곱셈 연산이 사용되었다고 추정하며, 상기 제 1 임계값은 상기 제 2 임계값보다 큰 값일 수 있다.

[0014] 또한, 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계는, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간구간에 상기 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함되고, 상기 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 상기 제곱 연산이 사용되었다고 추정할 수 있다.

[0015] 일 실시예에 따른 전력 분석 장치는, 암호화된 데이터의 전력 분석 장치에 있어서, 상기 암호화된 데이터의 전력 신호를 입력 받는 신호 입력부; 상기 입력 받은 전력 신호를 주파수 신호로 변환하는 주파수 신호 변환부; 상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 클러스터링부; 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 선정부; 및 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 추정부를 포함할 수 있다.

[0016] 또한, 상기 주파수 신호 변환부는, 상기 입력 받은 전력 신호에 국소 푸리에 변환(STFT: Short-Time Fourier Transform)을 수행하여 상기 주파수 신호로 변환할 수 있다.

[0017] 또한, 상기 클러스터링부는, K-평균 클러스터링(K-means Clustering) 알고리즘을 이용하여 상기 복수 개의 클러스터링 집단을 산출할 수 있다.

[0018] 또한, 상기 선정부는, 상기 복수 개의 클러스터링 집단 중, 평균 전력값이 가장 높은 두 개의 클러스터링 집단

을 선정할 수 있다.

[0019] 또한, 상기 암호화된 데이터에서 사용된 연산은, 제곱(square) 연산 또는 곱셈(multiply) 연산을 포함할 수 있다.

[0020] 또한, 상기 선정부에서 선정된 클러스터링 집단은, 제 1 클러스터링 집단 및 제 2 클러스터링 집단을 포함하고, 상기 추정부는, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간 구간에 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함될 경우 상기 제곱 연산이 사용되었다고 추정하고, 상기 전력신호의 소정의 시간구간에 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 상기 곱셈 연산이 사용되었다고 추정하며, 상기 제 1 임계값은 상기 제 2 임계값보다 큰 값일 수 있다.

[0021] 또한, 상기 추정부는, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 상기 소정의 시간구간에 상기 제 1 임계값 이상의 개수만큼 상기 제 1 클러스터링 집단이 포함되고, 상기 제 2 임계값 이상의 개수만큼 상기 제 2 클러스터링 집단이 포함될 경우 상기 제곱 연산이 사용되었다고 추정할 수 있다.

[0022] 일 실시예에 따른 컴퓨터 판독 가능한 기록매체는, 컴퓨터 프로그램을 저장하고 있는 컴퓨터 판독 가능 기록매체로서, 상기 컴퓨터 프로그램은, 프로세서에 의해 실행되면, 암호화된 데이터의 전력 신호를 입력 받는 단계와, 상기 입력 받은 전력 신호를 주파수 신호로 변환하는 단계와, 상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 단계와, 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 단계와, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계를 포함하는 방법을 상기 프로세서가 수행하도록 하기 위한 명령어를 포함할 수 있다.

[0023] 일 실시예에 따른 컴퓨터 프로그램은, 컴퓨터 판독 가능한 기록매체에 저장되어 있는 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은, 프로세서에 의해 실행되면, 암호화된 데이터의 전력 신호를 입력 받는 단계와, 상기 입력 받은 전력 신호를 주파수 신호로 변환하는 단계와, 상기 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출하는 단계와, 상기 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 상기 복수 개의 클러스터링 집단 중 일부를 선정하는 단계와, 상기 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함된 상기 선정된 클러스터링 집단을 기초로 상기 암호화된 데이터에서 사용된 연산을 추정하는 단계를 포함하는 방법을 상기 프로세서가 수행하도록 하기 위한 명령어를 포함할 수 있다.

발명의 효과

[0024] 일 실시예에 따르면, 전력 분석 장치를 이용하여 암호화된 데이터에서 사용된 연산 추정 결과를 자동으로 확인할 수 있기 때문에, 수동으로 암호화된 데이터의 전력을 분석하는 것보다 빠르게 암호화된 데이터의 연산 추정 결과를 획득할 수 있고, 암호 데이터에 사용된 연산 추정 결과의 정확성 및 신뢰성이 높아질 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시예에 따른 전력 분석 장치의 블록도이다.

도 2는 본 발명의 일 실시예에 따른 전력 분석 장치에서 입력 받은 암호화된 전력 신호의 파형이다.

도 3은 본 발명의 일 실시예에 따른 전력 분석 장치에서 변환된 주파수 신호의 파형이다.

도 4는 본 발명의 일 실시예에 따른 전력 분석 장치에서 클러스터링된 집단을 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따른 전력 분석 장치에서 클러스터링된 집단 중 선정된 클러스터링 집단을 설명하기 위한 도면이다.

도 6은 본 발명의 일 실시예에 따른 전력 분석 장치에서 변환된 주파수 신호에 대응되는 전력 신호의 파형이다.

도 7은 일 실시예에 따른 전력 분석 방법에 대한 예시적인 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로

다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

- [0027] 본 발명의 실시예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명의 실시예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0028] 도 1은 본 발명의 일 실시예에 따른 전력 분석 장치(100)의 블록도이고, 도 2는 본 발명의 일 실시예에 따른 전력 분석 장치에서 입력 받은 암호화된 전력 신호의 파형이고, 도 3은 본 발명의 일 실시예에 따른 전력 분석 장치에서 변환된 주파수 신호의 파형이고, 도 4는 본 발명의 일 실시예에 따른 전력 분석 장치에서 클러스터링된 집단을 설명하기 위한 도면이고, 도 5는 본 발명의 일 실시예에 따른 전력 분석 장치에서 클러스터링된 집단 중 선정된 클러스터링 집단을 설명하기 위한 도면이고, 도 6은 본 발명의 일 실시예에 따른 전력 분석 장치에서 변환된 주파수 신호에 대응되는 전력 신호의 파형이다.
- [0029] 도 1 내지 도 6을 참조하면, 본 발명의 일 실시예에 따른 전력 분석 장치(100)는 신호 입력부(110), 주파수 신호 변환부(120), 클러스터링부(130), 선정부(140) 및 추정부(150)를 포함할 수 있으나, 이에 한정되는 것은 아니다. 아울러, 이러한 전력 분석 장치(100) 및 이에 포함된 구성 각각은 소프트웨어 모듈이나 하드웨어 모듈 형태로 구현되거나 또는 소프트웨어 모듈과 하드웨어 모듈이 조합된 형태, 예컨대 컴퓨터나 스마트 기기 등에서 구현될 수 있고, 각각의 구성들은 전기적으로 연결될 수 있다.
- [0030] 신호 입력부(110)는 암호화된 데이터의 전력 신호를 입력받을 수 있다.
- [0031] 여기서, 신호 입력부(110)에서 입력 받은 암호화된 데이터는 RSA(Rivest-Shamir-Adleman) 암호 데이터의 복호화 과정에서 발생한 전력 신호일 수 있다.
- [0032] 이때, RSA(Rivest-Shamir-Adleman) 암호 데이터의 복호화 과정은 키(key)에 따라 연산이 수행될 수 있고, 연산의 종류에 따라 암호화 모듈의 전압이 달라지게 될 수 있다.
- [0033] 따라서, 신호 입력부(110)에서 입력받은 전력 신호는 도 2와 같이 암호화된 데이터의 부채널을 통해 발생하는 전력 파형이 암호화된 데이터의 연산구간마다 다르게 나타날 수 있다.
- [0034] 주파수 신호 변환부(120)는 신호 입력부(110)로부터 입력 받은 전력 신호를 주파수 신호로 변환할 수 있다.
- [0035] 예를 들어, 도 3과 같이 주파수 신호 변환부(120)는 신호 입력부(110)로부터 입력 받은 전력 신호에 국소 푸리에 변환(STFT: Short-Time Fourier Transform)을 수행하여 주파수 신호로 변환할 수 있다.
- [0036] 이때, 전력 분석 장치(100)는 신호 입력부(110)로부터 입력 받은 전력 신호를 주파수 신호로 변환함으로써, 암호화된 데이터의 주파수 신호를 이용하여 특징점을 산출할 수 있다.
- [0037] 클러스터링부(130)는 주파수 신호 변환부(120)로부터 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출할 수 있다.
- [0038] 예를 들어, 클러스터링부(130)는 K-평균 클러스터링(K-means Clustering) 알고리즘을 이용하여 주파수 신호 변환부(120)로부터 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출할 수 있다.
- [0039] 이때, 클러스터링부(130)는 도 4와 같이 총 4개의 클러스터링 집단이 산출될 수 있다.
- [0040] 예를 들어, 클러스터링부(130)는 전력 신호가 임계값 이하인 구간인 노이즈(noise) 집단으로서 산출되는 노이즈 클러스터링 집단, 암호화된 데이터의 연산이 수행된 후, 다시 연산이 수행되기까지의 대기 상태인 아이들(IDLE) 상태 집단으로서 산출되는 아이들(IDLE) 상태 클러스터링 집단, 암호화된 데이터에서 제곱(square) 연산이 수행되는 제 1 클러스터링 집단 및 암호화된 데이터에서 곱셈(multiply) 연산이 수행되는 제 2 클러스터링 집단을 산출할 수 있다.
- [0041] 선정부(140)는 클러스터링부(130)에서 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 복수 개의 클러스터링 집단 중 일부를 선정할 수 있다.
- [0042] 예를 들어, 선정부(140)는 도 5와 같이 클러스터링부(130)에서 산출된 복수 개의 클러스터링 집단 중, 평균 전력값이 가장 높은 두 개의 클러스터링 집단(예를 들어, 제 1 클러스터링 집단 및 제 2 클러스터링 집단)을 선정

할 수 있다.

- [0043] 추정부(150)는 선정부(140)에서 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 선정부(140)에서 선정된 클러스터링 집단을 기초로 암호화된 데이터에서 사용된 연산을 추정할 수 있다.
- [0044] 이때, 선정부(140)에서 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 소정의 시간구간은 선정된 클러스터링 집단에 기초하여 산출된 전력 신호의 시간구간이므로, 상기 소정의 시간구간 각각에는 반드시 제 1 클러스터링 집단 또는 제 2 클러스터링 집단이 하나 이상 포함될 수 있다.
- [0045] 여기서, 암호화된 데이터에서 사용된 연산은 제곱(square) 연산 또는 곱셈(multiply) 연산을 포함할 수 있다.
- [0046] 보다 상세하게, 추정부(150)는 선정부(140)에서 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 소정의 시간구간에 제 1 임계값 이상의 개수만큼 제 1 클러스터링 집단이 포함되어 있으면, 제곱 연산이 사용되어 있다고 추정하고, 상기 전력 신호의 소정의 시간구간에 제 2 임계값의 개수만큼 제 2 클러스터링 집단이 제 2 임계값 이상 포함되어 있으면 곱셈 연산이 사용되어 있다고 추정하며, 상기 전력신호의 소정의 시간구간에 제 1 임계값 이상의 개수만큼 제 1 클러스터링 집단이 포함되고, 제 2 임계값 이상의 개수만큼 제 2 클러스터링 집단이 포함될 경우에는 제곱 연산이 사용되었다고 추정할 수 있다.
- [0047] 여기서, 제 1 임계값은 제 2 임계값보다 큰 값을 가질 수 있다.
- [0048] 한편, 일 실시예로서 제 2 임계값은 “1”의 값을 가질 수 있으며, 이에 따라 추정부(150)는 선정부(140)에서 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 소정의 시간구간에 제 2 임계값 미만의 값을 가지는 제 2 클러스터링 집단이 발생되지 않기 때문에, 상기 소정의 시간구간에 제 2 임계값 미만의 제 2 클러스터링 집단이 발생하는 경우는 고려하지 않을 수 있다.
- [0049] 이때, 추정부(150)는 도 6과 같이, 선정부(140)에서 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 파형에서, 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간마다 연산을 추정할 수 있으며, 이때 도 6에서 녹색으로 표시된 부분은 암호화된 데이터에서 제곱 연산이 사용되었다고 추정하고, 빨간색으로 표시된 부분은 암호화된 데이터에서 곱셈 연산이 사용되었다고 추정할 수 있다.
- [0050] 더 나아가, 전력 분석 장치(100)는 DTW(Dynamic Time Warping) 알고리즘을 이용하여 추정부(150)에서 추정된 암호화된 데이터의 연산과 실제 암호화된 데이터의 연산과의 유사도를 평가할 수도 있다.
- [0051] 도 7은 일 실시예에 따른 전력 분석 방법에 대한 예시적인 흐름도이다. 도 7에 도시된 전력 분석 방법은 도 1에 도시된 전력 분석 장치(100)에 의해 수행 가능하다. 아울러, 도 7에 도시된 전력 분석 방법은 예시적인 것에 불과하다.
- [0052] 도 7을 참조하면, 신호 입력부(110)는 암호화된 데이터의 전력 신호를 입력받을 수 있다(단계 S100).
- [0053] 주파수 신호 변환부(120)는 신호 입력부(110)에서 입력 받은 전력 신호를 주파수 신호로 변환할 수 있다(단계 S200).
- [0054] 예를 들어, 주파수 신호 변환부(120)는 신호 입력부(110)에서 입력 받은 전력 신호에 국소 푸리에 변환(STFT: Short-Time Fourier Transform)을 수행하여 주파수 신호로 변환할 수 있다.
- [0055] 클러스터링부(130)는 주파수 신호 변환부(120)에서 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출할 수 있다(단계 S300).
- [0056] 예를 들어, 클러스터링부(130)는 K-평균 클러스터링(K-means Clustering) 알고리즘을 이용하여 주파수 신호 변환부(120)로부터 변환된 주파수 신호를 클러스터링하여 복수 개의 클러스터링 집단을 산출할 수 있다.
- [0057] 선정부(140)는 클러스터링부(130)로부터 산출된 복수 개의 클러스터링 집단 각각의 평균 전력값을 기초로 복수 개의 클러스터링 집단 중 일부를 선정할 수 있다(단계 S400).
- [0058] 보다 구체적으로, 선정부(140)는 클러스터링부(130)에서 산출된 복수 개의 클러스터링 집단 중, 평균 전력값이 가장 높은 두 개의 클러스터링 집단(제 1 클러스터링 집단 및 제 2 클러스터링 집단)을 선정할 수 있다.
- [0059] 추정부(150)는 선정부(140)에서 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 전체 시간구간을 소정의 구간으로 나눈 소정의 시간구간 각각에 포함되어 있는 상기 선정된 클러스터링 집단을 기초로

암호화된 데이터에서 사용된 연산을 추정할 수 있다(단계 S500).

[0060] 예를 들어, 추정부(150)는 선정부(140)에서 선정된 클러스터링 집단에 포함된 주파수 신호에 대응되는 전력 신호의 소정의 시간구간에 제 1 임계값 이상의 개수만큼 제 1 클러스터링 집단이 포함되어 있으면, 제곱 연산이 사용되어 있다고 추정하고, 상기 전력 신호의 소정의 시간구간에 제 2 임계값의 개수만큼 제 2 클러스터링 집단이 제 2 임계값 이상 포함되어 있으면 곱셈 연산이 사용되어 있다고 추정하며, 상기 전력신호의 소정의 시간구간에 제 1 임계값 이상의 개수만큼 제 1 클러스터링 집단이 포함되고, 제 2 임계값 이상의 개수만큼 제 2 클러스터링 집단이 포함될 경우에는 제곱 연산이 사용되었다고 추정할 수 있다.

[0061] 이상에서 살펴본 바와 같이, 일 실시예에 따르면, 전력 분석 장치를 이용하여 암호화된 데이터에서 사용된 연산 추정 결과를 자동으로 확인할 수 있기 때문에, 수동으로 암호화된 데이터의 전력을 분석하는 것보다 빠르게 암호화된 데이터의 연산 추정 결과를 획득할 수 있고, 암호 데이터에 사용된 연산 추정 결과의 정확성 및 신뢰성이 높아질 수 있다.

[0062] 본 발명에 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 인코딩 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 인코딩 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방법으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0063] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들 또는 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

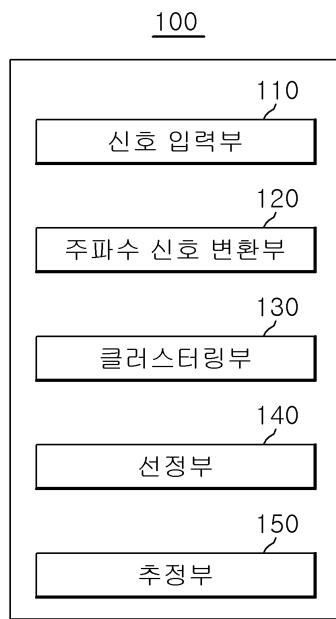
[0064] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 품질에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 균등한 범위 내에 있는 모든 기술사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

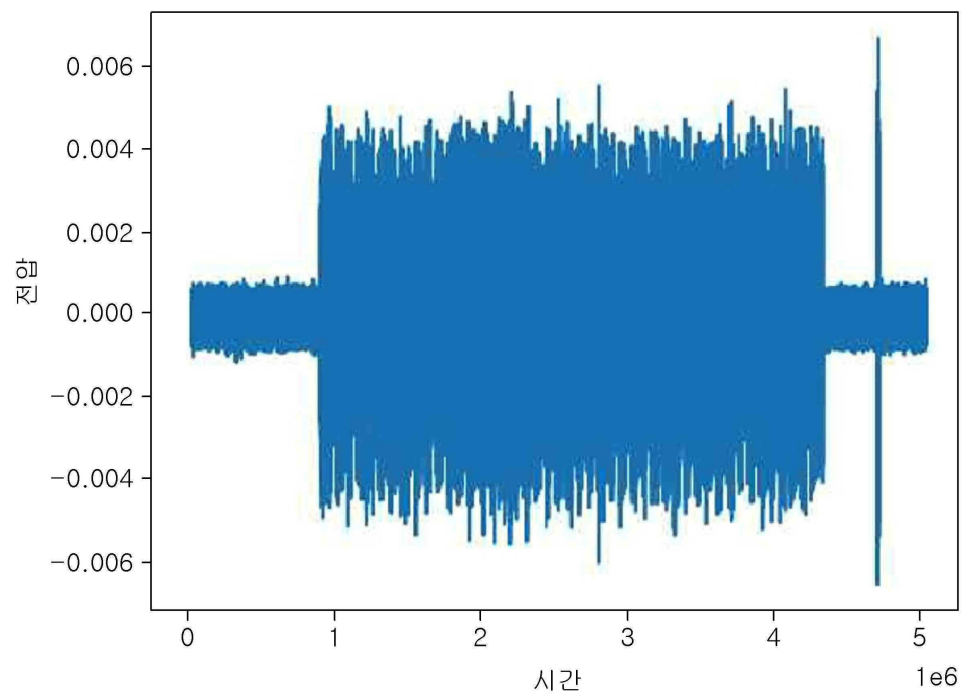
- [0065]
- 100: 전력 분석 장치
 - 110: 신호 입력부
 - 120: 주파수 신호 변환부
 - 130: 클러스터링부
 - 140: 선정부
 - 150: 추정부

도면

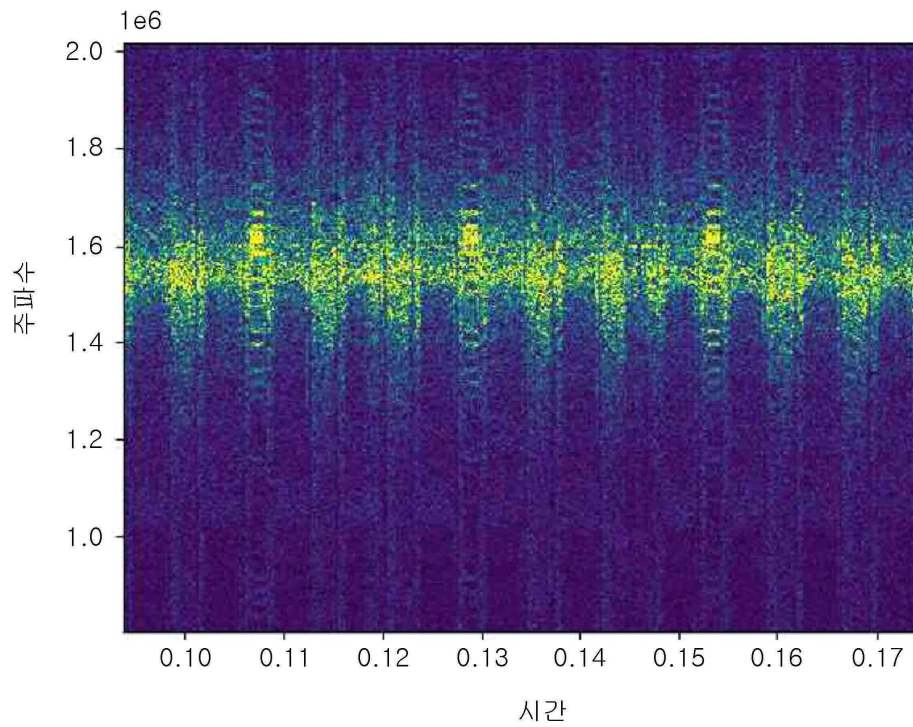
도면1



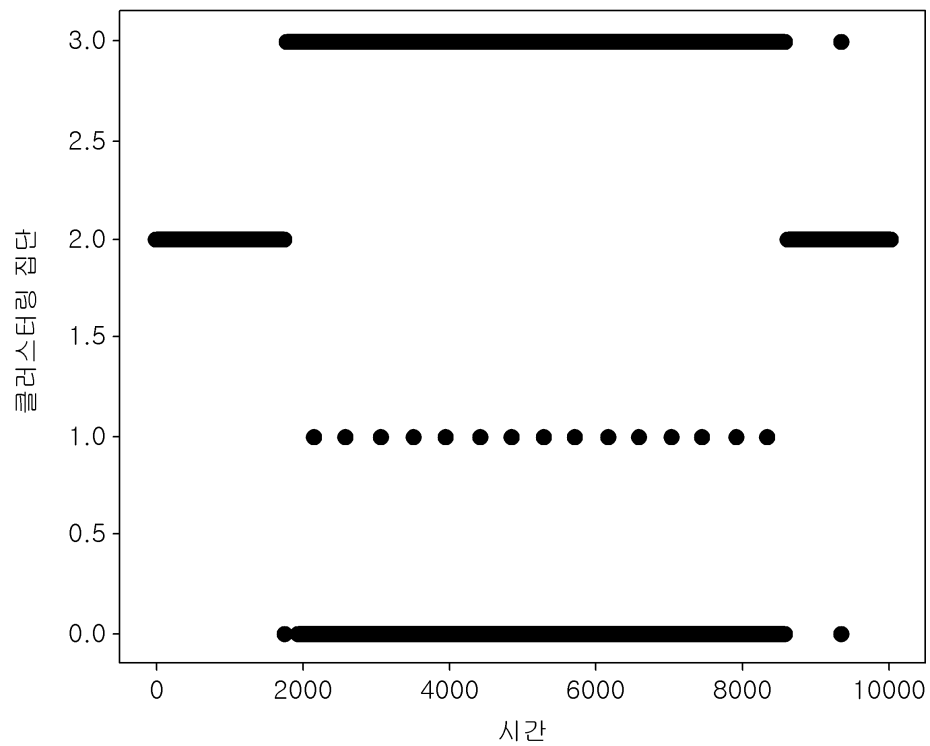
도면2



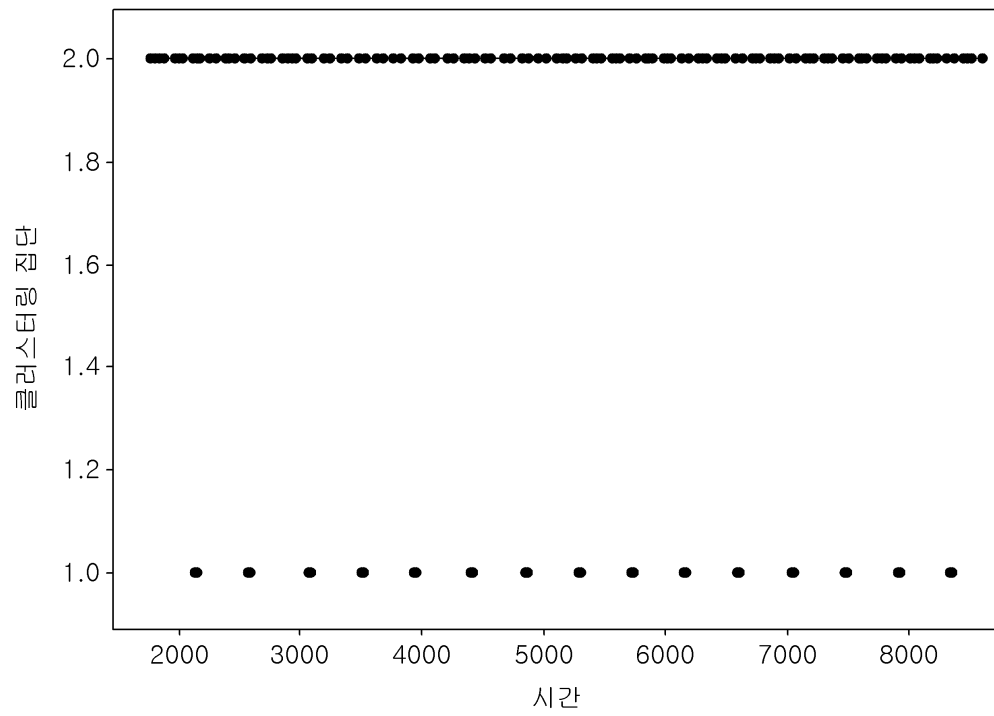
도면3



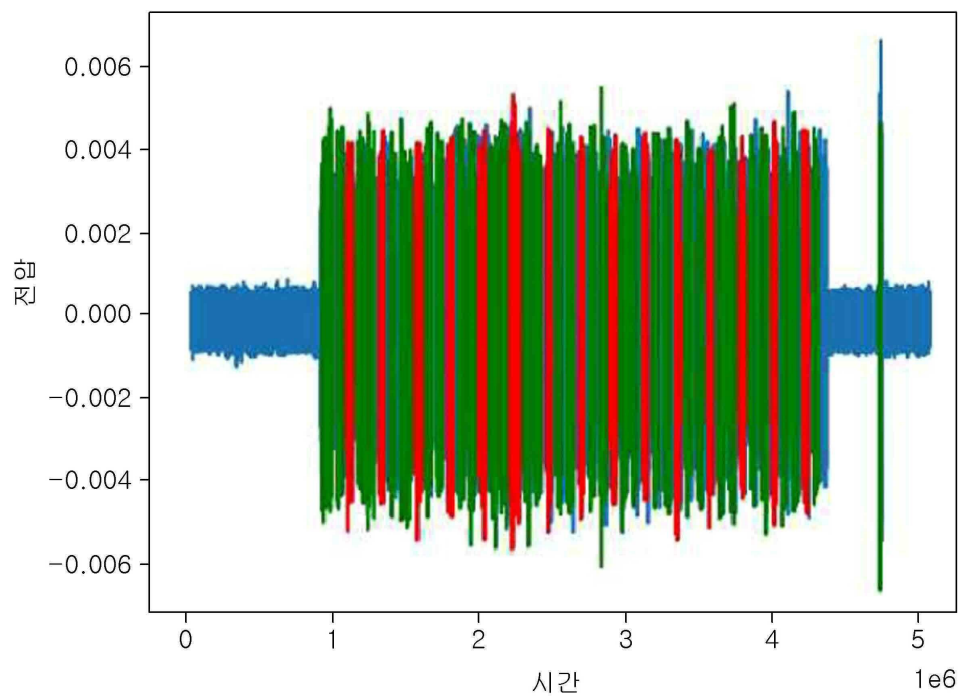
도면4



도면5



도면6



도면7

