Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.1, Feb. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.1.1

주파수 분석 기반 RSA 단순 전력 분석*

정 지 혁,[1†] 윤 지 원[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

Simple Power Analysis against RSA Based on Frequency Components*

Ji-hyuk Jung,[1†] Ji-Won Yoon[2‡]
[1,2]Korea University, School of Cyber Security(Graduate student, Professor)

요 약

본 논문은 RSA 복호화 과정에서 발생한 전력 신호로부터 암호연산을 예측하는 과정을 주파수 분석과 K-means 알고리즘을 이용하여 자동화하는 것을 제안한다. RSA 복호화 과정은 제곱 연산과 곱셈 연산으로 나뉘며, 시간에 따른 연산의 종류를 예측하게 되면, RSA 암호의 키(key)값을 알 수 있게 된다. 본 논문은 복호화 과정에서 발생한 전력 파형을 2차원 주파수 신호로 변환한 후, K-means algorithm을 이용하여 연산의 종류에 따라 주파수 벡터를 분류하였다. 이후, 이러한 분류된 주파수 벡터를 이용하여 연산의 종류를 예측한다.

ABSTRACT

This paper proposes to automate the process of predicting crypto-operations from the power signal generated in RSA decoding process by frequency analysis and K-means algorithm. RSA decoding process is divided into square and multiply operation, and if we can predict the type of operations over time, we will know the RSA key value. After converting the power signal generated in the process of decoding into two-dimensional frequency signal, this paper used K-means algorithm to classify the frequency vector according to the type of operation. these classified frequency vector were used to predict the types of operations.

Keywords: RSA, Side Channel Analysis, Automate, K-means

I. 서 론

부채널 분석은 암호 장치 내부에서 연산하는 과정 동안 나오는 전력이나 전자기파와 같은 물리적인 신호를 수집하여 암호의 연산 종류나 비밀키 등을 예측하는 기법이다. 암호 알고리즘에 따라 다양한 부채널 분석 기법이 소개되었고, 대표적으로 Correlation Power Analysis (CPA), Differential Power Analysis (DPA), Simple Power Analysis (SPA) 등이 있다[1-4]. CPA나 DPA의 경우 해밍 무게(Hamming weight)와 전력 소비 모델에 기반하여, 측정된 전력 값과 연산값 사이의 수학적인 선형 관계에 따라 추정하기 때문에 답이 명확한 분석 기법들이 잘 알려져 있는 반면에, SPA는 연산의 시계열 패턴을 보고 그 시간에 어떠한 연산이 일어났는지를 구분하여야 하기 때문에 더 복잡하고 정교한 추론 기법이 필요하다. 일례로 가장 보편적으로 이용되는 공개키 암호 알고리즘인 RSA 암호에서 제곱(Square) 연산과 곱셈(Multiply) 연산에서 유출되는 전력 신호 패턴이 다르다는 것을 이용하여 (SPA) 제곱 연산과 곱셈 연산을 유추한 후, 해당하는 이진수로 변환하여 복호화 키를 추출하였다

Received(10. 07. 2020), Modified(1st: 11. 23. 2020 2nd: 01. 11. 2021), Accepted(01. 12. 2021)
* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한. 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.
† 주저자, graycat@korea.ac.kr
‡ 교신저자, jiwon_yoon@korea.ac.kr(Corresponding author)

[1-2]. 기존 SPA에서 분석가들은 눈으로 전력 패턴을 분석하여 실제 일어난 연산을 유추하며 이를 기반으로 숨겨져 있는 키 값을 추정하였다. 최근에는 많은 데이터를 분석하여야 하기 때문에 이를 자동화하는 방안이 강구되며, 부채널 분석을 머신러닝 기법을 통해 접근하는 연구들이 많이 진행되었다[3-5]. 특히, [5]에서는 RSA의 SPA 과정을 확률 모델링을 통해 자동화하여 분석하였다. 본 논문은 [5]에서 해결하고자 하는 문제를 다른 방식으로 접근하여 RSA의 SPA를 자동화하는 방법을 제안한다.

[5]의 SPA 분석 기법은 전력의 크기를 주된 특징(feature)으로 이용하기 때문에 많은 전처리와 후처리 과정이 필요하였다. 특히 연산의 분절점의 위치를 추정하는 과정에서, 1차원의 전력 데이터만을 주된 특징으로 사용하다 보니 Markov Chain Monte Carlo (MCMC)와 같은 많은 경우의 수를 고려하여야 하는 무거운 알고리즘이 필요하였다. 본 논문은 RSA 연산 과정에서 추출된 전력 파형을 주파수 영역으로 변환하여 신호의 전처리와 후처리를 간단히 하였으며, 전력의 주파수 분포를 MCMC에 비해 가벼운 K-means 알고리즘을 통해 연산의 예측(SPA)을 자동화할 수 있음을 보인다. 전력 파형을 주파수 영역으로 변환하기 위해 시간에 따른 주파수 신호로 변환해주는 Short-Time Fourier Transform(STFT)를 이용한다. 이후, STFT로 변환된 주파수 신호의 각 시간에서 연산에 따른 잠재된 특성에 따라 분류하기 위해 K-means 기법을 이용하였으며, 분류된 특성을 연산 단위로 분리하여 각 연산을 추정하였다. 고차원의 특징을 이용하여 분류함으로써 우리는 기존 논문[5]보다 전처리와 후처리 과정을 줄였으며, 샘플링 기반의 알고리즘을 사용하지 않아 훨씬 빠른 분석 성능을 나타내었다.

II. Background

Textbook RSA 암호화 과정을 수식으로 나타내면 다음과 같다.

$$C = P^e \bmod N \quad (1)$$

$$P = C^d \bmod N \quad (2)$$

위 수식에서 C는 암호문이며, P는 평문을 의미한다. e, N은 공개키, d는 비밀키를 의미한다. 식 (1)은 RSA의 암호화 과정을 나타내며, 평문 P를 공개키 e로 제곱하여 N으로 모듈러 연산을 취하는 과정이다. 식 (2)는 복호화 과정으로 평문 P를 구하기 위해 암호문 C를 비밀키 d를 제곱한 후, N으로 모듈러 연산을 하는 과정이다. 이때, 계산과정의 효율성을 위해, Modular Exponentiation 방법을 이용한다. n bit의 비밀키 d에 대하여, 복호화 과정은 다음과 같다.

부채널 분석을 통한 RSA 암호에서의 키 예측에서는 위 Modular Exponentiation 과정에서 발생하는 전력 파형을 이용한다. Modular Exponentiation 과정에서 키 값 d에 따라, 제곱 연산과 곱셈 연산이 결정된다. 따라서, 부채널을 통해 발생하는 전력 파형을 통해 시간에 따른 연산의 종류를 추정하면 키 값 d를 알 수 있는 것이다.

Modular Exponentiation

input:C,n,d=$(b_{n-1}...b_1b_0)$ output:$P = C^d \bmod N$
P=1 k=n-1 for k → n-1 to 0: P = P*P mod N square operation if(b_k == 1): P= C*P mod N multiply operation

III. Proposed method

본 논문은 RSA 암호화 과정에서 발생한 전력 신호를 이용하여 어떠한 연산이 진행되었는지 추정하여 암호키를 추정하는 기법을 제안한다. Fig. 1.은 전체 추정 알고리즘을 요약한 순서도이다. 우선, 1차원 전력 신호의 주파수 특징을 추출하기 위해 전력 파형을 STFT를 이용하여 시간에 따른 주파수 신호로 변환한다(3.1절).

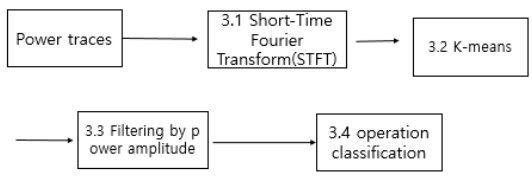


Fig. 1. Algorithm flow chart

변환된 각 시간 구간마다 주파수 신호를 K-means를 이용하여 군집화(Clustering)하였다(3.2 절). 전력 사용량을 이용하여 군집의 종류를 알아내었다(3.3 절). 마지막으로 각 단위 파형의 연산을 추정하였다(3.4절). Fig. 2.은 본 논문에서 이용한 전력 파형을 나타낸 것이다. 전력 파형은 1차원 신호로 시간 T까지의 신호를 $P_{1:T}$로 나타낼 것이며, 시간 t에서의 값을 $P[t]$로 나타내기로 한다.

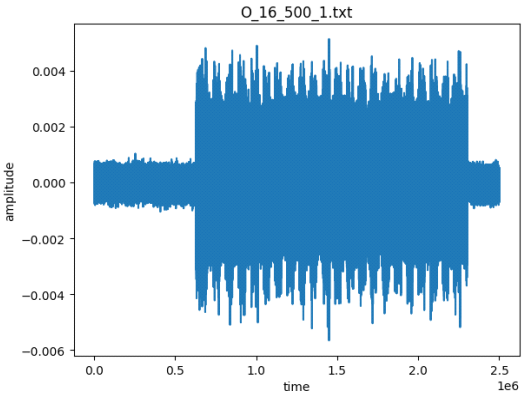


Fig. 2. A single power trace.

3.1 Short-Time Fourier Transform

본 논문은 전력 파형에서 연산에 따른 전압 크기의 변화를 잘 잡아내기 위해서 주파수 신호를 특징으로 이용하기로 하였다. STFT란 시간에 따른 주파수 분포를 구하기 위해 전체 신호를 구간으로 나누어, 각 구간의 1차원 시간 신호를 주파수 영역으로 변환하는 기법이다. 이를 수식으로 표현하면 다음과 같다.

$$F(m,k) = \sum_{t=0}^{T} P[t]w[t-mL]e^{-j\frac{2\pi}{N}kt} \quad (3)$$

$$w[t] = \begin{cases} 1, & 0 \le t \le T \\ 0, & T < t \end{cases} \quad (4)$$

$F(m,k)$는 m번째 프레임(시간)의 k번째의 주파수 값이며, T는 프레임의 길이이며, L은 프레임 사이의 거리이다. n과 N은 각각 시간과 전체 신호의 길이를 의미한다. $w(t)$는 프레임의 윈도우 함수이다.

Fig. 4.는 전력 파형 P와 2차원 신호로 변환된 $F(m,k)$을 스펙트럼으로 나타낸 것이다. 스펙트럼

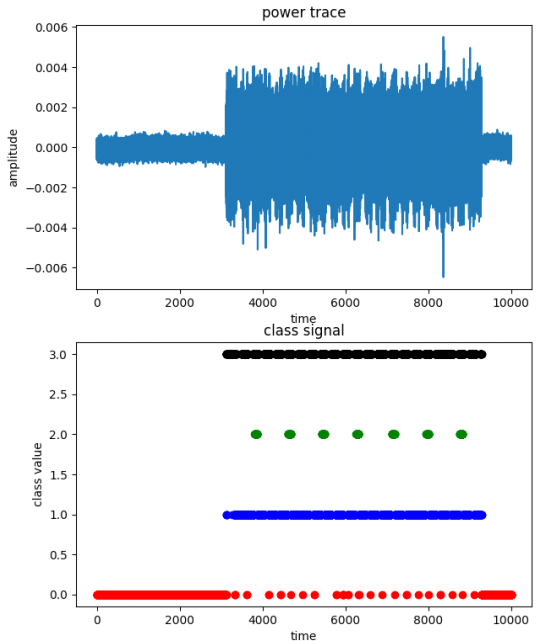


Fig. 3. Class signal in which a single power trace is classified into 4 classes.

상에서는 시간에 따라 전력의 크기가 큰 부분과 작은 부분이 반복되어 나타나는 것을 볼 수 있었으며, 전력이 큰 부분에서 패턴이 2가지로 나뉘는 것을 볼 수 있었다. 스펙트럼 상에서 육안으로 관찰한 패턴 2가지를 초록색 상자와 빨간색 상자로 표시하였으며, 이것은 전력 파형에서 육안으로 관찰한 연산의 패턴 위치와 비슷한 것을 볼 수 있다. 따라서, 주파수 영역에서 나타나는 패턴을 분류하면 각 시간이 어떤 연산에 속하는지 알 수 있을 것이다.

3.2 K-means algorithm

앞선 단계에서 전력 신호를 주파수 신호로 변환하였을 때, 전력이 큰 부분에서 연산의 패턴이 관찰되었다. 따라서, 본 논문에서는 수집된 전력 파형은 복호화 과정 전의 노이즈(noise) 부분과 복호화 과정 중의 연산 진행 중 사용 전력량이 낮은 부분(Idle)과, 제곱 연산에서 전력량이 큰 부분(square), 곱셈 연산에서 전력량이 큰 부분(multiply) 즉 총 네 부분으로 나누어진다고 가정한다. 기존 논문[5]은 전력 파형의 복호화 과정 부분에서만 실험을 진행하였으며, 복호화 과정을 Square, Multiply, Idle period 부분으로 나누었다, 이는 본 논문과 같다. 특정

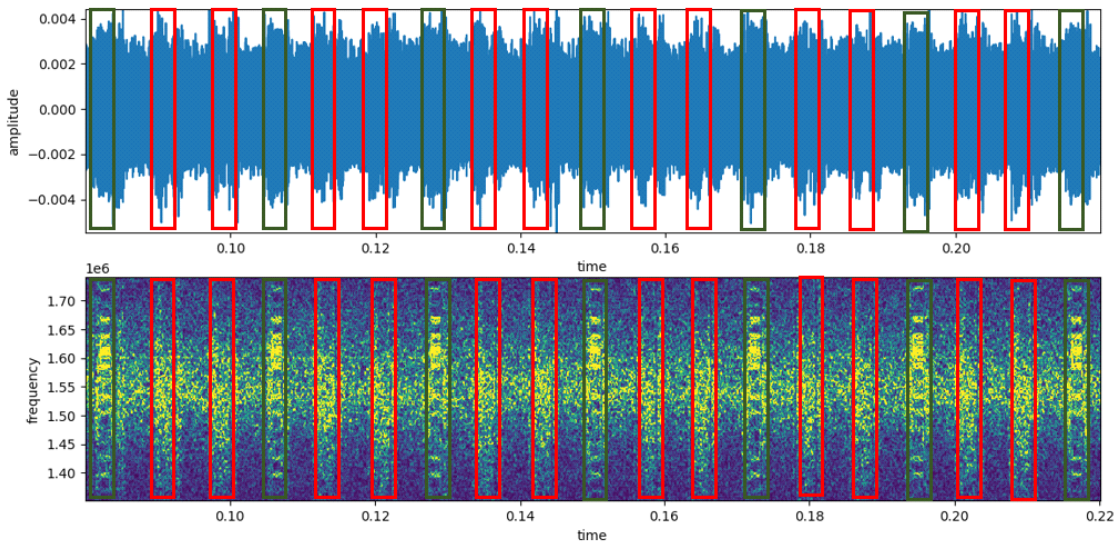


Fig. 4. Power trace and frequency spectrum. Green and Red square box are features of the operation observed with the naked eye.

시간에서의 주파수 분포들의 잠재된 특성을 분류하기 위해 본 논문은 K-means를 이용한다. K-means는 하이퍼파라미터(hyperparameter) K(군집수)가 정해지면, 이를 데이터의 잠재된 특성에 따라 K개의 군집으로 분류하는 기법이다[6]. K-means는 군집으로 분류된 데이터와의 거리의 합을 최소화하는 각 군집의 중심의 해를 구하는 것이다. 이러한 해를 구하기 위해, 초기 단계에는 각 군집의 중심을 임의로 정한다. 이후, 각 군집의 중심에 가장 가까운 것에 따라 데이터를 군집에 할당한다(Expectation 단계). 이후, 각 군집으로 분류된 데이터들의 평균을 군집의 중심으로 정한다. (Maximization 단계) 이러한 과정을 각 군집의 중심과 군집에 속하는 데이터와의 거리의 합이 미리 정한 기준치의 값보다 작아질 때까지 진행한다. 본 논문은 RSA 복호화 과정에서 추출한 전력 스펙트럼에서 각 시간의 주파수 분포를 4 종류로 분류할 것이므로 K를 4로 놓는다. 이러한 과정을 식으로 나타내면 다음과 같다. 모든 프레임 m에서 주파수 분포는 다음과 같은 벡터로 표현할 수 있다.

$$x_m = [F(m,0), F(m,2) \ldots F(m,[L/2])] \tag{5}$$

본 실험의 프레임 m에서의 주파수 분포 x_m을 4개의 클래스로 분류하는 과정은 식 (6)과 식 (7)을 만족하는 K(4)개의 배반집합 C_i를 찾는 것을 의미한다. c_i는 클래스 C_i에 속한 전체 벡터의 평균값(중심)이다.

$$X = \{x_1, x_2 \ldots x_M\} = C_1 \cup C_2 \cup \ldots C_k \tag{6}$$

$$\operatorname{argmin}_{C_1, C_2 \ldots C_k} \sum_{i=1}^{K} \sum_{x_j \in C_i} \| x_j - c_i \|^2 \tag{7}$$

스펙트럼 신호의 각 프레임은 한 개의 클래스로 분류되며, 각 주파수 분포를 클래스에 해당하는 수로 할당하여 스펙트럼은 1차원 신호로 변환할 수 있다. 스펙트럼 신호 $(x_1, x_2 \ldots x_M)$을 K-means를 통해 클래스 신호로 변환된다. x_j가 분류된 클래스의 할당된 값을 $C(x_j)$라하면, 시간에 따른 1차원 신호를 만들 수 있으며, 본 논문에서는 이를 클래스 신호라 할 것이다. 클래스 신호는 $(C(x_1), C(x_2), \ldots, C(x_M))$로 표현할 수 있으며, Fig. 3.은 전력 파형이 클래스 신호로 변환된 것을 보여준다.

3.3 Filtering by power amplitude

각 시간의 주파수 벡터를 4개의 클래스로 분류하였지만, 각 클래스가 어떠한 부분인지는 알 수 없다. 가장 간단한 방법은 4개의 클래스가 어떠한 종류(노이즈, 제곱 연산, 곱셈 연산, 전력 값이 낮은 부분)에 해당하는지에 대한 모든 경우의 수(4!) 결과를 예측한 후, RSA 암호의 패턴과 비교하여 최적의 결과를 나타내는 것을 찾아내면 된다. 하지만, 본 논문은 연산의 특징 부분이 전력을 많이 사용한다는 성질을 이용함으로써 4개의 클래스 중 평균 전력 값이 큰 두 개의 신호들을 추출하였다. 이를 통해, 4개의 클래스중에 연산 부분에 해당하는 부분을 찾아낼 수 있었다. 또한, RSA 복호화 과정은 제곱 연산이 곱셈 연산보다 많이 나타나기 때문에 추출된 두 개의 신호 중에서 더 빈번하게 관측되는 부분이 제곱 연산임을 추정할 수 있다. 이와 같은 추론 과정을 통해, 본 논문에서는 모든 경우의 수를 고려하지 않아도 바로 분류된 클래스 값이 어떠한 연산의 특징에 해당하는지 추정하였다. 전력 값에 의해 필터링 된 클래스 신호에서 우리는 연산 단위로 분리하여야 전력 파형에 해당하는 연산을 알아낼 수 있다. 본 실험에서는 연산 중간에 발생하는 전력량이 낮은 부분을 경계로 하여 연산을 구분하였다. 실험에서 연산특징을 분리하는 구간은 전력량이 낮은(Idle) 부분이 지속되는 구간으로 다음과 같이 정의하였다. 구간 [a,b]에 속하는 모든 m에 대하여, $C(x_m)$가 전력량이 낮은 부분의 클래스값이라면, 구간 [a,b]를 연산의 특징을 분리하는 구간이라 보았다. 하지만, K-means를 이용한 주파수 벡터의 군집화는 연산 내에 주파수 성질이 계속 일정하게 유지되어 완벽하게 분리되는 것이 아니기 때문에, 연산 특징 내부에서도 전력 값이 낮은 구간들이 존재한다. 이러한 것들은 연산특징을 분리하는 구간이 아니다. 따라서, 연산을 나누는 구간의 길이는 일정한 값 중심으로 분포할 것이며, 이러한 중심으로 모여있는 분포를 찾으면 될 것이다. 본 논문에서는 이를 위해 Kernel Density Estimation (KDE)를 이용하여 이러한 구간들을 찾아내었다. 연산과 연산 사이의 발생한 전력이 작은 부분의 구간 길이들을 KDE를 이용하여 확률분포로 변환하였으며, 확률분포의 피크 값을 중심으로 구간들을 나눌 수 있었다. 이들 중에 연산을 분리하는 구간이 분포하는 클러스터가 있을 것이다. 연산을 분리하는 구간의 개수는 연산의 개수와 같게 되며, n 비트

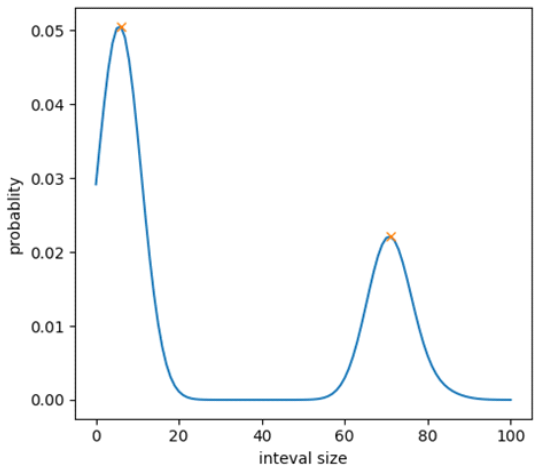


Fig. 5. Probability distribution of the interval using KDE

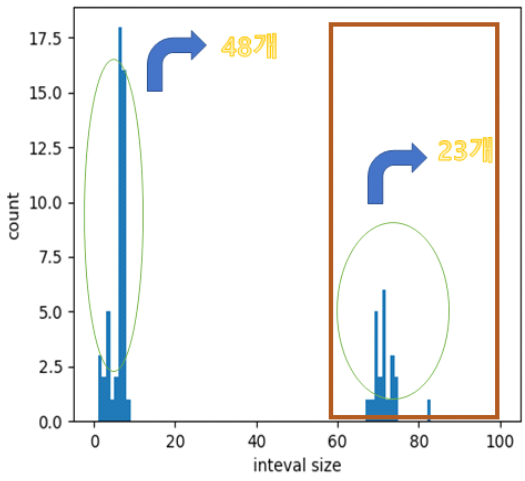
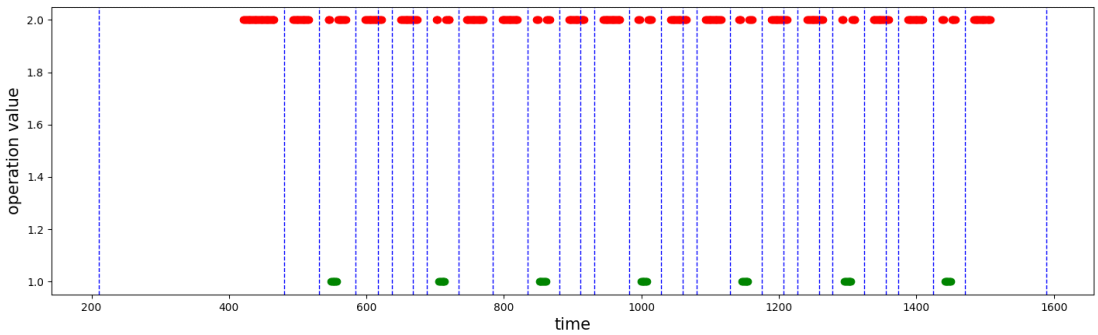
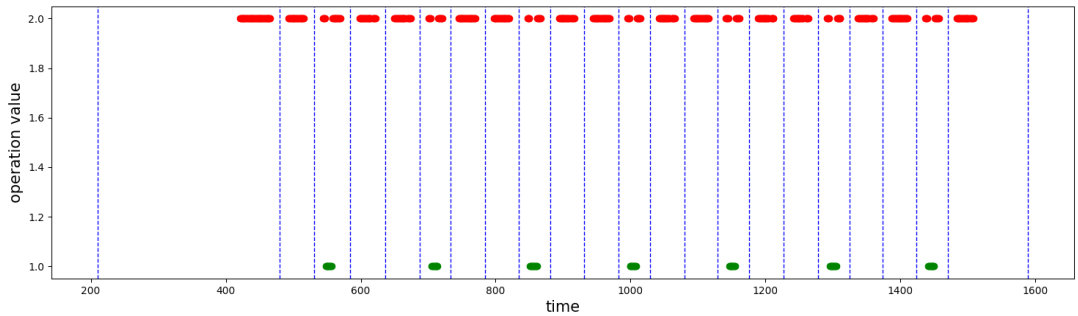


Fig. 6. Distribution of intervals at peak points

의 RSA 암호의 경우 제곱과 곱셈 연산의 총 개수는 최소 n개에서 최대 2n개이다. 따라서, 연산을 분리하는 군집에 해당되는 구간들의 개수가 n~2n개에 가까운 것이 연산을 분리하는 클러스터일 것이라 추정할 수 있다. 우리는 이를 이용해 연산을 분리하는 구간의 클러스터를 찾을 수 있었으며, 클러스터에 해당하는 구간만을 이용하여 연산을 분리하였다. Fig. 5.는 각 구간들의 분포를 이용하여, 확률분포를 구한 것이며, Fig. 6.은 각 피크 클러스터에서 구간의 개수를 나타낸 것이다. Fig. 6.에서 사용한 데이터는 16비트 RSA이며, 따라서, 연산의 개수는 16~32개일 것이다. 16과 32개의 중간값인 24에 가장 가까



(a) a result of separating calculation characteristics using all intervals.



(b) a result of separating calculation characteristics using intervals filtered.

Fig. 7. Comparison a result without and with filtering.

운 개수가 모여있는 60과 80사이의 피크 클러스터가 연산특징을 분리하는 구간의 클러스터가 된다. 따라서, 이들 구간만을 이용하여 연산을 분리한다. Fig. 7.은 모든 구간을 이용하여 분리하였을 때 (a)와 피크에 해당하는 구간만을 이용하여 연산 분리한 결과 (b)를 나타낸 것이다. (b)에서 보듯이, 각 연산이 확연하게 분리가 되는 것을 관찰할 수 있다. 빨간색 클래스는 제곱 연산, 녹색 클래스는 곱셈 연산, 그리고 점선은 전력이 낮은 구간에서의 중간지점에서 수직으로 그은 선이다.

3.4 Operation classification

본 실험에서 연산의 특징 부분으로 분리된 구간에서 연산은 곱셈(multiply) 연산으로 추정되는 특징점이 분포하면 곱셈 연산으로 분류하였으며, 없으면 제곱(square) 연산으로 분류하였다. 연산의 특징으로 분류된 각 구간을 전력 파형에 나타내면 Fig. 8.과 같다. 초록색 부분은 제곱 연산의 특징점, 빨간색 부분은 곱셈 연산의 특징점을 잡아낸 것이다. 파란색 부분은 노이즈(noise)와 전력 값의 크기가 작은 부분이다.

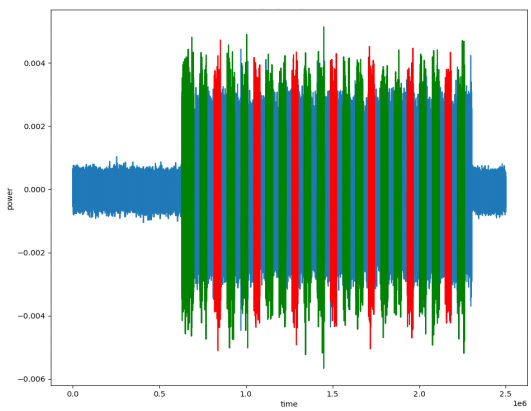


Fig. 8. Power waveforms labeled with the characteristics of the classified operation.

IV. Experiments

실험의 데이터는 RSA 복호화 과정 동안 오실리코프(Ocilliscope)를 이용하여, 샘플링 주파수와 복호화 키 비트를 달리하여 측정한 단일 전력 파형이다. 샘플링 주파수는 각각 500MS/s, 100MS/s, 10M

S/s이며, 복호화 키 비트는 16비트와 32비트로 나뉘어진다. 실험 데이터의 이름은 O_bit_sampling으로 나타내며, 여기서 bit는 복호화 키의 비트 크기를 의미하며, sampling은 오실리코프의 샘플링 주파수를 의미한다. 본 논문은 Intel(R) CoreTM i7-7700 CPU와 31.3 GiB의 메모리가 장착된 컴퓨터와 파이썬(python) 언어를 이용하여 실험하였다.

4.1 Evaluation

본 논문에서 제안한 방법을 통해 단일 전력 파형을 입력값으로 하여 예측 연산(output)을 실제 전력 파형을 생성한 연산(ground truth)과 비교하였다. 예측 연산 값과 실제 연산값이 다른 경우는 주로 연산이 잘 분리되지 않아 2개의 연산이 한 개의 연산으로 예측되는 경우이거나 전력 파형의 노이즈를 연산으로 예측하는 경우이다. 이러한 이유 때문에 예측 과정에서 실제 매칭될 연산 값의 순서가 달라지게 된다. 따라서, 연산의 순서를 고려한 비교 알고리즘을 이용해야 예측한 연산과 실제 연산의 정확한 비교를 할 수 있을 것이다. 이를 위해 본 논문에서는 Dynamic Time Warping(DTW) 알고리즘을 이용하였다. DTW란 서로 다른 길이의 두 신호의 유사도를 측정하기 위하여 최적의 동적 정렬 (Dynamic Alignment) 솔루션을 찾는 알고리즘이다[7]. 본 논문의 실험에서는 STFT의 프레임 길이에 따라, 알고리즘의 성능이 좋아지는지 알아보았다. DTW 알고리즘은 비교할 데이터들을 각각 x축과 y축에 놓음으로써 매칭이 되면 대각선으로 이동하여, 매칭이 되지 않을 때에는 오른쪽이나 위쪽으로 이동하게 된다. 따라서, 오른쪽이나 위쪽으로 이동한 개수가 많을수록 매칭이 안되었다고 볼 수 있다. 따라서, 실제 연산과 예측 연산의 비교 결과는 오른쪽과 위쪽으로 총 이동한 거리로 나타낸다. STFT 프레임 길이에 따른 비교 결과(거리)를 Table 2.에 나타내었다. 결과를 통해 제안 기법이 유효하기 위해서는 프레임 길이가 충분히 길어야 하며, 샘플링 주파수에 따라 다름을 볼 수 있다.

Table 1. Comparison between our method and [5]

	[5]	Our method
Algorithm	MCMC	K-means
Feature	raw signal	STFT
Dimension of feature	1	12,500
Execution time(s)	104.76	5.43

4.2 기존 논문과의 비교

본 논문의 알고리즘은 기존의 자동화된 예측 알고리즘[5]과 비교를 하였다. 자세한 내용은 Table 1.과 같다. [5]의 기법과 비교하였을 때, 제안하는 기법은 앞서 언급하였듯이, 약 20배의 빠른 실행 속도를 보이며, 이는 사용한 특징이 단순 1차원 전력 신호가 아닌 다차원의 주파수 벡터를 이용하였기 때문에 더 가벼운 알고리즘으로 효과적으로 최적해를 찾을 수 있는 양상을 보였다. 기존 알고리즘은 MCMC를 이용하였기 때문에 많은 계산량으로 인하여 속도가 느리다. 하지만, 본 논문의 알고리즘은 전력값을 주파수 신호로 변환하여, 클러스터링만으로 예측하기 때문에 속도 향상이 기존 논문보다 매우 빠르다. 기존의 논문에서는 500MS/s에서만 실험을 진행하였지만, 본 논문에서는 이외에, 100MS/s, 10MS/s에서도 실험을 진행하였다. 기존의 논문은 여러 신호 전처리 후에, 클러스터링을 진행하였기에, 다른 기기의 RSA 전력파형에서 응용이 본 논문보다 어렵다. 본 논문은 기존 알고리즘과 달리 전력의 변화(주파수)에 따라 패턴을 분류하기 때문에 전력의 크기에 견고한 알고리즘이 될 것이다.

V. Discussion

주파수 관점에서 전력 파형을 해석하는 것은 기존

Table. 2. DTW distance from the ground truth operation and the predicted operation according to the various frame lengths. DTW distance is defined as the distance traveled to the right and up.

Frame length	O_16_10	O_16_100	O_16_500	O_32_10	O_32_100	O_32_500
5e-6(s)	8	2	71	27	3	2
1e-5(s)	6	2	1	5	2	3
3e-5(s)	0	1	0	2	0	4

의 1차원 전력 파형의 특정 구간에서의 패턴을 통해 연산을 추정하는 것보다 연산 종류에 따른 특징(feature)이 잘 나타난다. 이러한 결과는 다른 부채널 분석에서도 이용할 수 있을 것이다. 하지만, 본 논문의 실험에서 사용한 전력 파형은 특정 기기에서 추출된 전력 신호이며, 샘플링 주파수와 키(key)의 비트(bit) 수만을 다양하게 한 채 연산의 종류는 한정하여 측정하였다. 따라서, 향후 여러 기기에서 추출한 전력 파형을 이용해야 할 것이며, 연산의 종류를 다양화하여 실험을 진행해야 할 것이다. 이외에, STFT를 이용한 신호 변환 시에 프레임의 크기에 따라 K-means의 성능이 달라졌다. 따라서, 전력 파형의 샘플링 주파수에 따라 적합한 프레임 크기를 이용하여야 한다. 분류된 신호를 연산 단위로 분리할 때, 전력 값이 낮은 구간을 이용하였다. 전력 값이 낮은 구간이 실제 연산을 분리하는 구간인가를 찾아내는 것도 연산 예측의 성능에 중요한 영향을 끼쳤으며, 본 논문은 전력 값이 낮은 구간길이를 확률분포로 추정한 후, 확률분포의 피크를 이용하여 연산을 분리하는 구간을 찾는 방법을 제안하였다. 본 논문의 방법론 이외에 다른 기법을 이용하여 연산 분리를 하는 방법을 찾는 것도 좋은 주제가 될 것이다.

VI. Conclusion

기존의 RSA 암호의 부채널 분석은 전력 파형을 사람이 패턴을 관찰하여, 연산을 추정하는 식으로 진행되었다. 본 논문의 실험에서 1차원 전력신호를 STFT를 이용하여 2차원의 주파수 신호로 변환한다면, 각 신호에 따른 특징을 1차원 신호에서보다 잘 관찰되는 것을 알 수 있었다. 2차원 신호를 K-means를 이용하여 특정 시간이 어떠한 연산으로 분류되는지 추정함으로써, RSA 암호의 복호화 과정에서 발생한 단일 전력 파형에서 연산을 예측하는 과정을 자동화할 수 있다는 것을 보여주었다. 하지만, 제한된 정보를 이용하여 단일 파형으로부터 하여 키의 예측을 한다는 것은 하이퍼파라미터를 설정해야 하는 것이나, 예측 정확도에는 한계가 있을 수 밖에 없다. 따라서, 향후 연구에서는 여러 파형의 정보를 이용하되 하이퍼파라미터의 값의 설정을 자동화하며, 예측 정확도를 높이는 연구를 진행해야 할 것이다.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptology, CRYPTO' 99, LNCS 1666, pp. 388-397, 1999

[2] Messerges, Thomas S, Ezzy A. Dabbish, and Robert H. Sloan, "Power analysis attacks of modular exponentiation in smartcards," Cryptographic Hardware and Embedded Systems, vol. 1717, pp. 144-157, August. 1999

[3] Picek, S., Heuser, A., Jovic, A., Ludwig, S. A., Guilley, S., Jakobovic, D., and Mentens, N, "Side-channel analysis and machine learning: A practical perspective," 2017 International Joint Conference on Neural Networks (IJCNN), pp. 4095-4102, May. 2017

[4] Lerman, Liran, Gianluca Bontempi, and Olivier Markowitch, "Power analysis attack: an approach based on machine learning," International Journal of Applied Cryptography, vol. 3, no. 2, pp. 97-115, June. 2014

[5] Hwang, Jeonghwan, and Ji Won Yoon, "An automated end-to-end side channel analysis based on probabilistic model," Applied Sciences, vol. 10, no. 7, pp. 2369-2384, Mar. 2020

[6] Bishop, C.M, Pattern recognition and machine learning, springer, pp. 423-455, 2006

[7] Silva, D. F., and Batista, G. E, "Speeding up all-pairwise dynamic time warping matrix calculation," Proceedings of the 2016 SIAM International Conference on Data Mining, pp. 837-845, June. 2016.

〈저자소개〉

정 지 혁 (Ji-hyuk Jung) 학생회원
2017년 2월: 서울대학교 수의학과 졸업
2019년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 신호처리, 머신러닝

윤 지 원 (Ji-Won Yoon) 종신회원
2008년: University of Cambridge 통계신호처리 박사
2011년~2012년: IBM Research Lab
2012년~현재: 고려대학교 정보보호대학원 교수
2016년~현재: 정보보호학회 이사
2016년 6월~현재: 서울경찰청 사이버 보안 자문위원
2019년 10월~현재: 국립전파연구원 전파보안 자문위원
〈관심분야〉 통계신호처리, 베이지안 기법, 인공지능