情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

고차 전력 분석에 대한 통계적 수식의 일반화*

김 민 수,† 김 희 석, 홍 석 희 ‡
고려대학교 정보경영공학전문대학원

Statistical Analysis of High-Order Power Analysis*

MinSu Kim,† HeeSeok Kim, Seokhie Hong ‡
Graduate School of Information Management and Security, Korea University

요 약

d차의 고차 전력 분석은 d차 마스킹 기법에 의해 안전하게 방어할 수 있다. 하지만 이러한 고차의 마스킹 기법의 적용은 차수가 높아질수록 암호 시스템의 성능을 현저히 떨어뜨린다. 기존의 고차 전력 분석에 대한 통계적 접근은 이차 전력 분석에 대해서만 이루어져 있다. 하지만 이는 암호 설계자가 삼차 이상의 마스킹 적용 시 특별한 안전성의 기준이 없음을 의미하며 이러한 기준의 부재는 무의미하게 높은 차수의 마스킹 기법 적용으로 인해 암호 시스템의 성능을 상당히 저하시킬 수 있다. 본 논문에서는 이러한 기준을 마련하고자 고차 전력 분석에 대한 통계적 수치를 일반화 하였다. 즉, 고차 전력 분석을 수행했을 때 연산되는 상관계수의 값을 일반화 시켰으며 이는 향후 마스킹 기법 사용 시 적용해야할 차수를 선택하기 위한 좋은 지표가 될 것이다.

ABSTRACT

dth-order power analysis can safely be defended by dth-order masking method. However, as the degree of applied masking method increases, it can significantly decrease effectiveness of cryptosystem. The existing statistical analysis on high-order power analysis contains only analysis on second power analysis. However, this means absent of safety standards when crypto engineers apply 3rd or more order masking. this absent of standards can lead to insignificant usage of masking method which can significantly decrease effectiveness of cryptosystem. In this dissertation, we have generalize statistical values on high-order power analysis to establish these standards. In other words, we have generalized the value of a correlation coefficient when calculation of high-order power analysis methods are performed. That is to say, it can greatly be used to indicate a degrees that can be applied on further usage of masking method.

Keywords: Side Channel Attack, Power Analysis, High-Order Power Analysis, masking Countermeasure

I. 서 론

이론적으로 안전한 것으로 알려진 암호 알고리즘조차도 실제 구현 단계에서 암호 설계자가 고려하지 못한 부가적인 정보의 누출로 인해 비밀 정보가 드러날 수 있음이 알려졌다. 부채널 공격 (side channel attack)[1]으로 정의되는 이러한 부류의 분석 방법에는 오류주입공격 (fault attack)[2], 시간 공격 (timing attack)[1,2], 전력 분석공격 (power analysis attack)[1,3,4,5,6,7,8,9,10] 등이 있다. 부채널 공격이 소개되면서 많은 암호시스템 설계자들은 효율적인 대응법들을 연구하기 시작했고, 부채널

접수일(2011년 1월 14일), 게재확정일(2011년 3월 15일)
*본 연구는 지식경제부 IT R&D 사업의 일환으로 수행하였음(유비쿼터스 환경에서의 정보보호 서비스를 위한 프라이버시 강화 암호 기술 개발)
† 주저자, kimminsu@cist.korea.ac.kr
‡ 교신저자, hsh@cist.korea.ac.kr

공격 중 하나인 일차 전력 분석에 대한 대응법으로는 일차 마스킹 대응법 (masking method)[7,8,11]이 활발히 연구되어지고 있다

하지만 이러한 일차 마스킹 대응법은 여전히 고차 전력 분석에 취약한 것으로 알려졌으며 이를 방어하기 위해 다양한 고차 마스킹 기법[7,12,13]들이 최근 연구되고 있다. $d-1$차 전력 분석[5,11]을 막기 위한 고차 마스킹 기법은 $d-1$차 마스킹 기법으로 정의되며 이 방법은 암호화 연산 시 일어나는 모든 중간 값을 d개의 난수로 분할 연산한다. 즉, 평문 m, 키 k, 암호문 c에 대해, 특정 암호 알고리즘 $c \leftarrow \epsilon(m,k)$의 연산은 $d-1$차 마스킹 기법을 적용 시, 다음과 같이 변형된다.

$$(c_0, ..., c_{d-1}) \leftarrow \epsilon'((m_0, ..., m_{d-1}), (k_0, ..., k_{d-1}))$$

위의 식에서 $\oplus_{i=0}^{d-1} m_i = m$, $\oplus_{i=0}^{d-1} k_i = k$, $\oplus_{i=0}^{d-1} c_i = c$의 식이 만족해야 하며, 각 m_i, k_i, c_i 값 들은 m, k, c에 모두 독립인 값들이어야만 한다 ($\oplus$: exclusive-or, XOR). 이는 $d-1$차 마스킹 알고리즘 ϵ'의 연산 중 일어나는 모든 중간 값에서도 동일하게 적용된다. 즉, 마스킹이 적용되지 않은 암호 알고리즘 ϵ이 연산하는 중간 값 Z에 대해 ϵ'은 이 값을 $(Z_0, Z_1, ..., Z_d)$의 형태로 바꾸어 연산해야만 한다. 물론 이 식에서도 $\oplus_{i=0}^{d-1} Z_i = Z$의 식은 만족되어야만 한다. 따라서 이 식을 만족하기 위해 d개의 난수 $M_1, M_2, ..., M_{d-1}$를 이용, $(Z_0, Z_1, ..., Z_d)$를 다음의 형태로 연산한다.

$$(M_1, M_2, ..., M_{d-1}, Z \oplus (\oplus_{i=1}^{d} M_i)) \quad (1)$$

이러한 연산 기법은 암호 연산 중간 값 중 특정 $d-1$개의 원소의 조합이 공격자가 예측할 수 있는 중간 값 Z와 연관성을 가지는 것을 방어할 수 있다. 하지만 이러한 마스킹 기법 역시 d차 전력 분석에는 역시 취약하게 된다. d차 고차 전력 분석은 암호 연산 시 소비되는 d 시점에서의 소비 전력을 조합했을 때, 조합된 값이 공격자가 예측할 수 있는 특정 중간 값과 연관성을 가질 경우 나타나는 취약성을 이용한 공격 방법이다[5]. [5]의 방법에서는 전력 파형들 간의 곱과 공격자가 예측한 중간 값 사이의 상관계수를 이용해 이 연관성을 찾아냈다.

차수가 높은 마스킹 기법은 높은 안전성을 제공할 수 있지만 시스템의 과부하를 초래한다. 따라서 실질적인 암호 시스템에서 고차 전력 분석을 수행했을 때 고차 전력 분석이 가질 수 있는 수치적 상관계수 값을 암호 시스템 설계자가 알 수 있다면 시스템의 성능을 최대한 저하시키지 않는 범위 내에서 마스킹 기법의 적정 차수 값을 판단할 수 있다. 하지만, 각 차수의 전력 분석 기법에서 이 두개의 값이 어느 정도의 연관성을 갖는지에 대한 기준, 즉 상관 계수 값에 대한 수치적 연구 결과는 현재 이차 전력 분석에 대해서만 이루어져 있으며 이로 인해 암호 설계자들은 삼차 이상의 고차 전력 분석에 안전한 암호 시스템 설계 시 어려움을 겪을 수밖에 없다. 본 논문에서는 이러한 어려움을 해결하기 위해 삼차이상의 고차 전력 분석에 대한 수치, 즉 상관 계수 값을 일반화하였다. 또한 이로부터 유도할 수 있는 다양한 이론적 결과를 통해 고차 마스킹 기법의 적용 시 활용할 수 있는 다양한 정보들을 제공하고자 한다. 따라서 본 논문의 결과에 따라 특정 환경에서의 상관계수 값을 결정할 수 있다. 또, 일차 전력 분석에서의 상관계수가 암호설계자가 알고 있을 경우 논문에서 일반화 시킨 수식을 통해 안전하다고 여겨지는 상관계수를 가지는 마스킹 기법 차수를 결정할 수 있다.

본 논문의 구성은 다음과 같다. 2절에서 전력 분석 및 마스킹 기법에 대해 설명하며 3절에서 고차 전력 분석의 상관계수 값을 수식적 접근을 통해 일반화 한다. 4절에서는 이 수치의 활용 방안 및 실험결과를 다루고 5절에서 본 논문을 결론 맺는다.

II. 전력 분석 및 마스킹 기법

2.1 일차 전력 분석

일차 전력 분석은 전력 분석에 대한 대응법이 고려되지 않은 알고리즘에 대한 분석으로 전력이 발생하는 한 시점(암호연산이 일어나는 시점)의 소비전력량과 공격자가 예측할 수 있는 중간 값과의 상관 계수 값을 이용하여 비밀 정보를 알아내는 방법이다. 이러한 일차 전력 분석이 가능한 이유는 암호화 장비가 연산하는 데이터의 해밍웨이트(H)에 의존해서 전력을 소비하기 때문이다. 해밍웨이트(H)란 데이터를 이진수로 표현했을 때 데이터가 가지는 1의 개수를 의미한다. 이때 암호 연산이 일어나는 시점의 소비 전력량을 P, 입력 평문은 M, 비밀 정보를 K, 공격자가 예측할 수 있는 중간 값을 $Z=f(M,K)$라고 정의하면 일차 전력 분석은 다음의 상관 계수 값을 이용해 비밀 정보를 알아 낼 수 있다. 예를 들어 표준 블록 암호 AES[14]에 대한 일차 전력 분석에서 중간 값 $Z=f(M,K)$은 입력 평문 M의 첫 바이트 M_0와 비밀 정보 K의 첫 바이

트 K_0에 대해서 $Sbox(M_0 \oplus K_0)$로 선택되어 사용될 수 있다.

$$\rho = \frac{Cov(P, H(f(M,K)))}{\sqrt{Var(P)}\sqrt{Var(H(f(M,K)))}}$$

공격자의 K에 대한 예측이 옳다면 위의 식은 틀린 예측에 의해 연산되는 상관 계수 값보다 상대적으로 높은 상관 계수 값을 가지게 된다. 따라서 공격자는 가장 높은 상관계수 값을 가지는 K를 암호화 장비의 비밀 정보로 판단할 수 있다.

2.2 고차 전력 분석 및 이차 전력 분석의 상관계수 수치

d차 전력 분석은 $d-1$차 마스킹이 적용된 암호 알고리즘에 대해 암호 연산이 일어나는 d개의 시점의 소비 전력을 이용해 분석을 수행한다. 즉, 전력을 소비하는 d개의 시점 t_1, t_2,$\cdots$,t_d에서의 소비 전력을 조합한 값과 공격자가 예측한 중간 값의 헤밍웨이트 사이의 상관 계수를 이용해 비밀 정보를 찾아내는 전력 분석 방법이다. 본 논문에서는 전력을 소비하는 시점 t_1, t_2, $\cdots$,t_d에서의 소비 전력을 [5]의 논문에서와 동일하게 Messerges가 제안한 일반적인 전력 소비 모델을 통해 정의 하도록 한다. Messerges가 제안한 전력 소비 모델(P)는 다음과 같다[10].

$$P = offset + \varepsilon H(Data) + Noise \qquad (2)$$

이때, $offset$, ε, $Noise$는 각각 상수, 해밍웨이트 1당 소비하는 전력량, $N(0,\sigma^2)$의 정규 분포를 따르는 노이즈 값을 의미한다.

d차 전력 분석에 대한 t_1, t_2,$\cdots$,t_d에서의 소비 전력은 식 (1), (2)에 의해서 다음과 같다.

$$P(t_1) = offset + \varepsilon H(M_1) + N_1$$

$$P(t_2) = offset + \varepsilon H(M_2) + N_2$$

$$\vdots$$

$$P(t_{d-1}) = offset + \varepsilon H(M_{d-1}) + N_{d-1}$$

$$P(t_d) = offset + \varepsilon H(M_1 \oplus M_2 \oplus \cdots \oplus M_{d-1} \oplus Z) + N_d$$

공격자는 이 두 시점의 전력을 $pre_d(P)$ 함수에 의해 조합한다 ($P = \{P(t_1), P(t_2), \cdots, P(t_d)\}$). 전력 분석의 차수 d에 따른 $pre_d(P)$ 함수는 다음과 같이 정의된다.

$$pre_d(P) = \prod_{i=1}^{d} (P(t_i) - E(P(t_i)))$$

공격자는 조합된 이 전력 값과 예측한 중간 값 Z의 헤밍웨이트 $H(Z)$ 사이의 상관계수를 구한다. d차 전력 분석의 상관 계수 값은 다음과 같이 연산되어질 수 있다 (사용되는 상관계수 ρ_d는 옳은 키를 예측했을 때의 상관계수 ρ_K에 대해서 $\rho_K \le \rho_d$을 만족한다.)[5].

$$\rho_d = \frac{\sigma(E[pre_d(P) \mid Z])}{\sigma(pre_d(P))} \qquad (3)$$

[5]의 논문에서는 공격 대상 장비가 n비트 프로세서일 때, (3)의 상관 계수 값을 이차 전력 분석에 대하여 일반화 하였다. 위의 상관 계수 식에서 상관 계수를 구성하는 값들은 $\sigma(E[pre_d(P) \mid Z])$, $\sigma(pre_d(P))$이다. 따라서 이 두 개의 값으로부터 상관계수 값을 연산할 수 있다.

우선 이차 전력 분석에 대해 (3)의 식의 분자 부분은 다음과 같이 연산되어 진다.

$$E[(P(t_1) - E(P(t_1)))(P(t_2) - E(P(t_2)))|Z]$$
$$= -\frac{1}{2}H(Z) + \frac{n}{4}$$

$$\sigma(E[(P(t_1) - E(P(t_1)))(P(t_2) - E(P(t_2)))|Z)]$$
$$= \sqrt{\frac{n}{4}(-\frac{1}{2})^2}$$

다음은 (3)의 식의 분모 부분에 대한 연산 결과이다.

$$\sigma((P(t_1) - E(P(t_1)))(P(t_2) - E(P(t_2))))$$
$$= \sqrt{\frac{n^2}{16} + \frac{n}{2}\sigma^2 + \sigma^4}$$

이 두 개의 식에 의해 (3)의 이차 전력 분석에 대한 상관계수 값을 정리하면 다음과 같다.

$$\rho_2 = \frac{\sqrt{n}}{\sqrt{n^2 + 8n\sigma^2 + 16\sigma^4}}$$

III. 고차 전력 분석에 대한 수식적 접근

높은 차수의 마스킹 기법은 전력 분석으로부터 높은 안전성을 제공할 수 있지만 이러한 마스킹 기법의 적용은 시스템의 과부하를 초래한다. 따라서 실질적인 암호 시스템에서 고차 전력 분석을 수행했을 때 d차의 고차 전력 분석이 가질 수 있는 수치적 상관 계수 값 ρ_d를 암호 설계자가 알 수 있다면 시스템의 성능을 최대한 저하시키지 않는 범위 내에서 마스킹 기법의 적

정 차수 값을 판단할 수 있다. 예를 들어, 암호 설계자가 전력 분석의 상관 계수치가 0.01 정도인 경우 시스템이 안전하다고 가정할 수 있다면, $\rho_m > 0.01 > \rho_{m+1}$을 만족하는 $m+1$을 찾아 $m+1$차 마스킹을 적용하면 이 시스템은 전력 분석에 안전하다고 가정할 수 있게 된다. 하지만 고차 전력 분석에 대한 상관계수 값을 연산한 수치는 이차 전력 분석에 대한 결과가 유일하며 이 결과는 암호 설계자에게 충분한 정보를 제공할 수 없다. 본 논문에서는 이차 전력 분석 결과를 일반화하여 d차 전력 분석의 상관 계수 값 ρ_d에 대한 수치를 일반화 하고자 한다.

$d-1$차 마스킹이 적용된 알고리즘에 대해 연산되는 d개의 연산시점의 전력량은 (1),(2)에 의해 다음과 같다.

$$P(t_1) = offset + \varepsilon H(M_1) + N_1$$

$$P(t_2) = offset + \varepsilon H(M_2) + N_2$$

$$\vdots$$

$$P(t_d) = offset + \varepsilon H(M_d) + N_d$$

각 시점 t_1, t_2, …, t_{d-1} 는 서로 독립적인 마스킹 난수를 생성하는 시점이고 t_d은 마스킹 된 값(M_d)이 연산되는 시점이다 ($M_d = M_1 \oplus M_2 \oplus \cdots \oplus M_{d-1} \oplus Z$).

n비트 프로세서에서 구동되는 $d-1$차 마스킹 기법에 대해 d차 전력 분석을 적용할 경우 우선 $pre_d(P)$를 연산하면 다음과 같다.

$$(\varepsilon H(M_1) - \frac{n}{2}\varepsilon + N_1)(\varepsilon H(M_2) - \frac{n}{2}\varepsilon + N_2)\cdots$$

$$(\varepsilon H(M_d) - \frac{n}{2}\varepsilon + N_d)$$

본 논문에서는 (3)의 식을 사용해서 상관계수 값을 구하고자 한다. 우선 (3)의 식의 분자 부분 $\sigma(E[pre_d(P)|Z])$에 대한 연산을 하도록 한다.

(3)의 식에서의 분자 부분에 대한 연산

정리 1. 서로 독립인 n비트 난수 $X_1, X_2, \cdots, X_{d-1}$가 생성되는 시점($t_1$, t_2, …, t_{d-1})과 값 $X_1 \oplus X_2 \oplus \cdots \oplus X_{d-1} \oplus Z (= X_d)$가 연산되는 시점($t_d$)에 대한 전력량을 $P(t_i)(1 \le i \le d)$라 할 때 식 (3)의 분자 값에 해당하는 $E[pre_d(P)|Z]$의 값은 다음과 같다.

$$E\left[\prod_{j=1}^{d}(P(t_j) - E(P(t_j)))|Z\right]$$

$$= \varepsilon^d\left\{E[H(X_1)H(X_2)\ldots H(X_{d-1})H(X_d)|Z] - (\frac{n}{2})^d\right\}$$

증명. 부록 1 참조.

정리1에서 $H(X_1 \oplus X_2 \oplus \cdots \oplus X_{d-1} \oplus Z)(= H(X_d))$은 **정리 2**에 의해 정리되어질 수 있다.

성질 1[비트연산] 모든 X, Y에 대해서 해밍웨이트 $X \oplus Y$은 다음을 만족한다.

$H(X \oplus Y) = H(X) + H(Y) - 2H(X \wedge Y)$

($\oplus$는 비트합, $\wedge$는 비트곱)

정리 2. 서로 독립인 n비트 난수 $X_1, X_2, \cdots, X_d$에 대해 다음의 식이 성립한다.

$$H(X_1 \oplus X_2 \oplus \cdots \oplus X_d)$$

$$= K_{1,d} + (-2)K_{2,d} + \cdots + (-2)^{d-1}K_{d,d}$$

$$= \sum_{t=1}^{d}(-2)^{t-1}K_{t,d}$$

$$(K_{t,d} = \sum_{i_1}^{d}\sum_{i_2=i_1+1}^{d}\cdots\sum_{i_t=i_{t-1}+1}^{d}H(X_{i_1} \wedge X_{i_2} \wedge \cdots \wedge X_{i_t}))$$

$$= \sum_{t=1}^{d}\left\{(-2)^{t-1}\sum_{i_1=1}^{d}\cdots\sum_{i_{t-1}=i_{t-2}+1}^{d}H(X_{i_1} \wedge \cdots \wedge X_{i_{t-1}})\right\} \quad (4)$$

증명. 부록 2 참조.

정리 3. 서로 독립인 n비트 $X_{i_1}, X_{i_2}, \cdots X_{i_l}$와 Z에 대해 $E(H(X_{i_1})H(X_{i_2})\cdots H(X_{i_l})(Z[j]\prod_{u=1}^{l}X_{i_u}[j])|Z)$($1 \le j \le n$, $i_1, i_2, \cdots, i_l$, $1 \le i_1 \le i_2 \le \cdots \le i_l \le d$) 다음을 만족한다.($X_i$에 대해서 $H(X_i) = \sum_{j=1}^{n}X_i[j]$이다. ($X_i[j]$: X_i의 j번째 비트, 각 비트는 서로 독립))

$$E(H(X_{i_1})H(X_{i_2})\cdots H(X_{i_l})(Z[j]\prod_{u=1}^{l}X_{i_u}[j])|Z)$$

$$(i_1, i_2, \cdots, i_l \ , \ 1 \le i_1 \le i_2 \le \cdots \le i_l \le d)$$

$$= (\frac{n+1}{4})^l Z[j] \quad (1 \le l \le d) \quad (6)$$

증명. 부록 3 참조.

따름정리 1. 서로 독립인 n비트 $X_1, X_2, \cdots X_d$와 Z에 대해서 다음의 식이 성립한다. 정리 3은

$$E(H(X_{i_1})H(X_{i_2})\cdots H(X_{i_l})(Z[j]\prod_{i=u}^{l}X_{i_u}[j])|Z)$$

$=(\frac{n+1}{4})^l Z[j]$ $(1 \le l \le d)$ 이고, Z의 모든 비트에 관한 것으로 나타내면 $1 \le j \le n$에 대해서 $\sum_{j=1}^{n}\left\{(\frac{n+1}{4})^l Z[j]\right\}=(\frac{n+1}{4})^l H(Z)(\because H(Z)=\sum_{j=1}^{n} Z[j])$로 정리될 수 있고 결국 다음과 같은 식이 성립하게 된다.

$E[H(M_1)\cdots H(M_{d-1})H(M_{i_1}\wedge\cdots\wedge M_{i_l}\wedge Z)|Z]$

$=(\frac{n}{2})^{d-1-l}(\frac{n+1}{4})^l H(Z)(\because E(H(M_i))=\frac{n}{2})$

정리 1, 정리 2, 정리 3에 의해 식 (3)의 분자 부분인 $\sigma(E[pre_d(P)|Z])$을 정리하면 다음과 같다 $(M_d = M_1 \oplus M_2 \oplus \ldots \oplus M_{d-1} \oplus Z)$.

$\sigma(E[pre_d(P)|Z])$

$=\sigma(E[\prod_{i=1}^{d}(\varepsilon H(M_i)-\frac{n}{2}\varepsilon+N_i)|Z])$

$=\sigma[\varepsilon^d\{E[H(M_1)H(M_2)\ldots H(M_{d-1})H(M_d)|Z]-(\frac{n}{2})^d\}]$ (∵ **정리 1**)

$=\varepsilon^d\sigma[E[H(M_1)H(M_2)\ldots H(M_{d-1})H(M_d)|Z]]$

위의 식에서 $E[H(M_1)H(M_2)\ldots H(M_{d-1})H(M_d)|Z]$는 Z에 관한 식으로 연산되며, 따라서 $\varepsilon^d\sigma[E[H(M_1)H(M_2)\ldots H(M_{d-1})H(M_d)|Z]]$의 값은 Z에 관한 표준편차 값이다. 즉, $H(M_1)H(M_2)\cdots H(M_{d-1})H(M_d)$의 식에서 Z와 연관되지 않은 항들은 표준 편차를 계산하면 0 값을 가진다. 따라서, $\varepsilon^d\sigma[E[H(M_1)H(M_2)\ldots H(M_{d-1})H(M_d)|Z]]$의식을 정리 2에 의해 정리한 후, Z 관련항만 나타내면 다음과 같다.

$\varepsilon^d\sigma\left[E\left[H(M_1)\ldots H(M_{d-1})\sum_{t=1}^{d}\left\{(-2)^{t-1}\sum_{i_1=1}^{d-1}\sum_{i_2=i_1+1}^{d-1}\cdots\sum_{i_{t-1}=i_{t-2}+1}^{d-1}H((M_{i_1}\wedge M_{i_2}\wedge\cdots\wedge M_{i_{t-1}})\wedge Z)\right\}\right]\right]$ (∵ **정리 2**)

$=\varepsilon^d\sigma\left[\sum_{t=1}^{d}\left\{(-2)^{t-1}\sum_{i_1=1}^{d-1}\sum_{i_2=i_1+1}^{d-1}\cdots\sum_{i_{t-1}=i_{t-2}+1}^{d-1}E[H(M_1)\cdots H(M_{d-1})H((M_{i_1}\wedge M_{i_2}\wedge\cdots\wedge M_{i_{t-1}})\wedge Z)]\right\}\right]$

$=\varepsilon^d\sigma\left[H(Z)\sum_{t=1}^{d}\left\{(-2)^{t-1}\sum_{i_1=1}^{d-1}\sum_{i_2=i_1+1}^{d-1}\cdots\sum_{i_{t-1}=i_{t-2}+1}^{d-1}\left(\frac{n}{2}\right)^{d-t}(\frac{n+1}{4})^{t-1}\right\}\right]$ (∵ **따름정리 1**)

$=\varepsilon^d\sigma\left[H(Z)\sum_{t=1}^{d}\left\{(-2)^{t-1}{}_{d-1}C_{t-1}\left(\frac{n}{2}\right)^{d-t}\left(\frac{n+1}{4}\right)^{t-1}\right\}\right]$

$=\varepsilon^d\sigma\left[H(Z)\sum_{t=1}^{d}\left\{{}_{d-1}C_{t-1}\left(\frac{n}{2}\right)^{d-t}\left(-\frac{n+1}{2}\right)^{t-1}\right\}\right]$

$=\varepsilon^d\sigma\left[H(Z)\left(\frac{n}{2}-\frac{n+1}{2}\right)^{d-1}\right]$

$=\frac{\varepsilon^d\sqrt{n}}{2^d}$ $(\because\sigma(H(Z))=\sqrt{\frac{n}{4}})$

따라서 (3)의 식의 분자부분인 $\sigma(E[pre_d(P)|Z])$은 다음과 같이 정리된다.

$$\sigma(E[pre_d(P)|Z])=\frac{\varepsilon^d\sqrt{n}}{2^d} \quad (7)$$

• (3)의 식에서의 분모부분에 대한 계산

$M_1, M_2, \ldots, M_{d-1}, Z\oplus\left(\bigoplus_{i=1}^{d-1}M_i\right)$, Z의 분포는 일차 종속이지만, Z를 제외한 $M_1, M_2, \ldots, M_{d-1}, Z\oplus\left(\bigoplus_{i=1}^{d-1}M_i\right)$의 분포는 일차 독립이다. 따라서, 각 시점 $t_1, t_2, \cdots, t_d$에서의 전력량이 독립임을 알 수 있다. 즉, $E[(pre_d(P))^2]$의 값은 $\prod_{i=1}^{d}E[\{P(t_i)-E(P(t_i))\}^2]$와 동일하다. 따라서, 각 $E(\{P(t_i)-E(P(t_i))\}^2)$의 값이 $E((\varepsilon H(M_i)-\frac{n}{2}\varepsilon+N_i)^2)=\frac{n}{4}\varepsilon^2+\sigma^2$ $(\because E(H(X)^2)=\frac{n^2+n}{4}$, $E(H(X))=\frac{n}{2}, E(N_i)=0$, $E(N_i^2)=\sigma^2)$임을 이용해 $E[(pre_d(P))^2]$을 정리하면 $(\frac{n}{4}\varepsilon^2+\sigma^2)^d$임을 쉽게 유도할 수 있다. $E(pre_d(P))=0$이므로 $\sigma[pre_d(P)]$의 값은 다음과 같다.

〔표 1〕 노이즈 표준편차 값의 변화에 따른 차수별 상관계수

고차 전력 분석 \ σ/ε	0	1	2	3
일차 전력 분석	1	0.8115	0.5321	0.4313
이차 전력 분석	0.3536	0.2357	0.1179	0.0643
삼차 전력 분석	0.1250	0.0680	0.0241	0.0097
사차 전력 분석	0.0442	0.0196	0.0049	0.0015

$$\sigma(pre_d(P)) = \sqrt{(\frac{n}{4}\varepsilon^2 + \sigma^2)^d} \quad (8)$$

식 (3), (7), (8)에 의해 d차 전력 분석에 대한 상관계수 값을 정리하면 다음과 같다.

$$\rho_d = \frac{\sigma(E[pre_d(P) \mid Z])}{\sigma(pre_d(P))} = \frac{\frac{\sqrt{n}}{2^d}}{\sqrt{(\frac{n}{4} + (\frac{\sigma}{\varepsilon})^2)^d}} \quad (9)$$

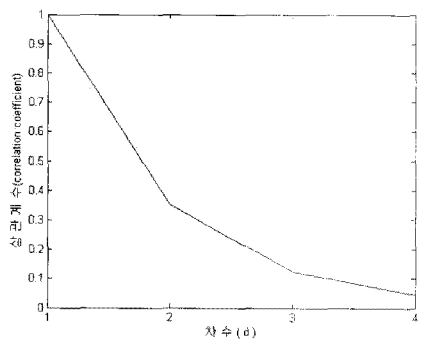
IV. 활용방안

본 절에서는 앞서 살펴본 것을 토대로 고차 전력 분석에 대한 정리를 하고 이를 활용할 방안에 대해서 알아보도록 한다.

4.1 노이즈 표준편차 값, 전력 분석의 차수에 따른 상관계수 표 및 그래프

본 논문에서 정의한 전력 소비 모델에서 노이즈 값 N_i는 가우시안 분포 $(0, \sigma^2)$를 따른다고 정의하였고 이에 따라서 상관계수의 값이 달라질 수 있다는 것을 확인할 수 있다. 또 전력 분석의 차수인 d 값에 따라서도 마찬가지로 확인 할 수 있다. 차수에 따른 상관계수 값과 노이즈 표준편차 값에 따른 상관계수 값을 각각 〔그림 1〕, 〔표 1〕로 나타내게 되면 다음과 같다 (〔그림 1〕은 노이즈가 0인 경우).

〔표 1〕은 $\frac{\sigma}{\varepsilon}$를 각각 0, 1, 2, 3라고 가정 했을 경우에 차수별 상관계수의 분포를 알 수 있다. 이에 따르면 $\frac{\sigma}{\varepsilon}$가 증가함에 따라 같은 차수에서도 상관계수가 낮아짐을 볼 수 있다. 이를 발전시켜 기존에 일차 전력 분석에서와 같은 환경에서 고차 전력 분석의 상관계수가 변하게 되는 것을 확인한다.



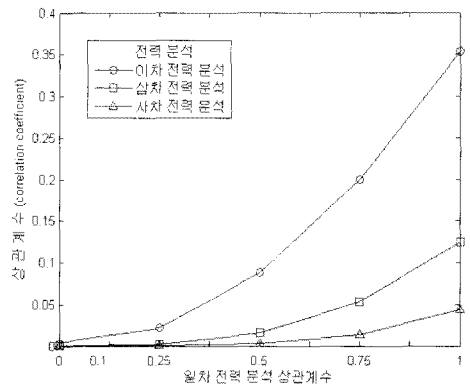
〔그림 1〕 차수에 따른 상관계수 값

4.2 일차 전력 분석과의 비교

여기에서 일차 전력 분석으로 얻을 수 있는 상관계수 최대값을 각각 1, 0.75, 0.5, 0.25, 0.1이라고 할 때 각각에 따른 사용되는 기기의 특성$(\frac{\sigma}{\varepsilon})$을 알 수 있다. 이를 전력 분석 차수가 높은 환경$(d=2,3,4)$에 적용해 보도록 한다. (이때 사용하는 기기의 특성$(\frac{\sigma}{\varepsilon})$을 역연산을 통해 알아낸다. 이때 사용하는 역연산은 고차 전력 분석의 일반화 식 (9)를 정리한 것$(n=8)$으로 $\frac{\sigma}{\varepsilon} = \sqrt{\sqrt[d]{\frac{8}{\rho_d^2 4^d}} - 2}$와 같다.)

이미 노이즈 표준편차는 상관계수에 대해서 반비례 관계를 가지고 있다는 것에 의존하여 본 논문에서는 실제 일차전력 분석 공격에서의 상관계수 값에 대해서 기존에 가지고 있던 수식을 활용하여 특정 상관계수에서의 기기의 특성$(\frac{\sigma}{\varepsilon})$을 예측하고 예측된 기기의 특성$(\frac{\sigma}{\varepsilon})$을 전력 분석 차수가 높은 환경$(d=2,3,4)$에 적용하여 충분히 의미 있는 정보를 생성해낼 수 있을 거라 예측하고 이를 활용한다.

앞서 〔표 1〕에서 본 것과 같이 노이즈 표준편차에 반비례하게 상관계수가 움직이는 것을 볼 수 있었는데 〔표 2〕를 살펴보게 되면 일차 전력 분석과 차수가 높은 환경$(d=2,3,4)$간의 상관계수 최댓값을 비교한 것



〔그림 2〕 일차 전력 분석 상관계수에 따른 고차 전력 분석에서의 상관계수 값

〔표 2〕 일차 전력 분석의 상관계수 변화에 따른 차수별 상관계수

$\rho_d(d=2,3,4)$ \ ρ_1	1	0.75	0.5	0.25	0.1
이차 전력 분석	0.3536	0.1989	0.0884	0.0221	0.0035
삼차 전력 분석	0.1250	0.0527	0.0156	0.0020	1.2500×10^{-4}
사차 전력 분석	0.0442	0.0140	0.0028	1.7263×10^{-4}	4.4194×10^{-6}

이다. 또, 〔그림 2〕는 이를 그래프로 나타낸 것이다.

4.3 활용 방안

암호 설계자는 해당 암호 시스템에 적당한 전력 분석 대응 기법을 적용해야 하며, 이를 적용하기 위해 우선 안전성 기준을 정해야만 한다. 암호 설계자가 전력 분석의 상관 계수치가 a이하의 값을 가질 때 암호 시스템이 안전하다고 기준치를 세울 경우, 설계자는 $\rho_d<a$의 식을 만족하는 d에 대하여 d차 마스킹을 적용해야 한다. 이러한 d를 찾는 과정을 단계별로 정리하면 다음과 같다.

1. 공격 대상 장비에서 대응법이 적용되지 않은 알고리즘에 대한 일차 전력 분석의 상관 계수치 ρ_1 계산
2. 식 (9)에 의해 ρ_1로부터 $\frac{\sigma}{\varepsilon}=\sqrt{\frac{2}{\rho_1^2}-2}$의 값을 연산
3. $\frac{\sqrt{n}}{2^d\sqrt{(\frac{n}{4}+(\frac{\sigma}{\varepsilon})^2)^d}}<a$를 만족하는 최소의 d연산

예를 들어 전력 분석에 안전하기 위해서 최대 상관계수가 0.01정도 나타나게 된다면 안전하다고 가정했을 때 암호설계자는 0.01을 안정성 기준으로 정하고 새로운 암호 알고리즘을 설계하거나 기존에 있는 알고리즘을 보완하는 곳에 충분히 사용할 수 있을 것이라고 여겨진다. 일차 전력 분석 공격에서 약 0.75의 상관계수를 가진다고 할 때 〔표 2〕와 위의 단계를 참고하면 약 사차 정도의 마스킹을 적용하게 되면 0.01보다 작은 최대 상관계수를 가지게 되고 이는 충분히 안정성을 가진다고 할 수 있다.

V. 결 론

본 논문에서는 고차전력 분석의 일반화를 통해서 전력 분석 공격의 차수에 따른 상관계수 값을 정의한다. 삼차 이상의 전력 분석에 대한 수식적 접근을 통하여 암호설계자들이 고차전력 분석에 안전한 대응기법의 설계에 도움을 주는 것을 알 수 있다. 실제로 일차 전력 분석과 같은 환경에서 d차 전력 분석을 적용했을 때의 상관계수 값을 알 수 있기 때문에 실용적이라고 볼 수 있다.

참고문헌

〔1〕 P. Kocher, J. Jaffe, and B. Jun, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Others Systems," Springer-Verlag, CRYPTO'96, LNCS-1109, pp. 104-113, 1996.

〔2〕 P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," White Paper, Cryptography Research, http://www.cryptography.com/dpa/technical Wed, 10 Jun. 1998

〔3〕 C. Rechberger and E. Oswald, "Practical Template Attacks," Springer-Verlag, WISA 2004, LNCS 3325, pp. 443-457, 2004.

〔4〕 E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen., "A Side-Channel Analysis Resistant Description of the AES S-box," Springer-Verlag, FSE 2005, LNCS 3557, pp. 3 - 423, 2005.

〔5〕 Emmanuel Prouff, Matthieu Ricain, Regis Bevan "Statistical Analysis of Second Order Differential Power Analysis" IEEE Transactions on computers, Vol.58 , No.6, pp.799 - 811, Jun. 2009

〔6〕 E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," Springer-Verlag, CHES 2004. LNCS 3156, pp. 16-29, 2004.

[7] Jovan D. Golic, Christophe Tymen. "Multiplicative Masking and Power Analysis of AES", Springer-Verlag, CHES 2002, LNCS 2523, pp. 198 - 212, 2003.

[8] Mehdi-Laurent Akkar and Christophe Giraud. "An Implementation of DES and AES, Secure against Some Attacks", Springer-Verlag, CHES 2001, LNCS 2162, pp. 309-318, 2001.

[9] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO 1999, Springer-Verlag, LNCS 1666, pp. 388-397, August 15 - 19 1999.

[10] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks of modular exponentiation in Smart cards," Springer-Verlag, Proc. of Workshop on Cryptographic Hardware and Embedded Systems, CHES, LNCS 1717, 1999, pp. 144-157. August 12 - 13 1999.

[11] B. Zakeri, M. Salmasizadeh, A. Moradi, M. Tabandeh, and M. Shalmani, "Compact and Secure Design of Masked AES S-Box," Springer-Verlag, ICICS 2007, LNCS 4861, pp. 216 - 229, 2007.

[12] J. Blömer, J. Guajardo, and V. Krummel. "Provably Secure Masking of AES," Springer-Verlag, SAC 2004, LNCS 3357, pp. 69 - 83, 2005.

[13] E. Oswald and K. Schramm. "An Efficient Masking Scheme for AES Software Implementations," Springer-Verlag, WISA 2005, LNCS 3786, pp. 292 - 305, 2006.

[14] Advanced Encryption Standard (AES), FIPS PUB 197, November 26, 2001, available at http://csrc.nist.gov/encryption/aes.

부록 1
(정리 1에 대한 증명과정)

$X_1 \oplus X_2 \oplus \cdots \oplus X_d = Z$ 이지만 $\{X_1, X_2, ..., X_d\}$에서 선택한 $d-1$개 이하의 원소로 이루어진 임의의 부분 집합은 Z에 대하여 독립이다. 따라서 $E\left[\prod_{j=1}^{k}\{P(t_{i_j}) - E(P(t_{i_j}))\}\right] = \prod_{j=1}^{k} E[P(t_{i_j}) - E(P(t_{i_j}))]$가 성립한다 ($i_1, i_2, \cdots, i_k$는 $1 \le i_1 < i_2 < \cdots < i_k \le d$을 만족하는 정수, $k \le d-1$). 이 식에서 각각의 시점에서의 $E[P(t_{i_u}) - E(P(t_{i_u}))] = E\left[\varepsilon H(X_{i_u}) - \frac{n}{2}\varepsilon + N_{i_u}\right] = 0$

$\because E(\varepsilon H(X_i)) = \frac{n}{2}\varepsilon, E(N_i) = 0$)이므로 $k \le d-1$인 경우 $E\left[\prod_{j=1}^{k}\{P(t_{i_j}) - E(P(t_{i_j}))\}\right] = 0$이 성립하게 된다.

$k \le d-1$인 경우 $E\left[\prod_{j=1}^{k}\{P(t_{i_j}) - E(P(t_{i_j}))\}\right] = 0$ [사실 1]을 이용해 $E\left[\prod_{j=1}^{d}\{P(t_j) - E(P(t_j))\} \mid Z\right]$의 식을 정리하면 다음과 같다.

$$E\left[\prod_{j=1}^{d}\{P(t_j) - E(P(t_j))\} \mid Z\right]$$
$$= E\left[\left\{\varepsilon H(X_d) - \frac{n}{2}\varepsilon + N_d\right\}\prod_{j=1}^{d-1}\{P(t_j) - E(P(t_j))\} \mid Z\right]$$
$$= E\left[\varepsilon H(X_d)\prod_{j=1}^{d-1}\{P(t_j) - E(P(t_j))\} \mid Z\right] +$$
$$E\left[\left(-\frac{n}{2}\varepsilon + N_d\right)\prod_{j=1}^{d-1}\{P(t_j) - E(P(t_j))\} \mid Z\right]$$
$$= E\left[\varepsilon H(X_d)\prod_{j=1}^{d-1}\{P(t_j) - E(P(t_j))\} \mid Z\right] +$$
$$\left(-\frac{n}{2}\varepsilon\right)E\left[\prod_{j=1}^{d-1}\{P(t_j) - E(P(t_j))\} \mid Z\right] \quad (\because N_d\text{은 평균이 } 0\text{인 노이즈 값이므로 독립})$$
$$= E\left[\varepsilon H(X_d)\prod_{j=1}^{d-1}\{P(t_j) - E(P(t_j))\} \mid Z\right]$$
$$(\because \text{[사실 1]})$$
$$= E\left[\varepsilon H(X_d)\left\{\varepsilon H(X_{d-1}) - \frac{n}{2}\varepsilon + N_{d-1}\right\}\prod_{j=1}^{d-2}\{P(t_j) - E(P(t_j))\} \mid Z\right]$$
$$= E\left[\varepsilon^2 H(X_d)H(X_{d-1})\prod_{j=1}^{d-2}\{P(t_j) - E(P(t_j))\} \mid Z\right] +$$
$$E\left[\varepsilon H(X_d)\left(-\frac{n}{2}\varepsilon + N_{d-1}\right)\prod_{j=1}^{d-2}\{P(t_j) - E(P(t_j))\} \mid Z\right]$$
$$= E\left[\varepsilon^2 H(X_d)H(X_{d-1})\prod_{j=1}^{d-2}\{P(t_j) - E(P(t_j))\} \mid Z\right] +$$
$$\left(-\frac{n}{2}\varepsilon\right)E\left[\varepsilon H(X_d)\prod_{j=1}^{d-2}\{P(t_j) - E(P(t_j))\} \mid Z\right]$$
$$= E\left[\varepsilon^2 H(X_d)H(X_{d-1})\prod_{j=1}^{d-2}\{P(t_j) - E(P(t_j))\} \mid Z\right] +$$

$$(-\frac{n}{2}\varepsilon)E\Big[\Big\{P(t_d)-E(P(t_d))+\frac{n}{2}\varepsilon-N_d\Big\}\prod_{j=1}^{d-2}\{P(t_j)-E(P(t_j))\}|Z\Big]$$
$$=E\Big[\varepsilon^2H(X_d)H(X_{d-1})\prod_{j=1}^{d-2}\{P(t_j)-E(P(t_j))\}|Z\Big]+$$
$$(-\frac{n}{2}\varepsilon)E\Big[\{P(t_d)-E(P(t_d))\}\prod_{j=1}^{d-2}\{P(t_j)-E(P(t_j))\}|Z\Big]$$
$$+(-\frac{n}{2}\varepsilon)E\Big[(\frac{n}{2}\varepsilon-N_d)\prod_{j=1}^{d-2}\{P(t_j)-E(P(t_j))\}|Z\Big]$$
$$=E\Big[\varepsilon^2H(X_d)H(X_{d-1})\prod_{j=1}^{d-2}\{P(t_j)-E(P(t_j))\}|Z\Big]$$
$$-(\frac{n}{2}\varepsilon)^2E\Big[\prod_{j=1}^{d-2}\{P(t_j)-E(P(t_j))\}|Z\Big]\ (\because\ [\text{사실 1}])$$
$$=E\Big[\varepsilon^2H(X_d)H(X_{d-1})\prod_{j=1}^{d-2}\{P(t_j)-E(P(t_j))\}|Z\Big]$$
$$(\because\ [\text{사실 1}])$$

위의 과정을 연속해서 d번 반복하게 되면 위의 식은 다음과 같이 정의된다.

$$=E\big[\varepsilon^{d-1}H(X_d)H(X_{d-1})\cdots H(X_2)\{P(t_1)-E(P(t_1))\}|Z\big]$$
$$=E\Big[\varepsilon^{d-1}H(X_d)H(X_{d-1})\cdots H(X_2)\Big\{\varepsilon H(X_1)-\frac{n}{2}\varepsilon+N_1\Big\}|Z\Big]$$
$$=E\big[\varepsilon^dH(X_d)H(X_{d-1})\cdots H(X_2)H(X_1)|Z\big]+$$
$$E\Big[\varepsilon^{d-1}H(X_d)H(X_{d-1})\cdots H(X_2)(-\frac{n}{2}\varepsilon+N_1)|Z\Big]$$
$$=E\big[\varepsilon^dH(X_d)H(X_{d-1})\cdots H(X_2)H(X_1)|Z\big]$$
$$-\frac{n}{2}\varepsilon^dE\big[(H(X_d))(H(X_{d-1}))\cdots(H(X_2))|Z\big]\ (\because \text{각 } X_i\text{의 분포가 독립},\ 1\le i\le d)$$
$$=E\big[\varepsilon^dH(X_d)H(X_{d-1})\cdots H(X_2)H(X_1)|Z\big]-(\frac{n}{2}\varepsilon)^d$$
$$(\because E(H(X_i))=\frac{n}{2})$$
$$=\varepsilon^d\Big\{E\big[H(X_1)H(X_2)\cdots H(X_{d-1})H(X_d)|Z\big]-(\frac{n}{2})^d\Big\}$$

부록 2
(정리 2에 대한 증명과정)

본 논문에서는 귀납법을 통해 정리 2를 증명하려고 한다.

$d=1$인 경우에는 $K_{1,1}=H(X_1)$이므로 (4)의 식은 성립한다. 또한 $d=2$인 경우에 성질 1에 의해 성립한다. 우선 $d=k-1$인 경우에 대해서 식 (4)가 성립함을 가정하면 다음식이 성립한다.

$$H(X_1\oplus X_2\oplus\cdots\oplus X_{k-1})$$
$$=K_{1,k-1}+(-2)K_{2,k-1}+\cdots+(-2)^{k-2}K_{k-1,k-1}$$

위의 식으로부터 다음의 식이 성질 1에 의해 성립한다.

$$H((X_1\oplus X_2\oplus\cdots\oplus X_{k-1})\oplus X_k)$$
$$=H(X_1\oplus X_2\oplus\cdots\oplus X_{k-1})+H(X_k)-2H((X_1\oplus X_2\oplus\cdots\oplus X_{k-1})\wedge X_k)$$
$$=K_{1,k-1}+(-2)K_{2,k-1}+\cdots+(-2)^{k-2}K_{k-1,k-1}+H(X_k)+(-2)H((X_1\oplus X_2\oplus\cdots\oplus X_{k-1})\wedge X_k)\quad(5)$$

위 식을 간단히 하기 위해서는$(-2)H((X_1\oplus X_2\oplus\cdots\oplus X_{k-1})\wedge X_k)=(-2)H((\bigoplus_{i=1}^{k-1}X_i)\wedge X_k)$에 대한 계산이 필요하다.

$(X_k\wedge X_k)=X_k$이고 (4)의 식이 $d=k-1$일 때 성립한다고 가정했으므로 $(-2)H((\bigoplus_{i=1}^{k-1}X_i)\wedge X_k)$의 식은 다음과 같이 정리된다.

$$(-2)H((\bigoplus_{i=1}^{k-1}X_i)\wedge X_k)=(-2)H(\bigoplus_{i=1}^{k-1}(X_i\wedge X_k))$$
$$=(-2)\sum_{t=1}^{k-1}\Big\{(-2)^{t-1}\sum_{i_1=1}^{k-1}\sum_{i_2=i_1+1}^{k-1}\cdots\sum_{i_{t-1}=i_{t-2}+1}^{k-1}H((X_{i_1}\wedge X_{i_2}\wedge\cdots\wedge X_{i_{t-1}})\wedge X_k)\Big\}$$

위의 식을 식 (5)에 대입하면 식 (5)는 다음과 같이 정리되어진다.

$$H((X_1\oplus X_2\oplus\cdots\oplus X_{k-1})\oplus X_k)$$
$$=K_{1,k-1}+(-2)K_{2,k-1}+\cdots+(-2)^{k-2}K_{k-1,k-1}+H(X_k)$$
$$+(-2)\sum_{t=1}^{k-1}\Big\{(-2)^{t-1}\sum_{i_1=1}^{k-1}\sum_{i_2=i_1+1}^{k-1}\cdots\sum_{i_{t-1}=i_{t-2}+1}^{k-1}H((X_{i_1}\wedge X_{i_2}\wedge\cdots\wedge X_{i_{t-1}})\wedge X_k)\Big\}$$
$$=K_{1,k}+(-2)K_{2,k}+\cdots+(-2)^{k-1}K_{k,k}$$
$$(\because K_{t,k-1}+\sum_{i_1}\sum_{i_2=i_1+1}^{k-1}\cdots\sum_{i_{t-1}=i_{t-2}+1}^{k-1}H(X_{i_1}\wedge X_{i_2}\wedge\cdots\wedge X_{i_{t-1}}\wedge X_k)=K_{t,k})$$

따라서 식 (4)는 $d=k$인 경우에 성립하여 귀납법에 의해 정리 2이 성립한다.

부록 3
(정리 3에 대한 증명과정)

본 논문에서는 귀납법을 통해 정리 3을 증명하려고 한다.

$d=1$인 경우에는 $E[H(X_{i_1})(X_{i_1}[j]Z[j])|Z]$

$=E\left[\sum_{i=1}^{n} X_{i_1}[i](X_{i_1}[j]Z[j]|Z\right]$

$=E(X_{i_1}[j]^2Z[j]+X_{i_1}[j]Z[j](\sum_{i=1,i\neq j}^{n} X_{i_1}[i])|Z)$

($\because X_i[j]$는 서로 독립 , $1\le j\le n$)

$=\frac{1}{2}Z[j]+\frac{1}{2}(\frac{n-1}{2})Z[j]=(\frac{n+1}{4})Z[j]$

($\because E(X_i[j])=E(X_i[j]^2)=\frac{1}{2}$, $E(\sum_{i=1,i\neq j}^{n} X_{i_1}[i])=\frac{n-1}{2}$)

따라서 $d=1$인 경우 식 (6)는 성립한다. 우선 $d=k-1$인 경우가 성립한다고 가정하면 다음식이 성립한다.

$E\left[H(X_{i_1})H(X_{i_2})\cdots H(X_{i_{l-1}})(Z[j]\prod_{u=1}^{l-1} X_{i_u}[j])|Z\right]$

$=(\frac{n+1}{4})^lZ[j]$ $(1\le l\le k-1)$

$d=k$인 경우를 다음과 같이 나타낼 수 있다.

$E\left[H(X_{i_1})H(X_{i_2})\cdots H(X_{i_l})(Z[j]\prod_{u=1}^{l} X_{i_u}[j])|Z\right]$

$=E\left[H(X_{i_1})H(X_{i_2})\cdots H(X_{i_{l-1}})(Z[j]\prod_{u=1}^{l-1} X_{i_u}[j])|Z\right]$

$E[H(X_{i_l})X_{i_l}[j]|Z]$ ($\because X_{i_l}$는 $X_{i_1},\cdots,X_{i_{l-1}}$과 독립)

$=(\frac{n+1}{4})^lZ[j](E(H(X_{i_l})X_{i_l}[j]))=(\frac{n+1}{4})^lZ[j]$

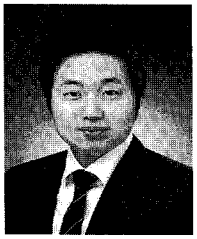
$E(X_{i_l}[j]^2+X_{i_l}[j]\sum_{i=1,i\neq j}^{n} X_{i_l}[i])$

$=(\frac{n+1}{4})^lZ[j]$ $(1\le l\le k)$

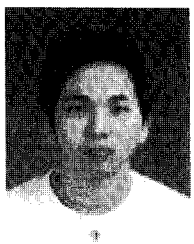
($\because X_i[j]$는 서로 독립 , $1\le j\le n$, $E(X_i[j])=E(X_i[j]^2)=\frac{1}{2}$, $E(\sum_{i=1,i\neq j}^{n} X_i[j])=\frac{n-1}{2}$)

따라서 식 (6)는 $d=k$인 경우 성립하며 귀납법에 의해 정리 3가 성립한다.

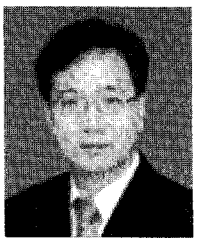
〈著者紹介〉



김 민 수 (MinSu Kim) 학생회원
2009년 2월: 중앙대학교 수학통계학부 수학과 학사
2009년 9월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 부채널 공격, 공개키 암호 알고리즘, 암호시스템 안전성 분석 및 고속구현



김 희 석(HeeSeok Kim) 학생회원
2006년 2월 연세대학교 수학과 학사
2008년 2월 고려대학교 정보보호대학원 공학석사
2008년~현재 고려대학교 정보보호대학원 박사과정
〈주관심분야〉 : 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술



홍 석 희 (Seokhie Hong) 정회원
1995년 2월: 고려대학교 수학과 학사
1997년 2월: 고려대학교 수학과 석사
2001년 2월: 고려대학교 수학과 박사
1999년 8월 ~ 2004년 2월: (주)시큐리티 테크놀로지스 선임연구원
2003년 3월 ~ 2004년 2월: 고려대학교 시간강사
2004년 4월 ~ 2005년 2월: K.U. Leuven 박사후연구원
2005년 3월~2008년 8월 고려대학교 정보보호대학원 조교수
2008년 9월~현재 고려대학교 정보보호대학원 부교수
〈관심분야〉 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식