情報保護學會論文誌
第20卷 第3號, 2010. 6

오류 확산 기법에 기반한 RSA-CRT 대응책에 대한 선택 메시지 공격

백 이 루,† 하 재 철‡
호서대학교 정보보호학과

Chosen Message Attack on the RSA-CRT Countermeasure Based on Fault Propagation Method

Yi-Roo Baek,† Jae-Cheol Ha‡
Dept. of Information Security, Hoseo University

요 약

중국인의 나머지 정리(Chinese Remainder Theorem)를 이용한 RSA 암호 시스템(RSA-CRT)에서의 연산은 기존의 일반 RSA 멱승 연산보다 빠르게 처리할 수 있어 디지털 서명이나 복호 과정에서 많이 사용된다. 그러나 RSA-CRT는 오류주입 공격에 매우 취약한 특성을 보여 많은 대응책이 제안되고 있다. 이 중에서 Yen 등은 오류 확산 기법을 사용한 두 가지 대응책을 제안하였는데 FDTC 2006에서는 그에 대한 새로운 공격 방법이 제시되었다. 그러나 Kim 등은 비트 연산 중 AND 연산의 특성을 이용하여 FDTC 2006에서 제시한 공격을 방어하는 방법을 제안하였다. 본 논문에서는 Kim 등이 제안한 AND 연산을 이용한 오류 확산 기법이 선택 메시지에 대한 오류주입 공격에 취약하여 안전하지 않음을 밝히고자 한다

ABSTRACT

The computation using Chinese Remainder Theorem in RSA cryptosystem is well suited in the digital signature or decryption processing due to its low computational load compared to the case of general RSA without CRT. Since the RSA-CRT algorithm is vulnerable to many fault insertion attacks, some countermeasures against them were proposed. Among several countermeasures, Yen et al. proposed two schemes based on fault propagation method. Unfortunately, a new vulnerability was founded in FDTC 2006 conference. To improve the original schemes, Kim et al. recently proposed a new countermeasure in which they adopt the AND operation for fault propagation. In this paper, we show that the proposed scheme using AND operation without checking procedure is also vulnerable to fault insertion attack with chosen messages.

Keywords: RSA-CRT, Fault attack, Fault Propagation, Checking procedure

I. 서 론

RSA는 현재 보안과 관련된 많은 분야에서 널리 사용되고 있는 공개키 암호 알고리듬이다[1]. RSA 알고리듬에서는 계산량의 효율성을 높이지 위해 중국인의 나머지 정리(Chinese Remainder Theorem)를 이용한 계산법(RSA-CRT)을 널리 사용하고 있다[2]. 그러나 이러한 RSA-CRT는 단 한 번의 오류주입만으로도 비밀키를 추출할 수가 있기 때문에 오류주입 공격에 매우 취약한 것으로 알려져 있다[3,4].

접수일(2009년 11월 23일), 수정일(2010년 2월 5일), 게재확정일(2010년 2월 19일)
† 주저자, blr83@nate.com
‡ 교신저자, jcha@hoseo.edu

이에 따라 1997년 Shamir의 오류주입 공격 대응 방법[5]이 제안된 이후 많은 대응 기법들이 연구되었다. 이 중에서 Yen 등에 의해 오류 확산 기법을 이용한 두 가지 대응책이 제안된 바 있다[6]. 하지만 이 역시 FDTC 2006에서 동일한 저자에 의해 새로운 공격 방법이 제시되어 오류주입 공격에 취약하다는 것이 밝혀졌다[7]. 그러나 최근 Kim 등은 논리연산 중 AND 연산을 이용하는 오류 확산 방법을 사용하여 Yen 등의 대응 방법을 사용할 수 있는 개선책을 제시하였다[8].

본 논문에서는 AND 연산만을 이용한 오류 확산 기법이 메시지 선택 오류주입 공격에 취약함을 보이고자 한다. 제안한 공격에 의하면 Yen의 대응 기법은 논문 [7]에서 증명한 바와 같이 여전히 오류주입공격에 취약한 특성을 그대로 유지하게 된다. 그리고 이를 보완할 수 있는 간단한 오류 확산 기법을 제시한다.

II. RSA-CRT에 대한 오류주입 공격 대응책

2.1 RSA-CRT 알고리듬과 오류주입공격

RSA 암호 시스템에서는 먼저 두 개의 큰 소수 p와 q를 선택하여 $n=p \cdot q$를 구하고, $\gcd(\phi(n), e)=1$이 되는 공개키 e를 선택하고 $ed \equiv 1 \bmod \phi(n)$을 만족하는 비밀키 d를 구한다.

RSA 암호 시스템에서는 입력 $m \in Z_n$에 대한 서명이나 복호 연산은 다음과 같은 멱승을 수행한다. 단, 본 논문에서는 이 연산 과정을 간단히 서명 과정이라고 부르기로 하고 그 결과를 서명 값이라 하자.

$$s = m^d \bmod n$$

그러나 이 연산은 계산의 효율성을 높이기 위해 CRT 기법을 적용하게 되는데 RSA-CRT 연산 방법은 아래와 같다.

$$s_p = m^{d_p} \bmod p$$
$$s_q = m^{d_q} \bmod q$$
$$s = CRT(s_p, s_q)$$

여기서 d를 이용하여 $d_p = d \bmod (p-1)$과 $d_q = d \bmod (q-1)$를 계산한다. 그리고 Garner 방법을 사용한 CRT 재결합(recombination) 단계는 다음과 같다.

$$s = CRT(s_p, s_q)$$
$$= s_q + q \cdot ((s_p - s_q) \cdot i_q \bmod p)$$

단, 여기서 $i_q = q^{-1} \bmod p$이다.

그러나 1997년 Boneh 등에 의해 RSA-CRT에 대한 오류주입 공격이 제안되었다[3]. 이 공격은 RSA-CRT 연산 과정에서 s_p나 s_q 둘 중에 어느 하나의 값에 오류를 주입하여 오류가 주입된 서명 s'을 얻을 수 있을 경우, 동일한 하나의 메시지에 대해 정상 서명 s와 오류 서명 s'을 이용하여 n을 소인수 분해하는 공격이다. 즉, 정상 서명 값이 s이고, s_p를 연산할 때 오류가 주입되어 생성된 값을 s_p'라고 하면, 오류 서명 s'을 이용하여 $GCD(s-s', n)$을 계산함으로써 비밀 소수 q를 구할 수 있다. 또한 Lenstra는 하나의 오류 서명만으로도 $GCD(s'^e - m, n)$와 같이 비밀 키를 다음과 같이 찾아낼 수 있음을 보였다[4].

2.2 Yen 등의 오류주입공격 대응 방법과 그 취약점

2.2.1 오류 확산을 이용한 오류주입 공격 대응책

2003년, Yen 등은 오류 확산 기법을 이용하여 상기한 오류주입 공격에 대응하는 두 가지 방법을 제안하였다[6]. 본 논문에서는 이 두 가지 방법을 CRT-1과 CRT-2라고 부르고 안전성과 공격 방법이 두 방법이 모두 동일하게 적용되므로 편의상 CRT-1을 중심으로 설명하고자 한다. Yen 등의 대응 알고리듬 CRT-1 알고리듬은 그림 1과 같으며 여기에 사용되는 정의는 다음과 같고 r은 작은 랜덤한 값이다.

$$d_r = d - r, \quad e_r = d_r^{-1} \bmod \phi(N).$$

2.2.2 대응책에 대한 공격

그러나 2006년 Yen 등은 FDTC 2006에서 2003년 자신들이 제안했던 CRT-1과 CRT-2 대응책이 오류주입 공격에 취약함을 보였다. Yen 등이 제안한 오류 모델은 CRT-1과 CRT-2에 동일하게 적용되므로 CRT-1 알고리듬으로 설명하도록 한다.

공격은 그림 1의 단계 3에서 $\tilde{m}$를 구하는 과정에서 k_q에 오류를 주입하는 경우를 가정한다. 그 외의 s_p나 s_q 그리고 k_p에 오류가 주입된 경우에는 오류주입 공격에 안전하다. k_q에 오류가 주입된 값을 k_q'이라 하고, $k_q' = k_q + t$로 표기한다.

여기서 t는 랜덤한 값인데 k_q'의 오류 종류에 따라 가변적인 값이다. 그러면 $\tilde{m}$를 구할 때, k_q에 오류가

Input : A message $m \in Z_n$
Output : $Sig := m^d \bmod n$

1. Compute both

$$k_p = \left\lfloor \frac{m}{p} \right\rfloor \text{ and } k_q = \left\lfloor \frac{m}{q} \right\rfloor$$

2. Compute $m^{d_r} \bmod n$ via a conventional CRT speedup as

$$s_p = m^{d_r \bmod (p-1)} \bmod p$$
$$s_q = \hat{m}^{d_r \bmod (q-1)} \bmod q$$

where $\hat{m} = ((s_p^{e_r} \bmod p) + k_p \cdot p) \bmod q$

3. A CRT recombination operation and some additional manipulation

$$s = CRT(s_p, s_q) \cdot \tilde{m}^r \bmod n$$

where $\tilde{m} = (s_q^{e_r} \bmod q) + k_q \cdot q$

4. Output s

〔그림 1〕 Yen 등이 제안한 CRT-1 알고리듬

주입되었을 경우 단계 3의 식은 다음과 같다.

$$\begin{aligned}\tilde{m}' &= (s_q^{e_r} \bmod q) + (k_q + t) \cdot q \\ &= \tilde{m} + t \cdot q = m + t \cdot q\end{aligned}$$

위의 식처럼 k_q에 주입된 오류가 $\tilde{m}$으로 확산되어 $\tilde{m}'$ 값이 나오게 되므로 오류 서명 s'는 다음과 같이 계산될 수 있다. 여기서 R_1과 R_2는 랜덤한 값이다.

$$\begin{aligned}s' &= CRT(s_p, s_q) \cdot \tilde{m}'^r \bmod n \\ &= CRT(s_p, s_q) \cdot (m + t \cdot q)^r \\ &= CRT(s_p, s_q) \cdot m^r + CRT(s_p, s_q) \\ &\quad \cdot R_1 \cdot q \bmod n \\ &= m^d + R_2 \cdot q \bmod n\end{aligned}$$

위의 식과 같이 비밀 소수 q가 포함된 값이 나오게 되므로 아래와 같은 식을 통해 비밀 소수 q를 찾을 수 있다. 여기서 R_3은 랜덤한 값이다.

$$\begin{aligned}\gcd(s'^e - m, n) &= \gcd((m^d + R_2 \cdot q)^e - m, n) \\ &= \gcd((m + R_3 \cdot q) - m, n) \\ &= q\end{aligned}$$

따라서 CRT-1 알고리듬은 오류주입 공격에 취약하다고 할 수 있으며 이 공격은 CRT-2 알고리듬에도 그대로 적용된다.

III. Kim 등의 대응 방법

2008년 Kim 등은 한국정보보호학회 논문에서 이런 점을 해결하기 위해 비교연산을 사용하지 않는 오류주입 공격에 안전한 RSA-CRT 기법을 제안하였다[8]. 제안 기법은 2003년 Yen이 제안했던 대응 기법을 개선한 것으로 논리 연산 중 AND 연산($\wedge$)을 이용하여 오류를 확산시키는 방법을 사용하였다.

Kim 등이 제안한 대응 기법은 $X \wedge X = X$가 되고, $X \wedge Y = Random\ Value$가 되는 AND 연산의 특성을 이용하여 그림 1의 CRT-1 대응 기법에서 단계 3의 $\tilde{m}$를 구하는 식에 AND 연산을 추가한 것으로 다음과 같이 개선하였다.

$$\begin{aligned}\tilde{m} &= m \wedge ((s_q^{e_r} \bmod q) + k_q \cdot q) \\ &= m \wedge ((m \bmod q) + m - (m \bmod q)) \\ &= m \wedge m = m\end{aligned}$$

위의 식과 같이 오류가 주입되지 않았을 경우 올바른 서명 값 s를 생성할 수 있다. 그리고 저저들은 단계 2에서 s_p나 s_q 또는 단계 3의 재결합 과정에서 k_q에 오류가 주입되더라도 단계 3에서 m과 AND 연산을 통해 랜덤한 값이 나오게 되므로 공격자가 오류 서명 값을 이용하여 비밀 정보를 추출할 수 없다고 주장하였다.

IV. Kim 등의 대응 방법의 문제점

4.1 메시지 선택 공격 모델

본 논문에서는 Kim 등의 대응 기법은 메시지 선택 공격에 취약할 수 있음을 보이고자 한다. 먼저 CRT-1의 오류 모델을 그대로 적용하여 $\tilde{m}$를 계산할 때, k_q에 오류가 주입되었다고 가정하면 다음과 같이 나타낼 수 있다.

$$\begin{aligned}\tilde{m}' &= m \wedge ((s_q^{e_r} \bmod q) + (k_q + t) \cdot q) \\ &= m \wedge (m + t \cdot q)\end{aligned}$$

위의 식과 같이 k_q에 오류가 주입되더라도 AND연산을 통해 $\tilde{m}'$ 값이 랜덤한 값이 되므로 공격자는 이 값을 이용해서 비밀 소수 q를 찾을 수 없어 보인다.

그러나 여기서 AND 연산의 특성 중 $A \wedge = A$가 되는 특성을 고려하면 메시지 선택 공격을 통해 AND 연산의 효과를 무력화시킴으로써 오류 서명을 유도할 수 있다.(여기서 [1]은 모든 비트가 1인 A보다 큰 값

을 의미한다.)

여기서 메시지 m의 길이가 l비트일 때 모든 비트가 1인 입력을 가정하자. 그러면 $m=2^l-1$을 입력으로 하고 k_q에 오류를 주입하는 공격을 시도하게 된다. 이 경우 단계 3의 오류 확산을 위한 식은 다음과 같이 나타낼 수 있다.

$$\begin{aligned}\widetilde{m}' &= m \wedge ((s_q^{e_r} \bmod q) + (k_q + t) \cdot q) \\ &= \wedge (m + t \cdot q) = m + t \cdot q\end{aligned}$$

즉, 여기서 1은 모든 비트가 1인 $(s_q^{e_r} \bmod q) + (k_q + t) \cdot q$보다 큰 값을 의미한다. 이때 주의할 점은 t 값이 오류 종류에 따라(즉, 오류 k_q'이 k_q보다 작게 되는 경우) 음수가 될 수 있다는 점이다. 위와 같이 AND 연산의 효과가 무력화되어 q를 포함한 오류 값이 $\widetilde{m}'$으로 확산되고, 이것은 FDTC 2006에서 제안한 오류주입 공격 모델과 동일하므로 비밀 소수 q를 찾을 수 있다.

그런데 메시지 m은 $m \in Z_n$이므로 l-비트가 모두 1인 메시지를 입력으로 사용할 수는 없다. 따라서 메시지 m은 상위 몇 비트가 0이고 나머지는 모두 1인 $2^{l-i}-1$(여기서 $i=1,2,3..$)의 형태이고 k_q에 오류를 주입하여 얻은 $(s_q^{e_r} \bmod q) + (k_q + t) \cdot q$ 값이 m보다 작은 경우에는 AND 연산에 의한 오류 확산 효과를 얻을 수 없어 쉽게 공격이 될 수 있다.

오류 주입 공격이 적용되는 구체적인 수치적 예를 들면 다음과 같다. 여기서 모든 수는 16진수로 표기하였으며 $n = p \cdot q = C1 \cdot B3 = 86F3$로 가정하자. 이 경우 메시지는 $m = 7FFF$로 하여 입력한다. 그리고 원래 $k_q = B7$인데 단계 3에서 오류가 주입되어 $k_q' = k_q + t = B7 - 1E = 99$로 바뀌었다고 가정한다.

그러면 단계 3의 값은 다음과 같이 전개되어 논리적 AND 연산은 오류 확산에 영향을 전혀 주지 못함을 볼 수 있다.

$$\begin{aligned}Y &= (s_q^{e_r} \bmod q) + (k_q + t) \cdot q \\ &= (m \bmod q) + (\lfloor m/q \rfloor + t) \cdot q \\ &= A + (B7 - 1E)B3 \\ &= 6B05\end{aligned}$$

$$\begin{aligned}\widetilde{m}' &= m \wedge ((s_q^{e_r} \bmod q) + (k_q + t) \cdot q) \\ &= 7FFF \wedge 6B05 \\ &= 6B05\end{aligned}$$

그러므로 AND 연산을 이용하여 오류를 확산하는 대응 기법은 선택 메시지를 사용한 오류주입 공격에 여전히 안전하지 않음을 알 수 있다. 이 공격 방법은 Kim 등이 제안한 CRT-1와 CRT-2에 대한 대응 기법에 모두 적용될 수 있다.

4.2 문제점에 대한 대응 기법

위에서 Kim 등이 제안한 기법은 AND 연산의 특성에 의해 메시지 선택 공격에 취약할 수 있음을 알 수 있었다. 본 논문에서는 논리 연산 중 흡수 법칙을 이용하여 오류를 확산하는 방법을 통해 오류주입 공격을 방어할 수 있는 대응 기법을 제안한다.

논리 연산에서 흡수 법칙(absorption law)은 다음과 같이 정의된다. 여기서 R은 임의의 값이다.

$$\begin{aligned}&X \vee (X \wedge R) = X \\ &X \wedge (X \vee R) = X \qquad (\wedge : AND,\ \vee : OR)\end{aligned}$$

위와 같이 흡수법칙은 AND 연산과 OR연산의 조합으로 이루어져 있으며 이러한 특성을 이용하여 대응 기법을 다음과 같은 원리로 구성할 수 있다.

$$\begin{aligned}&X \vee (Y \wedge R) \\ &X \wedge (Y \vee R)\end{aligned}$$

여기서 X는 원래의 값이고 Y는 오류 주입 여부를 검사하고자 하는 값이라 볼 수 있다. 위와 같이 $X = Y$일 경우 X값이 나오고, $X \neq Y$일 경우 랜덤한 값이 나오게 된다. 그러나 이와 같은 특성은 앞에서 언급했던 메시지 선택 공격이 가능할 수 있으므로 위의 두 식을 결합하여 다음과 같이 2중 흡수 법칙을 구성할 수 있다.

$$X \wedge ((Y \vee (X \wedge R)) \vee R)$$

위 식과 같이 두 종류의 흡수 법칙을 조합해도 $X = Y$일 경우 X값이 나오고, $X \neq Y$일 경우 랜덤한 값이 나오게 된다.

따라서 Kim 등의 대응 기법을 흡수 법칙으로 구성하면 $\widetilde{m}$을 계산하는 식을 다음과 같이 바꿔줄 수 있다. 서명이 정상적으로 이루어지면 중간 값 Y는 m과 같게 되며 $\widetilde{m} = m$이 된다.

$$\begin{aligned}Y &= ((s_q^{e_r} \bmod q) + k_q \cdot q) \\ \widetilde{m} &= m \wedge ((Y \vee (m \wedge R)) \vee R) \\ &= m \wedge ((m \vee (m \wedge R)) \vee R) \\ &= m \wedge (m \vee R) = m\end{aligned}$$

여기서 R은 임의의 랜덤한 값으로 시스템 내부에서 랜덤 수 발생기에 의해 생성된다. 주의할 점은 랜덤 수 R은 외부에서는 강제로 전체 비트를 0으로 만들거

나 1로 조작을 할 수 없다. 반면 제안하는 공격은 메시지 선택 공격이므로 입력 메시지 m은 공격자가 충분히 조작할 수 있다고 가정한다.

이제 메시지 m의 모든 비트가 0 또는 1인 경우를 가정하면 오류 주입 공격이 가능한지 분석해 보자. 그러나 실제 서명할 메시지가 0인 경우는 존재하지는 않는다.

1) $m=$ 인 경우
$\widetilde{m}= \wedge((Y\vee(\ \wedge R))\vee R)=$

2) $m=$ 인 경우
$\widetilde{m}= \wedge((Y\vee(\ \wedge R))\vee R)$
$= \wedge((Y\vee R)\vee R)$
$= Y\vee R$

위에서와 동일한 방법으로 수치적 예를 들어 오류 주입 공격이 적용되는지 살펴보자. 여기에서도 $n=p\cdot q=C1\cdot B3=86F3$로 하고 위에서와 동일하게 메시지는 $m=7FFF$로 하여 입력한다. 또한$k_q=B7$는 오류가 주입되어 $k_q'=k_q+t=99$로 바뀌었으며 임의의 랜덤 수 $R=38C7$이 발생되었다고 가정하자.

그러면 단계 3의 값은 다음과 같이 되어 이중 흡수법칙 연산에 의해 오류 확산 효과를 가진다.

$$\begin{aligned} Y&=(s_q^{e_r} \bmod q)+(k_q+t)\cdot q\\ &=(m \bmod q)+(\lfloor m/q\rfloor+t)\cdot q\\ &=A+(B7-1E)B3\\ &=6B05 \end{aligned}$$

$$\begin{aligned} \widetilde{m'}&=m\wedge((Y\vee(m\wedge R))\vee R)\\ &=7FFF\wedge((6B05\vee(7FFF\wedge 387C))\vee 387C)\\ &=7FFF\wedge((6B05\vee(387C))\vee 387C)\\ &=7FFF\wedge(7B7D\vee 387C)=7B7D \end{aligned}$$

위의 식에서 보는 바와 같이 Y값에 오류가 들어가더라도 최종적인 $\widetilde{m'}$값은 $6B05$가 나오지 않고 비밀키 q와 연관성이 없는 랜덤 수 $7B7D$값이 된다. 따라서 최종적으로 랜덤한 값이 되므로 선택 평문을 이용한 오류주입 공격에 안전함을 알 수 있다. 제안 기법은 흡수 법칙을 이용한 오류 확산 기법을 사용함으로써 오류주입 공격에 대응할 수 있으며 추가되는 연산량이 적기 때문에 효율적인 대응 기법이라 할 수 있다.

V. 결론

본 논문에서는 Kim 등이 제안한 오류주입공격 대응 기법의 안전성을 분석하고, AND 연산을 이용한 오류 확산 기법의 취약점을 발견하였다. 따라서 이를 해결할 수 있는 대응 기법으로 흡수법칙을 이용한 오류 확산 기법을 제안하였다.

제안 기법은 흡수법칙을 이용한 오류 확산 방법을 통해 선택 평문을 이용한 오류주입 공격에 대응할 수 있으며 간단한 논리 연산자들로 구성되어 매우 효율적인 대응 기법이 될 수 있다.

참 고 문 헌

[1] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[2] C. Couvreur and J. Quisquater, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," Electronics Letters, vol. 18, no. 21, pp. 905-907, Oct. 1982.

[3] D. Boneh, R. DeMillo, and R. Lipton, "On the Importance of Checking Cryptographic Protocols for Fault," EUROCRYPT'97, LNCS 1233, pp. 37-51, 1997.

[4] A.K. Lenstra, "Memo on RSA signature generation in the presence of faults," Manuscript, Sep. 1996. Available from Author at arjen.lenstra@citicorp. com.

[5] A. Shamir, "Method and Apparatus for Protecting Public Key Schemes from Timing and Fault attacks," US Patent 5991415, 23, Nov. 1999.

[6] S. Yen, S. Kim, S. Lim, and S. Moon, "RSA speedup with Chinese Remainder Theorem Immune Against Hardware Fault Cryptanalysis," IEEE Transaction on Computer, vol. 52, no. 4, pp. 461-472, Apr. 2003.

[7] S. Yen, D. Kim, and S. Moon, "Cryptanalysis of Two Protocols for RSA with CRT Based on Fault Infection," FDTC-06, LNCS 4236, pp. 53-61, Springer-Verlag, 2006.

[8] 김성경, 김태현, 한동국, 박영호, 홍석희, "비교연산을 사용하지 않는 오류주입 공격에 안전한 CRT 기반의 RSA," 정보보호학회논문지, 18(4), pp. 17-25, 2008년 8월.

〈著者紹介〉

백 이 루 (Yi Roo Baek) 학생회원
2008년 8월: 호서대학교 정보보호학과 졸업
2008년 9월~현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 네트워크 보안, 프로토콜, 스마트 카드 보안

하 재 철 (Jae Cheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2006년 1월: 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월: QUT in Australia 연구 교수
2007년 3월~현재: 호서대학교 정보호호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사, 논문지 편집위원
2009년 1월~현재: 한국산학기술학회 이사
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안