유비쿼터스 전자거래를 위한 쓰레시홀드 링 그룹 서명

성 순 화†

요 약

유비쿼터스 전자거래를 통하여 사용자는 언제 어디서나 네트워크에 접근하여 편리한 정보를 개인과 그룹, 그룹과 그룹 사이에서 교환할 수 있다. 사용자가 이러한 유비쿼터스 전자거래를 안전하게 사용하기 위해서는, 전자 정보의 무결성과 인증의 특성을 가지는 디지털 서명이 필수 조건이다. 유비쿼터스 네트워크에서의 디지털 서명은 언제 어디서나 필요에 따라 그룹을 만들기도 하고 해체하기도 하므로, 유비쿼터스 전자거래는 신뢰된 그룹 관리자와 셋업 프로시져 철회 프로시져 등이 필요없는 디지털 서명이 요구된다. 따라서 본 논문에서는 안전한 유비쿼터스 전자거래를 위한 디지털 서명으로서 쓰레시홀드 링 서명을 제안한다.제안된 디지털 서명은 위조의 위험이 없는(무결성) 링 서명과 메시지가 다른 서명자에 의해 서명되는 것을 증명할 수 없는 문제를 해결하는(인증) (n,t)링 서명을 사용한다. 그러므로 제안된 쓰레시홀드 링 서명은 무결성과 인증을 만족하는 차세대 유비쿼터스 그룹 서명이다.

키워드 : 링 서명, 쓰레시홀드 링 서명, 유비쿼터스 전자거래, 무결성, 인증

A Threshold Ring Group Signature for Ubiquitous Electronic Commerce

SoonHwa Sung†

ABSTRACT

Ubiquitous electronic commerce can offer anytime, anywhere access to network and exchange convenient informations between individual and group, or between group and group. To use secure ubiquitous electronic commerce, it is essential for users to have digital signature with the properties of integrity and authentication. The digital signature for ubiquitous networks is required neither a trusted group manager, nor a setup procedure, nor a revocation procedure etc. because ubiquitous networks can construct or deconstruct groups anytime, anwhere as occasion demands.

Therefore, this paper proposes a threshold ring signature as digital signature for secure ubiquitous electronic commerce using the ring signature without forgery (integrity) and the (n,t) ring signature solving the problem cannot prove the fact which a message is signed by other signer. Thus the proposed threshold ring signature is ubiquitous group signature for the next generation.

Key Words : Ring signature, Threshold ring signature, Ubiquitous electronic commerce, Integrity, Authentication

1. 서 론

디지털 서명은 무결성과 인증 특성 때문에 현재의 전자거래에서 중요한 역할을 한다. 무결성 특성은 받은 메시지가 수정되지 않았다는 것을 확실히 하고, 인증 특성은 보내는 사람이 모방되지 않았다는 것을 확실히 한다. RSA[1]와 DSA[2]와 같은 전통적인 디지털 서명은 한사람의 서명자가 유효한 서명을 생성하여 어떤 사람이 주어진 서명의 유효성을 검증할 수 있다. 그러나 많은 경우, 회사의 수표 발행과 같은 서명자들 집합의 메시지를 서명할 의무가 분배될 필요가 있다. 이런 경우 보안을 위해 회사의 수표는 각 개인의 그룹으로 서명되어야만 한다. 이러한 문제를 해결하기 위해 쓰레시홀드 서명안[3-5]과 멀티서명안[3, 6, 7]이 제안되었다. 쓰레시홀드 서명안과 멀티서명안의 주요한 차이점이 두가지 있다. 첫째 멀티서명안은 유효한 서명을 생성하기 위해 서명자의 수를 제한할 필요가 없다는 것이다. 쓰레시홀드 서명안은 멀티서명안과 반대로 쓰레시홀드 값 t가 시스템 보안을 위해 미리 결정되어야만 한다. 둘째 멀티서명안이 메시지를 서명하는 각 개인의 집합을 나타내는 서명인 반면, 쓰레시홀드 서명은 그룹에 의해 서명된 서명을 나타낸다.

따라서 (t, n) 쓰레시홀드 서명은 그룹의 구성원이 그룹을 대표하여 서명하는 서명 방법으로서 [4]에 의해 소개되었다. 즉 t 혹은 그 이상의 구성원들이 메시지를 서명할 수 있고, t-1 혹은 그 이하의 구성원들은 서명을 위조할 수 없다. 그러나 [8]에서 t 혹은 그 이상의 구성원이 공모를 한다면, 그들은 서명을 위조하기 위한 구성원들의 집합을 흉내낼 수 있다고 지적하였다. 이런 사실은 악의적인 구성원의 그룹이 어떠한 책임없이 서명을 위조할 수 있다는 것이다. 이는 $(t,$

† 종신회원 : 충남대학교 차세대통신인력양성사업단 BK전임교수
논문접수 : 2007년 3월 25일, 심사완료 : 2007년 5월 28일

n) 쓰레시홀드 서명안이 전통적 디지털 서명과 비밀 공유안이 결합한 것이기 때문에 t 혹은 그 이상의 구성원이 공모를 한다면, 그들은 서명을 위조하기 위한 구성원들의 집합을 흉내낼 수 있다는 사실이 당연하다.

중요한 원인은 (t, n) 쓰레시홀드 서명안에서 메시지를 서명하기 위해 사용된 비밀키가 비밀 공유안에서 shadow이기 때문이다. 비밀 공유안[9] 정의에 의하면, t 혹은 그 이상의 구성원이 쉽게 공유 비밀키를 얻을 수 있으므로 악의적인 t 혹은 그 이상의 구성원 그룹이 쉽게 다른 구성원 비밀키를 유도할 수 있다. 이 문제를 해결하기 위해 [8]에서 각 구성원이 가진 비밀키를 만들기 위해 shadow에 랜덤 수를 덧붙임으로써, 이 랜덤 수가 추적할 수 있는 (t, n) 쓰레시홀드 디지털 서명안을 만들어 준다. 따라서 위조가 의심되면 그 서명자들을 추적할 수 있다.

한편, 멀티서명안은 다중 비밀을 가진 다중 서명자들에 의한 서명을 생성할 수 있다[3]. 따라서 멀티서명안은 서명자들의 공개키들을 사용하여 검증되어야만 한다.

이러한 추적할 수 있는 멀티서명안과 그룹에 의해 서명된 (t, n) 쓰레시홀드 서명안을 결합하여 구성원들이 서로 결탁할 수 없고, 서명을 위조할 수 없는 새로운 (t, n) 쓰레시홀드 서명안이 [10]에서 제안되었다. 그러나 이러한 제안 방법은 신뢰된 그룹 관리자가 있어 그룹의 모든 구성원에게 안전한 shadow 분배와 그룹 비밀키를 결정해야만 한다.

그러나 현재의 유비쿼터스 환경에서는 언제 어디서나 안전한 전자거래가 가능해야 하므로 유비쿼터스 환경의 전자거래가 이루어질 때마다 신뢰된 그룹 관리자가 디지털 서명을 위한 매개변수를 정의하고 선택해야만 한다. 이러한 유비쿼터스 환경의 전자거래는 수많은 컴퓨팅 장치들이 통신을 하며, 필요에 따라 그룹을 만들기도 하고 해체하기도 하므로 신뢰된 그룹 관리자와 셋업 프로시져, 철회 프로시져 등이 필요없는 디지털 서명이 요구된다. 따라서 본 논문에서는 그룹 관리자, 셋업 프로시져, 비서명 구성원 등을 요구하지 않으며 유비쿼터스 환경의 전자거래에 알맞은, 익명성을 보호할 수 있는 링 서명[11]을 도입한다. 그러나 링 서명은 공격자의 위조 위험의 단점과 메시지가 다른 서명자에 의해 서명되는 것을 증명할 수 없는 단점을 가지고 있다. 이를 해결하기 위하여 본 논문에서는 새로운 쓰레시홀드 링 서명을 제안한다.

본 논문 구성은 2장에서는 링 서명에 대하여, 3장에서는 링 서명의 단점인 위조의 위험을 해결하는 링 서명에 대하여, 4장에서는 쓰레시홀드 링 서명에 관하여 서술한다. 그리고 5장은 유비쿼터스 전자거래 서비스를 위한 쓰레시홀드 링 서명을 제안하고, 6장 결론으로 이루어진다.

2. 링 서명

링 서명은 그룹 사용자들 중 각각의 키들을 가지고 있는 어떤 구성원에 의해 형성되는 디지털 서명의 한 형태로서, 서명 생성에 사용된 구성원 멤버 키가 누구의 것인지 판단하기 어려워야만 한다. 링 서명 정의를 살펴 보면 다음과 같다.

그룹 엔티티 각각은 공개키,비밀키 쌍 (P_{K1}, S_{K1}), (P_{K2}, S_{K2}), …, (P_{Kn}, S_{Kn})을 가진다고 가정한다. 파티 i는 입력(m, S_{Ki} , P_{K1} ,…, P_{Kn}) 으로 메시지 m에 관한 링 서명 σ를 계산할 수 있다. 이러한 링 서명의 유효성은 어느 누구나 확인할 수 있어야 하며, 어느 누구도 어떤 그룹의 비밀키를 알지 못한 채 어떤 메시지의 유효한 링 서명을 생성하기가 어려워야 한다.

이러한 링 서명은 그룹 서명과 비슷하나 두가지 키 방법에서 다르다.
첫째, 그룹 관리자가 없으므로 각각 서명의 익명성을 철회할 방법이 없고, 둘째, 사용자들의 어떤 그룹이 부가적인 셋업없이 즉흥적인 그룹으로서 사용될 수 있다. 링 서명 이름은 서명 알고리즘이 링과 같은 구조와 같은 데서 유래되었다.

전통적 그룹 서명과 다른점을 정리하면 다음과 같다.

1. 서명자는 어떤 메시지에 대해 그가 선택한 다른 사용자가 속해 있는 집합에 그의 이름을 올리고 이 집합에 속해 있는 익명자(사실은 자신)를 나타내는 링 서명을 생성한다. 이는 기존의 그룹 서명 정의에 의해 서명자가 그룹 멤버로 등록되는 것과 비교하면 불가능한 일이다. 특히 서명자가 아닌 멤버는 그가 그러한 서명에 속해 있는 것을 완전히 모른다.
2. 서명 폐지 관리자가 없는 것은 무조건적 익명을 허용한다. 이는 서명 폐지를 위해 인증 기관에 의해 사용된 트랩 도어 정보들이 있어야만 하는 기존의 그룹 서명에서는 이룰 수 없는 일이다.
3. 링 서명은 부가적인 셋업없이 매우 효과적으로 생성된다.

2.1 링 서명 역사

링 서명은 Rivest, Shamir, Tauman에 의하여 형식화되기 시작하였으며 아래와 같이 발전하였다.

2001(ASIACRYPT)

Rivest, Shamir, Tauman이 처음으로 링 서명 개념을 정립하여 RSA를 사용한 링 서명을 소개하였으며, 이는 RSA 가정 아래 이상적 암호모델에서 실제 선택된 메시지(적응성)가 안전하다는 것을 밝혔다[11].

2002(CRYPTO)

Bresson, Stern, Szydlo는 Rivest, Shamir, Tauman의 링 서명안을 수정하였다. 수정안은 RSA 가정 아래 랜덤 오라클 모델에서 실제 선택된 메시지(적응성)가 안전하다는 것을 증명하였다. 균등한 분할과 수정된 링 서명안을 사용하여 (t ,n)쓰레시홀드 링 서명안을 제안하였다. (t ,n)쓰레시홀드 링 서명안은 공격자가 t-1 서명자를 공격할 때, RSA 가정 아래 랜덤 오라클 모델에서 실제 선택된 메시지(적응성)가 안전하다는 것을 증명하였다[12, 13].

2002(CRYPTO)

Noar는 링 서명과 부인할 수 있는 인증을 결합하였다[14].

2002(ASIACRYPT)

Abe, Ahkubo, Suzuki는 링 구성원이 여러가지 서명안을 사용할 수 있도록 제시하였다. 어떤 예에서는 랜덤 오라클 모델에서 실제 선택된 메시지(적응성)가 공격에 안전하다는 것이 증명되었지만 일반적인 경우에서는 그렇지 않았다[15].

2003(Cryptology ePRINT Archive)

Herranz, Saez는 Schnorr 서명안을 바탕으로한 링 서명안을 제안하였다. 이 안은 이산대수 문제가 큰 소수(prime)의 큰 하위집단에 있다는 가정 아래, 랜덤 오라클 모델에서 실제 선택된 메시지(적응성)가 공격에 안전하다는 것이 증명되었다.

링 서명에 관한 더 많은 정보는 [16]에서 볼 수 있다.

2.2 링 서명 패러다임

링 서명자는 서명을 생성하기 위한 비밀키 S_K와 공개키 P_K를 가진다고 가정한다. 링 서명안은 서명을 생성하고 검증하기 위해 트랩도어 일방향 순열을 사용하며, 다음과 같은 두개의 프로시져로 구성된다.

• Ring sign

$(m, P_1, P_2, \cdots, P_r, s, S_s)$는 s번째 구성원의 비밀키 S_s와 r 링 구성원들의 공개키 $P_1, P_2, \cdots, P_r$ 이 주어졌을 때, 메시지 m의 서명 σ 를 생성한다.

• Ring verify

(m, σ)는 모든 가능한 서명자를 포함하는 메시지 m 와 서명 σ를 받아들여, "참" 혹은 "거짓"을 출력한다.

링 서명안은 셋업이 자유롭다. 즉 서명자는 링 구성원에 가입하려면 다른 링 구성원이 누구인지, 구성원의 동의, 보조 등이 필요없다. 필요한 것은 구성원들의 공개키만 알면 된다. 다른 구성원들은 다른 키와 서명 크기를 가진 독립된 공개키 서명안을 사용한다. 검증은 검증자가 $1/r$보다 큰 가능성을 가진 링 크기 r에서 서명자가 누구인지 결정할 수 없어야만 하며, 같은 링 구성원에 의해 생성된 메시지 서명 공격자는 그 링 구성원의 신원을 알 수 없을 뿐만 아니라 같은 서명자에 대한 부가적인 서명을 연결할 수 없어야만 한다.

• RSA 트랩도어 순열

링 구성원 A_i는 Z_{ni}의 트랩도어 일방향 순열 f_i 를 설명하는 RSA 공개키 $P_i=(n_i,e_i)$를 가진다.

$$f_i(x)=x^{ei} \pmod{n_i}$$

링 구성원 A_i만이 트랩도어 정보를 사용하여 어떻게 효과적으로 역 순열을 계산할 것인가를 안다. 이것은 공개키 암호를 위한 Diffie-Hellman 모델의 원리다.

여러 링 구성원의 트랩도어 RSA 순열은 다른 크기의 변역을 가진다 (모듈 n_i가 같은 비트수일지라도). 이것은 각 서명을 결합하기 어렵게 만들어, 모든 트랩도어 순열을 같은 집합 $\{0,1\}^b$ 변역(2^b는 모든 모듈 n_i 보다 큰 멱이다)으로 하기 위해 확장한다.

Z_{ni} 위의 각 트랩도어 순열 f_i 를 위하여, 다음과 같은 방법으로 $\{0,1\}^b$ 위의 확장된 트랩도어 순열 g_i를 정의한다.

b비트에 대한 입력 m은 $m=q_i\, n_i+r_i$와 $0 \le r_i < n_i$ 를 만족하기 위해 양의 정수 q_i와 r_i를 정의한다.

$$g_i(m)= q_i\, n_i + f_i(r_i) \quad \text{if } (q_i+1)\, n_i \le 2^b$$
$$\text{else } g_i(m)= m$$

여기서 f_i 역함수를 어떻게 구하는지 아는 사람만이 효과적으로 g_i 역함수를 구할 수 있기 때문에 함수 g_i는 $\{0,1\}^b$ 위의 순열이며 일방향 트랩도어 순열이다.

• 대칭 암호

길이 ℓ인 키 k의 대칭 암호 알고리즘을 가정한 함수 E_k는 b비트 스트링의 순열이다. 그리고 모든 파티들은 $E_k(x)$와 $E_k^{-1}(y)$의 새로운 쿼리에 대한 램덤 대답을 제공하는 오라클에 접근할 수 있는 램덤 오라클 모델을 사용한다.

• 해쉬 함수

길이 ℓ인 스트링에 대한 임의의 입력에 사상하는 충돌회피 해쉬함수 h를 정의하고, 이는 E의 키로서 사용된다.

• 결합 함수

결합 함수 $C_{k,v}(y_1, y_2,\cdots,y_r)$은 입력 키 k, 초기값 v, $\{0,1\}^b$ 위의 임의값 $y_1, y_2,\cdots,y_r$ 을 갖는다. 결합함수는 서브 프로시져로서 E_k 함수를 사용하여 고정된 값 k와 v를 위한 $\{0,1\}^b$의 z를 출력하여 다음과 같은 특성을 가진다.

1. 각 입력에 대한 순열

모든 다른 입력 y_i의 고정된값에 대하여 $i \neq s$, $1 \le s \le r$ 인 함수 $C_{k,v}$는 y_r에서 z로 일대일로 사상한다.

2. 단일 입력에 대한 효과적인 해결

y_s를 제외한 모든 입력 y_i를 위한 값과 b비트 값 z 가 주어지면(단, $1 \le s \le r$)

$C_{k,v}(y_1, y_2,\cdots,y_r) = z$ 인 y_s를 위한 b비트 값을 효과적으로 찾는 것이 가능하다.

3. 트랩도어가 없다면 모든 입력에 대한 불가능한 검증식

k, v, z 가 주어지고 공격자가 트랩도어 함수 $g_1, g_2,\cdots,g_r$의 역함수를 구할 수 없다면 $x_1, x_2,\cdots,x_r$ (각 g_i와 E_k 의 접근) 를 위한

$$C_{k,v}(g_1(x), g_2(x_2), \cdots,g_r(x_r)) = z \qquad (1)$$

(1) 등식 풀기가 불가능하다.

여기서 모든 모듈 n_i 가 같은 크기 b를 가지는 RSA 트랩도어 함수 $g_i(x_i)= x_i^{3} \pmod{n_i}$를 가정한다. 9개의 RSA 순열 중 어떤 하나도 역함수를 구하지 않고

$(x_1^3 \bmod n_1)+ (x_2^3 \bmod n_2)+\cdots\cdots+(x_9^3 \bmod n_9)=z(\bmod 2^b)$

의 검증식을 풀 수 있다.
따라서 결합함수 $C_{k,v}$ $(y_1, y_2,\cdots,y_r)$ 는 대칭 암호 함수 E_k 를 다음과 같이 활용할 수 있다.

$$C_{k,v}(y_1, y_2,\cdots,y_r) = E_k(y_r \oplus E_k(y_{r-1} \oplus E_k(\cdots \oplus E_k(y_1 \oplus v)\cdots)))$$

결합함수는 그림 1에서와 같이 $y_i = g_i(x_i)$인 $y_1, y_2, \cdots, y_r$에 적용되며, 결과 함수는 랜덤 오라클 모델에서 안전하다.

2.3 링 서명 생성 및 검증

• 링 서명 생성

서명자는 메시지 m, 모든 구성원의 공개키 $P_1, P_2, \cdots, P_r$, 비밀키 S_s를 가지고 다음과 같이 링 서명을 계산한다.

1. 키 선택

서명자는 먼저 메시지 m의 해쉬로 대칭키 k를 계산한다.

$$k=h(m)$$

2. 랜덤 초기값

서명자는 $\{0,1\}^b$에서 랜덤 초기값 v를 선택한다.

3. 랜덤 x_i's

서명자는 $\{0,1\}^b$로부터 모든 링 구성원들을 위한 독립적이고 유일한 x_i $(1 \le i \le r,\ i \neq s)$를 선택한다.

$$y_i = g_i(x_i)$$

4. y_s 풀기

$$C_{k,v}(y_1, y_2,\cdots,y_r) = v$$

다른 입력에 대한 임의의 값이 주어진다고 가정하면, 등식을 만족하는 유일한 y_s가 있어 효과적으로 계산된다.

5. 서명자의 트랩도어 순열 역함수 구하기

서명자는 x_s를 얻기 위하여 y_s의 g_s 역함수를 구하기 위한 트랩도어를 사용한다.

$$x_s = g_s^{-1}(y_s)$$

6. 링 서명 출력

메시지 m의 서명은 $(2r+1)$-tuple로 정의된다.

$$(P_1, P_2, \cdots, P_r ; v ; x_1, x_2,\cdots,x_r)$$

• 링 서명 검증

검증자는 메시지 m에 대한 서명 $(P_1, P_2, \cdots, P_r ; v ; x_1, x_2, \cdots, x_r)$를 검증할 수 있다.

1. 트랩도어 순열 적용

검증자는 $i = 1, 2,\cdots, r$에 대하여 $y_i = g_i(x_i)$를 계산한다.

2. k 구하기

검증자는 암호키 k를 계산하기 위해 메시지를 해쉬한다.

$$k=h(m)$$

3. 링 등식을 검증한다.

검증자는 y_i가 다음 등식을 만족하는지 체크한다.

$$C_{k,v}(y_1, y_2,\cdots,y_r) = v$$

이 만족하면 검증자는 유효한 서명으로 받아들이고, 그렇지 않으면 거절한다.

서명자는 먼저 v를 선택하여 시계 도는 방향으로 i_s -1의 1부터 시작하여 링을 돌고, 시계 반대 방향으로 i_s +1의 r에서 링을 돈다.
이때 트랩도어는 x_{is}의 근을 구할 수 있게 한다.
링 서명은 미리 링 멤버쉽이 알려지지 않기 때문에 서명의 부분으로 제공되어야만 한다. 따라서 [11]는 키와 함께 임의의 순열에 의해 모델화된 대칭형 암호를 바탕으로한 결합함수를 제안하였다.

링 서명[11]에서 결합 함수 $C_{k,v}(y_1, \cdots, y_r)$는 입력 키 k와 초기화 값 v, 그리고 같은 길이 ℓ의 임의 값을 가진다. $C_{k,v}$는 k, v, 인덱스 s, 그리고 고정된 값 $\{y_i\}i\neq s$에 대해 $z\in\{0,1\}^\ell$를 출력하는 $\{0,1\}^\ell$의 순열이다.

$$z = C_{k,v}(y_1,\cdots,y_r)=E_k(y_r \oplus E_k(y_{r-1} \oplus E_k(\cdots \oplus E_k(y_1 \oplus v)\cdots))) \quad (2)$$

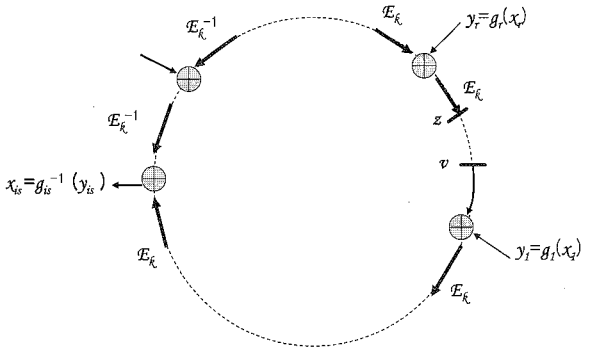
인덱스 s에 관해 다음과 같이 (2)식을 다시 정리함으로써 $C_{k,v}$가 결합 함수라는 것을 쉽게 검증할 수 있다.

$$y_s = E_k^{-1}(y_{s+1} \oplus \cdots E_k^{-1}(y_r \oplus E_k^{-1}(z))) \oplus E_k(y_{s-1} \oplus \cdots E_k(y_1 \oplus v)\cdots))$$

E는 $\{0,1\}^\ell$에 정의된 대칭 암호이며, E에 대한 대칭키를 정의하기 위해 해쉬함수 H를 사용한다.
메시지 m에 대한 링 서명은 $(v, x_1,\cdots,x_r)$을 구성하며, $z=C_{k,v}(f_1(x_1),\cdots, f_r(x_r))$를 셋팅함으로써 서명이 $z= v$이면 유효하다.

이러한 링 서명의 위조 방지는 확장된 RSA 순열 g_i의 역함수를 구하기 어려움에 있다. 즉 $y\in\{0,1\}^\ell$이 주어지고 ℓ 비트 세제곱근을 얻기 위해 링을 따라 두 개의 연속적인 E 함수 사이에 "틈새(gap)"로 y를 삽입한다. 그렇게 함으로써 E함수 입력과 출력 사이에 exclusive OR가 y에 놓여진다. 이러한 삽입으로 인덱스 i에서 도착 쿼리(query)는 다른 도착 쿼리가 시작한 후 질문을 받는다. 이러한 경우는 항상 위조의 위험에 있다.

따라서 링 서명은 링 등식이 시계 방향으로 가기 위한 인덱스 1보다 다른 시작점에서 검증되어야 한다. 예를 들면 서명자는 서명 내의 인덱스 i_0를 선택하여 링 등식 $E_k(y_{io} \oplus v) \oplus \cdots$를 시작해야만 한다. 이러한 간단한 수정은 E가 랜덤 순열이라는 가정을 제거해야만 한다. 따라서 해쉬 함수인 $H(m,x)$에 의해 $E_{H(m)}$ 로 대치할 수 있다[13].



(그림 1) 링 서명 패러다임

3. 수정된 링 서명 패러다임

링 서명 패러다임과 다른 점은 서명자 P_s는 자신의 인덱스 i_s로부터 시작하여 링을 따라 연속적인 값을 계산한다는 것이다. 이는 틈새의 삽입이 인덱스 i에서 다른 도착 쿼리가 시작한 후 도착 쿼리가 질문을 받으므로 항상 위조의 위험에 있기 때문에 이를 해결하기 위한 것이다.

먼저 램덤 시드 σ를 선택하여 링을 따라 가서 m||σ를 해쉬하여 $g_{is+1}(x_{s+1})$와 함께 XOR한다. 인덱스 n+1가 1이다는 것을 고려하여 다음과 같은 연속적인 값을 나타낸다.

$v_{is+1}=H(m, \sigma)$ $\qquad$ $v_{is+2}=H(m, v_{is+1} \oplus g_{is+1}(x_{s+1}))$

$\cdots\cdots\cdots\cdots$ $\qquad$ $v_{is}=H(m, v_{is-1} \oplus g_{is-1}(x_{s-1}))$

서명자는 링을 닫기 전에 마지막 입력을 얻기 위해 자신의 비밀키를 사용하여, $v_{is} \oplus g_{is}(x_{is})=\sigma$와 같은 x_{is}를 계산한다. 즉, 서명자는 자신의 인덱스 i_s와 시드(seed)값 σ으로 시작하여 그의 트랩도어를 사용하여 v_{is}를 계산할 때 링을 닫는다.

틈새는 $z=v$ 대신 $z=v \oplus E_k(0)$로 위조자가 위조할 수 없게 한다.

즉, 틈새 γ은 ℓ-bit 틈새값으로 $\gamma=0$일 때 $\gamma=E_k(0)$로 표현되며, z와 v 사이의 틈새로서 i_r 위치에서 두개의 연속적인 인덱스 사이의 틈새이다. 검증자는 인덱스 i_r 에서 해쉬하기 전 v_{ir} 대신 $v_{ir} \oplus \gamma$로 대치한 후 링을 돈다.

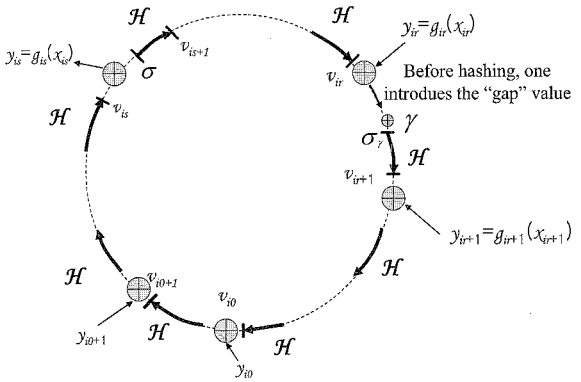
수정된 링은 그림 2와 같다.

검증자는 값 v_{i0}를 가진 i_0부터 시작하여 마지막 해쉬가 v_{i0}를 출력하는지를 검사한다.

시뮬레이터는 i_r과 링을 닫을 때만 γ를 정의하는 시드 σ_r로부터 시작하여 v_{ir}를 계산한다. 이때 H는 공개적인 해쉬 함수이다.

인덱스 i_r에서 발생하고 인덱스 i_0에서 시작하는 주어진 틈새값 γ은 수정된 결합 함수를 $C_{v,i0,m}$로 표기한다.

$$C_{v,i0,m}(i_r, \gamma, y_1, \cdots, y_n) = H(m, y_{i0-1} \oplus H(m, y_{i0-2} \oplus \cdots \underbrace{H(m, \gamma \oplus y_r \oplus H(\cdots \oplus H(m, y_{i0} \oplus v)\cdots))\cdots)}_{v_{ir+1} \text{ is computed from } \gamma \oplus y_r \oplus v_{ir}}$$



(그림 2) 수정된 링 서명 패러다임

링 등식은 $C_{v,i0,m}(.)=v$인지 검증하며, 틈새값을 가지는 수정된 링 서명은 [9]에서 주어진 정의를 일반화하여 $i_0=i_r=1$, $\gamma=0$을 가진다.

본 논문에서, 검증자는 항상 1부터 시작하여 i_0는 고정되어 있으며, 틈새가 인덱스 n과 1 사이에 나타나는 i_r 역시 고정되어 $v_1=H(v_n \oplus y_n \oplus \gamma)$ 이다는 것을 가정한다.

그림 2에서 서명자 P_s는 시드 σ_r를 사용하여 $y_s=C_{s,r,m}^{-1}(\sigma_s, y_1, \cdots, y_n)$를 계산한다.

따라서 i_r를 생략한 $C_{v,i0,m}(\gamma, y_1, \cdots, y_n)$을 사용하여

$$C_{v,i0,m}(\gamma, y_1, \cdots, y_n)=v$$

이면 검증자는 링 서명을 받아들인다[13].

그러므로 수정된 링 서명으로 공격자의 위조 위험을 막을 수 있지만, 다른 서명자에 의해 서명되는 메시지를 증명할 수가 없다. 이를 해결하기 위해 쓰레시홀드 링 서명을 제안한다.

4. 쓰레시홀드 링 서명(Threshold ring signature)

쓰레시홀드 링 서명은 t명 사용자들(자발적으로 등록된)이 있는 어떤 그룹이 n명이 있는 전체 그룹을 대신하여 공개적으로 검증 가능한 n에서 t서명을 생성할 수 있는 서명 방법으로서, 어떤 그룹의 멤버쉽을 모른 채 최소 사용자들이 서명을 생성하기 위해 서로 협력하는 서명 방식이다.

t명의 사용자들이 어떤 중요한 정보를 누설하기를 원한다고 가정하면, 어떤 검증자는 선택 그룹의 적어도 t명의 사용자들이 그 유효성을 입증해야만 한다는 것을 납득시켜야 한다.

분명, t 링 서명은 메시지가 다른 서명자에 의해 서명되는 것을 증명할 수 없다. 이러한 문제점을 해결하기 위해 쓰레시홀드 링 서명을 도입한다.

쓰레시홀드 링 서명은 어떤 그룹의 최소 사용자들이 부분 그룹의 정확한 멤버십을 숨긴 채 서명을 생성하기 위해 협력해야만 한다는 것을 효과적으로 증명한다[13].

4.1 쓰레시홀드 링 서명 개요

쓰레시홀드 링 서명안은 두개의 알고리즘으로 구성된다.

• T-ring-sign 알고리즘

입력 메시지 m에 대하여 n 공개키들을 가진 n 사용자들의 링과 t 구성원들의 비밀키들은 메시지 m에 대한 (t, n)-링 서명 σ를 출력한다.
이러한 σ은 링 구성원과 관련된 n 공개키들 뿐만 아니라 t 값을 포함한다.

• T-ring-verify 알고리즘

입력 메시지 m과 서명 σ에 대하여, T-ring-verify 알고리즘은 "참" 혹은 "거짓"을 출력한다.

효과적인 쓰레시홀드 링 서명을 위해 다음을 고려한다. r 구성원의 링과 링 서명을 생성하기 위해 서로 협력하고 있다는 것을 나타내기 원하는 r 구성원 중 두 사용자를 고려하기로 하자 .

먼저, 그룹을 2개의 부분 그룹으로 분리하여 이러한 부분 그룹의 각각이 한 서명자를 포함하고 있다는 것을 보인다. 그러나 그렇게 하는 것은 완전한 익명성에 대하여 손상을 입힌다. 왜냐하면 그러한 분리는 각 사용자의 익명성을 sub-ring에 제한을 주기 때문이다.

그 해결책은 그룹을 여러 번 분리하는 것으로 두 사용자들은 반드시 다른 sub-ring에 있는 분리이어야 한다. 이러한 분리들은 super-ring에 있는 노드들로 사용된다.
Super-ring은 적어도 하나의 분리로 해결된다는 것을 증명한다. 즉 두개의 sub-rings은 각각으로 해결되고, 다른 분리들(모든 해결되지 않은 sub-ring)에 대해서는 정확한 링 서명을 시뮬레이터해야만 할 것이다.

따라서 본 논문에서의 서명 방법을 제안하기 전에 링의 공평한 분할에 대하여 살펴 보기로 한다.
두 정수 $t < n$이 있다면, $[1,n]$의 분할을 가지고 있는 집합 Π는 다음을 만족하면 (n, t) 완전 분할 시스템이 된다. 즉 $[1,n]$ 범위에 있는 인덱스 t를 가진 집합 $I=\{i_1, \cdots, i_t\}$에 대하여 Π에 공평한 분할이 존재한다면.

$$\forall\ I \subset [1,n],\ \#(I)=t,\ \exists\ \pi=(\pi^1, \cdots, \pi^t) \in \Pi,\ \forall j \in [1,t],\ \#(I \cap \pi^j)=1$$

이러한 시스템의 완전성을 증명하기 위하여 완전한 해쉬 함수를 사용한다.
집합 I의 완전한 함수는 h에 사상(mapping)한다: I에 1-1 대응하는 $[1,n] \rightarrow [1,t]$ 완전한 해쉬 함수의 (n,t)-family H는 크기 t인 I에 대하여 I 에 완전한 $h \in H$가 존재한다.

그러므로 (n,t)-family의 각 구성원에 대한 t sub rings에 있어서 분할을 정의하는 것은 (n,t) 완전한 분할 시스템을 만든다.

4.2 (n, t) 링 서명

(n, t) 링 서명은 RSA 기반으로 공평한 분할과 완전한 해쉬 함수를 사용한다.
t 링 멤버가 메시지에 서명하기를 원한다고 가정하면, 각각의 서명자가 있는 분리된 sub-rings로 분할되어 각각의 서명자는 메시지에 서명할 수 있다. sub-rings가 서로 분리되어 있으므로 t 서명의 검증은 서로 다른 t 링 사용자들이 메시지에 서명하였다는 것을 보인다.

따라서 서명자 익명성이 각 sub-ring 내에서 줄어들기 때문에 하나 이상의 분할이 필요하다. 그리고 메시지에 서명하는 t 사용자들의 새로운 분할을 피하기 위하여 t 서명자들을 위해 적어도 하나의 분할만 존재해야만 한다. 이러한 sub-rings의 분할은 super-ring의 nodes로 사용된다. 서명자들이 없는 sub-rings에 대해서는 시뮬레이션 알고리즘을 사용하여 시뮬레이션된다. sub-ring 서명의 틈새값은 super-ring에서 사용되며, super-ring이 종료될 때 모든 sub-rings 서명들의 틈새값이 정의된다. 그래서 유효한 링 서명은 마지막 파티션의 각 sub-ring에서 생성되어야만 한다. 이러한 것은 각 sub-ring에 서명자가 있을 때만 수행될 수 있다.

따라서 각 서명자가 sub-ring에 있을 때만 수행됨으로 메시가 다른 서명자에 의해 서명되는 것을 증명할 수 없는 t 링 서명 단점을 해결할 수 있다.

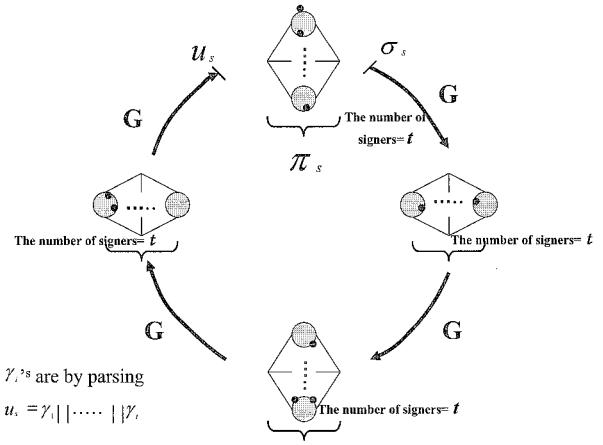
쓰레시홀드 시나리오의 경우에서 공평한 분할을 기본으로 한, t 서명자들의 집합과 (n,t)-완전한 분할 시스템을 고려하기로 한다.
π가 이러한 집합에 대한 공평한 분할이라면, π에 의해 정의된 모든 sub-rings을 해결할 수 있다. 다른 분할에 대해서는 sub-rings가 시뮬레이션되고 super-ring에 따라서 배치된다. 쓰레시홀드 서명은 $t2^t \log n$의 sub-ring 시뮬레이션을 요구하며, 각 sub-ring은 n/t 구성원을 가지고 하나의 super-ring 서명 생성을 가진다.

또 다른 함수 G는 $(t \times \ell)$-bit 스트링을 반환하는 임의의 해쉬 함수로 보고, $p=2^t \log n$ 를 나타낸다.
모든 정수 n과 $t <= n$에 대하여, (n,t)-완전한 분할 시스템은 공개적으로 이용할 수 있다고 가정한다: $\Pi_n=\{\pi_1, \cdots, \pi_p\}$ Sub-rings를 다루기 위해 $C_{v,i0,m}$ $(\gamma, y_j, j \in R)$를 도입한다.
인덱스 i_r에서 발생하고 인덱스 i_0에서 시작하는 주어진 틈새값 γ이 $C_{v,i0,m}$ $(i_r, \gamma, y_1, \cdots, y_n)$로 표현되어 $C_{v,i0,m}(.) = v$인지 검증한다.

5. 제안된 쓰레시홀드 링 그룹 서명

유비쿼터스 전자거래에 적합한 디지털 서명인 링 그룹 서명은 무결성과 인증을 만족하는 그룹 서명이지만, 위조의 위험과 다른 서명자에 의해 서명된 메시지를 증명할 수 없는 단점을 가지고 있다. 이를 해결하기 위해 본 논문에서는 위조의 위험을 해결하기 위한 3장의 수정된 링 서명(무결성)과 메시지가 다른 서명자에 의해 서명된 것을 증명할 수 없는 단점을 해결하기 위한 4장의 쓰레시홀드 링 서명(인증)을 사용한다.

수정된 링 서명은 틈새의 삽입이 인덱스 i에서 다른 도착 쿼리가 시작한 후 도착 쿼리가 질문을 받으므로 항상 위조의 위험에 있기 때문에 이를 해결하기 위해, 서명자 P_s는 자신의 인덱스 i_s로부터 시작하여 링을 따라 연속적인 값을 계산한다. 따라서 수정된 링 그룹 서명의 검증자는 $C_{v,i0,m}$ $(\gamma, y_1, \cdots, y_n)= v$를 확인하여 서명의 유효성을 결정한다. 한



(그림 3) 쓰레시홀드 링 패러다임

편 쓰레시홀드 링 그룹 서명은 $C_{v,i0,m}(i_r, \gamma, y_1, \cdots, y_n) = v$를 확인하여 유효성을 결정함으로써, 쓰레시홀드 링 그룹 서명이 인덱스 i_r를 참고로 한다는 것이 수정된 링 그룹 서명의 검증과 다른 점이다. 이는 다른 서명자에 의해 서명된 메시지를 증명할 수 있도록 인덱스 i_r에서 발생한 인덱스 i_0에서 시작하는 주어진 틈새값 γ이 $C_{v,i0,m}(i_r, \gamma, y_1, \cdots, y_n)$로 표현되어 $C_{v,i0,m}(.) = v$인지 검증할 수 있다.

5.1 서명 알고리즘

n 링 구성원들 중 적어도 t 서명자가 메시지 m에 대하여 서명하기를 원하는 부분 집합을 $P_{i1}, \cdots, P_{it}$라고 표시한다. 이것은 공평한 분할과 일치하는 부분 링 서명들을 해결하는 것으로서, 부분 링의 적어도 하나가 전체적으로 해결되기 위하여 링과 같은 구조를 적용하여 그 결과를 연결하는 것이다. 그렇게 하기 위해서 다음과 같이 진행한다: π_s는 $I=\{i_1, \cdots, i_t\}$를 위한 공평한 분할이고, 각 $j \in [1,t]$에 대하여 $i_j \in \pi_s^j$ 를 가진다.

1. 각 파티션의 각 sub-ring에 대한 임의의 시드(seed)를 선택한다.

For $i=1,\cdots, p$, Do
For $k=1,\cdots,t$, Do $v_i^k \xleftarrow{R} \{0,1\}^\ell$

2. π_s를 제외한 모든 파티션을 위한 링들을 시뮬레이션한다.

For $i=1,\cdots, p$, $i \neq s$, Do
For $j=1, \cdots, n$, Do $x_i^j \xleftarrow{R} \{0,1\}^\ell$, and $y_i^j \leftarrow g_j(x_i^j)$
For $k=1, \cdots, t$, Do
$z_i^k \leftarrow C_{v i,1,m}^k(0, y_i^j, j \in \pi_i^k(R))$ and $\gamma_i^k \leftarrow v_i^k \oplus z_i^k$

3. 틈새를 가진 super-ring을 계산한다.

$\sigma_s \xleftarrow{R} \{0,1\}^{t\ell}$, and $u_{v+1} \leftarrow G(\sigma_s)$
For $i=s+2, \cdots, p, 1, \cdots, s$, Do
$u_i \leftarrow G(u_{i-1} \oplus (\gamma_{i-1}^1 || \cdots || \gamma_{i-1}^t))$

4. super-ring을 종결한 후 sub-ring π_s 틈새값을 계산한다.

$(\gamma_s^1 || \cdots || \gamma_s^t) \leftarrow u_s \oplus \sigma_s$

5. 균일한 파티션 π_s를 위한 sub-ring을 설명한다.

For $j \in [1,n] \setminus I$, Do $x_s^j \xleftarrow{R} \{0,1\}^\ell$, and $y_s^j \leftarrow g_j(x_s^j)$
For $j \in I$, Do
$\sigma_k \xleftarrow{R} \{0,1\}^\ell$ for k such that $j \in \pi_s^k$
$y_s^j \leftarrow C_{j,s,m}^{-1}(\sigma_k, y_s^j j \in \pi_s^k(R))$ and $x_s^j \leftarrow g_j^{-1}(y_s^j)$

6. 서명을 출력한다.

$\nu \xleftarrow{R} [1,p]$ and output $(\nu, u_\nu, \bigcup_{1 \le i \le p}(\chi_i^1, \cdots, \chi_i^n, \upsilon_i^1, \cdots, \upsilon_i^t))$

5.2 검증 알고리즘

1. 인덱스 1에서 시작하는 모든 링들을 계산한다.

For $i=1,\cdots, p$, Do
For $j=1,\cdots,n$, Do $y_i^j \leftarrow g_j(x_i^j)$
For $k=1,\cdots,t$, Do
$z_i^j \leftarrow C_{v_i^k,1,m}^k(0, y_i^j, j \in \pi_i^k(R))$, and $\gamma_i^k \leftarrow \upsilon_i^k \oplus z_i^j$

2. 인덱스 υ와 틈새로부터 super-ring을 검증한다.

$u_\upsilon \overset{?}{=} G(\gamma_{\upsilon-1}^1 || \cdots || \gamma_{\upsilon-1}^t \oplus G(\cdots G(\gamma_\upsilon^1 || \cdots || \gamma_\upsilon^t \oplus u_\upsilon) \cdots))$

쓰레시홀드 링 그룹 서명은 링 구성원수 n과 서명자수 t가 많을수록 서명 크기가 커진다.
즉 (t, n) 링 서명 크기는 $2^{o(t)}[\log_2 n] \times (t*\ell + n*\ell) = O(\ell 2^t n\log n)$로서, 서명은 g함수의 t 역과 $O(2^t n\log n)$ 계산을 요구한다. 이는 일반적인 해결 방법인 $\binom{n}{t} = o(n^t)$ 크기보다 효율적이다[13].

6. 결 론

유비쿼터스 환경의 전자거래를 통하여 사용자는 언제 어디서나 네트워크에 접근하여 편리한 정보를 개인과 그룹, 그룹과 그룹 사이에서 교환할 수 있다. 그러나 사용자가 이러한 유비쿼터스 전자거래를 안전하게 사용하기 위해서는, 유비쿼터스 전자거래가 디지털 서명을 만족해야만 한다. 디지털 서명의 가장 중요한 특성은 무결성과 인증이다. 한편, 유비쿼터스 환경은 언제 어디서나, 필요에 따라 그룹을 만들기도 하고 해체하기도 하므로, 유비쿼터스 전자거래는 신뢰된 그룹 관리자와 셋업 프로시져, 철회 프로시져 등이 필요없는 디지털 서명이 요구된다. 따라서 본 논문에서는 유비쿼터스 전자거래 서비스를 위한 안전한 디지털 서명으로서 쓰레시홀드 링 서명을 제안하였다.

제안한 쓰레시홀드 링 서명은 그룹 관리자, 셋업 프로시져, 비서명 구성원 등을 요구하지 않는다. 따라서 본 논문은

익명성을 보호할 수 있는 링 서명[11]을 도입한 후, 링 서명의 단점인 공격자의 위조 위험(무결성 문제)과 메시지가 다른 서명자에 의해 서명되는 것을 증명할 수 없는 문제(인증 문제)를 해결하였다.

또한 제안한 쓰레시홀드 링 서명은 개인의 프라이버시 보호와 밀접한 익명성 보호에 관련된 분산 암호인 쓰레시홀드 암호학을 바탕으로한 것으로서, 전통적인 쓰레시홀드 서명보다 효율적이다. 즉, (t, n) 링 서명 크기는 $2^{o(t)}[\log_2 n] \times (t*\ell+n*\ell)=O(\ell 2^t\ n\log n)$로서, 서명은 g함수의 t 역과 $O(2^t\ n\log n)$ 계산을 요구함으로 일반적인 해결 방법인 $\binom{n}{t}=O(n^t)$ 크기보다 효율적이다.

그러나 제안한 쓰레시홀드 링 그룹 서명은 링 구성원수 n과 서명자수 t가 많을수록 서명 크기가 커진다. 링 서명 생성시 가정에서 공개키 $P_1, P_2,\cdots, P_r$가 주어지고 링 서명 $(P_1, P_2,\cdots,P_r ; v ; x_1, x_2,\cdots,x_r)$이 생성되므로 그룹 구성원의 크기가 증가하면 공개키의 수와 서명 크기도 증가하게 된다. 따라서 아주 큰 그룹일 경우, 그룹 크기에 독립적인 공개키 수와 서명 크기가 요구된다.

참 고 문 헌

[1] R.L.Livest, A. Shamir and L. M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.

[2] National Institute of Standards and Technology(NIST), "The digital signature standard, proposal and discussion," Communications of the ACM, Vol.35, No.7, pp.36-34, 1992.

[3] L. Harn, "Group oriented(t,n) threshold digital signature scheme and digital multisignature," in IEE Proceedings of Computer and Digital Techniques, Vol.141, No.5, pp.307-313, 1994.

[4] Y. Desmedt and Y. Frankel, "Shared generation of authentication and signatures," Advances in Cryptology-CRYPTO'91, pp.457-469, 1991.

[5] C. Li, T. Hwang and N. Lee, "Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders," Advances in Cryptology Proceedings of EUROCRYPT'94, pp.413-419, 1994.

[6] T. Hardjono and Y. Zheng, "A practical digital multisignature scheme based on discrete logarithm," Advances in Cryptology-Proceedings of Asiacrypto'92, pp.16-21, 1993.

[7] L. Harn and T. Kiesler, "New scheme for digital multisignatures," Electronics Letters, Vol.25, No.15, pp.1002-1003, 1989.

[8] C. Li, T. Hwang and N. Lee, "Remark on the threshold RSA signature scheme," Advances in Cryptology-CRYPTO'93, Lecture Notes in Computer Science, Vol.773, pp.413-420, 1994.

[9] A. Shamir, "How to share a secret," Communications of the ACM, Vol.22, No.11, pp.612-613, 1979.

[10] Wei-Bin Lee and Chin-Chen Chang, "(t,n) Threshold Digital Signature with Traceability Property," Journal of Information Science and Engineering 15, pp.669-678, 1999.

[11] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," In Asiacypt'01, LNCS 2248, pp.552-565.

[12] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad hoc groups," http://www.di.ens.fr/~bresson/.

[13] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," Advances of Cryptology-CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, Springer-Verlag, pp.465-480, 2002.

[14] M. Noar, "Deniable ring authentication," Advances of Cryptology-CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, Springer-Verlag, pp.481-498, 2002.

[15] M. Abe, M. Ohkubo, and K. Suzuki, "1-out of-n signatures from a variety of keys," Advances of Cryptology-ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, Springer-Verlag, pp.415-432, 2002.

[16] J. Herranz and G. Saez, "Forking lemmas in the ring signatures' scenario," Cryptology ePrint Archive, April 2003.

성 순 화

e-mail : shsung@cnu.ac.kr

1983년 경북대학교 전자공학과(전산학)(공학사)

2000년 한남대학교 컴퓨터공학과(공학석사)

2005년 충남대학교 컴퓨터공학과 (공학박사)

2000년~2004년 대덕대학 겸임교수

2002년~2005년 충남대학교 시간강사

2006년 충남대학교 부설 정보통신연구소 연구원

2006년~현 재 충남대학교 차세대통신인력양성사업단 BK전임교수

관심분야 : 정보 보안, 유비쿼터스 컴퓨팅 보안, 유무선 인터넷 보안, 유무선 인터넷 트래픽 솔루션, 차세대 인터넷을 위한 사용자 인증 시스템