일방향 키 분배 기능을 가지는 유연한 키 복구 시스템

유 준 석[†]·김 희 도[††]·전 종 민[†††]·원 동 호[††††]

요 약

급속한 암호의 민간 부문 확산에 따라 암호 사용으로 인한 부작용을 방지하기 위한 대책으로 키 복구에 대한 연구가 활발히 진행되고 있다. 그러나 지금까지 제시된 기존의 키 복구 기술들은 그 대부분이 정부의 법 집행권 보장에만 설계 초점을 맞추고 있기 때문에 다양한 사용자들의 요구를 충족시키기 어렵다. 본 논문에서는 키 복구 시스템에 대한 사용주체들의 입장을 고려하여 다양한 환경에서 사용할 수 있는 키 복구 시스템을 제안한다. 제안하는 방식은 암호통신 과정 중에 키가 분배되는 일방향 키 분배가 가능하고 기존의 시스템만큼 효율적이며, 충분한 유연성을 제공한다.

A Flexible Key Recovery System with One-way Key Distribution Property

Joon-Suk Yu[†] · Hee-Do Kim[††] · Jong-Min Jeon[†††] · DongHo Won[††††]

ABSTRACT

Many studies on the key recovery as a countermeasure for the side effects caused by rapid spread of cryptographic technology to private fields are going on. The majority of existing key recovery systems, however, have focused on law surveillance and so it is hard to meet the all requirements of entities using the system. In this paper, we examine various viewpoints about key recovery and propose a key recovery system which can be employed in various environments. The proposed key recovery system has one-way key distribution property. In addition, it is as efficient as existing ones and provides enough flexibility.

키워드 : 키 복구(Key recovery), 키 위탁(Key escrow), 키 캡슐화(Key encapsulation), 일방향 키 분배(one-way key distribution)

1. 서 론

현대 사회가 고도의 정보화 사회로 발전해 가면서 다양한 정보의 개방과 공유, 네트워크를 통한 업무 처리라는 무한한 가능성과 편리함을 제공하였으나, 정보의 침해라는 문제를 발생시켰다. 이로 인하여 정보보호 문제가 부각되었으며, 군사적 용도나 국가적 차원에서 주로 이용되던 암호 기술의 사용이 민간 부문으로 급속히 확대되었다.

암호의 사용은 정보의 기밀성 및 무결성을 보장해 주며, 인증 기능 등을 제공해 줌으로써 상거래나 결제 등과 같은 현실세계의 일들이 전자적으로 실현될 수 있게 하여 일반 사용자들에게 많은 편리함과 이점을 제공한다. 그러나 암호 기술이 범죄자에 의해 악용될 경우에는 사회의 안전을 위협할 수 있으며, 암호키가 손상되거나 분실되었을 경우에는 암호문의 소유자라도 암호문을 복호할 수 없는 등의 문제점이 존재한다.

키 복구(Key Recovery)는 이와 같은 암호 사용에 따른 부작용을 해결하기 위한 여러 가지 방법들 중에서 가장 효과적인 대안으로써 주목받고 있다. 키 복구는 일반적으로 암호문의 소유자만이 평문으로 복호할 수 있는 암호화 데이터에 대해 특정한 조건이 만족될 경우에 한해서 허가된 사람 또는 기관에게 복호 능력을 제공하는 기술 및 체계라고 정의할 수 있으며, 그 방식에 따라서 크게 키 위탁(Key Escrow) 방식과 키 캡슐화(Key Encapsulation) 방식으로 나눌 수 있다.

우선 키 위탁 방식은 복구될 사용자의 비밀키, 비밀키의 조각, 또는 키 관련 정보를 하나 이상의 신뢰되는 위탁기관에 위탁하고 정당한 키 복구 요청에 대해 위탁기관이 보관하고 있는 키 정보들로부터 키 또는 암호문의 평문을 얻어내는 방식이다. 이 방식에서는 위탁기관이 기본적으로 사용자들의 키를 안전한 곳에 보관해야만 하는데 사용자가 한시적으로 사용하는 세션키를 모두 저장한다면 막대한 저장소가 필요하

† 정 회 원 : 한국전자통신연구원(ETRI) 연구원
†† 준 회 원 : 영동전문대학 정보통신과 교수
††† 정 회 원 : (주)비씨큐어 암호기술연구소 주임 연구원
†††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
논문접수 : 2000년 9월 15일, 심사완료 : 2000년 12월 28일

며, 키를 위탁하는 과정에서 상당한 오버헤드가 발생하는 등 여러 가지 문제들이 발생하게 된다. 그러므로 전형적인 키 위탁 방식에서는 사용자들이 긴 주기동안 사용하는 키(이하 long-term 키)를 저장하고 위탁된 long-term 키를 사용하여 데이터 암호화에 사용된 세션키를 얻어내는 방법을 이용하고 있다[1].

반면 일반적인 키 캡슐화 방식은 복구될 사용자의 비밀키, 비밀키의 조각, 또는 키 관련 정보를 사용자의 키 복구 대행기관만이 복호할 수 있는 암호화된 영역내에 포함시키고 암호문에 첨부하고 정당한 키 복구 요청에 대해 키 복구 대행기관이 암호문에 첨부된 암호화 영역에서 키를 복구해 내는 방식이다. 이 방식에서는 일반적으로 사용자의 세션키 정보가 키 복구 대행기관의 공개키로 암호화된 영역에 포함되며, 키 복구 대행기관은 자신의 비밀키로 암호화 영역을 복호하여 사용자의 세션키를 얻어낸다[2].

이 외에도 키 복구 방식의 분류에 TTP(Trusted Third Party) 방식을 추가하는 경우도 있는데, TTP 방식은 사용자의 long-term 키를 신뢰기관이 저장한다는 점에서 키 위탁 방식과 비슷하지만 long-term 키를 TTP가 생성하고 long-term 키로부터 사용자들이 세션키를 생성한다는 점에서 키 위탁 방식과 다르다. 그러나 일부 키 복구 시스템들은 앞에서 살펴본 범주로 정확히 분류하기 힘들며 이러한 시스템들을 혼합(hybrid) 방식으로 분류하기도 한다.

이와 같이 키 복구 시스템들은 여러 가지 방식으로 분류되는데 법 집행권 보장을 목적으로 하는 키 복구 시스템들은 유사시에 신뢰기관에 보관된 정보들로부터 확실한 키 복구가 가능한 키 위탁 방식이나 TTP 방식을 주로 이용하며[3-5], 기업이나 일반 사용자 입장에서의 키 복구를 목적으로 하는 시스템들의 경우에는 저장 데이터의 복구가 용이하고 개인의 프라이버시 보호에 있어서 우수한 특징을 가지는 키 캡슐화 방식이 주류를 이루고 있다[6, 7].

키 복구에 대한 연구는 1993년에 미국이 EES(Escrowed Encryption Standard)라는 새로운 암호 시스템 개발을 발표하면서부터 활성화되기 시작하였는데, EES는 위탁된 키가 내장된 하드웨어(클리퍼 또는 캡스톤)를 사용하여 키를 복구해 내는 키 위탁 시스템으로써 클리퍼 칩이나 캡스톤 칩은 부당하게 변경할 수 없는 특성(tamper-resistant)을 가지고 있다[3]. 그러나 EES는 비공개 암호 알고리즘의 사용과 하드웨어 구현에 따른 고비용, 그리고 사용자의 long-term 키가 복구됨에 따라 사용자의 프라이버시가 침해될 수 있다는 문제점들이 지적되었고, 부당한 LEAF(Law Enforcement Access Field)를 첨부하여 키 복구 대행기관의 키 복구를 방해하면서 사용자가 암호통신을 할 수 있는 여러 가지 공격들이 제시되었다[8, 9].

1995년에 David M. Balenson 등은 [4]에서 공개키 암호에 기반을 두어 소프트웨어적 구현이 가능한 키 복구 시스템을 제시하였으며, 그 이후 EES의 문제점들을 해결하려는 여러 가지 키 복구 시스템들이 제안되었다. 그러한 시스템들은 공통적으로 공개 알고리즘과 공개키 방식을 이용함으로써 소프트웨어 구현이 가능하도록 하였고, 세션키가 복구되도록 함으로써 사용자들의 프라이버시 보호에 더욱 우수한 특성을 가지고 있다.

그러나 이러한 시스템들은 국가의 법 집행권 보장을 목적으로 하는 시스템들로써 통신 데이터만을 복구 대상으로 삼고 있으며, 이러한 특성은 저장 데이터를 주요 복구 대상으로 하는 기업이나 일반 사용자 입장에서는 바로 적용이 어렵다는 문제가 존재한다. 이러한 이유에서 1995년에 Stephen T. Walker 등은 [6]에서 저장 데이터의 복구가 가능한 commercial key escrow(TIS-CKE)라는 시스템을 제안하였으며, David P. Maher도 저장 데이터의 복구를 지원하는 상업 환경에서 적합한 키 복구 시스템을 제안하였다[7]. 그러나 이러한 시스템들은 소프트웨어로 구현됨으로써 사용자들에 의한 조작이 용이하기 때문에 키 복구 기능 우회를 방지하기 위한 방법이 필요하게 된다. 특히, TIS-CKE 경우에는 하나의 키 복구 대행기관만을 사용함으로써 키 복구 대행기관의 부정에 취약한 문제를 안고 있다.

이상에서 살펴본 바와 같이 지금까지의 시스템들은 여러 사용주체들의 키 복구에 대한 다양한 요구사항을 수용할 만큼 유연하지 않으며, 모든 요구사항을 완벽히 만족하는 키 복구 시스템을 설계하는 것은 기술적·정책적 이유 때문에 어려운 것이 사실이다.

본 논문에서는 이러한 점들을 고려하여 키 복구 시스템에 대한 각자 다른 사용 주체들의 입장을 살펴보며, 다양한 환경에 사용될 수 있는 유연하면서 효율적인 키 복구 시스템을 제안한다. 우선 제2장에서는 키 복구 시스템에 대한 다양한 입장과 키 복구 시스템의 평가기준으로 사용될 수 있는 요구사항들을 살펴보고 제3장에서는 기존의 키 복구 시스템들에 대해 간략히 알아본다. 제4장에서는 앞에서 제시한 요구사항들을 고려하여 제안하는 키 복구 시스템에 대해서 설명하고 제5장에서는 제안하는 키 복구 시스템의 주요 특징 및 안전성 등에 대해서 고찰하도록 하며, 제6장에서 결론을 맺는다.

2. 키 복구 시스템에 대한 입장과 요구사항

기밀성을 제공하기 위해 일반적으로 사용되는 암호기술은 송신자와 수신자간의 통신 데이터나 저장 데이터 모두에 적용되고 암호화된 데이터의 복구를 목적으로 하는 키 복구 시스템의 기본 기능을 고려할 때, 국가나 민간의 키 복구 시스템은 통신 데이터와 저장 데이터에 적용되어야 한다. 그러나 각 사용 주체의 키 복구 시스템에 대한 입장이나 사용목적은 상이하며, 그에 따라 키 복구 시스템의 설

계 목적 또한 달라진다. 따라서 각 사용 주체들의 요구사항을 만족하는 시스템을 설계하기 위해서는 사용 주체에 따른 키 복구를 살펴보고 이를 고려한 키 복구 시스템의 요구사항을 도출하는 것이 필요하다.

본 장에서는 키 복구 시스템의 사용주체를 국가와 민간으로 크게 나누어 각 사용주체에 따른 키 복구에 대한 입장을 살펴보고 이에 따라 키 복구 시스템이 만족해야 할 사항들에 대해 고찰한다.

2.1 사용 주체에 따른 키 복구

2.1.1 국가

국가 입장에서의 키 복구는 국가의 안전 및 공공의 안녕을 위한 법 집행권의 확보를 가장 큰 목적으로 하고있다. 그러나 법 집행권을 보장하기 위해 키 복구를 시행할 경우, 사용자의 프라이버시 침해 문제는 간과할 수 없는 문제이므로 국가는 법 집행권 확보와 사용자의 권익 보호라는 두 가지 사항을 모두 고려해야 한다. 또한 국가 기관의 입장에서는 암호화된 저장 데이터에 대해서도 키 복구가 가능해야 하는데 이러한 저장 데이터에 대한 키 복구는 민간의 입장과 동일하다. 그러나 일반 사용자의 저장 데이터에 대해서 법 집행권 시행을 목적으로 키 복구를 수행하는 것은 데이터 소유자의 동의없이 암호문을 획득하는 것 자체가 기술적으로 어려우므로, 사실상 법 집행권 확보를 위한 키 복구는 통신 데이터만을 대상으로 하고있다.

2.1.2 민간

민간에 있어서의 키 복구는 기업과 일반 사용자의 입장으로 나누어 생각할 수 있다. 우선 기업 환경에서의 키 복구는 크게 다음과 같은 두 가지 목적을 가지고 있다[10].

첫째로, 암호키의 분실이나 손상에 따른 데이터의 손실 방지를 가장 큰 목적으로 하고 있으며, 이는 기본적으로 저장 데이터에 적용된다.

둘째로, 기업의 이익을 해치는 암호 통신문에 대한 모니터링이며, 이는 주로 통신 데이터를 대상으로 한다. 그러나 기본적으로 기업내의 시스템을 통해 처리되는 데이터는 기업의 소유로 인정되므로 국가에 비해 사원들의 저장 데이터에 대한 접근 및 키 복구의 수행이 용이하다.

일반 사용자의 경우에는 기업이나 국가와는 달리 저장 데이터만을 키 복구의 대상으로 하며, 데이터의 손실 방지를 목적으로 하고 있다. 따라서 일반 사용자 입장에서의 키 복구에 대한 요구사항은 통신 데이터의 키 복구를 수행하기 위해 복잡한 메커니즘을 필요로 하는 다른 사용주체들의 요구사항에 비해 단순하다. 또한 일반 사용자 입장에서는 암호키 분실 및 손상에 대해 개인 저장장치에 키를 백업하거나 컴퓨터 레지스트리에 키를 복사하는 방법 등을 사용할 수도 있으므로, 키 복구는 선택적으로 사용될 수 있다.

지금까지 각 사용주체에 따른 키 복구의 입장을 살펴보았으며, <표 1>은 이를 간략히 나타내고 있다.

〈표 1〉 키 복구 시스템에 대한 입장 차이

분 류		목적 및 필요성	대 상
국 가		· 국가 및 공공 사회의 안녕을 위한 법 집행권 보장 · 암호키의 분실 · 손상에 따른 데이터 손실 방지	통신 및 저장데이터
민간	기 업	· 암호키의 분실 · 손상에 따른 데이터 손실 방지 · 기업 이익을 위한 모니터링	통신 및 저장데이터
	개 인	· 암호키의 분실 · 손상에 따른 데이터 손실 방지	저장데이터

2.2 키 복구 시스템 요구사항

본 절에서는 2.1절에서 살펴 본 키 복구 시스템을 이용하는 사용 주체들의 상이한 목적이나 대상을 고려하여 키 복구 시스템이 만족해야 할 사항들에 대해서 알아보도록 한다.

[요구사항 1] 집행권 보장(확실한 키 복구 가능)

국가, 기업 및 개인 사용자들은 각기 다른 목적으로 키 복구 시스템을 사용하지만, 목적에 상관없이 적절한 절차에 따른 정당한 키 복구 요구에 대해 키 복구가 가능해야 한다. 이는 사용 주체에 따라서 통신 데이터 뿐 아니라 저장 데이터에 대한 키 복구도 포함한다.

[요구사항 2] 집행권 제한

국가의 법 집행권 보장을 목적으로 하는 키 복구 시스템은 사용자의 프라이버시 침해를 막을 수 있는 기능을 제공해야 한다. 이 요구사항을 만족시키기 위한 가장 일반적인 조건은 복구되는 키가 사용자들이 일시적으로 사용하는 세션키가 되도록 해야한다는 것이다. 그러나 사원들이 기업에 속해있는 시스템을 사용하는 기업환경에서는 일반적으로 기업내 시스템을 통해 처리되는 모든 정보가 기업의 소유인 것으로 간주되므로 반드시 세션키가 복구될 필요는 없다.

[요구사항 3] 우회 어렵고, 쉽게 검출

키 복구 시스템을 사용하는 사용자들이 부당하게 키 복구 기능을 우회하면서 암호 통신을 할 수 없어야 한다. 그러나 현재까지 송신자와 수신자가 결탁한 경우(예 : Double Encryption Attack)에는 키 복구 기능을 우회할 수 있는 것으로 알려져 있으며, 본 논문은 한 명의 통신자만이 부정한 경우(Single rogue user)만을 고려한다.

[요구사항 4] 키 복구 대행기관 선택의 융통성

키 복구에 하나의 키 복구 대행기관만을 이용한다면 그 키 복구 대행기관은 공격자들의 주요 공격대상이 될 것이며[11], 키 복구 대행기관의 부정 또한 방지할 수 없다.

또한 사용자들은 자신이 원하는 키 복구 대행기관을 선택함으로써 기관에 대한 신뢰를 가질 수 있을 것이다. 따라서, 키 복구 시스템은 사용자가 선택한 다수의 키 복구 대행기관을 통하여 키 복구를 수행할 수 있어야 한다.

[요구사항 5] 시스템 세부사항 공개

키 복구 시스템의 사용자들이 시스템을 신뢰하는 것은 중요하며, 이는 시스템에 사용되는 알고리즘 뿐 아니라 시스템의 구체적인 동작과정 등이 전문가에 의해 검증됨으로써 시스템에 대한 확신을 가질 수 있게 해 준다.

[요구사항 6] 비용 및 성능

암호 시스템에 키 복구 기능이 추가됨으로써 일반적으로 시스템의 효율이 저하되며, 비용이 늘어난다. 따라서 키 복구 기능이 암호 시스템에 추가될 때에는 기존 암호 시스템의 효율 저하가 최소가 되도록 하여야 하며, 추가되는 비용이 암호화된 정보의 가치를 넘지 않아야 한다.

위에서 나열한 요구사항들은 키 복구 방식에 상관없이 평가가 가능하도록 포괄적인 내용을 담고 있으며, 이 외에도 여러 가지 요구사항이 있을 수 있다. 이후 본 논문에서는 위의 요구사항들에 중점을 두어 설명하도록 한다.

3. 기존의 키 복구 시스템

본 장에서는 주로 대표적인 두 가지 키 복구 시스템을 살펴보며, 앞에서 제시된 키 복구 시스템의 요구사항에 대한 각 시스템들의 문제점에 대해 살펴보도록 한다.

우선 90년대 초 미국 행정부가 정부 및 민간 부문의 정보 보호를 위한 새로운 대칭키 암호 시스템 개발을 명시하는 클리퍼(Clipper) 정책을 발표하면서 실제적인 추진이 이루어진 키 위탁 제도는 EES라는 표준으로 승인되었다. 하지만 EES 시스템은 다음과 같은 문제점들이 지적되었다.

- **사용자 암호문에 대한 불법적 복구 가능**
  복구되는 키가 사용자의 long-term 키이므로 일단 한 번 사용자의 키를 복구한 법 집행 기관은 법원의 허가 없이도 그 사용자의 암호문을 복호할 수 있다.
- **키 복구 기능의 우회 가능**
  법 집행 기관이 키를 복구할 수 없도록 키 복구 기능을 우회할 수 있는 다양한 공격들이 존재한다.
- **비공개 암호 알고리즘의 사용**
  비공개 암호 알고리즘인 SKIPJACK의 사용은 사용자들로부터 알고리즘 내에 trapdoor가 존재할 가능성이 있다는 의심을 사고있으며, DES 등에 비해 그 안전성이 경험적으로 증명되지 않았다.
- **비싼 비용**
  EES는 tamper-resistant 하드웨어의 사용을 필수로 하기 때문에 시스템을 구현하는데 많은 비용이 소모된다.

이 밖에도 EES는 지정된 키 위탁 기관의 사용, 저장 데이터에 대한 복구 불가 등과 같은 문제들을 지니고 있다.

또한 미국의 TIS사가 제안한 키 캡슐화 방식의 대표적인 시스템인 CKE(Commercial Key Escrow)에서는 키 복구를 위해 DRC(Data Recovery Center)라는 키 복구 대행기관을 두고 있다. 이 시스템은 DRC나 다른 어떤 장소에도 위탁되는 사용자의 키가 없으나 키 복구 대행기관인 DRC를 하나만 이용하고 키 복구시에 DRC의 공개키로 암호화된 세션키를 DRC가 비밀키로 복호해서 사용자에게 전송하기 때문에 사용자의 세션키가 DRC에게 직접 노출될 수 있다는 문제를 지니고 있다.

이 외에도 1997년에 Yung-Cheng Lee 등은 정부의 입장뿐 아니라 사용자의 입장을 고려하면서 일방향 키 분배 특성을 지니는 키 복구 시스템을 제안하였지만 저장 데이터의 복구를 고려하지 않는 등 앞에서 제시한 요구사항들을 만족하지 못하고 있다[12].

다음의 <표 2>는 2장에서 살펴 본 키 복구 시스템에 대한 몇 가지 요구사항과 그에 대한 각 시스템의 만족여부를 보여주고 있다.

〈표 2〉 기존 키 복구 시스템의 요구사항 만족여부

분 류	EES	TIS-CKE	바람직한 특성
요구사항 1	통신 데이터	통신 및 저장 데이터	통신 및 저장 데이터
요구사항 2	long-term 키	세션키	세션키
요구사항 3	×	×	○
요구사항 4	×	×	○
요구사항 5	×	○	○

본 논문의 이후 내용에서는 <표 2>에서 보는 바와 같이 여러 가지 바람직한 요구사항을 만족하도록 다양한 변형이 가능한 키 복구 시스템을 설명한다.

4. 제안하는 키 복구 시스템

본 장에서는 앞에서 제시된 다양한 요구사항들을 만족시킬 수 있도록 충분한 유연성을 가지면서도 효율적인 키 복구 시스템을 제안하고자 한다. 제안하는 시스템은 별도의 사전 키 분배가 필요없는 일방향 키 분배 기능을 가지는 시스템으로 쉽게 변경할 수 있다.

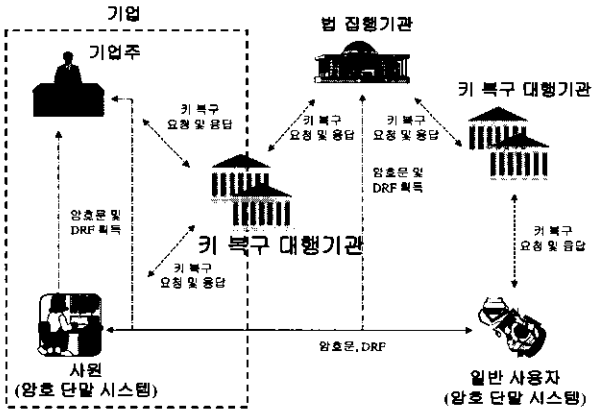
사용되는 용어 및 주요 구성요소들은 다음과 같으며, (그림 1)은 전체적인 시스템의 구성과 동작을 간략히 보여주고 있다.

- 암호 단말 시스템(Cryptographic End System : CES)
  데이터의 암호화 및 복호화를 수행하는 하드웨어 또는 소프트웨어로써 송신측에서는 데이터 복구 필드(Data Recovery Field : DRF)를 생성된 암호문에 덧

붙이는 역할을 수행하며, 수신측에서는 필요에 따라 DRF의 유효성 검사한다.

- 키 복구 대행기관(Key Recovery Agent : KRA)
  사용자의 암호화된 데이터나 키를 복구하는데에 필요한 정보를 안전하게 보관하고 있으며, 키 복구 요청자의 정당한 키 복구 요청에 의해 키 복구를 수행한다.

- 키 복구 요청자(Key Recovery Requestor : KRR)
  키 복구 요청자는 법 집행 또는 사용자의 키 복구 필요에 의해 암호화된 데이터의 복구를 키 복구 대행기관에 요청할 수 있는 권한을 가진 허가된 개체이다. 키 복구 요청자는 기업주나 개인 또는 법 집행기관 등이 될 수 있다.



(그림 1) 제안 시스템의 구성 및 동작

지금부터는 제안 시스템을 구체적으로 설명하며, 시스템의 사용자들은 각각 두 개의 KRA를 사용하는 것으로 가정한다.

4.1 시스템 설정 단계

시스템상의 신뢰기관은 2q+1의 형태를 지닌 큰 소수 p와 Z_p^*상의 생성자 g를 임의로 선택하여 공개하며, 모든 연산은 모듈러 p상에서 이루어진다. 그 외에 사용되는 파라미터 및 기호는 다음과 같다.

- p : 2q+1 형태의 큰 소수 (단, q는 충분히 큰 소수)
- g : Z_p^*상의 생성자
- x_A : 사용자 A의 비밀키
- y_A : 사용자 A의 공개키
- KT_{A_i} : 각 KRA가 선택하여 보관하는 비밀값 (단, $1 \le i \le$ A의 KRA 수)
- h_1, h_2 : 일방향 해쉬함수

이 때 h_1과 h_2는 비밀키 k를 파라미터로 가지는 해쉬함수로써 다음과 같은 형태와 특성을 지닌다.

$$H = h(k, m)$$

• 계산 불가성(Computation-resistance)

하나 이상의 입력과 해쉬값의 쌍 (m_i, H_i)가 주어졌을 때, 비밀키 k를 모르고 어떤 입력 $m(\neq m_i)$에 대한 해쉬값 H를 구하는 것과 $h(k, m_i) = h(k, m)$인 $m(\neq m_i)$을 찾는 것이 계산상 불가능하다[13].

4.2 사용자 등록 단계

사용자 등록 단계는 각 사용자들이 자신의 영역에 속하는 KRA에 등록을 하는 과정으로 사용자와 KRA 사이에 공유되는 비밀정보를 설정하는 단계이다. 사용자들은 각 조직(예 : 기업 또는 국가)의 정책에 따라서 하나 이상의 적당한 KRA를 선택할 수 있으며, 기업의 경우 기업내 또는 외부의 KRA를 사용할 수도 있다.

시스템 설정과 사용자 등록 단계는 [14]에서의 과정과 유사하며, 구체적인 사용자 등록 과정은 다음과 같이 수행된다.

① 사용자 A는 다음과 같은 비밀키, 공개키 쌍 (x_A, y_A)을 생성하며, 공개키 y_A를 자신이 선택한 KRA들에게 전송한다.

$$x_A \in_R Z_p^*$$
$$y_A = g^{x_A}$$

② 사용자 A의 공개키를 전송받은 각 KRA들은 KT_{A_i}값을 랜덤하게 선택하고 다음의 값들을 계산하여 $cert_{A_i}$, g^{a_i}를 사용자 A에게 전송한다.

$$a_i = h_1(KT_{A_i}, y_A)$$
$$\alpha_{A_i} = y_A^{a_i}$$
$$r_{A_i} = g^{\alpha_{A_i}}$$
$$cert_{A_i} = Sig(y_A, r_{A_i})$$

③ 사용자 A는 각 KRA들이 전송한 정보의 유효성을 확인하기 위해 다음을 계산한다.

$$\alpha_{A_i} = (g^{a_i})^{x_A}$$
$$r_{A_i} = g^{\alpha_{A_i}}$$

④ 사용자 A는 단계 ③에서 계산된 r_{A_i}와 $cert_{A_i}$에 포함된 r_{A_i}의 일치 여부를 검사함으로써 KRA로부터 전송된 정보의 유효성을 확인하며, 그 결과에 따라 각 KRA에게 Accept 또는 Reject 신호를 전송한다.

⑤ 각 KRA들은 사용자 A로부터 Accept를 수신하면 $cert_{A_i}$

를 공개하고, Reject를 수신하면 프로토콜을 종료한다.

4.3 암호통신 단계

두 사용자 A와 B가 암호통신에 사용할 세션키 KS는 임의의 키 분배 프로토콜을 이용하여 이미 설정되어 있다고 가정한다. (그림 3)은 전체적인 암호통신 과정을 보여주고 있으며, 구체적인 내용은 다음과 같다.

① 사용자 A가 사용자 B와 처음 통신을 하는 경우에 사용자 A는 공개된 사용자 B의 r_{B_1}, r_{B_2} 값과 자신의 α_{A_1}, α_{A_2} 값을 이용하여 다음을 계산한다.

$$\omega_1 = r_{B_1}^{\alpha_{A_1}}, \quad \omega_2 = r_{B_2}^{\alpha_{A_2}}$$

이 때 ω_i 값의 계산에 필요한 지수 연산의 횟수는 연관되는 KRA의 수와 동일하며, 계산된 ω_i 값은 이후에 동일한 사용자와의 계속되는 통신에 사용되기 위해 저장할 수 있다.

② 사용자 A는 다음과 같이 KEK(Key Encryption Key)를 생성한다. 단, SID(Session ID)는 임의의 세션 식별자로써 암호화하려는 파일 또는 메시지 마다 유일한 값이다.

$$KEK_1 = h_2(\omega_1, SID)$$
$$KEK_2 = h_2(\omega_2, SID)$$
$$KEK = KEK_1 \oplus KEK_2$$

③ 사용자 A는 이미 설정된 세션키 KS를 KEK로 암호화하여 ESK(Encrypted Session Key)를 생성한다.

$$ESK = E_{KEK}(KS)$$

④ 사용자 A는 파일 또는 메시지 M을 세션키 KS로 암호화하여 암호문을 생성한다.

$$C = E_{KS}(M)$$

⑤ 사용자 A는 다음과 같은 형태의 DRF를 암호문 C에 덧붙여서 사용자 B에게 전송한다.

$$DRF = ESK \| SID \| cert_{A_1} \| cert_{A_2} \| cert_{B_1} \| cert_{B_2}$$

이상은 사용자 A의 암호 단말 시스템에 의해 수행되며, 암호문을 수신한 사용자 B는 DRF의 유효성을 다음과 같이 검사한다. DRF의 유효성 검사는 세션키가 KRA에 의해 복구될 수 있음을 확인하기 위해 수행되고 이 과정은 정책에 따라 생략될 수도 있다.

⑥ 사용자 B가 사용자 A와 처음 통신을 하는 경우에는 다음과 같이 ω_1과 ω_2를 계산한다.

$$\omega_1 = r_{A_1}^{\alpha_{B_1}}, \quad \omega_2 = r_{A_2}^{\alpha_{B_2}}$$

⑦ 사용자 B는 계산된 ω_1, ω_2로부터 다음과 같이 KEK를 계산한다.

$$KEK_1 = h_2(\omega_1, SID)$$
$$KEK_2 = h_2(\omega_2, SID)$$
$$KEK = KEK_1 \oplus KEK_2$$

⑧ 사용자 B는 다음을 검사함으로써 사용자 A로부터 전송된 정보의 유효성을 확인한다.

$$ESK \stackrel{?}{=} E_{KEK}(KS)$$

⑨ DRF 유효성 검사를 통과한 경우에만 수신자 B는 사전에 분배된 세션키 KS를 사용하여 다음과 같이 암호문 C를 복호한다.

$$M = D_{KS}(C)$$

사용자 A	$cert_{A_1}, cert_{A_2}, cert_{B_1}, cert_{B_2}$,	사용자 B
$\omega_1 = r_{B_1}^{\alpha_{A_1}}$ $\omega_2 = r_{B_2}^{\alpha_{A_2}}$ 임의의 SID를 선택 $KEK_1 = h_2(\omega_1, SID)$ $KEK_2 = h_2(\omega_2, SID)$ $KEK = KEK_1 \oplus KEK_2$ $ESK = E_{KEK}(KS)$ $C = E_{KS}(M)$ $DRF = ESK \| SID \| cert_{A_1} \| cert_{B_1}$	$C \| DRF$ →	$\omega_1 = r_{A_1}^{\alpha_{B_1}}$ $\omega_2 = r_{A_2}^{\alpha_{B_2}}$ $KEK_1 = h_2(\omega_1, SID)$ $KEK_2 = h_2(\omega_2, SID)$ $KEK = KEK_1 \oplus KEK_2$ if $ESK \stackrel{?}{=} E_{KEK}(KS)$ then $M = D_{KS}(C)$

(그림 2) 암호통신 단계

4.4 키 복구 단계

3장에서 살펴보았듯이 키 복구 요청자는 사용주체에 따라 법 집행기관, 기업주 또는 개인이 될 수 있으며, 정당한 키 복구 요청자는 암호문을 취득하여 다음과 같이 키 복구를 수행한다.

① 키 복구 요청자는 복호하려는 암호문에서 추출한 DRF를 해당 KRA들로 전송한다.

② 키 복구 요청을 받은 각 KRA들은 다음과 같이 ω_i 값을

계산한다.

$$a_i = h_1(KT_{A_i}, y_A)$$
$$\alpha_{A_i} = y_A^{a_i}$$
$$\omega_i = r_{B_i}^{a_{A_i}}$$

③ 각 KRA들은 계산된 ω_i값을 통해 다음과 같이 KEK_i를 계산하여 키 복구 요청자에게 전송한다.

$$KEK_i = h_2(\omega_i, SID)$$

④ 각 KRA들로부터 KEK를 전송받은 키 복구 요청자는 다음과 같이 얻어진 KEK로부터 세션키 KS를 복구한다.

$$KEK = KEK_1 \oplus KEK_2$$
$$KS = D_{KEK}(ESK)$$

5. 제안 시스템의 특징 및 안전성

본 장에서는 제안하는 키 복구 시스템이 가지는 특징 및 안전성 등에 대해 설명하도록 한다.

5.1 일방향 키 분배

키 복구 시스템은 일반적으로 키 분배 메커니즘과 키 복구 메커니즘을 독립적으로 사용한다. 그러나, 제안하는 시스템은 사용자간에 별도의 키 분배 프로토콜을 이용하여 사전에 세션키를 설정하지 않고 암호통신 과정 중에 송신자가 전송하는 정보들로부터 수신자가 세션키를 얻어내는 일방향 키 분배가 가능한 시스템으로 변형이 가능하다. 일방향 키 분배가 가능한 시스템은 앞에서 제안한 시스템을 다음과 같이 변경함으로써 쉽게 구성할 수 있으며, 시스템 설정 및 사용자 등록 단계는 4장에 설명한 것과 동일하다.

- 암호통신 단계

일방향 키 분배는 다음과 같이 제안 시스템에서 KEK를 세션키 KS로 사용함으로써 구성할 수 있다. 이때 DRF의 유효성을 확인하기 위해 사용되었던 ESK는 필요하지 않다.

$$KEK_1 = h_2(\omega_1, SID)$$
$$KEK_2 = h_2(\omega_2, SID)$$
$$KS = KEK_1 \oplus KEK_2$$
$$DRF = SID \| cert_{A_1} \| cert_{A_2} \| cert_{B_1} \| cert_{B_2}$$
$$C = E_{KS}(M)$$

수신자는 4.3절의 DRF 검증 과정의 KEK를 구하는 방법으로 세션키 KS를 계산하여 암호문을 복호할 수 있다. 이와 같이 일방향 키 분배를 사용할 경우에 송신자가 KRA에 의한 키 복구를 우회할 목적으로 부당한 DRF를 암호문에 첨부한다면 수신자 또한 올바른 키를 구할 수 없게되므로 암호통신을 수행할 수 없게된다. 즉, 사용자는 부당하게 키 복구 기능을 우회하면서 기밀성 서비스를 받을 수 없는 것이다. 또한 별도로 키를 분배할 필요가 없으므로 키 분배에 따르는 오버헤드도 줄일 수 있는 장점을 지닌다.

5.2 저장 데이터의 복구

저장 데이터를 키 복구의 대상으로 하는 경우에는 수신자가 존재하지 않기 때문에 통신 데이터에 적용되는 시스템을 그대로 사용하는 데는 어려움이 있다. 따라서 제안하는 시스템을 저장 데이터에 적용하기 위해서는 다음과 같은 변경이 필요하며, 시스템 설정 및 사용자 등록 단계는 4장에 설명한 것과 동일하다.

- 암호통신 단계

우선 사용자 A는 자신의 r_{A_i}와 α_{A_i}를 이용하여 다음과 같이 ω_i값을 계산하며, 제안 시스템의 KEK를 세션키 KS로 사용한다. 또한 저장 암호문에 적용되는 키 복구 시스템은 DRF의 검증 과정과 수신자가 없으므로 DRF에 ESK와 $cert_{B_i}$를 포함할 필요가 없다.

$$\omega_i = r_{A_i}^{a_{A_i}}$$
$$KEK_1 = h_2(\omega_1, SID)$$
$$KEK_2 = h_2(\omega_2, SID)$$
$$KS = KEK_1 \oplus KEK_2$$
$$DRF = SID \| cert_{A_1} \| cert_{A_2}$$
$$C = E_{KS}(M)$$

이 때 사용자 A가 ω_i값을 저장하여 둔다면 이 후 키 복구 과정에서 KRA와 연결되지 않고 독자적인 키 복구가 가능하다. 이는 키 복구 과정에서의 오버헤드를 줄일 수 있다.

이와 같이 제안하는 시스템은 통신 및 저장 데이터에 모두 적용이 될 수 있고 따라서 그 만큼 다양한 환경에 적용할 수 있다. 그러나 이 특징은 앞에서 언급한 바와 같이 국가가 일반 사용자의 암호문을 획득하는 것 자체가 기술적으로 어렵기 때문에 국가보다는 민간의 입장에서 더 유용한 특성이다.

5.3 기타 특징

제안하는 시스템은 앞에서 언급한 특징 외에도 다음과 같은 주요 특징을 가지고 있다.

[특징 1] 세션키의 복구

키 복구 시스템에 대한 주요 논쟁은 사용자의 프라이버시가 침해될 수 있다는 것이고 이러한 논쟁에 대한 대안 중 하나로 복구되는 키가 세션키가 되게하는 방법이 있

다. 제안하는 시스템에서 복구되는 키는 각 세션 정보들을 통해 얻어지는 사용자의 세션키이므로 집행권의 제한이 가능하다.

[특징 2] KRA 선택의 융통성
제안하는 시스템에서 각 사용자들은 자신이 속해 있는 조직의 정책에 따라 하나 이상의 KRA를 선택할 수 있으며, 통신하는 각 사용자는 서로 다른 수의 KRA를 사용할 수 있다.

[특징 3] KRA와 연결없이 키 복구 가능
키 복구 시스템은 키 복구를 위해 KRA와의 연결이 필요하지만 키 복구시 마다 키 복구 대행기관과 연결된다는 것은 큰 오버헤드이며, 네트워크에 문제가 있을 경우에는 키 복구를 수행할 수 없게된다는 문제가 있다. 제안하는 시스템의 일반 사용자들은 암호문 생성시에 계산되는 ω_i 값을 저장하여 키 복구 수행과정에서 KRA와 연결될 필요가 없이 독자적으로 키 복구가 가능하다.

[특징 4] 소프트웨어 구현
제안하는 시스템은 공개키 암호를 기반으로 구성하므로 소프트웨어로 구현될 수 있고 이는 시스템의 비용이나 융통성, 조작성 등에서 하드웨어로 구현된 시스템보다 우수하다는 장점을 지닌다.

제안하는 키 복구 시스템은 <표 3>에서 보는 바와 같이 기존의 대표적인 키 복구 시스템에 비해서 우수한 특징들을 지니고 있기 때문에 다양한 환경에서 효과적으로 사용될 수 있다.

〈표 3〉 제안 시스템과 기존 시스템의 비교

분 류	EES	TIS-CKE	제안 시스템
일방향 키 분배	×	×	○
저장 암호문에 대한 독자적인 키 복구	×	×	○
복구 대상 데이터	통신	통신 및 저장	통신 및 저장
복 구 키	long-term 키	세션키	세션키

5.4 효율성

효율성은 키 복구 시스템의 주요 평가기준이자 요구사항 중의 하나이며, 본 절에서는 제안하는 시스템의 효율성에 대해서 각 수행 단계별로 언급하도록 한다.

[사용자 등록 단계]
사용자들이 시스템을 사용하기 위해서는 KRA에 등록을 해야하며, 이 과정에서 사용자는 자신이 선택한 각 KRA와 연결되어야 하는 오버헤드가 발생한다. 그러나 사용자 등록은 키 복구 시스템을 사용하기 위해 단 한 번만 수행되며, 이는 전체 키 복구 시스템에서의 오버헤드를 고려할 때 크지 않다.

[암호통신 단계]
암호통신 단계는 키 복구 시스템의 동작 과정 중에서 가장 많이 수행되는 단계이다. 이 단계에서는 처음 통신을 하는 사용자들 사이에서 지수연산을 필요로 하므로 전체 키 복구 시스템의 효율성에 가장 큰 영향을 미친다. 필요한 지수 연산의 최대 횟수는 통신자가 선택한 전체 KRA의 수와 같지만 한 번 계산된 ω_i 값을 이후 동일한 사용자와의 통신을 위해 저장함으로써 지수연산에 따른 오버헤드를 줄일 수 있다.

[키 복구 단계]
키 복구 단계는 키 복구 요청자에 의한 정당한 키 복구 요청이 있을 경우에만 수행되는 단계로써 각 KRA들은 ω_i 값을 계산하는데 지수연산을 필요로 하게된다. 이 단계에서 필요한 지수연산의 횟수 또한 암호통신 단계에서처럼 한 번 계산된 ω_i 값을 키 복구 요청자의 정당한 키 복구 요청기간 동안 저장함으로써 줄일 수 있다. 또한 저장 데이터의 경우에는 사용자가 ω_i 값을 저장한다면 키 복구 수행시에 사용자가 KRA와 연결되어야 하는 부담을 줄일 수 있다.

5.5 안전성

[파라미터의 선택]
시스템 파라미터 p는 모든 사용자들이 공통으로 사용하므로 전체 시스템의 안전성에 영향을 미친다. 따라서 다음과 같은 형태를 지닌 적절한 소수 p를 선택하는 것이 중요하며, 이러한 파라미터의 선택은 [15]에서 설명된 이산대수를 계산하는 공격을 어렵게 한다.

$p = 2q + 1$ (단, p는 512비트 이상,
q는 160비트 이상의 큰 소수)

[공격 시나리오]
제안하는 시스템에서 세션키를 구하기 위해 비밀정보인 α와 ω 값을 계산하려는 시도가 있을 수 있고 공격자가 이용할 수 있는 공개정보들은 다음과 같다.

공개 정보 : $g, y_A, y_B, r_A, r_B, g^a, g^b$, SID

① r_A와 g로부터 α_A를 구하려는 시도

$r_A = g^{\alpha_A}$인 α_A를 구하려는 공격은 이산대수 문제이며, 이산대수 문제를 푸는 것이 계산상 불가능하다면 공격자는 α_A를 구할 수 없다[15].

② y_A와 g^a로부터 α_A를 구하려는 시도

g^{x_A}와 g^a로부터 $\alpha_A = g^{x_A \cdot a}$를 구하려는 공격은 Diffie-Hellman 문제이며, Diffie-Hellman 문제를 푸는 것이 계

산상 불가능하다면 공격자는 α_A를 구할 수 없다[16].

③ α_B, r_A, ω를 알고 α_A를 구하려는 시도

이 공격은 사용자 B가 공격자일 경우에 가능한 공격으로써 이것 또한 Diffie-Hellman 문제이며, Diffie-Hellman 문제를 푸는 것이 계산상 불가능하다면 공격자는 α_A를 구할 수 없다.

④ r_A와 r_B로부터 ω를 구하려는 시도

g^{α_A}와 g^{α_B}로부터 $g^{\alpha_A \cdot \alpha_B}$를 구하려는 공격은 Diffie-Hellman 문제이며, Diffie-Hellman 문제를 푸는 것이 계산상 불가능하다면 공격자는 ω를 구할 수 없다.

⑤ KEK = h(ω, SID)인 KEK와 SID가 주어진 경우 ω를 구하려는 시도

이 경우에 4.1절에서 제시한 바와 같이, 사용하는 해쉬함수가 계산 불가성을 만족한다면 공격자는 ω를 알아낼 수 없다.

6. 결 론

암호기술의 확산은 일반 사용자들에게 전자상거래나 전자결제와 같은 여러 가지 편리한 서비스를 제공하였지만 범죄자들의 암호 악용이나 키의 손상 및 분실에 따른 부작용을 유발시켰다. 이러한 암호의 부작용에 대한 대안으로 제시된 키 복구는 시스템을 사용하는 주체에 따라 그 목적이 서로 상이하며 그에 따라 요구사항과 키 복구 대상 또한 달라진다. 그러나 지금까지 제시된 대부분의 키 복구 시스템들은 국가 입장에서의 키 복구 시스템 설계에 초점을 맞추었으며, 키 복구에 대한 다양한 요구를 수용하기가 어렵다.

제안하는 시스템은 저장 및 통신 데이터에 대한 키 복구가 가능하며, 세션에 기반한 정보를 통해 세션키를 복구하기 때문에 사용자의 프라이버시 보호에 좋은 특성을 가진다. 또한 사용자의 선택에 따라 키 복구 대행기관을 선택할 수 있는 유연성과 키 분배 기능을 암호통신에 포함시킴으로써 부정한 사용자에 의한 키 복구 기능의 우회를 막고 효율성을 높일 수 있다는 특성을 가진다. 더욱이 공개키에 기반하여 소프트웨어적 구현이 용이하여 경제적이고 사용이 용이하다. 이러한 다양한 특성들은 다양한 사용 주체들의 요구사항에 따라 여러 응용에 쉽게 적용될 수 있도록 충분한 유연성을 제공할 수 있을 것이다.

참 고 문 헌

[1] IBM SecureWay, "Towards a Framework-based solution to Cryptographic Key Recovery," available at http : //www-4.ibm.com/software/security/library.

[2] National Institute of Standards and Technology, "Requirements for Key Recovery Products," Report of the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure, Available at http : //csrc.nist.gov/keyrecovery, 1998.

[3] NIST, "Escrowed Encryption Standard," Federal Information Processing Standards Publication 185, 1994.

[4] David M. Balenson, Carl M. Ellison, Steven B. Lipner and Stephen T. Walker, "A New Approach to Software Key Escrow Encryption," Building in Big Brother : The Cryptographic Policy Debate, pp.180-207, Springer-Verlag, 1995.

[5] Ross Anderson and Michael Roe, "The GCHQ Protocol and its Problems," Eurocrypt'97, pp.134-148, 1997.

[6] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison and David M. Balenson, "Commercial Key Recovery," Communications of the ACM, Vol.39, No.3, pp.41-47, 1996.

[7] David Paul Maher, "Crypto Backup and Key Escrow," Communications of the ACM, Vol.39, No.3, pp.48-53, 1996.

[8] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," The 2nd ACM Conference on Computer and Communications Security, pp.59-67, 1994.

[9] Yair Frankel and Moti Yung, "Escrowed Encryption Systems Visited : Attacks, Analysis and Designs," Advanced in Cryptology-Crypto'95, pp.222-235, 1995.

[10] Business Scenarios Committee of the Key Recovery Alliance, "Business Requirements for Key Recovery Release 3.0," Available at http : //www.kra.org/whitepapers, 1997.

[11] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller and B. Schneier, "The Risk of Key Recovery, Key Escrow and Trusted Third Party Encryption," available at http : //www.cdt,org/crypto/risks98, 1998.

[12] Yung-Chen Lee and Chi-Sung Laih, "On the Key Recovery of the Key Escrow System," Proceedings of 13th Annual Conference on Computer Security Applications, pp.216-220, 1997.

[13] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography," pp.321-331, CRC Press, 1996.

[14] Colin Boyd, "Enforcing Traceability in Software," 1st International Conference on Information and Communication Security, ICICS'97, pp.398-408, 1997.

[15] S. C. Pohig and M. E. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance," IEEE Transaction on Information Theory, Vol. IT 24, No.1, pp.106-110, 1978.

[16] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory, Vol.IT 22, No.6, pp.135-145, 1976.

유 준 석

e-mail : jsyu92@etri.re.kr

1999년 성균관대학교 정보공학과 졸업 (학사)

2001년 성균관대학교 대학원 전기전자 및 컴퓨터 공학부(공학석사)

2001년~현재 한국전자통신연구원 연구원

관심분야 : 암호이론, 보안운영체제 등

김 희 도

e-mail : hdkim@yeongdong.ac.kr

1985년 서울산업대학교 전자공학과 졸업 (학사)

1988년 한양대학교 대학원 전자통신과 (공학석사)

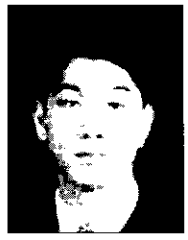
1998년~현재 성균관대학교 대학원 전기 전자 및 컴퓨터 공학부 박사과정

1989년~1994년 한국통신기술(주) 기술과장

1996년~현재 한국인력관리공단 출제 및 평가위원(정보통신분야)

1994년~현재 영동전문대학 정보통신과 조교수

관심분야 : 암호이론, 통신이론 등



전 종 민

e-mail : jjmin@bcqre.com

1999년 성균관대학교 정보공학과 졸업(학사)

2001년 성균관대학교 대학원 전기전자 및 컴퓨터 공학부(공학석사)

2001년~현재 (주)비씨큐어 암호기술연구소 주임 연구원

관심분야 : 암호이론, 디지털 컨텐츠 보호 등

원 동 호

e-mail : dhwon@simsan.skku.ac.kr

1976년 성균관대학교 전자공학과 졸업(학사)

1978년 성균관대학교 대학원 전자공학과 (공학석사)

1988년 성균관대학교 대학원 전자공학과 (공학박사)

1978년~1980년 한국전자통신연구원 전임 연구원

1985년~1986년 일본 동경공대 객원 연구원

1996년~1998년 국가정보화 추진위원회 자문위원

1998년~1999년 성균관대학교 정보통신기술연구소장

1999년~2000년 성균관대학교 전기전자 및 컴퓨터 공학부장

1982년~현재 성균관대학교 전기전자 및 컴퓨터 공학부 교수

1999년~현재 정보통신대학원장 (겸) 한국통신정보보호학회 부회장

관심분야 : 암호이론, 부호이론 등