1회 읽기 가능 메모리를 통한 오프라인 방식의 모바일 전자 지불 시스템 설계 및 구현

Design and Implementation of One-Time-Readable Memory-Based Offline Digital Payment System

박기웅[1], 박규호[2]
Ki-Woong Park, Kyu Ho Park

(300-716) 대전시 동구 대학로 62 대전대학교 해킹보안학과 시스템보안연구실[1]
(305-701) 대전시 유성구 대학로 291 KAIST 전기및전자공학과 컴퓨터공학연구실[2]
woongbak@dju.kr, kpark@core.kaist.ac.kr

요 약

기존 온라인 및 오프라인 전자 지불 방식은 인증 및 검증 연산이 네트워크를 통해 이뤄지기 때문에 인프라에 완벽히 독립적이지 못하다. 본 논문에서는 저장된 데이터를 1회에 한하여 읽을 수 있는 메모리인"One-Time Readable Memory(OTM)"를 제안하고 이를 차세대 메모리 개발 플랫폼으로 구현하였다. 이를 기반으로, 기존 전자 지불 방식과 달리, 네트워크를 통한 인증 및 검증연산이 없는 전자 지불 시스템을 디자인 및 구현하였다. OTM에 저장된 화폐 가치에 대응되는 디지털 데이터는 송금자의 전자 지불 매체로부터 읽히는 순간 비가역적으로 삭제됨과 동시에 수취인의 전자 지불 매체로 이동되고 OTM에 저장된 데이터는 OTM으로만 이동이 되기 때문에, 저장된 데이터는 유일성을 지니게 되어, 화폐로서의 역할을 수행할 수 있는 특징을 갖는다. 따라서 본 논문의 전자 화폐 및 전자 지불 시스템은 기존 전자 지불 방식의 네트워크를 이용한 인증 및 검증 연산 없이 신뢰성 있는 방법으로 전자 거래를 수행할 수 있게 된다.

Abstract

Conventional online/offline digital payment schemes are not completely independent from infrastructure such as authentication or verification servers in the Internet. As a remedy to this limitation, we designed and implemented a new electronic medium for offline digital payment, called One-Time Readable Memory (OTM) using next-generation memory development platform. OTM can provide uniqueness for digital information by both atomic movement operation and mutual authentication among OTMs so that it can be utilized as a medium of digital payment. Consequently, OTM makes it possible to perform offline digital payments without the authentication or verification servers of the conventional digital payment schemes in the Internet.

키워드: 1회읽기메모리, 모바일 시스템, 오프라인 지불 방식
Keyword: One-Time-Readable Memory, Mobile System, Offline Digital Payment

※ 본 논문은 2012학년도 대전대학교 신진교수학술연구비에 의해 지원되었음.

논문투고일자 : 2013. 01. 07 심사일자 : 2013. 01. 09 게재확정일자 : 2013. 02. 15

1. 서론

인류 초기 상거래에서는 돌 또는 조개와 같은 화폐의 기능을 담당하는 교환 매체 및 주화가 사용되었으며, 경제 규모가 커지면서 화폐가 발명되어 사용되기 시작하였다. 지불 수단으로는 종이 화폐 또는 은행 수표와 같은 표시 화폐 사용에 이어서 신용카드, 직불카드 등의 신용 지불 수단이 사용되었고, 최근에는 IT 기술의 발달로 전자 상거래가 활발하게 이용되면서 디지털 수표, 직불카드, 신용카드, 디지털 쿠폰, 전자 현금 등과 같은 다양한 형태의 전자 지불 수단들이 이용되고 있다.

화폐가 통용될 수 있는 가장 큰 이유는, 각 화폐의 일련번호, 위조 방지 특성 등이 가미되어 각 화폐의 유일성(Uniqueness)이 보장되기 때문이다. 이러한 유일성으로 사람들은 돈을 주고받을 시에 온라인을 통한 확인 없이 거래가 가능한 것이다. 반면, 디지털 쿠폰 또는 디지털 머니와 같은 전자 지불 방식에 있어서는 화폐 역할을 하는 정보가 디지털 정보로 구성되어 있어 복제가 용이하고 유일성을 보장하기 힘들게 된다. 이와 같은 이유로, 기존의 전자 지불 방식[1−10]은 네트워크를 통한 온라인 인증과정 또는 검증과정[11−15,25]을 거치게 된다. 기존의 전자 지불 수단을 이용한 지불 방법은 크게 온라인방식 [1−10]과 오프라인방식[11−15], 두 가지로 나눠질 수 있다. 온라인 방식은 구매자의 지불계좌가 네트워크를 통하여 개설된 금융기관(은행 또는 카드사)과 연결되어 인증과정을 거친 후 지불대금을 이체시켜 주는 방식이다. 즉, 온라인 전자 지불 방식은 금융기관의 보안 서버를 통한 인증을 기반으로 이루어지기 때문에, 지불 시 상호간의 인증을 위해서 지불 단말기와 서버가 통신망을 통해 접속되어 있어야 한다. 따라서 온라인 전자 지불 방식은 상호 인증을 위한 인증 서버가 없으면, 거래가 성사될 수 없어 인프라에 의존적이며, 거래 단말기에서 서버로의 접속소요시간, 서버 처리 시간, 서버에서 단말기로의 전송시간 등으로 인해, 지불처리를 위한 지연 시간이 존재한다는 단점이 있다. 반면, 오프라인 전자 지불 방식은 거래 시 송금자와 수취인은 온라인을 통한 인증 절차를 거치지 않고 현금과 비슷한 거래를 수행할 수 있는 방식이다. 이는 인프라에 의존적이지 않아, 언제 어디서나 1:1 거래가 가능하게 만들며, 거래량 증가에 따른 인프라 및 인증 시스템 확충의 부담을 줄이는 장점을 가지고 있다[10]. 반면, 기존 오프라인 전자 지불 방식은 거래 후 네트워크를 통한 유효화 절차가 필요하여, 완전한 오프라인 전자 지불은 “제공되지 않는다[15, 16].”

본 논문은 오프라인 전자 지불 기술 분야의 기술적 요구에 부응하기 위한 것으로, 온라인을 통하지 않고 전자적으로 지불이 가능한 전자 지불 매체를 제안한다. 그러므로 본 논문에서 제안하는 전자 지불 시스템은 기존 오프라인 전자 지불 방식과 달리, 인프라에 완전히 독립적으로 전자 지불이 가능하다. 이를 위하여, 본 논문에서는 “One−Time Readable Memory (OTM): 1회 읽기 가능 메모리” 라는 전자 지불 매체를 새롭게 제안하고 이를 차세대 메모리 개발 플랫폼을 통하여 구현하였다. 송금자의 OTM에 저장된 화폐 가치에 대응되는 디지털 데이터는 송금자의 전자 지불 매체로부터 득출되는 순간 비가역적으로 삭제됨과 동시에 수취인의 전자 지불 매체로 복사가 아닌 이동되고 OTM에 저장된 정보는 OTM으로만 이동이 되기 때문에, 저장된 정보는 유일성을 지니게 되어, 화폐로서의 역할을 수행할 수 있는 특징을 갖는다. 따라서 본 논문에 따른 전자 지불 시스템은 기존의 전자 지불 방식의 네트워크 기반의 인증 및 검증 연산 없이 신뢰성 있는 방법으로 전자 거래를 수행할 수 있게 된다. 본 논문의 OTM은 더 나아가 저작권 관리(DRM), 디지털 쿠폰, 일회용 음원 서비스에도 활용될 수 있다.

본 논문의 구성은 2장에서 관련 연구로서 기존의 온라인/오프라인 디지털 전자 결재 방법의 소개를 통해 기존 연구의 동향을 살펴보고, 3장 에서는 OTM과 그를 활용한 오프라인 결재방법 및 구현된 프로토타입을 제시하며, 4장에서는 제안한 방법의

안정성 및 성능을 검증한다. 마지막 5장에서는 결론 및 향후 연구방향을 도출한다.

2. 관련 연구 및 차별점

IT 기술의 발전에 힘입어 기존 지폐 위주의 결제 수단의 많은 부분을 대체한 전자 지불 수단은 지불 인증 방법에 따라, 온라인 방식과 오프라인 방식으로 분류 될 수 있다. 본 장에서는 관련 연구로서 기존의 온라인/오프라인 디지털 전자 결재 방법을 소개를 통해 기존 연구와의 차별점 및 본 연구의 지향점을 살펴본다.

2.1 온라인 전자 지불 방법에 관한 연구

온라인 전자 지불 방식은 전자 거래마다, 인프라에 존재하는 인증 서버를 통해 거래를 수행하는 것으로서, 인터넷을 통한 용역 및 재화의 구매 시에 온라인 소액결제수단으로 주로 사용된다. iKP[1]는 IBM에서 개발된 온라인 전자 지불 방법으로, 비대칭키 기반의 암호 연산을 통하여, 발급자, 송금자, 수취인의 인증, 무결성 및 부인방지 기능을 제공하는 프로토콜을 제안하였으며, 이는 추후 SET [3]라는 프로토콜로 표준화 되었고, 현재는 PayPal [4]라는 서비스로 상용화 되었다. 이들의 암호학적 연산 오버헤드를 감소시키고, 웹상에서 자주 발생되는 소액결재를 위하여, Micro-Payment방법이 연구되었으며, 제안된 연구 결과로는 NetBill[8], CAFE[9], u-iKP[1], MiniPay[5] 등이 있다. Micro-Payment는 매번 온라인을 통한 인증 과정 없이, 해시 체인 생성 및 이에 대한 검증 방법을 통하여, 일정 금액 단위의 소액결제를 효율적으로 수행할 수 있는 방법을 제시하였다. NetCash[10]는 상기 제안된 방법의 익명성을 보장하기 위하여 인증서의 발급자를 제외하고 디지털 서명을 생성하는 Blind Certificate방법을 제안하기도 하였다. 이와 같은 온라인 전자 지불 방법은 대규모의 사용자를 확보한 대형 포털, 지속적인 수요를 갖는 콘텐츠를 확보한 방송사나 인터넷 교육 업체, 사용자에게 사이버 커뮤니티 혹은 온라인 게임 및 소셜 네트워크 서비스 사업이 성숙화 되면서, 인터넷상에서 통용되는 소액결제수단으로 활용되게 되었다[16]. 온라인 전자 지불 방법은 매우 성숙된 지불 방법으로서, 상용화가 되어 안전성이 검증된 시스템이라는 장점이 있는 반면, 지불시 상호간의 인증[26]을 위해서 송금자와 수취인 모두 네트워크에 지불 단말기와 인증 서버가 통신망을 통해 접속되어 있어야 한다. 그러므로 온라인 방식 전자 지불 방식은 웹서비스의 유료 서비스를 위해서는 매우 적합한 지불 방법이나, 네트워크에 의존적이고, 지불 단말기에서 서버로의 접속소요시간, 서버 처리 시간, 서버에서 단말기로의 전송시간 등으로 인해, 지불처리를 위한 지연 시간이 존재한다는 단점이 있다.

2.2 오프라인 전자 지불 방법에 관한 연구

오프라인 방식은 온라인 방식과 달리 실시간 인증 서버를 통한 인증이 필요하지 않다는 특징을 가지고 있다. 거래 시 송금자와 수취인은 온라인을 통한 인증 절차를 거치지 않고 현금과 비슷한 거래를 수행할 수 있는 방식이다. eCash, NetCash, CyberCoin은 대표적인 오프라인 전자 지불 방법으로서, 익명성과 중복 지출(Double Spending)을 방지할 수 있는 방법을 제시하였다. 이후 스마트카드의 개발에 따라 Mondex[12], CLIP[13], EMV[14] 등이 개발되었으며, 이는 IC 카드라는 물리적 매체에 전자적 가치를 저장하였다가 가맹점의 단말기 등을 통한 오프라인 소액 결제 수단으로 사용하는 방식이다. 오프라인 전자 지불 방식은 온라인 방식과 달리, 인프라에 의존적이지 않아, 언제 어디서나 1:1 거래가 가능하게 만들며, 거래량 증가에 따른 인프라 및 인증 시스템 확충의 부담을 줄이는 장점을 가지고 있다. 반면 오프라인 방식은 전자 지불의 안정성 및 보안성을 수취인과 송금자 내부에서 해결하여야 하므로, 위·변조 방지 기술과 중복 지출 방지 기술이 관건이다. 현존하는 오프라인 전자 지불 방식은 거래 시에는 오프라인으로 수행을 할 수 있으나, 주기적으로 서버에 접속하여 Black List의 업데이트 및

위 · 변조, 중복지출에 대한 검증이 수행된다. 그러므로 완벽한 오프라인 디지털 전자 지불 방식을 지원하지 못한다[11,15]. 이는 디지털기반 전자 지불 방식에서는 화폐의 정보가 디지털 정보로 표현이 되기 때문에, 진위 및 유효성을 판별하기 위한 암호 연산 및 온라인 검증 과정이 필요하기 때문이다.

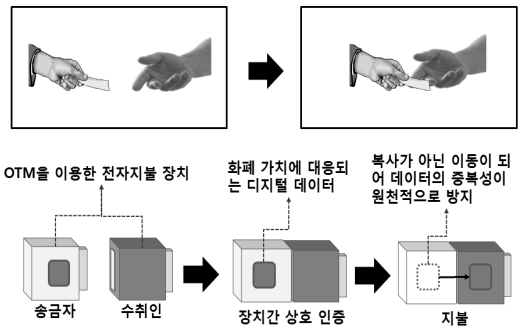
2.3 기존연구와의 차별점 및 지향점

본 논문에서 제안하는 OTM기반 오프라인 전자 지불 시스템은 기존 오프라인 전자 지불 방식의 위 · 변조 및 중복 지출에 대한 검증을 온라인이 아닌, OTM의 매체적인 특성을 이용하여 검증을 하는 것으로서, 디지털 기반의 전자 지불 시스템 임에도 불구하고, 완전한 오프라인으로 거래를 가능하게 한다. 또한 기존 EMV, NFC에 적용되어 보다 안전한 디지털 거래 매체로도 활용될 수 있다.

3. OTM 기반 오프라인 전자 지불 시스템

본 논문에서는 새로운 전자 지불 매체인 "One-Time Readable Memory (OTM): 1회 읽기 가능 메모리" 및 이를 이용한 전자 지불 프로토콜을 디자인 및 구현하였다. 본 논문에서 제안하는 전자 지불 시스템을 구현하기 위해, OTM은 다음과 같은 두 조건이 충족되어야 한다.

- 조건1) OTM에 저장된 데이터는 OTM으로만 이동이 가능해야 한다. OTM이 아닌 곳에서 OTM으로의 읽기 및 쓰기 연산은 발권자(예. 한국조폐공사) 만이 가능해야 한다.
- 조건2) OTM에 저장된 데이터는 한번만 읽기가 가능해야 한다. 예를 들어, 송금자의 OTM에 저장되어 있는 화폐 가치에 대응되는 디지털 데이터가 읽혀지는 순간 비가역적으로 삭제됨과 동시에 수취인의 OTM으로 복사가 아닌 이동된다.

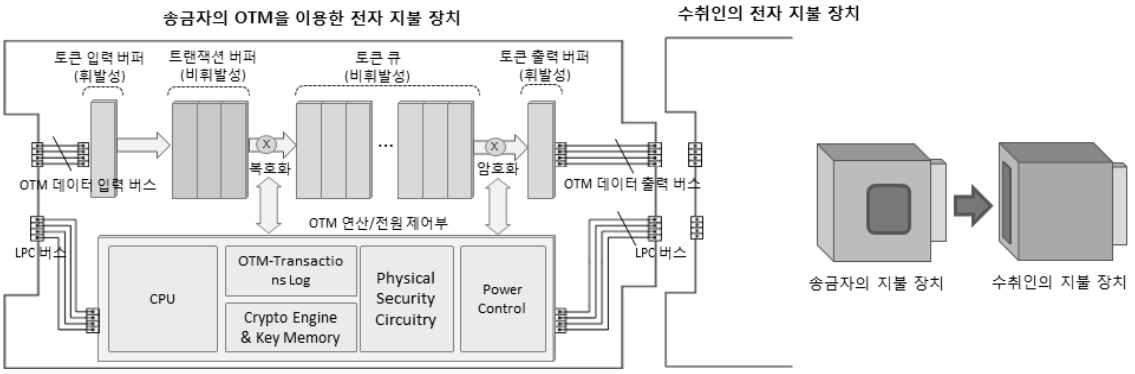


(그림 1) 화폐기반의 지불 방식과 OTM 기반 전자 지불 방식의 비교

위의 두 가지 조건을 만족하는 OTM은 내부에 저장된 디지털 데이터의 유일성을 보장할 수 있게 되어, 화폐를 이용한 거래방법과 동일한 방법으로 전자 거래를 할 수 있게 된다. (그림 1)은 기존 화폐 기반의 지불 방식과 OTM 기반 전자 지불 방식을 비교한 것이다. 예를 들어, 송금자가 수취인에게 특정 금액을 송금한다고 가정하면, 송금자의 OTM과 수취인의 OTM을 체결하여 조건1을 만족시키기 위한 인증을 수행한다. 인증 후에는 화폐 가치에 대응되는 디지털 데이터가 송금자의 OTM에서 수취인의 OTM으로 전송이 되는데, 조건2를 만족하는 OTM의 특징으로, 송금자의 메모리에 저장된 디지털 데이터는 수취인으로 복사가 아닌 이동이 된다. 이 때문에, 저장된 정보는 유일성을 지니게 되어, 화폐 가치에 대응되는 디지털 데이터는 화폐로서의 역할을 수행할 수 있게 된다. 이를 통해, 완전한 오프라인 방식으로 전자 지불을 가능하게 하는 것이다. 이번 장에서는 조건1 및 조건2를 만족시키기 위한 하드웨어적 구현과 전자 지불 "프로토콜을 설명한다."

3.1 OTM 기반의 전자 지불 시스템 구조

본 논문에서 제안하는 "One-Time-Readable Memory (OTM)"란 여러 번 저장 및 읽기가 가능한 특성을 가진 일반적인 메모리와 달리, 기록은 여러 번 가능하나, 읽기는 한 번만 가능한 메모리로 정의된다. 이는 쓰기(write) 연산을 통하여 기록하



(그림 2) OTM 기반 전자 지불 장치의 내부 및 체결 구조

면 비휘발성 메모리와 같이 전원이 차단된 후에도 데이터가 보존되나, 해당 데이터를 읽는 순간, 저장된 메모리는 물리적으로도 복구가 되지 않도록 삭제가 되는 특성을 가지고 있는 메모리이다.

(그림 2)는 OTM기반의 전자 지불 장치의 구조를 나타낸다. 제안하는 지불 장치는 OTM, OTM 연산/전원 제어부, 다른 전자 지불 장치와의 통신을 위한 데이터 버스 등으로 구성된다. OTM은 비휘발성 메모리인 토큰 큐와 트랜잭션 버퍼, 그리고 휘발성 메모리인 토큰 입출력 버퍼로 구성된다. OTM은 토큰 단위로 데이터를 저장하는데, 토큰은 화폐 가치에 대응되는 디지털 데이터를 의미한다.

3.1.1 OTM간 상호 인증(조건1)을 위한 시스템 구성

오프라인 전자지불에서 디지털 정보의 유일성을 보장해 주기 위해서는 OTM 내부에 저장된 토큰은 OTM으로만 이동이 가능해야 한다. 이를 위해서는 송금자의 OTM, 수취인 OTM 간 상호 인증 및 Secure Mount 메커니즘이 필요하다. 두 OTM 사이의 상호 인증 및 Secure Mount를 위한 프로토콜은 LPC(Low Pin Count)버스[24]를 통하여 수행된다. OTM 연산/전원 제어부 내부에는 자신이 OTM임을 입증하는 개인키 및 발권 일련번호를 이용한 인증 연산을 통해 서로가 OTM임을 증명하기 위한 상호 인증을 수행한다. 여기서 OTM에 저장되어 있는 개인키 정보는 OTM 연산/전원 제어부만이 읽을 수 있게 된다. 이와 같은 특성을 가진 반도체 모듈의 예로는 신뢰성 플랫폼 모듈(TPM: Trusted Platform Module)을 들 수 있다. 본 논문에서 제안하는 전자 지불 장치도 하나의 반도체로 집적되고, TCPA[22,27]에 따른 내부 정보 보호기술에 의해 보호되는 것이 필요하다. OTM 전원 제어부는 OTM에 인가되는 전원을 제어하는 모듈로서, 상호 인증이 성공적으로 완료된 후에만 OTM에 전원을 공급한다.

3.1.2 1회 읽기 특성(조건2)을 위한 시스템 구성

OTM은 토큰 이라고 하는 정해진 크기의 단위로만 데이터를 읽고 쓰는 특성을 갖는다. OTM 내부의 토큰 큐에 저장된 토큰의 개수에 따라 사용자가 소지하고 있는 화폐의 가치가 결정된다. 결국 OTM 기반의 거래 방식에서는 주고받는 토큰의 개수에 비례하여 화폐의 거래량이 결정되게 된다. OTM은 일반 메모리에서 주소(Address)를 입력하여 메모리의 특정 위치에 저장된 데이터를 가져 올 수 있는 것과 달리 FIFO(First-In First-Out)기반으로 먼저 기록된 토큰부터 순차적으로 읽혀진다. 읽혀진 데이터는 OTM 연산/전원 제어부에 의해 암호화/복호화 후에 OTM 데이터 입출력 버스로 연결되어 송수신 된다. 만약 하나의 OTM기반의 전자 지불 장치가 다른 OTM기반의 전자 지불 장치로부터 토큰을 수신할 경우, 수신된 토큰은 토큰 입력 버퍼에서 OTM 트랜잭션 버퍼로 일시적으로 저장된다. 이때 트랜잭션 버퍼에 저장된 토큰은 암호화가 되어있어

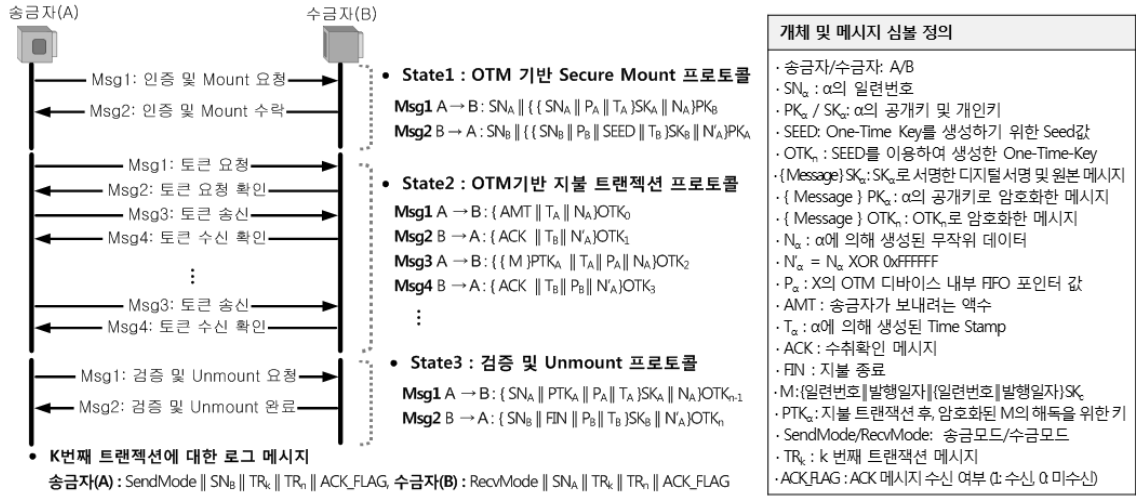
화폐로서 사용이 될 수 없으나, 토큰 전송 완료 후, 연산/전원 제어부는 OTM 트랜잭션 버퍼에 저장된 암호화된 토큰의 복호화 키를 수신하여, 트랜잭션 버퍼에 저장된 정보를 복호화 하여 토큰 큐에 저장한다. 이때, 송금자 측 토큰 큐에서 읽혀진 토큰은 수신자 측 토큰 입력 버퍼로 이동함과 동시에 비가역적으로 삭제되고, 현재의 트랜잭션 정보를 OTM 트랜잭션 로그에 기록하게 된다. 하나의 토큰이 송금자측 토큰 큐에서 수취인의 토큰 입력 버퍼에 저장되는 연산은 중간에서 중지될 수 없는 원자적 연산(Atomic Operation)으로 수행 된다. 이는 송금자 측의 OTM으로부터 출력된 토큰이 다시 송금자 측의 토큰 큐에 쌓이는 것을 막을 수 있어 조건2를 만족시킬 수 있게 된다.

3.2 OTM 기반 오프라인 전자 지불 프로토콜

(그림 3)은 OTM 기반 전자 지불 프로토콜을 나타낸 것으로서, 본 논문에서 제안하는 OTM 기반 오프라인 전자 지불 프로토콜은 3개의 State로 구성된다. 송금자의 OTM 장치와 수취인 OTM 장치의 상호 인증 및 Secure Mount를 수행하는 State1, Secure Mount 후에 전자 지불 연산을 위해 토큰을 전송하는 State2, 전자 지불 연산 완료 후 연결 해제 (Unmount) 및 검증 연산을 수행하는 State3로 구성된다. 예를 들어, 송금자와 수취인의 OTM 디바이스를 체결하여 전자 지불 프로토콜을 수행한다고 가정하면, 상호간의 인증을 위하여 State1에 진입하여 상호 인증을 수행한 후 Secure Mount를 하게 된다. Mount 후에는 송금자의 OTM에 저장되어 있던 토큰을 수취인의 OTM으로 이동하기 위한 State2로 진입하게 된다. 토큰을 전송한 후에는 State3에 진입하여 Unmount 연산 및 검증 연산을 수행하게 된다. 본 장에서는 각 상태를 처리하는데 필요한 메시지 및 "연산 프로토콜을 기술하였다."

3.2.1 State1: OTM 기반 Secure Mount 프로토콜

State1의 상호 인증에서 상대방의 공개키는 OTM 내부 연산/제어모듈에 저장되어 있으며, 연산/제어모듈 내부에서 상대방의 일련번호(SN)와 해시함수(SHA-1)를 이용하여 공개키를 유도하여 인증을 수행한다. 예를 들어, 전자 지불 매체의 SN이 16비트이고, 해시함수의 출력이 N 비트라면, 2^{16}개의 가능한 SN 집합은 2^N개의 공개키 쌍에 매핑이 되며, 연산/제어모듈내부에는 2^N개의 공개키와, 자신의 개인키가 저장되어 있다. 본 논문의 시스템에서는 해시함수 출력 값의 LSB(Least Significant



(그림 3) OTM 기반 오프라인 전자 지불 프로토콜

Bit) 10비트를 SN와 공개키 간의 매핑에 사용을 하였으며, 1024개의 공개키 테이블(128KB)이 OTM 내부 EEPROM에 저장되도록 구현을 하였다. 즉, 상대방 전자 지불 장치의 16비트 SN값을 수신하면, 내부 해시 매핑함수에 따라 그에 해당하는 공개키 값($PK_{A/B}$)을 얻을 수 있게 된다. 이러한 인증 연산은 송금자의 전자 지불 매체 및 수취인의 전자 지불 매체가 모두 OTM으로 구성된 전자 지불 매체라는 사실을 확인할 수 있도록 하고, 인증서와 디지털 서명 및 암호화의 사용은 결재의 안전성을 제공한다. 또한 각 전자 지불 매체의 토큰큐 포인터(P_α)는 OTM 내부 토큰큐에 Push/Pull이 될 위치를 저장하고 있으며, P_α값은 연산/제어 모듈 내부 메모리에 저장되고, 상대 OTM 전자 지불 매체로의 P_α값 전송은 LPC 버스로 전송되어 TCPA 기술에 의해 보호가 되어, 사용자 임의의 P_α값 조작은 불가능하게 된다. Seed값은 추후 송금자와 수취인 사이의 메시지 암호화에 사용될 1회성 키(OTK: One-Time Key)를 생성하는데 사용되는 Seed값이다. 이는 OTK를 생성하기 위한 난수생성기(Random Number Generator)의 Seed값으로 사용되며, 송금자/수취인의 전자 지불 매체는 n 번째 메시지에 대하여 수식 (1)을 이용하여 One-Time-Key (OTK_n)를 유도하여, 토큰을 암호화 시킨다. 상기 RNG는 통상적으로 사용되는 RC4[17], Rabbit[18], SEAL[19] 등의 스트리밍 암호화 알고리즘을 적용할 수 있다. 본 논문에서는 SEAL을 적용하여 구현하였다.

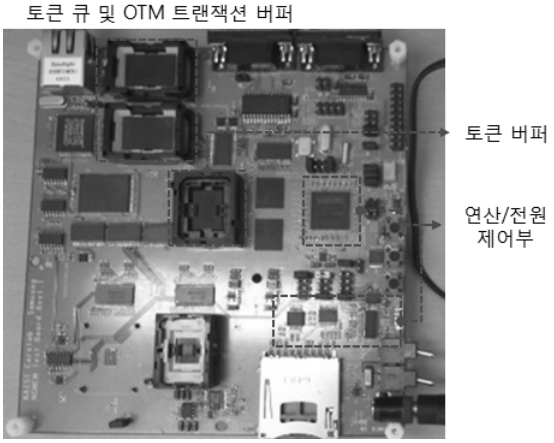
$$OTK_n = RNG(OTK_{n-1})\ n>1,\ OTK_0 = RNG(SEED) \quad (1)$$

3.2.2 State2: OTM 기반 지불 트랜젝션 프로토콜

State2는 State1의 상호 인증 및 Secure Mount 수행 후 실질적인 거래를 수행하는 상태로서, 송금자는 수취인에게 보낼 액수를 통보하고 (Msg1), 수취인은 이에 대한 ACK 메시지(Msg2)를 보내며, 이후 약속된 금액만큼 송금자와 수취인의 OTM 전자 지불 매체간 데이터를 송수신하는 단계 (Msg3, Msg4)로 구성된다.

Msg1/Msg2을 통하여 송신할 금액(AMT)을 확정지으며, Msg3/Msg4를 통하여 "AMT/토큰" 횟수만큼 반복하여 토큰을 전송하게 된다. 예를 들어, 하나의 토큰의 단위가 1,000원이고, 8,000원을 전송할 경우 8개의 토큰을 전송하게 된다. 연산/전원 제어부는 Msg3 – Msg4 트랜잭션의 원자성(atomicity)을 보장하도록 구현 되었다. 그러므로 지불 트랜잭션이 전원 차단 및 물리적 체결 중단으로 중단이 되었을 경우, 수취인은 암호화된 화폐 가치에 대응되는 디지털 정보({M}PTK_A)를 받았기 때문에 화폐로서 활용이 될 수 없게 된다. 단, Msg3 – Msg4의 트랜잭션이 원자적으로 수행되어 정보의 소실은 발생하지 않게 된다. 이와 같은 지불 트랜잭션의 연산 지속성을 보장해 주기 위하여, Msg1 – Msg4가 송수신 되는 순간, 송금자/수취인의 OTM 전자 지불 매체 내부에는 트랜잭션 로그 메시지를 OTM 연산/전원 제어부 내에 OTM 트랜잭션 로그에 기록하게 된다. 예를 들어 8,000을 전송하기 위해 8번의 지불 트랜잭션을 수행해야 하나, 4번 트랜잭션에서 프로토콜이 중단되었을 경우 OTM 트랜잭션 로그에 기록된 정보를 이용하여 OTM 전자 지불 매체가 재체결 시 연산을 지속시켜 나갈 수 있게 된다.

본 논문에서 OTM에 저장되는 단위인 토큰은 화폐의 가치와 매핑 되며, 각 토큰은 디지털 정보 블록이 이어진 일련의 스트링(string)으로 저장된다. 여기서 각 토큰(M)을 구성하는 하나의 디지털 정보 블록은, (그림 3)에 도시된 바와 같이, 발권날짜, 일련번호(SN), 및 발권자의 개인키 (SK_C)를 이용하여 추출된 "발권날짜"와 "지폐일련번호"의 정보 및 이에 대한 디지털 서명을 포함한다. 수취인은 발권자의 공개키(PK_c)를 이용하여, 진위 여부를 판별할 수 있다.



(그림 4) OTM 기반 오프라인 전자 지불 장치 플랫폼

3.2.3 State3: 검증 및 Unmount 프로토콜

State3는 State2를 통해 수행했던 지불 연산의 검증 및 종료를 위한 프로토콜로서, 송금자는 M을 암호화 하는데 사용하였던 PTK_A값을 전송해 주어 수취인이 해독하여 수취인의 토큰큐에 저장해 줄 수 있도록 하고, 수취인은 송금자 전자 지불 매체의 포인터 값의 변화, 즉, State1의 P_A값과 State3의 P_A값의 차이 값을 이용하여, 수취인이 수신한 토큰 개수와, 송금인이 전송한 토큰 개수의 비교를 통하여, 검증을 해 볼 수 있게 된다.

3.3 OTM 기반 전자 지불 시스템 구현

본 논문의 OTM으로 구성되는 전자 지불 매체는 하나의 반도체 칩으로 구성되는 것을 필요로 한다. 그러나 현재는 이와 같은 기능을 모두 지원할 수 있는 메모리 반도체가 존재 하지 않기 때문에 본 논문에서는 (그림 4)의 차세대 메모리 개발 보드를 이용하여 OTM의 하드웨어적 특성을 구현하였다.

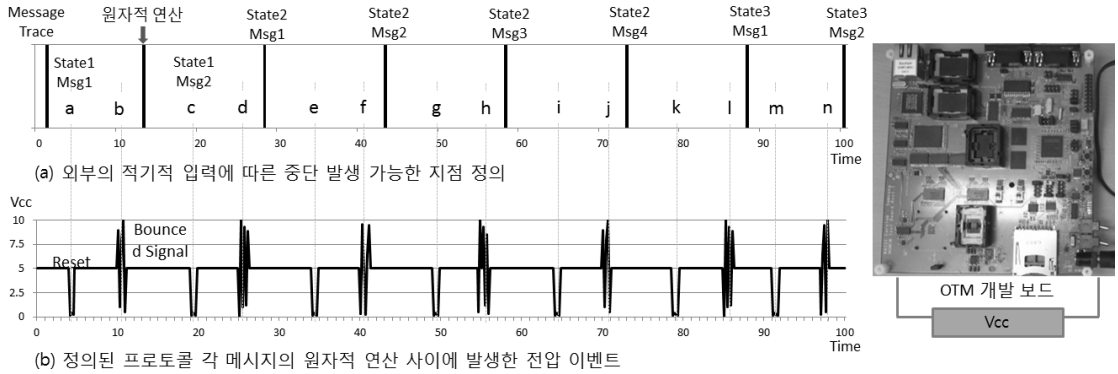
차세대 메모리 보드는 다양한 종류의 메모리 반도체를 테스트 할 수 있도록 설계하여 OTM 소자가 요구하는 비휘발성 및 휘발성 메모리 모두를 포함한다. 현재 개발 보드에서는 비휘발성인 NAND 플래시 메모리를 토큰큐로 맵핑하여 사용하고 휘발성 SRAM의 일종인 UtRAM[23]을 토큰 버퍼로 사용한다. 또한 개발 보드는 ARM 기반의 S3C2443 CPU를 사용하는데 이를 OTM 제어부로 사용함으로써 OTM에서 필요한 인증 연산 및 OTM 소자 제어를 수행한다. 마지막으로 개발된 보드의 2개의 스위치를 이용하여 OTM에 필요한 전원을 선택적으로 공급할 수 있도록 구현하였고 OTM이 분리된 경우 전원 스위치가 꺼진 것으로 맵핑하여 전원이 꺼질 시에 토큰큐에서 나온 데이터가 토큰 버퍼에 존재하더라도 전원이 꺼짐과 동시에 저장된 토큰이 제거되는 동작으로 구현하였다.

4. 안정성 및 성능 분석

본 장에서는 본 논문에서 제안하는 OTM기반 전자 지불 장치 및 프로토콜의 연산적 안정성 및 효율성을 평가하였다. 연산적 안정성이란, OTM기반 전자 지불 프로토콜 수행 중 외부적 요인에 의해 중단이 되더라도, 송금자와 수취인의 OTM 전자 지불 매체가 재결합 시에는 연산을 이어서 할 수 있는 연산적 안정성을 의미한다. 또한 본 논문에서 제안하는 OTM 기반 전자 지불 프로토콜의 연산 효율성을 평가하기 위하여 지불 트랜잭션의 양에 따른 연산 오버헤드 및 OTM 용량 오버헤드를 측정하였다.

4.1 제안한 OTM 기반 시스템의 연산 안정성 평가

시스템의 연산 안정성은 화폐 가치에 대응되는 디지털 정보를 송금자와 수취인이 안전하게 주고받기 위해 보장되어야 한다. 본 시스템에서는 연산 안정성을 평가하기 위하여 (그림 5)에 나타낸 것과 같이, 실제 구현된 OTM 시스템에 외부 전기적 충격을 유입시켜 지불 트랜잭션 수행 중 외부적 요인에 의해 중단이 되더라도 향후 수행됐던 연산을 지속시킬 수 있는지의 여부를 평가하였다. 화폐 가치에 대응되는 디지털 정보의 전송을 위한 송금자와 수취인간의 일련의 과정은 복수의 메시지를 주고받고 각자의 메모리에 읽고 쓰는 등의 작업들로 이루어져 있다. 연산적 안정성을 검증하기 위하여, 지불 트랜잭션을 수행하는데 외부적 입력에 따른 중단 발생 가능한 지점을 정의하고, 해당 지점에 외부 전



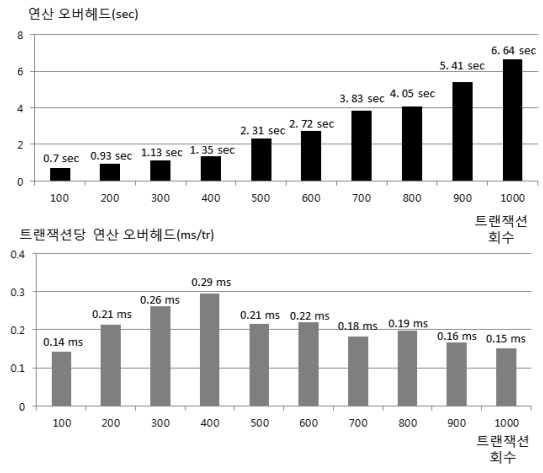
(그림 5) OTM 기반 전자 지불 플랫폼 연산 안정성 평가를 위한 외부 전기 입력 패턴

기적 입력을 가하여 안정성을 평가하였다. 검증을 수행하는데 있어서, 각 메시지의 내부 트랜잭션의 원자적 연산은 하드웨어에 의하여 보장된다고 가정을 하였고, 본장에서 검증하고자 하는 것은 하드웨어로 보장되는 여러 개의 원자적 연산들 간의 연산 안정성을 평가하는 것이다. (그림 5-a)는 외부적 입력에 따른 중단 발생 가능한 지점을 정의한 것이고, (그림 5-b)는 정의된 프로토콜 각 메시지의 원자적 연산사이에 발생한 전압 이벤트(Reset, Bounced Signal)을 나타낸 것이다. 정의된 (a, c, e, g, I, k, m)이벤트는 OTM 개발 보드에 Reset 신호가 가해진 경우이고 이는 실 상황에서 배터리 소진 또는 사용자에 의한 전원 차단 시의 상황에 해당된다. 정의된 (b, d, f, h, j, l, n)이벤트는 송금자와 수취인의 OTM 장치의 체결이 프로토콜 수행 중 중단이 되었을 경우, OTM 개발 보드에 외부적 전기 충격이 가해졌을 경우 또는 송금자와 수취인의 OTM 기기 사이의 신호 접촉이 불량했을 경우에 해당된다. 안정성을 평가하기 위하여 각 상황에 있어서 Voltage Regulator 장비를 이용하여 프로토콜 수행 중 (그림 5-b)에 해당하는 신호를 입력시킨 후, 프로토콜의 연산적 상태에 이상이 없는지, 송금자와 수취인의 OTM 장치가 다시 연결이 되었을 경우 이전의 프로토콜 상태가 유지가 되는지에 대한 실험을 수행을 하였다.

정의된 이벤트 (a, b, c, d)의 경우 인증 연산 중간에 외부적 전기 충격이 유입된 경우로서, 재체결 시에는 인증 연산(State1)부터 다시 시작이 되는 것을 확인할 수 있었고, (e, f, g, h, i, j, k, l, m, n)의 경우 인증 연산 후 지불 트랜잭션 중 외부적 전기 충경이 유입된 경우로서, 이 경우에는 재체결 시, OTM 내부에 저장되어 있던 로그 정보에 의하여 프로토콜이 계속적으로 수행되고 최종 완료가 되어, 어느 상황에서도 정상적인 동작 및 최종완료가 되는 것을 확인 할 수 있었다.

4.2 제안한 OTM 시스템의 연산 효율성 평가

안전하고, 정상적인 동작의 평가와 함께 이루어져야 하는 것이 연산 및 메모리 사용의 효율성이다. 화폐 가치에 대응되는 디지털 정보를 주고받는 데에 있어서 연산의 시간이 길어지면, 사용성이 떨어질 수 있으며, 화폐 가치에 대응되는 디지털 정보를 저장하는데 소요되는 메모리 사용량 역시 실효성 여부를 판별하는데 있어서 중요한 평가요소가 될 수 있다. 본 장에서는 제안하는 OTM 기반 전자 지불 프로토콜의 연산 효율성을 평가하기 위하여 지불 트랜잭션의 양에 따른 연산 오버헤드 및 OTM 용량 오버헤드를 측정하였다. (그림 6)은 트랜잭션 횟수에 따른 연산 지연시간을 측정한 것으로서, OTM 전자 지불 매체의 최소 단위가 1,000원일 경



(그림 6) 트랜잭션 횟수에 따른 연산 오버헤드

우 10번의 트랜잭션으로 10,000원을 전송할 수 있다. 본 실험에서는 트랜잭션의 횟수를 100에서 1,000까지 증가시키며 연산효율성을 측정하였다. 트랜잭션의 횟수가 증가함에 따라 연산 오버헤드 역시 증가하는 것을 관찰할 수 있다. 하지만, 트랜잭션의 횟수에 비례하여 증가하지 않는 것을 확인 할 수 있는데, 이는 상호 인증 (State1) 및 검증 (State3)는 비대칭키 연산을 수행하여 연산오버헤드가 큰 반면, 실질적인 트랜잭션 (State2)는 대칭키 기반의 연산을 수행하기 때문에 트랜잭션의 횟수가 증가함에 따라 트랜잭션 당 연산 오버헤드는 감소하는 것을 관찰할 수 있었다. 본 실험에서 지불매체의 최소단위가 1,000원일 경우 50만원을 전송하는데 있어서 약 2.31sec가 소요되나, 이는 트랜잭션의 기본 단위 또는, OTM 내부 연산 모듈에 따라 지연시간을 더욱 감소될 수 있다.

5. 결론 및 추후연구

본 논문에서는 1회 읽기 메모리(OTM)을 제안하였고, 그를 이용한 오프라인 전자 지불장치를 나타내었다. 본 논문의 전자 지불 매체는 제안된 전자지불 프로토콜과 더불어 정보의 유일성을 제공하여 화폐와 동일하게 사용될 수 있고, 온라인을 통한 인증절차 없이 전자 지불이 가능하여 금융기관 및 네트워크를 이용하는 복잡한 인증 작업 없이 (Infra-less) 디지털 기반 거래를 편리하고 신뢰성 있는 방법으로 행할 수 있다. 본 논문에서 제안한 디지털 매체 One-Time-Readable 메모리는 본 논문에 기술된 상호 인증 성 및 원자적 정보 이동 등의 두 조건이 만족되어야 보안성이 보장되는 바, 제안한 메모리 소자의 구현 가능성에 대해서 분석이 추후 과제로서 존재한다. 또한 기존 EMV, NFC에 적용되어 보다 안전한 디지털 거래 매체로도 활용될 수 있다. 추후 연구로서, OTM 소자를 이용한 전자 지불 매체에서는 디지털 정보의 유일성이 보장되어, 디지털 쿠폰, DRM(Digital Right Management), 인증 서비스, 일회용 음원 서비스 등 기존 온라인 기반 보안 서비스가 오프라인으로 가능하게 하는 시스템으로 확장할 수 있을 것이다.

참고문헌

[1] M. Bellare, Etc., "Design, implementation and deployment of the iKP secure electronic payment system", IEEE Journal on Selected Areas in Communications, 18(4):611-627, April 2000.

[2] Chaum, D, Fiat, A, and Naor, M, "Untraceable electronic cash", In Proceedings on Advances in Cryptology. S. Goldwasser, Ed. Springer-Verlag New York, New York, NY, 319-327, 1990.

[3] Kungpisdan, S., Srinivasan, B., and P. Dung,"A Practical Framework for MobileSET Payment", Proceedings of International ESociety Conference, 2003b, pp. 321-328

[4] On-Line PayPal Payment Service, "https://www.paypal.com", Paypal Co.Ltd, 2010

[5] A. Herzberg, H. Yochai, "Mini-pay: charging per click on the web", in: 6th World Wide Web Conference, Santa Clara, USA, April 1997.

〔6〕 R. Rivest, A. Shamir, "PayWord and MicroMint: two simple micropayment schemes", 1996 International Workshop on Security Protocols, Lecture Notes in Computer Science, vol. 1189, Springer, pp. 69 - 87

〔7〕 V. Patil, R.K. Shyamasundar, "An efficient, secure and delegable micro-payment system", 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, Taipei, Taiwan, 28 - 31 March 2004

〔8〕 B. Cox, J. D. Tygar, and M. Sirbu, "NetBill Security and Transaction Protocol,"Proc. First Usenix Electronic Commerce Workshop, Usenix, Berkeley, Calif., July 1995, pp. 77-88.

〔9〕 T. Pedersen, "Electronic Payments of Small Amounts," Lecture Note in Computer Science, No.1189, 1996, pp. 59-68.

〔10〕 G. Medvinsky and B.C. Neuman, "NetCash: A Design for Practical Electronic Currency on the Internet," Proc. First ACM Conf. Computer and Comm. Security, pp. 102-106, Nov. 1993.

〔11〕 G. Damme, "Offline NFC Payments with Electronic Vouchers", Proc. ACM MobiHeld 2009

〔12〕 Mondex Service, http://www.mondex.com/, 2010

〔13〕 CLIP, http://www.europay.com/, EuroPay Co.Ltd 2010

〔14〕 Smart Card Alliance Press, " http://www.smartcardalliance. org", 2010

〔15〕 C. Popsecu, "A Fair Off-Line Elctronic Cash System with Anonymity Revoking Truetee", Proc. ICTAMI 2004

〔16〕 김수형, 조진만, 문기영, 장종수, "국내 네트워크형 전자화폐 동향 및 시사점", 전자통신도양분석 제 19권 제4호 2004년8월

〔17〕 RSA Laboratory, "RC4 Specification", Technical Report 1994, RSA Press

〔18〕 M. Boesgaard, M. Vesterager, and E. Zenner., "The Stream Cipher Rabbit. New Stream Cipher Designs", Lecture Notes in Computer Science, 4986:69-83, 2008

〔19〕 P. Rogaway and D. Coppersmith, "A Software-Optimized Encryption Algorithm", Fast Software Encryption, Cambridge Security Workshop Proceedings,Springer-Verlag, 1994, pp. 56-63.

〔20〕 Samsung Press, "Datasheet: S3C2443 (ARM920T)", 2013

〔21〕 Samsung Press, "Datasheet: K9F2G08UXA (NAND flash memory)", 2013

〔22〕 Siani Pearson, Boris Balacheff, "Trusted computing platforms: TCPA technology in context", Prentice Hall. ISBN 0130092207.

〔23〕 Samsung Press, "Datasheet: K1S3216BCD (Uni-transistor random access memory)", 2010

〔24〕 Intel Press, "Low Pin Count Interface Specification Document", INTEL Development Center, 2012

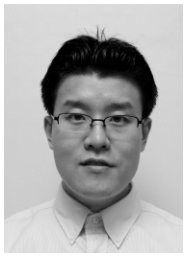
〔25〕 서병문, "랜덤 넌스와 타임스탬프 기반의 개선된 사용자 인증 스킴", 한국차세대컴퓨팅학회 논문지, Vol.8 No.6, pp.69-76, 2012년 12월

〔26〕 박미옥, "각 객체의 전방향 안전성과 해쉬연산 로드를 개선한 공개 채널상의 RFID 상호인증 프로토콜", 한국차세대컴퓨팅학회 논문지, Vol.6 No.5, pp.20-26, 2010년 10월

〔27〕 이영석, 유용덕, 박상현, 최훈, "웨어러블 컴퓨터 보안", 한국차세대컴퓨팅학회 논문지, Vol.2 No.2, pp.23-31, 2006년 6월

저자소개

◆ 박 기 웅



- 2005년 연세대학교 Computer Science 학사
- 2007년 KAIST Electrical Engineering 석사
- 2012년 KAIST Electrical Engineering 박사
- 2008년 Microsoft Research Graduate Fellow
- 2012년 국가보안기술연구소 연구원
- 2012년 ~ 현재 대전대학교 해킹보안학과 조교수
- 관심분야 : 시스템 보안, 모바일-클라우드 컴퓨팅, 보안 프로토콜, 디지털 포렌식 등

◆ 박 규 호

- 1973년 서울대학교 Electrical Engineering 학사
- 1975년 KAIST Electrical Engineering 석사
- 1983년 Paris XI대학 Computer Engineering 박사
- 1983년 ~ 현재 KAIST 전기 및 전자공학과 교수
- 관심분야 : 운영체제, 매니코어 시스템, 차세대 비휘발성 메모리, 플래시 메모리 등