情報保護學會論文誌
第19卷 第5號, 2009. 10

VANET를 위한 차량자체 갱신가능 익명ID 시스템*

김 상 진,[1†] 이 병 우,[2] 오 희 국[2‡]
[1]한국기술교육대학교, [2]한양대학교

Self Updatable Pseudonym System for VANET*

Sangjin Kim,[1†] Byeongwoo Lee,[2] Heekuck Oh[2‡]
[1]Korea University of Technology and Education, [2]Hanyang University

요 약

차량 애드혹 네트워크(VANET, Vehicular Ad hoc NETwork)에서 차량 간 교환되는 메시지가 위·변조되면 심각한 결과를 초래할 수 있어 중요 메시지의 인증은 반드시 필요하지만 이를 위해 일반 전자서명 기법을 사용하면 프라이버시가 침해될 수 있다. 따라서 VANET에서는 프라이버시를 보장하지만 문제를 발생시킨 차량을 식별할 수 있는 조건부 익명성이 제공되어야 한다. 이 논문에서는 각 차량에서 자체적으로 조건부 익명성이 보장되는 익명ID를 재암호화 기법을 이용하여 갱신할 수 있으며, 익명ID에 대한 표현문제를 이용하여 메시지를 서명한 다음 다른 차량에게 전달할 수 있는 VANET를 위한 새로운 인증시스템을 제안한다. 이 시스템은 ID의 사용기간을 제한하여 개별ID의 철회가 불필요하며, 필요할 경우에는 특정 차량의 서비스 참여를 제한시킬 수 있다. 제안된 시스템의 안전성은 일부 조작불가능한 하드웨어를 통해 제공하고 있다.

ABSTRACT

Since message forgery or alteration in VANET may cause severe consequences, authentication of critical messages must be provided. However, using normal digital signature may infringe privacy of drivers. Therefore, VANET requires authentication systems that provide conditional anonymity. In this paper, we propose a new authentication system for VANET. In our proposed system, each vehicle can update its pseudonym using re-encryption technique and digitally sign messages using representation problem on the pseudonym. By limiting the usage period, revocation of individual pseudonym is not required. Moreover, we also provide a way to revoke the vehicle itself. Secureness of our system partially rely on the usage of tamper-resistance hardware.

Keywords: VANET, conditionally anonymity, re-encryption, representation problem

I. 서 론

최근에 OBU(On-Board Unit)라고 하는 무선 통신을 지원하는 컴퓨팅 시스템을 차량에 설치하여 차량 간 통신(V2V, Vehicle to Vehicle)과 도로에 설치된 RSU(Road-Side Unit)를 이용한 차량과 인프라 간 통신(V2I, Vehicle to Infrastructure)을 통해 지능적인 서비스를 제공하는 차량 애드혹 네트워크에 대한 연구와 표준화가 활발히 진행되고 있다[1-7]. 사고가 발생하였을 때 접근하는 차량에게 응급신호를 보내는 안전운행 서비스, 신호등이 없는 교차로나 차선 변경할 때 서로 메시지를 교환하는 협력운전 서비스가 VANET에서 제공될 수 있는 대표적인 서비스이다[6].

VANET의 각 차량은 이와 같은 지능서비스를 실

접수일(2009년 5월 29일), 게재확정일(2009년 7월 27일)
* 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임. (KRF-2008-313-D01024)
* 이 논문은 2009년도 한국기술교육대학교 연구제 파견연구비 지원에 의하여 연구되었음.
† 주저자, sangjin@kut.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr

현하기 위해 자신의 상태와 관련된 정보(위치, 속도, 가속, 방향 등)를 지속적으로 주위 차량과 RSU와 교환하게 되며, 각 차량은 이와 같은 정보를 취합 및 해석하여 활용하게 된다. VANET은 다른 무선애드혹 네트워크와 마찬가지로 다중 홉 방식으로 데이터를 교환할 수 있지만 안전 운행과 관련된 메시지는 보통 단일 홉 방송(one-hop broadcasting)을 통해 전달된다[7].

안전 운행과 관련된 메시지의 내용이 거짓 정보이거나 내용이 위·변조되면 고의로 사고가 유발될 수 있어 적절한 보안 메커니즘 없이는 VANET를 이용한 안전운행 또는 협력운전 서비스를 도입하기 어렵다. 따라서 VANET에서 교환되는 개별 메시지의 인증은 반드시 제공되어야 한다. 하지만 단순히 전자서명을 통해 메시지를 서명하여 교환하면 현대 사회에서 중요시 여기는 프라이버시 문제를 야기 시킨다. 따라서 VANET에서는 일반 차량의 프라이버시는 보장하지만 악의적인 행동을 한 차량이나 사고에서 책임자를 선별할 수 있는 조건부 익명성이 지원되어야 하다.

VANET에서 조건부 익명성을 제공하기 위해 익명 인증서나 익명식별자를 이용한 신원기반 시스템을 사용할 수 있다. 하지만 프라이버시나 익명을 고려할 때 단일 메시지만을 생각하지 않는다. 즉, 불관찰성(unobservability) 뿐만 아니라 불연결성(unlinkability)을 제공해야 한다. 여기서 불관찰성이란 각 메시지가 어떤 차량에 의해 전송되었는지 알 수 없어야 한다는 것을 말하며, 불연결성이란 동일 차량에 의한 여러 메시지를 서로 연결할 수 없어야 한다는 것을 말한다. 불연결성은 하나의 메시지의 익명성이 철회되었을 때 노출되는 정보의 양을 줄이기 위해 필요하다.

VANET에서 조건부 익명성을 지원하기 위한 기존 연구는 크게 두 종류로 구분된다. 첫째는 다량의 익명 인증서를 차량에 유지하여 사용하는 것이다[1]. 하지만 유효기간 설정 문제 때문에 다량의 익명 인증서의 사용은 인증서 철회 메커니즘을 더욱 어렵게 만든다. 둘째는 그룹 서명(group signature)을 활용하는 것이다[2,3]. 그룹 서명은 조건부 익명성을 제공하는 기법이기 때문에 VANET에 어울리는 기법이지만 이 기법 역시 철회 메커니즘이 효과적이지 못하며, 그룹 서명 비용이 저렴하지 않기 때문에 효율성 측면에서도 문제가 있다.

이와 같은 두 가지 방법 외에 최근에 Zhang 등[4]은 차량의 OBU에 조작불가능한 하드웨어(TRH, Tamper-Resistant Hardware)를 포함하고 여기에 신원기반 시스템의 마스터키를 설치하여 차량 자체에서 신원기반 공개키 쌍을 매번 새롭게 생성하여 사용하는 시스템을 제안하였다. 즉, 다량의 익명 인증서를 사용하는 방식의 문제점을 극복하기 위한 대안으로 익명 인증서를 주기적으로 신뢰기관에서 받는 것이 아니라 차량 자체에서 생성할 수 있고, 그것의 사용 비용이 일반 서명 비용 정도이면 그룹 서명을 활용하는 방식보다 효과적인 방식이 된다. 더욱이 Zhang 등[4]과 같이 TRH를 적극 활용한다면 충분한 효율성을 갖춘 조건부 익명 인증시스템을 제공할 수 있다.

이 논문은 TRH를 활용하여 차량 자체에서 불연결성이 제공되도록 익명ID를 스스로 갱신할 수 있고, 이 ID를 이용하여 메시지를 전자서명한 다음 전달할 수 있는 새 시스템을 제안한다. 이 시스템은 조건부 익명성을 제공하기 위해 차량의 공개키를 신뢰기관의 공개키로 암호화한 값을 익명ID로 사용한다. 또 메시지마다 불연결성을 제공하기 위해 익명ID를 재암호화(re-encryption)하여 갱신한다. 여기서 TRH에 대한 가정을 이용하여 익명ID의 갱신 과정에 대한 공격을 방지하고 있다. 교환되는 메시지의 서명은 익명ID에 대한 표현증명 문제를 활용한다. 추가적으로 익명ID의 사용기간을 제한하여 개별ID의 철회 문제를 고려할 필요가 없도록 하였고, TRH를 활용하여 문제 차량에 대한 VANET 참여를 중단시킬 수 있다.

이 논문의 구성은 다음과 같다. 2장에서 이 논문의 바탕이 되는 수학적 배경과 이 논문과 관련된 기존 VANET 연구 결과를 소개한다. 3장에서는 이 논문에서 제안한 VANET를 위한 새 조건부 익명시스템을 소개한다. 4장에서 제안된 기법을 분석하고, 5장에서 결론과 향후 연구방향을 제시한다.

II. 연구 배경

2.1 수학적 배경

p가 매우 큰 소수이고 G_q는 위수가 소수 q인 Z_p^*의 부분군이라고 하자. 이 군에서 이산대수 문제는 계산적으로 어렵다고 가정한다. 이와 같은 곱셈순환군에서 표현문제(representation problem)[8]는 다음과 같이 정의된다.

정의 1. (표현) 길이가 $l \geq 2$인 생성자 튜플은 $(g_1, ..., g_l)$을 말하며, 이 때 g_i는 G_q의 생성자이고, $i \neq j$이면 $g_i \neq g_j$이다. 생성자 튜플 $(g_1, ..., g_l)$에 대한 $y \in G_q$

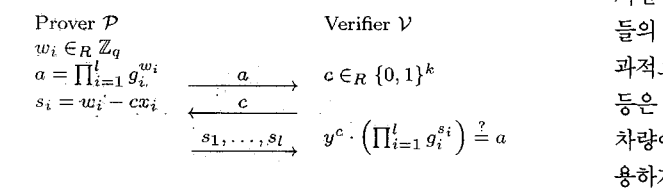
의 표현은 $y=\Pi_{i=1}^{l} g_i^{x_i}$인 색인 튜플 $(x_1, ..., x_l)$을 말한다. 이 때 $\forall x_i \in Z_q$이다.

만약 $y=1$이면 $(0, 0, ..., 0)$도 그것의 표현임을 쉽게 알 수 있다. 이와 같은 표현을 명백한 표현(trivial representation)이라 한다.

정의 2. (표현문제) 위수가 소수 q인 G_q에서 표현문제란 G_q, 생성자 튜플 $(g_1, ..., g_l)$, $y \in G_q$가 주어졌을 때, $(g_1, ..., g_l)$에 대한 y의 명백하지 않은 표현을 찾는 문제를 말한다.

정리 1. G_q에서 이산대수 문제를 해결하는 것이 계산적으로 어렵다고 가정하면 모든 $y \in G_q - \{1\}$에 대해 임의로 선택한 생성자 튜플 $(g_1, ..., g_l)$을 입력하였을 때, 무시할 수 없는 확률을 가지고 이 튜플에 대한 y의 표현을 찾는 다항시간 알고리즘은 존재하지 않는다.

이 정리에 대한 증명은 표현문제를 해결할 수 있으면 이산대수 문제를 해결할 수 있다는 모순에 의한 증명방법을 통해 간단히 증명할 수 있다[8]. G_q에서 생성자 튜플 $(g_1, ..., g_l)$에 대한 y의 표현을 알고 있음을 영지식으로 증명하는 프로토콜은 다음과 같다[8].



이 프로토콜은 c를 $c=H_q(g_1\|...\|g_l\|y\|a)$로 계산하여 비상호작용 증명으로 바꿀 수 있으며, 이 증명은 전자서명으로 사용가능하다. 여기서 $H_q: \{0,1\}^* \rightarrow Z_q^*$는 충돌회피 해쉬함수이다. 이 논문에서는 이 서명을 사용한다.

이산대수를 기반하고 있는 가장 대표적인 공개키 암호알고리즘은 ElGamal 알고리즘[9]이다. 이 알고리즘은 재암호화가 가능하다는 또 다른 특성을 가지고 있다. 예를 들어 G_q의 생성자가 g이며 개인키가 $x \in Z_q^*$이고 공개키가 $y=g^x$일 때, $m \in G_q$에 대한 ElGamal 암호는 쌍 $(\alpha, \beta)=(g^r, y^r m)$이 된다. 여기서 $r \in Z_q^*$은 암호화할 때 선택된 랜덤요소이다. 암호문 (α, β)는 또 다른 $r' \in Z_q^*$을 선택하여 $(\alpha', \beta')=(g^{r'}\alpha, y^{r'}\beta)$로 누구나 재암호화가 가능하다.

2.2 관련연구

Raya와 Hubaux는 다량의 익명인증서를 사용하는 시스템을 제안하였다[1]. 각 차량은 초기에 다량의 익명인증서와 인증기관의 인증서가 설치된 상태이며, 주기적으로 다량의 익명인증서를 발급받아 교체해야 한다. 따라서 차량에 많은 저장공간이 요구되며, 일반 인증서 철회 방법을 사용할 경우에는 CRL(Certificate Revocation List) 크기가 매우 커지는 문제점을 지니고 있다. 이것을 완화하기 위해 인증서의 유효기간을 짧게 만들 수 있지만 인증서가 발급될 시점과 사용될 시점이 다르므로 짧은 유효기간을 가진 인증서를 차량에 저장하는 것이 쉽지 않다. 이 때문에 인증기관이 철회될 인증서를 보유한 차량에 메시지를 보내어 해당 인증서의 사용을 못하도록 하는 방법을 제안하고 있다. 하지만 차량의 위치를 찾아 메시지를 전송하는 것은 간단한 문제가 아니며, 프라이버시에 위배되는 측면도 있다. 또한 해당 메시지가 도달되지 못하도록 차단할 경우에는 철회가 적절히 이루어진다는 것을 보장하기 어렵다.

Lin 등[2]은 Boneh 등의 그룹서명[10]과 신원기반 공개키 시스템을 활용한 시스템을 제안하였다. 이 시스템에서 차량 간 통신은 그룹서명을 사용하고, RSU가 차량에게 메시지를 전달할 때에는 일반 신원기반 서명기법을 사용하고 있다. Boneh 등[10]은 그들의 논문에서 제안하는 그룹서명이 VANET에서 효과적으로 사용될 수 있음을 제시하고 있었으므로 Lin 등은 이것을 구체화한 것이다. 하지만 철회 목록을 각 차량에게 전달하여 철회하는 형태를 VANET에서 사용하기에는 적절하지 못하며, 시기적절하게 이루어진다는 것을 보장할 수 없다. 또한 Boneh 등의 서명은 영지식 기술을 이용하는 서명이므로 서명자체가 효율적이지 못하다.

Calandriello 등[3]도 Lin 등과 마찬가지로 그룹서명 기법을 사용하지만 그룹서명을 사용하여 메시지를 서명하여 교환하는 것이 아니라 각 차량은 그룹서명키를 이용하여 익명인증서를 스스로 만들어 사용하는 방법을 제안하고 있다. 자체적으로 불연결성을 제공하는 익명의 공개키 쌍을 지속적으로 생성하여 사용할 수 있다는 장점을 지니고 있지만 생성된 익명인증서를 사용하기 위해서는 인증서를 확인하기 위해 그룹서명을 확인해야 하고 익명인증서를 이용하여 서명된 메시지를 확인해야 한다. 따라서 각 메시지를 확인하기 위한 비용이 비교적 크다.

Zhang 등[4]은 차량의 TRH에 신원기반 시스템의 PKG(Private Key Generator)의 마스터키를 포함하여 차량에서 지속적으로 신원기반 공개키 쌍을 만들어 사용하는 방법을 제안하고 있다. 따라서 이 제안은 Calendriello 등이 제안한 기법과 마찬가지로 차량에서 자체적으로 불연결성을 제공하는 익명의 공개키 쌍을 지속적으로 생성하여 사용할 수 있다. Zhang 등은 또한 일괄확인 서명 기법을 통해 서명들을 개별적으로 확인하지 않고 모아서 하나의 서명을 확인하는 비용으로 검증하여 효율성을 높이고자 하였다. 하지만 일괄확인 서명 기법은 서명들이 모두 유효할 경우에는 효율성을 높일 수 있는 수단이 되지만 일괄확인할 때 잘못된 서명이 포함되어 있을 경우에는 이를 식별하는 것이 어렵다는 문제점이 있다.

III. 제안하는 시스템

3.1 시스템 모델

3.1.1 조작불가능한 하드웨어

차량은 비용 측면에서 TRH를 충분히 활용할 수 있으며, 암호키들을 안전하게 유지하기 위해 TRH의 사용은 오히려 권장되어야 한다. Zhang 등[4]은 신원기반 시스템의 PKG의 마스터 키를 TRH에 유지하여 익명공개키 쌍을 생성하는 방법을 사용하였다. 이 논문에서도 TRH를 이용하여 차량 자체에서 매우 효과적으로 익명ID를 갱신한다. 이 논문에서는 TRH에 대해 다음을 가정한다.

- TRH 가정 1. TRH 내부에는 필요한 암호모듈이 구축되어 있으며, 이 모듈에서 이루어지는 연산에 대해서는 외부에서 영향을 줄 수 없다.
- TRH 가정 2. TRH 내부 비휘발성 메모리에 저장되어 있는 데이터(특히, 암호키)는 외부에서 얻거나 조작할 수 없다.
- TRH 가정 3. TRH는 정의된 특정 메시지를 받으면 동작을 중단한다.

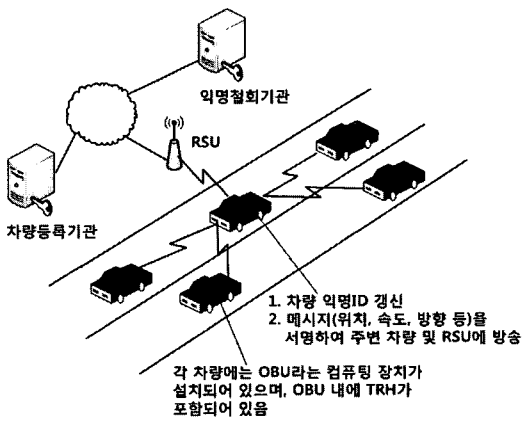
이 논문에서는 재암호화를 이용하여 익명ID를 갱신하는데 정의된 방법에 따라 갱신됨을 보장하여야 하고, 갱신된 ID를 변경하여 사용할 수 없어야 한다. 이를 위해 복잡한 증명기술을 사용할 수 있지만 TRH 가정 1과 2를 활용하면 간단한 방법으로 익명ID와 관련된 요구사항(정의된 방법으로 갱신, 변경하여 사용불가)을 충족시킬 수 있다. 이 때문에 이 논문에서는 TRH를 사용하고 있다.

3.1.2 조건부 익명성

VANET에서 프라이버시를 지원하지만 사고나 공격의 책임자를 식별하기 위해 조건부 익명성을 제공해야 한다. 본 논문에서는 신뢰기관의 공개키로 차량의 공개키를 암호화하여 익명ID를 생성한다. 따라서 신뢰기관은 언제든지 익명ID를 복호화화여 얻은 결과값을 데이터베이스에서 검색하여 메시지를 실제 서명한 차량을 식별할 수 있다. 또한 신뢰기관이 권한을 남용할 수 없도록 차량의 공개키를 암호화하기 위해 사용된 공개키에 대응되는 개인키는 임계 방식(threshold)[11]을 이용하여 여러 기관이 분산 공유하고 있다고 가정한다.

3.1.3 시스템 가정

이 논문에서는 [그림 1]과 같이 행정부에 소속된 차량등록기관, 사법부에 소속된 익명철회기관, 다수의 차량, 도로에 설치된 RSU의 참여를 가정한다. 차량간 통신과 차량에서 RSU간 통신은 프라이버시가 보장되어야 하지만 RSU에서 차량 간 통신은 프라이버시가 요구되지 않으므로 기존 보안 메커니즘을 사용하여도 무방하다. 따라서 이 논문에서는 주로 V2V 통신 중 단일 홉 방송 메시지에 초점을 맞추고 있다. V2I 중 V에서 I는 V2V와 동일한 방법으로 통신이 이루어짐을 가정한다. 이 논문에서 다음을 가정한다.



[그림 1] 제안하는 시스템의 환경

• 시스템 가정 1. 각 차량 OBU에는 3.1.1에 나열된 세 가지 가정이 충족되는 TRH가 설치되어 있다고 가정한다.

• 시스템 가정 2. 모든 차량에는 GPS(Global Positioning System)가 설치되어 있어 정확한 시간 동기화가 가능하다.

• 시스템 가정 3. 3.1.2에서 언급한 바와 같이 익명철회기관의 공개키에 대응되는 개인키는 임계 방식을 이용하여 분산 공유되어야 있다고 가정한다.

• 시스템 가정 4. RSU가 도로에 조밀하게 설치되어 있으며, 차량간 통신 및 차량과 RSU 간 통신은 단일 홉 방송을 통해 이루어진다고 가정한다.

3.2 제안하는 V2V 통신 및 차량 철회 기법

3.2.1 표기법

본 논문에서는 2.1 수학적 배경에서 사용된 표기법과 [표 1]에 제시된 표기법을 사용하여 제안된 시스템을 설명한다.

3.2.2 시스템 설정

차량등록기관은 512비트 보다 큰 소수 p를 선택하고 위수가 소수 q(160비트 이상)인 Z_p^*의 부분군 G_q를 선택한다. 또 이 기관은 G_q의 두 개의 생성자 g_T와 g_V를 선택하여 군 정보와 함께 공개한다.

익명철회기관은 공개키 y_T를 공개하는데, 이 공개키에 대응되는 개인키는 권한 분산을 위해 적절한 여러 기관과 비밀 공유 기법을 사용하여 생성한다.

[표 1] 표기법

표기	의미
g_T, g_V	G_q의 생성자
x_T	(t,n) 임계방식으로 비밀 공유된 익명철회기관의 개인키
$y_T = g_T^{x_T}$	익명철회기관의 공개키
x_V	차량의 개인키
$y_V = g_V^{x_V}$	차량의 공개키
$MAC.K(M)$	대칭키 K를 이용한 메시지 M의 MAC(Message Authentication Code) 값
$\{M\}.K$	대칭키 K를 이용한 메시지 M의 암호화

각 차량은 등록 과정에서 차량의 OBU에 있는 TRH에 다음이 설치된다.

- 사용하는 군 정보: p, q, g_T, g_V
- 익명철회기관의 공개키: y_T
- 차량의 개인키와 공개키: x_V, $y_V = g_V^{x_V}$
- 차량의 익명ID: $(\alpha_0, \beta_0) = (g_T^{r_0}, y_T^{r_0} y_V)$
- 익명ID를 생성할 때 사용된 랜덤값: r_0
- 공통 대칭키: K_{all}
- TRH 비밀키: K_i

차량 등록과정에서 차량의 공개키 쌍이 TRH를 저장되는데, 등록기관은 개인키를 얻을 수 없다고 가정한다. 모든 TRH에는 동일한 대칭키 K_{all}과 각 TRH마다 다른 대칭키 K_i가 설치된다. 이 K_i는 차량을 철회할 때 사용된다.

차량등록기관은 발급된 각 TRH마다 다음 정보를 포함한 VANET 서비스 제공하기 위해 필요한 각종 정보를 유지한다.

- 차량의 실제ID
- 차량의 공개키: y_V
- 암호화된 K_i : $(g_T^{w_i}, y_T^{w_i} g_T^{n_i})$, $N_i \oplus K_i$

여기서 $N_i = H_l(g_T^{n_i})$이며, $H_l : G_q \rightarrow \{0,1\}^l$는 충돌회피 해쉬함수이고, l은 시스템에서 사용하는 대칭키의 비트 길이이다. 이와 같이 K_i를 암호화하여 보관하는 것은 익명철회기관의 남용을 막기 위한 것이다.

도로 주변에 설치되어 있는 각 RSU에도 TRH가 설치되어 있으며, 이 TRH에는 RSU의 공개키 쌍과 K_{all}이 저장되어 있다. RSU는 정해진 주기마다 특정 메시지를 주변 차량들에게 방송한다.

3.2.3 익명ID의 갱신

차량의 TRH는 $r_i \in_R Z_q^*$를 선택하여 차량의 익명ID를 다음과 같이 재암호화하여 갱신한다.

$$(\alpha_i, \beta_i) = (g_T^{r_i} \alpha_{i-1}, y_T^{r_i} \beta_{i-1})$$

또한 지금까지 재암호화할 때 사용한 랜덤값들의 합 $R = \Sigma_{j=0}^{i} r_j$을 유지한다. R은 β_i에 대한 생성자 튜플

(y_T, g_V)에 대한 색인 튜플 중 하나이므로 나중에 메시지를 서명할 때 필요하다. 이와 같은 방법으로 익명ID 갱신하면 각 익명ID 간에 불연결성을 제공할 수 있다. 물론 재암호화 대신에 새롭게 암호화하여도 동일한 효과를 얻을 수 있다.

차량이 메시지를 전송할 때마다 새롭게 갱신한 익명ID를 포함한다면 두 메시지가 동일한 차량에 의해 전송한 메시지인지 알 수 없다. 이와 같은 익명ID를 사용할 경우에는 다음 두 가지가 추가로 해결되어야 V2V 통신에 사용이 가능하다.

- 익명ID 갱신 요구사항 1. 갱신된 익명ID를 조작하여 사용할 수 없어야 한다. 만약 조작이 가능하다면 나중에 익명 철회가 가능하지 않도록 익명ID를 조작하여 사용할 수 있기 때문이다.
- 익명ID 갱신 요구사항 2. 익명ID를 포함한 메시지를 전송할 때 해당 메시지가 익명ID를 사용하는 차량이 전송한 메시지인지 확인할 수 있어야 한다.

익명ID갱신 요구사항 1은 현재 익명ID가 유효한 이전 익명ID로부터 갱신된 값임을 증명해야 한다. 하지만 이전 익명ID를 함께 전송하여 증명할 경우에는 불연결성을 제공할 수 없을 뿐만 아니라 이전 익명ID의 유효성도 함께 증명되어야 한다. 즉, 이전 익명ID를 제공하지 않고 현재 익명ID가 유효한 익명ID임을 증명할 수 있어야 한다. 더욱이 이 증명은 짧고 효율적으로 검증가능해야 한다. 따라서 이 문제를 해결하기 위해 전자선거와 Mix 기술에서 사용된 영지식 증명과 같은 기술[12]을 사용하는 것은 VANET의 환경을 고려할 때 적절하지 않다.

이 논문에서 이 문제를 효과적으로 해결하기 위해 TRH를 활용한다. 보다 정확하게 설명하면 다음 두 가지를 통해 익명ID가 논문에서 정의된 방법으로 항상 갱신되고, 나중에 변경되어 사용될 수 없음을 보장한다.

- 첫째, ID 갱신을 위한 재암호화는 TRH 내부에서 이루어진다고 가정한다.
- 둘째, TRH는 모든 TRH에 공통으로 설치되어 있는 K_{all}을 이용하여 다음을 계산하여 익명ID를 새롭게 갱신할 때마다 함께 공개한다.

$$MAC.K_{all}(\alpha_i \| \beta_i \| T_V) \quad (1)$$

여기서 T_V는 익명ID의 만료시간을 나타낸다.

TRH 외부에서 익명ID를 얻어 누구나 조작가능하지만 유효한 익명ID가 되기 위해서는 유효한 MAC값이 함께 제시되어야 한다. 하지만 MAC값을 계산할 때 사용되는 K_{all}는 TRH 가정 2에 의해 누구도 얻을 수 없기 때문에 외부에서 익명ID를 조작하여 사용하는 것은 가능하지 않다. 차량등록기관과 RSU는 K_{all}을 알고 있지만 이들에 의한 오남용은 고려하지 않는다.

MAC 값에 포함된 T_V는 익명ID의 만료시간을 나타내며, 시스템 가정 2에 의해 모든 차량은 클럭 동기화가 가능하기 때문에 시작시간은 필요 없고, 종료시간만 나타내면 된다. 또 TRH가 설정하는 값이고 시스템 가정 2 때문에 발생할 수 있는 공격(클럭동기화 문제, 클럭값의 위변조)은 고려하지 않아도 된다. 메시지를 수신한 차량은 익명ID의 만료시간을 검토하며, 만료시간이 지난 익명ID를 이용한 메시지는 거부된다. 만료시간을 최대한 짧게 설정(1, 2분)하면 익명ID 철회를 위한 익명철회목록의 유지 및 분배는 불필요하다. 각 메시지마다 새롭게 갱신된 익명ID를 사용하는 것이 가장 이상적이지만 효율성 측면에서는 특정 기간 동안에는 하나의 ID를 사용하는 방법이 효과적이며, VANET 환경을 고려할 때 이와 같은 사용이 익명성에 큰 문제가 되지도 않는다. 즉, 짧은 시간에 여러 메시지에 서명하여 이들이 상호 연결되더라도 이들 메시지를 통해 노출되는 위치 정보는 지리적으로 매우 가까운 위치이기 때문에 문제가 되지 않는다는 것이다.

익명ID갱신 요구사항 2는 생성자 튜플 (y_T, g_V)에 대한 익명ID의 β_i에 대한 표현증명을 이용한 전자서명을 통해 제공할 수 있다. 생성자 튜플 (y_T, g_V)에 대한 익명ID의 β_i에 대한 표현은 색인 튜플 (R, x_V)이며, 이것은 해당 차량만이 알 수 있는 값이므로 이 차량 외에 다른 누구도 증명할 수 없다.

3.2.4 V2V 통신

각 차량은 메시지 m를 이웃 차량들에게 방송하고 싶으면 최근에 갱신한 익명ID (α_i, β_i)을 이용하여 다음과 같이 서명을 생성한다. 여기서 β_i에 대한 생성자 튜플 (y_T, g_V)에 대한 표현은 (R, x_V)이다.

- 단계 1. 차량은 $w_T, w_V \in_R Z_q^*$를 선택하고 $W = y_T^{w_T} g_V^{w_V}$를 계산한다.

• 단계 2. 다음을 계산하고,

$$c = H_q(\alpha_i \| \beta_i \| W \| m \| \gamma) \quad (2)$$

$s_T = w_T - cR$와 $s_V = w_V - cx_V$를 계산한다. 여기서 γ는 랜덤 값이거나 $\{\phi\}.K_{all}$이며, ϕ는 주변 RSU가 전달한 랜덤 값이다. 이것의 용도는 다음 절에서 설명한다.

즉, 메시지 m에 대한 서명값은 c, s_T, s_V이다. 차량이 전달하는 전체 메시지는 다음과 같다.

$$\alpha_i,\ \beta_i,\ MAC.K_{all}(\alpha_i \| \beta_i \| T_V),\ T_V,\ c,\ s_T,\ s_V,\ m,\ \gamma$$

m의 크기를 제외한 전체 메시지의 크기는 219바이트 정도(α_i, β_i: 각 64바이트, MAC값, c, s_T, s_V: 각 20바이트, T_V: 4바이트, γ: 7바이트)로 비교적 작다. 이와 같은 메시지를 수신한 차량은 다음과 같은 방법으로 메시지를 검증한다.

• 단계 1. 차량의 TRH는 메시지에 포함된 MAC 값을 확인한다. 이 때 T_V를 확인하여 만료시간이 경과되지 않은 경우에만 다음 단계를 진행한다.

• 단계 2. $c? = H_q(\alpha_i \| \beta_i \| \beta_i^c y_T^{s_T} g_V^{s_V} \| m \| \gamma)$를 확인한다.

단계 2의 검증의 정확성은 다음과 같이 확인할 수 있다.

$$\beta_i^c y_T^{s_T} g_V^{s_V} = y_T^{Rc} g_V^{x_V c} y_T^{s_T} g_V^{s_V} = y_T^{Rc+s_T} g_V^{x_V c+s_V} = y_T^{w_T} g_V^{w_V} = W$$

3.2.5 차량 철회

제안하는 익명ID의 경우 익명철회기관이 익명ID를 복호화하여 문제가 된 메시지를 전송한 차량을 식별할 수 있다. 하지만 제안하는 시스템에서는 각 차량에서 자체적으로 익명ID를 갱신하여 사용하기 때문에 지속적으로 문제를 일으키는 차량이 더 이상 VANET에 참여할 수 없도록 막을 수 있는 방법이 필요하다. 이를 VANET에서는 차량 철회(car revocation)[1]라 한다.

본 시스템의 차량 철회 방법은 다음과 같다.

• 단계 1. 차량등록기관은 먼저 차량의 데이터베이스 항에 보관되어 있는 암호문을 복호화하여 차량 TRH의 K_i와 공개키 y_V를 얻는다.

• 단계 2. 차량등록기관은 $\{\{y_V\}.K_i\}.K_{all}$를 모든 RSU에게 전달한다.

• 단계 3. RSU는 다음과 같은 메시지를 만들어 주변 차량들에게 방송한다.

$$\{msgType \| \phi \| \{y_V\}.K_i\}.K_{all} \quad (3)$$

여기서 ϕ는 RSU가 랜덤하게 선택한 주기적으로 방송되는 값으로 매번 다른 값이 사용된다.

• 단계 4. 각 차량이 이 메시지를 수신하면 TRH에 전달되며 TRH는 바깥쪽 암호문을 먼저 복호화하여 메시지의 종류를 파악한다. 이것이 차량 철회용 메시지이면 내부 암호문을 복호화하고, 결과 값이 차량의 공개키에 해당되면 TRH는 동작을 중단한다.

• 단계 5. TRH는 동작을 중단하기 전에 철회 메시지에 대한 확인 메시지를 전달한다. 확인 메시지를 받은 RSU는 이를 차량등록기관에 알린다.

• 단계 6. 차량 또는 차량등록기관으로부터 확인 메시지를 받으면 RSU는 다음 주기 때 차량 철회 메시지 대신에 일반 메시지를 방송한다.

단계 1에서 차량의 비밀키 복호화는 임계방식을 통해 복호화해야 하므로 차량등록기관이 단독으로 이 값들을 얻어 남용할 수 없다. 또 단계 5에서 확인 메시지는 3.2.4에서 설명한 일반 V2V 메시지와 동일한 방식으로 구성한다.

이와 같은 차량 철회 방식에 대한 보안 위협은 철회 메시지가 TRH에 전달되는 것을 막거나 확인 메시지를 차단하는 것이다. 이와 같은 보안 위협을 막기 위해 RSU는 주기적으로 아래와 같은 형태의 메시지를 방송하며, 차량이 이들을 처리하지 않을 경우 VANET 서비스를 사용할 수 없도록 한다.

$$\{msgType \| \phi \| padding\}.K_{all} \quad (4)$$

여기서 *padding*은 식 (3)과 (4)의 메시지 크기가 같도록 사용하는 채우기 정보이다. TRH는 이 메시지에 포함된 값을 익명ID를 갱신할 때 사용되는 MAC 값에 포함해야 한다. 즉, 식 (1)의 MAC 값은 $MAC.K_{all}(\alpha_i \| \beta_i \| T_V \| \phi)$로 변경되어야 하며, 최신의 ϕ가 사용되지 않는 메시지는 거부된다. 식 (3)과 (4)의 메시지는 서로 구분되지 않으므로 식 (3)의 메시지만을 차단하여 차량 철회를 방해할 수 없다.

철회에 대한 확인 메시지도 일반 메시지와 구분할 수 없도록 철회 차량은 $\{\phi\}.K_{all}$을 식 (2)의 c 값을 계산할 때 포함하고, 일반 차량은 $\{\phi\}.K_{all}$과 같은 크기의 랜덤 값 γ을 포함한다. 따라서 RSU는 확인 메시지를 식별할 수 있지만 다른 참여자들은 TRH를 조작하지 않는 이상 식별할 수 없다. RSU 중 하나가 철회에 대한 확인 메시지를 받으면 이를 차량등록기관에 전달한다. 차량등록기관은 이 사실을 다른 RSU에게 알린다. 차량이 현재 도로 상에 없는 경우에는 철회 메시지가 해당 차량에게 시기적절하게 전달되지 않을 수 있다. 따라서 확인 메시지를 받지 못한 경우에는 철회 메시지를 다시 작성하여 방송한다.

IV. 분석

4.1 안전성

보조정리 1. 제안하는 시스템에서 사용되는 전자서명 기법은 안전하다.

증명. 제안하는 시스템에서는 표현문제를 이용한 전자서명을 사용하여 메시지를 교환한다. 표현문제는 안전성이 증명된 문제[8]이므로 다른 참여자들이 주어진 값(익명ID)에 대한 색인 튜플을 알 수 없으면 서명을 위조하는 것이 계산적으로 어렵다. 이 색인 튜플은 TRH에 보관되어 있으므로 TRH 가정 2에 의해 해당 차량 외에는 얻을 수 없다. 따라서 이 보조정리는 성립한다. □

차량 철회 방법은 다음을 각각 보장해야 한다.

- **차량철회 요구사항 1.** 적절한 기관들의 협력이 없으면 특정 차량을 철회할 수 없어야 한다.
- **차량철회 요구사항 2.** 차량 철회 메시지나 확인 메시지를 차단하여 차량 철회를 방해할 수 없어야 한다.
- **차량철회 요구사항 3.** 차량 철회 메시지는 궁극에는 해당 차량에 전달되어 그 차량의 TRH의 동작을 중단시켜야 한다.

보조정리 2. 본 논문에서 제안한 차량 철회 방법은 차량철회 요구사항 1, 2, 3을 충족한다.

증명. 차량 철회 메시지를 생성하기 위해서는 해당 차량의 K_i가 필요하다. 하지만 K_i는 차량 TRH와 차량등록기관에 암호화되어 보관되어 있으므로 이들에 대한 노출 위협은 TRH 가정 2와 K_i를 암호화하기 위해 사용된 암호기법의 안전성 때문에 현실적으로 고려하지 않아도 된다. 따라서 차량철회 요구사항 1은 충족된다.

RSU는 주기적으로 일반 메시지 또는 차량 철회 메시지를 전달한다. 이 두 메시지는 K_{all}이 없으면 구분할 수 없다. 확인 메시지도 차량이 일반적으로 보내는 메시지와 K_{all}이 없으면 구분할 수 없다. 그런데 K_{all}는 차량과 RSU의 TRH에 유지되므로 TRH 가정 2에 의해 노출될 수 없어 공격자가 이를 구분하여 차단하는 것은 가능하지 않다. 차량등록기관도 K_{all}을 가지고 있으므로 노출되지 않도록 정책적, 물리적 보안을 충분히 하여야 한다. 따라서 차량철회 요구사항 2도 충족된다.

차량이 현재 운행 중이면 시스템 가정 4와 차량 철회 요구사항 2에 의해 차량 철회 메시지는 해당 차량에게 반드시 전달된다. 차량이 현재 운행되고 있지 않으면 메시지가 전달되지 않을 수 있지만 이 경우에는 VANET에 참여하는 것이 아니므로 보안 위협이 되지 않는다. 따라서 차량이 운행을 시작하면 주위 RSU로부터 철회 메시지를 받게 되므로 요구사항 3도 충족된다. □

4.2 프라이버시와 조건부 익명성

프라이버시와 조건부 익명성을 논하기 위해 다음과 같은 두 종류의 공격자를 고려한다.

- 공격자 종류 1. 도청만 가능한 공격자
- 공격자 종류 2. 특정 암호키를 가진 공격자

이와 같은 공격자 모델에서 단일 메시지의 불관찰성, 동일 차량에 의한 여러 메시지의 불연결성, 조건부 익명성 만족 여부에 대해 논한다.

보조정리 3. 공격자 종류 1은 단일 메시지를 전송한 차량을 식별할 수 없으며, 공격자 종류 2는 식별할 수 있지만 현실적인 보안 위협은 되지 않는다.

증명. 단일 메시지의 내용(속도, 방향, 시간 등)을 통해서는 차량을 식별할 수 없다고 가정하면 한 차량이 서명하여 전달하는 메시지는 사용된 익명ID를 복호화하지 않는 이상 이 메시지를 전송한 차량을 식별

할 수 없다. 따라서 공격자 종류 1에 대해서는 불관찰성이 보장된다. 익명철회기관의 개인키를 획득한 공격자는 익명ID를 복호화하여 이 메시지를 전송한 차량을 식별할 수 있다. 그러나 익명철회기관의 개인키는 비밀 공유 기법을 통해 분산되어 있으므로 노출되는 것은 현실적으로 고려하지 않아도 된다. 따라서 이 보조정리는 성립한다. □

보조정리 4. 공격자 종류 1은 동일 차량이 서로 다른 ID를 이용하여 전송한 메시지들을 상호 연결할 수 없으며, 공격자 종류 2는 연결할 수 있지만 현실적인 보안 위협은 되지 않는다.

증명. 한 차량이 사용하는 익명ID는 재암호화 기법을 사용하여 갱신되므로 이들 간에는 불연결성이 제공된다. 따라서 다른 익명ID를 이용하여 서명된 메시지 간에는 불연결성이 제공된다. 이 경우도 보조정리 2와 마찬가지로 익명철회기관의 개인키를 획득한 공격자는 각 메시지의 익명ID를 복호화하여 이 메시지를 전송한 차량을 식별할 수 있고, 나아가 같은 차량이 전송한 메시지들을 상호 연결할 수 있다. 그러나 보조정리 3에서 언급한 바와 같이 이 위협은 현실적으로 고려하지 않아도 된다. 따라서 이 보조정리는 성립한다. □

보조정리 5. 익명철회기관은 필요하면 단일 메시지를 전송한 차량을 식별할 수 있다.

증명. 본 시스템의 익명ID는 차량의 공개키를 익명철회기관의 공개키로 암호화하여 만든 값이기 때문에 필요하면 항상 익명철회가 가능하다. 참고로 철회 능력을 남용할 수 없도록 철회기관의 공개키에 대응되는 개인키는 임계방식을 통해 분산 공유 되어있다. 익명ID의 갱신은 차량 TRH 내부에서 이루어지므로 공격자가 접근하여 방해할 수 없다. 따라서 익명철회기관이 철회하지 못하도록 공격하는 유일한 방법은 TRH로부터 출력된 (α_i, β_i)를 조작하는 것이지만 조작된 값을 사용하기 위해서는 유효한 MAC 값이 필요하다. 하지만 MAC 값은 K_{all}이 없으면 만들 수 없으므로 K_{all}이 없는 공격자는 이와 같은 공격을 할 수 없다. 보조정리 2에서 언급한 바와 같이 K_{all}에 대한 노출위협은 TRH 가정 2와 차량등록기관의 안전성 때문에 현실적인 위협이 아니다. 따라서 이 보조정리는 성립한다. □

보조정리 3, 4, 5에 의해 제안한 시스템은 목표로 한 조건부 익명성을 제공하고 있다.

4.3 효율성

3.2.4에서 분석한 바와 같이 메시지 내용을 제외한 나머지 메시지의 크기는 219바이트이며, 여기에 3.2.5에서 고려한 ϕ(64비트)가 추가되더라도 256바이트를 초과하지 않는다. 따라서 이 논문에서 사용되는 메시지의 크기는 현실적으로 사용하기에 무리가 없는 정도의 크기이다. 각 메시지를 생성하기 위해 필요한 연산 비용도 3개 지수승(표현계산은 하나의 지수승만큼의 비용으로 최적화하여 계산할 수 있음[8]), 2개 곱셈, 3개 해쉬연산(MAC을 2개의 해쉬연산 비용

〔표 2〕 Zhang 등의 시스템과의 비교

		Zhang 등의 시스템[4]	제안된 시스템
익명ID 또는 공개키 생성 방법		PKG의 마스터 키를 TRH에 포함하여 차량에서 자체적으로 신원기반의 공개키 생성	각 차량의 공개키를 익명철회기관의 공개키로 암호화하여 차량에서 자체적으로 생성
서명 방식	특징	결정적이며 일회용 • 생성된 키 쌍으로 하나의 메시지만 서명 가능	확률적 • 하나의 익명ID로 여러 메시지 서명 가능
	서명비용	3개의 곱선형 사상 필요	일반 지수 연산 사용
	서명크기(공개키,ID포함)	3개의 타원곡선 점(60 바이트)	208 바이트
일괄확인 기법		안전성이 증명되어 있지 않은 기법 사용	제공하지 못함
조건부 익명성		임계방식 사용이 어려움	권한 남용을 방지하기 위한 임계방식을 고려함
키 철회 문제		일회용이므로 고려할 필요 없음	짧은 유효기간으로 해결함
차량 철회 문제		고려하지 않음	차량 철회 가능

으로 고려)이 소요(재암호화비용, 증명비용, MAC비용)된다. 또 이를 검증하기 위한 비용도 1개 지수승, 2개 해쉬연산 비용이 소요된다. 이와 같은 비용은 그룹서명을 사용하는 방법[2,3]들이나 겹선형 쌍함수를 사용하는 신원기반 시스템을 사용하는 방법[4]에 비해 효율적인 방법이다. 다만, [4]처럼 여러 서명을 일괄로 확인할 수 있는 방법이 없어 매우 많은 전자서명이 교환될 경우에는 부담이 될 수 있다. 하지만 Scheuer 등[5]이 제안하였듯이 모든 메시지를 공개키 기반 전자서명하여 교환하기보다는 중요한 메시지만을 전자서명한다면 이 논문의 제안도 VANET에 매우 효과적인 방법이 될 수 있다. 제안된 시스템과 가장 유사한 Zhang 등의 시스템[4]과 비교 결과는 [표 2]에 요약되어 있다. 이 표에서 알 수 있듯이 서명 길이와 일괄 확인 측면을 제외하고는 본 시스템이 우수하다.

V. 결 론

이 논문에서는 차량 자체에서 재암호화 기법을 이용하여 익명ID를 갱신할 수 있고, 갱신된 ID를 이용하여 메시지를 서명하여 교환할 수 있는 VANET를 위한 새 인증시스템을 제안하였다. 제안된 시스템에서 갱신된 익명ID는 기존 익명ID와 불연결성이 제공되지만 차량의 공개키를 암호화하여 구성된 ID이므로 필요하면 복호화하여 익명을 철회할 수도 있다. 이 철회 능력을 남용할 수 없도록 임계방식을 통해 권한을 분산하고 있다. 또 개별익명ID의 사용기간을 제한하여 개별익명ID의 철회 필요성이 없도록 하였으며, 문제가 된 차량이 더 이상 VANET 서비스를 방해할 수 없도록 참여를 제한시킬 수 있는 방법도 제공하고 있다. 제안된 시스템의 안전성은 일부 각 개별 차량에 설치된 조작불가능한 하드웨어를 통해 제공하고 있지만 이를 통해 매우 효과적이고 효율적인 시스템 제안이 가능하였다.

참 고 문 헌

[1] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. of Computer Security, vol. 15, no. 1, pp. 39-68, Jan. 2007.

[2] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[3] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," Proc. of the 4th ACM Int. Workshop on Vehicular Ad Hoc Networks, pp. 19-28, Sep. 2007.

[4] C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," Proc. of the IEEE INFOCOM 2008, pp. 246-350, Apr. 2008.

[5] F. Scheuer, K. Plobi, and H. Federrath, "Preventing profile generation in VANET," Proc. of the IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communication, pp. 520-525, Oct. 2008.

[6] Y. Toor, P. Muhlethaler, A. Laouiti, and A. Fortelle, "Vehicular ad hoc networks: Applications and related technical issues," IEEE Communication Surveys & Tutorials, vol. 10, no. 3, pp. 74 - 88, 2008.

[7] Vehicular Safety Communications Project, Final Report, DOT HSA 810 591, Apr. 2006.

[8] S. Brands, "Untraceable off-line cash in wallets with observers," Advances in Cryptology, Crypto 1993, LNCS 773, pp. 302-318, 1994.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," Advances in Cryptology, Crypto 1984, LNCS 196, pp. 10-18, 1984.

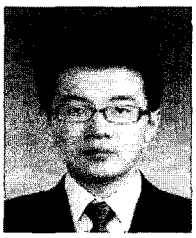
[10] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," Advances in Cryptology, Crypto 2004, LNCS 3027, pp. 41-55, 2004.

[11] T.P. Pedersen, "A threshold cryptosystem without a trusted party," Advances in Cryptology, Eurocrypt 1991, LNCS 547, pp. 522-526, 1991.

[12] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," Advances in Cryptology, Eurocrypt 2000, LNCS 1807, pp. 539-556, 2000.

〈著者紹介〉

김 상 진 (Sangjin Kim) 종신회원
1995년 2월: 한양대학교 전자계산학과(학사)
1997년 2월: 한양대학교 전자계산학과(석사)
2002년 8월: 한양대학교 전자계산학과(박사)
2003년 3월 ~ 현재: 한국기술교육대학교 인터넷미디어공학부 부교수
〈관심분야〉 암호기술 응용
URL: http://infosec.kut.ac.kr/sangjin/



이 병 우 (Byeongwoo Lee) 학생회원
2008년 2월: 한양대학교 전자컴퓨터공학부(학사)
2008년 3월 ~ 현재: 한양대학교 컴퓨터공학과(석사과정)
〈관심분야〉 네트워크 보안

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과(학사)
1989년: 아이오와주립대학 전자계산학과(석사)
1992년: 아이오와주립대학 전자계산학과(박사)
1993년 ~ 1994년: 한국전자통신연구원 선임연구원
1995년 3월 ~ 현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안
URL: http://infosec.hanyang.ac.kr/~hkoh/