Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.753

차량 익명성을 보장하는 그룹 서명기반 차량용 결제 프로토콜 설계*

정 명 우,† 김 승 주‡
고려대학교 정보보호대학원

A Design of Group Signature Based Vehicle Payment Protocol to Ensure Vehicle Anonymity*

Myung-woo Chung,† Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

CV(Connected Vehicle) 기술은 크게 차량에 안전 관련 서비스와 사용자 편의성 관련 서비스를 제공한다. 안전 관련 서비스는 차량 운행에 관한 정보들을 지속적으로 주변 차량 혹은 기지국에 전송하므로 프라이버시 문제가 생길 수 있다. 이에 안전 관련 서비스는 프라이버시 보호를 위해서 차량 익명성을 제공해야 한다. 그러나 결제 서비스와 같은 편의성 관련 서비스가 차량 익명성을 제공하지 못할 경우 안전 관련 서비스와 관련된 개인정보 또한 보호받을 수 없다. 이에 본 논문에서는 BU(Backward Unlinkability)-익명성과 추적성(traceability)을 제공하는 그룹 서명 기법과 ECQV(Elliptic Curve Qu-Vanstone) 묵시적 인증서를 기반으로 결제 프로토콜을 설계하였다. 제안하는 결제 프로토콜은 결제 시스템 구성요소의 역할을 분리하여 거래내역으로부터 차량을 추적할 수 없게 하였다. 또한 차량용 결제 프로토콜이 만족해야하는 보안 요구사항들을 정의하고 제안한 프로토콜이 이를 만족함을 보였다.

ABSTRACT

CV(Connected Vehicle) technology provides safety-related services and user convenience-related services to vehicle. Safety-related services can cause privacy problem by continuously transmitting vehicle information to nearby vehicles or base stations. Therefore, safety-related services should provide vehicle anonymity for privacy protection. However, if convenience-related services such as payment services fail to provide vehicle anonymity, driver information related to safety-related services may also be leaked. In this paper, we design a payment protocol based on ECQV(Elliptic Curve Qu-Vanstone) impicit certificate and group signature that provides BU-anonymity and traceability. The proposed payment protocol makes it impossible to track vehicles from payment transactions history by separating roles of payment system components. Moreover, we define the security requirements that the vehicle payment protocol must satisfy and show that the protocol satisfies the requirements.

Keywords: Vehicle Anonymity, Payment Protocol, Group Signature, Connected Vehicle

Received(06. 03. 2019), Modified(07. 22. 2019), Accepted(08. 13. 2019)

* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음 (과제번호 H2101-18-1001)

† 주저자, jung4651@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

CV는 V2V(Vehicle-to-Vehicle), V2I(Vehicle-to-Infrastructure) 통신을 통해 안전 관련 정보 혹은 교통 관련 정보를 지속적으로 교환 혹은 공유하는 기술을 말한다[1]. NHTSA(National Highway Traffic Safety Administration)의 연구 결과에 의하면 교차로에서 운전 중인 차량에 CV 안전 응용 프로그램을 적용하는 경우 매년 592,000건의 사고와 270,000건의 부상을 예방할 수 있다고 예상하였다[2]. 이에 미국은 USDOT의 주도하에 CV와 관련된 연구를 진행하고 있으며, 탬파, 뉴욕, 와이오밍주에서 현재 연구된 기술들을 바탕으로 파일럿 테스트(pilot test)를 진행하고 있다[3, 4].

CV에서 제공할 수 있는 서비스는 크게 안전 관련 서비스와 사용자 편의성 관련 서비스로 나눌 수 있다[5, 6, 7]. 안전 관련 서비스는 차량의 안전에 영향을 끼칠 수 있는 정보들을 제공하는 서비스이며, 사용자 편의성 관련 서비스는 교통 관련 정보, 결제 서비스 등 사용자에게 편의성을 제공해주는 서비스들을 말한다. CV에서 제공하는 안전 관련 서비스의 경우 안전과 직접적으로 연관이 있기 때문에 메시지와 송/수신자에 대한 신뢰성이 중요하다. 또한 NHTSA는[2]에서 소비자들이 CV 기술을 수용하기 위해서는 프라이버시를 고려하여 연구를 진행해야 함을 강조하였다. 이에 안전 관련 서비스에서 차량이 지속적으로 다른 차량 혹은 기지국에 전송하는 BSM(Basic Safety Messages)로부터 차량을 추적할 수 없도록 차량 익명성을 제공해야 한다. 현재 안전 관련 서비스와 차량 익명성 연구[8, 9, 10, 11, 12, 13, 14, 15, 16]에 비교적 많은 연구가 진행되고 있지만, 편의성 관련 서비스가 다양한 사업 모델을 제공할 수 있으므로 추후 해당 서비스의 연구 및 개발에 많은 연구가 진행될 것으로 기대된다[6].

사용자 편의성 관련 서비스 중에서 차량용 결제 서비스 관련 연구[6, 7, 16, 17, 18, 19, 20, 21]가 몇몇 연구자에 의해 진행되었다. 차량에서 결제 서비스를 제공하기 위해서는 결제 프로토콜이 차량 통신의 요구사항들을 만족해야한다. 특히 차량의 높은 이동성에 의한 네트워크 휘발성[5, 22, 23, 24]과 차량이 금융기관과 직접적인 통신을 할 수 없는 특징[24, 25]을 고려하여 결제 프로토콜을 설계해야 한다. 이에 이전 연구들에서는 효율적이면서도 안전하게 결제 요청을 전달할 수 있는 결제 서비스에 초점을 맞추어 시스템을 설계하였다. 그러나 위의 결제 프로토콜들은 차량 익명성을 제공하지 않는다. 결제 시스템이 차량 익명성을 제공하지 않는 경우 공격자는 결제 관련 정보로부터 차량을 추적할 수 있는 정보들을 수집할 수 있다. 더욱이 안전 관련 서비스에서도 공격자가 수집한 결제 관련 정보와 BSM으로부터 차량을 추적할 수 있다. 즉, 차량 소유주의 개인정보를 보호하기 위해서 차량의 결제 시스템 또한 차량 익명성을 제공해야 한다.

이에 본 논문에서는 결제 내역으로부터 차량을 추적할 수 없는 결제 서비스를 제공하기 위한 차량용 결제 프로토콜을 설계하였다. 차량을 추적할 수 없도록 역방향 불연결성[26] 및 추적성[27]을 만족하는 그룹 서명 기법[10, 26]과 지역을 기반으로 그룹을 분리하여 효율적으로 그룹키를 폐지할 수 있는 DKM(Distributed Key Management)[11]을 사용하여 결제를 수행하며, 결제 참여자의 역할을 분리하여 결제 과정에서 수집한 정보를 바탕으로 차량을 추적할 수 없도록 하였다. 또한 차량만이 자신의 지역 그룹 개인키를 발급받을 수 있도록 ECQV(Elliptic Curve Qu-Vanstone) 묵시적 인증서[28] 기반의 티켓[15] 발급 과정을 적용하였다. 해당 결제 서비스는 다양한 결제 서비스 중에서 스마트 주차 혹은 주유소와 같은 서비스를 제공한다. 또한 차량은 은행과 직접 통신을 할 수 없는 환경이며, 판매자를 통해 서비스 제공자와 통신하는 상황으로 가정한다.

II. 관련 연구

2.1 키오스크 중심(Kiosk-Centric) 결제 모델 및 주요 트랜잭션

키오스크 중심 결제 모델은 Fig.1.과 같이 PG(Payment Gateway), M(Merchant), C(Client), C의 거래은행 I(Issuer), M의 거래은행 A(Acquirer)로 구성되어 있다. 해당 모델은 C가 I와 직접적으로 통신할 수 없는 제한된 환경에서 M이 프록시처럼 행동하여 C와 I의 통신을 가능하게 한다[7, 29].

해당 모델에서 결제를 수행하기 위해서는 크게 3가지 트랜잭션을 수행해야 한다[30]. *Payment* 트랜잭션은 C에 의해서 만들어지며 M에게 대금을 지급하고 서비스 혹은 재화를 받기 위한 메시지이다. *Value Substraction*은 C가 자신의 계좌로부터 돈

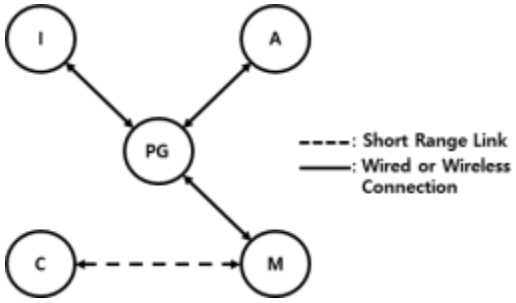

Fig. 1. Kiosk-Centric Payment Model

을 출금하기 위하여 PG에 보내는 요청이다. *Value Claim*은 M에 의해서 만들어지며 자신의 계좌로 돈을 입금하기 위하여 PG에 요청하는 메시지이다.

2.2 차량용 결제 프로토콜 연구 사례

차량용 결제 프로토콜은 차량 통신의 추가적인 요구사항들을 고려하여 설계해야 한다. 이에 KCM-VAN(Kiosk Centric Model payment protocol for-VANet) 프로토콜[6]은 기존의 전자 서명 기법을 사용하지 않고 자체-인증 공개키를 사용하여 결제 프로세스의 효율성을 증가시켰으며, 가명ID를 사용하여 차량 익명성을 제공하려 하였다. [18]에서 제안한 결제 프로토콜의 경우 [6]의 자체-인증 공개키 기법을 기반으로 프로토콜을 설계하였으며, 자체-인증 키 동의 프로토콜을 제안하여 차량과 판매자가 안전하게 대칭키를 공유하게 하였다. 그리고 스트리밍 서비스와 같은 세션 기반 결제와 이벤트 기반 결제를 지원한다. 또한 [6]과 마찬가지로 가명-ID를 사용하여 차량 익명성을 제공하려하였다. 이외에도 [7]에서는 대칭키 암호화 기법만을 사용한 결제 프로토콜을 제안하였으며, [20]에서는 선불카드 기반의 결제 프로토콜을 제안하였다.

현재까지 제안한 프로토콜들의 경우 가명ID만을 사용하여 차량 익명성을 제공하려 하였다. 그러나 가명ID를 지속적으로 사용하면 결제 내역을 기반으로 차량을 추적할 수 있는 문제점을 가지고 있다. 또한 결제 참여자들의 경우 가명ID에 해당하는 차량을 알 수 있기 때문에 내부 공격자에 의한 프라이버시 침해를 방지할 수 없다.

2.3 그룹 서명기반의 차량 통신 연구 사례

그룹 서명 기법은 서명자의 익명을 보장하며 그룹에 가입된 멤버만이 서명을 수행할 수 있다. 이에 차량 익명성을 제공하기 위한 다양한 그룹 서명 기법들이 제안되고 있다. [12]는 차량의 프라이버시를 보호하고 차량 통신의 보안 요구사항을 만족시키기 위해서 Boneh 그룹 서명[31]기반의 그룹 서명 기법과 ID 기반 서명 기법을 사용한 GSIS(Group Signature and Identity-based Signature)를 제안하였다. GSIS는 차량과 차량의 통신에 그룹 서명을 사용하며 차량과 RSU(Road Side Unit) 혹은 특수 차량간의 통신에 ID 기반 서명 기법을 사용하였다. 또한 저자는 그룹의 멤버가 폐지되면 그룹 전체의 키를 업데이트해야하는 기존의 연구와 RL(Revocation List)의 크기가 커지는 문제를 해결하기 위해서 임계값을 설정하여 RL의 크기가 임계값을 넘을 경우에만 그룹의 키를 업데이트하는 방식을 사용하였다. 그러나 GSIS는 서명의 길이가 길고 무죄 입증성을 만족하지 않으며 역방향 불연결성을 만족하지 않는 문제를 가지고 있다. [32]연구에서는 필요한 경우 서명자를 쉽게 추적할 수 있으며 무선 네트워크, 센서 네트워크와 같은 환경에서 사용할 수 있는 그룹 서명 기법을 제안하였다. 그러나 서명의 길이가 길며 단일 기관에서 차량을 추적할 수 있다. 또한 역방향 불연결성을 제공하지 않는 문제가 있다. [10, 13, 26, 33] 연구에서는 차량 익명성을 제공하면서 역방향 불연결성을 만족하는 그룹 서명 기반의 인증 기법을 제안하였다. 역방향 불연결성을 만족시키기 위해 해당 논문은 키 생성 단계에서 시간에 의존적인 폐지 토큰을 발급하고 이를 RL에 추가하여 차량의 폐지 여부를 확인한다. 그러나 해당 연구들의 경우 단일 기관에서 폐지 토큰을 관리하므로 이를 통해 서명을 수행한 차량을 찾을 수 있다. 또한 [13, 26, 33] 연구는 역방향 불연결성을 만족시키기 위해 서명의 길이가 길어지는 문제점이 있다. [15]는 가명ID 발급 프로세스에 참여한 기관이 차량에서 사용하는 가명ID를 모두 알고 있는 문제점을 해결하기 위해 가명ID 발급 기관을 티켓 발급 기관과 토큰 발급 기관으로 분리하였다. [11]에서는 그룹 서명 기법에서 폐지와 관련된 메커니즘의 오버헤드가 커지는 문제점을 해결하기 위해 지역을 기반으로 그룹을 분리한 그룹 서명 기법을 제안하였다. 해당 연구에서는 차량이 TA(Trusted Authority)로부터

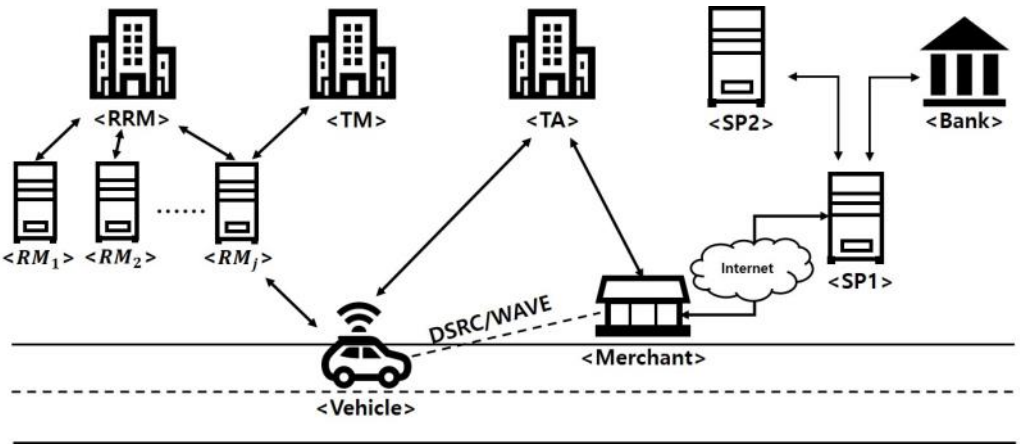

Fig. 2. Components of Payment Protocol

그룹 개인키를 발급받으며, 이를 기반으로 각 지역을 담당하는 RM(Regional group Manager)으로부터 키 업데이트 정보를 수신하여 지역 그룹 개인키를 발급받는다. 기존의 논문의 경우 TA의 신뢰를 기반으로 키를 발급을 수행하지만 해당 연구에서는 RM을 기반으로 키를 발급받으므로 RM에 대한 신뢰가 중요하다. 그러나 차량들이 RM을 신뢰할 수 없으므로 해당 논문에서는 차량이 어떤 지역 그룹 개인키를 소유하고 있는지 RM과 TA가 알 수 없게 하여 부인방지를 제공한다. 그러나 TA가 차량의 그룹 개인키를 알고 있으므로 차량으로 위장하여 RM에게 키 업데이트 정보를 발급받을 수 있어 무죄 입증성(excul pability)을 만족하지 못한다.

이에 본 논문에서는 위의 연구들이 가지고 있는 문제점들을 해결하기 위해 BU-익명성 및 추적성을 만족하면서 지역을 기반으로 그룹을 분리한 그룹 서명 기법과 ECQV 묵시적 인증서 기반으로 결제 프로토콜을 설계하였다.

III. 배경지식

본 장에서는 제안하는 차량용 결제 프로토콜의 구성요소와 요구사항 및 결제 프로토콜에 사용되는 표기법들을 설명한다.

3.1 제안하는 차량용 결제 프로토콜 구성요소

본 논문에서 제안하는 결제 프로토콜은 키오스크 중심 모델을 따른다. 이는 차량 통신의 특성상 제한된 환경에서 결제를 수행하기 위한 것이다. 본 논문에서 제안하는 결제 프로토콜의 구성요소는 Fig. 2.와 같다.

- **차량**: 차량은 OBU(On Board Unit)를 탑재하며 다른 차량, 판매자 혹은 RSU와 DSRC(Dedicated Short Range Communications)/WAVE(Wireless Access in Vehicle Environment)를 통해 메시지를 주고받는다. 본 논문에서 차량은 판매자로부터 제품 혹은 서비스를 구매하고자 하는 결제 서비스의 소비자로 가정한다.
- **판매자**: 판매자는 서비스 혹은 물품을 제공하는 구성요소이다. 본 논문에서는 판매자를 주유소, 톨게이트 등과 같은 물리적인 존재로 가정한다[7]. 판매자는 차량과 DSRC /WAVE로 통신하며 SP(Service Provider)와 인터넷을 통해 연결되어 있다. 또한 판매자는 판매자 거래은행을 통해 거래를 수행한다.
- **서비스 제공자1(SP1)**: SP2, 은행 그리고 인터넷에 연결되어 각 네트워크에서 중간자 역할을 수행한다. 인터넷을 통해 결제 요청을 처리하고, 이에 대한 응답을 차량 및 판매자에 전송한다.
- **서비스 제공자2(SP2)**: SP2는 SP1에서 받은 정보들을 바탕으로 결제 요청 차량의 등록 여부 및 인증을 수행한다. 그리고 등록된 차량에 대응되는 가상 계좌로부터 SP의 계좌로 금액을 인출하는 역할을 수행한다.
- **RRM(Root RM)**: RRM은 각 지역을 관리하는 RM들에 그룹 개인키를 발급하는 역할을 수행한다. RRM은 TA와 그룹 파라미터 및 그룹 비밀

키를 공유한다.

- **RM**: RM_j는 $Region_j$를 관리하는 기관으로 차량에 키 업데이트 정보를 발급한다. RM은 RRM으로부터 그룹 개인키를 발급받으며, TM과 협력하여 차량의 신원을 밝힐 수 있다.
- **TA**: TA는 차량에 그룹 개인키와 티켓을 발급하는 기관이다. TA는 티켓 발급에 필요한 ECC 키 쌍과 그룹 공개키 및 비밀키를 소유하고 있으며 RRM과 그룹 파라미터 및 비밀키를 공유한다.
- **TM(Trace Manager)**: TM은 RM_j와 같이 부정거래가 발생한 차량의 신원을 확인하는 역할을 수행한다.

3.2 제안하는 차량용 결제 프로토콜 보안 요구사항

본 장에서는 차량의 익명성을 유지하면서 안전한 결제를 수행하기 위해 결제 프로토콜이 만족해야하는 보안 요구사항들을 분석한다[10, 16, 34, 27, 35, 36, 37].

3.2.1 차량 보안 요구사항

- **V1 요구사항(차량 자산 보호)**: 계좌와 연결되어 있는 차량 V가 아닌 다른 차량 혹은 장치에서 V의 계좌로 결제를 수행할 수 없어야한다. 또한 악의적인 판매자, 인가받지 않은 판매자 혹은 SP에 의해 의도하지 않은 결제가 수행되었을 때, 해당 결제를 승인하지 않았음을 증명할 수 있어야 한다.
- **V2 요구사항(결제 승인 확인)**: 차량은 결제 요청 후 자신의 계좌에서 돈이 인출되었음을 확인할 수 있는 증명 값을 수신해야한다.
- **V3 요구사항(차량 익명성)**: 차량이 수행한 거래의 트랜잭션은 잠재적 차량 집합 내에서 익명성을 유지할 수 있어야 한다. 즉, 트랜잭션으로부터 특정한 차량이 결제를 수행했음을 알 수 없어야 한다.
- **V4 요구사항(역방향 불연결성)**: 부정 거래가 발생하여 차량의 식별 정보를 확인한 경우, 부정 거래가 발생한 시점 이전에 수행된 거래내역과는 연결시킬 수 없어야 한다.

3.2.2 판매자 및 SP 보안 요구사항

- **R1 요구사항(판매자 자산 보호)**: 판매자 M이 의도하지 않은 결제가 수행될 수 없어야하며 해당 결제를 승인하지 않았음을 증명할 수 있어야 한다.
- **R2 요구사항(입금 확인에 대한 응답)**: 판매자는 자신의 은행으로부터 입금사실을 입증할 수 있는 증명을 수신해야 한다.
- **R3 요구사항(조건부 차량 식별)**: 익명의 차량에 의해서 부정 거래가 발생하였을 경우 해당 차량을 식별할 수 있어야하며, 이는 다른 참가자들과의 협력을 통해 수행되어야 한다.

IV. 제안하는 차량용 결제 프로토콜

해당 장에서는 제안하는 차량용 결제 프로토콜의 결제 서비스 등록 및 결제 과정을 서술하며 이를 수행하기 위한 티켓 및 지역 그룹 개인키 발급 과정을 서술한다. 또한 부정 거래를 수행한 차량ID를 식별하고 지역 그룹 개인키를 폐지하는 과정을 설명한다.

4.1 차량의 지역 그룹 개인키 발급 과정

4.1.1 시스템 초기화

해당 장에서는 차량에 그룹 개인키 $gsk_i = < x_i, A_i >$와 티켓 δ_v를 발급하기 위한 시스템 초기화 절차를 소개한다. 시스템 초기화에는 차량에 티켓 δ_v와 그룹 개인키 gsk_i를 발급하기 위한 TA, 지역 j를 관리하며 차량에 키 업데이트 정보를 발급하는 RM_j, 각 지역의 RM_j를 관리하며 RM_j에 그룹 개인키 $rgsk_j$를 할당하기 위한 RRM, 폐지 토큰을 발급하기 위한 TM의 초기화 절차가 포함되어 있다.

① TA는 그룹 키 발급에 필요한 그룹 파라미터[26, 33] $(G_1, G_T, p, e, g_1, g_T)$, 그룹 비밀키 $\gamma \in Z_p^*$, 그리고 그룹 공개키 $w = g_1^{\gamma}$을 계산하고 RRM과 $(G_1, G_T, p, e, g_1, g_T, \gamma)$를 공유한다. 또한 티켓 발급을 위한 타원 곡선 매개변수[28] (q, a, b, G, n, h)를 선택한다.

② RRM은 지역 j를 관리하는 RM_j에 그룹 개인키 $rgsk_j = < x_j, A_j = g_1^{1/\gamma + x_j} >$을 발급한다.

③ TM은 모든 시간 $t \in [1, T]$에 대하여 $r_t \in Z_p^*$를 선택하여 $h_t = g_1^{r_t}$을 계산한다.

최종적으로 TA는 그룹 공개키를 $gpk = (g_1, g_T,$

$w, h_1, h_2, \cdots, h_T$)로 설정한다. 그리고 TM은 폐지 토큰 비밀정보 $rtsk_{TM}=r_t$, RM_j는 그룹 개인키 $rgsk_j=<x_j, A_j>$, TA와 RRM은 그룹 비밀키 $gmsk=\gamma$를 안전하게 저장한다.

4.1.2 차량 티켓 발급

본 논문에서 제안하는 프로토콜의 경우 차량 i가 RM_j로부터 키 업데이트 정보를 받기 위해서 자신이 결제 서비스 그룹 멤버임을 증명할 수 있는 티켓 δ_{v_i}를 발급받아야 한다. [11]에서는 TA가 차량에 발급한 비밀정보 $gsk[i]$를 모두 알고 있으므로 TA는 차량으로 위장하여 키 업데이트 정보를 부적절한 방법으로 발급받을 수 있다. 이에 본 논문에서는 그룹 개인키 이외에 ECQV 묵시적 인증서 기반의 티켓 발급 과정을 추가하여 차량만이 알고 있는 비밀 값을 키 업데이트 발급 과정에서 사용할 수 있다. 티켓 발급 과정은 SCMS(Security Credential Management System)[8]의 등록 인증서 발급환경과 유사하게 차량 제조사와 TA간의 안전한 채널을 기반으로 수행되며, 그 과정은 Fig. 3.과 같다.

① 그룹 개인키 발급 요청: 차량 V_i는 임의의 ECC 키 쌍 $k_{v_i}\in[1,...,n-1]$와 $R_{v_i}=k_{v_i}G$를 생성하고 R_{v_i}를 TA에게 전송한다.

② 그룹 개인키 발급 응답: TA는 임의의 값 $c\in[1,...,n-1]$를 선택하고 자신의 ECC 키 쌍 (Q_{TA}, d_{TA}), 그룹키 쌍 (γ, w)으로 공개키 추출 값 $P_{v_i}=R_{v_i}+cG=(k_{v_i}+c)G$와 그룹 개인키 $gsk_i=<x_i, A_i=g_1^{1/\gamma+x_i}>$를 생성하여 P_{v_i}, $<x_i, A_i>$와 결제 서비스 그룹 ID인 GID를 차량에 전송한다.

③ 티켓 발급 요청: V_i는 P_{v_i}, $<x_i, A_i>$, GID를 수신하고 임의의 값 r_0를 선택하여 $W_1=g_1^{r_0}$, $W_2=g_1^{x_i}$, $\eta=A_i^{r_o}$를 계산하여 TA에 전송한다.

④ 티켓 발급 응답: TA는 $e(\eta, w W_2)=e(W_1, g_1)$을 확인하여 V_i가 그룹 개인키 gsk_i를 수신하였음을 확인한다. 이후 $\phi=h(P_{v_i}, GID, W_1, W_2, \eta)$로부터 비밀키 추출 값 $r_{v_i}=\phi c+d_{TA}$를 계산하여 r_{v_i}값을 V_i에 전송한다.

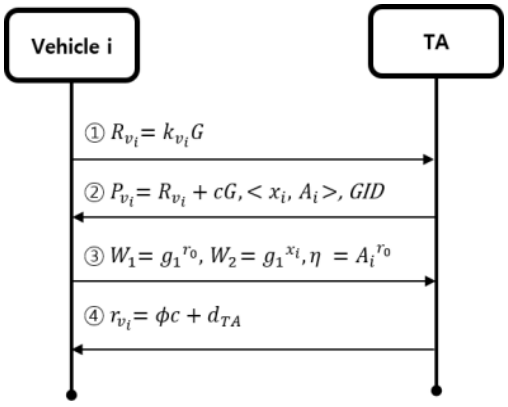

Fig. 3. Ticket Issuance Process

비밀키 추출 값을 수신한 V_i는 티켓의 비밀키 $s_{v_i}=\phi k_{v_i}+r_{v_i}$와 공개키 $Pk_{v_i}=s_{v_i}G=\phi P_{v_i}+Q_{TA}$를 계산하고 Table 1.와 같이 티켓 δ_{v_i}를 저장한다. 이후 V_i는 δ_{v_i}, $<x_i, A_i>$, r_0를 저장한다.

차량의 티켓 발급 과정과 유사하게 판매자 또한 TA로부터 판매자 ID_m으로 티켓 δ_m을 발급받아야 한다. 해당 티켓을 통해 판매자는 차량에 자신이 정당한 판매자임을 증명할 수 있다. 판매자의 경우 익명성을 제공할 필요가 없다. 이에 본 논문에서 판매자는 ECQV 묵시적 인증서를 사용하여 안전하면서도 효율적인 통신을 지원하도록 한다. 판매자의 티켓 발급 절차는 [28]와 같다. 티켓 발급 절차를 완료한 M은 서명에 사용할 비밀키$s_m=\phi r_m+k_m$을 계산하고 이에 대응되는 공개키 $Pk_m=\phi P_m+Q_{TA}$를 계산하여 저장한다. 이에 판매자 M의 티켓은 $\delta_m=\{ID_m, P_m\}$으로 구성되어 있다.

판매자는 수신한 티켓을 기반으로 ECDSA와 같은 효율적인 서명 기법을 사용할 수 있다[38]. 판매자의 서명을 수신한 차량은 MRL(Merchant Revocation List)에 포함된 판매자의 ID_m을 보고 서명의 유효성을 판단할 수 있으며 효율적으로 서명을 검증할 수 있다.

Table 1. Format of TIcket δ_{v_i}

GID	η, W_1, W_2	P_{v_i}

4.1.3 차량의 키 업데이트 정보 발급

[11]에서는 지역을 기반으로 그룹을 분리한 키 업데이트 절차를 통해 효율적인 그룹키 폐지 절차와 폐지 여부 확인을 지원한다. 그러나 티켓 발급 기관이 차량으로 위장하여 키 업데이트 정보를 수신할 수 있는 문제가 존재한다.

이에 본 논문에서는 차량 티켓 δ_i와 그룹 개인키 $< x_i, A_i >$를 기반으로 업데이트 정보를 받을 수 있게하여 TA가 차량으로 위장할 수 없도록 하였다. 또한 티켓에 차량의 그룹 개인키 관련 정보를 포함하도록 하여 [11]의 그룹 개인키 확인 절차를 제거하였으며, 겹선형 쌍함수 기반의 서명 대신 ECDSA와 같은 서명 기법을 사용하여 효율적으로 업데이트 정보를 받을 수 있도록 개선하였다. RM_j의 지역 그룹 공개키 $rgpk_j=\{Pk_j^1, Pk_j^2, Pk_j^3, Pk_j^4\}$[11]를 사용한 키 업데이트 정보 발급 과정은 다음과 같다.

① 키 업데이트 정보 발급 요청($V_i \rightarrow RM_j$): V_i는 RM_j에 키 업데이트 정보 발급을 요청한다. 이에 차량은 $Req=(T, x_i, t, \varphi=(Pk_j^2)^{r_0})$를 생성하고 자신이 발급받은 티켓 δ_{v_i}에 대응되는 s_{v_i}로 Req에 서명을 수행 후 $Req \| \delta_{v_i} \| Sig_{v_i}(Req)$을 전송한다.

② 키 업데이트 정보 발급 응답($RM_j \rightarrow V_i$): RM_j는 티켓 δ_{v_i}로 Pk_{v_i}를 계산하여 해당 티켓이 유효함을 확인하며 V_i가 유효한 그룹 개인키를 소유하고 있음을 알 수 있다. 이후 Pk_{v_i}로 서명 $Sig_{v_i}(Req)$를 검증한다. 검증에 성공하면 Req에 포함된 x_i 값이 블랙리스트에 포함되어 있는지 확인한다. 블랙리스트에 포함되어 있다면 키 업데이트 정보 발급을 중단하며, 그렇지 않은 경우 티켓 δ_{v_i}의 η값과 φ로부터 키 업데이트 정보 θ를 생성하여 V_i에 전송한다. θ를 수신한 V_i는 다음과 같이 지역 그룹 개인키 $A_i^{j,t}$를 계산한다.

$$A_i^{j,t} = \theta^{\frac{1}{r_0}} = A_j^{\frac{1}{(x_j + h(j\|t))(x_i+\gamma)}} \quad (1)$$

이후 V_i는 RM_j로부터 발급받은 지역 그룹 개인키가 지역 j를 관리하는 RM_j로부터 발급받았으며 시간 t에 대한 개인키임을 다음과 같이 검증할 수 있다.

$$e(A_i^{j,t}, Pk_j^1 g_1^{h(j\|t)}) \stackrel{?}{=} e(A_i, A_j) \quad (2)$$

4.1.4 그룹 서명 및 검증

지역 그룹 개인키를 수신한 차량 V_i는 [10]의 그룹 서명 생성 및 폐지 절차를 수행하며, 기존의 그룹키가 아닌 지역 그룹 개인키로 서명을 수행하기 위해 RM_j의 지역 그룹 공개키 $rgpk_j$로 [11]의 P_1과 P_2를 계산한다. 이후 서명 생성 및 검증 절차는 다음과 같다.

① 메시지 M에 대한 서명 σ을 생성할 차량 V_i는 $\alpha \in Z_p^*$를 선택하고 T_1, T_2를 계산한다.

② 이후 $r_\alpha, r_{x_i} \in Z_p^*$를 선택하여 다음과 같이 $R_1 = e(Pk_j^2, Pk_j^2)^{r_\alpha} e(T_1, P_1)^{-r_{x_i}}, R_2, c, s_\alpha, s_{x_i}$를 계산한다.

③ 차량은 서명 $\sigma=(T_1, T_2, c, s_\alpha, s_{x_i})$와 메시지 M을 전송한다.

서명을 수신한 판매자는 다음과 서명 검증과 폐지 여부를 확인한다.

① 판매자는 서명 검증을 위해 R_1'과 R_2'을 계산한다.

$$R_1' = e(Pk_{RM_j}^2, Pk_{RM_j}^2)^{s_\alpha} e(T_1, P_1)^{-s_{x_i}} e(T_1, P_2)^{-c} \quad (3)$$

② 이후 판매자는 R_1', R_2'로부터 $c' = h(M \| j \| t \| T_1 \| T_2 \| R_1' \| R_2')$을 계산하여 $c'=c$이 성립할 경우 유효한 서명임을 알 수 있다.

③ 판매자는 RL_j에 포함된 $(grt_{i,j,t}^1, grt_{i,j,t}^2)$로부터 서명자의 폐지 여부를 확인할 수 있다.

$$e(T_1, grt_{i,j,t}^1) = e(T_2 grt_{i,j,t}^2, Pk_j^2) \quad (4)$$

해당 식이 성립할 경우 차량 i가 폐지된 것으로 간주한다.

4.1.5 차량 ID 식별 및 그룹 개인키 폐지 절차

기존의 그룹 서명 기법[10, 14, 26, 32, 33]의 경우 단일 기관인 GM(Group Manager)에서 폐지 토큰을 계산하여 서명자의 신원을 밝힐 수 있는 문제가 존재하며, [11]은 그룹키 폐지 절차를 제공하지 않는다. 또한 그룹키 폐지 절차를 수행하기 위해서 모든 그룹 멤버의 폐지 토큰을 비교해야 하며 GM이 모든 그룹 멤버의 폐지 토큰을 저장하고 있어야 한다.

이에 본 논문에서는 부정 거래를 식별한 SP가 TM에 폐지 요청 메시지를 전송하여 RM_j와 협력을 통해 폐지 절차를 수행하도록 한다. 또한 부정 거래가 발생한 시간 t와 지역 j에서 키 업데이트 정보를 받은 차량ID 집합만을 비교하여 폐지 절차를 수행하여 효율적이고 모든 그룹 맴버의 폐지 토큰을 저장할 필요가 없다. 자세한 절차는 다음과 같다.

① 그룹 개인키 폐지 요청(SP → TM): SP는 부정 거래를 탐지하고 해당 거래에 포함된 $h(h(OI)\|h(PI))$, $GSig_{v_i}(h(h(OI)\|h(PI)))$, T_{v_i} 그리고 ID_m을 TM에게 전송한다.

② 차량ID 식별 관련 정보 전송(TM → RM_j): TM은 T_{v_i}, ID_m으로부터 t와 j를 선택하고 서명에 포함된 T_1으로부터 $T_1^{r_t}$을 계산하여 RM_j에 전송한다.

③ 차량ID 식별 및 그룹 개인키 폐지(RM_j → TM): $T_1^{r_t}$값을 수신한 RM_j는 t시간에 키 업데이트 정보를 발급 받은 차량 $\{x_i\}$로부터 $e(T_1^{r_t}, g_1^{(x_i+\gamma)(x_j+h(j\|t))})$와 $e(T_2 h_t^{-x_i}, A_j)$를 계산하여 두 값이 같은 경우 x_i를 블랙리스트에 추가하고 폐지 절차를 수행한다. 이후 RM_j는 폐지 토큰 생성 정보 RI(Revocation Information)$= w^{(x_j+h(j\|t))} g_1^{x_i(x_j+h(j\|t))}$와 폐지 토큰 $grt_{i,j,t}^2 = h_t^{-x_i}$을 생성하여 RL_j에 추가한 후 RI를 TM에게 전송한다.

④ 폐지 토큰 생성 및 추가(TM → RM_j): 위의 정보를 수신한 TM은 부정 거래 발생시간에 대응되는 r_t로부터 $grt_{i,j,t}^1 = RI^{r_t} = h_t^{(x_i+\gamma)(x_j+h(j\|t))}$을 계산하여 RM_j에게 전송한다. 이를 수신한 RM_j는 $grt_{ij,t}^1$를 RL_j에 추가한다. 그리고 다른 RM_{j^*}에게 x_i를 전송하여 블랙리스트에 추가하도록 하며, i에 대한 지역 j^*의 폐지 토큰을 RL_{j^*}에 추가하도록 한다.

4.2 결제 서비스 등록 및 수행 절차

본 장에서는 차량이 결제 서비스를 등록한 후 판매자를 통해 재화를 구입하는 절차를 서술한다. 이때 SP1과 SP2, SP1과 은행간의 통신은 안전한 환경에서 수행된다고 가정한다. 이에 본 논문에서는 [34]에서 보인 결제 프로토콜과 동일하게 결제를 위해 필요한 정보들을 보내는 절차만을 서술한다.

4.2.1 결제 서비스 등록 단계

차량이 SP를 통해 결제를 수행하기 위해서는 사전에 SP에 차량을 등록하고 SP에서 관리하는 가상 계좌를 발급받아야 한다. 이를 위해서 차량은 TA로부터 발급받았던 티켓 δ_{v_i}를 사용하여 결제 서비스 그룹의 멤버임을 증명하고 SP와 결제에 필요한 정보를 공유한다. 결제 서비스 등록 절차는 다음과 같다.

① 서비스 등록 요청(V_i → SP1): 차량 V_i는 사전에 TA로부터 발급받았던 티켓 δ_{v_i}를 기반으로 등록 요청 메시지 $RegReq$(Registration Request)를 계산한다. V_i는 가상 계좌 인증에 사용될 대칭키 $K_{v_i-sp2} \in Z_p^*$를 선택하고 SP1으로 부터 계좌관련 정보를 숨기기 위해 sk_{v_i-sp2}를 계산한다. V_i는 $r_{v_i sp2} \in [1, n-1]$를 선택하고 SP2의 인증서 공개키 Pk_{sp2}로부터 $sk_{v_i-sp2} = s_{v_i} r_{v_i sp2} Pk_{sp2}$를 계산한다. 이후 익명 신원 정보 AID를 선택하여 $RegReq$를 $SP1$에 전송한다.

$$RegReq = \{\delta_{v_i}, r_{v_i sp2} Pk_{v_i}, E_{sk_{v_i-sp2}}(AID, K_{v_i-sp2}), Sig_{v_i}(r_{v_i sp2} Pk_{v_i}, E_{sk_{v_i-sp2}}(AID, K_{v_i-sp2}))\} \quad (5)$$

② 가상 계좌 발급 요청(SP1 → SP2): V_i로부터 등록 요청을 받은 SP1은 δ_{v_i}로부터 공개키를 추

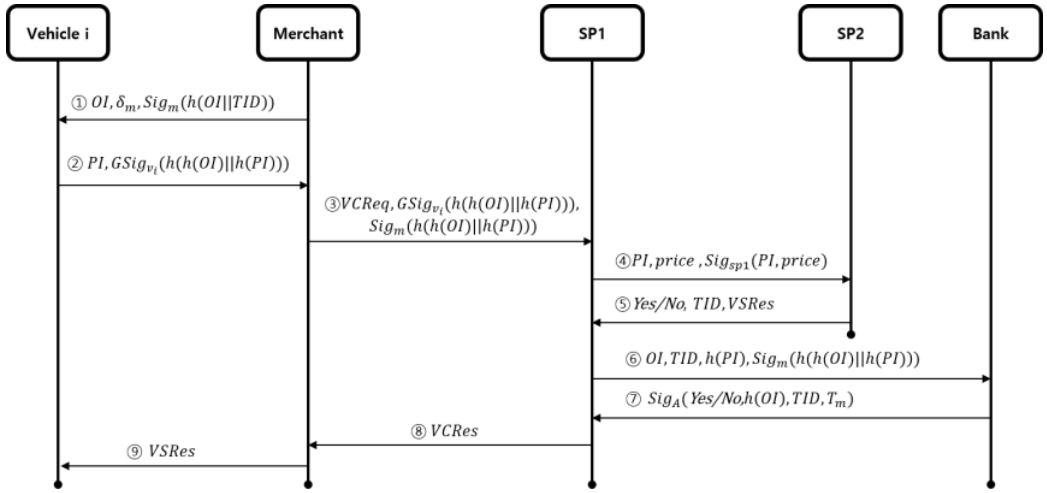

Fig. 4. Payment and Authorization Phase

출하여 서명을 검증한다. 이후 가상계좌 발급을 위해 SP2에 $r_{v_i sp2}Pk_{v_i}, E_{sk_{v_i-sp2}}(AID, K_{v_i-sp2})$를 전송한다.

③ 가상 계좌 발급 응답(SP2 → SP1): SP2는 $r_{v_i sp2}Pk_{v_i}$로부터 $sk_{v_i-sp2}=s_{sp2}r_{v_i sp2}Pk_{v_i}$를 계산하고 AID 및 K_{v_i-sp2}를 추출한다. 이후 가상 계좌 VA_{v_i}를 발급하고 sk_{v_i-sp2}로 암호화한 후 서명 $Sig_{sp2}(AID, K_{v_i-sp2}, VA_{v_i})$와 같이 SP1에게 전송한다.

④ 등록 요청 응답(SP1 → V_i): SP1은 SP2로부터 수신한 정보를 차량에 전달한다. 이후 차량은 Pk_{sp2}로 서명을 검증하고 가상 계좌 VA_{v_i}와 K_{v_i-sp2}를 저장한다.

4.2.2 결제 및 승인 단계

본 논문에서 제안한 결제 프로토콜은 톨게이트, 주유소, 스마트 주차 등에 사용되는 것으로 가정하므로 판매자 M이 결제 요청을 V_i에게 보내는 것으로 시작한다. 위의 예들이 아닌 다른 서비스들의 경우 프로토콜을 적절하게 변경하여 결제를 진행할 수 있다. 결제 단계에서 V_i는 초기화 단계를 통해 가상 계좌에 일정한 금액을 입금한 상태로 가정한다. 결제 및 승인 절차는 Fig. 4.와 같다.

① 결제관련 정보 전송: M은 결제 관련 정보 OI (Order Information) = $\{ID_m, T_m, OD$ (Order Description), $price\}, \delta_m, Sig_m(h(OI\|TID))$를 V에게 전송한다.

② 결제 요청: V_i는 δ_m으로부터 Pk_m을 계산하여 서명을 검증하고 OI를 확인한다. 그리고 소유하고 있는 SP2의 인증서로부터 대칭키 $sk_{v_i-sp2}=s_{v_i}r_{v_i sp2}Pk_{sp2}$를 계산한다. 그리고 $r_{v_i sp2}Pk_{v_i}$를 포함하는 다음과 같은 메시지를 작성한다.

$$VSReq(\text{Value Substraction Request}) = MAC(TID, T_{v_i}, AID, price, K_{v_i-sp2}) \quad (6)$$

$$PI = \{TID, T_{v_i}, r_{v_i sp2}Pk_{v_i}, E_{sk_{v_i-sp2}}(AID, VSReq)\} \quad (7)$$

이후 V는 다음과 같은 메시지를 M에게 전송한다.

$$PI(\text{Payment Information}), GSig_v(h(h(OI)\|h(PI))) \quad (8)$$

③ 결제 승인 요청: M은 RM_j의 지역 그룹 공개키 $rgpk_j$를 사용하여 서명 $GSig_v(h(h(OI)\|h(PI)))$을 검증한다. 이를 통해 M은 V_i가 OI에 대한 결제를 요청하였음을 확인할 수 있다. 이후 $VCReq$(Value Claim Request) $=\{PI, OI, \delta_m, ID_A\}$를 계산하여 SP1에게 다음과 같은 메시지를 전송한다.

$$VCReq, GSig_{V_i}(h(h(OI)\|h(PI))),$$
$$Sig_m(h(h(OI)\|h(PI))) \quad (9)$$

④ 차량 등록 여부 확인: SP1은 위의 메시지를 수신하고 V_i와 M의 서명을 검증한다. 이를 통해 M과 V_i가 OI에 대한 결제를 승인하였으며 같은 주문에 대한 결제 요청임을 확인할 수 있다. 또한 해당 서명이 결제를 요청한 M과 V_i에 의해서 작성되었으며, 각 $VSReq, VCReq$가 위/변조되지 않았음을 알 수 있다. 이후 SP1은 PI, $price$, $Sig_{sp1}(PI, price)$를 SP2에게 전송한다.

⑤ 결제 금액 인출: SP2는 sk_{v_i-sp2}를 계산하고 AID 및 K_{v_i-sp2}를 추출하여 차량을 인증한다. 인증에 성공하면 SP2는 차량의 VA_{v_i}로부터 $price$에 해당하는 금액을 인출하여 자신의 가상 계좌로 돈을 입금한다. 그리고 $VSRes$(Value Substraction Response)=$\{Yes/No, Sig_{SP2}(Yes/No, AID, TID, T_{v_i}, price)\}$를 작성하고 Yes/No, TID, $VSRes$를 SP1에게 전송한다.

⑥ 입금 요청: SP1은 V_i의 가상 계좌 VA_{V_i}로부터 돈이 입금되었음을 확인하고 판매자 은행 A에 입금 요청 메시지 $\{OI, TID, h(PI), Sig_m(h(h(OI)\|h(PI)))\}$을 전송한다.

⑦ 입금 응답: 이를 수신한 A는 SP의 계좌에서 M의 계좌로 돈을 입금한다. 이후 A는 SP1에게 입금에 대한 확인으로 $Sig_A(Yes/No, h(OI), TID, T_m)$를 전송한다.

⑧ 결제 승인 응답: SP1은 입금 요청 $VCReq$에 대한 응답 $VCRes$(Value Claim Response)=$\{VSRes, Sig_A(Yes/No, h(OI), TID, T_m)\}$를 M에 전송한다.

⑨ 결제 응답: $VCRes$를 수신한 M은 A의 서명을 확인하여 정상적으로 결제가 완료되었음을 확인하고 V_i에 $VSRes$를 전송한다. 이에 V_i는 $VSRes$를 확인하여 정상적으로 결제가 완료되었음을 확인할 수 있다.

V. 제안한 프로토콜 분석

5.1 보안 요구사항 분석

본 장에서는 본 논문에서 제안하고 있는 결제 프로토콜이 3.2절에서 정의한 보안 요구사항을 만족하는지 분석한다. 보안 요구사항 분석에 필요한 그룹 서명의 추적성 및 BU-익명성에 대한 증명은 본 논문의 부록에 서술하였다.

5.1.1 차량 보안 요구사항 분석

- **V1 요구사항(차량 자산 보호)**: 본 요구사항은 차량 V_i이외의 장치 혹은 기관에서 V_i에 대한 결제를 수행할 수 없음을 만족해야함을 말한다. 이를 위해서 V_i이외의 차량 혹은 M에 의해서 V_i의 결제 승인에 대한 $VSReq$와 증명 값을 만들어 낼 수 없으며, 해당 정보의 위변조 및 재전송에 대한 탐지가 가능함을 보여야 한다. 이를 위해서 초과 지출(overspending) 및 재전송 공격에 안전함을 보이며, 계좌 인증 관련 정보의 탈취가 불가능함을 보인다.

① A_1 공격자(초과 지출 공격): 먼저 악의적인 판매자 A_1이 실제 재화 및 서비스의 가격보다 높은 가격으로 결제를 수행하는 경우 SP가 이를 탐지할 수 있음을 보인다. A_1은 V_i와 합의하였던 OI의 $price$가 아닌 OI'의 $price'$으로 결제 요청을 전송하려 한다. A_1은 V_i로부터 OI에 대한 결제 요청 $VSReq=MAC(TID, ..., price, K_{v_i-sp2})$, PI 그리고 서명 $GSig_{v_i}(h(h(OI)\|h(PI)))$을 수신한다. 이후 A_1은 $VCReq=\{PI, OI', \delta_{m'}, ID_A\}$를 계산하여 차량의 서명 및 $Sig_{A_1}(h(h(OI')\|h(PI)))$을 SP1에게 전송한다. 이를 수신한 SP1은 $VCReq$의 PI와 OI'으로부터 $h(OI')$와 $h(PI)$을 계산하여 서명을 검증한다. 이때 함수 h가 충돌저항성을 만족한다면, $h(OI) \neq h(OI')$이므로 V_i의 서명 검증을 통과할 수 없다. 또한 서명 검증에 통과했다 하더라도 SP2에서 $VSReq$를 검증하는 과정에서 서로 다른 주문 정보에 대한 결제 요청임을 탐지할 수 있다. 즉, A_1이 초과지출 공격에 성공하기

위해서는 차량 V_i의 서명을 변조해야 한다. 그러나 [27]에서 추적성을 만족하는 서명 기법은 위조 불가능성을 제공할 수 있다 하였으며, 해당 그룹 서명 기법은 부록에서 보인바와 같이 추적성을 만족하므로 A_1이 해당 공격을 수행할 수 없음을 알 수 있다.

② A_2 공격자(재전송 공격): 다음으로 공격자 A_2가 이전 거래 TID에 대한 증명 값 $GSig_{v_i}(h(h(OI)\|h(PI)))$를 다음 거래인 TID'에서 재사용하는 공격을 탐지할 수 있음을 보인다. 이때 $OI=OI'$ 그리고 $PI=PI'$인 경우는 타임스탬프 T_{v_i}와 T_{A_2} 그리고 TID에 의해서 SP1이 거래 메시지 재사용을 탐지할 수 있으므로 다음과 같은 공격을 가정해본다. A_2는 V_i와 평소와 같이 거래를 수행하며 T_{A_2}와 TID'를 제외한 나머지 주문 정보를 이전 주문과 동일하게 하여 V_i에게 전송한다. 이후 V_i는 TID'에 해당하는 증명 값을 A_2에게 전송한다. 이를 수신한 A_2는 $VCReq'=\{PI', OI' ...\}$과 TID의 증명 값을 SP1에게 전송한다. 이를 수신한 SP1은 현재 시간 T와 T_{A_2} 및 T_{v_i}' 그리고 저장된 TID값과 TID'값을 비교하여 해당 메시지가 재사용되지 않았음을 확인할 수 있다. 그러나 $h(OI)\neq h(OI')$이며 $h(PI)\neq h(PI')$이므로 증명 값에 대한 검증과정을 통과할 수 없다. 즉, 해당 공격을 성공하기 위해서는 초과지출 공격과 마찬가지로 서명의 변조가 필요하므로 A_2는 해당 공격을 수행할 수 없다.

공격자가 V_i의 계좌 인증 정보를 탈취하여 V_i의 계좌로 결제를 수행할 수 없음을 다음과 같이 보일 수 있다. 이를 증명하기 위해 공격자는 차량의 역할을 수행하며 결제 서비스 등록 단계의 내용들을 도청하는 수동적 공격자 A_3와 티켓 δ_{v_i}의 비밀키 s_{v_i}를 탈취 후 V_i로 위장하여 결제 서비스 등록을 수행하는 능동적 공격자 A_4로 나눌 수 있다.

③ A_3 공격자(수동적 공격자의 도청 공격): 수동적 공격자 A_3가 결제 서비스 등록 단계에서 얻을 수 있는 정보들은 다음과 같다.

$$r_{vsp2}Pk_v,\ E_{sk_{v-sp2}}(AID,\ K_{v-sp2}),$$

$$E_{sk_{v-sp2}}(VA_v) \tag{10}$$

이때 공격자 A_3가 $AID, K_{v_i-sp2}, VA_{v_i}$를 얻기 위해서는 암호화키 sk_{v_i-sp2}를 계산할 수 있어야 한다. 그러나 sk_{v_i-sp2}의 경우 $r_{v_isp2}Pk_{v_i}$와 s_{sp2}를 통해 계산할 수 있으므로 s_{sp2}를 알고 있는 사용자만이 계산할 수 있다. 즉, 공격자 A_3는 V_i의 계좌 인증 정보를 알기 위해서는 SP2의 비밀키를 알고 있어야하므로 해당 공격을 수행할 수 없다. 이때 SP2의 비밀키를 탈취 할 수 없음을 보이기 위해서 공격자 A_4의 능동적 공격이 불가능함을 보인다. SP2의 인증서와 차량의 티켓은 ECQV 묵시적 인증서를 사용하므로 차량 티켓의 안정성을 보임으로써 SP2의 비밀키를 탈취할 수 없음을 보일 수 있다.

④ A_4 공격자(능동적 공격자의 위장 공격): 능동적 공격자 A_4가 δ_{v_i}의 비밀키 s_{v_i}를 탈취하였다 가정하였을 때, A_4는 V_i로 위장하여 결제 서비스 등록을 수행할 수 있다. 그러나 TA라 할지라도 δ_{v_i}에 대응되는 차량의 비밀키 s_{v_i}를 탈취하는 것이 계산적으로 불가능함을 ECDLP 문제를 기반으로 증명할 수 있다. A_4를 차량 V_i의 공개키 및 티켓 발급 과정에서 나온 정보들로부터 비밀키 s_{v_i}를 추출할 수 있는 공격자라 가정하며, 증명에 사용된 파라미터들은 4.1.1의 시스템 초기화 과정에 사용된 타원 곡선 파라미터와 동일하다. 이때 효율적인 공격자 A_4가 존재한다면 ECDLP 문제를 해결할 수 있는 챌린저 C가 존재함을 보일 수 있다. A_4는 TA의 역할을 수행하며, 챌린저 C는 차량 V_i의 역할을 수행한다. 먼저 챌린저 C는 (G, rG)를 입력 값으로 받아 $(R_{v_i}=rG, c, d_{TA}, \phi)$를 생성하여 A_4에게 전송한다. 이를 수신한 A_4는 위의 정보들을 기반으로 차량의 비밀키 s_{v_i}을 출력한다. 이에 C는 $r=(s_{v_i}-d_{TA})/\phi$를 계산하여 r을 출력함으로써 ECDLP 문제를 해결할 수 있다. 그러므로 능동적 공격자 A_4는 V_i의 티켓 비밀키를 알 수 없으며, SP2의 인증서 또한 ECQV 인증

서를 사용하므로 수동적 공격자 A_3에 의해서 수행되는 공격 또한 불가능함을 알 수 있다.

위의 공격이 불가능함을 보임으로써 계좌와 연결되어 있는 차량 V_i가 아닌 다른 차량 혹은 장치에서 V_i의 계좌로 결제를 수행할 수 없음을 증명하였다. 또한 증명 값 $GSig_{v_i}(h(h(OI)\|h(PI)))$이 추적성을 만족하므로 무죄 입증성을 제공할 수 있다[27]. 즉, 결제 그룹에 참여한 차량들의 연합 혹은 증명 값으로부터 차량의 신원을 밝힐 수 있는 공격자라 할지라도 해당 증명 값을 생성할 수 없음을 의미한다. 그러므로 차량 V_i는 자신이 의도하지 않은 결제가 발생하였을 때 결제를 승인하지 않았음을 증명할 수 있다.

- **V3 & V4 요구사항(차량 익명성 & 역방향 불연결성)**: 본 요구사항은 거래 내역으로부터 차량을 식별할 수 없으며, 차량이 폐지된 시점 이전에 수행된 거래 내역에 대해서 익명성을 보장해야함을 말한다.

본 논문에서 제안한 결제 프로토콜의 경우 결제 단계에서 차량이 생성한 서명과 $VSReq$에 포함된 AID와 K_{v_i-sp2}는 임의의 차량에 대응시킬 수 있는 정보를 포함하고 있다. SP1이 해당 값을 알고 있을 경우 TID, T_{v_i} 그리고 $price$로부터 $VSReq$를 계산하여 어떤 차량의 결제 요청인지를 알 수 있다. 이에 결제 서비스등록 과정에서 AID와 K_{v_i-sp2}는 V_i와 SP2만이 알 수 있도록 sk_{v_i-sp2}로 암호화되어 전송된다. V1 요구사항에서 보인바와 같이 차량 혹은 SP2의 비밀키를 알고 있어야만 암호화키 sk_{v_i-sp2}를 계산할 수 있으므로 외부에서 해당 값을 탈취할 수 없다. 또한 SP1은 차량 인증과 거래의 적정성만을 판단하며 SP2는 계좌 소유주 인증만을 수행하도록 분리하였다. 이에 SP2는 SP1으로 부터 가격을 제외한 결제와 관련된 어떠한 정보도 수신하지 않으므로 차량 V_i의 계좌 정보와 거래 내역간의 연관성을 알 수 없다. 즉, 임의의 거래에 대해서 어떤 차량이 결제를 수행했는지 알 수 없다.

다음으로 차량 V_i가 부정거래로 시간 t에 폐지되었다 가정해보자. 이때 SP1은 폐지 토큰으로부터 서명을 검증하여 시간 t 이후에 차량 V_i가 수행한 거래 내역들을 확인할 수 있다. 그러나 그룹 서명 기법이 BU-익명성을 만족하므로 $t' > t$를 만족하는 V의 폐지 토큰을 알고 있다 하더라도 시간 t 이전에 차량 V_i로부터 수행된 거래내역들은 식별할 수 없다. 그러므로 제안하는 결제 프로토콜은 본 요구사항을 만족한다.

5.1.2 판매자 및 SP 보안 요구사항 분석

- **R1 요구사항(판매자 자산 보호)**: 본 요구사항은 판매자가 의도하지 않은 결제가 수행될 수 없으며, 해당 거래를 승인하지 않았음을 증명할 수 있어야 함을 말한다. 해당 요구사항을 만족함을 보이기 위해서 판매자와 합의한 금액보다 작은 금액으로 결제를 수행하려는 공격과 판매자로 위장하여 경제적 손실을 입히는 공격을 수행할 수 없음을 증명한다. 또한 판매자만이 결제 요청에 대한 증명 값을 계산할 수 있음을 보인다.
  ① A_5 공격자(결제 금액 변조 공격): 공격자 A_5가 판매자 M과 합의한 결제 금액 $price$가 아닌 이보다 작은 $price'$로 결제를 수행하려 한다. A_5는 기존의 결제 절차와 똑같이 OI를 수신하고 PI를 작성한다. 이때 A_5는 OI의 $price$가 아닌 $price'$을 입력 값으로 $VSReq$를 계산한다. 이후 PI값과 서명값을 M에게 전송한다. 이를 수신한 M과 SP1은 $VSReq$를 검사하지 않으므로 A_5가 $price'$로 결제를 수행하려는 사실을 탐지하지 못한다. 이에 SP1은 A_5와 M의 결제 요청이 유효한 것으로 판단하여 OI에 포함된 $price$와 PI를 SP2에게 전송한다. SP2는 이 값들을 기반으로 $VSReq'$을 생성하고 A_5의 $VSReq$와 비교한다. 이때 $price \neq price'$임으로 $VSReq \neq VSReq'$이다. 즉, SP2는 해당 결제 요청이 잘못되었음을 탐지할 수 있다.
  ② A_6 공격자(판매자 위장 공격): 공격자 A_6는 판매자 M으로 위장하여 의도하지 않은 결제를 수행하려 한다. 차량 A_6는 판매자 M으로 위장하여 의도하지 않은 결제를 수행하는 절차는 다음과 같다. A_6는 실제 물품의 금액보다 낮은 금액으로 $VCReq$를 계산하고 자신의 서명과 M의 서명 $Sig_m(h(h(OI)\|h(PI)))$를 생성

하여 SP1에게 결제를 요청하여 정상적인 결제를 수행할 수 있다. 이때 A_6가 해당 공격을 성공하기 위해서는 M의 결제 요청 승인에 대한 증명 값 $Sig_m(h(h(OI)\|h(PI)))$를 올바르게 생성할 수 있어야 한다. [38]에서 보인바와 같이 ECQV 묵시적 인증서 기반의 ECDSA 서명 기법을 사용하였을 때 존재적 위조가 불가능하므로 해당 서명을 올바르게 생성하기 위해서는 M의 티켓 δ_m에 대한 비밀키 s_m을 알아야만 한다. 이때 δ_m으로부터 s_m을 알아내는 것은 V1 요구사항에서 보인바와 같이 ECDLP 문제와 동치임을 알 수 있다.

해당 요구사항의 증명 과정에서 보인바와 같이 티켓의 비밀키는 판매자만이 알고 있으며 ECQV 기반의 ECDSA 서명 기법은 존재적 위조가 불가능하므로 판매자는 해당 서명 값을 통해 의도하지 않은 결제에 대해 결제를 승인하지 않았음을 증명할 수 있다.

- **V2 & R2 요구사항(결제 승인 응답 & 입금 확인에 대한 응답)**: V2 및 R2 요구사항은 차량과 판매자가 SP2 및 은행으로부터 결제에 필요한 입출금이 완료되었음을 확인할 수 있어야 함을 말한다. 요구사항을 만족하기 위해서 판매자는 SP1이 판매자 은행에 입금 요청을 하지 않고 입금 완료 응답을 판매자에게 전송할 수 없어야 한다. 또한 차량은 SP2에 의해서 생성된 응답 값을 항상 수신해야할 수 있어야 한다.

  판매자는 결제 진행 과정에서 은행으로부터 $Sig_A(Yes/No, h(OI), TID, T_m)$를 수신하여 입금 사실을 확인할 수 있다. 해당 값은 TID와 T_m을 포함하고 있어 SP1에 의한 재전송 공격을 방지할 수 있다. 또한 R2 요구사항에 의해서 서명의 위변조가 불가능함을 확인할 수 있으므로 판매자는 SP1이 입금 요청을 하지 않고 입금 완료 응답 메시지를 전송하였음을 탐지할 수 있다.

  본 논문에서 제안한 결제 프로토콜은 키오스크 모델을 기반으로 설계하였다. 키오스크 모델의 경우 차량이 SP와 직접적으로 통신할 수 없는 환경을 가정하므로 판매자가 차량에 응답메시지를 의도적으로 보내지 않을 수 있다. 이에 차량이 판매자로부터 응답 값을 받지 못한 경우 차량이 RSU를 통해 SP와 통신을 수행할 수 있다. 차량은 RSU를 통해 SP에 해당 거래 관련 정보를 제공하여 응답 메시지를 수신하거나 부정행위를 일으킨 판매자의 폐지를 요청할 수 있다.

- **R3 요구사항(조건부 차량 식별)**: 해당 요구사항은 익명의 차량에 의해서 부정거래가 발생하였을 때, 해당 차량을 식별 할 수 있어야 함을 말한다. 본 논문에서 제안하는 결제 프로토콜의 경우 SP는 결제 완료 후 $VCReq$와 차량 및 판매자의 서명 값을 저장한다. 이후 부정 거래가 발생하였을 때 SP는 T_v, ID_m 그리고 차량의 서명으로부터 차량을 식별할 수 있다. 차량의 신원을 식별하는 절차는 4.1.5절의 차량 ID 식별 및 그룹 개인키 폐지 절차를 따른다.

  본 결제 프로토콜이 해당 요구사항을 만족하기 위해서는 SP에 의해서 식별된 차량의 ID와 서명을 수행한 차량의 ID가 동일해야 한다. 이는 SP가 항상 거래 내역으로부터 차량ID를 식별할 수 있음을 의미하며, 차량의 서명 기법이 추적성을 만족하므로 서명으로부터 차량의 x_i 값을 식별할 수 있는 공격자 혹은 결제 그룹 멤버들의 연합이라도 추적이 불가능한 서명을 만들 수 없음을 알 수 있다. 즉, SP는 항상 거래내역으로부터 실제 차량의 ID를 식별할 수 있다. 또한 4.1.5에서 보

Table 2. Group signature performance comparisons

	$\|\sigma\|$(bits)	Signing	Verification
[31]	1533bit	8ME	6ME+1BM
[14]	1192bit	8ME+2BM	6ME+(3+2|RL|)BM
[26]	2893bit	11ME	7ME+(1+|RL|)BM
[33]	1533bit	8ME	5ME+(1+2|RL|)BM
[10]	852bit	5ME	3ME+(1+2|RL|)BM
Our Scheme	852bit	5ME	3ME+(1+2|RL|)BM

Table 3. Payment protocol performance and requirements comparison

	Computation Cost	Requirement					
		R1	R2	R3	R4	R5	R6
[6]	$14T_{\text{Exp}}+10T_H+8T_{mul}+6T_m$	○	○	X	△	X	X
[17]	$6T_{sym}+4T_H+2T_{MAC}$	X	X	X	△	X	X
[18]	$4T_{sym}+T_H+4T_{EC}$	△	△	X	X	X	X
Our Scheme	$2T_{Ver}+2T_{EC}+T_{MAC}+4T_H$ $+2T_{sym}+5T_{\text{Exp}}$	○	○	○	○	○	○

인바와 같이 RM과 TM의 협업을 통해서 차량의 ID를 밝힐 수 있으므로 단일 기관에서 거래내역으로 부터 차량ID를 식별할 수 없다.

5.2 비교 분석

해당 결제 프로토콜은 효율적인 그룹 서명을 기반으로 위의 요구사항들을 만족한다. Table 2.는 이전의 그룹 서명 기법들과 본 논문에서 제안한 그룹 서명 기법의 서명 길이, 서명 생성 및 검증에 필요한 계산 오버헤드를 비교한 것이다. 다른 기법과 마찬가지로 제안한 기법은 p를 170 비트, G_1의 요소를 171비트 그리고 G_T의 요소가 1020 비트인 MNT 곡선[33]을 사용한다. 여기서 다중 지수 연산과 겹선형 쌍함수를 ME와 BM으로 표기한다. 계산 오버헤드 계산 기준은 [14]와 [31]을 따른다. 표에서 보는바와 같이 제안하는 그룹 서명 기법은 기존의 그룹 서명 기법에 비해 서명 길이가 짧으며 서명 생성 및 검증을 효율적으로 수행할 수 있다. 또한 기존의 기법은 서명자의 신원을 밝히기 위해서 그룹 멤버의 수만큼 비교 연산을 수행해야하나, 제안하는 기법은 지역을 기반으로 그룹을 분리하였으므로 지역 그룹에 포함된 멤버의 수만큼의 비교연산만을 수행하면 된다. 즉, 기존의 기법들보다 효율적으로 서명자의 신원을 밝힐 수 있다.

그룹 서명에 대한 비교를 바탕으로 차량 결제와 관련된 이전 연구들과의 계산 오버헤드 및 요구사항 만족 여부를 비교하면 다음 Table 3.과 같다. 표기법은 [18]을 따르며, T_{Ver}은 서명 검증 시간, T_{MAC}은 MAC 동작 시간을 뜻한다. 여기서 계산 오버헤드는 차량에서 수행되는 세션키 생성 및 결제 수행단계만을 포함하여 계산한다. 표에서 보는바와 같이 제안하는 결제 프로토콜이 기존의 연구들보다 높은 계산 오버헤드를 요구한다. 그러나 기존의 연구들은 익명성을 제공하지 않으며, 결제 프로토콜의 요구사항 또한 만족하지 않는다. [6]의 경우 사전에 SA와의 등록과정에서 발급받은 비밀키와 공개키 쌍으로부터 서명 및 암호화를 수행하지만 공개키와 차량의 신원 ID_P를 대응시킬 수 있다. 또한 [17]의 경우 결제를 수행할 때 결제 참여자와 차량이 사전에 키를 공유했다 가정하고 결제를 수행하는 한계가 존재한다. [18]의 경우 결제 요청 메시지의 위/변조를 탐지하기 위한 서명이 포함되어 있지 않으며, [6] 연구와 마찬가지로 차량의 신원 ID_V가 지속적으로 사용되어 결제 내역으로부터 차량을 추적할 수 있다. 그러므로 본 논문에서 제안한 결제 프로토콜은 익명성을 제공하면서도 효율적으로 결제 서비스를 제공할 수 있음을 알 수 있다.

VI. 결 론

CV에서 차량의 추적을 방지하기 위해서는 안전 관련 서비스 이외에도 결제 서비스와 같은 사용자 편의성 서비스 또한 차량 추적을 방지할 수 있어야 한다. 특히 결제 서비스의 경우 거래 내역으로부터 차량을 추적하기 쉬우며, 이를 통해 안전 관련 서비스에서 사용되었던 메시지도 추적이 가능하다. 이에 본 논문에서 제안한 결제 프로토콜은 차량 익명성을 만족하며, 추적성 및 BU-익명성을 만족하는 그룹 서명을 기반으로 결제 프로토콜을 작성하여 공격자가 거래 내역 혹은 다른 정보들로부터 차량을 추적할 수 없도록 설계하였다. 차량은 TA로부터 티켓과 그룹 개인키를 발급받고 지역 j에서 RM_j로부터 키 업데이트 정보를 수신하여 지역 그룹 개인키를 발급받는다. 또한 거래 요청 메시지에 차량의 고유 특성을 식별할 수 있는 정보들이 포함되어 있지 않아 거래내역

으로부터 차량을 식별할 수 없다. 그리고 단일 기관에서 차량을 추적할 수 없도록 기관의 역할을 분리하였으며 역방향 불연결성을 만족시키는 폐지 토큰을 사용한다. 마지막으로 해당 결제 프로토콜이 3.2절에서 정의한 보안 요구사항들을 만족함을 보였다.

Appendix

본 논문에서 제안하는 그룹 서명 기법에 대한 정의와 추적성과 BU-익명성 정의는 다음과 같다.

정의1. 본 논문의 그룹 서명기법은 다음과 같은 알고리즘으로 구성된다.

▪ $KeyGen(N, T, J)$: 해당 알고리즘은 TA, RRM, TM에 의해 수행되는 확률적 알고리즘으로써, 그룹 맴버 집합의 크기 N, 시간 간격 집합 T, RM 집합의 크기 J를 입력 받아 그룹 공개키 gpk, 그룹 맴버의 그룹 개인키 $\{gsk_1,...,gsk_i,...,gsk_N\}$, RM의 그룹 서명키 $\{rgsk_1,...,rgsk_j,...,rgsk_J\}$를 계산한다. 또한 그룹 맴버와 TA간의 상호 작용을 통해 그룹 맴버의 티켓 $\{\delta_1,...,\delta_i,...,\delta_N\}$을 발급한다.

▪ $Update(gpk, rgpk_j, gsk_i, rgsk_j, \delta_i, j, t)$: 해당 알고리즘은 TA로부터 티켓 δ_i를 발급받은 그룹 맴버 $i \in [1,N]$와 지역 $j \in [1,J]$에 속한 RM_j간의 상호 작용을 통해 시간 $t \in [1,T]$와 지역 j에 유효한 키 업데이트 정보를 맴버 i에게 발급한다. 그룹 맴버 i는 키 업데이트 정보를 통해서 지역 그룹 개인키 $A_i^{j,t}$를 계산한다.

▪ $Sign(gpk, rgpk_j, A_i^{j,t}, j, t, M)$: 해당 알고리즘은 확률적 알고리즘으로 그룹 맴버 i에 의해서 수행되며, $gpk, A_i^{j,t}$ 그리고 $rgpk_j$를 사용하여 지역 j 및 시간 t에 유효한 메시지 M에 대한 서명 σ를 생성한다.

▪ $Verify(gpk, rgpk_j, RL_j, j, t, M, \sigma)$: 검증 알고리즘의 경우 지역 그룹 공개키 $rgpk_j$, 그룹 공개키 gpk, 지역 j에 유효한 폐지 토큰 집합 RL_j 그리고 메시지 M에 대한 서명 σ을 입력 값으로 하며 $valid$ 혹은 $invalid$를 반환한다. $invalid$의 경우 유효하지 않은 서명이거나, 폐지된 그룹 맴버에 의해 생성된 서명의 경우 가능한 결과 값이다.

▪ $Open(gpk, rgpk_j, RL_j, j, t, \sigma)$: 해당 알고리즘은 RM_j와 TM에 의해서 수행된다. 지역 j와 시간 t에 생성된 서명 σ에 대응되는 서명자 i의 ID를 밝혀내고 폐지 토큰 $grt_{i,j,t}$를 생성하여 RL_j에 추가한다. 또한 다른 지역을 관리하는 모든 RM_{j^*}가 RL_{j^*}에 폐지 토큰을 추가할 수 있도록 폐지된 서명자의 ID 값인 x_i를 전송한다. 서명자의 신원을 밝히지 못한 경우 $\perp$를 반환한다.

다음으로 BU-익명성은 역방향 불연결성을 가지는 익명성을 보장하기 위한 요구사항이다. 이때 BU-익명성 게임은 다음과 같이 정의한다.

▪ $Setup$: 챌린저 C는 키 생성 알고리즘과 업데이트 알고리즘을 수행하여 $(gpk, rgpk, rgsk, gsk, ugsk, grt)$를 얻을 수 있으며 공격자 A에게 gpk와 $rgpk$를 전송한다.

▪ $Queries$: C는 모든 시간 간격 $t \in [1,T]$의 시작 부분에서 A에게 t의 시작을 알리며 t 값은 계속해서 증가한다. 그리고 현재 시간 t에 A는 C에게 다음과 같은 쿼리를 할 수 있다.

- $Signing$: A는 임의의 맴버 i와 지역 j 그리고 현재 시간 t에 대해서 임의의 메시지 M에 대한 서명을 C에 요청할 수 있다. C는 해당 쿼리에 대한 응답으로 메시지 M에 대한 서명을 A에게 전송한다.
- $Corruption$: A는 임의의 맴버 i에 대한 비밀키 gsk_i를 요청한다.
- $Revocation$: A는 시간 t와 임의의 지역 j에 대한 맴버 i의 폐지 토큰을 요청하며 C는 이에 대한 응답으로 $grt_{i,j,t}$를 A에 전송한다.

▪ $Challenge$: A는 임의의 i_0와 i_1에 대한 $Corruption$ 쿼리를 요청하지 않았으며, 지역 j에서 시간 t이전에 i_0, i_1에 대한 $Revocation$ 쿼리를 요청하지 않은 경우 (M, i_0, i_1, j_0, t_0)를 출력한다. C는 무작위로 $\Phi \in \{0,1\}$을 선택하고 맴버 i_Φ에 대해서 메시지 M에 대한 서명을 A에게 전송한다.

▪ $Restricted\ Queries$: A는 지역 j와 시간 t 이전에 i_0와 i_1에 대한 $Corruption$ 그리고 $Revocation$ 쿼리를 요청할 수 없다. 이를 제외한 $Signing$, $Corruption$ 그리고 $Revocation$ 쿼리를 요청할 수 있다.

▪ $Output$: 마지막으로 A는 Φ에 대한 추측값 Φ'을 출력한다.

$\Phi = \Phi'$인 경우 A는 BU-익명성 게임에서 승리

한 것으로 간주하며, A의 이점(advantage)을 $|\Pr[\Phi-\Phi']-1/2|$로 정의한다.

정의2(BU-익명성). BU-익명성은 다항 함수 시간에 동작하는 모든 A에 대해서, BU-익명성 게임에 대한 A의 이점이 무시할 정도로 작아야 한다.

추적성 요구사항을 통해 그룹 서명의 위조 불가능성과 무죄 입증성를 제공할 수 있다. 이때 공격자 A와 C의 추적성 게임은 [10, 14, 26, 33]에 정의된 바와 유사하여 본 논문에서는 이에 대한 설명을 생략한다.

정의3(추적성). 추적성은 다항 함수 시간에 동작하는 모든 A에 대해서, 추적성 게임에 대한 A의 이점이 무시할 수 있을 정도로 작아야한다.

다음 정리를 통해서 결제 프로토콜에서 사용된 그룹 서명이 BU-익명성과 추적성을 만족함을 보일 수 있다.

정리1. q_R번의 *Revocation* 쿼리와 q_C번의 *Corruption* 쿼리 이후 제안하는 그룹 서명 기법의 BU-익명성을 이점 ϵ으로 깰 수 있는 공격자 A가 존재한다면, $(1-\frac{q_R|T'|+q_c}{N})\frac{2}{NJT}\epsilon$ 이점으로 G상에서 DLDH 가정을 깰 수 있는 알고리즘 B가 존재한다.

증명) B의 입력값은 $u,v,h\in G$ 및 $a,b,c\in Z_p^*$이며, $Z=h^{a+b}$이거나 $Z=h^c$일 때 (u,v,h,u^a,v^b,Z)라고 하자. 이때 B는 A와의 상호작용을 통해 다음과 같이 Z 값을 결정할 수 있다:

▪ *Setup*: B는 $KeyGen(N,T,J)$를 다음과 같이 시뮬레이션 한다.

① B는 $g_1=u$로 설정하고 $i^*\in[1,N]$, $t^*\in[1,T]$ 그리고 $j^*\in[1,J]$를 선택한다.

② t^*를 제외한 모든 $t\in[1,T]$에 대해서 B는 $r_t\in Z_p^*$를 선택하여 $h_t=g_1^{r_t}$를 계산한다. 그리고 t^*에 대해서는 $h_{t^*}=h$로 설정한다.

③ i^*를 제외한 모든 $i\in[1,N]$에 대해서 B는 $x_i\in Z_p^*$를 선택하고 $A_i=g_1^{\frac{1}{x_i+\gamma}}$를 계산한다. i^*에 대해서는 $x_{i^*}=a$ 그리고 $A_{i^*}=g_1^{\frac{1}{a+\gamma}}$로 설정하며 B는 a 값을 모르기 때문에 해당 값 또한 알지 못한다.

④ $j\in[1,J]$에 대해서 $x_j\in Z_p^*$를 선택하고 $A_j=g_1^{\frac{1}{x_j+\gamma}}$를 계산한다.

⑤ i^*를 제외한 모든 $i\in[1,N]$, j 그리고 t에 대해서 B는 $A_{i,j,t}=A_j^{\frac{1}{(x_j+h(j\|t))(x_i+\gamma)}}$를 계산한다. i^*에 대해서는 $A_{i^*,j,t}=A_j^{\frac{1}{(x_j+h(j\|t))(x_{i^*}+\gamma)}}$로 설정하며 B는 해당 값을 알지 못한다.

⑥ B는 i^*를 제외한 모든 i,t 그리고 j에 대해서 $grt_{i,j,t}=(h_t^{(\gamma+x_i)(x_j+h(j\|t))},h_t^{-x_i})$를 계산한다. 그리고 t^*을 제외한 모든 j와 t에 대해서 i^*에 대한 폐지 토큰을 다음과 같이 계산한다.

$$grt_{i^*,j,t}=(g_1^{r_t(x_{i^*}+\gamma)(x_j+h(j\|t))},g_1^{-x_{i^*}r_t})=(u^{r_t(a+\gamma)(x_j+h(j\|t))},u^{-ar_t}) \quad (11)$$

그리고 i^*,t^* 그리고 모든 j에 대해서 B는 $grt_{i^*,j,t^*}=(h^{(x_{i^*}+\gamma)(x_j+h(j\|t^*))},h^{-x_{i^*}})$로 설정하며 r_{t^*}와 x_{i^*}를 모르기 때문에 해당 값을 알지 못한다.

▪ *Hash*: A는 언제든지 해시 함수 h를 쿼리 할 수 있다. 이에 B는 일관성이 있는 랜덤 값으로 응답한다.

▪ *Phase*1: A는 시간 t와 지역 j에 대해서 *Signing*, *Corruption* 그리고 *Revocation* 쿼리를 요청할 수 있다. $i\neq i^*$인 경우 B는 맴버 i의 비밀키로 부터 쿼리에 대한 응답을 할 수 있다. 만약 $i=i^*$라면 B는 i^*의 비밀키를 알지 못하기 때문에 다음과 같이 응답한다:

· *Signing* Query: B는 다음과 같이 i^*에 대한 그룹 서명을 계산한다:

- $t\neq t^*$인 경우

① 무작위로 $r\in Z_p^*$를 선택한 후 다음과 같이 T_1을 계산한다.

$$T_1=g_1^{\frac{r}{(x_j+h(j\|t))(x_j+\gamma)}g} \quad (12)$$

② 이후 $\alpha=r(a+\gamma)$로 설정하고 T_2 값을 계산한다.

$$T_2 = g_1^{r_t r a} g_1^{r_t r \gamma} g_1^{r_t a} = g_1^{r_t r(a+\gamma)} g_1^{r_t a} = h_t^{(\alpha+a)} \quad (13)$$

③ B는 R_1, R_2를 계산하기 위해 무작위로 $c, s_\alpha, s_{x_{i^*}} \in Z_p^*$를 선택하고 $c = h(M \| j \| t \| T_1 \| T_2 \| R_1 \| R_2)$로 설정한다. 이후 R_1'과 R_2'을 계산하여 메시지 M에 대한 서명 $\sigma = (T_1, T_2, c, s_\alpha, s_{x_{i^*}})$을 응답한다.

- $t = t^*$인 경우

① 리스트 L을 빈 상태로 초기화 한다.

② 리스트 L이 비어있다면 $r \in Z_p^*$와 $T_1 \in G$를 선택하고 $\alpha = r - a$로 설정한다. 그리고 $T_2 = h_{t^*}^r$을 계산하고 L에 (T_1, T_2, r)을 추가한다. 리스트 L이 비어있지 않은 경우, $r' \in Z_p^*$를 선택한 후 $(T_1)^{r'}, (T_2)^{r'}$을 계산하고 리스트 L을 $((T_1)^{r'}, (T_2)^{r'}, rr')$로 업데이트 한다.

③ 이후 $t \neq t^*$인 경우와 같이 메시지 M에 대한 서명 $\sigma = (T_1, T_2, c, s_\alpha, s_{x_{i^*}})$를 생성하여 응답한다.

• *Revocation* 쿼리: $t > t^*$인 경우, B는 $grt_{i^*,j,t}$를 응답한다. 그렇지 않으면, B는 랜덤 추측 값 $w' \in \{0,1\}$과 *abort*를 출력한다.

• *Corruption* 쿼리: B는 랜덤 추측 값 $w' \in \{0,1\}$과 *abort*를 출력한다.

▪ *Challenge*: A는 메시지 M, 현재 시간 t, 지역 j 그리고 *Corruption*이 요청되지 않았으며 시간 t 이전에 *Revocation*을 요청하지 않은 i_0와 i_1을 출력한다. 만약 $t \neq t^*$이거나 $j \neq j^*$인 경우 B는 랜덤 추측 값 $w' \in \{0,1\}$을 출력한다. 그렇지 않으면, B는 $\Phi \in \{0,1\}$을 선택한다. $i_\Phi \neq i^*$라면 B는 랜덤 추측 값 $w' \in \{0,1\}$과 *abort*를 출력한다. $i_\Phi = i^*$인 경우 다음과 같이 응답한다:

① B는 $\alpha = b$와 $T_2 = Z$로 설정한다. 만약 $Z = h^{a+b}$라면, $T_2 = h_{t^*}^{\alpha + x_{i^*}}$이다.

② 이후 B는 *Phase*1과 같은 절차에 따라 메시지 M에 대한 서명 σ를 출력한다.

▪ *Phase*2: 해당 과정은 i_0와 i_1에 대한 *Corruption* 쿼리와 시간 t이전에 *Revocation* 쿼리를 요청할 수 없는 것을 제외하고는 *Phase*1과 동일하다.

▪ *Output*: A는 추측 값 Φ'을 출력한다. $\Phi' = \Phi$인 경우 $w' = 1$을 출력하며 이는 $Z = h^{a+b}$임을 의미한다. $\Phi' \neq \Phi$인 경우는 $w' = 0$을 출력하며 $Z = h^c$임을 의미한다. 변수 $w \in \{0,1\}$가 Z의 상태를 나타낸다고 하자. 만약 $Z = h^{a+b}$라면 $w = 1$이 된다. 이때 B의 이점은 다음과 같다.

$$\begin{aligned} &|\Pr[B(u,v,u^a,v^b,Z=h^{a+b})=1] - \\ &\qquad \Pr[B(u,v,u^a,v^b,Z=h^c)=1]| \\ &= |\Pr[w'=1|w=1] - \Pr[w'=1|w=0]| \\ &= \Pr[\overline{abort}]\epsilon \end{aligned} \quad (14)$$

해당 프로토콜은 *Corruption*, *Revocation* 그리고 *Challenge* 쿼리에서만 *abort*가 발생한다. *abort*가 발생하지 않을 확률은 i^*에 대한 *Corruption* 쿼리를 요청하지 않았거나 시간 t^*와 지역 j^*에 대해서 i^*의 *Revocation* 쿼리를 요청하지 않은 경우 *Challenge*에서 i^*, j^* 그리고 t^*를 선택할 확률과 동일하다. q_C를 *Corruption* 쿼리의 수라하며, q_R은 $T' = \{t_1, t_2, t_3, ..., t^*\} \subseteq T$ 라 할 때, 임의의 시간 t에 요청할 수 있는 *Revocation* 쿼리의 수라고 하자. 이때 i^*에 대해 *Corruption* 그리고 *Revocation* 쿼리를 요청하지 않을 확률은 최소 $(1 - \frac{q_R|T'| + q_c}{N})$이다. 반면에, B가 올바른 t와 j를 추측할 확률은 $1/JT$이며, *Challenge*에서 i^*을 올바르게 추측할 확률은 최소 $2/n$이다. 그러므로 B의 이점은 $Adv_B \geq (1 - \frac{q_R|T'| + q_c}{N}) \frac{2}{NJT} \epsilon$임을 알 수 있다. □

정리2. q_H번의 *Hash* 쿼리와 q_S번의 *Signing* 쿼리 이후 제안하는 그룹 서명 기법의 추적성을 이점 ϵ으로 깰 수 있는 공격자 A가 존재한다면, $\{\epsilon/(n-1) - 1/p\}^2/(16q_H)$ 이점으로 G상에서 $(n+1)$-SDH 가정을 깰 수 있는 알고리즘 B가 존재한다.

증명) 추적성에 대한 증명 과정은 [10, 14, 26, 33]과 유사하므로 본 논문에서는 이를 생략한다.□

References

[1] USDOT, “"what public officials need to know about connected vehicles“ https://www.its.dot.gov/factsheets/pdf/JPO_

PublicOfficials_v6.pdf, May. 2019.
〔2〕 J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons and J. Wang, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," DOT HS 812 014, U.S. Department of Transportation, Aug. 2014.
〔3〕 USDOT, "Connected vehicle basic - Intelligent Transportation Systems" https://www.its.dot.gov/cv_basics/cv_basics_what.htm, May. 2019.
〔4〕 USDOT, "Connected Vehicle Pilot Deployment Program" https://www.its.dot.gov/pilots/index.htm, May. 2019.
〔5〕 K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2377-2396, Jun. 2015.
〔6〕 J.T. Isaac, J.S. Camara, S. Zeadally and J.T. Marquez, "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks," Computer Communications, vol. 31, no. 10, pp. 2478-2484, Mar. 2008.
〔7〕 J.T. Isaac, S. Zeadally and J.S. Cámara, "A lightweight secure mobile payment protocol for vehicular ad-hoc networks (VANETs)," Electronic Commerce Research, vol. 12, no. 1, pp. 97-123, Dec. 2012.
〔8〕 B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn and R. Goudy, "A Security Credential Management System for V2X Communications," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 12, pp. 3850-3871, Dec. 2018.
〔9〕 USDOT, "Security Credential Management System (SCMS)" https://www.its.dot.gov/resources/scms.htm, Jan. 2019.
〔10〕 L. Wei, and J. Liu. "Shorter verifier-local revocation group signature with backward unlinkability," International Conference on Pairing-Based Cryptography, LNCS 6487, pp. 136-146, Dec. 2010.
〔11〕 Y. Sun, Z. Feng , Q. Hu and J. Su. "An efficient distributed key management scheme for group signature based anonymous authentication in VANET," Security and Communication Networks, vol. 5, no. 1, pp. 79-86, Mar. 2012.
〔12〕 X. Lin, X. Sun and P. Ho, "GSIS: A secure and privacy-preserving protocol for vehicular communications," IEEE Transactions on vehicular technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.
〔13〕 J. Zhang, L. MA, W. Su and Y. Wang, "Privacy-preserving authentication based on short group signature in vehicular networks," ISDPE 2007, pp. 138-142, Nov. 2007.
〔14〕 D. Boneh and S. Hovav, "Group signatures with verifier-local revocation," Proceedings of the 11th ACM conference on Computer and communications security, pp. 168-177, Oct. 2004.
〔15〕 D. Huang and S. Misra, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 3, pp. 736-746, Sep. 2011.
〔16〕 N. Saxena, S. Grijalva, V. Chukwuka and A.V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," IEEE Wireless Communications, vol.24, no.4, pp.88-98, Aug. 2017.
〔17〕 J.T. Isaac, S. Zeadally and J.C. Sierra, "Implementation and performance evaluation of a payment protocol for ve

hicular ad hoc networks," Electronic Commerce Research, vol. 10, no. 2, pp. 209-233, Jul. 2010.

[18] W. Li, Q. Wen, Q. Su and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," Computer Communications, vol. 35, no. 2, pp. 188-195, Sep. 2012.

[19] J. Song, F. Yang and L. Wang, "Secure authentication in motion: A novel online payment framework for drive-thru Internet," Future Generation Computer Systems, vol. 76, pp. 146-158, Aug. 2017.

[20] C.L. Chen and W.C. Tsai, "Using a stored-value card to provide an added-value service of payment protocol in VANET," Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 660-665, Jul. 2013.

[21] J. Song, F. Yang, K. Choo, Z. Zhuang, and L. Wang, "SIPF: A secure installment payment framework for drive-thru internet," ACM Transactions on Embedded Computing Systems (TECS), vol. 16, no.2, Jan. 2017.

[22] N. Lu, N. Cheng, N. Zhang, X. Shen, and J.W. Mark, "Connected vehicles: Solutions and challenges," IEEE internet of things journal, vol. 1, no. 4, pp. 289-299, May. 2014.

[23] H. Hasrouny, A.E. Samhat, C. Bassil and A. Laouiti, "VANet security challenges and solutions: A survey," Vehicular Communications, vol. 7, pp. 7-20, Jan. 2017.

[24] E. Ahmed, and H. Gharavi, "Cooperative vehicular networking: A survey," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 3, pp. 996-1014, Mar. 2018.

[25] Z. MacHardy, A. Khan, K. Obana and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," IEEE Communications Surveys & Tutorials, vol. 20, no.3, pp.1858-1877, Aug. 2018.

[26] T. Nakanishi and N. Funabiki, "Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps," ASIACRYPT 2005, LNCS 3788, pp. 533-548, Dec. 2005.

[27] P. Andreas and M. Hansen. "Anonymity, unobservability, and pseudonymity -a proposal for terminology," International workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, pp. 1-9, Mar. 2001.

[28] SECG SEC 4, "Standards for Efficient Cryptography SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme(ECQV)," SECG, Jan. 2013.

[29] T.S. Fun, L.Y. Beng and M.N. Razali, "Review of mobile macro-payments schemes," Journal of Advances in Computer Networks, vol.1, no.4, pp.323-327, Dec. 2013.

[30] J.T. Issac and S. Zeadally, "An Anonymous Secure Payment Protocol in a Payment Gateway Centric Model," Procedia Computer Science, vol. 10, pp. 758-765, Jun. 2012.

[31] D. Boneh, X. Boyen and H. Shacham. "Short group signatures," Annual International Cryptology Conference, CRYPTO 2004, LNCS 3152, pp. 41-55, Aug. 2004.

[32] A. Sudarsono and M.U.H.Al. Rasyid, " An anonymous authentication system in wireless networks using verifier-local revocation group signature scheme, " 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA), Jul. 2016.

[33] T. Nakanishi and N. Funabiki, "A short verifier-local revocation group signature scheme with backward unlinkab

ility," International Workshop on Security(IWSEC) 2006, LNCS 4266, pp. 17-32, Oct. 2006.

[34] M. Bellare, J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E.V. Herreweghen and M. Waidner, "Design, implementation, and deployment of the iKP secure electronic payment system," IEEE Journal on selected areas in communications, vol. 18, no.4, pp. 611-627, Apr. 2000.

[35] J. Petit, F. Schaub, M. Feiri and F. Kargl. "Pseudonym schemes in vehicular networks: A survey," IEEE communications surveys & tutorials, vol. 17, no. 1, pp. 228-255, Aug. 2015.

[36] F. Schaub, Z. Ma and F. Kargl. "Privacy requirements in vehicular communication systems," 2009 International Conference on Computational Science and Engineering, vol. 3, pp. 116-145, Aug. 2009.

[37] C. Cao and X. Zhu, "Strong anonymous mobile payment against curious third-party provider," Electronic Commerce Research, pp. 1-20, Mar. 2018.

[38] D.R. Brown, M.J. Campagna and S.A. Vanstone, "Security of ECQV-Certified ECDSA Against Passive Adversaries," IACR Cryptology ePrint Archive, vol. 2009, pp. 620, Mar. 2011.

〈저자소개〉

정 명 우 (Myungwoo Chung) 학생회원
2017년 2월: 고려대학교 세종캠퍼스 정보수학과 이학사
2017년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 V2X 보안, 결제 프로토콜, 암호학

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2017년~현재: 고려대학교 사이버무기시험평가연구센터(CW-TEC) 부센터장
2004년~현재: 한국정보보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: (사)화이트해커연합 HARU 및 국제해킹대회 SECUINSIDE 설립자 및 이사
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 국방보안연구소 정보보호분야 자문위원
2017년~현재: 여신금융협회 신용카드 단말기 시험 인증위원회 위원
〈관심분야〉 보안공학 및 SDL, 위협 리스크 모델링, 보안성 평가/인증, 암호학, Usable Security