8-2017

HIBS-KSharing: Hierarchical identity-based signature key sharing for automotive

Zhuo WEI
Huawei Shield Lab

Yanjiang YANG
Huawei Shield Lab

Yongdong WU
Institute for InfoComm Research

Jian WENG
Jinan University - China

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1109/ACCESS.2017.2737957

Citation

WEI, Zhuo; YANG, Yanjiang; WU, Yongdong; WENG, Jian; and DENG, Robert H.. HIBS-KSharing: Hierarchical identity-based signature key sharing for automotive. (2017). *IEEE Access*. 5, 16314-16323. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/3786

Published in IEEE Access, 2017 August, Volume 5, Pages 16314-16323
http://doi.org/10.1109/ACCESS.2017.2737957

HIBS-KSharing: Hierarchical Identity-Based Signature Key Sharing for Automotive

ZHUO WEI[1], YANG YANJIANG[1], YONGDONG WU[2], JIAN WENG[3], AND ROBERT H. DENG[4], (Fellow, IEEE)
[1]Huawei Shield Lab, Singapore 117674
[2]Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore 138632
[3]Jinan University, Guangzhou 510632, China
[4]Singapore Management University, Singapore 178902

Corresponding author: Zhuo Wei (phdzwei@gmail.com)

This work was supported in part by the National Natural Science Funds of China under Grant No. 61402199, U1636209, 61472165, and 61373158, by the Nature Science Funds of Guangdong under Grant 2015A030310017, by the Guangdong Provincial Engineering Technology Research Center on Network Security Detection and Defence under Grant No. 2014B090904067, by the Guangdong Provincial Special Funds for Applied Technology Research and Development and Transformation of Important Scientific and Technological Achieve under Grant No. 2016B010124009, by the Zhuhai Top Discipline–Information Security, and Guangzhou Key Laboratory of Data Security and Privacy Preserving, Guangdong Key Laboratory of Data Security and Privacy Preserving.

ABSTRACT Equipped with various sensors and intelligent systems, modern cars turn into entities with connectivity, autonomy, and safety. Car rental/car sharing is an innovative transportation concept and integral in today's urban living. It enables users to access a fleet of vehicles located throughout cities. Complementing public transportation, the car-sharing service helps people to meet their transportation needs economically and in an environmentally responsible manner. When a customer wants to rent a car from a rental company or an owner wants to share a private car with his/her friends or family members, the customer or the user should gain admission to the car, such as unlocking the door and starting the engine. In this paper, we proposed a novel and secure key-sharing system named hierarchical identity-based signature key sharing (HIBS-KSharing), which consists of key generation, key transmission, and key management (e.g., remote issuing, revocation of access rights, and their delegation to other users or sharers). We implemented our proposed system based on Nexus smartphones and near-field communication devices. Compared with existing key-sharing schemes of car rental/sharing, our proposed HIBS-KSharing system is secure and easily extended.

INDEX TERMS Car sharing, identify based signature, automotive cyber security, NFC communication, electronic key.

I. INTRODUCTION

Car rental and car sharing [1], [2] are an innovative transportation concept and popular in today's urban living. They allow the users to have the freedom of accessing a fleet of vehicles located throughout cities. In Europe, car sharing or rental players consists of DriveNow [3], Car2Go [4], Flinkster, Autolib, CarUnity and Tamyca. Players in North America include DriveNow, Zipca [5], Turo (formerly RelayRides [6]), and so on. In Asia-Pacific, there are Orix and Park24 in Japan, as well as PPzuche and EVCard in China. Cars may be available at fixed stations which are dedicated parking spots located around a city, or on a free-floating basis, which allows users to park their vehicle at any legal spot, where it awaits the next user.

In Singapore, Car Club [7] was established as the go-to car rental service for the everyday users. Easily accessible through a vast interconnected network of hubs across the island, Car Club features a fleet of cars that caters to the driving needs of the heart lander. Singapore will launch an electric vehicle (EV) car-sharing programme in collaboration with Bollor Group by mid-2017, named BlueSG [8]. EVs will be deployed in every single Housing & Development Board (HDB) town by 2020, to allow as many residents as possible to enjoy car-sharing facilities.

Passing physical key to a guest user is a traditional way of key sharing, which is inconvenient and low efficient. Personal smartphone is a good alternate choice due to its pervasiveness, connectivity and equipment with multiple communication interfaces (e.g., GSM, WiFi, Bluetooth, and NFC). Smartphone-based E-Key sharing is a desirable and trending solution for car sharing and rental. The Car Connectivity Consortium (CCC), an organization driving global technologies for phone-centric car connectivity solutions, announced the publication of a white paper outlining the standard based solution for using smart derives as key for cars, which described how existing standard technologies, such as Global Platform, GSMA, Bluetooth, and NFC can be used to define a standard for using smart devices as digital keys for cars.

With the cellular connection, the smartcar could connect and communicate with the remote cloud server and smartphone Apps, e.g., remote management and diagnosis, the guest user utilizes cellular network to obtain a digital key and controls a rental or sharing car. That is, the guest user utilizes his/her smartphone to send commands to cloud server, the cloud server verifies the guest identity and message integrity (e.g., unlocking/locking door), and forwards them to the rental or sharing car. The Easycar Club and Car Club exploit above architecture and system; however, communication may be delay or disconnection sometime due to unstable network of urban area. Another solution is Bluetooth-based system. Owner generates and delivers E-Key to a guest user with cellular network, then the guest's smartphone communicates with car by using Bluetooth protocol. As the car verifies the legitimacy of E-Key, then the guest user is authorized to use smartphone app to control the car. For example, Volvo just takes use of this Bluetooth-based architecture to make car sharing easy among multiple owners. However, Bluetooth-based key sharing system has following two shortcomings. One is that pairing time may be variable or unacceptable, and the other is that it is hard to correctly calculate and control the distance of automatic pairing, such as obstacle objects. It is possible that DoS or relay attack happens between car and smartphone. The third solution is WiFi-based solution, which is similar to Bluetooth. Smartphone connects to Car's WiFi hotspot and completes identity verification and message transmission. However, WiFi-based solution belongs to short range communication and has several problems, e.g., DOS attacks, relay attacks and serious energy cost. The last solution is NFC-based solution. A guest wipes his smartphone NFC device over car's NFC interface, transmitting verification information and commands. For example, BMW and DriveNow car sharing service advocate NFC communications technology to achieve car access control, car rental and sharing services [9]. It has several advantages, e.g., efficiency and independence from networks. However, key sharing system of existing NFC-based solutions are not secure and difficult to management. For each transmission session, if it uses symmetric key algorithm, it had to generate a new session key; if it uses public key algorithm, it has to deal with cumbersome PKI.

In this paper, we proposed a key sharing system for car rental/sharing services based on hierarchical identity-based signature, named HIBS-KSharing. The proposed system can not only be employed by car rental services of companies, but also be suitable for car sharing of owners of private cars. Guest users' E-keys can be remotely issued, revoked, delegated by companies or owners, then they utilize their smartphones to access cars with NFC communication protocol. In addition, authorized guest users may permit their friends or family members to use the rented or shared cars after they further generate a new heretical IBS key for their friends or family members. The proposed heretical key sharing architecture which consists of root and leafs roles could be flexible for reality requirements. We implemented our proposed system under Android smartphone and NFC devices. Compared with existing key sharing systems, proposed HIBS-KSharing scheme is secure and easily extended.

Our contributions of this paper are as following:

- NFC-based key sharing architecture. Proposed architecture takes use of NFC protocol to achieve the communication between smartphone and car. NFC communication depends on physical touch in order to guarantee the valid information or data transmission.
- HIBS-KSharing system. Proposed system is suitable for current business models and ecosystems of car sharing and car rental. Hierarchical key sharing operation is conveniences such that it is easily adopted by users (e.g., company or owner).
- Secure IBC-based protocol. Proposed identity-based cryptography is secure and lightweight, which satisfies security and real time requirements.
- HIBS-KSharing system implementation. We implemented proposed system on Android smartphone and NFC devices, including protocol designing of cryptography and NFC, and source code development of server and client Apps.

Remaining of the paper is organizes as following. Section II summaries previous key sharing systems of car sharing and rental. Section III describes the secure HIBS-KSharing system, i.e., key generation, sharing, revocation and delegation. Section IV gives the experiment implementation. Section V are security analysis, performance evaluation and comparison. The last Section VI draws a conclusion and future works.

II. RELATED WORKS

For future connected cars, most of car manufactories realized the huge potential market of car sharing or rental, including locking/unlocking/starting a car, provisioning of keys, sharing of keys, etc. The main players are General Motors, Volkswagen, Daimler, RealVNC, HTC, PSA, Honda, LG Electronics, Hyundai, Alpine, Toyota. In this section, we will survey existing digital key sharing schemes of car sharing and rental systems, i.e., digital key/smartlocker [10] but not physical key, and explain signature-based encryption and authentication, respectively.

A. KEY SHARING

Authors in [11] proposed a key sharing scheme for vehicles. They created an innovative vehicle sharing system for electric vehicles, which can easily be accessed by users with little required infrastructure and few intermediaries. NFC-based communication system is also used by car immobilizer. For example, Bauer *et al.* [12] proposed the security framework for secure authorization system, which uses public key technology to implement delegation of access rights, and the system is communicated over Bluetooth. Timpner *et al.* [13] presented a smartphone-based registration and key deployment system for Vehicle-to-Cloud communications. The proposed system addresses how drivers can securely register their vehicle with cloud services and deploy keys for securing vehicular communications. The work by Han *et al.* [14] presented vehicle-to-mobile pairing protocols, based on various out-of-band channels such as sound, light, and its assumption is that the vehicle and the mobile phone to be paired do not pre-share any secrets. The work most related to this invention is [15], which also focuses on car sharing and delegation of access rights. It assumes a trusted server to issue keys for vehicle access to car owners. In addition, to avoid registering a car owners authentication key to the car owners vehicle, a token containing the key (the token can be understood to be a sealed e-envelope) is also issued and the token can only be decrypted by the vehicle. In vehicle accessing, authentication data generated by using the authentication key together with the token is sent to the vehicle, which then decrypts the token to get the authentication key, and in turn uses the key to check against the authentication data. Groza *et al.* [16] explored the design and implementation options for a protocol that can be deployed in a car-sharing scenario where multiple users can share or gain access rights to the same vehicle. Due to inherent constraints of platform, they keep the protocol simple and rely on inexpensive symmetric key primitives while still providing advanced options, e.g., rights sharing capabilities. Mark Elkins of TrustPoint Innovation Technologies in [17] proposed a peer-to-peer approach to digital key sharing for vehicle access control. It depends on PKI architecture to generate public and private keys, and smartphone and vehicle take use of NFC or Bluetooth protocol to verify each other.

B. IDENTIFY-BASED CRYPTOGRAPHY POLICY

Identify-based cryptography was firstly designed by Shamir [18] in 1984. Identify-based cryptography schemes are within the class of asymmetric key based cryptography. Instead of generating and using a random public/private key pairs in a public key cryptosystem such as RSA which is one of the first practical public-key cryptosystems and is widely used for secure data transmission. It conceived the option of utilizing a user's name or his network address as a public key, with the corresponding private component being generated by a trusted key generation centre, called Private Key Generator (PKG). In fact, any type of identifier, e.g., telephone number, address, email, and so on, can be used, so as it can uniquely identify the user and it readily available to the party that uses it.

The identity-based public key cryptosystem is an alternate for certificate-based PKI, particularly once economical key management and moderate security are needed. Compared to ancient PKI, it saves storage and transmission of public keys and certificates that is very enticing for devices forming MANETs. For a protracted time once Shamir revealed his plan, the event on IBC was terribly slow. The construction of an identity-based encryption (IBE) scheme was left as an open problem. Since then, there were numerous attempts to realise Shamirs vision of identity-based encryption, such as those in [19]–[24]. However, none of these proposals were fully satisfactory. Either they did not provide adequate security or they were not feasible to implement in practical environments. Meanwhile, there were further proposals for IBS schemes in [25] and [26], also based on the RSA primitive. Only in 2000, Joux [27] showed that Weil pairing is used for good by mistreatment it during a protocol to construct multilateral one-round Diffie-Hellman key agreement. This was one in all the breakthroughs in key agreement protocols. After this, Boneh and Franklin [28] conferred at Crypto 2001 Associate in Nursing identity-based secret writing theme supported properties of linear pairings on elliptic curves, which is the first absolutely useful, economical and incontrovertibly secure identity-based secret writing theme.

III. SECURE HIBS-KSHARING SYSTEM

In this section, we will give a detail description of HIBS-KSharing system. The proposed system can not only be exploited by company of car sharing and rental, but also be accepted by owner of private car.

A. SECURE ARCHITECTURE

Figure 1 illustrates the architecture of proposed HIBS-KSharing system. It consists fours components: *KGC* (Key Generation Center) belonging to OEM, *UMC* (User Management Center) belonging to the third cloud platform, *KMM* (Key Management Module) of car's on-board system and *SCM* (Secure Communication Module) of smartphone apps. There are different layers of users under the HIBS-KSharing system. The first layer is owners of private car and companies of car sharing/rental; the second layer is family member (or friend) of owner of private car and customers of car sharing/rental. Under this kind of architecture, company (owner) and car can communicate information and data through *KGC*, company (owner) and customer (user) can transfer key and information through *UMC*, and customer (owner, user) can unlock/lock car with NFC communication. We will introduce two services, respectively.

B. SERVICE OF CAR SHARING/RENTAL

Assume that a car sharing/rental company is $\mathcal{C}$, a customer is u and a car is c. Each entity has an unique identity, $ID_{\mathcal{C}}$, ID_u, and ID_c, respectively. *KGC* of OEM has a pair of master public key *mpk* and master private key *msk* for an identity-based signature scheme. For $\mathcal{C}$, *KGC* generates a private key $sk_{\mathcal{C}}$ using *msk* based on $ID_{\mathcal{C}}$ (see subsection III-E). Then, *KGC* delivers $sk_{\mathcal{C}}$ to $\mathcal{C}$ in a secure manner; also, *KGC* is responsible for installing $ID_{\mathcal{C}}$ into all cars bought by $\mathcal{C}$.

When a customer u wants to rent a car c from the company $\mathcal{C}$, the latter will generate a private key sk_u based on ID_u as well as ID_c with the use of $sk_{\mathcal{C}}$. sk_u will be delivered to u securely via *UMC*, and *KGC* also passes ID_u to the car c

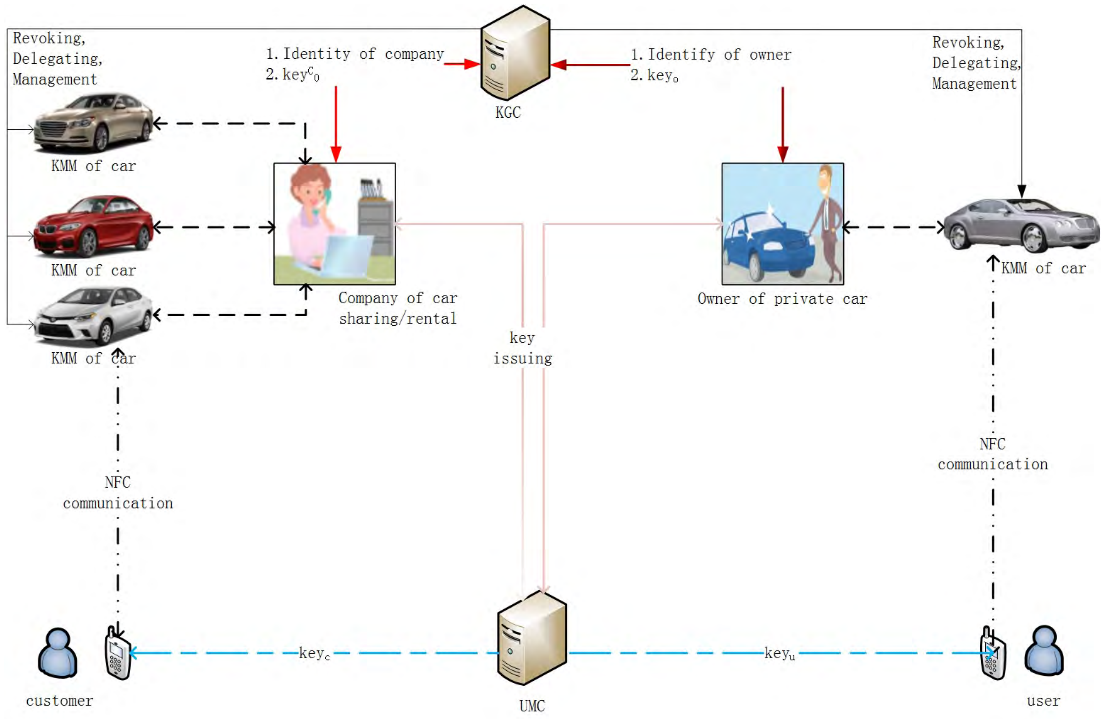


FIGURE 1. Architecture of HIBS-KSharing system.

who keeps a white name list containing all valid users for that particular car.

C. SERVICE OF PRIVATE CAR

Another service is about sharing of private car to family members or friends, that is, the car owner remotely issues a digital key to a user (e.g., family members or friends), then the user could access private car with his smartphone. Assume owner, user, and car are O, u and c, respectively.

When an owner O firstly purchases his car c, KGC of OEM generates a private key sk_O for the car owner based on the owner's identity ID_O with the master key msk. Then, sk_O is delivered to the smartphone of owner O securely, and ID_O is installed into KMM of car's on-board system. As last, the car owner can unlock/lock the car c with his smartphone Apps under the proposed NFC-based authentication and authorization protocols.

Similar to the owner O, a user u should also be firstly required to register his identity and driver licence to UMC in order to get a valid account/id ID_u from UMC. Once the user obtains his ID_u, u can apply an digital sharing key from the car owner O. By using owner's private key sk_O and the user's identity ID_u, O generates the user key sk_u for u with smartphone Apps, and sends sk_u to UMC which will forward the key to u in a secure manner (see subsubsection III-D). On the other hand, KGC offers an interface to O, allowing O to manage authorization and revocation configuration on the car c. Specifically, O sends and updates ID_u to car c through KGC in order to add an entry for u in its white name list. Besides ID_u, other authorization information, such as parameter $\mathbb{P}$ (authorized time duration or permitted functions), will be also stored and managed at both KGC and c.

D. SECURE CHANNELS

In this proposed HIBS-KSharing architecture, there are two segments of secure communication channels, i.e., the secure channel between KGC and one company/owner, and the secure channel among UMC, one company/owner, and authorized users.

1) SECURE CHANNEL BETWEEN *KGC* AND COMPANY/OWNER

This channel is mainly used for KGC to securely deliver private keys to a car owner or a car sharing/rental company when they purchase cars. The security of the channel can be established with credential mode. For example, a password (generated by the OEM, and thus known to KGC) is sealed and given to the car buyer, i.e., company or private owner. The car buyer (an owner or company) can authenticate to KGC with sharing password, and the two sides further negotiate a secret session key between them by running a password authenticated key exchange protocol.

2) SECURE CHANNEL AMONG UMC, COMPANY/OWNER, AND AUTHORIZED USERS

UMC essentially acts as an App server. It is logically a separate entity from KGC, but in effect it can be managed by OEM as well. As such, the secure channel between UMC and company/owner can be established with the same mechanism as used between KGC and company/owner. This segment of secure channel is used by the company/owner to send private keys of authorized users to UMC which manages users' keys (such as delegation or revocation).

When a user u wants to rent a public car from a rental company or borrows a private car from a car owner, the user need download and install client App on his/her smartphone, then submits his/her legal informations (such as, citizen ID, license or biometric data) to UMC in order to complete user registration. The registration of UMC will help u to create a private password. As a result, the secure channel between UMC and u can be established with the two executing a password authenticated key exchange protocol, which helps to guarantee the secure transmission of the private key generated by the rental company or the car owner.

E. KEY GENERATION AND SHARING

Proposed HIBS-KSharing gives a concrete of hierarchical identity-based signature scheme to achieve the key sharing. For simplicity, it assumes that the architecture consists of three levels of entities. That is, the top level is KGC, the second level is car owner O or rental company C, and the lowest level is users u. We prefers HIBS-KSharing to be implemented over elliptic curves for better performance.

Let G be a cyclic group with prime order q, and g be a generator of G. Let $H(.)$ denote a cryptographic hash function. The master public key and master private key possessed by KGC is $mpk = g^x$ and $msk = x \in_R Z_q^*$, respectively.

1) GENERATION OF sk_O

In order to generate a private key sk_O for a car owner O, KGC selects a random number $r \in_R Z_q^*$, and computes $R = g^r$ and $s \equiv r + x.H(R, ID_O, car\ info) \pmod{q}$, where ID_O is the identity of the car owner, and $car\ info$ may contain information on the car, such as OEM brand, purchased date, vehicle identification number (VIN) , and so on. The private key of owner O is thus $sk_O = (R, s)$. Note that $(g^s = R.y^{H(R,ID_O,car\ info)}, s)$ constitutes a public/private key pair for ElGamal-type digital signature schemes, so that any digital signature schemes, e.g., Schnorr Signature, can be employed to issue signatures.

2) GENERATION OF sk_u

In order to generate a private key sk_u for a registered and authorized user. Car owner O initially selects a random number $r' \in_R Z_q^*$, and computes $R' = g^{r'}$ and $s' \equiv r' + s.H(R', ID_O, ID_u, ID_c, \mathbb{P}) \pmod{q}$, where ID_O, ID_u, ID_c are the identities of the car owner, the user and the car, respectively; $\mathbb{P}$ denotes the authorization policy containing information, such as authorization duration and place. Note that $(g^{s'} = R'.(R.y^{H(R,ID_O,car\ info)})^{H(R',ID_O,ID_u,ID_c,\mathbb{P})}, s')$ is a public/private key pair for ElGamal-type digital signature schemes.

F. KEY REVOCATION

For the rental/sharing car c, it assumes that a trust storage is installed, e.g., Trustzone, TMP (Trusted Platform Module) or secure element chip. The secure storage of car c maintains a white name list, which manages the identities (ID) of users, and stores information of the owner O and other authorized users u. In order to revoke an authorized user, it simply concerns that the owner O deletes the entry corresponding to that particular user from the car's white name list. Specifically, the owner O sends an revocation requirement of the user's key to KGC which also maintains white name list. KGC further forwards the revocation command to the car c whose KMM will delete the user identify and information (e.g., authorization policy) from trust storage.

G. AUTHENTICATION AND AUTHORIZATION PROTOCOL

The owner O or an authorized user u unlocks or locks the car door by running an authentication and authorization protocol with the car c. The communication protocol consists of three steps as follows.

1) FOR OWNER O

Step 1: The owner O sends $ID_O, car\ info$ to the car c to initiate the protocol.

Step 2: In response, the car c replies a random challenge $chal$.

Step 3: The owner O generates a signature $Sig(sk_O, chal)$ on $chal$ using sk_O and then returns $Sig(sk_O, chal)$ to c. Upon receipt of the message, the car c verifies the signature, and unlocks or locks the car door if the signature is valid, otherwise, c denies the owner or user's requirement if the signature is not valid.

2) FOR AUTHORIZED USER u

Step 1: The user u sends $ID_O, car\ info, ID_u, \mathbb{P}$ to the car c to initiate the protocol.

Step 2: In response, the car c replies a random challenge $chal$.

Step 3: The user u generates a signature $Sig(sk_u, chal)$ on $chal$ using sk_u, and then returns $Sig(sk_u, chal)$ to the car c. Upon receipt of the message, the car c verifies the signature, and unlocks or locks the car door if the signature is valid, otherwise, c denies the owner or user's requirement if the signature is not valid.

IV. IMPLEMENTATION

Our simulation experimental environment consists of the interface of NFC, the server, and the client (App of smartphone). Specifically, NFC chip acts as the interface between the server and the client; the server refers to the car KMM as a locker controller module; the client (App of smartphone) plays the interface of authorized user. The server and client communicate and verify identities between each other with the technology of Near Field Communication (NFC) protocol. We will describe the implementation of the proposed system with smartphones and NFC devices as following.

A. NFC, OPEN LIBRARY, AND PROTOCOL

Since the proposed HIBS-KSharing system takes use of NFC chips as communication channel, we will explain NFC itself, two open important libraries and one communication protocol of NFC.

1) NFC

Near Field Communication (NFC) is an open platform technology that provides wireless communication between devices that are compatible with the ISO/IEC 18092 [29] and ISO/IEC 21481 [30] standards. It was proposed as a unifying successor for the available RFID technologies. The NFC standard wraps older RFID modulations like the ISO/IEC 14443 [31], ISO/IEC 15693 [32] and JIS X 6319-4 [33]. There are a number of devices compatible with NFC technology like GSM phones and other peripheral computer equipments. NFC consists of two working modes. Firstly, it acts on reader/writer, a reader feeds, via an electromagnetic field at the 13,56 MHz frequency, a card including an antenna and a low power consumption secure microcontroller. Secondly, it works with Peer to Peer (P2P), i.e., two devices (the Initiator and the Target) exchange packets over a 13,56 MHz radio link. Both devices could manage their own energy resources in the active mode, or the Target is fed by the Initiator in the passive mode.

2) LIBNFC

Open-source Libnfc is a software package that works with most commercially-available NFC readers, which is the first libre low level NFC SDK and Programmers API released under the GNU Lesser General Public License.

3) SNEP COMMUNICATION PROTOCOL

The Simple NFC Data Exchange Format (NDEF) Exchange Protocol (SNEP) is a request or response protocol. A SNEP client sends a request to a SNEP server, the request contains following elements, e.g., protocol version, request method, the length of an information field in octets, and information field. The purpose of the Simple NDEF Exchange Protocol is to exchange NDEF messages. NDEF messages are transmitted in the information field of SNEP request or response messages. Figure 2 illustrates the SNEP Communication Model.

4) LIBLLCP

Libllcp is an implementation of NFC Logical Link Control Protocol (LLCP) for libnfc. It is secures P2P sessions due to the well-known TLS/SSL protocol. LLCP and TLS associated with a set of rules build the LLCPS protocol. SNEP service is over LLCPS, which is used for access control. When the user taps his NFC "card" against an NFC "device", a TLS session is opened over the P2P connection. Thereafter NDEF content is pushed over SNEP.

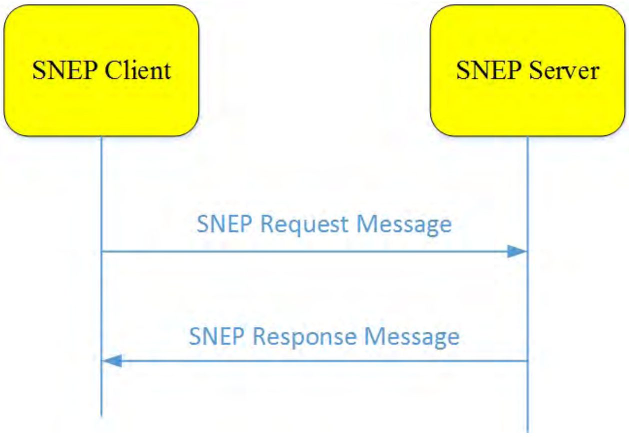


FIGURE 2. SNEP communication model.

B. HARDWARE

1) SERVER PLATFORM

The NFC device of server consists of three components, i.e., antenna matching circuit, central processing unit (PN532) and serial port communication. PN532 is a highly integrated transceiver module for contactless communication at 13.56 MHZ based on the 80C51 microcontroller core. It supports six different operating modes. The proposed system adopts ISO/IEC 18092, ECMA 340 Peer-to-Peer operating mode, and can be connected to an external antenna for data exchange with the client by PN532 transceiver. Finally, the server transmits information with the control system of car by High Speed UART (HSU). In this paper, we take use of a laptop to simulate the system of car. Figure 3 illustrates the server platform and process.

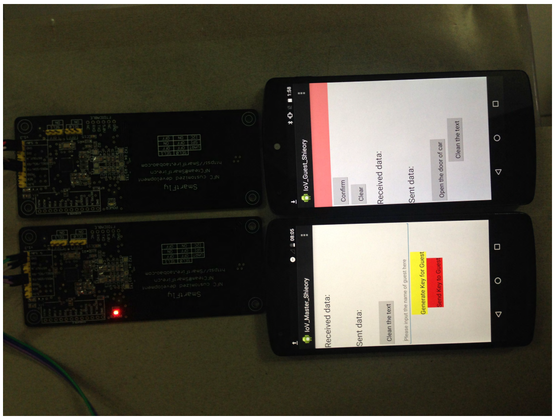
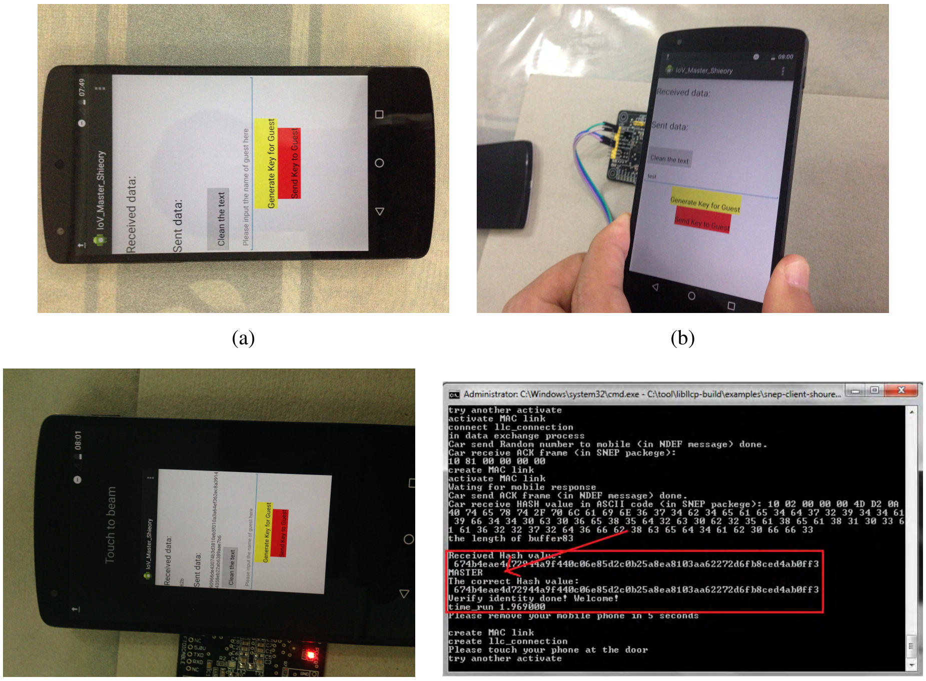


FIGURE 3. Server simulation.

2) CLIENT

In experimental simulation environment, any kind of smartphones with a NFC sensor can be adopted to act as a client. We chose one NEXUS 5 (with a NFC sensor) running Android 6.0.1 and another NEXUS 5 running Android 4.4.4 to verify proposed HIBS-KSharing system. Android 4.0 and above support a P2P application named "Android Beam", based on the SNEP (Simple NDEF Exchange Protocol).



(a)

(b)

(c)

(d)

```
Administrator: C:\Windows\system32\cmd.exe - C:\tool\libllcp-build\examples\snep-client-shoure...
try another activate
activate MAC link
connect llc_connection
in data exchange process
Car send Random number to mobile (in NDEF message) done.
Car receive ACK frame (in SNEP packege):
10 81 00 00 00 00
create MAC link
activate MAC link
Wating for mobile response
Car send ACK frame (in NDEF message) done.
Car receive HASH value in ASCII code (in SNEP packege): 10 02 00 00 00 4D D2 0A
40 74 65 78 74 2F 70 6C 61 69 6E 36 37 34 62 34 65 61 65 34 64 37 32 39 34 34 61
 39 66 34 34 30 63 30 36 65 38 35 64 32 63 30 62 32 35 61 38 65 61 38 31 30 33 6
1 61 36 32 32 37 32 64 36 66 62 38 63 65 64 34 61 62 30 66 66 33
the length of buffer83

Received Hash value:
 674b4eae4d72944a9f440c06e85d2c0b25a8ea8103aa62272d6fb8ced4ab0ff3
MASTER
The correct Hash value:
 674b4eae4d72944a9f440c06e85d2c0b25a8ea8103aa62272d6fb8ced4ab0ff3
Verify identity done! Welcome!
time_run 1.969000
Please remove your mobile phone in 5 seconds

create MAC link
create llc_connection
Please touch your phone at the door
try another activate
```

FIGURE 4. Owner demo. (a) Master interface. (b) Put master smartphone close to NFC device. (c) Client: Communication between owner smartphone and NFC device. (d) Server: Communication between owner smartphone and NFC device.

C. SOFTWARE

Both server and client are made of four software layers. The first layer is MAC layer, i.e., NFC controller chip provides radio framing and MAC facilities, which are specified by the NFCIP-1 standard. The second layer is the LLCP layer, which manages P2P sessions. The third layer is a TLS layer, which utilizes the well-known OPENSSL library on the Initiator side, and runs in a secure element on the Target side. The last layer is a SNEP layer, which provides a communication service for the Initiator and the Target.

After some necessary initiations with libnfc and libllcp, the server will create an MAC link (MAC and LLCP layers) in order to wait for communicating requirement from an approached client. Upon creating NFC channel (TLS layer), the server opens a secure channel to send a frame with NFC Data Exchange Format (NDEF) to the client according to Simple NDEF Exchange Protocol. Because the NDEF is a general standard data exchange format in NFC, which was defined by NFC Forum. Hence, the client can receive and parse the data under NFC protocol. At last, the client and server send challenges and verify each other. Figure 4 and Figure 5 illustrate the demonstrations of the owner and user.

V. EVALUATION AND ANALYSIS

A. SECURITY ANALYSIS

The above hierarchical identity-based signature scheme is an extension of the identity-based signature scheme from ISO/IEC 29192-4 standards, which has been proven secure in the random oracle model. In the same way, the security of proposed hierarchical identity-based signature scheme can be proven in the random oracle model as well.

The above authentication and authorization protocol is a simple challenge-response signature based entity authentication protocol whose security has been well studied. On the premise of the security of the hierarchical identity-based signature scheme, security of the authentication and authorization protocol is easily derived.

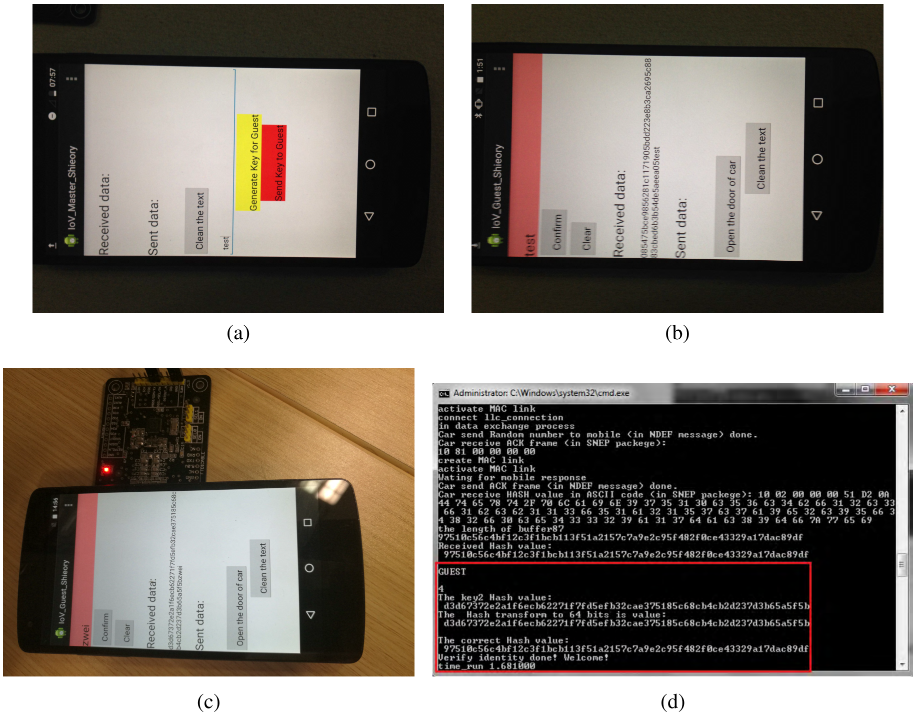
TABLE 1. Time consuming.

Operation	Transferring	Signature of client	Verification of server
time (ms)	440	0.54	136

B. PERFORMANCE EVALUATION

In this subsection, we will present the performance measurements for the authentication protocols.

Under experimental simulation environment, we calculate the time cost and communication cost for proposed HIBS-KSharing system. Time cost includes transferring time, signature time, and verifying time as shown in Table I. Transferring time cost is average 440 ms for each route (including of initiation, connection/pairing, sending requirements and receiving data). Verifying time considers both smartphone and car sides. The signature time under Android Nexus 5 is about 0.54 ms, while the verification time under car side is about 1.36 ms. Hence, the total time cost of NFC-based unlock/lock is no more 1 second, which is efficient and real



```
activate MAC link
connect llc_connection
in data exchange process
Car send Random number to mobile (in NDEF message) done.
Car receive ACK frame (in SNEP packege):
10 81 00 00 00 00
create MAC link
activate MAC link
Wating for mobile response
Car send ACK frame (in NDEF message) done.
Car receive HASH value in ASCII code (in SNEP packege): 10 02 00 00 00 51 D2 0A
44 74 65 78 74 2F 70 6C 61 69 6E 39 37 35 31 30 63 35 36 63 34 62 66 31 32 63 33
 66 31 62 63 62 31 31 33 66 35 31 61 32 31 35 37 63 37 61 39 65 32 63 39 35 66 3
4 38 32 66 30 63 65 34 33 33 32 39 61 31 37 64 61 63 38 39 64 66 7A 77 65 69
the length of buffer87
97510c56c4bf12c3f1bcb113f51a2157c7a9e2c95f482f0ce43329a17dac89df
Received Hash value:
 97510c56c4bf12c3f1bcb113f51a2157c7a9e2c95f482f0ce43329a17dac89df
GUEST

4
The key2 Hash value:
 d3d67372e2a1f6ecb62271f7fd5efb32cae375185c68cb4cb2d237d3b65a5f5b
The  Hash transform to 64 bits is value:
 d3d67372e2a1f6ecb62271f7fd5efb32cae375185c68cb4cb2d237d3b65a5f5b

The correct Hash value:
 97510c56c4bf12c3f1bcb113f51a2157c7a9e2c95f482f0ce43329a17dac89df
Verify identity done! Welcome!
time_run 1.681000
```

FIGURE 5. **Guest demo. (a) Master set key for guest. (b) Guest smartphone collects key by NFC protocol. (c) Client: Communication between guest smartphone and NFC device. (d) Server: Communication between guest smartphone and NFC device.**

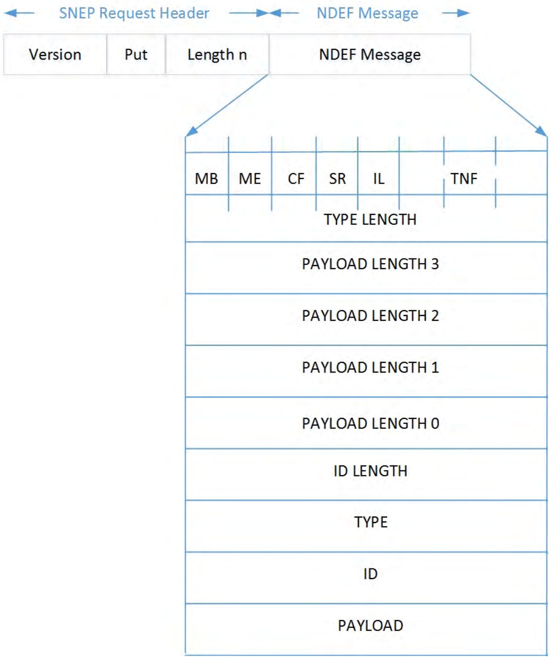


FIGURE 6. **SNEP header and NDEF package.**

time.

The communication cost is the payload of SNEP package which contains SNEP header and NDEF payload as shown in Figure 6. Table 2 illustrates the SNEP format. SNEP header is 6 bytes, while NDEF consist 9 bytes header and various payload, such as 32 bytes of hash value. Hence, the maximum communication overhead is about 47 bytes for our SNEP package.

TABLE 2. **Communication overhead.**

Element	SNEP header	NDEF header	NDEF payload
size (byte)	6	9	32

C. COMPARISON

In this subsection, we give the comparison between proposed system with existing systems. Compared with existing vehicle-sharing systems which take use of smartphones but depend on the third parties to delegate and revoke keys. For example, Enjoy[1] and Car Club [7] are the systems which do not require a membership card to access vehicles. Smartphone Apps control the vehicle with a central sever with following steps. Firstly, commands send by the client are processed by central server, then central server will forward above commands to the sharing vehicles. However, delay may happen due to worse network conditions, which cannot satisfy real time requirements of lock/unlock door.

Compared with the electronic vehicle access system in [15]. Firstly, the authentication keys of all the car owners are issued by or known to a trusted third party server, while proposed HIBS-KSharing system suggests that cars independently generate their own secret keys and in turn the

[1] enjoy.enti.com

corresponding car owners authentication keys. The benefit is that the car owner controls all secret keys associated with his/her car. In addition, even if a car is compromised and the secret key it contains is exposed, no other cars will be affected. Therefore, there is no a single point of vulnerability of the entire system. Secondly, the system in [15] essentially adopts a token-based authentication method, where a car owner gets the authentication key and delegation key from the server, along with a sealed e-envelope containing these keys, which can only be opened by the car; in accessing the car by the car owners or a delegated users, the sealed e-envelope must be communicated to the car, together with the actual authentication data. The sealed envelope adds to the communication overhead. In comparison, proposed system performs a hierarchical key generation method for car, car owners and delegated users. HIBS-KSharing has the same properties with the system in [15], i.e., do not need to register the authentication keys of the car owners and the delegated users to the car, while proposed system further avoid the redundant communication overhead of the sealed envelope.

VI. CONCLUSIONS AND FUTURE WORKS

In this paper, we proposed a secure HIBS-KSharing system for car sharing and rental, which is secure and efficient. With issued digital keys, authorized users or customers can access cars with their smartphones. HIBS-KSharing system takes use of IBS-based scheme to generate keys. In addition, since proposed scheme is a hierarchical architecture, top level of authorized users or customers can further generate next level keys for new users or customers. Our experimental simulation environment is under Android smartphones and NFC devices, compared with existing digital key sharing systems, HIBS-KSharing system is an efficient and secure one.

Our future works focus on data security and privacy for car sharing and rental. Private data include user data (e.g., behaviour and favourite setting) and car status data (such as GPS and commends).

REFERENCES

[1] Millard-Ball, G. Murry, J. Ter Schure. C. Fox, and J. Burkhardt, "TCRP report 108: Car-Sharing: Where and how it succeeds," Trans. Res. Board, Washington, DC, USA, Tech. Rep., vol. 108, 2005.

[2] J. Hong, J. Shin, and D. Lee, "Strategic management of next-generation connected life: Focusing on smart key and car–home connectivity," *Technol. Forecasting Soc. Change*, vol. 103, pp. 11–20, Feb. 2016.

[3] *DriveNow*. Accessed on Mar. 10, 2017. [Online]. Available: https://uk.drive-now.com/

[4] *Car2Go*. Accessed on Mar. 10, 2017. [Online]. Available: http://www.car2go.com/

[5] *Zipca*. Accessed on Mar. 10, 2017. [Online]. Available: http://www.zipcar.com/

[6] *RelayRides*. Accessed on Mar. 10, 2017. [Online]. Available: http://www.relayrides.com/

[7] *Car Club*. Accessed on Mar. 10, 2017. [Online]. Available: https://www.carclub.com.sg/

[8] *Joint News Release by the Land Transport Authority (LTA) and EDB—Electric Vehicles (EVS) in Every HDB Town by 2020*. Accessed on Mar. 10, 2017. [Online]. Available: https://www.lta.gov.sg/apps/news/page.aspx?c=2&id=e030e95d-a82c-49b4-953c-fc4b3fad7924

[9] *Is Near Field Communication (NFC) Finally Coming to Cars?* Accessed on Mar. 10, 2017. [Online]. Available: http://blog.ihs.com/is-near-field-communication-nfc-finally-coming-to-cars

[10] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, 2016, pp. 461–472.

[11] A. G. Bianchessi *et al.*, "Green move: A platform for highly configurable, heterogeneous electric vehicle sharing," *IEEE Intell. Transp. Syst. Mag.* vol. 6, no. 3, pp. 96–108, Fall 2014.

[12] L. Bauer, S. Garriss, J. McCune, M. Reiter, J. Rouse, and P. Rutenbar, "Device-enabled authorization in the Grey system," in *Proc. Int. Conf. Inf. Secur.*, 2005, pp. 431–445.

[13] J. Timpner, D. Schürmann, and L. Wolf, "Secure smartphone-based registration and key deployment for vehicle-to-cloud communications," in *Proc. ACM Workshop Secur., Privacy Depend. Cyber Veh.*, 2013, pp. 31–36.

[14] J. Han, Y.-H. Lin, A. Perrig, and F. Bai, "MVSec: Secure and easy-to-use pairing of mobile devices with vehicles," in *Proc. ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2014, pp. 51–56.

[15] C. Busold *et al.*, "Smart keys for cyber-cars: Secure smartphone-based NFC-enabled car immobilizer," in *Proc. 3rd ACM Conf. Data Appl. Secur. Privacy*, 2013, pp. 233–242.

[16] B. Groza, T. Andreica, and P.-S. Murvay, "Designing wireless automotive keys with rights sharing capabilities on the MSP430 microcontroller," in *Proc. 3rd Int. Conf. Veh. Technol. Intell. Trans. Syst.*, Porto, Portugal, Apr. 2017, pp. 173–180.

[17] M. Elkins, *A Peer-to-Peer Approach to Digital Key Sharing for Vehicle Access Control*, Embedded Secure Cars, Detroit Metropolitan, MI, USA, Jun. 2017.

[18] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, 1984, pp. 47–53.

[19] Y. Desmedt and J. Quisquater, "Public-key systems based on the difficulty of tampering," in *Proc. CRYPTO*, 1987, pp. 111–117.

[20] U. M. Maurer and Y. Yacobi, "A non-interactive public-key distribution system," *Des., Codes, Cryptograph.*, vol. 9, no. 3, pp. 305–316, 1996.

[21] E. Okamoto, "Key distribution systems based on identification information," in *Proc. CRYPTO*, 1988, pp. 194–202, 1988.

[22] H. Tanaka, "A realization scheme for the identity-based cryptosystem," in *Proc. CRYPTO*, 1988, pp. 340–349.

[23] S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 4, pp. 467–473, Apr. 1989.

[24] S. A. Vanstone and R. J. Zuccherato, "Elliptic curve cryptosystems using curves of smooth order over the ring Z_n," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp. 1231–1237, Jul. 1997.

[25] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. CRYPTO*, 1987, pp. 186–194.

[26] L. C. Guillou and J.-J. Quisquater, "A 'paradoxical' indentity-based signature scheme resulting from zero-knowledge," in *Proc. CRYPTO*, vol. 403. 1990, pp. 216–231.

[27] A. Joux, "A one round protocol for tripartite Diffie-Hellman," in *International Algorithmic Number Theory Symposium*. Berlin, Germany: Springer, 2000, pp. 385–393.

[28] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in CryptologyCRYPTO*. Berlin, Germany: Springer, 2001, pp. 213–229.

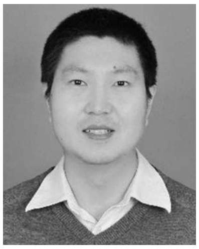
[29] *Information Technology Telecommunications and Information Exchange Between Systems Near Field Communication Interface and Protocol 1*, NFCIP-1 ISO/IEC 18092, International Organization for Standardization (ISO), Geneva, Switzerland, 2004.

[30] *Information Technology Telecommunications and Information Exchange Between Systems Near Field Communication Interface and Protocol 2*, NFCIP-2 ISO/IEC 21481, International Organization for Standardization (ISO), Geneva, Switzerland, 2005.

[31] *Identification Cards Contactless Integrated Circuit Cards Proximity Cards*, ISO/IEC 14443, International Organization for Standardization (ISO), Geneva, Switzerland, 2001.

[32] *Identification Cards Contactless Integrated Circuit(S) Cards Vicinity Cards*, ISO/IEC 15693, International Organization for Standardization (ISO), Geneva, Switzerland, 2000.

[33] *Specification of Implementation for Integrated Circuit(s) Cards*, JICSAP/JSA JIS X 6319, Japan IC Card System Application Council (JICSAP), 2005.



ZHUO WEI received the B.A. degree from Jilin University, China, and the M.S. and Ph.D. degrees from Huazhong University of Science and Technology, China. He is currently a Research Scientist with Huawei International Co., Singapore. His interests include image processing and video processing, multimedia security, and vehicle security. He received the Best Paper Award from CMS 2012.

YANG YANJIANG received the Ph.D. degree from National University of Singapore in 2005. He is a Senior Researcher on information security at Shield Lab, Huawei, Singapore. From 2008 to 2015, he was with the Institute for Infocomm Research, Singapore, as a Scientist. From 2005 to 2008, he was a Postdoctoral Fellow at Singapore Management University. His research spans a wide spectrum of information security areas in wireless sensor network, trusted computing, cloud security, multimedia security, and cyber-physical security. His current research interest is IoT security and applied cryptography.

YONGDONG WU received the B.Eng. and the M.S. degrees from Beihang University, China, the Ph.D. degree from the Institute of Automation, Chinese Academy of Science, and the Master for Management of Technology from National University of Singapore. He is currently a Senior Scientist with Infocomm Security Department, Institute of Infocomm Research (I2R), Agency for Science Technology and Research (A*STAR), Singapore. He is also an Adjunct Associate Professor with Singapore Management University. His research interests include multimedia security, eBusiness, digital right management, and network security. He has published more than 100 papers, and holds seven patents. His research results and proposals were incorporated in the ISO/IEC JPEG 2000 security standard 15444-8 in 2007. He received the Best Paper Award from the IFIP Conference on Communications and Multimedia Security (CMS) 2012.

JIAN WENG received the M.S. and B.S. degrees in computer science and engineering from South China University of Technology in 2004 and 2000, respectively, and the Ph.D. degree in computer science and engineering from Shanghai Jiao Tong University, China, in 2008. From April 2008 to March 2010, he was a Postdoctoral in the School of Information Systems, Singapore Management University. Currently, he is a Professor and Executive Dean with the School of Information Science and Technology, Jinan University. His research interests include cryptography, information security, and artificial intelligence. He has published more than 80 papers in cryptography conferences and journals, such as CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, and IEEE TPAMI. He served as a PC Co-Chair or PC Member for more than 30 international conferences. He has won the 2014 Cryptographic Innovation Award from the Chinese Association for Cryptographic Research, the Best Paper Award from the 28th Symposium on Cryptography and Information Security (SCIS 2011), the Best Student Award from the 8th International Conference on Provable Security (ProvSec 2014), and the Best Student Award from the 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017).

ROBERT H. DENG (F'16) received the B.Eng. degree from National University of Defense Technology, China, in 1981, and the M.Sc. and Ph.D. degrees from Illinois Institute of Technology, Chicago, USA, in 1983 and 1985, respectively. He has been a Professor at the School of Information Systems, Singapore Management University (SMU) since 2004. His research interests include data security and privacy, multimedia security, and network and system security. He is the Co-Chair of the Steering Committee of ASIACCS. He received the University Outstanding Researcher Award in 1999 and the Lee Kuan Yew Fellow for Research Excellence from SMU in 2006. He was named Community Service Star and Showcased Senior Information Security Professional by (ISC) under its Asia-Pacific Information Security Leadership Achievements program in 2010. He received the Distinguished Paper Award of NDSS 2012 and the Best Paper Award of CMS 2012.