Hindawi
Security and Communication Networks
Volume 2018, Article ID 8053967, 8 pages
https://doi.org/10.1155/2018/8053967

Research Article

Practical Secure Transaction for Privacy-Preserving Ride-Hailing Services

Chenglong Cao [1] **and Xiaoling Zhu** [2]

[1] *Department of Xueyan Trade, Anhui Finance and Trade Vocational College, Hefei 230601, China*
[2] *School of Computer and Information, Hefei University of Technology, Hefei 230009, China*

Correspondence should be addressed to Chenglong Cao; chenglongcao@sina.cn

Received 4 November 2017; Accepted 14 January 2018; Published 11 February 2018

Academic Editor: Pino Caballero-Gil

Ride-hailing service solves the issue of taking a taxi difficultly in rush hours. It is changing the way people travel and has had a rapid development in recent years. Since the service is offered over the Internet, there is a great deal of uncertainty about security and privacy. Focusing on the issue, we changed payment pattern of existing systems and designed a privacy protection ride-hailing scheme. E-cash was generated by a new partially blind signature protocol that achieves e-cash unforgeability and passenger privacy. Particularly, in the face of a service platform and a payment platform, a passenger is still anonymous. Additionally, a lightweight hash chain was constructed to keep e-cash divisible and reusable, which increases practicability of transaction systems. The analysis shows that the scheme has small communication and computation costs, and it can be effectively applied in the ride-hailing service with privacy protection.

1. Introduction

In recent years, more and more consumers use ride-hailing services with the rapid development of online transportation companies such as DiDi and Uber. Compared with a traditional taxi service, a ride-hailing service has the characteristics of convenience and efficiency. Nowadays, it plays an important role in people's life [1]. On the other hand, since online service platform is easy to collect sensitive information such as user identities and trip paths, privacy disclosure issues are becoming serious with the expansion of ride-hailing services.

Current research on transportation privacy mainly focuses on public transportation. Radio frequency identification (RFID), as noncontact automatic identification technology, is widely used in transportation. Heydt-Benjamin et al. [2] suggested an encrypted RFID payment scheme. Arfaoui et al. [3] used near field communication technology to design an electronic traffic ticket scheme with privacy protection. Isern-Deya et al. [4] designed an anonymous automatic ticket checking system. Based on zero knowledge proof, a toll scheme is proposed to prevent a driver from cheating [5]. Troncoso et al. [6] designed a secure system to collect vehicle insurance fees, which relies on the security of vehicle equipment. Because pick-up points and drop-off points are relatively fixed in public transportation, a passenger is not easy to be distinguished from other passengers if their pick-up or drop-off points are the same.

Compared with public transportation, the privacy issues involved in online transportation services are different, and the related research is little. Friginal et al. [7] proposed a distributed solution using social networks and the solution requires users to conduct peer to peer communications. Pham et al. [8] presented a privacy-enhanced scheme. In the scheme, a driver and a passenger establish a secure channel to exchange messages with the help of online service platform; for a passenger, the platform cannot associate his identity with his location; but the paper did not provide specific communication details.

As for the security of mobile payment in general application scenarios, some methods have been provided [9]:

password, symmetric and asymmetric cryptography, and certificateless digital signature. Abughazalah et al. [10] presented a mobile payment scheme based on one-time passwords and tamper-resistant keys. Qin et al. [11] provided a novel approach to secure a mobile wallet by incorporating digital signature and pseudoidentity techniques. But the payment platform in the schemes [10, 11] knows the relationship between the pseudonym and the real identity of a user. If he wants, he can track all the transactions.

In order to solve the above issues, based on anonymous e-cash, we designed an authenticated hash chain and further proposed a privacy protection scheme for the ride-hailing service. The main features are as follows: (1) Payment pattern is transformed from third-party transfer payment to e-cash payment. E-cash is unforgeable and partially blinded, which makes payment secure and anonymous. (2) A lightweight trusted hash chain is constructed to keep e-cash divisible and reusable, which enhances convenience and practicability of a payment system. (3) The main process is similar to prevailing systems. Therefore, our scheme can be deployed on the existing platforms.

The remainder of this paper is organized as follows. Firstly, we introduce security requirements including security requirements and transaction framework in Section 2 and cryptographic preliminaries in Section 3. We describe the proposed scheme in detail in Section 4. We then analyze the security and performance in Sections 5 and 6, respectively. Finally, we conclude the paper in Section 7.

2. System Model

2.1. Security Requirements. There are some security threats to ride-hailing services. In order to get illegal profits, the service platform may infer private information from request messages and further track passengers. External attackers may eavesdrop on the communication channel or impersonate legal users. To resist the attacks, the security requirements are as follows:

(i) Antieavesdropping: for external attackers, it is computationally infeasible to obtain privacy information of passengers

(ii) Anonymity: it is computationally infeasible to infer the identity of a user from his service request

(iii) Authenticity: it is computationally infeasible to impersonate others to apply for e-cash, make a payment, or deposit e-cash

(iv) Unforgeability: for a passenger, a service platform, and a malicious user, it is computationally infeasible to forge e-cash

(v) Nonlinkability: it is computationally infeasible to infer the relationship between trip trajectory and user identity from request messages

(vi) Accountability: a service platform can revoke the anonymity of illegal passengers under certain conditions

Considering the practical environments, we assume that the platform is honest and curious, and the platform expects to obtain user privacy. From the perspective of the development of enterprise, the platform will not initiate active attacks. On the other hand, the driver has to share his location to pick up passengers, so he is not anonymous.

2.2. Transaction Framework. A ride-hailing system at least includes the following entities:

1. Passenger (P): a passenger has a smartphone with Internet access. P's identity, public key, private key, and public key certificates are ID_P, PK_P, SK_P, and Cert_P, respectively
2. Driver (D): if a driver wants to provide ride-hailing service, he should be online and send his location to the platform. His identity, public key, private key, and public key certificate are ID_D, PK_D, SK_D, and Cert_D, respectively
3. Online transportation network (OTN) platform: according to received data from passengers and drivers, OTN makes a match and returns nearby vehicle information to P. OTN is also responsible for calculation of trip fees. His identity, public key, private key, and public key certificate are $\mathrm{ID}_{\mathrm{OTN}}$, $\mathrm{PK}_{\mathrm{OTN}}$, $\mathrm{SK}_{\mathrm{OTN}}$, and $\mathrm{Cert}_{\mathrm{OTN}}$, respectively
4. Third-party payment (TPP) platform: TPP is an independent institution in transactions. Because the activities, such as withdraw and deposit, need to be carried out on the cash accounts, all trading entities should register on TPP. TPP's identity, public key, private key, and public key certificate are $\mathrm{ID}_{\mathrm{TPP}}$, $\mathrm{PK}_{\mathrm{TPP}}$, $\mathrm{SK}_{\mathrm{TPP}}$, and $\mathrm{Cert}_{\mathrm{TPP}}$, respectively

In the existing ride-hailing system, OTN sends P's phone number to D and sends D's phone number to P. At the end of the trip, OTN deposits money to OTN's account and D's account according to prearranged proportion. So TPP knows P's cash account and trip fees. OTN knows P's identity, location, and fees. When OTN and TPP are conspiring together, more privacy will be disclosed.

We adopt e-cash payment pattern, which includes the communications among P, D, OTN, and TPP:

1. P obtains enough e-cash from TPP.
2. P inputs his pick-up and drop-off points and sends them to OTN. OTN estimates trip fees and sends them to P. If P agrees, he accepts it. Otherwise, he quits.
3. OTN confirms the vehicle and returns D's identity, phone number, license plate number, possible arrival time, and other information to P.
4. P contacts D: once P gets on the car, D tells OTN and OTN starts billing. When P arrives at the destination point, D notices OTN.
5. According to the actual trip and duration time, OTN returns the service price. P makes a payment using e-cash.

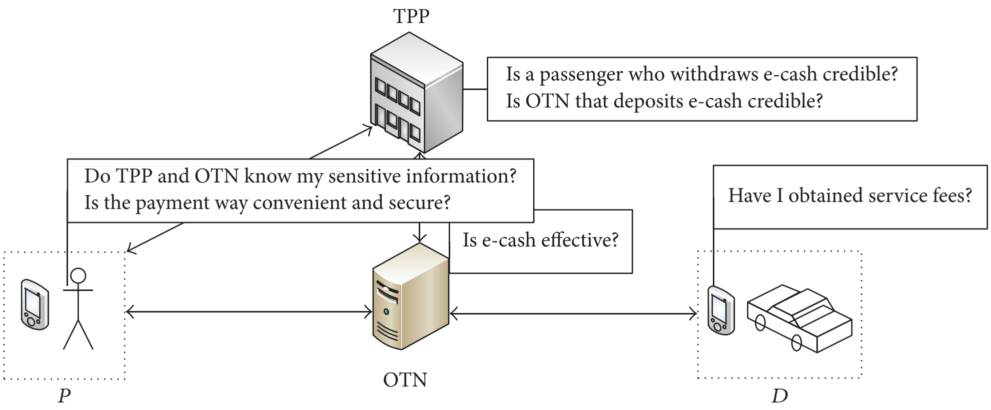

TPP
Is a passenger who withdraws e-cash credible?
Is OTN that deposits e-cash credible?
Do TPP and OTN know my sensitive information?
Is the payment way convenient and secure?
Have I obtained service fees?
Is e-cash effective?
P
OTN
D

Figure 1: Security and privacy issues in ride-hailing services.

6. Within the validity period of e-cash, OTN sends e-cash and D's identity to TPP. TPP deposits money into D's and OTN's accounts.

In the above process, there are some security and privacy concerns (Figure 1). When P withdraws e-cash from TPP, he may be worried about the disclosure of his identity and location. When P makes a payment, he expects that TPP can provide a secure and convenient payment way. For OTN, he needs to determine whether the payment is effective. For D, he expects to obtain service rewards successfully. For TPP, he expects that P is credible when P applies e-cash; meanwhile, he expects that OTN is credible when OTN deposits e-cash.

3. Preliminaries

3.1. Cryptographic Primitives. Smartphones has become mainstream mobile devices. As we know, since mobile devices are generally energy-intensive and computing-power-limited, complex algorithms and protocols are not suitable for them. Considering hash function with the features of low power consumption and being one way and collision-free [11], a trusted hash chain is constructed in our model. Let $H_1 : \{0,1\}^* \rightarrow \{0,1\}^l$, $H_2 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*$, and $H_3 : \{0,1\}^* \rightarrow Z_q^*$ be collision-free hash functions. Define ${H_1}^i(x)$ as the result of i executions of $H_1(x)$.

In general, encryption and signature methods are used to ensure secure transmission of messages. Compared with other public key cryptography algorithms, elliptic curve cryptography (ECC) requires smaller keys to provide equivalent security. So an elliptic curve $E_p(a,b)$: $y^2 = x^3 + ax + b$ on the finite field GF(p) is chosen, where $4a^3 + 27b^2 \neq 0 \bmod p$. (p,a,b,q,G) are common parameters, and G is the point of order q. On the elliptic curve, define Enc(PK, m) as encryption function of message m using the public key PK. Similarly, Dec(SK, c) is a decryption function using the private key SK. Sign(SK, m) is a signature function. Ver(PK, m, σ) is a signature verification function using the public key PK. Define the symbol ‖ as a string concatenation operation.

3.2. Divided e-Cash. When e-cash is divided, it can be reused. This brings convenience for payment. But a traditional divided e-cash scheme has large amount of calculation [12]. Based on hash authentication and partially blind signature, we combine hash chain with e-cash to make a practical payment. As long as e-cash does not run out, it can continue to be used.

First choose a random number r_N and compute $r_{N-1} = H_1(r_N)$, $r_{N-2} = H_1(r_{N-1}), \ldots, r_1 = H_1(r_2)$, and $r_0 = H_1(r_1)$, forming the hash chain $r_N \rightarrow r_{N-1} \rightarrow r_{N-2} \rightarrow \cdots \rightarrow r_1 \rightarrow r_0$. And then the root node r_0, OTN's identifier $\mathrm{ID}_{\mathrm{OTN}}$, the denomination N, the expiry date T, and TPP's signature are embedded into e-cash.

The credential material for the first payment is e-cash ‖ i ‖ r_i, where i is the trip expense and r_i is the corresponding chain node. If $h^i(r_i) = r_0$, the node r_i is effective. Second payment credential material is e-cash ‖ k ‖ r_j, where $j = i + k$ and k is the second expense. If $h^k(r_j) = r_i$ and $j \leq N$, r_j is the effective node. Later payment processes are done in a similar way.

To sum up, an effective payment requires the following: (i) E-cash is used within the validity period. In particular, payment and deposit time is not more than the deadline. (ii) TPP's signature to e-cash is correct. (iii) The hash chain is trusted; that is, all nodes should pass validity check.

4. Proposed Scheme

The scheme includes nine protocols: initialization, withdrawal, ride, payment, deposit, repeated payment, refund, collaborative tracking, and high anonymous payment. Among them, repeated payment, refund, collaborative tracking, and high anonymous payment protocols are optional according to different consumption demands and privacy requirements. For example, if P has surplus e-cash, he may use it once again (repeated payment) or refund his money (refund). When a malicious event happens, OTN may contact D to track P. Additionally, P with high privacy requirements may choose the high anonymous payment protocol.

4.1. Initialization. P, D, and OTN need to register their cash accounts on the payment platform TPP, which works as a debit system. If the denomination of e-cash issued to P is N, P's account will be reduced by N. We assume that TPP is in the secure environment and all the accounts data stored in TPP will not be leaked illegally.

4.2. Withdrawal. When P applies for e-cash, the withdrawal protocol is executed between TPP and P. Using a partially blind signature method, TPP issues e-cash as follows:

(1) TPP randomly chooses k and computes and sends kG to P.

(2) P sends a request for e-cash to TPP.

(a) Choose r_N randomly, and generate a hash chain $r_N \to r_{N-1} \to r_{N-2} \to \cdots \to r_1 \to r_0$.

(b) Choose the blind factors α and β randomly and compute

$$A = \alpha \left(kG + \beta Q\right), \tag{1}$$

where $Q = \mathrm{PK}_{\mathrm{TPP}} = dG$ and $d = \mathrm{SK}_{\mathrm{TPP}}$.

(c) Compute

$$c = H_2 \left(m_1, m_2, A_x\right), \tag{2}$$

where $m_1 = r_0$, $m_2 = \mathrm{ID}_{\mathrm{OTN}} \parallel N \parallel T$, and A_x is x coordinate of point A on the elliptic curve. In particular, m_2 is a common message negotiated by P and TPP; N and T are the denomination and expiration date of e-cash, respectively.

(d) Blind c and obtain

$$c' = \beta - \alpha^{-1} c. \tag{3}$$

(e) Send c' and P's signature and certificate

$$c' \parallel \mathrm{Sign}\left(\mathrm{SK}_P, c'\right) \parallel \mathrm{Cert}_P. \tag{4}$$

(3) TPP verifies whether Cert_P and $\mathrm{Sign}(\mathrm{SK}_P, c')$ are correct. If satisfied, TPP further confirms whether P's account balance is greater than N. If satisfied, TPP reduces N from P's account, and then he makes a partially blind signature,

$$s' = k + H_3 \left(m_2\right) + c'd, \tag{5}$$

and sends it to P. Otherwise, he aborts.

(4) P removes the blind factor from s' and obtains

$$s = \alpha \left(s' - H_3 \left(m_2\right)\right). \tag{6}$$

(5) P checks the equation

$$c = H_2 \left(m_1, m_2, A'_x\right), \tag{7}$$

where $m_1 = r_0$, $m_2 = \mathrm{ID}_{\mathrm{OTN}} \parallel N \parallel T$, and $A' = sG + cQ$.

(6) If (7) does not hold, P aborts. Otherwise, P obtains

$$\text{e-cash} = \left(r_0, \mathrm{ID}_{\mathrm{OTN}} \parallel N \parallel T, c, s\right). \tag{8}$$

4.3. Ride

(1) P sends the pick-up point and drop-off points to OTN; OTN returns the estimated price to P.

(2) If P accepts the price, then he confirms the service; otherwise, he aborts.

(3) OTN selects the nearby vehicle and returns D's contact information to P.

(4) P calls D. When P gets on the car, D notices OTN. When P arrives at the destination, D sends the actual arrival time and place to OTN.

(5) OTN calculates the actual price and sends it to P.

4.4. Payment

(1) P confirms payment and sends OTN

$$\mathrm{Enc}\left(\mathrm{PK}_{\mathrm{OTN}}, \text{e-cash} \parallel i \parallel r_i\right). \tag{9}$$

(2) OTN decrypts and checks whether the date and signature of e-cash are valid. If they are valid, he further checks

$$h^i \left(r_i\right) = r_0. \tag{10}$$

If satisfied, he records (e-cash, i, r_i). Otherwise, the payment has failed.

4.5. Deposit

(1) During the validity period of e-cash, OTN sends TPP

$$\mathrm{Enc}\left(\mathrm{PK}_{\mathrm{TPP}}, m \parallel \mathrm{Sign}\left(\mathrm{SK}_{\mathrm{OTN}}, m\right)\right), \tag{11}$$

where $m = \text{e-cash} \parallel i \parallel r_i \parallel \mathrm{ID}_{\mathrm{OTN}} \parallel \mathrm{ID}_D$.

(2) TPP decrypts and verifies whether e-cash is validated. If verification is passed, he records (e-cash, i, r_i). Then TPP deposits money into OTN's and D's accounts according to the agreed proportion, respectively.

The above withdrawal, payment, and deposit protocols are shown in Figure 2.

4.6. Repeated Payment. When e-cash has not been used up, P may spend the remainder. If the amount of another consumption is k, the payment protocol is modified as follows: P sends $c = \mathrm{Enc}(\mathrm{PK}_{\mathrm{OTN}}, \text{e-cash} \parallel k \parallel r_j)$ to the OTN, where $j = i + k$ and $j \le N$. When the condition

$$h^k \left(r_j\right) = r_i \tag{12}$$

is satisfied, OTN updates (e-cash, i, r_i) to (e-cash, j, r_j). If $j = N$, it indicates that e-cash is used up.

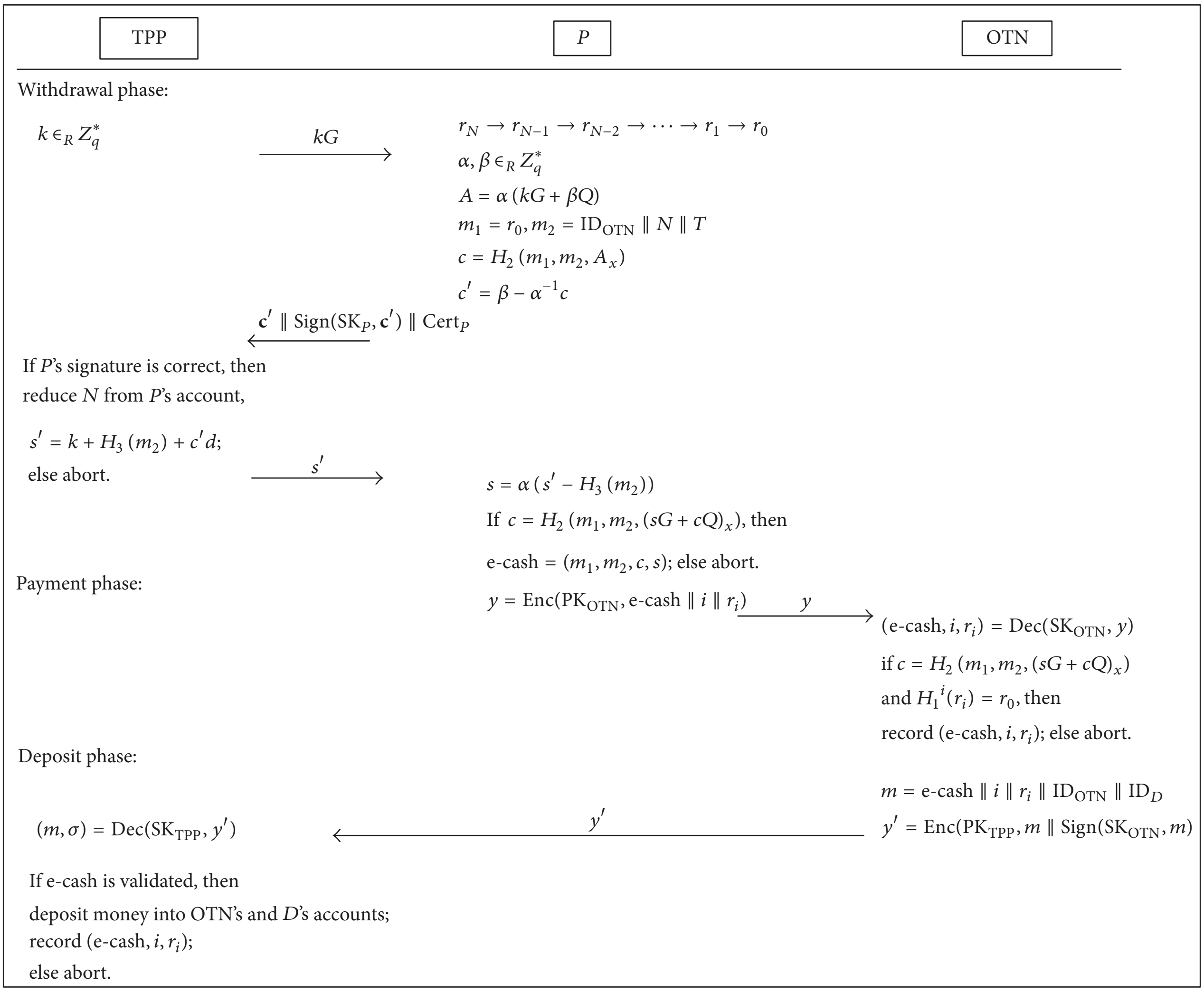

TPP
P
OTN
Withdrawal phase:
$k \in_R Z_q^*$
kG
$r_N \to r_{N-1} \to r_{N-2} \to \cdots \to r_1 \to r_0$
$\alpha, \beta \in_R Z_q^*$
$A = \alpha(kG + \beta Q)$
$m_1 = r_0, m_2 = \mathrm{ID_{OTN}} \parallel N \parallel T$
$c = H_2(m_1, m_2, A_x)$
$c' = \beta - \alpha^{-1} c$
$\mathbf{c}' \parallel \mathrm{Sign}(\mathrm{SK}_P, \mathbf{c}') \parallel \mathrm{Cert}_P$
If P's signature is correct, then
reduce N from P's account,
$s' = k + H_3(m_2) + c'd$;
else abort.
s'
$s = \alpha(s' - H_3(m_2))$
If $c = H_2(m_1, m_2, (sG + cQ)_x)$, then
e-cash = (m_1, m_2, c, s); else abort.
Payment phase:
$y = \mathrm{Enc}(\mathrm{PK_{OTN}}, \text{e-cash} \parallel i \parallel r_i)$
y
$(\text{e-cash}, i, r_i) = \mathrm{Dec}(\mathrm{SK_{OTN}}, y)$
if $c = H_2(m_1, m_2, (sG + cQ)_x)$
and $H_1{}^i(r_i) = r_0$, then
record (e-cash, i, r_i); else abort.
Deposit phase:
$m = \text{e-cash} \parallel i \parallel r_i \parallel \mathrm{ID_{OTN}} \parallel \mathrm{ID}_D$
$y' = \mathrm{Enc}(\mathrm{PK_{TPP}}, m \parallel \mathrm{Sign}(\mathrm{SK_{OTN}}, m)$
y'
$(m, \sigma) = \mathrm{Dec}(\mathrm{SK_{TPP}}, y')$
If e-cash is validated, then
deposit money into OTN's and D's accounts;
record (e-cash, i, r_i);
else abort.

Figure 2: Withdrawal, payment, and deposit protocols.

4.7. Refund. During the period from T (deposit deadline) to $T+x$ (refund deadline), P can refund his money. First, P sends

$$\mathrm{Enc}\left(\mathrm{PK_{TPP}}, \text{e-cash} \parallel N - i \parallel r_N \parallel \mathrm{ID}_P\right). \tag{13}$$

After TPP confirms that e-cash is valid, he returns the money $N - i$ into P's cash account and updates the record (e-cash, i, r_i) to (e-cash, N, r_N). When the time passes $T + x$, TPP deletes the record.

4.8. Collaborative Tracking. When a malicious event occurs, P's identity needs to be recovered. In the ride protocol, P contacts D, and thus D knows P's contact information. If TPP needs to obtain P's identity, he will contact D. Then TPP and D track P collaboratively.

4.9. High Anonymous Payment. TPP does not know P's identity when e-cash is reused. But multiple trips are paid with the same e-cash, which give away the fact that the different routes belong to the same person.

For a passenger with high privacy requirements, he may choose alternative payment protocol, where e-cash can only be used once. If the ride price is N, the denomination of requested e-cash is also N. P makes the first payment with e-cash $\parallel N \parallel r_N$, and then e-cash runs out once.

5. Security Analysis

Proposition 1. *Partially blind signature protocol is correct.*

Proof. From the withdrawal protocol, we can see

$$\begin{aligned} A' &= sG + cQ = \alpha\left(s' - H_3(m_2)\right)G + cQ \\ &= \alpha\left(k + H_3(m_2) + c'd - H_3(m_2)\right)G + cQ \\ &= \alpha\left(k + \left(\beta - \alpha^{-1}c\right)d\right)G + cQ \\ &= \alpha(kG + \beta Q) - cQ + cQ = \alpha(kG + \beta Q) = A. \end{aligned} \tag{14}$$

Then $H_2(m_1, m_2, A'_x) = H_2(m_1, m_2, A_x) = c$. Therefore, the blind signature can be verified by (7). □

Proposition 2. *E-cash can be divided.*

Proof. P sends e-cash $\|$ i $\|$ r_i to TPP for the first payment. And the remaining $N - i$ can be reused. For the second payment, P shows e-cash $\|$ k $\|$ r_j. Similarly, e-cash can be used repeatedly until $j = N$. Therefore, e-cash is divided.

On the other hand, e-cash $\|$ k $\|$ r_j cannot be reused because OTN searches for the last used hash node (e-cash, i, r_i) to decide whether this payment is valid. If the share r_j is reused, then $H_1{}^k(r_j) \neq r_i$. So r_j is rejected. □

Proposition 3. *E-cash is unforgeable.*

Malicious P, OTN, or TPP may expect to forge e-cash. For example, P wants to increase N; OTN wants to embed false $\mathrm{ID}_{\mathrm{OTN}}$. Our withdrawal protocol based on blind signature has the existential unforgeability under the random oracle model and the assumption of difficulty in solving the $Q = dG$ problem on an elliptic curve. Specific proof is as follows.

The challenger $\mathscr{C}$ receives an instance (P, $Q = dG$) of the discrete logarithm problem and his goal is to compute d. Let $\mathscr{A}$ be a probabilistic polynomial Turing machine to find a valid signature. $\mathscr{C}$ calls $\mathscr{A}$ to solve the discrete logarithm problem. If $\mathscr{A}$ is a sufficiently efficient forger, then it follows from the forking lemma. $\mathscr{A}$ obtains two distinct forgeries (m_1, m_2, c_1, s_1) and (m_1, m_2, c_2, s_2) with $c_1 \neq c_2$ and $s_1 \neq s_2$. From the signature process, we can obtain that $s_1 G + c_1 Q = \alpha(kG + \beta Q)$ and $s_2 G + c_2 Q = \alpha(kG + \beta Q)$. Thus $s_1 G + c_1 Q = s_2 G + c_2 Q$. Then $(c_1 - c_2)Q = (s_2 - s_1)G$. So

$$d = (c_1 - c_2)^{-1} (s_2 - s_1) \tag{15}$$

is the solution to the discrete logarithm problem.

Proposition 4. *It is difficult for an attacker to impersonate a legitimate user to obtain e-cash and further make a successful payment.*

Proof. (1) The request for e-cash is signed by P, which ensures the authenticity of requester identity and unforgeability of request message.

(2) Since a complete hash chain is only owned by a legitimate user, illegal passenger fails to offer correct node to make a successful payment.

(3) During payment and deposit phases, e-cash and chain node are encrypted and transmitted, which prevents the leakage of credentials. □

Proposition 5. *In the face of OTN and TPP, P is anonymous.*

Proof.

(1) E-Cash Has Partial Blindness. Any legitimate signature (m_1, m_2, c, s) and any of intermediate variables (kG, c', s') satisfy the following equations:

$$sG + cQ = \alpha \left(kG + \beta Q\right), \tag{16}$$

$$c' = \beta - \alpha^{-1} c, \tag{17}$$

$$s = \alpha \left(s' - H_3\left(m_2\right)\right). \tag{18}$$

From the withdrawal protocol, $s' = k + H_3(m_2) + c'd$. Further, we determine the unique value $\alpha = s(s' - H_3(m_2))^{-1} = s(k + c'd)^{-1}$ from (18) and $\beta = c' + \alpha^{-1} c$ from (17). Thus,

$$\begin{aligned} \alpha\left(kG + \beta Q\right) &= \alpha kG + \alpha\left(c' + \alpha^{-1} c\right) Q \\ &= \alpha\left(kG + c'Q\right) + cQ \\ &= s\left(k + c'd\right)^{-1}\left(kG + c'Q\right) + cQ \\ &= sG + cQ. \end{aligned} \tag{19}$$

Since α and β satisfy (16), there must be blind factors between any of the intermediate variables and any legitimate signature. So TPP cannot associate the signature result with the specific signing process to obtain P's identity.

(2) Anonymous Payment. P withdraws e-cash from TPP and then pays e-cash to OTN. Because there is no identity in e-cash, a ride service cannot directly be associated with user's identity. On the other hand, when e-cash is reused, OTN can associate the different ride routes with the same e-cash, and thus P is not completely anonymous. Alternative protocol is provided to make P use new e-cash in each ride service. □

Proposition 6. *A ride route cannot be linked with a certain passenger identity.*

Proof. (1) For a single trip, there is no identity information in the communications between P and OTN and between OTN and TPP. Thus, it is difficult to associate P's identity with one ride route.

(2) For several trips under the high anonymous payment protocol, one e-cash can only be used once; OTN cannot infer whether several trips belong to a single passenger. □

Proposition 7. *P can be tracked under certain conditions.*

Proof. Because D knows P's contact information, OTN can track an illegal person through the collaborative tracking protocol with the help of D. So P's identity can be recoverable under certain conditions.

We compare our scheme with other schemes that are intended to ensure security and privacy of mobile payment. The results are shown in Table 1.

The schemes [7, 8] provide antieavesdropping, anonymity, and nonlinkability. Scheme [7] does not use e-cash, and it does not provide traceability. Scheme [8] and our scheme both track illegal passengers and use e-cash. But divided e-cash has not been mentioned in [8]. □

Table 1: Security and privacy comparisons.

	Antieavesdropping	Anonymity	Nonlinkability	Traceability	Divided e-cash
[7]	Yes	Yes	Yes	No	No
[8]	Yes	Yes	Yes	Yes	No
Ours	Yes	Yes	Yes	Yes	Yes

6. Evaluation

6.1. Performance of Our Scheme. Among the required protocols, the initialization protocol occurs in the registration phase; and the ride protocol is similar to existing services. So we mainly analyze the performance of withdrawal, payment, and deposit protocols.

Communication Cost. It concludes 5-step communications among three entities. (1) TPP sends kG to P. (2) P submits a request $c' \parallel \mathrm{Sign}(\mathrm{SK}_P, c') \parallel \mathrm{Cert}_P$ to TPP. (3) TPP generates the blinded e-cash s' to P. (4) P sends encrypted e-cash y to OTN for payment. (5) OTN sends encrypted e-cash y' to TPP for deposit.

Define the symbol $|\cdot|$ as the length of a string. The communication cost of concern includes (1) the withdrawal cost $|kG|+|\mathbf{c}'|+|\mathrm{Sign}(\mathrm{SK}_P, \mathbf{c}')|+|\mathrm{Cert}_P|+|s'|$, (2) the payment cost $|y|$, and (3) the deposit cost $|y'|$.

Computation Cost. For convenience, to evaluate the computation cost, we ignore some operations such as a hash function and a multiplication operation because they are quite light in terms of load. We focused on some time-consuming operations defined in the following notations. T_S, T_V, T_E, T_D, T_G, T_{BS}, and T_{BV} denote the time of signature, verification, encryption, decryption, point multiplication, blind signature, and validation operations on the elliptic curve, respectively. The computation cost of concern can be broken up into 3 parts. (1) During the withdrawal phase, P computes $A = \alpha(kG + \beta Q)$ and $\mathrm{Sign}(\mathrm{SK}_P, c')$; TPP checks Cert_P and $\mathrm{Sign}(\mathrm{SK}_P, c')$; P checks $c = H_2(m_1, m_2, (sG{+}cQ)_x)$. The time of these operations is $T_S + 2T_V + 4T_G$. (2) During the payment phase, P computes $\mathrm{Enc}(\mathrm{PK}_{\mathrm{OTN}}, \text{e-cash} \parallel i \parallel r_i)$, and OTN decrypts it and checks $c = H_2(m_1, m_2, (sG + cQ)_x)$. The operations take $T_E + T_D + 2T_G$. (3) During the deposit phase, OTN computes $\mathrm{Enc}(\mathrm{PK}_{\mathrm{TPP}}, m \parallel \mathrm{Sign}(\mathrm{SK}_{\mathrm{OTN}}, m))$; TPP decrypts it. We assume that OTN will no longer need to check the effectiveness of blind signature after he makes the first confirmation. Then the time during the phase is $T_S + T_V + T_E + T_D$. Therefore, the overall computation costs during the three phases are $2T_S + 3T_V + 2T_E + 2T_D + 6T_G$.

Performance Evaluation. In order to provide the precise comparisons of computation and communication costs, we use the experiment data in [13] to evaluate them. On the elliptic curve (p, a, b, q, G), 0.6 ms is required to perform scalar multiplications if $|q| = 20$ bytes and $|G| = 20$ bytes. For the elliptic curve digital signature algorithm (ECDSA), if the key is 28 bytes, the signature result is 53 bytes, and the public certificate is 84 bytes; 0.8 ms is required to perform signature and 4.2 ms is required to perform verification. Additionally, for the elliptic curve integrated encryption scheme (ECIES), the encryption time is approximately $2T_G$; the decryption time is approximately T_G; and the cipher text length is twice as large as the plaintext. Specifically, we assume $|\mathrm{ID}_{\mathrm{OTN}}| = 10$, $|N| = 8$ bytes, and $|T| = 2$ bytes; then $|m_2| = 10 + 8 + 2 = 20$ bytes and $|\text{e-cash}| = 20 + 20 + 20 + 20 = 80$ bytes. Therefore, the withdrawal cost is $20 + 20 + 53 + 84 + 20 = 197$ bytes; the payment cost is $2 * (80 + 8 + 20) = 216$ bytes; and the deposit cost is $2 * (80 + 8 + 20 + 10 + 10 + 53) = 362$ bytes.

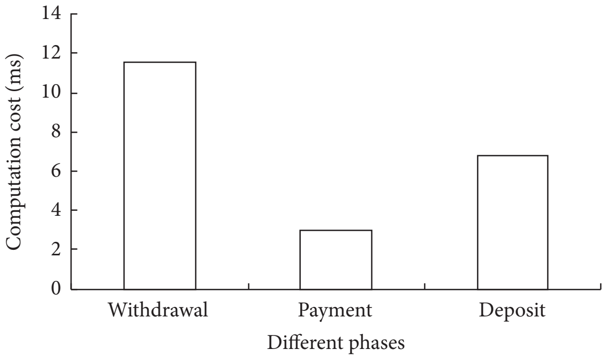


Figure 3: Computation costs during different phases.

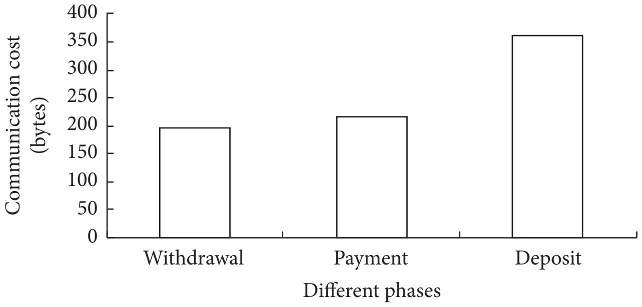


Figure 4: Communication costs during different phases.

Figures 3 and 4 show computation and communication costs during the three phases of withdrawal, payment, and deposit, respectively. It is seen that the computation cost during payment phase is the smallest among the three phases. Considering that payment occurs most frequently among three activities, it is beneficial to improve the overall performance of the ride-hailing system.

6.2. Performance Comparisons. E-cash is used in [8], whose system architecture is partly similar to ours. We shall compare the two schemes. Table 2 shows comparisons of computation and communication costs. In particular, the costs of the

Table 2: Performance comparisons.

	Communication	Computation
[8]	≥4	$T_{BS} + T_{BV} + 4T_{SE} + 4T_{SD} + 4T_G$
Our scheme	5	$2T_S + 3T_V + 2T_E + 2T_D + 6T_G$

scheme in [8] are for the withdrawal and secure channel establishment phases; meanwhile, the costs of our scheme are for the withdrawal, payment, and deposit phases. In the table, T_{BS}, T_{BV}, T_{SE}, and T_{SD} represent the time of blind signature, blind verification, symmetric encryption, and symmetric decryption, respectively. From the overall performance, our scheme is better than the scheme in [8].

The scheme in [8] used DH key exchange protocol to establish secure channel between a passenger and a driver. Just the two phases of withdrawal and secure channel establishment require at least four steps. If payment and deposit are taken into account, the communication cost of the scheme in [8] is more than ours.

In the scheme in [8], a symmetric encryption method is used to prevent e-cash from being stolen. The computation cost of symmetric encryption is small relative to that of asymmetric encryption, but the key agreement protocol for distributing a session key increases the cost. Moreover, the scheme does not provide the specific description of blind signature. In our scheme, an authenticated hash and e-cash are used to design the repeated payment and refund protocols. It not only reduces costs but also improves practicability.

7. Conclusion

We construct a trusted hash chain with anonymous e-cash and then provide a privacy protection scheme for ride-hailing services. It consists of nine protocols: initialization, withdrawal, ride, payment, deposit, repeated payment, refund, collaborative tracking, and high anonymous payment. The latter four protocols are optional protocols. Security analysis shows that e-cash is divided and unforgeable; the scheme has antieavesdropping, anonymity, and nonlinkability. Performance analysis shows that the scheme has a small amount of communication and computation overhead because a lightweight hash chain is introduced. Moreover, its main business process is basically consistent with the prevailing services. Therefore, it can be deployed on the existing transaction systems.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Natural Science Foundation of Anhui Province (Grant 1608085MF141), the Major Research Project for Social Science Innovation and Development of Anhui Province (Grant 2017ZD005), and the Visiting Scholar Projects of Anhui Province for Excellent Young and Middle-Aged Backbone Talents (Grant gxfxZD2016305).

References

[1] Y. Liu, “Defects in the development and the improvement of transportation network services,” *Social Sciences*, vol. 2016, no. 11, p. 297, 2016.

[2] T. S. Heydt-Benjamin, H. J. Chae, B. Defend, and L. Fu, “Privacy for public transportation,” in *Proceedings of the International Workshop on Privacy Enhancing Technologies*, pp. 1–19, Springer, Berlin, Germany, 2006.

[3] G. Arfaoui, J. F. Lalande, J. Traore, and N. Desmoulins, “A practical set-membership proof for privacy-preserving NFC mobile ticketing,” *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 25–45, 2015.

[4] A. P. Isern-Deya, A. Vives-Guasch, M. Mut-Puigserver, M. Payeras-Capellà, and J. Castellà-Roca, “A secure automatic fare collection system for time-based or distance-based services with revocable anonymity for users,” *The Computer Journal*, vol. 56, no. 10, pp. 1198–1215, 2013.

[5] S. Meiklejohn, K. Mowery, S. Checkoway, and H. Shacham, “The phantom tollbooth: privacy-preserving electronic toll collection in the presence of driver collusion,” in *Proceedings of the USENIX Security Symposium*, vol. 201, no. 1, pp. 1–16, 2011.

[6] C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, “PriPAYD: privacy-friendly pay-as-you-drive insurance,” *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 742–755, 2011.

[7] J. Friginal, S. Gambs, J. Guiochet, and M.-O. Killijian, “Towards privacy-driven design of a dynamic carpooling system,” *Pervasive and Mobile Computing*, vol. 14, pp. 71–82, 2014.

[8] A. Pham, I. Dacosta, B. Jacot-Guillarmodb, and J. P. Hubaux, “Private ride: a privacy-enhanced ride-hailing service,” in *Proceedings of the 17th Privacy Enhancing Technologies Symposium (PETS ’17)*, pp. 38–56, 2017.

[9] P. Pukkasenung and R. Chokngamwong, “Review and comparison of mobile payment protocol,” in *Advances in Parallel and Distributed Computing and Ubiquitous Services, Proceedings of Pdcat*, pp. 11–20, 2015.

[10] S. Abughazalah, K. Markantonakis, and K. Mayes, “Secure mobile payment on NFC-enabled mobile phones formally analysed using CasperFDR,” in *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom ’14)*, pp. 422–431, IEEE, Beijing, China, September 2014.

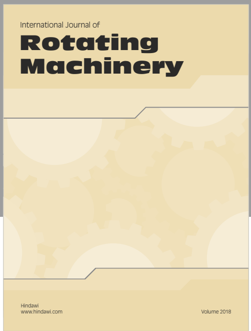
[11] Z. Qin, J. Sun, A. Wahaballa, W. Zheng, H. Xiong, and Z. Qin, “A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing,” *Computer Standards & Interfaces*, vol. 54, pp. 55–60, 2017.

[12] Y. Yu, X. Dong, and Z. Cao, “A trust-based and efficient divisible e-cash scheme,” *Journal of computer research and development*, vol. 52, no. 10, pp. 2304–2312, 2015.

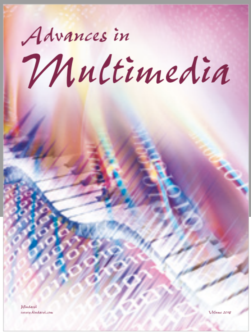
[13] L. Chen, S.-L. Ng, and G. Wang, “Threshold anonymous announcement in VANETs,” *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 605–615, 2011.

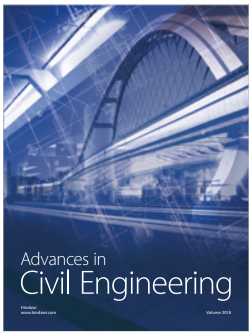
Journal of
Engineering

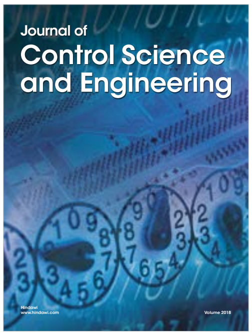
The Scientific World Journal


International Journal of
Rotating Machinery

Journal of
Sensors

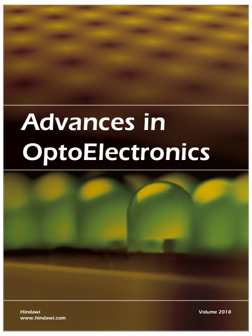

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science and Engineering

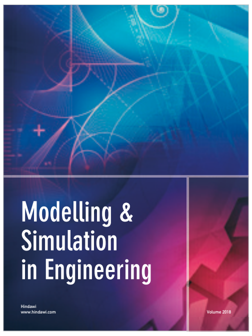
Journal of
Robotics

Journal of
Electrical and Computer Engineering

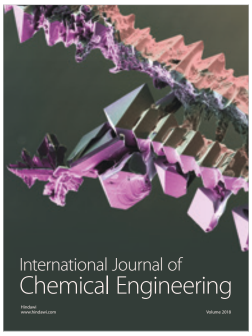

Advances in
OptoElectronics

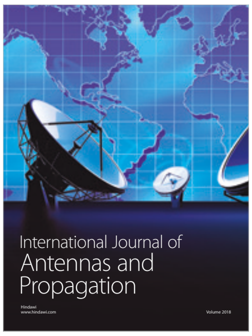
VLSI Design

International Journal of
Navigation and Observation

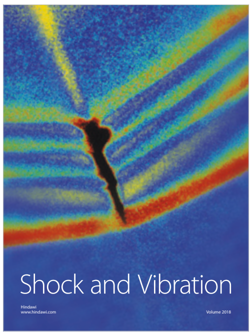

Modelling &
Simulation
in Engineering

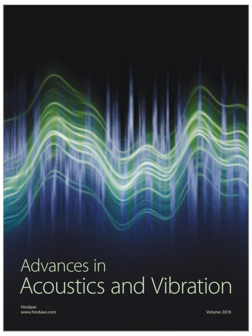
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration