Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 7823979, 11 pages
https://doi.org/10.1155/2018/7823979

Research Article

NTRU Implementation of Efficient Privacy-Preserving Location-Based Querying in VANET

Bo Mi,[1] Darong Huang,[1] and Shaohua Wan [2]

[1] *Institute of Information Science and Engineering, Chongqing Jiaotong University, Chongqing 400074, China*
[2] *School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan 430073, China*

Correspondence should be addressed to Shaohua Wan; shaohua.wan@ieee.org

Received 26 January 2018; Accepted 21 March 2018; Published 3 May 2018

Academic Editor: Xuyun Zhang

The key for location-based service popularization in vehicular environment is security and efficiency. However, due to the constrained resources in vehicle-mounted system and the distributed structure of fog computation, disposing of the conflicts between real-time implementation and user's privacy remains an open problem. Aiming at synchronously preserving the position information for users as well as the data proprietorship of service provider, an efficient location-based querying scheme is proposed in this paper. We argue that a recent scheme proposed by Jannati and Bahrak is time-consuming and vulnerable against active adaptive corruptions. Thus accordingly, a postquantum secure oblivious transfer protocol is devised based on efficient NTRU cryptosystem, which then serves as the understructure of a complete location-based querying scheme in ad hoc manner. The security of our scheme is proved under universal composability frame, while performance analysis is also carried out to testify its efficiency.

1. Introduction

With the development and fusion of techniques such as sensing, controlling, communication, positioning, and fog computation, vehicular ad hoc network (VANET), which is identified as a specific application of Internet of Things (IoT), has become a promising understructure to enhance traffic safety and convenience. As an important element of the intelligent transportation system (ITS), VANET is typically composed of numerous on-board units (OBU) equipped on vehicles and road-side units (RSUs) serve as infrastructure [1]. Different from traditional networking, vehicular ad hoc network emphasizes heavily on adaptive computation as well as communication of end-users and edge devices, which is characterised as localized data storage, dense geographical distribution, boundary service providing, and compound data aggregation or analysis. A wide range of applications can be supported taking advantage of such fundamental installation; for example, when driving on the road, one can fall back on the VANET to locate services (shops, gas stations, etc.) on his route, or even be notified of any forecasted traffic condition along her itinerary. Though it is envisioned that the future transportation would be "information-driven" and "wirelessly enabled," the problems of confidential and privacy-preserving communication remain insufficiently solved due to the broadcasting nature of VANET [2]. Moreover, since one of the most attractive applications of VANET is location-based querying, it is always self-extended to traditional networks such as Internet. As illustrated in Figure 1, any authorized on-board unit may access the querying service providers (QSPs) in backbone or local RSUs to inquire about interested information via various communication channels, which makes the security issue more complicated in such foggy environment.

As for privacy, the user may not want anybody, including the infrastructure units or service providers, to be aware of any information about her query. That means it should either be impossible to link up a query with the real identity of the user or make the query itself indistinct to some extent. In order to accomplish privacy requirement, two research lines are followed in literatures.

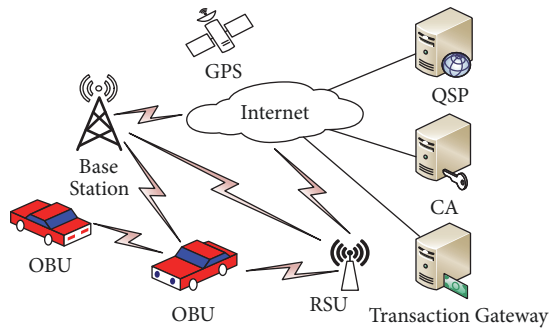

Figure 1: VANET extension.

1.1. Correlation Concealment. Due to the interactive nature of location-based querying, one can easily associate the identity of a user with a specific location which may severely violate the privacy of personal health condition, social relationships, habits, and so on. Accordingly, once the connectivity of inquired location and user ID are obscured, the sensitive information may be preserved to some extent. This kind of privacy-protection method includes the following.

1.1.1. Anonymity and Pseudonym. The goal of cryptonym methods is to prevent an adversary from reidentifying the data source by exploiting any exposed information. It generally relies on the fact that most location-based services are not strictly dependent on the knowledge of user's identity. Thereby, the most challenging issues turn into pseudonymous authentication, integrity, and nonrepudiation. Specifically, a large number of certificates are usually preloaded for each vehicle, which will be abandoned after usage in a short period of time. Coupled with reputation mechanisms, those certificates can thus be used to appraise credibility of anonymous sources or to fulfil the backtracking purpose [3]. Nevertheless, anonymity and pseudonym schemes are only robust to semihonest secure model, because malicious vehicles may not discard or update their certificates as required by the protocols [4].

1.1.2. Mix Zones. The technique of mix zones is originally introduced by Beresford and Stajano [5], where the pseudonym should be exchange amongst all users within a same zone. The time interval when a vehicle passes through a mix zone is called the silent period, which means it must dumb its position so as to break off the connection between its identities at the entry and exit points. Palanisamy and Liu [6] investigated various context information in traffic environment that may reveal detailed trajectories such as geometrical or temporal constraints and devised the MobiMix approach directing against such privacy infringement. It is worth mentioning that the idea of k-anonymity presented by Gruteser and Grunwald [7] is always served as a combination of anonymity (pseudonym) and mix zone implementation. For example, Caballero-Gil et al. [8] exploited the spatial and temporal cloaking to calculate the k-anonymity set, which makes a vehicle indistinguishable from other $k - 1$ counterparts. To avoid active corruption, if a number of complaints are received pertinent to a malicious node, a track algorithm can also be carried out to prevent further detriment. Aiming at Sybil attack, Feng et al. [9] bounded k-anonymity and reputation schemes together, which can effectively suppress the spread of false messages when updating the anonymity.

1.2. Query Fuzzification. The service of location-based querying can be deemed as a process of information retrieval, which means only the users care about the correctness or precision of the research outcomes. Therefore, lots of approaches are presented taking the advantage of information asymmetry between users and the server, including the following.

1.2.1. Position Dummies. It is aiming to deceive the QSP by confounding the user's true position together with multiple false locations [10–13]. Nevertheless, since the traffic networks are always scattered but structured, it is difficult to create dummies indistinguishable from the true position. In order to generate plausible dummies, Shankar et al. [14] proposed the SybilQuery approach, which obfuscates the real position with dummies chosen from a historical traffic database.

1.2.2. Obfuscation. The idea behind position obfuscation is to intentionally reduce the precision of inquiry messages. Typically, the protocol proposed by Ardagna et al. [15] used a circular area to substitute the exact position of a user. Though the obfuscation area can be allodially determined by the querier, the trade-off between privacy and precision is of great significance. Thus, accordingly, Reynold et al. [16] introduced a model for probabilistic range queries depending on the overlapping size of the query area and the obfuscation shapes. Another way to obfuscate the user's position is the coordinate transformation, where some geometric mappings are carried out on a series of users' coordinates before sending to the server. However, in order to ensure the functionality of the QSP, it is impossible to find an all-sided protection scheme purely based on coordinate transformation because the service provider has to be able to determine the relative position of objects and areas to each other [17]. In addition, to preserve the trajectory of user, a great deal of spatiotemporal location obfuscation schemes are also proposed, which also took the temporal information associated with positions into account [18–25].

Table 1: Security parameters for diffident public key cryptosystems.

Mathematical problem	Integer factorization	Elliptic curve discrete logarithm	Discrete logarithm
Security level	RSA (bits)	ECC (bits)	ElGamal (bits)
Low security	1024	160	1024
Moderate security	2048	224	2048
Standard security	3072	256	3072
High security	7680	384	7680
Highest security	15360	512	15360

1.2.3. Position Sharing. With the existence of several untrusted servers, location information can be mathematically calculated as a series of shares and distributed on different databases. This approach was first proposed by Dürr et al. [26] who split up the location information into shares of strictly limited precision. After retrieving adequate shares from multiple servers, the user can execute a combination algorithm which fuses them into a message of higher precision. In order to prevent attackers from deriving the precise position via coordinate relationships of a map, Skvortsov et al. took map knowledge into account [27] and further improved their protocol by optimizing the placement of shares in terms of servers' trustworthiness [28]. Though position sharing schemes can also be implemented on account of obfuscation or coordinate transformation [29], cryptography-based fashions are preferable due security consideration [30].

1.2.4. Cryptographic Approaches. Due to the capacities such as confidentiality, integrity, and authenticity, cryptographic primitives are taken as desirable building blocks to realize position privacy. For the sake of concealing the real identity of a user, ring or group signature are generally used to confound the querier as a member of a vehicular set [31, 32]. By using private information retrieval (PIR) technique, a QSP can answer queries without learning or revealing any information of the query [33, 34]. Meanwhile, since the computational result of ciphertext matches that of the plaintext, homomorphic cryptosystems are also valued as promising tools for location privacy application [35, 36].

Nevertheless, the aforementioned approaches took only the querier's position information as a target for protection and simply lost the sight of QSP's data ownership. Practically, the charging models in nowadays always lie on a per-query basis which enable drivers to use the service in ad hoc manner and pay for their queries according to the quantity. With regard to the proprietorship of QSP's records, Paulet et al. [37] proposed a location-based querying approach in the light of 1-out-n oblivious transfer (OT_n^1). Their scheme made use of an ElGamal cryptosystem which imposed an additional privacy property for the sender such that the receiver could learn at most one of the retrieved items. However, Jannati and Bahrak [38] caught the sight of its security defect arguing that the receiver is able to decrypt all ciphered records; thus the QSP's data ownership cannot be preserved. In order to rectify the vulnerability of Paulet's scheme, they also reconstructed the oblivious transfer part of it at the cost of higher computational overhead.

Table 2: Security parameters for NTRUEncrypt.

Mathematical problem	Shortest vector problem		
Security level	N	q	p
Moderate security	401	2048	3
Standard security	439	2048	3
High security	593	2048	3
Highest security	743	2048	3

It is well known that ElGamal encryption is defined over a cyclic group G, whose security depends on the difficulty of computing discrete logarithms. Therefore, a large security parameter must be considered in order to make sure that it is unbreakable. Though other traditional public key cryptosystems may also be exploited as basic primitives to realize oblivious transfer, they are deficient in efficiency due to computational hardness assumptions depending on large parameters. For the same reason, these cryptosystems tend to be vulnerable with the advent of quantum machine era. The comparison of security parameters amongst diffident cryptosystems is given in Table 1.

During encryption phase, ElGamal requires two exponentiation operations, while one exponentiation should be correspondingly carried out for decryption. Since exponentiation on large numbers is always time-consuming and occupies a lot of memory, we argue that Jannati's scheme is not efficient enough, especially under embedded environments. Moreover, though their scheme is proved to be secure under game-based verification, active and adaptive corruptions are simply ignored because CCA (chosen ciphertext attack) security is unachievable by ElGamal cryptosystem itself [39].

In order to eliminate the defects of Jannati's protocol, we take the advantage of NTRUEncrypt to implement privacy-preserving location-based querying. As a relatively new public key cryptosystem developed in 1996, the number theory research unit encryption (NTRU) [40] runs faster compared to other asymmetric encryption schemes and is more competitive to be realized in resource-constraint environments such as mobile devices or smart cards. Up till 2017, literatures can be found that introduce new parameters to resist currently known attacks and increase its computation power [41, 42]. According to the latest research [43], the parameters in Table 2 are considered secure.

As for Table 2, the parameters, where N defines a truncated polynomial ring $R = Z[x]/(x^N - 1)$ used in NTRUEncrypt and q, p are two moduli, are relatively smaller

than that of traditional public key cryptosystems. Moreover, it uses only simple polynomial multiplications; the time of performing an NTRU operation increases only quadratically. Taking moderate security for example, if both exponentiation and polynomial multiplication are composed of $\log_2 q$-bits modular multiplications, the former must invoke the basis $q^2/\log_2 q$ times compared to $N \log_2 N$ of the latter. It is reported that, using a modern GTX280 GPU, a throughput of up to 200,000 encryptions per second can be reached at a security level of 256 bits [44], which is only approximately 20 times slower than a recent AES implementation [45]. Accordingly, we resort to the characteristics of high efficiency as well as postquantum security and employ NTRUEncrypt as a building block to realize oblivious transfer. Then, based on the novel OT_n^1 protocol, an adaptive secure location-based querying scheme can thus be achieved.

The rest of this paper is organized as follows. We first give some preliminaries about oblivious transfer and NTRUEncrypt in Section 2. In Section 3, a NTRU-based 1-out-n oblivious protocol will be devised in advance which is then used to structure the secure location-based querying scheme after describing the system model. Security analyses and performance evaluations are given in Sections 4 and 5. The paper is finally concluded in Section 6.

2. Preliminaries on 1-Out-n Oblivious Transfer and NTRUEncrypt

Oblivious transfer, originally introduced as conjugate coding, owns its name to Rabin [46]. Amongst different flavors of OT, 1-out-n oblivious transfer has been extensively studied in the literature since any cryptographic task can be achieved by this extremely basic primitive [47]. In cryptography, a 1-out-n oblivious transfer is a type of protocol in which a receiver R is entitled to obtain 1 out of n messages held by a sender S without learning any other messages, while the sender do not know which massage has been chosen. The protocol is formally described as in Table 3.

In order to optimize the performance of oblivious transfer protocol, several tricks can be imposed on it. For example, [48] enables the computation of many OTs with a small elementary cost from k OT at a normal cost and also enables to reduce oblivious transfers of long strings to oblivious transfers of short strings using a pseudorandom generator.

In this paper, an efficient and secure OT_n^1 protocol will be constructed based on NTRUEncrypt in the light of its linearity and resistance to quantum machines. The NTRU encryption algorithm works on a truncated polynomial ring $R = Z[x]/(x^N - 1)$ with convolution multiplication and all polynomials in the ring have integer coefficients and degree at most $N - 1$:

$$\mathbf{a}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}. \tag{1}$$

Similar to the prime decomposition problem exploited by RSA, the security of NTRUEncrypt relies on hardness of factoring a reducible polynomial, which is equivalent to the shortest vector problem. Thus, it is infeasible to usurp the secret key if the parameters are chosen secure enough.

Table 3: Oblivious transfer paradigm $\mathcal{F}_{\mathrm{OT}}$.

Input
(i) S input $m_0, m_1, \ldots, m_{n-1} \in M$
(ii) R input $\delta \in \{0, 1, \ldots, n-1\}$
Output
(i) S output $\perp$ (i.e., nothing)
(ii) R output m_δ

For each system, three integer parameters (N, p, q) are specified, where p and q are two moduli who truncate the ring R as $R_p = (Z/pZ)[x]/(x^N - 1)$ and $R_q = (Z/qZ)[x]/(x^N - 1)$. It is always assumed that N, p are prime while q is coprime to both q and N. To generate a key pair, two key polynomials f and g whose coefficients lie within $\{-1, 0, 1\}$ must be generated in advance. An additional requirement that there exist two inverses f_p, f_q, where $f \cdot f_p = 1 \bmod p$ and $f \cdot f_q = 1 \bmod q$, must also be satisfied. Then, f together with f_p can be preserved as the secret key, while $h = p \cdot f_q \cdot g$ will be published to be the public key.

During encrypting phase, a message m should be represented as a binary or ternary string and transformed into a truncated polynomial within the ring R. Then a binding polynomial r with small coefficients should be randomly chosen to calculate the ciphertext as

$$c = r \cdot h + m \pmod q. \tag{2}$$

In order to decrypt the cryptograph c, the receiver first computes

$$a = f \cdot c \pmod q \tag{3}$$

and then lifts its coefficients to interval $[-q/2, q/2]$ and achieves the plaintext as

$$m = f_p \cdot a \pmod p. \tag{4}$$

In order to prove the correctness of our protocols, a polynomial set $\mathcal{T}(d_1, d_2)$ specified by two parameters is defined in advance.

Definition 1. For any positive integers d_1 and d_2,

$$\mathcal{T}(d_1, d_2) = \left\{ \mathbf{a}(x) \in R_q : \begin{array}{l} d_1 \text{ cofficients of } \mathbf{a}(x) \text{ are } 1 \\ d_2 \text{ cofficients of } \mathbf{a}(x) \text{ are } -1 \\ \text{other cofficients of } \mathbf{a}(x) \text{ are } 0. \end{array} \right. \tag{5}$$

According to Definition 1, the correctness of NTRU decryption can be guaranteed in terms of the condition described as below.

Lemma 2. *If the polynomials of NTRU cryptosystem are chosen from*

$$\begin{aligned} f &\in \mathcal{T}(d+1, d), \\ g &\in \mathcal{T}(d, d), \\ r &\in \mathcal{T}(d, d), \end{aligned} \tag{6}$$

whose coefficients satisfy

$$q > p(6d + 1), \tag{7}$$

then a legal receiver can accurately recover ciphertext c with her private key.

Proof. Since all polynomials of

$$a = p \cdot g \cdot r + f \cdot m \pmod q \tag{8}$$

are provided with coefficients designated by formula (6), the parameters of $g \cdot r$ after convolution polynomial multiplication will never overrange $[-2d, 2d]$. Similarly, the parameters of f as well as m are located within $[-p/2, p/2]$ which means that the maximal parameter of $f \cdot m$ is $p(d + 1/2)$ to its very extent. As a result, once the condition of $q > p(6d + 1)$ is met, all parameters of (8) can be lifted to $[-q/2, q/2]$ without losing any information. Then by computing

$$f_p \cdot a = f_p \cdot p \cdot g \cdot r + m = m \pmod p, \tag{9}$$

the message can accurately be recovered. □

3. Location Privacy-Preserving Querying Based on NTRU

In this paper, a novel location-based querying scheme is proposed aiming at not only protecting the position privacy of drivers but also preserving the data proprietary of QSP. Specifically, three goals must be achieved in terms of security and feasibility.

(a) Within authenticated but not confidential communication environments, any malicious third party is incapable of gaining or efficaciously modifying any information of the conversation.

(b) Even if active and adaptive corrupted participant exists, the driver must be insensible of any data hold by QSP except the one she requested while keeping her querying information concealed.

(c) The protocol should be feasible on both vehicle-mounted devices as well as location-based servers, which means that low computation and communication burden must be fulfilled.

For clarity, a novel 1-out-n oblivious transfer protocol will be presented in the first place. Then we will employ it as the building block to complete our entire scheme.

3.1. NTRU Implementation of 1-Out-n Oblivious Transfer. Different from traditional public key cryptosystems, NTRU is structured on a truncated polynomial ring which is provided with both addition and multiplication. Since the time of performing convolution multiplication is much faster than that of modular exponentiation on large numbers, the preferable efficiency and security property of NTRU are more appropriate to construct the basic oblivious transfer protocol.

In order to realize the NTRU-based 1-out-n oblivious transfer, the messages held by the sender are presented as $m_0, m_1, \ldots, m_{n-1}$, which must be kept unacquainted from the receiver except for m_δ. Accordingly, we describe the primitive 1-out-n oblivious transfer protocol as below.

During key generation phase, the sender constructs a key pair as in Section 2, she releases her public key $pk = h$ to all potential receivers or stores it in a communal database, while keeping the secret key $sk = (f, f_p)$ private.

In oblivious transfer phase, the sender is supposed to choose n random polynomials $\gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ from $\mathcal{T}(d, d)$, where $r_i \cdot h$ can be represented as $p \cdot f_q \cdot \gamma_i$, and encrypt all plaintexts to be

$$c_i = r_i \cdot h + m_i \pmod q, \quad (i = \{0, 1, \ldots, n-1\}), \tag{10}$$

which is then sent to the receiver.

When all ciphertexts are received, the receiver first generates a random polynomial s belonging to $\mathcal{T}(d, d)$ and figures out its inverse $s^{-1} \pmod p$. If the inverse of polynomial s does not exist, she can simply resample another one and repeat the inversion process.

After that, the receiver must single out the δth ciphertext and compute it as

$$c'_\delta = r' \cdot h + s \cdot c_\delta \pmod q, \tag{11}$$

utilizing another random polynomial r' chosen from $\mathcal{T}(d, d)$. The result will be sent back to the sender.

Depending on the altered ciphertext c'_δ, the sender can calculate

$$\begin{aligned} a_\delta &= f \cdot c'_\delta \pmod q, \\ b_\delta &= a_\delta \pmod p \end{aligned} \tag{12}$$

and then

$$c''_\delta = f_p \cdot b_\delta \pmod p \tag{13}$$

to be her response for the driver.

Since the driver is aware of polynomial s, she can achieve the expected messages m_δ by multiply c''_δ with s^{-1} modulo p.

The above process is also characterized in Table 4.

Correctness of the 1-out-n oblivious transfer protocol relies on the computation of polynomials in truncated polynomial ring, as follows.

Lemma 3. *The driver can correctly obtain message m_δ if $q > 2p(2d^2 + 5d)$.*

Proof. Since the parameters of $g \cdot r$ or $\gamma_\delta \cdot s$ are seated within $[-2d, 2d]$ and the coefficients of $f \cdot s \cdot m_\delta$ cannot exceed $p(2d^2 + d)$ for polynomial $a_\delta = p \cdot g \cdot r' + p \cdot \gamma_\delta \cdot s + f \cdot s \cdot m_\delta \pmod q$. No information will be lost when lifting the coefficients of a_δ to $[-q/2, q/2]$, if $q > 2p(2d^2 + 5d)$ the same as Lemma 2. By computing $m_\delta = c''_\delta \cdot s^{-1} \pmod p$, where $c''_\delta = s \cdot m_\delta \pmod p$, the driver can achieve the exact message m_δ she expected. □

3.2. Efficient and Secure Location-Based Querying. The system is modelled as a QSP and a series of vehicles. More specifically, the QSP can be considered working in a distributed

Table 4: OT_n^1 protocol based on NTRUEncrypt.

Server	*Driver*
Holds n messages $m_i \in \{0,1\}^N$, $i = \{0,1,\ldots,n-1\}$.	Holds δ, $\delta \in \{0,1,\ldots,n-1\}$.
Key generation phase	
$(q, p, f, f_q, f_p, g) \leftarrow KeyGen(\kappa)$, $sk : (f, f_p)$, $pk : h$, Sends pk to the driver.	
Oblivious transfer phase	
For all $i = \{0,1,\ldots,n-1\}$, $\gamma_i \leftarrow_R \mathcal{T}(d,d)$, $c_i = p \cdot f_q \cdot \gamma_i + m_i (\mathrm{mod}\, q)$, Sends all c_i to the driver.	
	$r' \leftarrow_R \mathcal{T}(d,d)$, $s \leftarrow_R \mathcal{T}(d,d)$, where s is reversible modulo p, $c'_\delta = r' \cdot h + s \cdot c_\delta (\mathrm{mod}\, q)$, Sends c'_δ back to the server.
$a_\delta = f \cdot c'_\delta (\mathrm{mod}\, q)$, $b_\delta = a_\delta (\mathrm{mod}\, p)$, $c''_\delta = f_p \cdot b_\delta (\mathrm{mod}\, p)$, Sends c''_δ to the driver.	
	$m_\delta = c''_\delta \cdot s^{-1} (\mathrm{mod}\, p)$.

manner, which is composed of a centralized authentication server together with numerous delivery RSUs. The reason behind such configuration is to separate data retrieval from transaction process, which not only preserves the driver's position privacy but also abates the operating load of service centre. Resorting to the OBUs equipped on vehicles, drivers are able to determine their current position via localization devices such as GPS or WiFi.

In *initialization phase*, the QSP first generates its key pair and divides the geography to be a public grid G composed of V rows and W columns. For each cell $v \times w$ of the grid, she assembles all related data as a message d_i, where $i = w + v \cdot W$, $0 \le v \le V-1$, and $0 \le w \le W-1$, and encrypts it as $d'_i = E_{m_i = k_v \oplus k_w}(d_i)$ by symmetric cryptosystem E according to the keys k_v, k_w designated to each row and column. Then, the QSP stores its key pair together with all k_v, k_w as well as d'_i in distributed RSUs.

In *retrieving phase*, the driver should complete both the payment and oblivious transfer process as follows.

In order to actualize the requirement of pay-per-retrieval for location-based service, the driver should ask for a random number $\overline{r}$ from its adjacent RSU and sign it using her private key corresponding to the valid digital certificate. After verifying the digital signature sent by the driver, the authentication server should launch a preconcerted E-commerce protocol to accomplish the transaction, resign the random number $\overline{r}$ in terms of her own private key, and then send it back to the driver. Availing herself of the signed random number, the driver can thus prove to the RSU that she has paid for the service.

After that, the driver is in a position to interact with the adjacent RSU and acquire k_{v_δ} as well as k_{w_δ} corresponding to her interested coordinates in the light of the aforementioned 1-out-n oblivious transfer protocol. Then she retrieves all encrypted messages and decrypts $d_\delta = D_{m_\delta = k_{v_\delta} \oplus k_{w_\delta}}(d'_\delta)$ to recover the data she expected.

It is worth noting that the driver may retrieve all encrypted messages only once and store some of them for further queries. In addition, even if the driver's identity is exposed during the authenticating process, it will not jeopardize the confidentiality of her queried position due to the intrinsic nature of oblivious transfer.

The process is illustrated in Table 5.

In fact, the aforementioned protocol can be regarded as being based on 2-out-n oblivious transfer since two symmetric keys k_{v_δ}, k_{w_δ} should be retrieved. However, all encrypted data need only to be transmitted once during retrieval phase, which means the extra computation and communication overheads are trivial. Moreover, the public key pair of driver is only used for authentication and payment but not necessarily for oblivious transfer.

4. Security Analysis

We investigate the server's data proprietorship and the driver's position privacy in oblivious transfer at first. It should be noted that the messages obliviously transferred are symmetric keys k_{v_δ}, k_{w_δ} instead of m_δ actually; however, we will alternatively apply these notations for smooth representation.

Table 5: The proposed privacy-preserving location-based querying scheme.

Central Server	*RSUs*
Holds $V \times W$ messages d_i, $i = w + v \cdot W \in \{0, 1, \ldots, V \times W - 1\}$.	
Initialization phase	
$(sk, pk) \leftarrow KeyGen(\kappa)$, $G \leftarrow Geography$, G is a $V \times W$ grid, For all $v \in \{0, 1, \ldots, V-1\}$ and $w \in \{0, 1, \ldots, W-1\}$, $k_v, k_w \leftarrow_R \{0,1\}^\kappa$, $m_i = k_w \oplus k_v$, $i = w + v \cdot W$, $d_i' = E_{m_i}(d_i)$, Put sk, pk and all k_v, k_w, d_i' in RSUs.	
	Receives and stores sk, pk as well as all k_v, k_w, d_i' locally.
Local RSU	*Driver*
Holds sk, pk and all k_v, k_w, d_i' as above.	Holds (v_δ, w_δ), $v_\delta \in \{0, 1, \ldots, V-1\}$, $w_\delta \in \{0, 1, \ldots, W-1\}$.
Authentication and transaction phase	
	Requests for service.
$\bar{r} \leftarrow_R \{0,1\}^\kappa$ and sends it to the driver.	
	$\mathrm{Sign}_{sk_{\mathrm{driver}}}(\bar{r})$, Completes the authentication as well as payment process with the central server.
	Receives $\mathrm{Sign}_{sk}(\bar{r})$ from the central server and sends it to the RSU.
Verifies $\mathrm{Sign}_{sk}(\bar{r})$.	
Retrieving phase	
	Retrieves all d_i' from local RSU.
Executes the NTRU-based OT protocol with the driver.	Executes the NTRU-based OT protocol with the RSU and gets k_{v_δ} and k_{w_δ}. $\delta = w_\delta + v_\delta \cdot W$, $m_\delta = k_{v_\delta} \oplus k_{w_\delta}$, $d_\delta = D_{m_\delta}(d_\delta')$.

As for the driver's position privacy, we claim the following.

Lemma 4. *The QSP gains no information on the driver's choice δ in the proposed OT protocol.*

Proof. Using the private key sk, the QSP can compute $c_\delta'' = s \cdot m_\delta (\mathrm{mod}\ p)$. However, she is ignorant of the driver's secret polynomial s and thereby cannot differentiate the choice δ from any other by comparing it with possessed messages, though the QSP may fortunately figure out $r' + r_\delta \cdot s (\mathrm{mod}\ q)$ if g is reversible, which means she can further achieve $(r' + r_\delta \cdot s) \cdot (s \cdot m_\delta)^{-1} = r' \cdot s^{-1} \cdot m_\delta^{-1} + r_\delta \cdot m_\delta^{-1}$. Nevertheless, since r' and s are uniformly distributed, m_δ is totally indistinguishable. □

The server's data proprietorship can be found as follows.

Lemma 5. *The driver gains no information on m_i if $i \neq \delta$.*

Proof. The driver is aware of $c_i = r_i \cdot h_S + m_i (\mathrm{mod}\ q)$ for all messages. Since she does not possess the server's private key, the mistiness of m_i from c_i is straight-forward.

With regard to the processes of authentication and transaction, the driver would interact with a central server directly to achieve a voucher signed by the QSP's private key. That means the RSU is incapable of linking the driver's current position up to her identity. Moreover, since the voucher is generated according to a provisional random number chosen by the RSU, the chance that a driver replay her voucher to cheat the QSP out of her service is negligible. Thanks to the intrinsic characteristic of OT, even if the identity of the driver is exposed in case that the RSU colludes with the central server, the confidentially of required coordinate would never be compromised. Supposing that the driver's identity privacy is obligatory in certain circumstances, anonymous authentication schemes such as that of [49] are further suggested. □

Now, we argue UC security of the complete scheme. In order to testify that a real-world implementation of our scheme is indistinguishable from its simulation, the ideal functionality is firstly defined as follows.

Definition 6. The ideal functionality $\mathcal{F}_{\mathrm{OT}}^{-}$ receives a coordinate $(v_\delta, w_\delta) \in \{0, 1, \ldots, V-1\} \times \{0, 1, \ldots, W-1\}$ together with an identity from the driver and a vector of l-bits messages, that is, $(d_0, d_1, \ldots, d_{V \times W - 1})$, from the server S, but only outputs a l-bits string d_δ to the driver D.

Table 6: Comparison of computation and communication overheads.

	QSP		Driver	
	Jannati and Bahrak	Ours	Jannati and Bahrak	Ours
Modular exponentiation	$3(V+W+1)$	0	9	0
Modular (polynomial) multiplication	$2(V+W)+1$	$V+W+4$	7	6
Generating random numbers (polynomials)	$V+W+2$	$V+W$	2	4
Secret keys	2	1	2	0
Public keys	2	1	0	0
Communication burden (polynomials)	$V+W+1$	$V+W+2$	2	2

In line with Definition 6, two simulators $\mathcal{S}_1$, $\mathcal{S}_2$ can be established to emulate the corrupted QSP and driver, respectively. Since

$$\Pr\left[\mathcal{F}_{\mathrm{OT}}^{-}=\delta\right]=\frac{1}{(V\times W)}, \tag{14}$$

it is obvious that

$$\left|\Pr\left[\mathcal{F}_{\mathrm{OT}}=\delta\right]-\Pr\left[\mathcal{F}_{\mathrm{OT}}^{-}=\delta\right]\right|<\varepsilon(\kappa) \tag{15}$$

according to Lemma 4. So the indistinguishability

$$\begin{aligned}&\mathcal{S}_1\left(\kappa,\mathrm{ID}_{\mathrm{driver}},(d_0,d_1,\ldots,d_{V\times W-1})\right)\\&\quad\cong\mathrm{VIEW}_{\mathrm{QSP}}\left(\mathrm{ID}_{\mathrm{driver}},(d_0,d_1,\ldots,d_{V\times W-1}),\right.\\&\quad\left.(v_\delta,w_\delta)\right)\end{aligned} \tag{16}$$

is straight-forward.

Similarly, once the symmetric cryptosystem (E,D) is noncommitting, the distributions of $d'_{i\neq\delta}$ in $\mathcal{F}_{\mathrm{OT}}$ and $\mathcal{F}_{\mathrm{OT}}^{-}$ are both uniform and indiscernible, which means

$$\Pr\left[\mathcal{F}_{\mathrm{OT}}=d'_{i\neq\delta}\right]=\Pr\left[\mathcal{F}_{\mathrm{OT}}^{-}=d'_{i\neq\delta}\right]=\frac{1}{(|M|-1)}, \tag{17}$$

where $|M|$ stands for the size of plaintext space, and

$$\begin{aligned}&\mathcal{S}_2\left(\kappa,(v_\delta,w_\delta),\left(d'_0,d'_1,\ldots,d'_{V\times W-1}\right)\right)\\&\quad\cong\mathrm{VIEW}_{\mathrm{driver}}\left((v_\delta,w_\delta),\left(d'_0,d'_1,\ldots,d'_{V\times W-1}\right)\right),\end{aligned} \tag{18}$$

due to the ignorance of $k_{v_{i\neq\delta}}$ and $k_{w_{i\neq\delta}}$ on driver's side in terms of Lemma 5.

Thus we claim the folowing.

Theorem 7. *Our protocol securely implements the functionality $\mathcal{F}_{OT}^{-}$ if the symmetric encryption scheme (E,D) is noncommitting.*

5. Performance Evaluation

Since only simple polynomial multiplications are needed for NTRU cryptosystem, it features high speed, low memory requirements, and reasonably short and easily created keys. The moduli used in NTRUEncrypt specially are logarithmically smaller than that of traditional asymmetric cryptosystems based on integer factorization or discrete logarithm, which implies preferable efficiency and practicability. According to the report from [50], the speed of NTRU is up to 1300 times faster than 2048-bit RSA and 117 times faster than ECC NIST-224 when comparing the number of encryptions per second. Our experimental results also signified that the ratio of encryption times between 2048-bit ElGamal and NTRU in moderate security is 355 : 1.

In order to impartially compare with Jannati's protocol, only retrieval process will be considered in the following performance analysis. Though authentication and transaction are introduced in our scheme for pay-per-service purpose, the extra overheads are ineluctable but negligible compared to that of oblivious transfer. Table 6 illustrates the comparison of computation as well as communication overheads between our and Jannati's scheme. However, since the basic operations used in NTRU are absolutely different from that of ElGamal, it should be noted that modular multiplications and modular polynomial multiplications are correspondingly applied to one of them.

Compared to Jannati's protocol in Table 6, it is obvious that no exponentiations would be necessary in our scheme and the overhead of modular multiplication is also halved even without regard for the scale of moduli. It is worth mentioning that, though the number of transmitted messages are almost the same between Jannati's scheme and ours, we have evidently depressed the communication burden because a ElGamal encryption works on a large cyclic group and produces a double expansion in size from plaintext to ciphertext. Meanwhile, our scheme is more applicable since the receiver is free of generating or distributing any public key during oblivious transfer process.

We also simulated our and Jannati's protocol by C program. The experiment is carried out on an Intel Core i3-2330M processor (Sandy Bridge) where each party runs on one core. The computation burden and communication overhead for each retrieval are averaged by 500 tests.

According to Table 7, it is obvious that our scheme dramatically outperforms Jannati's protocol with respect to both computation and communication overheads. Specifically, taking the resource limits of OBU into account, the operational efficiency is 479 times that of Jannati's protocol, which means our scheme is more applicative in embedded and real-time environments. We simply neglected the delivery

Table 7: Timings in milliseconds and delivery loads in kilobytes for per retrieval (moderate security).

	QSP		Driver	
	Jannati and Bahrak	Ours	Jannati and Bahrak	Ours
Running time	993.23	3.26	47.85	0.10
Data size ($V + W = 64$)	34.12	8.10	1.08	0.23

load of queried data in our experiment; however, retrieving all d_i' indistinguishably from the server is inevitable due to the query privacy for any oblivious transfer. Fortunately, the driver can only retrieve the ciphered messages ones and keep all expected portions in the local storage, or she may ignore any other messages except for d_δ' when receiving the QSP's broadcast.

6. Conclusion

This paper proposed a privacy-preserving location-based querying scheme in virtue of NTRUEncrypt. Thanks to the intrinsic nature of NTRU cryptosystem such as postquantum security, high speed, low storage requirements, and short keys, our scheme is resistant to active adaptive corruptions and more practicable within vehicular ad hoc network. Specifically, the computational overheads are only 0.33 and 0.21 percent while the communication burdens are 24 and 21 percent compared to those of a recent scheme presented by Jannati and Bahrak Besides the theoretical and experimental performance analyses, we also depicted the detailed process of authentication and transaction for pay-per-service purpose. In the light of universal composability frame, it is believable that our scheme is secure with the functionality of oblivious transfer realized. For further work, we expect to reduce the interactive round of retrieving phase from 3 to 2 and decrease the RSU's overheads to a higher degree.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was supported by National Natural Science Foundation under Grants 61703063, 61663008, 61573076, and 61004118; the Scientific Research Foundation for the Returned Overseas Chinese Scholars under Grant 2015-49; the Program for Excellent Talents of Chongqing Higher School under Grant 2014-18; the Petrochemical Equipment Fault Diagnosis Key Laboratory in Guangdong Province Foundation under Grant GDUPKLAB201501; the Research Project for the Education of Graduate Students of Chongqing under Grant yjg152011; Chongqing Association of Higher Education 2015-2016 Research Project under Grant CQGJ15010C; Higher Education Reform Project of Chongqing Municipal Education Commission under Grant 163069; the Key Research Topics of the 13th Five-year plan of Chongqing Education Science under Grant 2016-GX-040; the Chongqing Natural Science Foundation under Grants CSTC2015jcyjA0540 and CSTC2017jcyjA1665; and Science and Technology Research Project of Chongqing Municipal Education Commission of China under Grants KJ1600518, KJ1705139, and KJ1705121.

References

[1] F.-Y. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: An IEEE intelligent transportation systems society update," *IEEE Pervasive Computing*, vol. 5, no. 4, pp. 68-69, 2006.

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

[3] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A Robust and Privacy-Preserving Reputation Management Scheme for Pseudonym-Enabled VANETs," *International Journal of Distributed Sensor Networks*, vol. 12, no. 3-4, Article ID 6138251, pp. 1–15, 2016.

[4] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: why simple pseudonym change is not enough," in *Proceedings of the IEEE/IFIP International Conference on Wireless On-Demand Network Systems and Services (WONS '10)*, pp. 176–183, February 2010.

[5] A. R. Beresford and F. Stajano, "Mix zones: user privacy in location-aware services," in *Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 127–131, Orlando, Fla, USA, March 2004.

[6] B. Palanisamy and L. Liu, "MobiMix: protecting location privacy with mix-zones over road networks," in *Proceedings of the IEEE 27th International Conference on Data Engineering*, pp. 494–505, Hannover, Germany, April 2011.

[7] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, pp. 31–42, ACM, San Francisco, Calif, USA, May 2003.

[8] C. Caballero-Gil, J. Molina-Gil, J. Hernández-Serrano, O. León, and M. Soriano-Ibañez, "Providing k-anonymity and revocation in ubiquitous VANETs," *Ad Hoc Networks*, vol. 36, pp. 482–494, 2016.

[9] X. Feng, C.-Y. Li, D.-X. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 306–314, 2017.

[10] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proceedings of the 2nd International Conference on Pervasive Services (ICPS '05)*, pp. 88–97, IEEE Press, July 2005.

[11] L. Qi, X. Zhang, W. Dou, and Q. Ni, "A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2616–2624, 2017.

[12] L. Qi, X. Xu, X. Zhang et al., "Structural Balance Theory-based E-commerce recommendation over big rating data," *IEEE Transactions on Big Data*, p. 1, 2016.

[13] L. Qi, W. Dou, C. Hu, Y. Zhou, and J. Yu, "A context-aware service evaluation approach over big data for cloud applications," *IEEE Transactions on Cloud Computing*, p. 1, 2015.

[14] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location-based services with sybilquery," in *Proceedings of the 11th ACM International Conference on Ubiquitous Computing, UbiComp'09*, pp. 31–40, Orlando, Fla, USA, October 2009.

[15] C. A. Ardagna, M. Cremonini, E. Damiani, S. de Capitani di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," in *Data and Applications Security XXI*, vol. 4602 of *Lecture Notes in Computer Science*, pp. 47–60, Springer, Berlin, Germany, 2007.

[16] C. Reynold, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving user location privacy in mobile data management infrastructures," in *Privacy Enhancing Technologies*, G. Danezis and P. Golle, Eds., vol. 4258 of *Lecture Notes in Computer Science*, pp. 393–412, Springer, Berlin, Germany, 2006.

[17] A. Gutscher, "Coordinate transformation - A solution for the privacy problem of location based services?" in *Proceedings of the 20th IEEE International Parallel and Distributed Processing Symposium, IPDPS 2006*, p. 7, IEEE, Rhodes Island, Greece, April 2006.

[18] J. Yang, Z. Zhu, J. Seiter, and G. Tröster, "Informative yet unrevealing: Semantic obfuscation for location based services," in *Proceedings of the 2nd ACM SIGSPATIAL Workshop on Privacy in Geographic Information Collection and Analysis, GeoPrivacy*, New York, NY, USA, 2015.

[19] F. Li, S. Wan, B. Niu, H. Li, and Y. He, "Time obfuscation-based privacy-preserving scheme for Location-Based Services," in *Proceedings of the 2016 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2016*, pp. 465–470, IEEE, Doha, Qatar, April 2016.

[20] J. D. Park, E. Seglem, E. Lin, and A. Züfle, "Protecting User Privacy," in *Proceedings of the the 1st ACM SIGSPATIAL Workshop*, pp. 1–4, Redondo Beach, CA, USA, November 2017.

[21] L. Qi, H. Xiang, W. Dou, C. Yang, Y. Qin, and X. Zhang, "Privacy-preserving distributed service recommendation based on locality-sensitive hashing," in *Proceedings of the 2017 IEEE International Conference on Web Services (ICWS)*, pp. 49–56, Honolulu, Hawaii, USA, June 2017.

[22] X. Zhang, L. Qi, W. Dou et al., "MRMondrian: Scalable Multidimensional Anonymisation for Big Data Privacy Preservation," *IEEE Transactions on Big Data*, p. 1, 2017.

[23] S. Wan, Y. Zhang, and J. Chen, "On the Construction of Data Aggregation Tree with Maximizing Lifetime in Large-Scale Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 16, no. 20, pp. 7433–7440, 2016.

[24] W. Huang, S.-K. Oh, and W. Pedrycz, "Fuzzy Wavelet Polynomial Neural Networks: Analysis and Design," *IEEE Transactions on Fuzzy Systems*, vol. 25, no. 5, pp. 1329–1341, 2017.

[25] S. Wan, "Energy-efficient adaptive routing and context-aware lifetime maximization in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 11, Article ID 321964, 2014.

[26] F. Dürr, P. Skvortsov, and K. Rothermel, "Position sharing for location privacy in non-trusted systems," in *Proceedings of the 9th IEEE International Conference on Pervasive Computing and Communications, PerCom 2011*, pp. 189–196, IEEE, Seattle, Wash, USA, March 2011.

[27] P. Skvortsov, F. Dürr, and K. Rothermel, "Map-aware position sharing for location privacy in non-trusted systems," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 7319, pp. 388–405, 2012.

[28] P. Skvortsov, B. Schembera, F. Dürr et al., Optimized Secure Position Sharing with Non-trusted Servers, 2017.

[29] J. Venkatanathan, J. Lin, and M. Benisch, Who, when, where: Obfuscation preferences in location-sharing applications, 2011.

[30] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for Fog Computing," *Future Generation Computer Systems*, vol. 78, pp. 799–806, 2018.

[31] S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, 2015.

[32] Z. Zhao, J. Chen, and Y. Zhang, "Efficient revocable group signature scheme with batch verification in VANET," *Journal of Cryptologic Research*, vol. 3, no. 3, pp. 292–306, 2016.

[33] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in *Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD '08)*, pp. 121–132, ACM, 2008.

[34] S. Bittl, "Privacy conserving low volume information retrieval from backbone services in VANETs," *Vehicular Communications*, vol. 9, pp. 1–7, 2017.

[35] M. Hur and Y. Lee, "Privacy Preserving Top-k Location-Based Service with Fully Homomorphic Encryption," *Journal of the Korea Society For Simulation*, vol. 24, no. 4, pp. 153–161, 2015.

[36] P. Hu and S. Zhu, "POSTER: Location privacy using homomorphic encryption," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 198, pp. 758–761, 2017.

[37] R. Paulet, M. G. Kaosar, X. Yi, and E. Bertino, "Privacy-preserving and content-protecting location based queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1200–1210, 2014.

[38] H. Jannati and B. Bahrak, "An oblivious transfer protocol based on elgamal encryption for preserving location privacy," *Wireless Personal Communications*, vol. 97, no. 2, pp. 1–11, 2017.

[39] S. Tan, H. Mingxing E, and S. Zeng, "CCA secure extended ElGamal encryption scheme over CF (p~n)," *Journal of Xihua University*, vol. 36, no. 1, pp. 12–16, 2017.

[40] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: a ring-based public key cryptosystem," in *Algorithmic Number Theory*, vol. 1423, pp. 267–288, Springer, Berlin, Germany, 1998.

[41] H. B. A. Wahab and T. A. Jaber, "Improve NTRU algorithm based on Chebyshev polynomial," in *Proceedings of the 2015 World Congress on Information Technology and Computer Applications (WCITCA)*, pp. 1–5, IEEE, Hammamet, Tunisia, June 2015.

[42] D. H. Duong, M. Yasuda, and T. Takagi, "Choosing Parameters for the Subfield Lattice Attack Against Overstretched NTRU," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 10599, pp. 79–91, 2017.

[43] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, "Choosing parameters for NTRUEncrypt," *Lecture Notes in Computer Science (including subseries Lecture Notes*

in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface, vol. 10159, pp. 3–18, 2017.

[44] https://tbuktu.github.io/ntru/.

[45] J. Hermans, F. Vercauteren, and B. Preneel, "Speed records for NTRU," in *Cryptographers' Track at the RSA Conference*, vol. 5985, pp. 73–88, Springer, Berlin, Germany, 2010.

[46] M. O. Rabin, "How To Exchange Secrets with Oblivious Transfer," *Cryptology ePrint Archive*, 2005.

[47] J. Kilian, "Founding cryptography on oblivious transfer," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, STOC 1988*, pp. 20–31, Chicago, Ill, USA, May 1988.

[48] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivious transfers efficiently," in *Advances in Cryptology CRYPTO*, vol. 2729, pp. 145–161, Springer, Berlin, Germany, 2003.

[49] R. Chen and D. Peng, "A novel NTRU-based handover authentication scheme for wireless networks," *IEEE Communications Letters*, vol. 22, no. 3, pp. 586–589, 2017.

[50] J. Hermans, F. Vercauteren, and B. Preneel, "Speed records for NTRU," in *Topics in Cryptology CT-RSA*, vol. 5985 of *Lecture Notes in Computer Science*, pp. 73–88, Springer, Berlin, Germany, 2010.