applied sciences

MDPI

Article

Lightweight NFC Protocol for Privacy Protection in Mobile IoT

Kai Fan [1,*], Chen Zhang [1], Kan Yang [2], Hui Li [1] and Yintang Yang [3]

1 State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China; czhangsce@163.com (C.Z.); lihui@mail.xidian.edu.cn (H.L.)
2 Department of Computer Science, University of Memphis, Memphis, TN 38152, USA; kan.yang@memphis.edu
3 Key Laboratory of the Ministry of Educ. for Wide Band-Gap Semiconductor Materials and Devices, Xidian University, Xi'an 710071, China; ytyang@mail.xidian.edu.cn
* Correspondence: kfan@mail.xidian.edu.cn; Tel.: +86-139-9193-6634

Received: 31 October 2018; Accepted: 2 December 2018; Published: 5 December 2018

Abstract: The Internet of Things (IoT) aims to achieve the interconnection of all devices in our lives. Due to the complex network environment, the IoT with mobile devices often faces many security problems, such as privacy leakages and identity forgery attacks. As a developing technology in mobile IoT, near field communication (NFC) is widely used in electronic payments and identity authentications. The current NFC studies mainly focus on payment technology, but there are a few studies on privacy protection and the lightweight requirements in the mobile IoT authentication protocol. We focus on the lightweight privacy protection authentication technology in mobile IoT. In the paper, we summarize the clustering model in mobile IoT networks and propose a lightweight authentication protocol. A security analysis shows that the protocol can resist many security threats, such as privacy leakages, identity forgeries, and replay attacks. The simulation also shows that the protocol is lightweight, with the utilization of look-up-tables (LUTs) and registers in our protocol being less than 0.5%. Our work can provide a secure and lightweight mobile authentication serve in the NFC-based mobile IoT network such as smart home and office attendance.

Keywords: Internet of Things; lightweight; NFC; authentication; privacy protection

1. Introduction

With the rapid development of the Internet of Things (IoT), many researchers have focused on security and privacy protection. The concept of the IoT was proposed by MIT in 1999. It is an extension of the Internet and can be applied to financial, logistics, retail, military, smart city, industrial, and other scenarios. The core goal of the IoT is to achieve the interconnection of terminal devices.

Any device in the IoT needs to be authenticated before the commencement of communication. Radio frequency identification (RFID) technology is used to achieve mutual authentication and communication between devices in the IoT [1]. As shown in Figure 1, the structure in the RFID system mainly includes three parts: the tag, the reader, and the server. In such a system, the reader authenticates tags before collecting the data. Due to possible attackers, it is essential to have a trusted third-party server in the authentication system [2]. During the authentication process, there are often various security problems, such as the identity forgery problem and identity leakage problem.

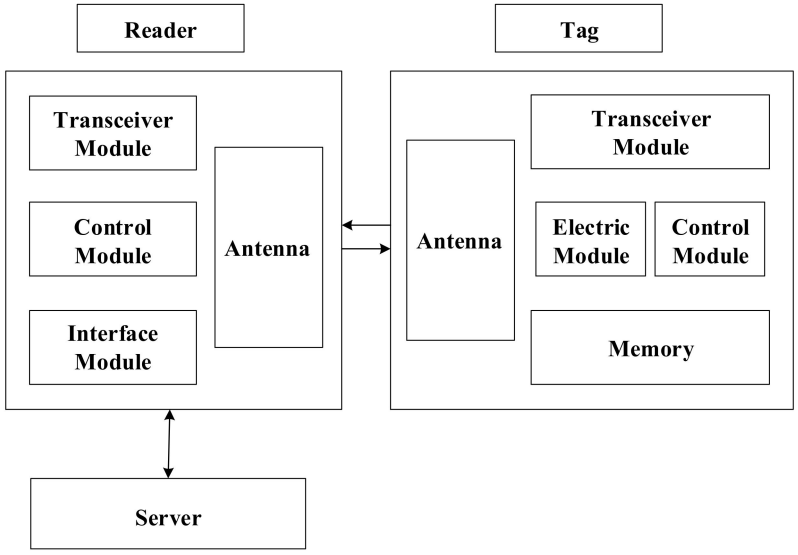

Figure 1. The communication components of the radio frequency identification system.

Near Field Communication (NFC) is a new and developing communication technology, which is often used in mobile IoT network. It primarily works in the 13.56 MHz band with a data transmission speed of 106–424 kbps. NFC is inherited from RFID, and like RFID, it works on special chips and communicates with other devices through antennas. The difference between NFC and traditional RFID is that NFC emphasizes short-distance contactless communication. It uses a unique signal attenuation technology and the effective radio range is below 20 cm. NFC is designed to provide a low-cost, high-bandwidth, low-energy communication method for mobile devices in IoT. It can be applied to various situations such as electronic payment, identity authentication, logistics tracking, and data collection in mobile IoT [3].

The motivation of our study of NFC authentication protocol is the security requirement and communication overhead during the authentication in mobile IoT networks. In the paper, we propose a new lightweight NFC identity authentication protocol for mobile NFC IoT networks. The protocol can achieve the access control and management of NFC devices from a system view with the double key-management model. Such a model has never been seen in previous NFC/RFID authentication protocols. Our work can provide a secure and lightweight mobile authentication service in the NFC-based mobile IoT network, such as smart homes and Office attendances. Our protocol includes the following advantages:

- Our protocol needs less computational overhead and memory storage. Only the XOR and Modulo-Plus function are included in our protocol without hash or other encryption operations. The most complicated operation in our system is the random number generation.
- Our protocol can resist typical attacks in the IoT environment such as denial of service (DoS) attacks, de-synchronization attacks, replay attacks, and identity leakages. The protocol also achieves tag anonymity and the mutual authentication of the IoT system.

2. Relative Works

For any network, identity authentication and identity trust are the key considerations because security threats are diverse and complex. There are many research articles [4–9] focusing on solving the security issues in IoT, such as intrusion detection in sensor networks and trust models in networks. Even machine learning has been applied to help defeat security threats [10]. In addition, the human factor is also an important subject which attracts the attention of researchers [11].

Identity authentication is also very important in radio frequency communication and can be used against complex security threats [12]. There are some protocols proposed to solve the identity

authentication problem in the IoT. To make the protocol safer, these protocols use strong encryption operations excessively, such as symmetric encryption and the hash function [13–15].

Later, researchers found that the abuse of encryption often results in a high communication overhead and requires high hardware resources [16–18]. On the other hand, with the development of society, people are increasingly concerned about their privacy and security, and the requirements for privacy protection are getting higher. Some researchers are working on privacy protection and tag anonymity in authentication [19–21].

In 2015, Baek and Youm proposed a secure and lightweight authentication protocol for NFC tag-based services [22]. Tags require less memory storage and computational overhead in the protocol. Moreover, they announced that the protocol effectively achieves security by preventing spoofing, DoS, data modification, and phishing attacks. However, the protocol still cannot resist the de-synchronization attack.

As we can see, all these lightweight protocols above still have many problems. In 2016, Gildas Avoine and Xavier Carpent offered us some recommendations in order to avoid some typical mistakes. This work, as a sanity check, can help designers of RFID, NFC, and sensor networks-based security solutions to improve the security, reliability, and longevity of lightweight authentication protocols [23].

When it comes to mobile IoT, especially when an authentication system contains phones, these protocols become less effective. Firstly, the mobile IoT prefers NFC technology for authentication. Secondly, the system model is also complex. An NFC phone can work in a tag mode and a reader mode, the role of the device in mobile IoT is changeable and uncertain. Thirdly, people have higher requirements for the anonymity and privacy of the IoT in which mobile devices participate in. Lastly, battery power limitations, communication overhead, and hardware costs are also important considerations for mobile IoT.

2.1. The Requirements of Mobile IoT

An NFC system is mainly composed of three parts: NFC tags, an NFC device, and a cloud server. Tags are used to collect data in the IoT environment, the NFC device is just like readers, it is used to retrieve data from tags. The cloud server is used to authenticate tags and readers, and even the stored data read from NFC devices [16,24]. When we want to achieve authentication between devices, we mainly focus on the following two requirements.

2.1.1. Security Requirements

Compared to a traditional RFID reader in an authentication system, NFC-enable devices make the message reading much easier. However, such devices also bring some security problems. On the one hand, it can deal with the events in real-time and undertake the process faster and more efficiently. On the other hand, although short distance communication enhances the privacy property, the mobile IoT network still leads to many security challenges.

In an unsafe authentication system, an attacker can interact with a tag to uncover its identifier and then deduce the nature of the product it is attached to. Weaker attacks can also compromise privacy [16]. Meanwhile, some typical attacks, such as DoS attack, replay attack, forgery attack, may exist in the system.

In a secure authentication system, the following requirements are often considered [25]:

- Tag Anonymity: A tag's identity should be protected during the transmission on the channel.
- Prevent Replay Attacks: Even if attackers can get legitimate messages sent from the tag to the reader, the data cannot be sent repeatedly to trick the authentication server.

Prevent Denial of Service Attacks: Even if attackers send lots of authentication messages to paralyze the system, the authentication system can still provide a service.

- Mutual Authentication: Each party in the system is able to confirm that the other parties are legitimated.

- User privacy: Even if an attacker can get legitimate information sent from the tag to the reader, the tag's identity and other private information remain confidential.
- Prevent Man in the Middle Attack: Even if attackers can sniff the data transportation in the communication channel, they cannot get any useful information after analysis.

2.1.2. Lightweight Requirements

A low overhead can reduce costs and time consumption and we can see that the lightweight requirements are crucial. In the past, we relied too much on various encryption methods to solve the security problems during the authentication. As a result, the overhead of the protocol was very high. The balance between the overhead and security are highly important in an authentication system. We focused on two aspects in order to achieve the lightweight requirements in the system.

Computational cost should always be considered. The hash function and some symmetric encryption operations always bring about a large computational cost. This means that if we use these operations in an authentication system, a tag would spend more time and use more electric power to deal with the data.

Meanwhile, the memory cost is also an important part. The more data a tag stores, the more manufacturing costs a tag will require.

2.2. System Model

The IoT network contains many authentication systems. The traditional radio frequency identification authentication system in IoT consists of three parts: the tag, reader, and server. Readers authenticate tags. The cloud server is an essential part of the authentication system. As a trusted third party, it verifies or decrypts the authentication messages [26]. The cloud server also stores authentication information, such as the device keys and device identities. There may be a large number of tags in a system, but the number of readers and servers is small. Such a single system is in a kind of pyramid structure. When it comes to mobile IoT, the structure changes. For the NFC mobile IoT network, the system contains a cloud server and multiple NFC devices, such as NFC tags, NFC phones, NFC watches, special NFC readers, and many other NFC smart devices. Here we have to point out that NFC mobile phones are very special. The NFC mobile phone has three working modes that it can work in: it can work in the card mode as a tag, in the reader mode, and it can also support peer-to-peer file sharing between phones. There may be authentication requirements between devices so the relationship becomes confusing. Such a system is a kind of reticular structure. In order to achieve the interconnection of the devices, the mobile IoT must consider how to achieve mutual authentication between the devices while providing security services. There are many studies focus on the authentication model for IoT clouds. They consider the authentication from the cloud point of view, such as the authentication model for IoT clouds that Luciano Barreto has proposed. Barreto's work is a perfect summary of the previous IoT authentication protocols and it will also be of great help to future research [27].

We notice that although the relationship is complex, devices in IoT can be divided into different groups that rely on their authentication systems. They have clustering characteristics, which means that they belong to a system and provide the same service. Let us take the smart home as an example. In such a typical mobile IoT network, all the NFC devices in the house only serve that particular family. Any device from outside is illegal in the network. Figure 2 shows the clustering characteristics of the mobile authentication system in the smart home.

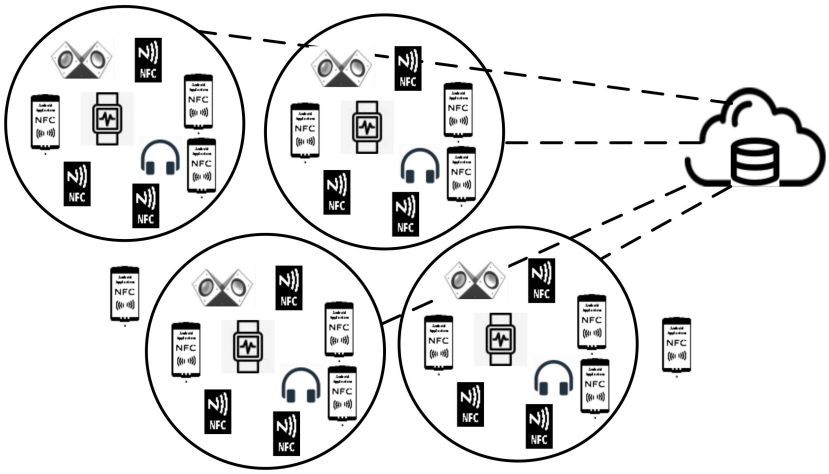

Figure 2. The groups in the mobile Internet of Things (IoT) network. NFC: near field communication.

A system with clustering characteristics has three features. Firstly, devices outside the clustering system are considered illegal if they attempt to participate in authentication. Secondly, only when the authentication begins can we know the role of the devices. For example, when the mobile phone wants to authenticate the tag, the mobile phone acts as a reader. When mobile phone X authenticates mobile phone Y, phone X acts as a reader and phone Y acts as a tag. Thirdly, a legal device in the group cannot forge the identity of other devices. Figure 3 shows the detail of the system model.

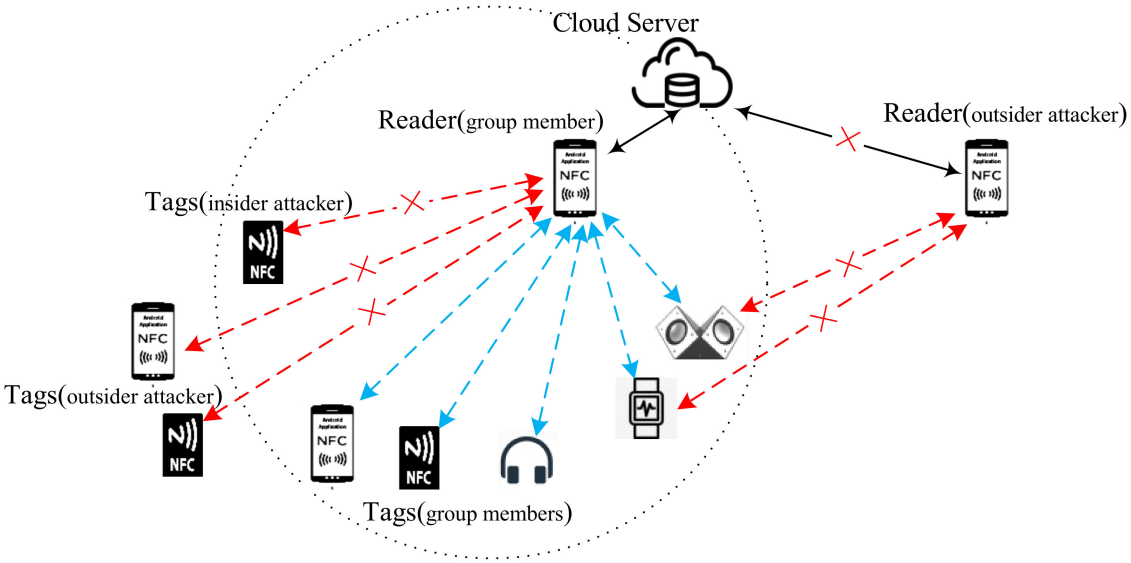

Figure 3. The authentication in the mobile IoT network.

In the next section, we propose a group-based lightweight authentication protocol from the perspective of the relationship between tags and mobile devices in the mobile IoT. The clustering characteristics in the IoT system give us inspiration. Using the group-based access control, the protocol can be well protected against replay attacks, tag forgery, and other security issues. Meanwhile, devices in the group are anonymous to each other, which protects the privacy of the devices. Our lightweight protocol does not use strongly encrypted arithmetic units, but still provides a high level of security.

3. Lightweight NFC Protocol for Privacy Protection in Mobile IoT

3.1. Key Management System Model

Here we propose a new key management model used in our protocols. Each device in our system holds two kinds of keys, the group key and device key. We assign the group key to the devices in a the same NFC system as if a secret shared by members of the group. For an NFC system, this may include a large number of tags, some readers, and an authentication cloud server. The cloud is trusted and provides authentication services to the NFC devices. This is a prerequisite for further authentication and any data encrypted with the group key can be decrypted and verified by others members. The group key is used to overcome outside attackers and can only be distinguished if a device belongs to the group. In order to overcome the insider attack and achieve mutual authentication, it is also necessary to distinguish the different devices in the group. Thus, the private device key is used to distinguish the identities and encrypt the message. On this basis, we have achieved mutual authentication and access control between the devices. Figure 4 shows the details of the model.

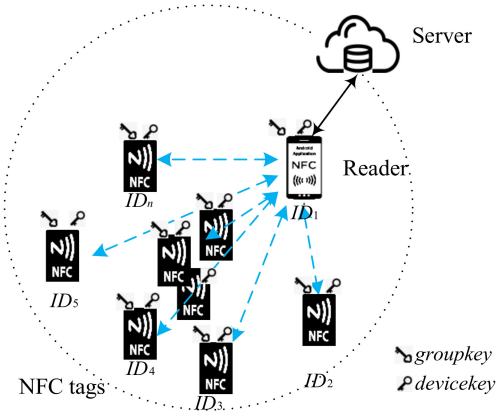

Figure 4. Our key-management model in the mobile IoT authentication system.

3.2. Notations

It is necessary to declare the notations and their meanings used in the protocol. The details of notations are shown in Table 1.

Table 1. The notation descriptions. NFC: near field communication; *XOR*: exclusive or

Notation	Description
Query	The startup flag of the authentication protocol
IDt	The identification of an NFC tag
IDp	The identification of a Mobile Phone
mt, mt'	Random numbers generated by a tag
mp, mp'	Random numbers generated by a phone
ms, ms'	Random numbers generated by the cloud server
VID	The virtual identification generated by an NFC device
VID'	The old virtual identification of an NFC device
Kt	The device key owned by a tag
Kt'	An old device key owned by a tag
Kp	The device key owned by a phone
Kgroup	The group key owned by a valid member
PRNG()	The Pseudo Random Noise Generation function
$\oplus$	The bitwise *XOR* operation
$\|\|$	The concatenation operation
$+$	The modulo-plus operation
Token	An authenticate credential generated by the cloud server

3.3. Registration

The proposed protocol contains three roles: NFC tags, the NFC phone, and the Cloud Server. The registration must be done before authentication.

The purpose of registration is to distribute the keys of each party and record the device's information into the database. Each device has a pair of keys: a group key and a secret device key. The detail of registration is following.

3.3.1. NFC Tag Registration

The NFC tags represent the IoT devices with NFC chips which are used to collect data in the IoT. NFC chips contain ID information when they are manufactured. The registration details are as follows:

1. The IoT devices with NFC chips initiate registration requests to the server through a reader.
2. After the server receives the message and records the information of the NFC tag, it generates the device key Kt and the group key $Kgroup$.
3. The NFC chip downloads a pair of keys and sends the ACK information to the cloud server.
4. After receiving the information, the server updates the items in the database.
5. Finally, the tag has the following: IDt, Kt and $Kgroup$. Registration is complete.

3.3.2. NFC Reader

Here, the NFC phones represent the readers in the IoT authentication system. The registration details are the following:

1. The NFC-enabled phone sends a request to the cloud server for private key generation. The request contains its identity information (IDp).
2. After the server receives the messages, it generates the phone's private key Kp and initializes $Kp\prime$, $VIDp$, $VIDp\prime$, and records them in the database. Then, the server sends Kp to the phone.
3. After the phone receives Kp, it sends a group key distribution request.
4. After the server receives the request, it sends the $Kgroup$ to the phone. The server also records the phone's $Kgroup$ in the database.
5. Once the phone receives $Kgroup$, the registration is completed. After that, the phone has finished the registration and has the following: IDp, $Kgroup$ and $Kphone$.

3.4. Data Table in Server

The server preserves a data table which contains the message of devices in the authentication system. In our protocol, the records of the tags and phones are in the same data table, as indicated by Table 2.

Table 2. The data table in the server.

ID	***VID***	***VID′***	**Group Key**	**Device Key**	**Device Key′**
$IDp1$	$IDp1 \oplus Kp1$	$IDp1 \oplus Kp\prime 1$	$Kgroup1$	$Kp1$	$Kp\prime 1$
$IDp2$	$IDp2 \oplus Kp2$	$IDp2 \oplus Kp\prime 2$	$Kgroup1$	$Kp2$	$Kp\prime 2$
...	...	...	...	...	...
$IDt1$	$IDt1 \oplus Kt1$	$IDt1 \oplus Kt\prime 1$	$Kgroup1$	$Kt1$	$Kt\prime 1$
$IDt2$	$IDt2 \oplus Kt2$	$IDt2 \oplus Kt\prime 2$	$Kgroup1$	$Kt2$	$Kt\prime 2$

As shown in Table 2, a device record contains 6 items, where the $VIDı$ and Device Key′ represent the device's virtual identity and device key in the last communication. Meanwhile, the VID and Device Key are the authentication messages used in the next session.

In addition, the group key determines which group the device belongs to. Such a design has two advantages. Firstly, the mobile authentication system may contain more than one reader. Secondly, some readers may change into tags. As mentioned, an NFC phone can work in both the reader mode and the tag mode. That is why we design the readers and tags in the same style.

3.5. The Proposed Protocol

Figure 5 shows the proposed authentication protocol. The details of the protocol are as following:

Step 1. In order to communicate with the tag, the NFC enabled device generates a random number mp, then encrypts mp with $Kgroup$ using the " $\oplus$ " operation and sends the authentication query $Query, Kgroup \oplus mp$ to the NFC tag.

Step 2. After the NFC tag receives the query from the phone, it gets mp. Then the tag uses the group key $Kgroup$ to encrypt the tag's identity. Then we have $Kgroup \oplus VIDt$. In the expression $VIDt = Kt \oplus IDt$, $VIDt$ represents the tag's secret identity. In addition, the tag generates a random number mt and then it calculates $Kt \oplus (mt||IDt \oplus mp)$. Lastly, the tag sends the two parts to the phone.

Step 3. After the NFC phone receives message $Kgroup \oplus VIDt||Kt \oplus (mt||IDt \oplus mp)$, it gets $Kt \oplus mt$ from the second part of the message and calculates $Kt \oplus mt \oplus IDp$. Afterward, we obtain $Kgroup \oplus VIDt||Kt \oplus (IDp \oplus mt||IDt \oplus mp)$ and encrypt this expression with the phone's private key Kp. We also add $Kgroup \oplus IDp \oplus Kp$ and IDp to the message. After that, the phone sends the following message to the authentication server: $VIDp||(Kgroup \oplus vid||Kgroup \oplus IDp||Kn \oplus (IDp \oplus mn||IDn \oplus mp)) \oplus Kp$.

Step 4. After receiving the message, the cloud server searches a set of values with $VIDp$ and gets $IDp, Kp, Kgroup$. Then the server decrypts the message and gets $VIDt$. After searching for $VIDt$ in the database, the server gets $IDt, Kt, Kgroup$. Lastly, the server gets mt, mp. During inspection and decryption, if the server finds that the identity of the device or tag is wrong, the protocol will stop. If the inspection and decryption pass, then the server generates a random number ms and also a $Token$, where $Token$ is equal to $(IDt + mt + ms) \oplus (mp + ms)$. Then the server calculates $(Token||Kt \oplus ms||mp) \oplus Kgroup \oplus Kp$ and sends the message to the NFC phone. After decryption, the phone sends the message to the tag.

Step 5. Step 5. After the tag receives the message, it gets ms. Then $Token\prime = (IDt + mt + ms) \oplus (mp + ms)$, if $Token = Token\prime$ and the tag can confirm that the server and phone are reliable. In the next step, the tag lets the server know that it has received the $Token$. The tag generates random number $mt\prime$ and calculates $Kt \oplus mt\prime||mt\prime \oplus ms$. Lastly, it sends the calculation result to the server through the phone.

Step 6. Once it has received the relevant message from the mobile phone, the server gets $mt\prime$ after decryption. The message can be divided into 2 parts. Each part can be used to verify the other. If the $mt\prime$ is right, the server can confirm that the tag has received the $Token$. In order to resist against brute attacks, we should make sure that Kt, Kp is changed after each communication. To do this we generate new device keys and synchronize them. The server generates $ms\prime, ms\prime\prime$ and then Update $Kt\prime, VIDt\prime, Kp\prime, VIDp\prime$. After that, the server generates a new $Kt, Kp, VIDt$ *and* $VIDp$. After completing the above steps, the server calculates $(Kt\prime \oplus ms\prime||mt\prime \oplus ms\prime||Kp\prime \oplus ms\prime\prime||mp \oplus ms\prime\prime, ACK) \oplus Kp\prime$ and sends it to the tag through the phone.

Step 7. Once it has received the message, the phone gets $ms\prime\prime$ from $Kp\prime \oplus ms\prime\prime||mp \oplus ms\prime\prime$ and then updates Kp as $Kp\prime \oplus mp + ms\prime\prime$. After that, the phone sends $Kt\prime \oplus ms\prime||mt\prime \oplus ms\prime, ACK\prime$ to the tag.

Step 8. Once it has received the relevant message from the mobile phone, the tag gets $ms\prime$ after decryption. The two parts of the message can be mutually verified. If $ms\prime$ is right, the tag updates Kt as $Kt \oplus mt\prime + ms\prime$. After that, the protocol is complete.

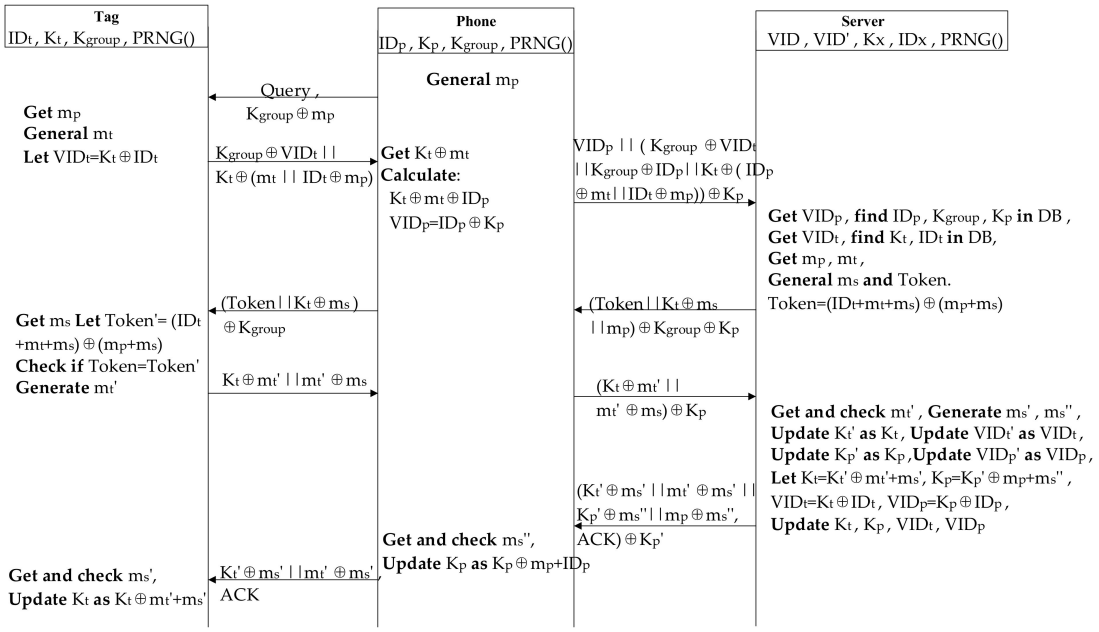

Figure 5. The proposed authentication protocol.

4. Security and Performance Analysis

4.1. Security Analysis

In this section, we give the security analysis of our protocol.

- Tag Anonymity

In an authentication system, we often use ID to distinguish the different devices. The ID represents the identity of a device in the IoT system. Once it receives a message, the server searches for the other authentication information by ID. If we send the ID directly in an unsafe channel, attackers may falsify the tag's identity or analyze the tag's behavior. The identity information is private information that should be protected. In our scheme, we use VID to protect the device's identity, which can be understood as encrypted ID information. VID maintains the anonymity to readers and even sniffing attackers. Even if the attacker gets the VID in some way, it does not make sense as the VID will also change after each communication. Anonymity is one of the requirements of a secure authentication system.

- Replay Attack Resistance

A replay attack refers to an attacker intercepting a certain step message on the communication channel and repeatedly transmitting and using it. In our scheme, we use random numbers to keep every message fresh. Even if the attacker obtains the data of the tag and the mobile phone communication in some way, the next communication's details cannot be predicted as we generate a random number each time. Thus, it can be seen that our protocol is effective against replay attacks.

- Consistent De-synchronization

From step 6 and step 8 we achieve the update and synchronization of the device key. In step 6, the server receives the message and generates the secret device key that is used for the next session. In step 7, we update the phone's secret device key. In step 8, we update the tag's secret device key. After doing this, the key synchronization is completed. Due to uncontrollable factors such as network problems, the tag and phone may not receive the Synchronization message, which will cause the de-synchronization problem. In order to solve the problem, the server side will also store the old device key while generating the new key.

- Mutual Authentication

The protocol also achieves the mutual authentication between the tags and the mobile phone, the mobile phone and the server, and the tags and the server. In step 4, after the server receives the message from the mobile phone, if it can be decrypted normally, the mobile phone and tag are considered legitimate. Then the server sends $mp \oplus Kp \oplus Kgroup$ to the mobile phone and sends $(Token||Kt \oplus ms) \oplus Kgroup$ to the tag. After checking this, the phone believes that the server is legitimate and then transmits $(Token||Kt \oplus ms) \oplus Kgroup$ to the tag. In step 5, after checking, the tag believes that the server is legitimate. On the other hand, if the tag receives the right message from the server, it means that the server believes that the phone is legitimate. Thus, the tag also believes that the phone is legitimate. Thus, our protocol achieves mutual authentication.

- Anti-DoS attack

The possible avoidance of denial of service attacks is shown in steps 4 and 6. In step 4, we solve the DoS problem by step-by-step querying: checking before computation. Once the server receives the message $VIDp||(\bullet||Kgroup \oplus IDp||\bullet) \oplus Kp$, it uses only one query and two XOR operations to check the phone's identity. Firstly, the server searches for $VIDp$ in database so that it can get the phone's information item. Then it checks if the IDp is right. If $VIDp$ does not exist in the database or if the check fails, the protocol will stop. Only after ensuring that the phone is legitimate does the protocol go to the next step. In step 6, the server uses three XOR operations to check if the message is legitimate. Only after ensuring that the message is legitimate will the server generate a new random number. From this point of view, the cost of these two steps is relatively small and this method can protect the interaction against the exhaustion of resources caused by the DoS problem.

4.2. Security Comparison

In this section, we select some typical protocols [10–12,15,16,18,19] to compare with ours. Table 3 shows the comparison results intuitively, where "√" means that the corresponding attribute is satisfied and "×" means that the corresponding attribute is not satisfied.

Table 3. The security performance comparison.

Authentication Protocols	Tag Anonymity	Replay Attack Resistance	De-Synchronization Attack Resistance	Mutual Authentication	Anti-DoS Attack
Chien Protocol [12]	×	√	√	√	×
Gossamer Protocol [15]	√	×	×	√	×
Xie Protocol [16]	×	√	√	×	√
Wang Protocol [10]	√	√	×	√	×
Wei Protocol [11]	√	√	√	×	×
Baek Protocol [19]	√	√	×	×	√
Sarah Protocol [18]	×	√	√	√	√
New Protocol	√	√	√	√	√

As we see from the Table 3, Chien, Xie, and Sarah's protocols do not guarantee the anonymity of the tags. Compared with those protocols, our scheme guarantees the anonymity of the tags and

readers. Our protocol also resists the de-synchronization attack, while Gossamer, Wang, and Baek's protocols cannot.

Meanwhile, Wei, Wang, Chien and Gossamer's protocols cannot resist DoS attacks, which means that the server involved in these protocols will face DoS threats. However, our protocol uses ultralightweight computational operations which can resist the DoS problem. Overall, the protocol we proposed can provide a high level of security for the mobile IoT system.

4.3. Performance Analysis and Simulation

In Table 4, we compare the computational cost and memory cost, as well as cost functions of the protocols."Rot" and "$MixBits$" represent two different displacement operations, and "$PRNG$" represents the random number generator. "$Hash$" is the relative high-cost operation. As shown in Table 4, only Gossamer's protocol and ours avoid using the "$Hash$" function. Compared to Gossamer's protocol, our protocol uses fewer computation operations and less computation time. Our protocol costs relatively less computational resources. When it comes to the memory cost, our devices need to store two keys and an ID, which will bring a higher storage overhead compared to the protocols with hash operations. However, this problem can be overcome because the storage overhead is related to the length of the keys and the ID. Our protocol's memory cost is consistent with Gossamer's. Overall, our protocol has a smaller resource cost.

Table 4. The cost comparison.

Protocol	Cost Function	Tag's Computational Cost	Tag's Memory Cost
Gossamer protocol	$\oplus$, $+$, Rot^2, $\|\|$	4$\oplus$, 18$+$, 10Rot, 3$MixBits$	3
Xie protocol	$\oplus$, $\|\|$, $Hash$	1$\oplus$, 4Hash, 1PRNG	3
Sarah protocol	$\oplus$, $\|\|$, $Hash$	2$\oplus$, 5Hash, 1PRNG	2
Wang Protocol	$\oplus$, $\|\|$, $Hash$	1$\oplus$, 3Hash, 1PRNG	1
Wei Protocol	$\oplus$, $\|\|$, $Hash$	5$\oplus$, 3Hash, 1PRNG	2
Baek protocol	$\oplus$, $\|\|$, $Hash$	2$\oplus$, 2Hash, 1PRNG	2
New protocol	$\oplus$, $+$, $\|\|$	9$\oplus$, 4$+$, 2PRNG	3

In order to get the computational consumption of the tags in our protocol, we simulated the tag's communication on the field programmable gate array (FPGA) simulation platform (Software Version: vivado 2017.3(64 bit); Virtual Board Version: Kintex-7:xc7k70tfbv676-1; Xilinx, Silicon Valley, California, US, 2017) shown in Figure 6.

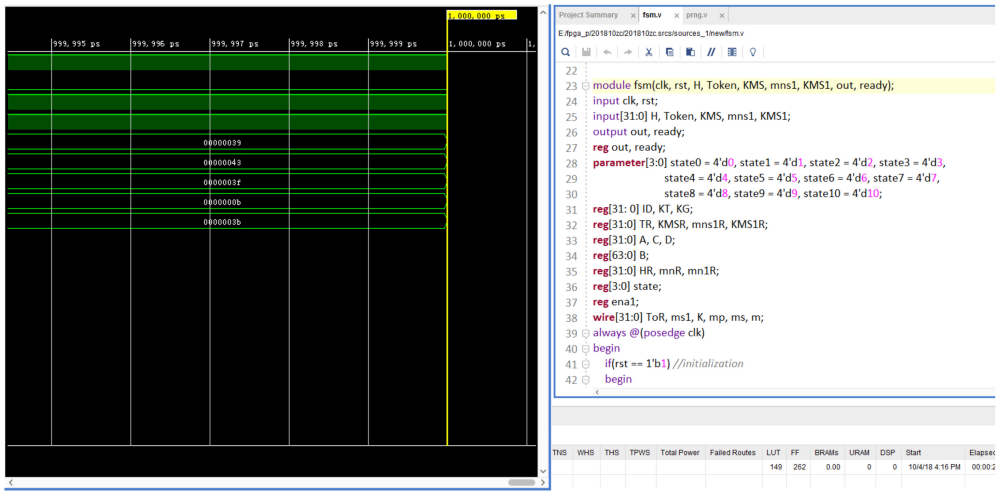

Figure 6. The proposed authentication protocol.

Table 5 shows the synthesis report (resource utilization) of the proposed design on Kintex-7 with 32-bit input data, where the "Available" column denotes the available resources provided by the FPGA system whereas the "Used" column shows the computational costs of the tag.

Table 5. The resource utilization of the proposed protocol for an FPGA. FPGA: field programmable gate array

Site Type	Used	Available	Utilization%
Slice LUTs	149	41,000	0.36
LUT as Logic	149	41,000	0.36
LUT as Memory	0	13,400	0.00
Slice Registers	262	82,000	0.32

As indicated in Table 5, the implementation of the Kintex-7 xc7k70tfbv676-1 device for 32-bit architecture occupied 149 LUTs and 262 slice registers. The utilization of the LUTs and registers in our scheme is less than 0.5%. The result shows that fewer resources are required for the tags.

Therefore, our authentication scheme is lightweight. Such a result is also shown in the NFC authentication.

5. Conclusions

Security and being lightweight are the two major requirements for the IoT. NFC is a developing communication technology used in mobile IoT. In this paper, we focus on how to use the lightweight NFC authentication protocol to solve privacy protection and some typical attacks under the mobile Internet of Things. We have proposed a lightweight NFC authentication protocol based on the clustering key-management model. A security analysis shows that our protocol can achieve device anonymity that prevents privacy leakage. The protocol can also resist replay attacks and the de-synchronization problem. The cloud server in the system also resists DoS attacks. Besides, our protocol only uses XOR operations or random numbers to encrypt and decrypt the message. A performance analysis and simulation show that the protocol reached the lightweight requirements. Our protocol can be used in many typical mobile IoT networks, such as smart-homes and school attendances. Although the protocol is designed for NFC mobile IoTs, it can also work in RFID authentication systems and provide a lightweight privacy protection solution for traditional IoT networks.

The future work is to design an authentication protocol for a more complex situation, in which mobile NFC devices have multi-roles and belong to different authentication groups at the same time. This is essential to keep the balance between the resource costs and security requirements.

Author Contributions: Conceptualization, K.F. and C.Z.; Data curation, H.L. and Y.Y.; Formal analysis, K.Y., H.L. and Y.Y.; Funding acquisition, K.F. and H.L.; Investigation, K.F. and C.Z.; Methodology, K.F. and C.Z.; Project administration, K.F.; Writing-original draft, K.F. and C.Z.; Writing-review & editing, K.Y.

Funding: This work was funded by the National Key R&D Program of China (No. 2017YFB0802300), the National Natural Science Foundation of China (No. 61772403 and No. U1401251), Natural Science Basic Research Plan in Shaanxi Province of China (No. 2017JM6004), the Fundamental Research Funds for the Central Universities, and National 111 Program of China B16037 and B08038.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Sarawi, S.; Anbar, M. Internet of things (IoT) communication protocols: Review. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017; Volume 8, pp. 67–73.

2. Karam, Y.; Baker, T.; Taleb-Bendiab, A. Security Support for Intention Driven Elastic Cloud Computing. In Proceedings of the 2012 Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation, Valetta, Malta, 14–16 November 2012; pp. 67–73.
3. Ylinen, J.; Kostela, M.; Iso-Anttila, L. Near Field Communication Network Services. In Proceedings of the Third International Conference on the Digital Society, Cancun, Mexico, 1–7 February 2009; pp. 89–93.
4. Otoum, S.; Kantarci, B.; Mouftah, H.T. Detection of known and unknown intrusive sensor behavior in critical applications. *IEEE Sens. Lett.* **2017**, *1*, 1–4. [CrossRef]
5. Guan, Z.; Li, J.; Wu, L.; Zhang, Y. Achieving Efficient and Secure Data Acquisition for Cloud-supported Internet of Things in Smart Grid. *IEEE Internet Things* **2017**, *4*, 1934–1944. [CrossRef]
6. Otoum, S.; Kantarci, B.; Mouftah, H.T. Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017.
7. Du, X.; Xiao, Y.; Guizani, M.; Chen, H.H. An Effective Key Management Scheme for Heterogeneous Sensor Networks. *Ad Hoc Netw.* **2007**, *5*, 24–34. [CrossRef]
8. Otoum, S.; Kantarci, B.; Mouftah, H.T. Mitigating False Negative intruder decisions in WSN-based Smart Grid monitoring. In Proceedings of the 2017 IEEE 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017.
9. Du, X.; Guizani, M.; Xiao, Y.; Chen, H.H. A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks. *IEEE T. Wirel. Commun.* **2009**, *8*, 1223–1229. [CrossRef]
10. Otoum, S.; Kantarci, B.; Mouftah, H.T. Adaptively Supervised and Intrusion-Aware Data Aggregation for Wireless Sensor Clusters in Critical Infrastructures. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018.
11. Ghafir, I.; Saleen, J.; Hammouhed, M.; Faour, H.; Baker, T. Security threats to critical infrastructure: The human factor. *J. Supercomput.* **2018**, *74*, 4986–5002. [CrossRef]
12. Nyikes, Z. Information security issues of RFID. In Proceedings of the IEEE 14th International Symposium on Applied Machine Intelligence and Informatics, Harlan, Slovakia, 21–23 January 2016; pp. 111–114.
13. Wang, G.C.; Wang, Y.; Li, Y.Z. Authentication Protocol of RFID System Based on Security Policy. In Proceedings of the 2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control, Shenyang, China, 21–23 September 2013.
14. Yang, Y.; Zhen, L.; Chen, Z. Security Analysis of a Mutual Authentication Protocol for RFID Systems. In Proceedings of the IEEE 2th International Conference on Instrumentation, Measurement, Computer, Communication and Control, Harbin, China, 8–10 December 2012.
15. Chien, H.Y.; Chen, C.H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Comput. Stand. Interface* **2007**, *29*, 254–259. [CrossRef]
16. Thammarat, C.; Chokngamwong, R.; Techapanupreeda, C. A Secure Lightweight Protocol for NFC Communications with Mutual Authentication Based on Limited-Use of Session Keys. In Proceedings of the IEEE International Conference on Information Networking, Cambodia, Cambodia, 12–14 January 2015; pp. 133–138.
17. Maimut, D.; Ouafi, K. Lightweight cryptography for RFID tags. *IEEE Secur. Priv.* **2012**, *10*, 76–79. [CrossRef]
18. Bilal, Z.; Masood, A.; Kausar, F. Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol. In Proceedings of the 2009 International Conference on Network-Based Information Systems(NBIS), Indianapolis, Indiana, 19–21 August 2009; pp. 260–267.
19. Xie, W.; Xie, L.; Zhang, C. Cloud-based RFID authentication. In Proceedings of the 2013 IEEE International Conference on RFID, 30 April–2 May 2013; pp. 168–175.
20. Hameed, S.; Hameed, B.; Hussain, S.A. Lightweight Security Middleware to Detect Malicious Content in NFC Tags or Smart Posters. In Proceedings of the IEEE 13th International Conference on Trust Security and Privacy in Computing and Communications (TrustCom), Beijing, China, 24–26 September 2014; pp. 900–905.
21. Abughazalah, S.; Markantonakis, K.; Mayes, K. Secure improved cloud-based RFID authentication protocol. In Proceedings of the 9th DPM International Workshop on Data Privacy Management (DPM 2014), Vienna, Austria, 10 September 2015; pp. 147–164.

22. Baek, J.; Youm, H.Y. Secure and Lightweight Authentication Protocol for NFC Tag Based Services. In Proceedings of the 10th Asia Joint Conference on Information Security, Kaohsiung, Taiwan, 24–26 July 2015.
23. Avoine, G.; Carpent, X.; Hernandez-Castro, J. Pitfalls in Ultralightweight Authentication Protocol Designs. *IEEE Trans. Mob. Comput.* **2015**, *19*, 1–17. [CrossRef]
24. Baoyun, W. Review on Internet of Things. *J. Electron. Meas. Instrum.* **2009**, *23*, 1–7.
25. Chen, B.C.; Yang, T.C.; Yeh, H.Y.; Lin, C.C. Mutual Authentication Protocol for Role-Based Access Control Using Mobile RFID. *Appl. Sci.* **2016**, *6*, 215. [CrossRef]
26. Suzuki, Y.; Niigata, A.; Hamada, M. In-house practice of cloud-based authentication platform service focusing on palm vein authentication. *Fujitsu Sci. Tech. J.* **2016**, *52*, 8–14.
27. Barreto, L.; Celesti, A.; Villari, M.; Fazio, M.; Puliafito, A. An Authentication Model for IoT Clouds. In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Paris, France, 25-28 August 2015; pp. 1032–1035.