# Identity-Based Group Devices Authentication Scheme for Internet of Things

Jian Shen [⋆], Anxi Wang, Leiming Yan, Yongjun Ren, and Qi Liu

School of Computer and Software,
Nanjing University of Information Science & Technology, Nanjing, China 210044
s_shenjian@126.com,anxi_wang@126.com

**Abstract.** Internet of things (IoT) is used to provide real-time data collection and analysis of the target area by the cooperation of low-cost devices. The authentication towards multiple devices has become the research hot-spot considering of the requirement in real applications. Sensitivity and privacy of data have caused widespread concerns because low-cost devices are neither tamper-proof nor capable of performing public key cryptography efficiently. However, many researchers only focus on the authentication between two devices in the network. They ignore the authentication among group devices attached to one network. In this paper, we propose an identity-based group devices authentication scheme for IoT. Note that one device group to be authenticated consists of a group of smart devices. The personal digital assistant (PDA) as the group leader controls authentication operations in its group. From the security analysis, our scheme can resist to various attacks. In addition, the performance analysis shows that our scheme has lower computational cost than the existing scheme.

**Keywords:** Internet of things, group devices authentication, lightweight, practical.

## 1 Introduction

Internet of things (IoT) is the reasonable association of physical devices, vehicles, buildings, and other things which are equipped with electronics, software, sensors, actuators and so on. IoT enables these intelligent objects to collect and exchange data [3] [2] [11] for different usages. Nowadays, IoT can be widely used in all walks of life. It can collect the distributed information and connects everything in the world, so applications of IoT mainly includes the following areas: health-care, transport, logistics, smart home, and so on. Note that IoT has very broad application prospects and markets in these areas.

In IoT, each user can use electronic tags to connect real devices to the network. In the network, users can find one thing's specific location, running state

[⋆] corresponding author

MOBIMEDIA 2018, June 21-22, Qingdao, People's Republic of China

DOI 10.4108/eai.21-6-2018.2276595

and other parameters of interest. The cloud servers are usually used in IoT as service providers [14] to provide storage and computation services. Internet users on the network can use IoT for personnel management, centralized control, remote control and other similar control systems. At the same time, other major breakthroughs to smart cities can be achieved based on analyzing the collected data [13]. With the development of Internet technology, IoT can be widely used in smart home, so as to provide people with a higher quality of life. However, security issues can not be ignored, such as the theft of sensitive data leading to personal privacy leaks, illegal invasion of smart home, etc.. In addition, devices used in IoT are usually lightweight and have restrictions on resources such as storage, computation and so on. So applying non-lightweight public-key cryptography (PKC) to these devices is challenging. What's more, owing to the limit on the storage, the size of key should not be large. Compared with traditional systems, IoT is an easy target for attackers because communications are done in wireless environment. In this paper, we pay attention to data security and users' privacy protection by applying identity-based authentication protocol into IoT.

### 1.1 Related Work

In last decades, many security authentication schemes have been proposed for network security. We mainly introduce device authentication schemes in networks here.

In [4], Gupta *et al.* proposed an authentication protocol using elliptic curve cryptography, which can intercept malicious nodes outside the sensor network. However, the protocol uses computationally intensive operations that require huge memory, which may be impractical for resource constrained sensor networks. In [20], Zhang *et al.* proposed a hierarchical authentication and key management framework for hierarchical wireless networks. However, this solution is implemented between the leader nodes, and there is no authentication method for the common devices in the network. Later, the KDC based authentication scheme was proposed [19], which employs a trusted third party to assist the authentication operations. In [19], two devices agree a pair of keys and store the keys in their database. Note that devices can authenticate themselves so as to generate a session key for data transmission. The drawback of this scheme is the dependence on the trusted third party and the lack of scalability.

The limitation on devices presents big challenges to design secure authentication schemes. Note that ECC [10] achieves high level security with small key size [9] compared with RSA. Using small key size in authentication scheme can achieve higher computation efficiency and save bandwidth, memory and energy. It is obvious that ECC is more suitable for resource limited devices in IoT [7].

### 1.2 Main Contributions

A user can hold many intelligent devices with the control of a PDA. By collecting and analyzing the information from smart devices, the user sends control message to a specified device by PDA to complete the corresponding operation.

In this paper, we design a group devices authentication scheme for IoT. The main contributions of this paper are listed as follows:

- We propose an identity-based group devices authentication scheme. Devices deployed in the same intelligent system form a group. The identity of each device is used into the authentication operation to guarantee the network security before data collection and data analysis stage.
- We design a group conference key agreement scheme. Through the scheme, a conference key can be generated without consuming large amount of devices' energy resource. The generated key can be used to guarantee the security during the following data collection operations in IoT.

The rest of the paper is sketched as follows. In Section 2. we discuss some preliminaries. In Section 3, we propose a group authentication scheme to authenticate all devices with a PDA in the network. In Section 4, we provide rigorous security analysis. Then we provide the performance analysis in Section 5. Finally, we conclude this paper in Section 6.

## 2 Preliminaries

In this section, some necessary preliminaries are introduced, including elliptic curve cryptography, Weil pairing and secret sharing scheme.

### 2.1 Elliptic Curve Cryptography

In the ECC cryptography system [6], the elliptic curve equation is defined as $E_p(a, b) : y^2 = x^3 + ax + b(mod\ p)$ over $F_p$, where $b \in F_p$, $p > 3$ and $4a^3 + 27b^2 \neq 0(mod\ p)$. In general, the security of ECC depends on the following difficult problems.

**Definition 1** *For two different points $P$ and $Q$ over $E_p(a, b)$, the elliptic curve discrete logarithm problem (ECDLP) [5] is to find an integer $s \in F_p$ such that $Q = sP$.*

**Definition 2** *Given three points $P, sP$ and $tP$ over $E_p(a, b)$ for $s, t \in F_p$, the CDH problem [16] is to find the point $(st)P$ over $E_p(a, b)$ without knowing $s$ and $t$ [1].*

**Definition 3** *$G$ is a generator of $G_1$ and $G_2$ is the subgroup of $F_{p^2}$ containing all elements of order $q$. A modified Weil pairing is a map $\hat{e} : G_1 \times G_1 \to G_2$. The properties of the map have been shown in [15].*

### 2.2 Secret sharing

The secret sharing (SS) scheme was proposed by Shamir in 1979 [12] which has been considered as one important tool in information security. In this paper, we use the SS scheme to accomplish group device authentication. In this subsection, we give an overall review of SS scheme. Note that $n$ users, a server and two algorithms are included. In the generation algorithm, server $S$ selects a random polynomial function $f(x) = a_0 + a_1x + a_2x^2 + ... + a_{t-1}x^{t-1}$ and sets $s = f(0)$. Then, users send their public messages $x_i$ to $S$. After getting users' public messages, $S$ computes $f(x_i)$ and returns it to users via a secure channel. In the reconstruction algorithm, each user broadcasts $f(x_i)$ to other users in the system. Each user attempts to recover $s$ by Lagrange interpolating formula. If the recovered value is equal to $s$, participating devices are certified; otherwise, authentication failed. Security requirements of the SS scheme are as follows: 1) Anyone can reconstruct $s$ with $t$ or more than $t$ shares. 2) No one can get anything about $s$ with fewer than $t$ shares.

## 3 Group Devices Authentication Scheme

In this section, group devices authentication scheme in IoT is introduced in detail, which is available for multiple lightweight smart devices. Note that smart devices in one group are controlled by a PDA. In our assumption, smart devices in a smart home system have no need to transfer data packages to the credible service provider (CSP). The PDA plays the role of collecting data from devices and uploading to the CSP. Similar to heterogeneous wireless sensor networks (HWSNs), the data upload operation is completed by cluster head nodes [17]. Smart devices communicate with the CSP according to their identities and communicate with the PDA according to their public keys. The CSP gathers secret information from devices and generates the proof by secret sharing scheme. The notations used in our scheme are described in Table 1.

**Table 1.** Notation used in the group devices authentication scheme

| Notation | Interpretation |
|---|---|
| $CSP$ | Credible service provider |
| $PDA$ | Personal digital assistant |
| $SD_i$ | The $i-th$ smart device |
| $f(x)$ | A random $(n-1)th$ degree polynomial function |
| $h(x)$ | A one-way hash function |
| $r_{SD_i}, r_i$ | The pseudo-random number generated for $SD_i$ |
| $ID_{SD_i}$ | The identity of $SD_i$ |
| $P_{CSP}$ | The public key of the CSP |
| $E_p, Z_p$ | The number fields |
| $TempID_{SD_i}$ | The temporary identity of $SD_i$ |
| $f_{SD_i}, SS_{SD_i}$ | The shared secret of $SD_i$ |
| $a_0$ | The secret of the CSP |
| $GSK_{CSP}, GSK_{PDA}$ | The generated conference key between the CSP and the PDA |

It is assumed that a large set of group needs to be authenticated where smart devices are assigned in network areas. Moreover, the CSP and the PDA can generate session keys with the help of authorized devices for data uploading.

### 3.1 Scheme Design

Note that there are $n$ smart devices in our scheme. $SD$ denotes the set of smart devices. Device $SD_i \in SD, i = 1, 2, ..., n$. $SD_i$ is registered at the CSP and is controlled by the PDA to form a group. The polynomial function $f(x) = \sum_{i=0}^{n-1} a_i x^i$ generated by the CSP is a random $(n-1)th$ degree function. When the input of $f(x)$ is 0, the output is $a_{CSP}$ which is the secret shared by the CSP. Each smart device obtains a part of $a_{CSP}$ by sending tokens to the CSP. Note that the authentication operation is executed by the PDA after collecting each device's $f_{SD_i}$. Here, the group devices authentication scheme can be divided into the initialization phase, device login phase, group authentication phase and key agreement phase. There are three parts involved in our scheme including the CSP, the PDA and devices. In the initialization phase, each part of the system generates necessary information which will be used in the device login phase, group authentication phase and key agreement phase. Then, smart devices will get the shared secret from the CSP in the device login phase. Next, the PDA calculates $a_{CSP}^{'}$ from received tokens and compares it with $a_{CSP}$ which is obtained from the CSP. If two values are equal, the authentication phase is successful. Otherwise, the PDA will run adversary detection operation. At last, the PDA and the CSP generate a session key for data uploading with the help of smart devices.

**Initial Phase** The initial phase is done by the CSP, the PDA and SD as follows. $SD_i$ selects a random number $x_i$ in a finite field $GF(p)$. Then, $SD_i$ sends $\{ID_{SD_i}, x_i\}$ to the CSP. The CSP selects an elliptic curve $E_p$ over $Z_p$, $p$ being a large prime. Then, the CSP selects a base point $P$ of order $d$ over $E_p$ such that $d * P = O$. The CSP also chooses its private key $r_{CSP}$ and computes the corresponding public key $P_{CSP} = r_{CSP} * P$. Note that the CSP selects a polynomial function of $n-1$ degree: $f(x) = \sum_{i=0}^{n-1} a_i * x^i \ mod\ p$. A collision-resistant one-way cryptographic hash function $h()$ is selected by the CSP too. The PDA generates the private key $r_{PDA}$ and computes the public key as $P_{PDA} = r_{PDA} * P$. An encrypt function $Encry()$ and a decrypt function $Decry()$ are selected by the CSP. At the end of this phase, the CSP broadcasts $\{p, GF(p), E_p, Z_p, P, P_{CSP}, h(), Encry(), Decry()\}$ to each participant in the system.

**Device Login Phase** In this phase, smart devices register after exchanging messages with the CSP. The PDA needs to collect information from all devices to authenticate devices. Here, $n$ devices are registered at the CSP and are assigned into one group by the PDA. If one device does not provide the right part of the shared secret, the authentication scheme can not pass. As a consequent, the PDA and CSP cannot get the same session key and the adversity detection operation will be performed by the PDA. The device login phase are introduced as follows:

- $SD_i$ randomly selects two numbers $r_{SD_i}$ and $x_i$ for itself. Then $SD_i$ encrypts $x_i$ to obtain $x_{SD_i} = Encry(x_i, P_{CSP})$. Note that $SD_i$'s public key is calculated by $P_{SD_i} = r_{SD_i} * P$. Then $SD_i$ delivers $(ID_{SD_i}, x_{SD_i},)$ to the CSP via a public channel and broadcasts $P_{SD_i}$ to other devices.
- The CSP generates a random number $r_i$ for $SD_i$ and stores $(ID_{SD_i}, r_i)$ locally. Then, the CSP calculates $x_i$ by the private key $r_{CSP}$ according to $x_i = Decry(x_{SD_i}, r_{CSP})$. After getting $x_i$, the CSP takes $x_i$ as the input of $f(x)$ and gets $f(x_i)$. To avoid exposing the shared secret, the CSP encrypts $f(x_i)$ by $f_{SD_i} = Encry(f(x_i), P_{SD_i})$. In addition, the secret is $a_{CSP} = f(0) = a_0$. Finally, the CSP sends $(f_{SD_i}, h(r_i, ID_{SD_i}))$ to $SD_i$ and delivers $h(a_{CSP})$ to the PDA for authentication. After this step, each device obtains the shared secret and necessary information for the following steps.
- $SD_i$ computes $R_{SD_i} = h(r_i, ID_{SD_i}) * P$ and acquires $f(x_i)$ from $f_{SD_i}$ by its own private key $r_{SD_i}$. $SD_i$ stores $\{ID_{SD_i}, f(x_i)\}$ in its own database for special circumstances. Then, $SD_i$ calculates $SS_{SD_i} = Encry(f(x_i), P_{PDA})$ and sends $(SS_{SD_i}, R_{SD_i})$ to PDA via a public channel.

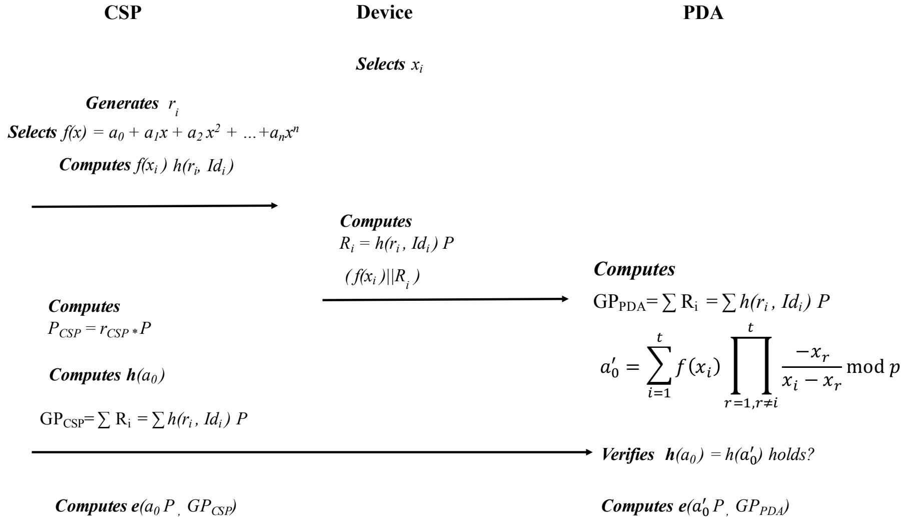
CSP
Device
PDA
Selects $x_i$
Generates $r_i$
Selects $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$
Computes $f(x_i)$ $h(r_i, Id_i)$
Computes
$R_i = h(r_i, Id_i) P$
$(f(x_i)||R_i)$
Computes
$GP_{PDA} = \sum R_i = \sum h(r_i, Id_i) P$
$a'_0 = \sum_{i=1}^{t} f(x_i) \prod_{r=1, r\neq i}^{t} \frac{-x_r}{x_i - x_r} \bmod p$
Computes
$P_{CSP} = r_{CSP} * P$
Computes $h(a_0)$
$GP_{CSP} = \sum R_i = \sum h(r_i, Id_i) P$
Verifies $h(a_0) = h(a'_0)$ holds?
Computes $e(a_0 P, GP_{CSP})$
Computes $e(a'_0 P, GP_{PDA})$

**Fig. 1.** Group authentication phase of the authentication scheme

**Group Authentication Phase** The main task of this phase is completed by the CSP and the PDA with unconstrained resource. This phase plays the most important role in the whole scheme. The PDA gathers shared secrets from devices and authenticates devices by comparing with $h(a_{CSP})$. Instead of using devices$'$ real $ID$s, we use the temporary identity $TempID_{SD_i} = h(r_i, ID_{SD_i})$ which is the hash value of a random number $r_i$ and the real $ID_{SD_i}$. The $TempID_{SD_i}$ of device $SD_i$ is obtained from the CSP at the login phase and transferred to the PDA by $SD_i$ at the beginning of the group authentication phase, which provides strong resistance to the tracing problem on smart devices. In addition, the random number $r_i$ is selected by the CSP and will be upgraded at the next round. In this phase, when devices make no response. the PDA will wait until the timer expires. If the PDA does not receive enough shared secret parts from devices, the PDA will send some empty packets to the CSP to get enough parts of shared secret, which makes the authentication scheme more efficient. Note that the number of empty devices is less than $n-1$. The main steps of the group authentication phase are shown as follows:

- After receiving $(SS_{SD_i}, R_{SD_i})$ from each device, the PDA computes group devices key by aggregating $R_{SD_i}$ $(GP_{PDA} = \sum_{i=1}^{n} R_{SD_i} = \sum_{i=1}^{n} h(r_i, ID_{SD_i}) * P)$.
- Then, the PDA resolves $f(x_i)$ from $SS_{SD_i}$. After getting enough parts of shared secrets, the PDA uses Lagrange interpolation method to calculate $a_0^{'} = \sum_{i=1}^{n} f(x_i) \prod_{r=1, r\neq i}^{n} \frac{-x_r}{x_i - x_r} \bmod p$.
- At last, the PDA compares $h(a_0^{'})$ with $h(a_{CSP})$. If $h(a_0^{'})$ and $h(a_{CSP})$ are equal, all devices pass the authentication scheme. In addition, the group session key between the CSP and the PDA will be computed if the authentication scheme succeeds.

The above three steps will be stopped if the authentication phase fails. And the PDA starts the fault detection. The fault detection process is ignored in our scheme, which can be done by referring to [18]. When all devices pass the authentication phase, the state of this system can be confirmed. We can guarantee the normal operation of the scheme by adding empty devices. In this way, some devices are not totally credible, but the network can still work well. In addition, the PDA will obtain identities of untrustworthy devices through the authentication information received from the CSP, which is very convenient for the operation of network maintenance without checking all devices in IoT. Fig. 1 gives the brief description of this phase.

**Key Agreement Phase** In the key agreement phase, the generated random number of $r_i$ as well as sequence numbers of all devices in IoT are covered into the group session key. The CSP computes $GP_{CSP} = \sum_{i=1}^{n} h(r_i, ID_{SD_i}) * P$ by itself. The PDA aggregates devices' information to compute $GP_{PDA}$ which has been introduced in step 1 of the group authentication phase.

The group session key is used to guarantee secure data uploading between the CSP and the PDA. The CSP computes $GSK_{CSP} = e(a_{CSP} * P, GP_{CSP})$

$= e(P,P)^{a_{CSP} * \sum_{i=1}^{n} h(r_i, ID_{SD_i})}$ and the PDA calculates $GSK_{PDA} = e(a_0^{'} * P, GP_{PDA}) = e(P,P)^{a_0^{'} * \sum_{i=1}^{n} h(r_i, ID_{SD_i})}$. It is obvious that $GSK_{CSP}$ and $GSK_{PDA}$ are equal if the shared secret is equal in each side.

## 4 Security Analysis

In this section, some security properties of our scheme are analyzed. Our scheme can resist various attacks, such as replay attack, eavesdropping attack, physical attack, man-in-the middle attack, and so on. Moreover, the scheme can also be used to track devices. The PDA controls and monitors the entire network changes in the authentication process.

- **Replay Attack.** In our scheme, replay attack is prevented by the selected pseudo-random numbers $r_{SD_i}$ and $x_i$. In the device login phase, $r_{SD_i}$ and $x_i$ are all selected by the smart device itself. The information communicated between the PDA and the device is protected by the random numbers. In the next authentication round, the device will change the value of $r_{SD_i}$ and $x_i$, so replay attack is prevented.
- **Eavesdropping.** The identity of the smart device and the secrets are encrypted during communication. Public key encryption are used to protect the communication between the device and the CSP. So the proposed scheme can resist to eavesdropping.
- **Physical Attack.** The smart device may be stolen by the adversary and all stored information can be exposed to the adversary. In this case, the PDA can still accomplish the authentication without the stolen device, since the SS scheme can guarantee the authentication with disable devices in the group. The adversary cannot interrupt the authentication operation unless it corrupt all the devices. This is difficult and worthless. Note that the PDA is assumed to be well protected. Physical attacks to the PDA is not taken into consideration in our scheme.
- **Man-In-The-Middle Attack.** Even if the communicated message sent by the device is blocked, the adversary cannot get $x_i$ and private key together owing to the public key encryption technology. The PDA will ask for message from other devices after a period time, and the authentication process can be operated without the blocked message. Hence, this attack is prevented by our design.
- **De-Synchronization Attack.** Devices' real IDs are hidden and random numbers are used to substitute real IDs in our scheme. The stored real ID in the device needs no update. If the information between the CSP and devices is not synchronized, the authentication operation will not succeed. Hence, smart devices in IoT are prevented from de-synchronization attack according to our design.

## 5 Performance Analysis

In this section, the performance of the proposed scheme is analyzed and simulated compared with b-SPECS scheme[8]. Simulation result shows that our scheme is more lightweight and practical.

According to the design of the group devices authentication scheme, each device receives messages from the CSP and sends messages to the PDA. After receiving these messages, the devices perform necessary operations including addition, pairing computation, point multiplication and so on. For the convenience of evaluating the total computational cost, we let $T_H, T_{AO}, T_{PC}, T_{PM}$ be the time cost of implementing a hash function, an addition operation, a modified Weil pairing and an elliptic curve point multiplication. As described in Section 3, the total computational cost in our group authentication scheme is $2T_H + 2T_{PC} + T_{PM} + 3T_{AO}$. The comparison between our scheme and b-SPECS scheme is shown in TABLE 2.

**Table 2.** Comparison results

| **Protocol Properties** | **Computational Cost** | **Round** | **Device Authentication** |
|---|---|---|---|
| b-SPECS [8] | $3T_H + 2T_{PC} + 6T_{PM} + 1T_{AO}$ | 3 | yes |
| Our scheme | $2T_H + 2T_{PC} + 2T_{PM} + 3T_{AO}$ | 2 | yes |

The performance of our scheme are simulated by using C programming language with the Pairing-Based Cryptography (PBC) library on a Ubuntu OS with Intel Core Xeon E5-2650M processors running at 2.60 GHz and 8 G memory, Ubuntu 14.04 X64. From the simulation result, the time required to perform a hash function, a pairing computation, a point multiplication and an addition is approximately 8.065 ms, 2.067 ms, 3.069 ms and 0.016 ms. The total time cost of each user in our scheme is $2 \times 8.065 + 2 \times 2.667 + 2 \times 3.069 + 3 \times 0.016 = 27.65ms$. Similarly, the total computational cost in b-SPECS can be computed as $46.779ms$.

The CSP and the PDA are the trusted third parts which do not consume resources from the smart devices. Therefore, the computational cost consumed by the CSP and the PDA are not taken into consideration. Fig. 2 shows that the computational cost increases as the number of devices increases. It is obvious that the computational cost in our scheme is lower than that in b-SPECS in different number of devices.

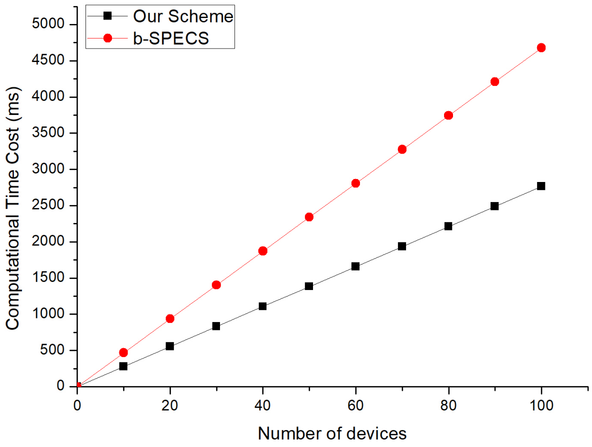

**Fig. 2.** Computational cost in different number of users

## 6 Conclusion

Deploying multiple devices in one group can not only increase the authentication success rate, but also increase the chance for accurate positioning, which satisfies the real application requirements. In this paper, an identity-based group devices authentication scheme is proposed. The authentication scheme is based on the SS scheme, which can efficiently assist the PDA to authenticate the group devices. In addition, an efficient conference key agreement scheme is designed to guarantee the security of data uploading between the PDA and the CSP. The security and performance analysis shows the better performance of our scheme compared with the existing scheme.

**Acknowledgments.** This work is supported by the National Science Foundation of China under Grants no. 61672295, no. 61672290, no. 61772280, no. U1405254; the State Key Laboratory of Information Security under Grant no. 2017-MS-10; the 2015 Project of six personnel in Jiangsu Province under Grant no. R2015L06; the CICAEET fund; and the PAPD fund.

## References

1. Dan, B., Franklin, M.: Identity-Based Encryption from the Weil Pairing. Society for Industrial and Applied Mathematics (2001)
2. Daz, M., Martn, C., Rubio, B.: State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. Journal of Network and Computer Applications 67(C), 99–117 (2016)

3. Floerkemeier, C., Langheinrich, M., Fleisch, E., Mattern, F., Sarma, S.E.: The internet of things. Electronics World 297(6), 949 – 955 (2017)
4. Gupta, S., Verma, H.K., Sangal, A.L.: Security attacks and prerequisite for wireless sensor networks. International Journal of Engineering and Advanced Technology (5), 558–566 (2013)
5. Gura, N., Patel, A., Wander, A., Eberle, H., Shantz, S.C.: Comparing elliptic curve cryptography and rsa on 8-bit cpus. In: CHES. vol. 4, pp. 119–132. Springer (2004)
6. Hankerson, D., Menezes, A.J., Vanstone, S.: Guide to elliptic curve cryptography. Springer Science & Business Media (2006)
7. Hassan, A., Iqbal, U.: Authentication protocols for wsn using ecc and hidden generator. International Journal of Computer Applications 133 (2016)
8. Horng, S.J., Tzeng, S.F., Pan, Y., Fan, P., Wang, X., Li, T., Khan, M.K.: b-specs+: Batch verification for secure pseudonymous authentication in vanet. IEEE Transactions on Information Forensics and Security 8(11), 1860–1875 (2013)
9. Kumar, S.N.: Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System (2015)
10. Lu, M.: Study on secret key management project of wsn based on ecc. Journal of Networks 7(4) (2012)
11. Misra, S., Maheswaran, M., Hashmi, S.: Securing the internet of things. Computer Fraud and Security 2016(4), 15–20 (2016)
12. Shamir, A.: How to share a secret. ACM (1979)
13. Shen, J., Liu, D., Liu, Q., Sun, X., Zhang, Y.: Secure authentication in cloud big data with hierarchical attribute authorization structure. IEEE Transactions on Big Data (2017)
14. Shen, J., Shen, J., Chen, X., Huang, X., Susilo, W.: An efficient public auditing protocol with novel dynamic structure for cloud data. IEEE Transactions on Information Forensics & Security (2017)
15. Shen, J., Wang, A., Wang, C., Li, J., Zhang, Y.: Content-centric group user authentication for secure social networks. IEEE Transactions on Emerging Topics in Computing (2017)
16. Shparlinski, I.: Computational diffie-hellman problem. In: Encyclopedia of Cryptography and Security, pp. 240–244. Springer (2011)
17. Wang, A., Pan, S., Wang, C., Shen, J., Liu, D.: A novel clustering solution for wireless sensor networks. In: International Conference on Green, Pervasive, and Cloud Computing. pp. 313–322 (2017)
18. Wang, Z., Karpovsky, M., Bu, L.: Design of reliable and secure devices realizing shamir's secret sharing. IEEE Transactions on Computers 65(8), 2443–2455 (2016)
19. Wen, X., Shao, L., Xue, Y., Fang, W.: A rapid learning algorithm for vehicle classification. Information Sciences 295, 395–406 (2015)
20. Zhang, J., Shankaran, R., Orgun, M.A., Sattar, A., Varadharajan, V.: A Dynamic Authentication Scheme for Hierarchical Wireless Sensor Networks (2012)