EURASIP Journal on Wireless Communications and Networking

RESEARCH

Open Access

A remote attestation mechanism using group signature for the perception layer in centralized networking

Jing Huang, Hui-Juan Zhang*, Shen He, Jia Chen and Zhe-Yuan Sun

*Correspondence: zhanghuijuan@chinamobile.com
Research Institute of China Mobile Communications Corporation, Beijing 100032, China

Abstract

As the important transmission approach of the perception data, the security and privacy of the perception layer nodes have been paid more and more attention. To evaluate the credibility of the perception nodes and protect autologous identity privacy, a remote attestation mechanism using group signature (GS-RAM) for the perception layer of centralized networking is proposed in this paper. First, a RAM, based on the computational Diffie–Hellman (CDH) problem and GS, is established for the data source of the perception nodes. Second, the specific construction of the proposed GS-RAM is given to identify the trusted state of data sources without exposing the privacy of the perception nodes. Then, a strict security certification was carried out to verify the correctness, unforgeability, anonymity, traceability, unrelatedness, non-framing, anti-joint aggression and forward security of the proposed GS-RAM. Finally, simulation experiments are carried out to verify that the proposed scheme has better security and dynamic adaptability.

Keywords: Perception nodes, Credibility, Identity privacy, A remote attestation mechanism, Group signature

1 Introduction

In recent years, with the continuous development of the Internet of Things (IoT), the devices in the Internet of Things have become a digital carrier to drive the rapid development of economy. The Internet of Things is designed to collect and transmit data and perform limited computing tasks. In terms of logical architecture, the Internet of Things can be divided into three layers, respectively, the perception layer responsible for information collection and terminal recognition, the network layer responsible for information transmission and processing, and the application layer responsible for intelligent control based on the network state combined with specific industries. Among them, the perception layer, as the source of data collection and information exchange [1], carries the work of information collection, identity authentication, data integration and forwarding. The perception layer plays a core role in the Internet of Things. As the starting point of data source of IoT, the security of the perception nodes are vital for the stabilization of IoT [2, 3].

As for the perception layer of the IoT, due to its heterogeneity and complexity. It is very vulnerable to be attacked by criminals, resulting in security threats to the source of the perceptual data [4, 5]. Ensuring the credibility of the perception nodes and the source of perception data is the cornerstone of ensuring the safe operation of the perception layer. Simultaneously, it is also one of the key issues that need to be solved at present. Therefore, the analysis and research on the security mechanism of the perception layer of the Internet of Things is crucial to the development of the ecology of the Internet of Things.

In order to verify whether the terminal is in a safe state, it is necessary to ensure the integrity of its underlying devices. A remote attestation can enable remote verification devices to verify the credibility of data source nodes. This technology is a key security mechanism after the extension of trusted computing technology to the Internet of Things. However, the current security mechanism for perceptual nodes is not universal and inefficient. Meanwhile, it is unable to guarantee the reliability of perceptual nodes.

So as to solve the issue that the current models lack of objectivity and dynamic, thereby cannot be contented with the current situation of the Internet of things. In this paper, according to the measurement results of perceptual nodes estimating trust status on trusted logical grouping to build a trusted group with different trust level. Based on the trusted logical grouping of the perception layer [6], a remote attestation mechanism using group signature (GS-RAM) for the perception nodes of centralized networking is proposed to ensure the credibility and protect the privacy in this paper. The experimental simulation shows that this mechanism has high operation efficiency and low computational performance consumption, the mechanism can effectively verify the state of the sensing data source. The main contributions of this paper are as follows.

1. A remote attestation mechanism (RAM), based on the CDH problem, is established for the data source of the perception nodes of centralized networking.
2. The specific construction of the proposed RAM is given to identify the trusted state of data sources and guarantee the privacy exposure of the perception nodes.
3. The security properties of the proposed GS-RAM, including the correctness, unforgeability, anonymity, traceability, unrelatedness, non-framing, anti-joint aggression and forward security, are testified.

The remaining parts of this paper are organized as follows. Section 2 is concerned with the related work. Section 3 introduces the preliminary knowledge about GS, bilinear mapping and the CDH problem. Section 4 describes the GS-RAM in detail. Then, the various security property certifications of the proposed GS-RAM are given to demonstrate the effectiveness of GS-RAM in Section 5. Simulation experiments are carried out to verify that the proposed scheme has better security and dynamic adaptability in Sect. 6. Section 7 concludes this paper.

2 Related work

Terminals in the Internet of Things usually sense, process and transmit perceptual information, which often contains sensitive data and is vulnerable to malicious attacks. Remote attestation is a key security mechanism after the extension of trusted computing technology to the Internet of Things, compared to the present authentication mechanism has many advantages. For example, the present identity authentication mechanisms can only meet a simple authentication, but also there is no way to make trustworthiness attestation on the properties and performance of the entire computing platform. Moreover, it cannot resist platform identity attack, forgery attack, conspiracy attack, etc. While through the remote attestation, the correctness and integrity of information can be checked. Besides, the remote verifier can complete the authentication of the whole platform in the process of interaction, and can verify the trusted state [7].

D. Boneh et al. proposed a short local verifier group signature based on the strong Diffie–Hellman hypothesis and the decision linearity hypothesis in bilinear groups. But it did not have backward irrelevance [8]. Brickell et al. was the first to propose a direct anonymous remote attestation scheme to protect the privacy of platform configuration in 2004. The scheme can be extended in many forms [9].The scheme proposed by Brickell et al. protected the privacy of signers through direct anonymous authentication, which solved some limitations. However, the scheme cannot revoke the identity of malicious nodes and does not protect platform configuration information [10]. Literature [11] proposed a attestation mechanism based on TPM to confirm platform identity by providing TPM data verification to users. It authenticate itself by using a certificate to accomplish remote attestation. The remote attestation selection platform uses AIK key to sign the PCR value of the environment state to complete the integrity measurement. The scheme proposed by Sailer et al. described the brief process of TCG for remote attestation. The prover sends the identity information and configuration information of the computing platform to the interrogator, and the interrogator checks the credibility and integrity of the prover according to the configuration information [12]. Literature [13] pointed out that in the process of remote attestation of TCG remote proof protocol, the prover would realize the attestation of the interrogator by signing its own configuration information. Awad et al. proposed a attestation mechanism based on TCG o ensure the integrity of the system by using TPM. The solution provided both hardware and software attestation. Software attestation verified system software and data, while hardware attestation detected tampering at the system level [14].

The simple remote attestation schemes described above use metrics as a state indicator of the system. However, these mechanisms have some issues, such as management problems caused by the complexity and variability of the system, security problems caused by digital signature using AIK as a measure, etc. The remote attestation mechanisms based on TCG still have some shortcomings, such as can't perform attestation dynamically and can't resist replay attack.

In order to solve these problems in TCG remote proof mechanism, the domestic and oversea scholars have carried out further research on remote attestation. Zhao et al. proposed a credential attestation scheme based on attribute certificates. By abstracting the attributes of the computing platform into certificates, privacy exposure was avoided and the efficiency of the attestation process was improved [15]. Awad proposed an attribute-based attestation scheme, which was easier to manage than the hashing attestation scheme in TCG specification. The solution also provided platform-specific integrity and identity authentication technology. However, the scheme is not perfect because it cannot be fully applied to the current situation of the perception layer [16]. Zhu et al. proposed a semantics-based remote attestation model, which combined semantics-based virtual machine technology with remote attestation. This model was independent and dynamic based on the platform [17]. Liu et al. proposed a remote automatic anonymous attestation scheme based on trusted computing, which achieved the purpose of anonymous attestation and privacy protection through ring signature. However, the scheme can not accurately abstract the external platform attribute value and external attribute certificate [18].

In conclusion, due to the application of the Internet of things is more and more widely. Especially, the IoT perceptual technology has become increasingly complex, the perceptual data has increased explosively. However, the present remote attestation mechanisms that applicable to the perception layer have not been fundamentally figure out these issues, such as how to effectively protect the privacy of authentication nodes' information. Therefore, we need to study a remote attestation scheme for data sources, which applicable to the perception layer of the Internet of Things.

3 Preliminary knowledge

3.1 Group signature (GS)

As shown in Fig. 1, the scheme of GS consists of four roles: group manager, group member, verifier and opener [19–22]. The group manager is responsible for the dispensation of signature key and member certificate for each group member. Group members with certificates can generate group signatures, and meanwhile maintain the autologous anonymity. The verifier can judge the legality of signature, but cannot identify the identity of signer. The opener can use the initial key to identify the signer of the corresponding signature, when the behavior of member is abnormal. The detailed procedures include:

1. Initialization: security parameters are considered as the input, and public/private key pairs of group manager and opener are regarded as the output;

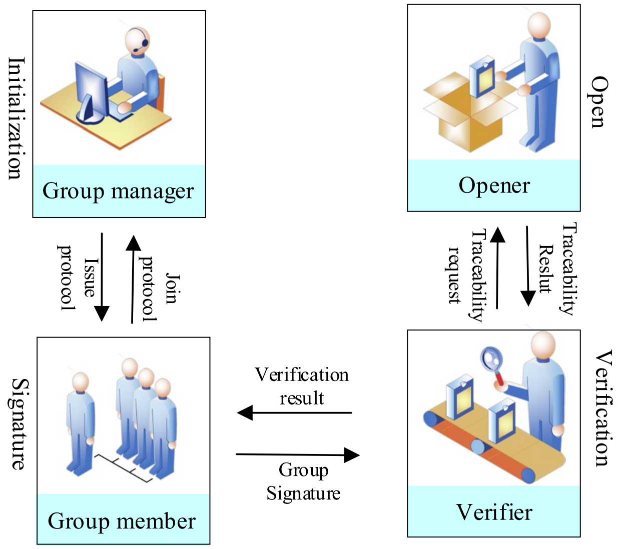


Fig. 1 The scheme of group signature. Describes the process of group signature. The scheme of GS consists of four roles: group manager, group member, verifier and opener [18–21]

2. Join: The group public key, private key of the group manager, the public key of the group member is the input, and output the group certificate corresponding to the public key of group member is the output;
3. Signature: The group public key, a message to be signed, the signature key of signer and the member certificate is the input, and the signature of the message is output;
4. Verification: The group public key, a message and the group signature of the message is the input, and the verification result of signature is output;
5. Open: The group signature and initial key is the input, and the confirmed identity result of opener is the output.

3.2 Bilinear mapping

$G_1 = <g_1>$ and $G_2 = <g_2>$ are defined as the multiplicative cyclic group of order p, p is a prime number, g_1 and g_2 are the generators of G_1 and G_2 respectively, e: $G_1 \times G_1 \rightarrow G_2$ is a computable mapping [23, 24]. if satisfies the following properties.

1. Bilinear: There is a mapping e: $G_1 \times G_1 \rightarrow G_2$ makes all αG_1, $\beta \in G_2$, $\forall x$, $y \in Z$ and exists $e(\alpha^x, \beta^y) = e(\alpha, \beta)^{xy}$.
2. Non-degeneration: There exists $g_1 \in G_1$, $g_2 \in G_2$, $e(g_1, g_2) \neq 1$.
3. Computability: For $\forall \alpha \in G_1$, $\forall \beta \in G_2$, there is an effective algorithm to calculate $e(g_1, g_2)$.
4. $G_1 \times G_1 \rightarrow G_2$ are the bilinear mapping.

3.3 The CDH problem

Given the group of $G = <g>$, If g, g^a, g^b are known and a, $b \in Z_p$, it is difficult to calculate g^{ab} when a and b are unknown [25, 26].

3.4 Remote attestation mechanism using group signature

The perception nodes should be credible, when transmitting data in a perceptual nodes group of centralized networking. In this proposed GS-RAM, to prove the credibility of this node, the trusted value and relevant data will be transmitted to remote verification node, which can determine the confidence of data source node, using the received information. When the data source node is in an untrusted state, the remote verification node can trace back to the superior node (management node) of the data source node to further evaluate the credibility of the data source node. Based on the final evaluative results, the remote verification node determines whether or not to interact (Shown in Fig. 2). The detailed processes are as follows:

1. In the perception layer of centralized networking mode, the superior node in a perception node group will perform a real-time trust measurement of the data source node. Then, the data source node formalizes the measurement value, timestamp and some other related attributes into a remote proof vector.

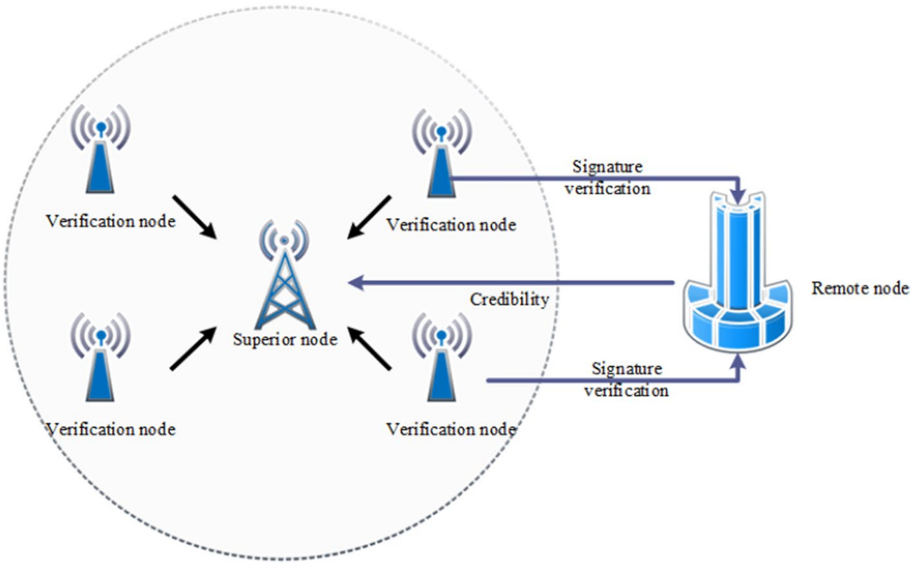


Fig. 2 The scheme of GS in centralized networking. Describes the processes of GS in centralized networking

2. When a member node in the node group is verified by the remote verification node, the data source node only needs to prove that it belongs to the trusted group, which can avoid the disclosure of node identity.
3. According to the security strategy of the remote verification node, the credibility of source node can be evaluated. The doubtful of source node can unfold its group signature to examine the corresponding information, or carry out the query from superior node of source node. If the result is unreliable, the data transmission of source node can be refused.

Remark 1 Comparing with some security mechanisms, the proposed GS-RAM can efficiently evaluate the credibility of data source node to ensure data transfer more secure between source node and remote node. Moreover, this GS-RAM obtains the characteristics of being measurable, traceable, monitored and extensible.

4 Construction of GS-RAM

This part describes the signing, verification and signature opening process of GS-RAM scheme. The symbol and corresponding meaning explanation can be summarized in Table 1.

(1) The parameters initialization of GS-RAM

GM initializes the information of GS-RAM, consisting of private key, public secret key and the corresponding function. First, GM sets a safety factor m and randomly selects a secret large prime Q. Specifying a bilinear mapping: e: $G_1 \times G_1 \rightarrow G_2$, $(G_1, +)$ and $(G_2, \cdot)$ are the cyclic groups of the order Q, G is the generator of G_1. Then,

Table 1 Symbol description of GS-RAM scheme

Mathematical symbols	Description
GM	Group manager
CIN_i	Group member
ID_i	Group membership information
V	Signature verifier
g_s	Group private key
g_x	Group public key
s_i	Group member private key
Si	Group member public key
L_1	List of group member information for the group administrator
L_2	List of signature information for the group administrator

given the collision-free hash function H: $\{0, 1\}^* \to G_1$, GM randomly selects $\alpha \in Z_q^*$ and makes $g_s = \alpha$ as the private key of the group, thus the public key of the group is $g_x = \alpha G \in G_1$. Finally, g_s is regarded as the private parameter and the public parameters $(G_1, G_2, e, Q, G, H, g_x)$ is released.

(2) The registration of group member

The perception node needs to conduct an identity interactive authentication protocol with GM, when it wants to join the group. The participant node randomly selects $s_i \in Z_q^*$ as its private key and regards $S_i = s_i G$ as the public key. Then, participant node transmits the public key S_i to GM, and meanwhile requests registration. GM authenticates the participant node and arbitrarily selects $\alpha_i^c \in Z_q^*$. If $\alpha_i^g = (\alpha - \alpha_i^c)(\mathrm{mod}Q)$, the verification are successful and GM will transmit α_i^c to this participant node. The participant node becomes a new CIN_i and GM will record $(\alpha_i^g, \mathrm{S}_i)$ in set L_1 of legal information of group member.

(3) The key update of GS-RAM

CIN_i selects $r_0^c \in Z_q^*$, and obtains $k_0^c = s_i + \alpha_i^c + r_0^c$, $T_{i,0}^c = r_0^c G$, k_0^c is the initial key. Then, CIN_i chooses $rc\ t \in Z_q^*$ in time t

$$k_t^c = k_{t-1}^c + r_t^c = s_i + \alpha_i^c + \sum_{j=0}^{t} r_j^c, \tag{1}$$

$$T_{i,t}^c = T_{i,t-1}^c + r_t^c G = \sum_{j=0}^{t} r_j^c G. \tag{2}$$

Thus, it can be seen that the key of CIN_i at time t is k_t^c, r_t^c and k_{t-1}^c will be discarded.

```
CINi PROCESS
  input  $s_i$  $\alpha_i^c$  $G$
    choose  $r_0^c \in Z_q^*$
      $k_0^c = s_i + \alpha_i^c + r_0^c$  $k_0^c$ is the initial key
      $T_{i,0}^c = r_0^c G$
    choose  $r_t^c \in Z_q^*$ when tth time
      $k_t^c = k_{t-1}^c + r_t^c = s_i + \alpha_i^c + \sum_{j=0}^{t} r_j^c,$
      $T_{i,t}^c = T_{i,t-1}^c + r_t^c G = \sum_{j=0}^{t} r_j^c G.$
  output $k_t^c$  the key of CINi at time t
  end
```

GM selects $r_0^g \in Z_q^*$ and obtains $k_0^g = \alpha_i^g + r_0^g$, $T_{i,0}^g = r_0^g G$, k_0^g is the initial key. Then, GM arbitrarily chooses $r_t^g \in Z_q^*$ at time t

$$k_t^g = k_{t-1}^g + r_t^g = \alpha_i^g + \sum_{j=0}^{l} r_j^g, \tag{3}$$

$$T_{i,t}^g = T_{i,t-1}^g + r_t^g G = \sum_{j=0}^{t} r_j^g G. \tag{4}$$

Thus, the key of GM is k_t^g at time t, r_t^g and k_{t-1}^g are discarded.

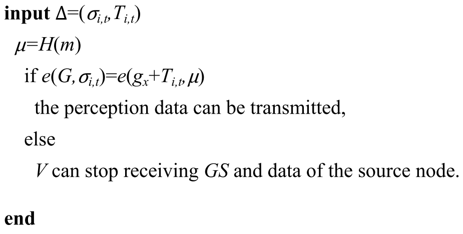
```
input  $s_i$  $\alpha_i^g$  $G$
choose  $r_0^g \in Z_q^*$
  $k_0^g = \alpha_i^g + r_0^g$  $k_0^g$ is the initial key
  $T_{i,0}^g = r_0^g G$
choose  $r_t^g \in Z_q^*$ when tth time
  $k_t^g = k_{t-1}^g + r_t^g = \alpha_i^g + \sum_{j=0}^{l} r_j^g,$
  $T_{i,t}^g = T_{i,t-1}^g + r_t^g G = \sum_{j=0}^{t} r_j^g G.$
output $k_t^g$  the key of GM at time t

end
```

(4) The generation of GS

The signed message m consists of the credibility value T of CIN$_i$ and other related attributes OR, thus $m = (T||\mathrm{OR})$. '||' is the connecting symbol. CIN$_i$ gets the signature

$\alpha^c_{i,t} = k^c_t H(m)$, and then transmits $(m, \alpha^c_{i,t}, S_i, T^c_{i,t})$ to GM. Then, GM evaluates the identity of CIN_i, using the obtained $(m, \alpha^c_{i,t}, S_i, T^c_{i,t})$. If the perception node fails to authentication, GM can reject the connection. If the node identity certification is successful, GM can calculate the signature key k^g_t at time t, and get $\alpha^g_{i,t} = k^g_t H(m)$. Then, GM checks the results of $e(G, \alpha^c_{i,t} + \alpha^g_{i,t}) = e(g_x + S_i + T^c_{i,t} + T^g_{i,t}, H(m))$. If the formula is equal, GM can obtain $\sigma_{i,t} = \alpha^c_{i,t} + \alpha^g_{i,t}$ and $T_{i,t} = T^c_{i,t} + T^g_{i,t} + S_i$, and meanwhile record $(S_i, T^c_{i,t}, T^g_{i,t}, H(m))$ to the signature information set L_2 of group member. In addition, the group signature of message m is recorded as $\Delta = (\sigma_{i,t}, T_{i,t})$.

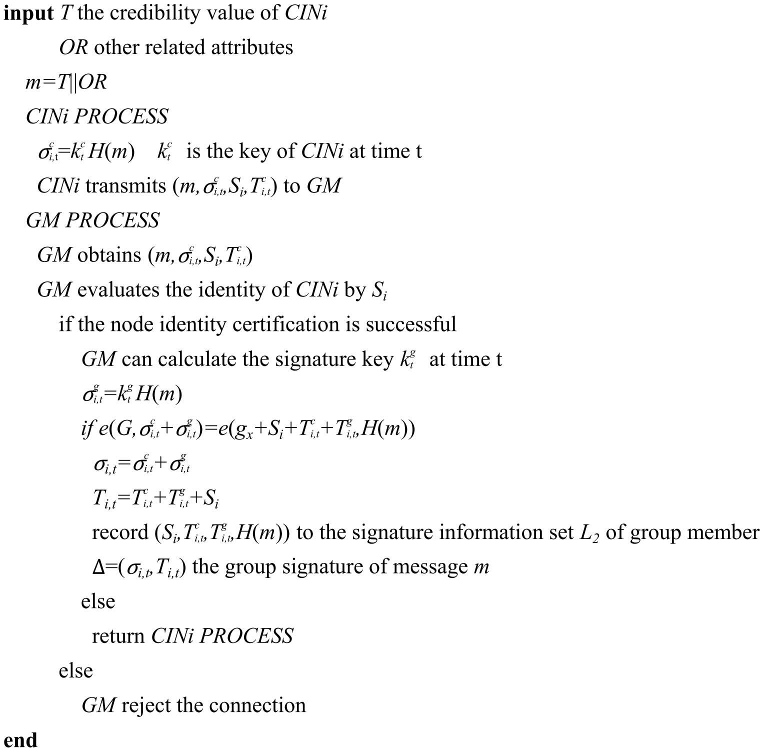


```
input $\Delta$=($\sigma_{i,t}$,$T_{i,t}$)
  $\mu$=$H(m)$
   if $e(G,\sigma_{i,t})$=$e(g_x$+$T_{i,t}$,$\mu)$
     the perception data can be transmitted,
   else
     $V$ can stop receiving $GS$ and data of the source node.

end
```

(5) The verification of GS-RAM

The remote verification node V can calculate $\mu = H(m)$, and judge $e(G, \sigma_{i,t}) = e(g_x + T_{i,t}, \mu)$,When receiving GS $\Delta = (\sigma_{i,t}, T_{i,t})$. The perception data can be transmitted, after finishing validation by the remote verification node V. If signature verification is unsuccessful, V can immediately stop receiving GS and data of the source node.



```
input $T$ the credibility value of $CINi$
        $OR$ other related attributes
   $m$=$T||OR$
   $CINi$ $PROCESS$
     $\sigma^c_{i,t}$=$k^c_t H(m)$    $k^c_t$  is the key of $CINi$ at time t
     $CINi$ transmits ($m$,$\sigma^c_{i,t}$,$S_i$,$T^c_{i,t}$) to $GM$
   $GM$ $PROCESS$
     $GM$ obtains ($m$,$\sigma^c_{i,t}$,$S_i$,$T^c_{i,t}$)
     $GM$ evaluates the identity of $CINi$ by $S_i$
        if the node identity certification is successful
          $GM$ can calculate the signature key $k^g_t$  at time t
          $\sigma^g_{i,t}$=$k^g_t H(m)$
          if $e(G,\sigma^c_{i,t}$+$\sigma^g_{i,t})$=$e(g_x$+$S_i$+$T^c_{i,t}$+$T^g_{i,t}$,$H(m))$
            $\sigma_{i,t}$=$\sigma^c_{i,t}$+$\sigma^g_{i,t}$
            $T_{i,t}$=$T^c_{i,t}$+$T^g_{i,t}$+$S_i$
            record ($S_i$,$T^c_{i,t}$,$T^g_{i,t}$,$H(m)$) to the signature information set $L_2$ of group member
            $\Delta$=($\sigma_{i,t}$,$T_{i,t}$) the group signature of message $m$
          else
            return $CINi$ $PROCESS$
        else
          $GM$ reject the connection
end
```

(6) The open of GS-RAM

When GS is questioned by the remote verifier V, the group member generating GS can be traced with the help of GM. GM can open $\varDelta=(\sigma_{i,t}, T_{i,t})$, and then verify the signature node using the information set L_1 of legal group member and the information set L_2 of group member signature recorded by the GM.

(7) The verification of GS-RAM

The group manager GM can perform the calculation of $k'=k_t^g G=T_{i,t}^g+\alpha_i^g G$ and $\varepsilon_{i,t}=\sigma_{i,t}-k_t^g\mu$ to verify the legality of $\varDelta=(\sigma_{i,t}, T_{i,t})$ which is the signature of information m by CIN_i at time t.

5 Results and discussion

To ensure the security of the proposed GS-RAM, the correctness, unforgeability, anonymity, traceability, non-relatedness, non-frameability, anti-joint aggression and forward security of GS-RAM can be verified.

(1) Correctness

(a) The correctness verification of GS. $\varDelta=(\sigma_{i,t}, T_{i,t})$ is the signature of the message m by the group member node CIN_i at time t. The remote verifier V obtains the signature $\varDelta=(\sigma_{i,t},T_{i,t})$ and calculate

$$\begin{aligned}
e(G,\sigma_{i,t}) &= e\left(G,\sigma_{i,t}^{c}+\sigma_{i,t}^{g}\right)\\
&=e\left(G,k_t^cH(m)+k_t^gH(m)\right)\\
&=e\left(G,\left(\alpha_i^c+s_i+\sum_{i=0}^{t}r_i^c\right)H(m)+\left(\alpha_i^g+\sum_{i=0}^{t}r_i^g\right)H(m)\right)\\
&=e\left(G,\left(\alpha+s_i+\sum_{i=0}^{t}r_i^c+\sum_{i=0}^{t}r_i^g\right)H(m)\right)\\
&=e\left(\left(\alpha+s_i+\sum_{i=0}^{t}r_i^c+\sum_{i=0}^{t}r_i^g\right)G,H(m)\right)\\
&=e\left(gx+S_i+T_{i,t}^c+T_{i,t}^g,H(m)\right)\\
&=e\left(gx+T_{i,t},H(m)\right),
\end{aligned} \tag{5}$$

Based on Eq. (5), the correctness of GS-RAM has been proved.

(b) The verification of GS. To verify that $\Delta=(\sigma_{i,t}, T_{i,t})$ is the signature of CIN_i for the message m at time t, GM can calculate

$$\begin{aligned} e\left(G,\sigma_{i,t}^{c}\right) &= e\left(G,\sigma_{i,t}-k_t^g\mu\right)\\ &= e\left(G,\sigma_{i,t}-k_t^gH(m)\right)\\ &= e(G,\sigma_{i,t})e\left(G,k_t^gH(m)\right)^{-1}\\ &= e\left(gx+T_{i,t},H(m)\right)e\left(T_{i,t}^g+\alpha_i^gH(m)\right)^{-1}\\ &= e\left(gx-\alpha_i^gG+T_{i,t}-T_{i,t}^g,H(m)\right)\\ &= e\left(\alpha_i^cG+S_i+T_{i,t}^c,H(m)\right)\\ &= e\left(gx+T_{i,t}-s_i,H(m)\right) \end{aligned} \tag{6}$$

According to Eq. (6), $\sigma_{i,t}$ must be generated by group manager GM and the group member CIN$_i$.

(2) Unforgeability

If ($\sigma_{i,t}$, $T_{i,t}$) is the signature of message m by CIN$_i$, then it can calculate

$$\begin{aligned} (\sigma_{i,t},T_{i,t}) &= \sigma_{i,t}^{c}+\sigma_{i,t}^{g}\\ &= k_t^cH(m)+k_t^gH(m)\\ &= \left(\alpha_i^c+s_i+\sum_{i=0}^{t}r_i^c\right)H(m)+\left(\alpha_i^g+\sum_{i=0}^{t}r_i^g\right)H(m)\\ &= \alpha H(m)+s_iH(m)+\sum_{i=0}^{t}\left(r_i^c+r_i^g\right)H(m)\\ &= \Theta_1+\Theta_2+\Theta_3, \end{aligned} \tag{7}$$

where θ_1 is the signature of the group member CIN$_i$ and the group manager GM, θ_2 is the BLS signature of the group member CIN$_i$ on message m, and θ_3 is the BLS signature of the group manager GM and the group member CIN$_i$ on message m. θ_1, θ_2 and θ_3 satisfy unforgeability, thus $\Delta = (\sigma_{i,t}, T_{i,t})$ meets unforgeability.

(3) Anonymity

The anonymity of GS means that only the group manager GM can open the signature and trace to the real signature node for a given GS. Assume that there are different CIN$_i$ and CIN$_h$ ($i \neq h$) signing the same message m, ($\sigma_{i,t}$, $T_{i,t}$) and ($\sigma_{h,t}$, $T_{h,t}$) are indistinguishable. If an attacker obtains the key of GM, CIN$_i$ and CIN$_h$, the attacker can open any signature except $\Delta = (\sigma_{i,t}, T_{i,t})$ by cooperating with the group manager GM which is in a trusted state. For the message m, if the attacker obtains ($\sigma_{i,t}$, $T_{i,t}$) and ($\sigma_{h,t}$,$T_{h,t}$), it means that the attacker can solve the CDH problem on G_1.

If knowing a GS of CIN$_i$ for message m and the key of GM and CIN$_i$, it can get: $\omega = \alpha H(m)$, $\mu_i = s_iH(m)$, $v_i = \sigma_{i,t} - \omega - \mu_i$. $T_{i,t}^c + T_{i,t}^g = T_{i,t} - S_i$ and $T_{i,t}^c + T_{i,t}^g$, $H(m)$ belongs to G_1, so a and b belongs to Z_p^*. let $T_{i,t}^c + T_{i,t}^g = aG$, $H(m) = bG$, and

$$
\begin{aligned}
e(G, v_i) &= e(G, \sigma_{i,t} - \omega - \mu_i) \\
&= e(G, \sigma_{i,t}) e(G, \omega)^{-1} e(G, \mu_i)^{-1} \\
&= e\Big(gx + S_i + T^c_{i,t} + T^g_{i,t}, H(m)\Big) e(gx, H(m)^{-1} e(S_i, H(m)^{-1} \\
&= e\Big(T^c_{i,t} + T^g_{i,t}, H(m)\Big) = e(aG, bG) = e(G, abG)\Big)
\end{aligned}
\tag{8}
$$

Based on Eq. (8), v_i is equal to abG, which means that although an attacker can solve a difficult the CDH problem, this problem cannot be calculated on G_1. Therefore, the attacker cannot successfully attack. The anonymity of GS-RAM has been proved.

(4) Traceability

According to the proposed GS-RAM, $\Delta = (\sigma_{i,t}, T_{i,t})$ is produced by the collaboration of GM and CIN$_i$. If the CIN$_i$ wants to provide a legal group signature, it must cooperate with GM. In addition, the identity and public key (S_i, $T^g_{i,t}$, $T^c_{i,t}$, $H(m)$) of the CIN$_i$ are also recorded by GM. When the remote verifier V has a query after receiving the signature, GM can open $\Delta = (\sigma_{i,t}, T_{i,t})$ and then trace the real signature node according to the group member information list recorded in the GM.

(5) Un-relevance

Theorem 1 *If there are two signatures, and only GM can identify whether they are signed by the same CIN$_i$, the two signatures are non-relevance.*

Proof Suppose ($\sigma_{i,t}$, $T_{i,t}$) is the GS of CIN$_i$ at time t for the information m_t and ($\sigma_{i,t+\Delta t}$, $T_{i,t+\Delta t}$) is the GS of CIN$_i$ at time ($t+\Delta t$) for the information $m_{t+\Delta t}$, the attack can distinguish ($\sigma_{i,t}$, $T_{i,t}$) and ($\sigma_{i,t+\Delta t}$, $T_{i,t+\Delta t}$). Moreover, the attack can also obtain the signature ($\sigma_{i,t}$, $T_{i,t}$) for the information m_t and the private key of GM and CIN$_i$. To ensure the security of GM, thus $\omega = \alpha H(m_t)$, $\mu_i = s_i H(m_t)$, $v_i = \sigma_{i,t} - \omega - \mu_i$, $T^c_{i,t} + T^g_{i,t} = T_{i,t} - S_i$, which can prove that ($T^c_{i,t} + T^g_{i,t}$, G, $H(m_t)$,v_i) is the CDH problem of group G_1. Therefore, it is impossible to judge the relevance of ($\sigma_{i,t}$, $T_{i,t}$) and ($\sigma_{i,t+\Delta t}$, $T_{i,t+\Delta t}$) without unfolding them, because the CDH problem of group G_1 is inextricable.

(6) Non-frameability

Based on the above analysis, the proposed GS-RAM is unforgeable. Therefore, it is impossible to forge a legal signature node for signature under the premise that no other node except the signature node has the key of the group member. Therefore, this GS-RAM cannot be framed.

(7) Anti-joint attack

This GS-RAM is unforgeable. Therefore, GM can verify the legality of CIN$_i$, when GM wants to cooperate with signature node CIN$_i$ to generate an effective GS. Some nodes in the group want to jointly forge a legal signature, it is impossible to construct a legal group signature, if GM does not cooperate with them.

(8) Forward safety

Assuming that CIN_i can change the key k_t^c using an arbitrarily r_t^c, the change of the time period cannot affect the selection of the random number, and the signature key can be updated without restriction. If knowing that the key of CIN_i at time t is k_t^c and wanting to get the key before the time t, the attacker must obtain r_k^c of CIN_i before the $(t-1)$ time period. However, every r_k^c getting the key at time t will be destroyed. Therefore, if the attacker wants to obtain r_{t-1}^c at time $(t-1)$ by computing $T_{i,t-1}^c - T_{i,t-2}^c = r_{t-1}^c G$, this process can be considered as solving the discrete logarithm difficult problem on group G_1. This proposed GS-RAM scheme has forward security.

Remark 2 Based on the above analysis, for the centralized networking mode of the perception layer, the proposed GS-RAM can realize the credibility attestation of data source. Moreover, it can be seen that this proposed GS-RAM can effectively protect the concealment of group member's identity, has the correctness, unforgeability, anonymity, traceability, non-relatedness, non-frameability, anti-joint aggression and forward security by analyzing the security of GS-RAM.

The group signature length of GS-RAM is short, which can effectively reduce the computational cost and is more practical.

The communication cost and efficiency of the proposed remote attestation scheme are compared with those proposed in other published literatures. Table 2 shows the comparison results of communication efficiency in attestation process with those proposed in references [27–29]. Where, PA represents the number of bilinear pair operations required in the scheme, MUL represents the number of dot product operations required in the scheme, and EXP represents the number of power exponential operations required in the scheme. SIG indicates the signcryption phase, and UNSIG indicates the unsigncryption phase. As can be seen from Table 2, the remote attestation scheme implemented in this paper has one advantage in power exponent calculation. It is very important to reduce the number of bilinear pair operation, dot product operation and power index operation in the attestation scheme to improve the communication efficiency and the use value of the scheme. The remote attestation scheme in this paper has more advantages, which can reduce the communication cost and improve the efficiency.

6 The simulation experiment

In this section, the remote attestation process between nodes in the perception layer is simulated. Simultaneously, the malicious nodes attack method described in the literature [7] is adopted to test the correctness and effectiveness as well as the dynamic adaptability of the proposed scheme.

Figures 3 and 4 respectively show the comparison results of the rate of receiving trusted data at points when malicious nodes account for 5% and 15% of all nodes.

Table 2 Efficiency comparison

Scheme	PA		MUL		EXP	
	SIG	UNSIG	SIG	UNSIG	SIG	UNSIG
Literature [27]	2	3	3	2	2	2
Literature [28]	1	5	3	0	1	0
Literature [29]	1	4	3	1	1	0
The scheme	1	3	2	1	0	0

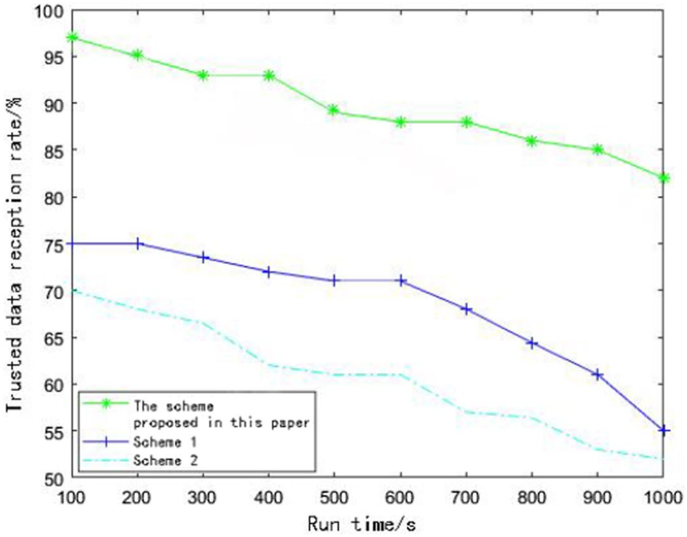


Fig. 3 The trusted data rate of the malicious nodes in 5%

Scheme 1 represents the conventional perceptual nodes authentication scheme [30], and scheme 2 represents the interactive scheme without remote attestation.

As can be seen from Figs. 3 and 4, when malicious nodes account for 5% and 15% in the perception layer. The remote attestation scheme proposed in this paper can effectively ensure the trusted data rate of data received by remote nodes. The reason why this scheme is superior to scheme 1 and 2 is that the remote attestation scheme proposed in this paper can guarantee the security and credibility of the nodes before the data source nodes transmits data.

As can be seen from Fig. 5, the energy consumption of the scheme proposed in this paper is slightly higher than scheme 1 and scheme 2's energy consumption. The reason is that the computational complexity is higher than those of scheme 1 and scheme 2. Therefore, the rate of energy consumption per unit time must be higher than those of scheme 1 and scheme 2. While it will not affect the service life of the perceptual nodes significantly, however, it can be seen from the above that the security of this scheme is far superior to scheme 1 and 2. By comprehensively weighing the comparison of security and energy consumption, the remote attestation scheme in this paper achieves better security through less energy consumption and it is more suitable for the perception layer of IoT.

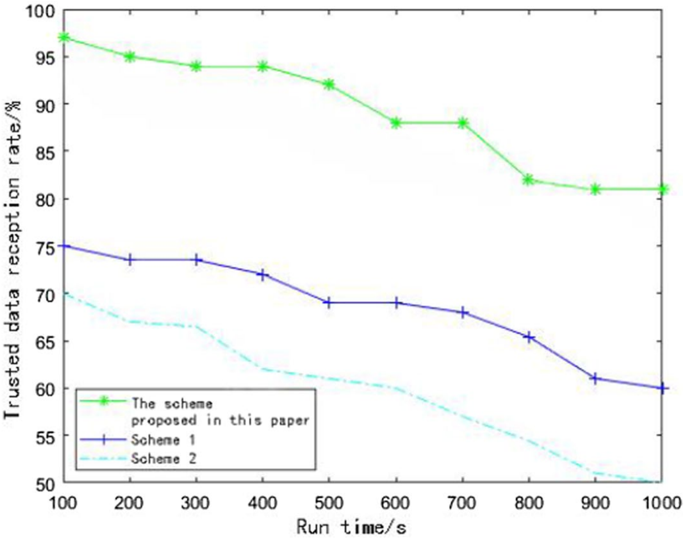


Fig. 4 The trusted data rate of the malicious nodes in 15%

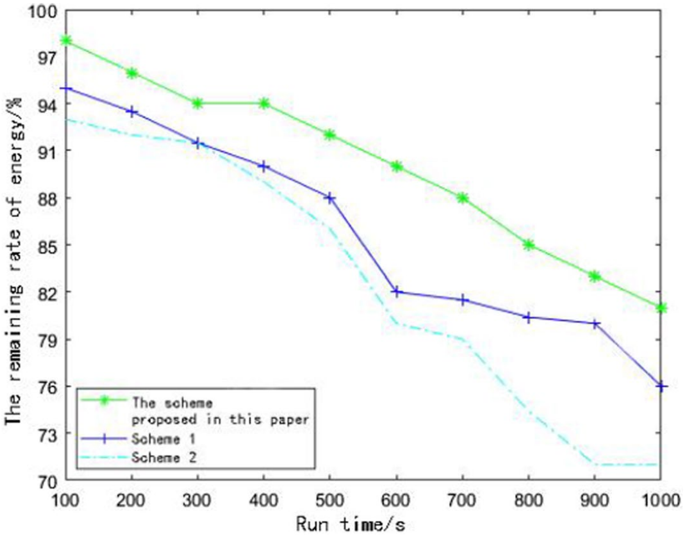


Fig. 5 The remaining rate of energy

Due to the existence of many unstable reasons, the perception layer may change at any time. Therefore, the ability of the perception layer to operate credibly despite the influence of external factors is called dynamic adaptability. If a trust model is not affected by external complex and dynamic factors, and can still accurately and continuously measure the perception nodes. It can be considered that the trust model is effective and has strong dynamic adaptability.

In the different perception layer of the Internet of Things, due to different deployment environments, there will be great differences in the interaction between nodes. For example, due to limited computing resources in the perception layer, some nodes will not interact with each other continually.

Another example is in the environment of Internet of vehicles, where frequent interaction between nodes may be required. Therefore, the dynamic adaptability of the proposed scheme is verified by comparing with scheme 1 and scheme 2.

The simulation experiment in this paper reflects the perceptual network environment of different situations through two indicators SRF and TDF.

1. SRF represents the communication frequency between nodes. The value can be used to represent the busy state of the perception network. The variation range of this value is [0,1]. The larger the value is, the more frequent the communication between nodes will be. This value is generally set to a constant depending on the development environment of the perceptual network deployed.
2. TDF represents the dynamic change frequency of the whole perceptual network. Since the perception nodes may join or quit at any time, this value can represent the dynamic change of the perceptual network. The change range of this value is [0,1]. This value is generally set to a constant depending on the development environment of the perceptual network deployed.

In this simulation experiment, the success rate of node trusted interaction TSSP represents the dynamic adaptability of the remote attestation model. The larger TSSP becomes, the stronger dynamic adaptability the model has. It is stipulated that ST(ΔT) is the record of successful communication between nodes. GT(ΔT) is all times of communication between nodes including communication failure. Therefore E can be expressed as:

$$\mathrm{TSSP} = \frac{\mathrm{ST}(\Delta T)}{\mathrm{GT}(\Delta T)}, \quad \Delta T \text{ is communication time window}$$

Figures 6 and 7 show the comparison of dynamic adaptability between the remote attestation scheme in this paper and other schemes in different perceptual network environments.

In Fig. 6, SRF = 0.3, TDF = 0.2. It indicates that the perceptual network does not change frequently and the communication frequency between nodes is not frequent in this scenario.

In Fig. 7, SRF = 0.9, TDF = 0.8. It indicates that the perceptual network changes frequently and the communication between nodes is frequent in this scenario.

In conclusion, compared with the scheme 1 and 2, the scheme proposed in this paper is more suitable for the perception layer of IoT. Because the remote attestation scheme for the node based on trusted measurement of comprehensive real-time, it fully consider the characteristics of the awareness of different networking nodes. Meanwhile, it can more accurately and objectively describe the safety of the node. Therefore, this scheme has better network dynamic adaptability.

7 Conclusions

In this paper, a GS-RAM was designed to evaluate the credibility of the perception nodes and protect the autologous identity privacy. Then, the specific construction of the proposed GS-RAM is given, which GS-RAM can query credibility of the perception nodes and trace

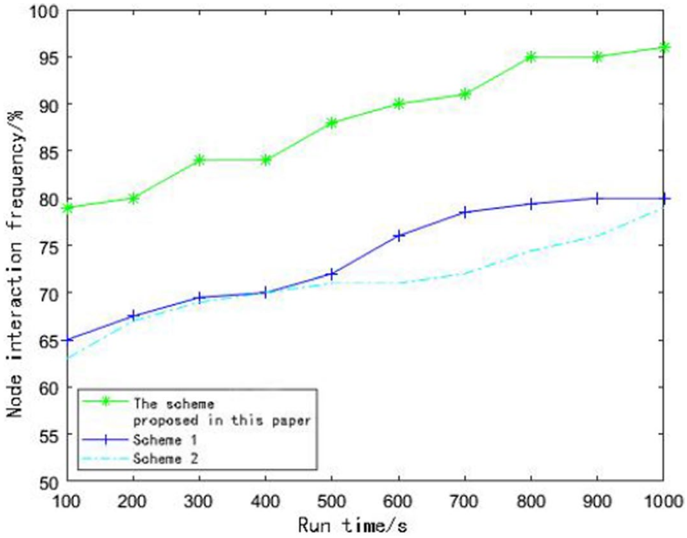


Fig. 6 The adaptability in low-frequency-aware network of dynamic

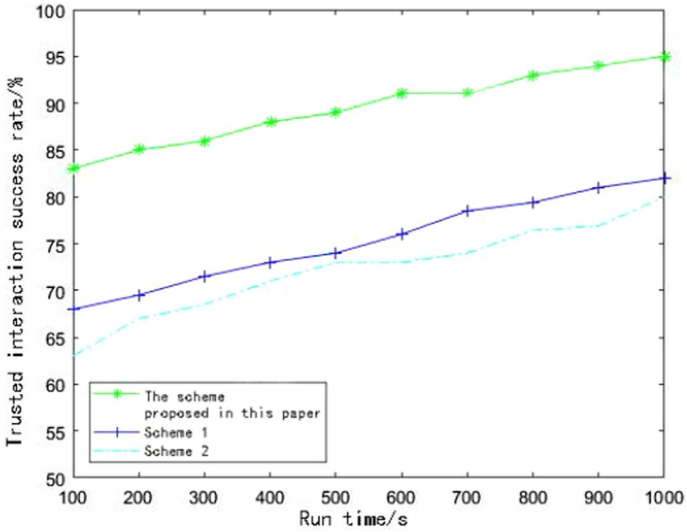


Fig. 7 The adaptability in high-frequency-aware network of dynamic

suspicious nodes. Finally, the correctness, unforgeability, anonymity, traceability, unrelatedness, non-framing, anti-joint aggression and forward security of the proposed GS-RAM was verified. The analysis results demonstrated that this proposed GS-RAM is safe and efficient to apply into the perception layer of centralized networking. Finally, simulation experiments are conducted to compare the proposed scheme with other remote attestation schemes, which verify the correctness and effectiveness of the proposed scheme, which has better security and dynamic adaptability. However, this scheme only applies to centralized networking. Besides, with the rise of quantum cryptography, some new attacks have emerged. The scheme proposed in this paper is still a little weak in resisting quantum attack. Therefore, how to improve the security of encryption means under the condition of low consumption has become an important research direction. At the same time, the limit length of the existing 128-bit RSA key may have unknown risks. Therefore, in the future research and work, a more secure mechanism is needed to ensure the security of the remote attestation process of nodes of the perception layer in the Internet of Things. In addition, anti-quantum attack research and improvement are needed to gradually optimize the performance and efficiency to better meet the needs of the sensing layer of the Internet of Things. In addition, it is necessary to conduct research and improvement on anti-quantum attack and gradually optimize the performance and efficiency to meet the needs of the perception layer of the Internet of Things superiorly.

Abbreviations

GS-RAM: Remote attestation mechanism using group signature; RAM: Remote attestation mechanism; GS: Group signature; CDH: The computational Diffie–Hellman; IoT: Internet of things; ECC: Elliptic curve cryptography; MD5: Message-digest algorithm 5; RFID: Radio frequency identification.

Authors' contributions

JH and H-JZ contributed in investigation, the overall design, design of the septuple formula and the scalar multiplication algorithm, result analysis, and draft manuscript writing. SH and Z-YS contributed in methodology, reviewing and editing the manuscript, and funding acquisitions. All the authors read and approved the final manuscript.

Availability of data and materials

The data used to support the findings of this study is included within the article.

Declarations

Competing interests

No conflict of interest exits in the submission of this manuscript, and manuscript is approved by all authors for publication. I would like to declare on behalf of my co-authors that the work described was original research that has not been published previously, and not under consideration for publication elsewhere, in whole or in part. All the authors listed have approved the manuscript that is enclosed.

Received: 7 July 2021 Accepted: 20 January 2022
Published online: 08 February 2022

References

1. D. Wang, J. Zhao, A new approach to heterogeneous wireless sensor networks reliability evaluation based on perception layer in internet of vehicles. Photonic Netw. Commun. **37**(2), 179–186 (2019)
2. N. Ye, Y. Zhu et al., An efficient authentication and access control scheme for perception layer of internet of things. Appl. Math. Inform. Sci. **8**(4), 1617–1824 (2014)
3. B. Ndibanje, H.J. Lee, S. Lee, Security analysis and improvements of authentication and access control in the internet of things. Sensors **14**, 786–805 (2014)
4. M. Zhou, L. Han, H. Lu et al., Intrusion detection system for IoT heterogeneous perceptual network. Mob. Netw. Appl. **4**, 42–54 (2020)
5. P. Zhang, J. Gao, W. Jia et al., Design of compressed sensing fault-tolerant encryption scheme for key sharing in IoT multi-cloudy environment. J. Inf. Secur. Appl. **47**, 65–77 (2019)
6. B. Gong, Y. Zhang, Y. Wang, A remote attestation mechanism for the sensing layer nodes of the Internet of Things. Future Gener. Comput. Syst. **78**, 867–886 (2018)
7. Trusted Computing Group, *Protection Profile of PC Client Specific Trusted Platform Module TPM Family 1.2[EB/0L]* (2011), http://www.trustedcomputinggroup.org/resources/tpm_l2jprotection_profile/
8. D. Boneh, H. Shacham, Group signatures with verifier-local revocation, in: *Proceedings of the 11th ACM conference on Computer and Communications Security* (2004), pp. 168–177
9. E. Brickell, J. Camenisch, L. Chen, Direct anonymous attestation, in: *Proceedings of the 11th ACM conference on Computer and communications security* (2004), pp. 132–145
10. E. Brickell, J. Li, Enhanced privacy ID: a direct anonymous attestation scheme with enhanced revocation capabilities, in: *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society* (20070, pp. 21–30
11. Trusted Computing Group, *TCG Specification Architecture Overview Specification Revision 1.2 [EB/OL]* (2011), http://www.trustedcoinputinggroup.org
12. R. Sailer, X.L. Zhang, T. Jaeger, L.V. Doom, Design and implementation of a TCG-based integrity measurement architecture, in: *Proceedings of the 13th USENIX Security Symposium* (Usenix Press, San Diego, 2004), pp. 16–16
13. TCG Group, *TCG Architecture Overview Specification Design Principles Specification Version 1.2* (2003). https://www.Trustedcomputinggroup.org/home

14. A. Awad, S. Kadry, B. Lee, G. Maddodi, E. O'Meara, Integrity assurance in the cloud by combined pba and provenance, in: *2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST)* (IEEE, 2016), pp. 127–132
15. J. Zhao, Z. Han, J. Liu, R. Zhang, Remote attestation based on trusted cryptography module. J. Beijing Jiaotong Univ. **34**(02), 33–37 (2010)
16. A. Awad, S. Kadry, B. Lee, S. Zhang, Property based attestation for a secure cloud monitoring system, in: *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing* (IEEE, 2014), pp. 934–940
17. L. Zhu, Z. Zhang, L. Liao et al., *A secure robust integrity reporting protocol of trusted computing for remote attestation under fully adaptive party corruptions* (Springer, Berlin, 2012), pp. 211–217
18. J. Liu, J. Zhao, Y. Zhao, Study of remote automated anonymous attestation in trusted computing. Chin. J. Comput. **32**(07), 1304–1310 (2009)
19. M.F. Ezerman, H.T. Lee, S. Ling et al., Provably secure group signature schemes from code-based assumptions. IEEE Trans. Inf. Theory **66**(9), 5754–5773 (2020)
20. M.H. Sun, B.J. Chen, T.H. Wang, Cryptanalysis of group signature scheme using self-certified public keys. Electron. Lett. **35**(22), 1938–1939 (1999)
21. J. Bootle, A. Cerulli, P. Chaidos et al., Foundations of fully dynamic group signatures. J. Cryptol. **33**(2), 1–49 (2020)
22. K.J. Zhang, S. Ying, T.T. Song et al., Cryptanalysis of the quantum group signature protocols. Int. J. Theor. Phys. **52**(11), 4163–4173 (2013)
23. T. Mori, T.V. Nguyen, Y. Mori et al., Preservation of Lyapunov functions under bilinear mapping. Automatica **42**(6), 1055–1058 (2006)
24. M.S. Floater, The inverse of a rational bilinear mapping. Comput. Aided Geom. Des. **33**, 46–50 (2015)
25. J. Zhang, Y. Yu, Short computational Diffie–Hellman-based proxy signature scheme in the standard model. Int. J. Commun. Syst. **27**(10), 1894–1907 (2014)
26. R.B. Amarapu, P.V. Reddy, Efficient identity-based parallel key-insulated signature scheme using pairings over elliptic curves. J. Sci. Ind. Res. **77**(1), 24–28 (2018)
27. F.G. Li, H. Zhang, T. Takagi, Efficient signcryption for heterogeneous systems. IEEE Syst. J. **7**(3), 420–429 (2013)
28. F.G. Li, Y.Y. Han, C.H. Jin, Practical signcryption for secure communication of wireless sensor networks. Wirel. Person. Commun. **89**(4), 1–22 (2016)
29. Z. Eslami, N. Pakniat, Certificateless aggregate signcryption. J. King Saud Univ. Comput. Inf. Sci. **26**(3), 276–286 (2014)
30. P. Gasti, J. Šeděnka, Q. Yang, G. Zhou, K.S. Balagani, Secure, fast, and energy-efficient outsourced authentication for smartphones. IEEE Trans. Inf. Forensics Secur. **11**(11), 2556–2571 (2016)

Publisher's Note