Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2014, Article ID 687158, 7 pages
http://dx.doi.org/10.1155/2014/687158

Research Article

Property-Based Anonymous Attestation in Trusted Cloud Computing

Zhen-Hu Ning,[1] Wei Jiang,[1,2] Jing Zhan,[1] and Peng Liang[1]

[1] *College of Computer Science, Beijing University of Technology, Beijing 100124, China*
[2] *School of Computer, National University of Defense Technology, Changsha 410073, China*

Correspondence should be addressed to Zhen-Hu Ning; ning_zhenhu@163.com

Received 17 December 2013; Accepted 3 February 2014; Published 25 March 2014

Academic Editor: Weifeng Sun

Copyright © 2014 Zhen-Hu Ning et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the remote attestation on Trusted Computer (TC) computing mode TCCP, the trusted computer TC has an excessive burden, and anonymity and platform configuration information security of computing nodes cannot be guaranteed. To overcome these defects, based on the research on and analysis of current schemes, we propose an anonymous proof protocol based on property certificate. The platform configuration information is converted by the matrix algorithm into the property certificate, and the remote attestation is implemented by trusted ring signature scheme based on Strong RSA Assumption. By the trusted ring signature scheme based on property certificate, we achieve the anonymity of computing nodes and prevent the leakage of platform configuration information. By simulation, we obtain the computational efficiency of the scheme. We also expand the protocol and obtain the anonymous attestation based on ECC. By scenario comparison, we obtain the trusted ring signature scheme based on RSA, which has advantages with the growth of the ring numbers.

1. Introduction

With the development of information technology, cloud computing has been the important trend of the third revolution in information technology, after the personal computer and the Internet, and the focus of industry and, Science [1]. Many cloud providers offer services at various layers of the cloud computing. Weather providers offer services of basic computational infrastructure and allow their customers to develop their own applications and effectively control their own computations and data, PaaS providers allow their costumers to develop cloud applications of their own, or SaaS providers allow their costumers to create their own documents using the applications and to get out of control of their computations and data. So the trustiness attestation to platforms becomes an important problem needed to be resolved in cloud computing [2].

A security scheme was supported in [3, 4] based on the research on the potential security problems existing in current IasS. In this scheme, hardware, network connection, platform virtualization, software for cloud computing, utility computing, and service level agreement are enhanced in the IaaS.

Trusted computing was introduced into IaaS firstly and a concept called Trusted Cloud Computing Platform (TCCP) was proposed in [5, 6]. All virtual computing nodes are guaranteed to be trusted by configuration-based remote attestation. However, since the configuration of the latest restart of the platform is static, the dynamic attacks such as buffer overflow and DMA attack cannot be handled. Moreover, since the signature is carried out by the Endorsement Key of TPM, the leakage of privacy may be caused based on the fact that the usage of Endorsement Key can be tracked.

A remote attestation for virtual computing node was supported in [7, 8]. The following events such as changing, updating, and patching the configuration of virtual platform are updated in the attestation by TPM. However, this scheme is actually a static remote attestation based on configuration and it cannot attest the running states of virtual computing node.

The authors in [7, 8] support remote attestation for virtual machine; virtual TPM is improved to update attestation

by the means of the following events such as changing, updating, and patching the configuration of virtual platform. However, it is actually a static remote attestation based on configuration, while it cannot attest the running states of virtual platform. Additionally, this scheme only deals with the trust root based on software and lacks both trusted guarantee provided by TPM and attestation of physical platform on which the virtual machines are running.

The goal of trusted computing is to improve the security and trustworthiness of computing platforms [9–12], and the well-known group—TCG—has published many specifications, such as the Trusted Platform Module (TPM) [13, 14] and library Trusted Software Stack (TSS) [15].

Remote attestation is one of the core technologies of trusted computing. In TCG1.1 specification, the attestation is designed with challenge information in plain text [16, 17]. In the process of the remote attestation, one platform sends a challenge information and random number to obtain one or more PCR values in order to validate the platform state. Each TPM has only an Endorsement Key (EK), issued by the TPM manufacturers, to identify the identity of the Trusted Platform. For security and privacy, EK does not directly support encryption or remote attestation. Instead, using the signature key AIK generated by EK and registered by PCA to achieve the remote attestation, the attestor signs the PCR with AIK and sends the signature and the corresponding measure attached log SML and AIK certificate to the challenger. Then, the challenger verifies the proof to guarantee the trust and security of the platform.

However, the proof protocol has some evident shortage. First, the protocol uses PCR to achieve the proof, which will expose the local platform configuration information (including hardware and software). Second, the proof protocol cannot guarantee the anonymity of attestor.

In recent years, Direct Anonymous Attestation (DAA) [18, 19] has been proposed as the protocol of remote attestation between platforms. The protocol has become part of TCG1.2 specification. DAA protocol is based on three entities, that is, the TPM platform, DAA signatory, and DAA verifiers. The DAA protocol consists of two steps. First, the signatory validates TPM platform and generates the DAA certificate for the TPM platform. Second, the TPM platform interacts with verifiers using the DAA certificate. By zero-knowledge proof, verifiers verify the DAA certificate without violating the premise of the platform privacy. However, since the DAA protocol has many times of zero-knowledge proof, which induces very large computational complexity, the DAA protocol is difficult to be a viable protocol.

A property-based attestation for computing platforms was introduced in [20]. A trusted third party converts the platform configuration information into the property certificates, which can avoid the leakage of information of platform. Based on [20], the paper in [21] proposed a protocol for property-based attestation. Property certificates corresponding to the platform configuration information are issued and managed by a trusted third-party CA; the protocol achieves anonymous proof by a series of complex interactions' agreement. However, lots of zero-knowledge proofs may induce a high complexity. Moreover, the trusted third party must know all of the platform status information, which is actually to transfer part of work of the verifiers to a trusted third party and to increase the burden of CA. The paper [19] proposed an anonymous protocol of remote attestation based on property certificates. Due to involvement of lots of interactions, the computational complexity is very large.

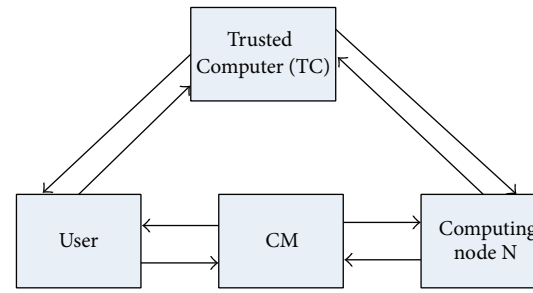


Figure 1: The interactions of the remote attestation.

Remote attestation based on the TCCP has many defects. First, every proof involves the operation of TC, which aggravates the burden of TC. Second, the remote attestation cannot guarantee the anonymity of platform. To overcome these defects, we introduce a protocol based on trusted ring signature. In the protocol, the signature of both the public and the private keys is replaced with TPM signature key, so that the security of remote attestation is guaranteed by TPM. The proof does not directly require TC, and TC only provides a series of TPM signature public keys, which reduces the burden on TC. Trusted ring signature can guarantee unconditional anonymity of the signature party and protect the privacy of the platform.

2. Protocol Description

In this paper, the process of remote attestation consists of two steps. First, TC converts the platform configuration information PCR of computing nodes into property certificate. Second, computing nodes provide the property certificate for verifier by remote attestation. Figure 1 shows the interactions of the protocol.

2.1. Property Certificate Issue. The Trusted Computer (TC) is responsible for the issue of the property certificates of the corresponding computing nodes. TC has all of the property certificates of the platform, denoted as $P = \{P_1, \ldots, P_n\}$. Let $\{\mathrm{PCR}_1, \ldots, \mathrm{PCR}_m\}$ denote all of the platform configuration information PCRs. We define the set $C = \{C_1, \ldots, C_m\}$ as follows.

If the remote attestation of PCR_i is verified as in [3, 4], then $C_i = 1$. Otherwise, $C_i = 0$. The map between property certificates and corresponding platform configuration information is defined as follows:

$$P = AC, \quad A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}, \tag{1}$$

where a_{ij} is 0 or 1 and $P_i = \bigcap_{a_{ij}=1} C_j$. If $P_i = \bigcap_{a_{ij}=1} C_j$, then TC issues a property certificate P_i, which identifies a platform that has the property P_i. Otherwise, TC issues the property certificate which indicates that the platform does not have the property P_i.

For example, if the computing node N involves the property certificate P_i, then computing node N requires a series of remote attestations of $\{\mathrm{PCR}_j \mid a_{ij} = 1\}$. Then, TC issues property certificate P_i in accordance with the above-described method and sends property certificate P_i to TPM N securely.

We simplify the process as follows.

(1) TPM N checks the current PCR to determine whether it needs to start the process of generating the property certificates. If the current PCR is not equal to the PCR used to generate the latest property certificate by TC, TPM N start the process of generating the property certificates.

(2) TC sends the challenge N_T PCRs to N.

(3) TPM N sends the result of the remote signature $\mathrm{Sig}\{\mathrm{PCR}, N_T\}_{Sk}$, PCR, SML to TC.

(4) TC uses PCR to generate the property certificates.

3. Anonymous Attestation Based on RSA

3.1. Attestation Execution. Before attestation, TPM generates a signature key (pk, sk); sk is stored by TPM and pk is registered by TC, so that TC stores all of the signature public keys of computing nodes in cloud computing. In the remote attestation, TC supports signature public keys required in the trusted ring signature. Let $H : \{0,1\}^* \rightarrow \{0,1\}^k$ be secure hash function. The process of remote attestation is as follows.

Let A be user and let B be cloud computing node; B provides remote attestation for A, and A verifies the attestation.

(1) A sends request for remote attestation and $N_A \in \{0,1\}^k$ to B.

(2) TPM B obtains $t-1$ valid signature public keys $pk_2, \ldots, pk_t$ from TC. We assume that TPM B has signature key (pk_1, sk_1).

(3) TPM B generates the signature of P_L with $pk_2, \ldots, pk_t$. Let $D\{\mathrm{data}, K\}$ denote decryption by K, and let $E\{\mathrm{data}, K\}$ denote encryption by K; TPM B chooses $N_B, r_2, \ldots, r_t \in \{0,1\}^k$ and generates the signature as follows:

$$\begin{aligned} M &= D\{N_B, pk_A\}, \\ c_i &= D\{r_i, pk_i\} \quad (2 \le i \le t), \\ c_1 &= H(P_L \parallel N_A \parallel N_B) - \sum_{i=2}^{t} c_i, \\ r_1 &= E(c_1, sk_1). \end{aligned} \tag{2}$$

(4) B sends $pk_1, \ldots, pk_t, r_1, \ldots, r_t, M, P_L$ to A.

(5) A verifies the signature as follows:

$$\begin{aligned} N_B &= E\{M, sk_A\}, \\ \sum_{i=1}^{t} D\{r_i, pk_i\} &= H(P_L \mid N_A \parallel N_B). \end{aligned} \tag{3}$$

(6) A verifies the property certificate P_L and sends N_B to B.

(7) B verifies N_B to guarantee the success of the remote attestation.

Remark 1. Since $pk_1, \ldots, pk_t$ are different from each other, then, we can choose suitable N_B to overcome this aforementioned shortcoming, because the protocol has requirement that $pk_1, \ldots, pk_t$ have the same bits, for example, 2048 bits.

3.2. Correctness. In the signature scheme, the signing and verifying are consistent with each other as follows:

$$\begin{aligned} \sum_{i=1}^{t} D\{r_i, pk_i\} &= D\{r_1, pk_1\} + \sum_{i=2}^{t} D\{r_i, pk_i\} \\ &= c_1 + \sum_{i=2}^{m} c_i = H(P_L \parallel N_A \parallel N_B). \end{aligned} \tag{4}$$

3.3. Unconditional Anonymity. Ring signature scheme is characterized by anonymity. Let $Sig = \{r_1, \ldots, r_m\}$ be a valid ring signature for message m, and let U_i be a member of the ring. Then U_i can generate the ring signature. From the verification, we can obtain that the probability that the user distinguishes the signer is $1/t$. So the scheme is unconditional anonymous.

3.4. Security Analysis. The security analysis is based on the Strong RSA Assumption. Strong RSA Assumption is a given RSA modulus, and a given random number $z < N$. It is difficult to find $r, y (r > 1, y < N)$, satisfying $y^r = z$.

The proof of security can be simplified as the following theorem.

Theorem 2. *Assume that the attacker F with the ability of adaptive chosen message and identity can break our scheme by a nonnegligible probability ε within PPT time. Then, there exists an algorithm C, which can solve the problem of the Strong RSA Assumption by a nonnegligible probability $\varepsilon' = O(\varepsilon)$ within PPT time, where $O(\varepsilon)$ represents $O(\varepsilon) \ge k\varepsilon$, and k is a constant not dependent on ε.*

Proof. We assume that C is a challenger. The target of C is to obtain a solution of the Strong RSA Assumption by F.

(1) *Setup*. C runs the setup algorithm. C maintains t signature public keys $pk_1, \ldots, pk_t$. Let H_1, H_2 be two random oracles, and the construction of the machine H_1, H_2 is listed as follows. C sends $\{pk_1, \ldots, pk_t, H_1, H_2\}$ to the attacker F as public parameters.

Table 1: The efficiency of the signature.

	E	D	H
Amount of calculation of the computing node	1	$t-1$	1
Amount of calculation of the user	0	t	1

(2) *Inquiring* H_1. C maintains a list H_1^L containing the array $\{N_{Ai}, h_i\}$. C chooses q_{H_2} random numbers $h_1, \ldots, h_{q_{H_1}}$ as answers. When F inquires H_1-value of N_{Ai}, C recovers $\{N_{Ai}, h_i\}$ from H_1^L and sends h_i to F.

(3) *Inquiring* H_2. C maintains a list of the array $\{N_{Ai}, R_i\}$, $R_i = \{r_2, \ldots, r_t\}$. C chooses q_{H_2} random numbers $R_1, \ldots, R_{q_{H_2}}$ as answers. When F inquires H_2-value of N_{Ai}, C recovers $\{N_{Ai}, R_i\}$ from H_2^L and sends R_i to F.

(4) *Inquiring Signature*. C maintains a list of the array $\{N_{Ai}, R_i'\}$, $R_i' = \{r_1, \ldots, r_t\} = r_1 \cup R_i$. When F inquires signature of N_{Ai}, C checks whether N_{Ai} is in H_1^L. Then, C recovers $\{N_{Ai}, R_i'\}$ and sends R_i' to F.

C simulates TPM, and the attacker F makes interaction with C. The output of C obeys the above strategy.

Then, F stops inquiring, and F generates a signature R' about N_A (N_A has never been asked) by simulating TPM, which meets $\mathrm{Ver}(N_A, pk_1, \ldots, pk_t, R') = 1$. C recovers $\{N_A, h\}$ from H_1^L and recovers $\{N_A, R\}$ from H_2^L. Letting $c = h - \sum_{i=2}^{t} r_i$, we have $c^{pk} = r_1$, which resolves the problem of Strong RSA Assumption.

It is easy to obtain that the probability that C successfully resolved the problem of Strong RSA Assumption is $\varepsilon' = O(\varepsilon)$. There is a question that $c = h - \sum_{i=2}^{t} r_i$ had been asked before the signature. However, by a simple analysis, we can obtain that the probability is $1/2^{\sqrt{k}}$, which can be omitted. So the probability that C successfully resolves the problem of Strong RSA Assumption is also $\varepsilon' = O(\varepsilon)$. □

3.5. Efficiency. In our trusted ring signature scheme, there are three operations that are involved, such as nonsymmetric encryption, nonsymmetric decryption, and hash operations. Let E denote the nonsymmetric encryption operation, let D denote the nonasymmetric decryption operation, and let H denote hash operation. The efficiency of the signature is listed as follows.

In the remote attestation, the computing node conducts nonsymmetric encryption once, nonsymmetric decryption t many times, and hash operation once. Then, the total amount of calculation is $E + (t-1)D + H$, see Table 1.

Since the hash operation can be omitted with respect to the nonsymmetric operation, the amount of calculation of computing node can be simply represented by the nonsymmetric encryption E. By calculation, the total amount of calculation is approximately $S = (1 + 4t/3n)E$.

4. Anonymous Attestation Based on ECC

4.1. Attestation Execution. Let G_1, G_2 be defined as multiplicative group whose order is p, and g is the generator of G_1. Bilinear map is $G_1 \times G_1 \to G_2$, where $e(g, g) = I$. Let $x_1, \ldots, x_n$ be TPM signature private keys and let $g^{x_1}, \ldots, g^{x_n}$ be the corresponding TPM signature public keys.

Let A be user and let B be cloud computing node; B provides remote attestation for A, and A verifies the attestation.

(1) A sends request for remote attestation and $N_A \in Z_q^*$ to B.

(2) TPM B obtains $t-1$ valid signature public keys $pk_2, \ldots, pk_t$ from TC. We assume that TPM B has signature key (pk_1, sk_1).

(3) TPM B generates the signature of P_L with $pk_2, \ldots, pk_t$. TPM B chooses $r_2, \ldots, r_t \in Z_q^*$ and generates the signature as follows:

$$\begin{aligned} P &= H(P_L \parallel N_A), \\ s_i &= g^{r_i} \quad (2 \le i \le t), \\ s_1 &= \frac{1}{x_1}\left(P - \sum_{i=2}^{t} pk_i^{r_i}\right). \end{aligned} \tag{5}$$

(4) B sends $pk_1, \ldots, pk_t, s_1, \ldots, s_t, P_L$ to A.

(5) A verifies the signature as follows:

$$e(P, g) = \prod_{i=1}^{t} e(pk_i, s_i). \tag{6}$$

(6) A verifies the property certificate P_L.

This anonymous attestation is based on Boneh's ring signature scheme [20]. We obtain the analysis of the scheme as follows.

4.2. Correctness. In the signature scheme, the signing and verifying are consistent with each other as follows:

$$\begin{aligned} \prod_{i=1}^{t} e(pk_i, s_i) &= e(pk_1, s_1) \prod_{i=2}^{t} e(pk_i, s_i) \\ &= e\left(g, P - \sum_{i=2}^{t} g^{x_i r_i}\right) \prod_{i=2}^{t} e(g, g^{x_i r_i}) = e(P, g). \end{aligned} \tag{7}$$

4.3. Unconditional Anonymity. Similar with anonymous attestation based on ECC, we can easily obtain that the probability that the user distinguishes the signer is $1/t$. So the scheme is unconditional anonymous.

4.4. Security Analysis. The security analysis is based on the CDHI problem. CDHI problem is a given g^x (x is unknown). It is difficult to calculate $g^{1/x}$. Similar to Theorem 2, we can obtain the following theorem.

Theorem 3. *Assume that the attacker F with the ability of adaptive chosen message and identity can break our scheme*

by a nonnegligible probability ε within PPT time. Then, there exists an algorithm C, which can solve the problem of the CDHI problem by a nonnegligible probability $\varepsilon' = O(\varepsilon)$ within PPT time, where $O(\varepsilon)$ represents $O(\varepsilon) \geq k\varepsilon$, and k is a constant not dependent on ε.

4.5. Efficiency. In the remote attestation, the computing node conducts ECC $2t - 1$ times and hash operation once. Then, the total amount of calculation is $T = (2t - 1)\widetilde{E} + H$, where $\widetilde{E}$ is the ECC encryption.

5. Formalized Proof of the Protocol

Here, we give the key exchange process of the protocol. Let $K_{\text{TC\_}B}$ be the shared key between TC and TPM B, and let $K_{\text{TC\_}A}$ be the shared key between TC and A; the target of this section is to obtain the shared key K_{AB} between A and TPM B. The detailed process is listed as follows:

$$\begin{aligned} A &\longrightarrow \text{CM}, \qquad \text{CM} \longrightarrow B : A, N_A, \\ B &\longrightarrow \text{TC} : A, B, N_B, \\ TC &\longrightarrow B : \left\{N_B, K_{AB}, A, \right. \\ &\qquad \left. \{N_A, K_{AB}, \text{CM}\}_{K_{\text{TC\_}A}}\right\}_{K_{\text{TC\_}B}}, \\ B &\longrightarrow A : \{N_A, K_{AB}, \text{CM}\}_{K_{\text{TC\_}A}}\{N\}_{K_{AB}}, \\ B &\longrightarrow \text{CM}, \qquad \text{CM} \longrightarrow A : \{N+1\}_{K_{AB}}. \end{aligned} \tag{8}$$

To guarantee the anonymity of B, the shared key K_{AB} is actually a shared key between CM and A. A does not know that B is the signer.

Here, we use the Ban Logic [21] to obtain the formalized proof of the protocol.

Detailed description of the protocol is the following:

$$\begin{aligned} \text{TC} &\longrightarrow B : \left\{N_B, A \overset{K_{AB}}{\longleftrightarrow} B \right. \\ &\qquad \left. \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{K_{\text{TC\_}A}}\right\}_{K_{\text{TC\_}B}}, \end{aligned} \tag{9}$$

$$B \longrightarrow A : \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{\text{TC\_}A}, \qquad \left\{N, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{K_{AB}}, \tag{10}$$

$$A \longrightarrow B : \left\{N, \left(A \overset{K_{AB}}{\longleftrightarrow} B\right)\right\}_{K_{AB}}. \tag{11}$$

Assumption is as follows:

$$A \mid\equiv A \overset{K_{\text{TC\_}A}}{\longleftrightarrow} \text{TC}, \tag{12}$$

$$B \mid\equiv B \overset{K_{\text{TC\_}B}}{\longleftrightarrow} \text{TC}, \tag{13}$$

$$\text{TC} \mid\equiv A \overset{K_{\text{TC\_}A}}{\longleftrightarrow} \text{TC}, \tag{14}$$

$$\text{TC} \mid\equiv B \overset{K_{\text{TC\_}B}}{\longleftrightarrow} \text{TC}, \tag{15}$$

$$\text{TC} \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B. \tag{16}$$

The credibility of TC is given as follows:

$$A \mid\equiv \left(\text{TC} \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B\right), \tag{17}$$

$$B \mid\equiv \left(\text{TC} \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B\right), \tag{18}$$

$$A \mid\equiv \left(\text{TC} \Longrightarrow \#\left(A \overset{K_{AB}}{\longleftrightarrow} B\right)\right), \tag{19}$$

$$B \mid\equiv \left(\text{TC} \Longrightarrow \#\left(A \overset{K_{AB}}{\longleftrightarrow} B\right)\right). \tag{20}$$

Freshness of random numbers is given as follows:

$$A \mid\equiv \#\left(N_A\right), \tag{21}$$

$$B \mid\equiv \#\left(N_B\right), \tag{22}$$

$$B \mid\equiv \#\left(N\right). \tag{23}$$

Target of the protocol is the following:

$$A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B, \tag{24}$$

$$B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B, \tag{25}$$

$$A \mid\equiv B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B, \tag{26}$$

$$B \mid\equiv A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B. \tag{27}$$

Some rules of the Ban Logic applied in this paper are listed as follows:

$$\frac{P \mid\equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}K}{P \mid\equiv Q \sim X}, \tag{28}$$

$$\frac{P \mid\equiv \#\left(X\right), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}, \tag{29}$$

$$\frac{P \mid\equiv Q \mid\Longrightarrow P, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}, \tag{30}$$

$$\frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)}, \tag{31}$$

$$\frac{P \mid\equiv (X, Y)}{P \mid\equiv X}, \tag{32}$$

$$\frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X}, \tag{33}$$

$$\frac{P \mid\equiv Q \mid\sim (X, Y)}{P \mid\equiv Q \mid\sim X}, \tag{34}$$

$$\frac{P \lhd (X, Y)}{P \lhd X}, \tag{35}$$

$$\frac{P \mid\equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\} K}{P \lhd X}, \tag{36}$$

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X, Y)}. \tag{37}$$

Proof. From (9), we have

$$B \lhd \left\{\left(N_B, A \overset{K_{AB}}{\longleftrightarrow} B\right), \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{K_{\mathrm{TC\_}A}}\right\}_{K_{\mathrm{TC\_}B}}. \tag{38}$$

From (13) and (27), we obtain

$$B \mid\equiv \mathrm{TC} \sim \left(N_B, A \overset{K_{AB}}{\longleftrightarrow} B\right), \quad B \mid\equiv \mathrm{TC} \sim \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{K_{\mathrm{TC\_}A}}. \tag{39}$$

It follows from (22) and (29) that

$$B \mid\equiv \mathrm{TC} \mid\equiv \left(N_B, A \overset{K_{AB}}{\longleftrightarrow} B\right), \quad B \mid\equiv \mathrm{TC} \mid\equiv \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{K_{\mathrm{TC\_}A}}. \tag{40}$$

By (22) and (33), we obtain

$$B \mid\equiv \mathrm{TC} \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B, \quad B \mid\equiv \#\left(A \overset{K_{AB}}{\longleftrightarrow} B\right). \tag{41}$$

By (18), (20), and (30), we have

$$B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B. \tag{42}$$

Then, (25) holds true.

It follows from (10) that

$$A \lhd \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{K_{\mathrm{TC}_A}}, \tag{43}$$

$$A \lhd \left\{N, A \overset{K_{AB}}{\longleftrightarrow} B\right\}_{K_{AB}}. \tag{44}$$

By (13) and (27), we have

$$A \mid\equiv \mathrm{TC} \sim \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}. \tag{45}$$

It follows from (21) and (29) that

$$A \mid\equiv \mathrm{TC} \mid\equiv \left\{N_A, A \overset{K_{AB}}{\longleftrightarrow} B\right\}. \tag{46}$$

By (18), (20), and (30), we obtain

$$A \mid\equiv \mathrm{TC} \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B, \tag{47}$$

$$B \mid\equiv \#\left(A \overset{K_{AB}}{\longleftrightarrow} B\right). \tag{48}$$

By (17), (19), and (30), we have

$$A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B. \tag{49}$$

Then, (24) holds true.

With (44) and (49), we have

$$A \mid\equiv B \sim \left\{N, A \overset{K_{AB}}{\longleftrightarrow} B\right\}. \tag{50}$$

It follows from (48) that

$$A \mid\equiv B \mid\equiv \left\{N, A \overset{K_{AB}}{\longleftrightarrow} B\right\}. \tag{51}$$

Then,

$$A \mid\equiv B \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B. \tag{52}$$

Then, (26) holds true.

From (10), we have

$$B \lhd \left\{N, A \overset{K_{AB}}{\longleftrightarrow} B\right\}. \tag{53}$$

By (27) and (42), we obtain

$$B \mid\equiv A \sim \left\{N, A \overset{K_{AB}}{\longleftrightarrow} B\right\}. \tag{54}$$

Then, we have

$$B \mid\equiv A \mid\equiv A \overset{K_{AB}}{\longleftrightarrow} B. \tag{55}$$

□

6. Scenario Comparison

Compared with anonymous attestation based on ECC, whose amount of calculation is $T = (2t - 1)\widetilde{E} + H$, then we have

$$\frac{T}{S} = \frac{t\widetilde{E}}{(1 + 4t/3n)E} = \frac{3n\widetilde{E}}{4E} \times \frac{2 - (1/t)}{3n/4t + 1}. \tag{56}$$

Then, $\lim_{t \to \infty} T/S = 3n\widetilde{E}/2E$. So it means that if $S > T$, then $\widetilde{E} < 2E/3n$ which is hard to meet, since modern commercial ECC computing cannot have both a stronger security than RSA-2048 and a less calculation satisfying $\widetilde{E} < 2E/3n$. So the anonymous attestation based on RSA has advantages with the growth of the ring numbers.

7. Conclusion

In this paper, we studied the anonymous remote attestation based on property certificate. We obtained property certificates by matrix replacement algorithm from platform configuration information and designed a trusted ring signature based on RSA Strong Assumption. By an analysis, the scheme is effective to resolve the security of cloud computing nodes. By simulation, we obtained the computational efficiency of the scheme. We also expand the protocol to the anonymous attestation based on ECC and give the scenario comparison between two schemes. However, in this paper, we only use the operation and deduce the property value, which has some limitations. So it is the next work to expand the scheme and make it more applicable.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was partially supported by the program "Major Projects of the Wireless Mobile Communications" (2012ZX03002003), The Research Fund for the Doctoral Program (New Teachers), Ministry of Education of China (Grant no. 20121103120032), Humanity and Social Science Youth Foundation of Ministry of Education of China (Grant no. 13YJCZH065), Opening Project of Key Lab of Information Network Security of Ministry of Public Security (The Third Research Institute of Ministry of Public Security), China Postdoctoral Science Foundation, and General Program of Science and Technology Development Project of Beijing Municipal Education Commission of China.

References

[1] CCID, "White Paper of Chinese Cloud Computing Industry Development," http://tech.ccidnet.com/zt/.

[2] C.-L. Tsai and U.-C. Lin, "Information security of cloud computing for enterprises," *Advances in Information Sciences and Service Sciences*, vol. 3, no. 1, pp. 132–142, 2011.

[3] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: challenges and solutions," in *Proceedings of the 7th International Conference on Informatics and Systems (INFOS '10)*, pp. 1–8, March 2010.

[4] Microsoft Corporation, "Building a secure platform for trustworthy computing," White Paper, Microsoft Corporation, 2002.

[5] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in *Proceedings of the USENIX Workshop on Hot Topics in Cloud Computing*, San Diego, Calif, USA, 2009.

[6] C. Mundie, P. de Vries, P. Haynes, and M. Corwine, "Microsoft white paper on trustworthy computing," Tech. Rep., Microsoft Corporation, 2002.

[7] K. Goldman, R. Sailer, D. Pendarakis, and D. Srinivasan, "Scalable integrity monitoring in virtualized environments," in *Proceedings of the 5th ACM Workshop on Scalable Trusted Computing (STC '10)*, pp. 73–78, Chicago, Ill, USA, October 2010.

[8] D. Safford, "Clarifying misinformation on TCPA," White Paper, IBM Research, 2002.

[9] D. Safford, "The need for TCPA," White Paper, IBM Research, 2002.

[10] Trusted Computing Group, *TPM Main Specification*, Main Specification Version 1. 2 Rev. 85, Trusted Computing Group, 2005.

[11] Trusted Computing Platform Alliance, *Main Specification*, Version 1.1b, 2002.

[12] T. C. Group, "TCG software stack specification," 2003, http://www.trustedcomputinggroup.org/.

[13] Trusted Computing Group, "TCG specification architecture overview, Specification Revision 1. 4," 2007.

[14] Trusted Computing Group, "Trusted computing platform alliance (TCPA) main specification, Version 1. 1a. Republished as Trusted Computing Group (TCG) main specification, Version 1. 1b," 2001, http://www.trustedcomputinggroup.org/.

[15] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 132–145, ACM, Washington, DC, USA, October 2004.

[16] Trusted Computing Group, "TPM main specification, main specification Version 112 revision 94," 2006, http://www.trustedcomputinggroup.org/.

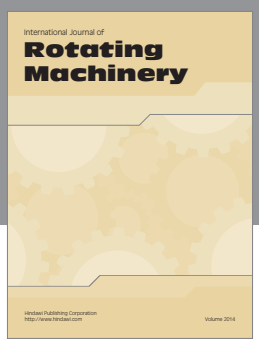
[17] A.-R. Sadeghi and C. Stüble, "Property-based attestation for computing platforms: caring about properties, not mechanisms," in *Proceedings of the New Security Paradigms Workshop*, pp. 67–77, Virginia Beach, Va, USA, September 2004.

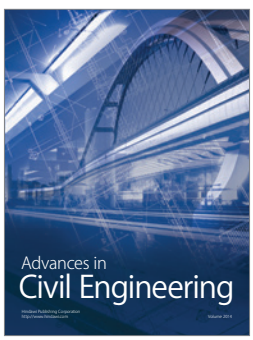
[18] L. Chen, R. Landfermann, H. Löhr, M. Rohe, A.-R. Sadeghi, and C. Stüble, "A protocol for property-based attestation," in *Proceedings of the 1st ACM Workshop on Scalable Trusted Computing*, pp. 7–16, Alexandria, Va, USA, November 2006.

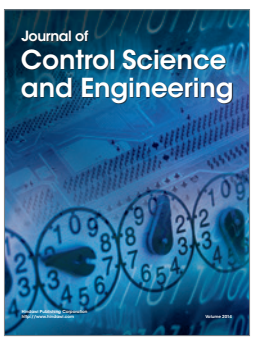
[19] D. J. Luo, "Efficient certificatieless anonymous attestation to trusted cloud coputing platforms," *International Journal of Advancements in Computing Technology*, vol. 4, no. 17, 2012.

[20] D. Boneh, C. Gentry, B. Lynn et al., "Aggregate and verifiably encrypted signatures from Bilinear maps," in *Advances in Cryptology: Proceedings of Enrocrypt*, pp. 416–432, Springer, Heidelberg, Germany, 2003.

[21] M. Burrows, M. Abadi, and R. Needham, "Logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.







Hindawi
Submit your manuscripts at
http://www.hindawi.com