Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2015, *9,* 415-421

Open Access

Design and Implementation of Remote Anonymous Attestation Protocol Based on Trusted Cloud Computing Platform

Liu Yan[1,*] and Xia Bin[2]

[1]*College of Information Engineering, Zhongzhou University, Zhengzhou, 450044, P.R. China;* [2]*School of Information and Management Science, Henan Agricultural University, Zhengzhou, 450002, P.R. China*

Abstract: Trusted cloud computing platform is a combination of the use of virtual machine technology and trusted computing technology of cloud computing platform. Virtual machine technology because of its high separability of the client and the resource of high controllability, which greatly improves the security of the system; and the trusted computing technology is through the establishment of a trusted root in the hardware layer, solve the credibility and safety problem of the system fundamentally, because of the close combination of Trusted Computing and the virtual machine technology to establish a "trusted cloud computing" can ensure that the user data and application in cloud environment fundamentally safe. In this paper, the trusted computing technology and properties of signature mechanism based on the proposed a trusted cloud is simple, safe and efficient computing platform remote anonymous attestation protocol RAA-TCCP protocol. The protocols without bilinear pairings, also need not attribute certificate and AIK certificate, which greatly simplifies the certificate management, and simultaneously realize the identity and integrity of the state of computing nodes to prove. The protocol has unforgeability, platform identity anonymity, privacy protection and allocation of collusion resistance, also has the very high efficiency even in a high security strength, good to meet the safety requirements and performance requirements of the cloud environment, remote attestation.

Keywords: Protocol, remote attestation, trusted cloud computing, Virtual machine technology.

1. INTRODUCTION

Trusted cloud computing platform is a combination of the use of virtual machine technology and trusted computing technology of cloud computing platform. Virtual machine technology because of its high separability of the client and the resource of high controllability, which greatly improves the security of the system; and the trusted computing technology is through the establishment of a trusted root in the hardware layer, solve the credibility and safety problem of the system fundamentally, because of the close combination of Trusted Computing and the virtual machine technology and the establishment of a "trusted cloud computing", can ensure the user data and application in cloud environment fundamentally safe.

At present, the trusted platform remote attestation mainly has two forms: proof of identity for the platform and platform for state integrity proof. Platform for proof of identity the typical Privacy based CA (Privacy Certificate Authorities [1]) proof, proof of based ring signature [2, 3]. Proof based on ring signature is a kind of more effective remote attestation scheme, it will ring signature is hidden in the ring members, to avoid the leakage of TPM platform identity, but a number of ring members determines the length of the ring signature and the anonymity, efficiency, by reducing the number of ring members reduce ring signature length and Improve the efficiency of the signature will sacrifice anonymity for the price. And according to the platform integrity state proved that the typical TCG binary proof (Binary Attestation), based on the attributes of the proof of (Property-based Attestation, PBA) etc. The TCG binary proved to be the most basic method of remote attestation; Remote Attestation Based on attribute to overcome the existing remote attestation complexity, privacy leakage and abuse of proven results and other defects. However, these remote attestation methods have low efficiency, certificate management difficulty is big, can not resist collusion attack and other issues, practicality is not high. For cloud computing platform, due to the uncertainty, mobility and opacity of compute nodes, these methods are more difficult to use. So it is urgent to an efficient, anonymous remote attestation scheme to solve the problem of cloud computing platform to prove the credibility. To this end, in 2009, Santos proposed a trusted cloud computing platform (Trusted Cloud Computing Platform, TCCP) model, turned to address cloud computing platform credibility ideas proved problem using trusted computing technology [4].

This paper assumes that the hardware resources is credible, combining with binary certificate and attribute based ring signature to prove, using the idea, design a simple, efficient cloud computing platform remote anonymous attestation protocol. The protocols without bilinear pairings, also need not attribute certificate and AIK certificate, it is through the use of an off-line trusted third party, application of trusted computing binding and sealing mechanism and attribute based ring signature (Property-Based Ring Signature, PBRS [5]) mechanism, and realizes the identity and integrity of the state of computing nodes to prove, and can not be and

1874-110X/15

collusion resistance forgery, identity anonymity, privacy protection configuration. In this paper, called RAA-TCCP (Remote anonymous authentication of trusted cloud computing platform) protocol.

2. PROTOCOL DESCRIPTION

In this paper, RAA-TCCP protocol from the abstract of a group, the platform configuration register (PCRs) in binary metric value into one or more attribute values, and with the platform, and then on the basis of attribute based ring signature (PBRS), credibility by verifying the ring signed the legitimacy to judge the computing nodes the. PBRS is using a ring signature concept attribute based signature. It will have the same attribute members form a ring, ring members can be with the one or more attributes as the identity. Because of the number of members with the same attributes of the unknown, so the identity of the signer can be hidden in the ring, and he takes a certain property or some attributes as the identity release news, but also can make the verifier believe the authenticity of the message. PBRS has the advantage of flexible, intuitive, and ring signature length and number of ring members independently, so PBRS can be conveniently and efficiently applied to anonymous authentication system.

The dependability of RAA-TCCP protocol suitable for IaaS, PaaS, SaaS and so on the different levels of service to prove. Without loss of generality, to provide the IaaS service as an example to describe the RAA-TCCP protocol. The RAA-TCCP protocol is divided into two phases of proof preparation and proof implementation as shown in Fig. (**1**). In the proof of the preparation stage, the compute nodes based on the N have EK certificate and PCR set of metrics signature key to a trusted third party TC application, TC binary verify its trusted after given its attribute value based on the sign and seal and signature key. In the proof of the implementation stage, the compute nodes N ring signature using the signature key, prove its security properties of the corresponding, user U and then through the validation of ring signature to determine the credibility of N, and then will be entrusted to the virtual machine to the trusted computing nodes. In order to facilitate the description, the following definitions symbol: EK_A^P shows the EK public key of A; P_A shows A generated public key; $\{X\}_K$ shows X is generated by key K ciphertext; K_{AB} shows between A and B session key; $A \to B$: X shows A sent message X to B; n_A shows nonce by A, to prevent replay attacks; TPM_A shows a trusted platform module A; V_{PCR-A} shows a group $PCRG_{PCR-A}$ value of TPM_A.

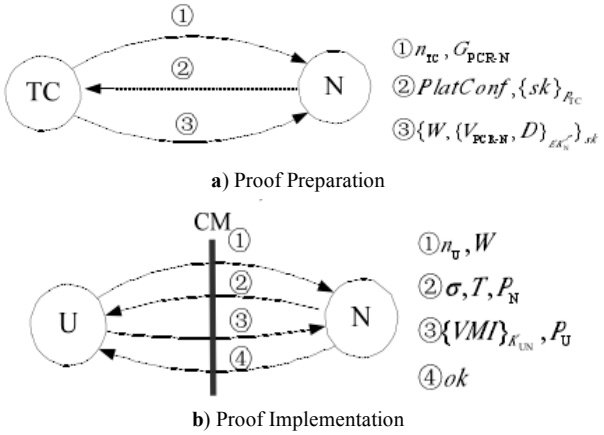

Fig. (1). RAA-TCCP protocol.

2.1. Proof Preparation

(1) System Established

Let E be the elliptic curve over a field F_q, q is a prime number, $E(F_q)$ is the set of all points of E, $\#E(F_q)$ is factorial of E, $P \in E(F_q)$ is the generating element elliptic curve of group $\langle p \rangle$, the order for a divisible $\#E(F_q)$ the big prime number p. TC randomly selects a private key $x \in Z^*_p$ and the two has the following form of collision free one-way Hash function: $H_0 : \{0,1\}^* \to \{0,1\}^K$, $H_1 : \{0,1\}^* \to Z^*_p$. where $\{0,1\}^K$ is the session key space. The complete definition of attribute value is Z_p. Remember x coordinates of $Q \in \langle P \rangle$ is $x_Q = [Q]_x$.

TC public p, P, H_0, H_1 and public key $P_{TC} = xP$, secure private key x.

(2) Attribute Certification

TC first N certification which has given security attributes, and attribute value. Because the property is an abstract concept, how will the property abstract information into the concrete numerical method based on attribute is the key. In this paper, the attribute abstraction method as shown in Fig. (**2**).

Definition 1: Attribute abstract is a function solving process from the PCR set of metrics to the attribute values as shown in Fig. (**2**), figure $\xrightarrow{f_i}$ shows mapping relation of $f_{i(i=1,2,3,4,5,6)}$, on which the digital representation of the

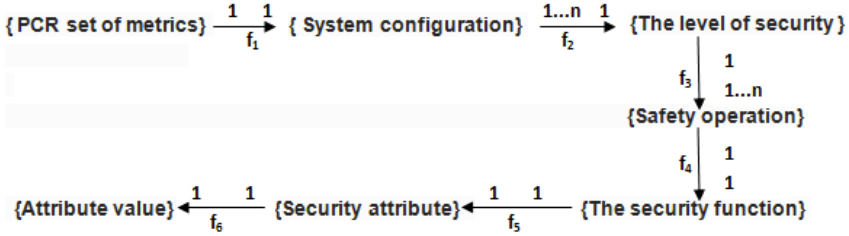

Fig. (2). Attribute abstraction method.

mapping types: f_1, f_4, f_5 and f_6 is a one to one mapping, f_2 is a many to one mapping, f_3 is the one to many mapping. This process is denoted as $F = F \circ f_1$, wherein, f_1 is called to verify the configuration function, its value is determined by SML, $F = f_6 \circ f_5 \circ f_4 \circ f_3 \circ f_2$ is called the attribute verification function, its value is determined by the security attribute evaluation criteria.

Note GPCRVALS represents a collection of {PCR set of metrics}, PROPVALS represents a collection of {attribute values}, it is not difficult to infer from Fig. (**2**), function $F : GPCRVALS \rightarrow PROPVALS$ is a many to many mapping. This function to PCR set of metrics Abstract property, because the PCR value represents the platform configuration state, and reflects the system components to start the order, so that the abstract is more simple and accurate properties.

Based on the function of F, the N property of the certification procedure is as follows:

$$TC \rightarrow N : n_{TC}, G_{PCR-N}$$

TC sends challenge n_{TC} to N, request N provides G_{PCR-N} of PCR group, as shown in Fig. (**1a**).

$$N \rightarrow TC : PlatConf, \{SK\}_{P_{TC}}$$

N interacts with TSS, request TPM_N to generate a session key generated sk, generate $\{SK\}_{P_{TC}}$ and $PlatConf = \{V_{PCR-N}, n_{TC}, SML, EndCred, PlatCred, ConCred\}_{sk}$, and then send it to the TC, as shown in Fig. (**1a**) ②. Among them, SML is the metric log of the corresponding to V_{PCR-N}; $EndCred$ is a certificate for EK (Endorsement Credential), is used to prove TPM manufacturer identity certificate; $PlatCred$ is a platform Certificate, is used to prove the platform manufacturer identity; $ConCred$ is a Conformance Credential, is used to prove TPM as a trusted building blocks (TBB) parts one of its design and implementation, consistent with the evaluation criteria.

The TC message is received after the verification certificate, is correct, whether the message is reproduced. If the verification is successful read SML and assembly standard value, imitation PCR extended operation, get the PCR desired set of metric values and standard PCR set of metrics. If the two is equal to V_{PCR-N}, N is proved credible and configuring security, so the calculation of TC value of the N attribute $F(V_{PCR-N})$, and then enter the key issue stage; or otherwise.

(3) Key Issue

Assuming that N has a security attribute set $W = \{\omega_i\}_{1 \le i \le n} = F(V_{PCR-N})(\omega_i \in Z_P)$, TC issued for the key steps are as follows:

1. Select a random number $r \in Z_P^*$, calculate G=rP, e= $H_1(W)$ mod p, t=$(xe+r)$ mod p, output signature key D=(G,t).
2. The TC obtains the $EK_N{}^P$ from the EK certificate, binding and sealing for the formation of D, then create $\{V_{PCR-N}, D\}_{EK_N{}^P}$. This D can only be decrypted by TPM_N, and only when the value G_{PCR-N} equal to V_{PCR-N}, D can be released.
3. The TC generated $\{W\{V_{PCR-N}, D\}_{EK^P{}_N}\}_{SK}$, and send it to N, then N saves it, as shown in Fig. (**1a**).

2.2. Proof Implementation

After N obtained the signature key, can prove its corresponding security properties set to the user U, as shown in Fig. (**3b**). The steps are as follows:

$$U \rightarrow N : n_U, W$$

U sends to the N challenge n_U, request N proves to have property set W.

$$N \rightarrow U : \sigma, T, P_N$$

N components ring as W, generating property signature σ. First of all, N interactive TSS, loading $\{V_{PCR-N}, D\}_{EK_N{}^P}$ to TPM_N. TPM_N checks that if V_{PCR-N} equal to G_{PCR-N}. If equal, TPM_N provides D = (G, t), or otherwise. If D is open, $s, r' \in Z_P^*$ were randomly selected by TPM_N, and calculate P_N = sP, $m = H_1(n_u, W, P_N)$, $Q = r'(P+G)$ $(Q \neq G)$, $\sigma_1 = (m + x_Q)$ mod p, $\sigma_2 = (r' - t\sigma_1)$ mod p, $T = (\sigma_1 + r')G$, generate property signature $\sigma = (\sigma_1, \sigma_2)$. N return σ together with T, P_N to U.

$$U \rightarrow N : \{VM\ I\}_{K_{UN}}, P_U$$

After U received the message ②, the calculate $e = H_1(W) \bmod p$, $m = H_1(n_U, W, P_N)$, $x_{Q'} = [\sigma_2 P + e\sigma_1 P_{TC} + T]_X$, $\sigma'_1 = (m + X_Q) \bmod p$, to verify the equation $\sigma'_1 = \sigma_1$ (1) Whether to set up. If established, then the N signature key issued by TC and is sealed, so N is trusted, then U select the random number $K \in Z_P^*$, $P_U = kP$, $K_{UN} = H_0(kP_N)$ calculation, and then generate $\{VMI\}_{K_{UN}}$, together with P_U sent to the N, let the virtual machine image VMI loaded on N start or otherwise;

$$N \rightarrow U : ok$$

After N received message ③, interact with the TSS, TPM_N compute $K_{NU} = H_0\left(sP_U\right)$, obviously $K_{NU} = K_{UN}$, and then decrypt $\left\{VM\ I\right\}_{K_{UN}}$. So N can start the user virtual machine, returns a successful information *ok*

Then, if the user virtual machine needs from the source node to the destination node A transplantation B, a virtual machine migration message exchange, as shown in Fig. (**3**).

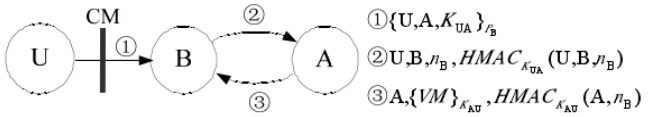

Fig. (3). Virtual machine migration message exchange.

1. U first use the method to validate the B credible, then generate $\left\{U, A, K_{UA}\right\}_{P_B}$ sent to the B;
2. The B to K_{UA} of $\left(U, B, nB\right)$ generates the hash message authentication code $HMAC_{K_{UA}}\left(U, B, nB\right)$ is sent to the A.
3. A was K_{AU} verified by $HMAC_{K_{AU}}\left(U, B, nB\right)$ as legitimate, then the virtual machine of U users use K_{AU} encryption to send to B. Thus to ensure user virtual machine running confidentiality and controllable.

3. PROTOCOL ANALYSIS

3.1. Correctness

Theorem (1) When attribute signature σ is true, equation is correct.

Proof: when σ true, correctness of equation (1) is as follows:

$$
\begin{aligned}
x_{Q'} &= \left[\sigma_2 P + e\sigma_1 P_{TC} + T\right]_x \\
&= \left[\sigma_2 P + e\sigma_1 P_{TC} + \sigma_1 G + r'G\right]_x \\
&= \left[\sigma_2 P + \sigma_1 (xe + r)P + r'G\right]_x \\
&= \left[(\sigma_2 + \sigma_1 t)P + r'G\right]_x \\
&= \left[r'P + r'G\right]_x = x_Q \qquad (1)
\end{aligned}
$$

So $\sigma_1' = \left(m + x_{Q'}\right) \bmod p = \left(m + x_Q\right) \bmod p = \sigma_1$.

3.2. Safety

Theorem (2) Under assumption of *DLP* problem, the attribute signature σ is unforgeable. Accurate to say, if the attacker can A with non negligible probability of forging property signature σ^*, then there exists a probability of a C attack algorithm can use the A to solve the *DLP* can not be ignored. p

Proof: assume that the attacker A can forge property signature σ^* point at certain platform attributes set W^*, C in order to solve the DLP, first set the public parameters of *paramas*: P, $P_{TC} = xP$, and then *paramas* told the attacker A, and kept secret private key x. In order to realize the consistency of *Oracle* queries of the attacker A, C maintain the following lists: L_{H_1} is used to store the *Hash Oracle* H_1 query and response data; L_1 is used to store the key of the simulation process of *Oracle Issue* query and response data; L_S is used to store the property proved that the simulating process in *Oracle Attest* query and response data.

Hash simulation: Set A oracle H_1 asked to attribute set W, if the previous to ask, then return the same result, otherwise C randomly selected $h \in Z_P^*, H_1\left(w\right) = h$, answer, and $\left(W, h\right)$ is added to the L_{H_1}.

The key issue of simulation: Set A to the set of attributes of $W\left(W \neq W^*\right)$ Oracle *Issue* asked if the previous to ask, then return the same result, otherwise the C first in the list of query in 1HL to record $\left(W, h\right)$, and then randomly selected $\bar{r} \in Z_p^*$, answer $\overline{D} = \left(\overline{G}, \bar{t}\right)$, where $\overline{G} = \bar{r}p$, $\bar{t} = \left(x\bar{e} + \bar{r}\right) \bmod p$, $\bar{e} = h \bmod p$, and the $\left(W, \overline{D}\right)$ is added to the L_1.

Proving Properties Simulation: let n_A be A nonce produced by the attacker, the attacker chooses $\left(n_u, W\right)$ request proved to possess the attribute set to W before W, if asked Oracle *Attest*, it returns the same result, otherwise the C first in the list of query in IL to record $\left(W, \overline{D}\right)$, and then randomly selected $\overline{R}' \in Z_P^*$, $P_C = \overline{S}P_1$ calculation, $\overline{m} = H_1\left(n_A, W, P_C\right)$, $\overline{Q} = \bar{r}'\left(P + \overline{G}\right)\left(\overline{Q} \neq \overline{G}\right)$, $\overline{\sigma_1} = \left(\overline{m} + X_{\overline{Q}}\right) \bmod p$, $\overline{\sigma_2} = \left(\bar{r}' - \bar{t}\,\overline{\sigma_1}\right) \bmod p$ answer property signature $\overline{T} = \left(\overline{\sigma_1} + \bar{r}'\right)\overline{G}$ $\overline{\sigma} = \left(\overline{\sigma_1}\,\overline{\sigma_2}\right)$ and $\overline{T}$, P_C, and $\left(\overline{m}, W, \overline{\sigma}, \overline{T}, P_C\right)$ into L_S.

Assuming the $\left(m^*, w^*\right)$ without being asked, if the attacker A in the choice of message m^* and choose Properties under w^* attack with non-negligible probability of successfully forged a property signature we can assume that A signed in before forged attribute query q_s Oracle Attest, the SQ is the name of a query answer to sign

$\sigma^{(i)} = (\sigma_1^{(i)}, \sigma_2^{(i)}) \neq (\sigma_1^*, \sigma_2^*)(i = 1,2,...,q_s)$, the following two approaches to discuss properties of signature unforgeability.

1) For the $\sigma^{(i)} = (\sigma_1^{(i)}, \sigma_2^{(i)})(i = 1,2,...,q_s)$, at least in the presence of $\varepsilon/2$ probability satisfy $\sigma_2^* + x\sigma_1^* = \sigma_2^{(i)} + x\sigma_1^{(i)}$. Calculates the A in this case $x = ((\sigma_2^{(i)} - \sigma_2^*)/(\sigma_1^* - \sigma_1^{(i)})) \bmod p$ so C can use A to solve the DLP.

2) For the $\sigma^{(i)} = (\sigma_1^{(i)}, \sigma_2^{(i)})(i = 1,2,...,q_s)$, at least by $\varepsilon/2$ probability satisfy $\sigma_2^* + x\sigma_1^* \neq \sigma_2^{(i)} + x\sigma_1^{(i)}$. At this point, according to verify the equality (1): $\left[\sigma_2^* P + e^* \sigma_1^* P_{TC} + T^*\right]_x = \left[\sigma_2^* P + e^* \sigma_1^* xP + \sigma_1^* r'^* P + r'^* r^* P\right]_x = \left[r'^* P + r'^* r^* P\right]_x$ professional $T^* = (\sigma_1^* + r'^*)G^*$, $G^* = r^* P$, $e^* = H_1(W^*)$, $r^*, r'^* \in Z_p^*$ two random number'pr is produced in the process of A forging. So A Computing: $x = ((r'^* - \sigma_2^* - \sigma_1^* r^*)/(\sigma_1^* e^*)) \bmod p$, so C can also use A to solve the DLP.

In short, if the attacker A can with non negligible probability ε of forging property signature σ^*, the probability of existence of C attack algorithm can use the A to solve the DLP can not be ignored.

Theorem (3) RAA-TCCP protocol with anonymity, platform collusion resistance and configuration of privacy protection.

Proof: This article built on RAA-TCCP protocol based on the attributes of a ring signed on, due to the function $F: GPCRVALS \to PROPVALS$ is a many to many mapping, $l = \left|\left\{V_{PCR-X} \middle| V_{PCR-X} \in GPCRVALS, F(V_{PCR-X}) = \{\omega\}_{1 \le i \le n} \subseteq PROPVALS\right\}\right| \ge 1$, and l is usually the number of computing nodes with $\{\omega\}_{1 \le i \le n}$, so the adversary guess probability ring outside the real signer's identity is not more than $1/l$, the probability of ring inside adversary guess the real signer's identity is not more than $1/(l-1)$, that is, the RAA-TCCP protocol has platform identity anonymity.

In addition, although the RAA-TCCP protocol in attribute certification requirements of N provide EK certificate and platform configuration information to the TC, but the agreement prove to U in N,N only provides property signature information σ and T, TC even with signature key $D = (G, t)$ of N, cannot be calculated σ and T, which makes N are anonymous to U and TC, so U cannot TC N and conspiracy to get the true identity of. At the same time, TC also can't and N conspiracy to deceive the U, because the signature key can only be issued by TC generating property legal signtheature, and the sinatuer key by binding and sealing cannot be migrated to other nodes using TC, this cannot be denied. Terefore, the RAA-TCCP protocol has the collusion resistance. Because of this platform identity anonymity and collusion resistance, the platform configuration information provided to TC N will also not be exposed, therefore, the RAA-TCCP protocol has the configuration privacy protection.

3.3. Validity

RAA-TCCP protocol is a simple, effective. Firstly, the RAA-TCCP protocol and realizes the identity and integrity of the state of computing nodes to prove. In the proof of the preparatory phase, EK certificate, certificate of conformance certificate platform and platform identity, SML and group PCR value platform integrity attestation state. While only verify the success to the corresponding security attributes and signature key, and sealing, binding to the signature key. To ensure that such implementation stage in the proof, only the holder of the signature key and the corresponding security configuration can generate legitimate property signature. The U attribute can be verified by the legitimacy of the signature to judge the credibility of N. When the user virtual machine migration occurs, the target host only be verified as authentic to obtain the session key, which can generate a valid HMAC, the source host according to the user virtual machine encryption to the target host, effectively ensure the confidentiality and user controllable virtual machine running.

Secondly, greatly enhance the efficiency of remote attestation. Adopting off-line trusted third party, the communication cost is low, the elimination of the efficiency bottleneck caused by using the online form; ring signature based on the attributes, so that the number of ring signature length and ring members independently, be fixed length of ring signature, eliminates the efficiency bottleneck number of ring members brought in to maintain anonymity, but also improve the efficiency of. In particular, the RAA-TCCP protocol to construct the whole scheme based on elliptic curve discrete logarithm problem, because the elliptic curve scalar multiplication cost far less than the bilinear pairing, thus greatly improve computational efficiency, than the proof protocol based on bilinear pairing at the same time, there are strict requirements on the bilinear nature of the elliptic curve, and its computational efficiency in high security intensity (1024-bit RSA the above security strength) will cause a series of problems [6]. Therefore, prove that the protocol without pairing will have lower computational complexity and higher universality. In order to efficient RAA-TCCP protocol description, in the 1024-bit RSA the same security level, the RAA-TCCP protocol and the existing typical based on bilinear pairing calculation comparison on the amount in the certification and verification proved that the scheme of PBA-BM [7] and AA-ABRS [8]. The PBA-BM scheme and AA-ABRS scheme of bilinear pairings and safety parameter selection based on literature [9] the method chooses the most efficient (160-bit r, 512-bit q) Type A curve, RAA-TCCP select 160-bit protocol stochastic elliptic curve. This paper only considers the time-consuming three operating larger: the pairing operations, scalar multiplication and exponentiation, while the PBA-BM scheme and AA-ABRS scheme known for advance computing bilinear.

Table. 1. Comparison of calculation amount with PBA-BM, AA-ABRS scheme.

Scheme	The Length of the Signature /bits	Prove the Amount of Calculation	Verify the Amount of Calculation
PBA-BM	5061	$_0T_a+_7T_b+_{12}T_c$	$_4T_a+_4T_b+_7T_c$
AA-ABRS	1026	$_0T_a+_5T_b+_0T_c$	$_2T_a+_0T_b+T_c$
RAA-CCP	320	$_0T_a+_2T_b+_0T_c$	$_0T_a+_3T_b+_0T_c$

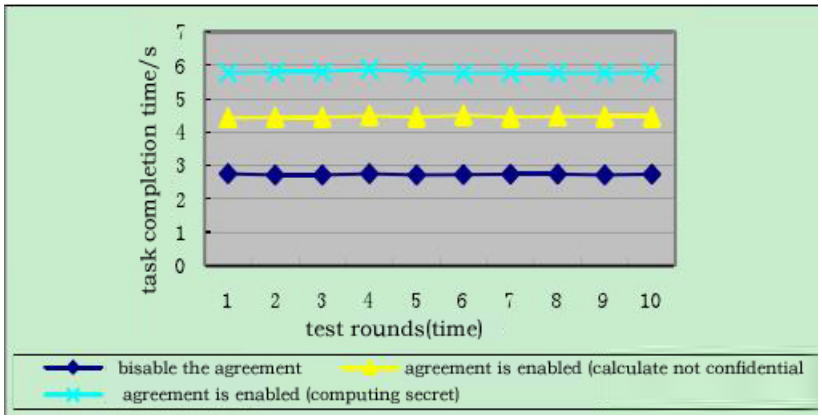

Fig. (4). RAA-TCCP protocol for computing the performance test results in the platform in the cloud.

Wherein T_a represents a bilinear pairing operation time, T_b represents a scalar multiplication time, T_c said one exponentiation time. It is seen from Table **1**, compared with the PBA-BM scheme of the new scheme, property signature length decreased from 5061 bits to 320 bits, 14.82 times shorter, certification and verification process is no longer a bilinear pairings and exponentiation, certification and verification efficiency has been greatly improved. At the same time, the new scheme without trusted third party issued by attribute certificate, attribute is judged through the ring signature be bound and sealed within the TPM signature key generated, so there is no attribute revocation checking problem; while the PBA-BM scheme also need to rely on an online trusted third party attribute revocation check, which increased the system management difficulty, also reduces the efficiency of the system. In addition, the new scheme in collusion resistance and no AIK certificate have unique advantages, the above characteristics make the new scheme in cloud computing has very good application platform. While the AA-ABRS scheme while also has the new scheme has the platform identity anonymity, configuration of privacy protection, collusion resistance and no attribute certificate and AIK certificate and other advantages, but because it still has 2 pairing and 1 exponentiation, so the operating efficiency of the new scheme is still high, and the properties of signature a new scheme of short length than.

4. EXPERIMENT RESULTS AND ANALYSIS

In order to verify the efficiency of the RAA-TCCP protocol, with a case of cloud computing based on Hadoop platform, a proof of the RAA-TCCP protocol implementation process simulation experiment. On the platform with MapReduce mode of 221 8-bit random integer (total 2MB) performs a counting task, counting using heap sort method, in order to avoid the difference of different random sequence sorting efficiency. The platform consists of 5 Pentium 4 CPU 2.0GHz, 512M memory, and are connected by a 100Mbps Ethernet computer built, of which 1 stations for the client, 1 to CM, the remaining 3 Taiwan as computing nodes. The CM is set to master, the calculation of the node is set to slaves, the 3 slaves is master assigned tasks are proved. Due to the current real TPM does not support the protocol of elliptic curve cryptography, this paper uses BouncyCastle library, use NIST 256-bit elliptic curve, RIPEMD160 hash, 128-bitAES symmetric cryptography, is the time to complete the task in the enabled RAA-TCCP co disable RAA-TCCP protocol, protocol (Computing unclassified), enable RAA-TCCP protocol (computing the confidential) for such as shown in Fig. (**4**). At the same time, in the same security level, single proof and verification process of the RAA-TCCP protocol, the PBA-BM scheme and AA-ABRS scheme also made analogy experiment. The experiment, in order to avoid the bilinear pairing initiated in high security problems in the strength, 160-bit *r* select the PBA-BM scheme and AA-ABRS scheme, the 512-bit *q* TypeA curve, the jPBC Library (Java Pairing-based Cryptography Library) [10] implementation; and the RAA-TCCP protocol, the choice of 160-bit random elliptic curve, the performance of the control as shown in Fig. (**5**).

Experimental results show that the RAA-TCCP protocol has high operation efficiency of computing platform in the cloud. In the 3072-bit RSA security strength, for counting task 221 integer 8-bit, in the calculation of confidential, the average task completion time is 4.454s; in

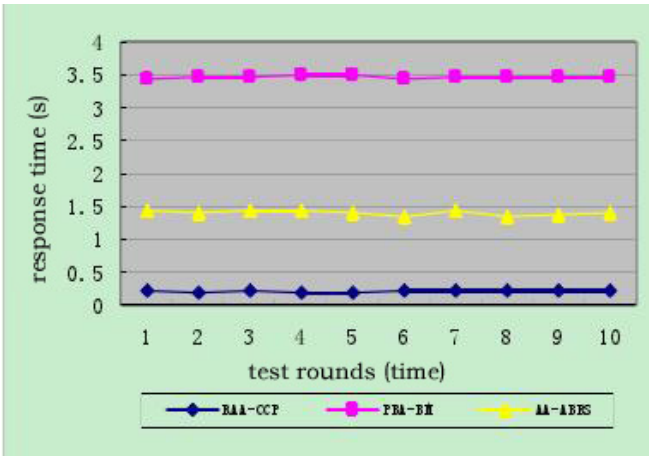

Fig. (5). RAA-TCCP and PBA-BM, the performance of AA-ABRS.

The calculation of secrecy, the average task completion time is 5.787s; and when to disable the RAA-TCCP protocol, the average task completion time for 2.721s, delay RAA-TCCP protocol brought in calculation is not confidential and keep were 4.454-2.721=1.734s and 5.787-2.721=3.066s. But in the process, the RAA-TCCP protocol is executed 3 times, computational secrecy, 1MB task 128-bitAES of data encryption - decryption executed 4 times, therefore, a delay in bringing single RAA-TCCP protocol process average of only 1.734/3=0.578s, delayed 0.578/2.721 * 100%=21.24%; delay of single 1MB mission data encryption or decryption brought only an average of (3.066-1.734)/(2*4) =0.167s, delayed 0.167/2.721* 100%=6.14%. Comparison of PBA-BM and AA-ABRS in the 1024-bitRSA scheme, RAA-TCCP protocol security strength, the average response time for 0.207s, PBA-BM average response time is 3.467s (excluding attribute revocation check time), the average response time for the 1.407s AA-ABRS scheme, the new scheme is 15.76 times faster than the PBA-BM scheme, AA-ABRS scheme is 5.80 times faster than. The above performance is mainly because the new scheme is no longer a bilinear pairings and exponentiation, therefore, even in a high security level, also has the very high operating efficiency.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was financially supported by the Henan Science and Technology Key Project Foundation (122102210507).

ABOUT THE AUTHORS

First Author Liu Yan, University lecturer of Zhongzhou University, Master. The author's major is Information Security.

Second Author Xia Bin, University lecturer of Henan Agricultural University, Master. The author's major is Data mining.

REFERENCES

[1] T. C. P. Alliance, "TCPA design philosophies and concepts (version 1)," https://www.trustedcomputinggroup.org, 2001.

[2] J. Liu, J. Zhao, and Y. Zhao, "Remote automatic anonymous attestation in trusted computing," *Chinese Journal of Computers*, vol. 7, pp. 1304-1310, 2009.

[3] L.Q. Chen, and H. Löhr, and M. Manulis, "Property-based attestation without a trusted third party," *Proceedings of 11th International Conference on ICS,* Taiwan, pp.31-46, 2008.

[4] N. Santos, and K.P. Gummadi, and R. Rodrigues, *Towards Trusted Cloud Computing*: CA, Berkeley, pp.56-68, 2009.

[5] W. Q. Wang and S. Z. Chen, *An Efficient Attribute-Based Ring Signature Scheme*: CA, Piscataway, pp.147-150, 2009.

[6] L. Hu, "Compression of Tate pairings on elliptic curves", *Journal of Software*, vol. 18, pp. 1799-1805, 2007.

[7] D. G. Feng, and Y. Qin, "A property-based attestation protocol for TCM," *Sciences China*, vol. 53, no. 3, pp. 454-464, 2010.

[8] D. J. Luo, and J. Zhang, "An efficient anonymous attestation attribute ring signature based on the property ring signature anonymity prove efficient protocol," *Computer Application Research*, vol. 12, no. 5, pp. 3470-3474, 2012.

[9] B. Lynn, *On the Implementation of Pairing-Based Cryptosystems,* Stanford University, California, pp. 420-441, 2007.

[10] B. Lynn, "The pairing-based cryptography library," http://crypto.stanford.edu/pbc/times.html, 2006.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014