Anonymous Identity-based Blind signature in the Performance Evaluation

Bo Zhao
College of computer science and information
Guizhou University
Guiyang, China
e-mail: 605340867@qq.com

Shiping Yang
College of Mingde
Guizhou University
Guiyang, China
e-mail: 907629797@qq.com

Abstract—**With the rapid development of science technology, especially the popularization of information construction, the performance evaluation under the network environment has become increasingly widespread. This paper describes the scheme and application about the performance evaluation. Firstly, we discuss the needs of the practical application of the performance evaluation, second, we study the classic identity-based blind digital signature-the Boneh identity-based cryptosystem. On this basis, we put Finally, applying this new scheme in performance evaluation, this paper constructs an online performance evaluation program based on the new blind signature scheme forward a new safe and efficient identity-based blind signature scheme we propose a new performance evaluation signature scheme by introducing the new concept of anonymous identity and analyze the security. After a rigorous analysis, the new program not only achieves the security requirements that the online performance evaluation should have, but also solves the key escrow problem, so this program has the features of operability and practicality.**

Keywords-Performance Evaluation; Information Security; Digital Signature; Annoymous Identiy; Bilinear Pairing

I. Introduction

Performance Evaluation of applications in the network environment has become increasingly widespread. Compared with the traditional way, the online performance evaluation has the outstanding features, which are evaluation management automation, information transparency, fairness and efficiency, so that the performance evaluation management is simple and easy for enterprises and government[1].

An ideal evaluation process should have the following characteristics.

a) Legitimacy: The process can only be evaluated by the legal evaluator.

b) Anonymity: The evaluation results of the evaluators are confidential and cannot be obtained unlawfully in the evaluation process.

c) Non-repeatability: Any legal evaluators cannot evaluate twice.

d) Verifiability: Under the premise that they cannot sacrifice their own personal secret information, the evaluators can check whether their evaluation information count in the results and publish or not[2].

To achieve a safe and reliable environment in the performance evaluation of complex Internet, digital signature technology plays a very important role[3-4]. In this paper, on the basis of identity-based blind signature, we introduce the concept of anonymity. From the needs of the practical application of the performance evaluation, we construct a new blind signature scheme and its application of online performance evaluation. The scheme can solve the above security needs. so this scheme has the features of operability and practicality.

II. Related Work

A. *Bilinear Pairings[5-7]*

The Let G_1, G_2 be the addition cyclic group with big prime number order and the multiplicationcyclic group with big prime number order. Let P be one $\mathrm{e}(\mathrm{P},\mathrm{Q})$ generator $G_1 =< \mathrm{P} >$. Assume the problem in the group G_1, G_2 is profound. Assume Bilinear Pairings $\mathrm{e}: G_1 \times G_1 \to G_2$ is a mapping which satisfy the conditions below:

- Bilinearity: $\mathrm{e}(aP, bQ) = \mathrm{e}(P, Q)^{ab}$ is valid for any $\mathrm{P}, \mathrm{Q} \in G_1$ and $\mathrm{a}, \mathrm{b} \in Z_q$.
- Non-degeneration: there exist $\mathrm{P}, \mathrm{Q} \in G_1$, which makes $\mathrm{e}(\mathrm{P}, \mathrm{Q}) \neq 1$.
- Computability: There exists a valid algorithm to calculate $\mathrm{e}(\mathrm{P}, \mathrm{Q})$.

Define some cryptography problems on the group G_1:

- Discrete Logarithm Problem (DLP): Suppose that P and Q are two elements from group G_1. It's difficult to find one integer $\mathrm{n} \in Z_q^*$ to satisfy $\mathrm{Q} = \mathrm{nP}$.
- Deduce Diffie-Hellman Problem (DDHP): Given $\mathrm{P}, \mathrm{aP}, \mathrm{bP}, \mathrm{cP} \in G_1$, $\mathrm{a}, \mathrm{b}, \mathrm{c} \in Z_q$. It is difficult to deduce that if $\mathrm{c} \equiv \mathrm{ab} \bmod \mathrm{q}$ is valid.
- Calculate Diffie-Hellman Poblem (CDHP): Given $\mathrm{P}, \mathrm{aP}, \mathrm{bP}$, it is difficult to calculate abP.

- Gap Diffie-Helloman Problem (GDHP): Given $\mathrm{P}, \mathrm{aP}, \mathrm{bP}, \mathrm{cP} \in G_1$ on group G_1, It's easy to deduce $\mathrm{c} \equiv \mathrm{ab} \bmod \mathrm{q}$, but it is easy to calculate abP. That is to say, DDHP is easy to solve, however, CDHP is difficult to solve on group G_1. Define the group as Gap Diffie-Hellman Group (GDH Group).

B. Boneh-Franklin Solution[8]

Boneh and Franklin put forward a identity-based signature solution, which is named Boneh -Franklin Solution. The solution divided into the following four steps:

1) The construction of system parameters

Produce two groups G_1, G_2 of order prime q, e is a bilinear pairings, select a generator $\mathrm{P} \in G_1$ arbitrarily. Let $\mathrm{a} \in Z_q^*$ and calculate $P_{pub} = sP$, s is the main encryption key. Select a Hash function $h : \{0,1\}^n \rightarrow G_1$, this Hash function matches the users' identity to the element in G_1. Select a Hash function $h_1 : \{0,1\}^n \rightarrow Z_q^*$, the Hash function decides the plaintext space $\{0,1\}^n$ The open system parameter is $\{G_1, G_2, e, n, q, P, P_{pub}, h, h_1\}$.

2) The production of user's private key

Suppose the only identifiable mark of user A is ID, calculate $Q_{ID} = h(ID)$, it is an element from G_1,the open key based on identity. Believable center calculate the matching private key according to the applicants' identity ID, the private key for user A is $S_{ID} = sQ_{ID}$.

3) The process of signature

The signer A select $\mathrm{r} \in_R Z_q^*$for the message $\mathrm{m} \in \{0,1\}^n$, calculate $U = rQ_{ID}$,$r_1 = h_1(m, U)$, $\mathrm{V} = (\mathrm{r} + r_1)S_{ID}$ .The signature of message m is (U, V).

4) The process of verification

Everyone can verify that if $\mathrm{e}(\mathrm{P}, \mathrm{V}) = \mathrm{e}(P_{pub}, \mathrm{U} + r_1 Q_{ID})$ is tenable for the signature of m.If the result is tenable,the signature is efficient.

III. A NEW IDENTIY-BASED BLIND DIGITAL SIGNATURE SCHEME

Based on identity-based blind signature, we introduce the concept of anonymity and construct a new blind signature scheme in this paper. This scheme can solve the key escrow problem and eliminate the leak of the actual identity radically.

The new scheme involves three participants, the key generation center KGC, user A, the owner of the message B, respectively. Here, we assume that KGC cannot be trusted. The scheme includes six stages: the establishment of system parameters, the generation of user's anonymous identity, the authentication of user's anonymous identity, the generation of user's keys, the generation of user's signature and the verification of user's signature.

1) The establishment of system parameters

Let G_1 be the cyclic addition group generated by the generator P, G_2 be the cyclic multiplication group with the same prime order q. $\mathrm{e}: G_1 \times G_1 \rightarrow G_2$ is a bilinear mapping. Define fine safe hash functions $H : \{0,1\}^n \rightarrow Z_q^*$, $H_1 : G_1 \rightarrow Z_q^*$, $H_2 : G_1 \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^n \times G_1 \rightarrow G_1$, $H_4 : \{0,1\}^n \times G_1 \rightarrow Z_q^*$. KGC selects a main encryption key $s \in Z_q^*$ randomly and calculates $P_{pub} = sP$ and the generation tag $M_{ID} = sP_{pub}$. KGC makes the parameter $params = \{G_1, G_2, e, q, P, P_{pub}, H, H_1, H_2, H_3, H_4\}$ public and keeps main encryption key s 和 M_{ID}.

2) The generation of user's anonymous identity

Assume the actual indentity of user A is ID.

- A selects $r_1 \in Z_q^*$ randomly and calculates $W' = r_1 P$. KGC saves (ID, W').
- KGC selects $k \in Z_q^*$ randomly and calculates $W = kW'$ and $S' = k^{-1} P_{pub}(H(ID) + H_1(W))$. Then sends the generation tag M_{ID} and (W, S') back to user A.
- A calculates $S = r_1^{-1} S'$ to throw off blindness. Then calculate $ID' = H_2(S)$ and ID' is the anonymous identity of user A.

3) The authentication of user's anonymous identity ers:

User can submit (ID, W, S, ID') to KGC to inspect if the equation below is tenable.

$$e(\mathrm{W}, S) = e(P, P_{pub})^{H(ID)+H_1(W)}$$

If tenable, calculates $ID_1' = H_2(S)$ and $ID_1' = ID'$ to verify whether ID' is the legal or not.

4) The generation of user's keys

User A selects $r_2 \in Z_q^*$ randomly and sends the anonymous identity ID', the generation tag M_{ID} and the value $r_2 P$ to KGC together. KGC first judges the legitimacy of user A by the value of M_{ID}, then calculates $Q_{ID} = H_3(ID', r_2 P)$, $S_{ID} = sQ_{ID}$ and treats S_{ID} as the part private key and sends back to A in a safe way. So the public key[9-10] of A is Q_{ID} and the private key is (S_{ID}, r_2).

5) The generation of user's signature:

Suppose m as the user B's message to sign, A selects $t \in Z_q^*$ randomly, and sends $U' = tQ_{ID}$ and $r_2 P$ to user B. B selects $\alpha, \beta \in Z_q^*$ as the blind factors and calculates $U = \beta U'$ and $h = \alpha\beta H_4(m, U)$, and B sends h to A. Then A sends $T' = th(r_2 Q_{ID} + S_{ID})$ back to B. Then B calculates $T = \alpha^{-1} T'$, and $(U, T, r_2 P)$ is the blind signature of the message m.

6) The verification of user's signature.

The verifier gets the blind signature of the message m $(U, T, r_2 P)$, calculates $h' = H_4(m, U)$ and inspects if the equation below is tenable.

$$e(P, T) = e(P_{pub}, H_1(m, U) * U)$$

IV. APPLICATION OF THE BLIND DIGITAL SIGNATURE IN THE PERFORMANCE EVALUATION

For the security requirements in the practical application of the Performance Evaluation, this paper proposes a Performance Evaluation signature scheme based on Elliptic Curve.

The participants in this scheme are as follow:

- Group Manager. The group manager is the highest rights center in the performance evaluation and is responsible for the initialization phase.
- Evaluator. The evaluators are the main subjects in the performance evaluation process. Submit the relevant evaluation information to verify if the evaluation results are modified.
- Authorization Center. Sign the sequence number of the evaluation and return it to the evaluators as to achieve the authorization purpose of the evaluation behavior.
- Statistical Center. Assess and collect the results of the legal evaluator and be responsible for publishing the results of the evaluation.

The process of online Performance Evaluation scheme is as following.

1) Step 1. The initialization of the scheme:

- Group Manager constructs the parameter of this scheme $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$ and make it public. s is the main private key.
- Evaluator V_i contact with Grout Manager GM and gets the anonymous identity ID'.
- The private key of valuator V_i is (S_{V_i}, r_{V_i}), and the public key is Q_{V_i} and $r_{v_i} P$ is also public. The evaluation authorization center AC chooses and publics the encryption algorithm E_{AC}, the signature algorithm S_{AC}, the public key (S_{ACS}, r_{AC}) and $r_{AC} P$. Keep the private key (S_{ACS}, r_{AC}) as private.
- Here, Group manager selects the specific meaning of the value of M_i, and makes it known to public.

2) Step 2. The authorization of Evaluator:

- V_i selects $w \in Z_q^*$ randomly as the valid sequence number of evaluation results. Calculate $H_5(w)$, $w' = H_5(w^{r_{V_i}})$, $m = H_5(w')$, and V_i encrypt them with the public keys of AC. Send the encryption result $E_{AC}(m \,||\, ID')$ to AC.
- AC decrypts $E_{AC}(m \,||\, ID')$ and gets m, ID'. First AC checks whether ID' is the first time to receive and it is the unique. After checking, it means that AC allows V_i uses $w \in Z_q^*$ as the legitimate sequence number and signs the message m and gets the signature $S_{AC}(m) = (U, T, r_{AC} P)$.

3) Step 3. The evaluation of Evaluator:

V_i gets the actual result of evaluation, then encrypts the result with the public keys of SC and gets $E_{SC}(w' \,||\, S_{AC}(m) \,||\, result)$ .Then send the encryption result to SC by anonymous channel.

4) Step 4. The final statistics and publication of the evaluation results:

- After receiving $E_{SC}(w' \,||\, S_{AC}(m) \,||\, result)$, SC decrypts it. SC first checks whether the evaluator V_i is the first time to evaluate, then judges the legality of the signature $S_{AC}(m)$.
- Statistics the result, and save the information $(w' \,||\, S_{AC}(m) \,||\, result)$. Make the information $(w', result)$ public.

5) Step 5. Evaluator send the information to Evaluation Statistical Agency:

The evaluator V_i could use w' to check whether own result is in the publish list of the SC and whether the content of the result is modification or not. Safety Analysis

V. CONCLUSION

The scheme can meet the practical security requirements of the performance evaluation process, the specific safety performance is as follows:

1) Legitimacy: To generate an annoymous identiy information for the user, The group manager must check whether the information submitted by the user is according to the actual indentiy information registering previous. Only registered, the user has the right to apply the annoymous identiy. Therefore illegal users want to impersonate legitimate evaluators, them must address the check of group manager. But it is impossible. So ther scheme meets legitimacy.

2) Non-repeatability: For legal evaluators, the group manager generates the correspinding anonymous identity for them and checks whether it is the frist time to get the annonymous identity. Likewise, the authorization center of evaluation also will check whether it is the first time to get the authorization of evaluation. If the evaluators want to evaluate more than one time, theyn must forge the signatures of the authorization center ,but it is considered to be very difficult.

3) Anonymity: One of the most important aspects is anonymity in this Performance Evaluation scheme. That is, it requires that Evaluation Verification Center can not know the specific result of Evaluator. In this paper, the scheme introduces the innovative concept of ‘annoymous identity’. The evaluators user their own anonymous identity participating the whole evaluation process, including the interactive with the authorization center, the transmission of the evaluation results. Even the public and private keys for evaluating is requested by annonymity identity. This evaluation process ensures absulute annoymity. Only the legal evaluators themselves could link the actual identity with the anonymity identity, other entities like the group manager, authorization center cannot get the relation.

4) Verifiability: When the evaluation is completed, the evaluator should be able to query whether the result of the evaluation is counted and modified or not. In this scheme, after having counted all the results of the evaluation, the statistical center publishes all evaluation results information. The evaluator checks whether ownself result information is publicly known in order to judge if his own evaluation result is counted or not; if known, then query whether the result is modified or not. Thus finish the query of the evaluation result.

From the above analysis and discussion of the scheme, we can see that this scheme is a comprehensive online Performance Evaluation scheme.

VI. Conclusion

In this paper, we introduce the concept of anonymous identity based on the classic blind identity-based digital signature scheme and construct a new identity-based blind signature scheme. It is obvious that the demand of security in the practical application of performance evaluator can be exactly met. In a word, the scheme in this paper has a good application value.

References

[1] Koziolek H. Performance evaluation of component-based software systems: A survey[J]. Performance Evaluation, 2010, 67(8): 634-658.

[2] Bakhshi R, Cloth L, Fokkink W, et al. Mean-field framework for performance evaluation of push–pull gossip protocols[J]. Performance Evaluation, 2011, 68(2): 157-179.

[3] Y. A. Xiao, L. Y. Li, “Study of digital signature techniques,” Jourmal of Wuhan Unieversity of Technology(Transportation Science and Engineering), 2002,26(6), pp.737-740.

[4] Neal Koblitz, The State of Elliptic Curve Cryptography, Designs Codes and Cryptography, 2000.19, pp.173-193.

[5] S.Seys.Anonymity and privacy in electronic serices[EB/OL]. http://www.cosic.esa-t.kuleuven.ac.be/apes/docs/d2_final.pdf, 2002

[6] Zhang L, Zhang F, Qin B, et al. Provably-secure electronic cash based on certificateless partially-blind signatures[J]. Electronic Commerce Research and Applications, 2011, 10(5): 545-552.

[7] Baldimtsi F, Lysyanskaya A. On the security of one-witness blind signature schemes[M]//Advances in Cryptology-ASIACRYPT 2013. Springer Berlin Heidelberg, 2013: 82-99.

[8] He D, Chen J, Zhang R. An efficient identity-based blind signature scheme without bilinear pairings[J]. Computers & Electrical Engineering, 2011, 37(4): 444-450.

[9] M. Rabin, Digital sigatures and public-key functions as intractable as factorization, MIN Lab of Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979.

[10] IEEE 1360-2000, “Standard Specifications for Public-Key Cryptography”, Available at: http://www.ieee.org/grouper/1363