TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.1, January 2014, pp. 802 ~ 808
DOI: http://dx.doi.org/10.11591/telkomnika.v12i1.3456

Id-Based Aggregate Signature Scheme and Its Application in Authenticated Routing

Daxing Wang*[1] , Jikai Teng[2]
[1]School of Mathematical Sciences, Chuzhou University, Chuzhou, Anhui, China 239000
[2]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China 100190
Corresponding author, e-mail: starleewipm@126.com, jikai@is.iscas.ac.cn

Abstract

An aggregate signature scheme can aggregate n signatures on n distinct messages from n distinct signers into a single signature. Thus, n verification equations can be reduced to one. So the aggregate signature adapts to Mobile Ad hoc Network (MANET). In this paper, we propose an efficient ID-based aggregate signature scheme with constant pairing computations. Compared with the existing ID-based aggregate signature schemes, this scheme greatly improves the efficiency of signature communication and verification. In addition, in this work, we apply our ID-based aggregate signature to authenticated routing protocol to present a secure routing scheme. Our scheme not only provides sound authentication and a secure routing protocol in ad hoc networks, but also meets the nature of MANET.

Keywords*: identity-based cryptography, aggregate signature, bilinear pairings, authenticated routing scheme*

1. Introduction

In the past decades, mobile communications have experienced an explosive growth. In particular, one area of mobile communication, the Mobile Ad hoc Networks (MANET) have attracted significant attention due to its multiple applications. MANET is a network consisting of mobile nodes which communicate with each other through wireless medium without any fixed infrastructure such as access points or base stations. Each node in ad hoc networks carries out networking functions such as packet forwarding, routing and network management, while only dedicated nodes like routers support networking functions in the wired network. Due to these characteristics, ad hoc network is especially exposed to security threats. Therefore, security in ad hoc networks is an essential component for basic networking functions.

The concept of aggregate signature was introduced by Boneh et al [1]. Idea of the aggregate signature scheme is to combine n signatures on n different messages, signed by n (possibly different) signers, and to obtain a single aggregate signature which provides the same certainty as the n initial signatures.

An approach to the construction of IBS schemes is a generic transformation that converts any standard signature (SS) schemes into IBS schemes. This approach is to use a SS scheme and simply attach a certificate containing the public key of the signer to the signature. This certification-based approach is apparently folklore. Bellare et al. [2] formalized the idea by providing a generic and secure construction of IBS schemes from any secure SS scheme. Recently, Galindo et al. [3] proposed a generic construction of IBS schemes with additional properties by extending Bellare et al.'s construction. Their results contain a generic construction of IBAS schemes from SS schemes which allow constant-length aggregations [4, 5]. However, the length of its resulting IBAS is linear with respect to the number of signers n because it consists of the aggregate signature from base standard signatures together with additional n public keys. Also, the technique has few applications because there is only one SS scheme which is constant-length aggregations, namely, BLS short signature schemes its AS scheme [6-8]. In that case, the converted IBAS scheme from Galindo et al. construction based on BLS scheme requires O(n) pairing computations. In practical situations where IBS provided by multiple signers for a long period of time are verified simultaneously, the verification cost and the flexibility would be preferable to the communication cost. We note that the pairing computation is the most time consuming in pairing-based cryptosystems. Although there have

Received June 13, 2013; Revised July 26, 2013; Accepted August 30, 2013

been many works discussing the complexity of pairings and how to speed up the pairing computation, the computation of the pairing still remains time-consuming. Thus, to construct a practically usable scheme, the number of pairing computations should be minimized [9-13]. In this paper, we propose an IBS scheme which allows an IBAS scheme with constant pairing computations. Our IBAS scheme requires neither an extra communication round nor a certain synchronization for aggregating randomness, while it does not achieve compactness.

We note that the pairing computation is the most time consuming in pairing-based cryptosystems. Although there have been many works discussing the complexity of pairings and how to speed up the pairing computation, the computation of the pairing still remains time-consuming. Thus, to construct a practically usable scheme, the number of pairing computations should be minimized. In this paper, we propose an IBS scheme which allows an IBAS scheme with constant pairing computations. Our IBAS scheme requires neither an extra communication round nor a certain synchronization for aggregating randomness, while it does not achieve compactness. The rest of the paper is organized as follows. In Section 2, we provide the preliminaries about aggregate signature. In Section 3, we propose a new IBAS scheme and compare with existing ones. After that, we present a security authenticated routing protocol in Section 4. Concluding remarks are given in section 5.

2. Preliminaries

2.1. Definitions and Computational Assumptions

Let G_1 be a cyclic additive group of order q, G_2 be a cyclic multiplicative group of order q, a map $e: G_1 \to G_2$ is said to be bilinear if it satisfies the following properties:

(1) Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and for all $a, b \in Z$.

(2) Non-degeneracy: There exists $P \in G_1$ such that $e(P, P) \neq 1$.

(3) Computability: There is an efficient algorithm to compute $e(P, P)$ for any $P, Q \in G_1$.

We call such a bilinear map as a admissible bilinear map. The Weil pairing and Tate pairing associate with super-singular elliptic curve can be modified to create such bilinear map.

The Computation Diffie-Hellman Problem (CDHP) is to compute abP for given $P, aP, bP \in G_1$. The Bi-linear Diffie-Hellman Problem (BDHP) is to compute $e(P, P)^{abc}$ for given $P, aP, bP, cP \in G_1$ for any $a, b, c \in Z_p$.

2.2. Components of IBAS Schemes

An IBAS scheme

$$IBAS = (setup, Extract, Sign, Agg, AVerify)$$

based on the IBS scheme

$$IBS = (setup, Extract, Sign, Verify)$$

is specified by five polynomial time algorithms with the following functionality:

Setup. The randomized parameter generation algorithm Setup takes input 1^k, where $k \in Z$ is the security parameter and outputs some publicly known system parameters.

Extract. The randomized private key extraction algorithm Extract takes input a user identity ID and a master secret msk, and outputs a private key

$$S_{ID} \leftarrow Extract(msk, m).$$

Sign. The randomized signing algorithm Sign takes input a private key S_{ID} corresponding to ID and a message $m \in \{0,1\}^*$, and outputs a signature

$$\sigma \leftarrow Sign(S_{ID}, m).$$

Verify. The randomized verification algorithm Verify takes input an identity ID , a message $m \in \{0,1\}^*$, and outputs True if

$$\textbf{Verify}(m, ID, \sigma) = 1,$$

or False otherwise.

Agg. The aggregate signature generation algorithm Agg based on the Sign algorithm takes input a sequence of signatures $\{\sigma_i\}_{i=1}^n$ on $\{m_i\}_{i=1}^n$ for $\{ID_i\}_{i=1}^n$ and outputs an aggregate signature

$$\sigma \leftarrow Agg(\sigma_1, \mathrm{L}\ , \sigma_n).$$

AVerify. The aggregation verification algorithm AVerify takes input a sequence of identities $(ID_i, \mathrm{L}\ , ID_n)$, messages $(m_1, \mathrm{L}\ , m_n)$ and an aggregate signature σ and outputs True if

$$\textbf{AVerify}(m_1, \mathrm{L}\ , m_n, ID_1, \mathrm{L}\ , ID_n) = 1$$

Or False otherwise.

3. New Efficient ID-Based Aggregate Signature Scheme

3.1. Proposed ID-Based Aggregate Signature Scheme: IBAS

Now, we propose a new IBS scheme which allows to construct an efficient IBAS scheme.

Setup. Given a security parameter $k \in Z$, the algorithm works as follows:

(1) Run the parameter generator on input k to generate a prime q , two groups G_1, G_2 of order q , a generator P in G_1 and an admissible pairing $e: G_1 \times G_2 \to G_2$.

(2) Pick a random $s \in Z_q^*$ and set $P_{pub} = sP$.

(3) Choose cryptographic hash functions

$$H_1: \{0,1\}^* \to G_1 \text{ and}$$
$$H_2: \{0,1\}^* \to Z_q .$$

The system parameters is

$$Params = (q, G_1, G_2, e, P, P_{pub}, H_1, H_2).$$

Extract. For a given string $ID \in \{0,1\}^*$,

(1) Compute $Q_{ID} = H_1(ID) \in G_1$.

(2) Set the private key S_{ID} to be $s \cdot Q_{ID}$, where s is a master secret.

Sign. Given a private key S_{ID} and a message $M \in \{0,1\}^*$,

(1) Choose $r \in_R Z_q^*$ and compute

$$U = r \cdot P \in G_1.$$

(2) Compute

$h = H_2(ID, M, U) \in Z_q$, and

$$V = S_{ID} + h \cdot r \cdot P_{pub} \in G_1 .$$

The signature on m is

$$\sigma = (U, V) .$$

Verify. Give a signature $\sigma = (U, V)$ of m for an identity ID,
(1) Compute

$$Q_{ID} = H_1(ID) \in G_1 \quad \text{and}$$
$$h = H_2(ID, M, U) \in Z_q .$$

(2) Verify where

$$e(V, P)$$
$$= e(Q_{ID} + h \cdot U, P_{pub})$$

holds or not. If it holds, accept the signature.
By bilinearity of the pairing e, the consistency of the scheme is easy to verify:

$$e(V, P)$$
$$= e(S_{ID} + h \cdot r \cdot P_{pub}, P)$$
$$= e(Q_{ID} + h \cdot U, P_{pub})$$

Agg. Let $A = \{A_1, \mathrm{L}\ , A_n\}$ be the set of users. For an aggregating subset of users $S \subseteq A$, assign to each user an index i, ranging from $1 to\ k = |S|$.
(1) Each user $A_i \in S$ computes (U_i, V_i) on a message $M_i \in \{0,1\}^*$.
(2) Compute

$$V = \sum_{i=1}^{k} V_i \quad \text{and output}$$
$$\sigma = (U_1, \mathrm{L}\ , U_k, V)$$

as an aggregate signature.
AVerify. Given an aggregate signature $\sigma = (U_1, \mathrm{L}\ , U_k, V)$ as above,
(1) Compute

$$Q_i = H_1(ID_i) \quad \text{and}$$
$$h_i = H_2(ID_i, m_i, U_i) , \quad i = 1, \mathrm{L}\ , k.$$

(2) Verify where

$$e(V, P)$$
$$= e(\sum_{i=1}^{k} (Q_i + h_i \cdot U_i), P_{pub})$$

holds or not. If it holds, accept the aggregate signature, Or reject otherwise.

3.2. Comparison

Here, we will compare our scheme with schemes in Refs. [4-6] in terms of the computational efficiency (i.e., number of expensive cryptographic operations such as exponentiations or bilinear maps). The detailed comparison result is given in Table 1. We use P and SM as abbreviations for pairing computation and scalar multiplications respectively.

Table 1. Comparison of schemes

IBAS Scheme	Signature length	Sign	Averify
[4]	$(k+1)\|G\|$	2 *SM*	$(2k+1)P$
[5]	$(k+1)\|G\|$	3 *SM*	$(k+1)P+kSM$
[6]	$(k+1)\|G\|$	1 *SM*	$(k+1)P+kSM$
Our scheme	$(k+1)\|G\|$	2 *SM*	$2P+kSM$

4. Security Routing Scheme

In this subsection, we present a security routing scheme with on-demand routing protocol which consists of three phase: Initialization phase, route discovery phase and route maintenance phase. The security of it is based on the ID-based aggregate signature presented above.

4.1. Initialization Phase

Initialization phase is performed only once prior to the formation of the Ad hoc network. In this phase, off-line server sets up system parameters and distributes each node's private key securely.

4.2. Route Discovery Phase

Route discovery makes a node discover dynamically a route to any other node. Route discovery has three stages: the initiator node broadcasts a route discovery packet called RDP, the intermediate nodes process the RDP message, and the target node receiving the RDP message returns a route reply message called REP to the initiator node. By verifying the aggregate signature, the target node can authenticate each intermediate node on a path and check the integrity of the message. The main advantage is that it requires less communication cost. Moreover, it needs no certificate chain. A route request message contains six fields:

<RDP, IPA, IPX, seq, nodelist, aggsign>.

The RDP is a packet type identifier, IPA and IPX are the node A and X's IP address respectively. The seq is incremented whenever node A issues a new RDP, the nodelist is a list of intermediate nodes on the route between initiator and target node X, and the aggsign is an aggregate signature integrated by node A and intermediate nodes. When any node receives an RDP, it processes the message according to the following steps:

Step 1 If the RDP message from node A has received recently, namely the pair (IPA, seq) for the RDP is found in this node's received request list, then discard the message and do not process it further.

Step 2 Otherwise, if this node is not the target of the RDP, then add this node's identity to the nodelist and generate its own signature on the following fields:

<RDP, IPA, IPX, seq, nodelist>,

and aggregate its signature into the aggregate signature, then re-broadcast the message.

Step 3 Otherwise, if this node is the target of RDP, then verify the aggregate signature in the RDP.

(1) If the aggregate signature is valid, then return a REP message to node A;
(2) Otherwise, discard the message and do not process it further.

A route reply message contains the following fields:

<REP, IPX, seq, nodelist, sign>.

The REP is a packet type identifier and IPX, seq, nodelist fields are set to the corresponding values from the RDP message. The seq is incremented whenever the target node issues a new RDP and the sign is a signature of node X. To describe this procedure given in Firgue 1 in details, we take an example that the initiator Node A attempts to discover a route to the target node X. Let node A's next hop be Node B, Node B's next hop be Node C, and Node C's next hop be the target node X.

$$A \to Sign_A[RDP, IP_A, IP_X, seq(A)]$$
$$Aggsign = Sign_A[RDP, IP_A, IP_X, seq(A)]$$
$$B \to Sign_B[RDP, IP_A, IP_X, seq(B)]$$
$$Aggsign = Aggsign + Sign_A[RDP, IP_A, IP_X, seq(B)]$$
$$C \to Sign_C[RDP, IP_A, IP_X, seq(B,C)]$$
$$Aggsign = Aggsign + Sign_C[RDP, IP_A, IP_X, seq(B,C)]$$
$$X: Verify\ the\ aggregate\ signature$$
$$Aggsign \stackrel{?}{=} (Sign_A + Sign_B + Sign_C)$$
$$X \to A: Sign_X[REP, IP_A, IP_X, seq(B,C)]$$
$$Sign_X = Sign_X[REP, IP_A, IP_X, seq(B,C)]$$

Figure 1. The procedure of REP

4.3. Route Maintenance Phase

If, for example, node B discovers that the link to node C is broken, it sends an error message (ERR) towards the source of the route. The ERR message has the following format:

SignB< ERR, IPA, IPX, seq, nodelist >

Since it is in general difficult to distinguish malicious ERR message from correct ERR messages, especially in very volatile networks, it may be useful to maintain a count of the number of ERR messages that each node generates. If a node generates an abnormally high number of ERR messages (compared with other nodes), it is likely that this node is malicious (since ERR are signed and it can be verified that such a node actually generated those messages). Hence such a node must be avoided during routing.

5. Conclusion

In this paper, we proposed a new IBAS scheme with constant pairing computations. It achieves a dramatic improvement in computational complexity for verification. In addition, based on the new aggregate signature, we design a secure routing protocol scheme, which could provide sound authentication in ad hoc networks without certificate management problem, and reduces communication cost significantly.

Acknowledgments

This research was supported by the Natural Science Research Project of Education Office of Anhui Province (KJ2013B185), and the Natural Science Research Project of Chuzhou University (2012kj001Z).

We want to thank the members of our research group, who provided a lot of helpful advice for this paper.

References

[1] D Boneh, C Gentry, B Lynn. *Aggregate and verifiably encrypted signatures form billinear maps*. Proceedings of Advances in Cryptology-Eurocrypt' 2003, Warsaw. 2003: 416.432.

[2] Bellare M, Namprempre C, Neven G. *Security proofs for identity-based identification and signature schemes*. Advances in Cryptology: Eurocrypt'04, LNCS 3027. London. 2004: 268-286.

[3] Galindo D, Herranz J, Kiltz E. *On the generic construction of identity-based signatures with additional properties*. Advances in Cryptology: Asiacrypt'06, LNCS 4284. Shanghai. 2006: 179-193.

[4] Xu J, Zhang Z, Feng D. *ID-based aggregate signatures from bilinear pairings.* CANS'06, LNCS 3810. Berlin. 2006: 110-119.

[5] Yoon HJ, Cheon JH, Kim Y. *Batch verification with ID-based signatures*. ICISC'08, LNCS 3506. Springer-Verlag. 2008: 233-248.

[6] Herranz J. Deterministic identity-based signatures for partial aggregation. *The Computer Journal*. 2011; 49(3): 322-330.

[7] Gentry C, Ramzan Z. *Identity-based aggregate signatures* , 9th International Conference on Theory and Practice of Public Key Cryptography, LNCS. Berlin, 2006: 257-273.

[8] Bellare M, Namprempre C Neven G. *Unrestricted aggregate signatures*, Proceedings of ICALP 2007. LNCS 4596, Springer-Verlag. 2007: 411-422.

[9] Yifei Zhang and Hongli Zhang. An Experience-Based Algorithm for Securing Network Coordinate Systems. *ICIC Express Letters, Part B: Applications*. 2011; 2(4): 995-1002.

[10] Li Yifan, Chen Huiyan. Application of Id-Based Aggregate Signature in MANETs. *Journal Of Electronics*. 2012; 27(4): 516-521.

[11] Kang BY, Boyd C, Dawson E. A novel identity-based strong designated verifier signature scheme. *The Journal of Systems and Software*. 2011; 82(2): 270-273.

[12] Zhifeng Yan, Futai Zhang, Wenjie Yang. Cryptanalysis to a certificateless threshold signa- ture scheme. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1496-1502.

[13] YULIAN Shang, Wuyuan Jia, Lanhua Zhang. A General Threshold Signature and Authenti- cated Encryption Scheme Based on ElGamal System. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(7): 3789-3797.