A Novel Certificateless Aggregate Signature Scheme without Bilinear Pairings

Xiao TIAN

Department of Health Management, Nanyang Medical College, Nanyang, China

tianxiaoxiao1988@126.com

Keywords: Certificateless, Aggregate Signature, Bilinear Pairings

Abstract. Most of the aggregate signature schemes are based on identity public cryptosystem that these identity-based aggregate signatures have certificate management and key escrow problems. And most of these schemes use the bilinear pairings and efficiency is not high. A novel aggregate signature scheme (CLAS-BP) is proposed based on the certificateless public key cryptography theory. This scheme solves the key escrow problem of the identity-based public key cryptography and not uses the bilinear pairings. The analysis shows that this scheme provides a high security and efficient.

Introduction

Aggregate signature can aggregate signatures of n signers to n different message into a signature that make n signature verification into one signature verification. The aggregate signature is proposed to provide for several signatures of several users to verify and it is convenience that only needs once verification for several users. The message being signed is only known by the signer and key generation center (KGC) and the private key to be used for signing is related to identity, so the aggregate signature is widely used in the e-commerce, e-government and electronic money system. On other hand, the aggregate signature is also can be applied well to the secure communication to design the verifiably encrypted signature and ring signature.

Boneh[1] et al. proposed the aggregate signature in 2003. Aggregate signature can provide non-repudiation service for several users and messages. It can compress any number signatures into a signature that reduce the signature of storage space and the computational effort for signing and verifying greatly. Lysyanskaya[2]and Ostrovsky[3] et al. proposed the corresponding sequence aggregate signature schemes respectively. Cheon[4] et al. use the forking lemma developed the first identity-based aggregate signature scheme in 2004. Herranz[5] et al. proposed a definitive identity-based partially signature scheme. Gentry[6] et al. proposed an identity-based signature scheme. Camenisch[7] et al. proposed a batch processing validation short signature scheme. However, these schemes have the key escrow problems and use more bilinear pairings that some extent influences the signature efficiency. In order to improve the signature efficiency, we proposed the CLAS-BP based on the certificateless public key cryptography theory. This scheme satisfies the security requirements of aggregate signature and has more efficiency.

In this paper, firstly we introduced the difficult problems, assumptions and the basic model of certificateless signature. Secondly we proposed a novel CLAS-BP scheme. Our scheme use certificateless public key cryptography theory to solve the key escrow problem and the CLAS-BP scheme satisfies most of the security requirements of aggregate signature. Thirdly, our scheme without uses the bilinear pairings and provides a high efficient.

Paper organization is as follows: section 2 introduces the difficult problems, assumptions and the basic model of certificateless signature. The CLAS-BP is described in section 3. Section 4 gives the security analysis of CLAS-BP. The efficiency analysis is described in section 5.The conclusion is drawn in section 6.

Preliminary Knowledge

Difficult Problems and Assumptions

Computational Diffie-Hellman (CDH) problem: p,q are two prime numbers, and $q|(p-1)$, g is an order for the generation of q element, $a,b \in Z_p^*$, and $g,g^a,g^b \in Z_p^*$,to calculate $g^{ab} \in Z_p^*$.The probability of success to solve the CDH problem:

$$Succ_{Z_p^*,A}^{CDH} = \Pr[g^{ab} \leftarrow A(g,g^a,g^b)] \tag{1}$$

The probability calculation is based on a,b in Z_p^* random selection and the random selection for algorithm A.

Define 2.1[8]. CDH hypothesis: For any polynomial algorithm A, the probability to solve the CDH problem is negligible.

Discrete logarithm (DL) problem:p,q are the two prime numbers, and $q|(p-1)$, g is an order for the generation of q element and $g,g^a \in Z_p^*$to find $a \in Z_p^*$. The probability of success to solve the DL problem:

$$Succ_{Z_p^*,A}^{DL} = \Pr[a \leftarrow A(g,g^a)] \tag{2}$$

The probability calculation is based on a,b in Z_p^* random selection and the random selection for algorithm A.

Define 2.2[8]. DL hypothesis: For any polynomial algorithm A, the probability to solve the DL problem is negligible.

The Basic Model of Certificateless Signature

In 2003 certificateless public key cryptography (CL-PKC) was proposed by Riyami and Paterson [6].It doesn't require the use of certificates in traditional public key cryptography and solves the key escrow problem of the identity-based public key cryptography. The signature based on certificateless cryptography includes seven algorithms, these are as follows:

System setup: Enter the security parameter k,KGC output system master key x and system parameters params.

Partial key extract: Enter system parameters, master key x, user A's identity ID_A, and output user's partial private key.

Set secret value: Enter system parameters, user A's identity ID_A, and the user A randomly selects x_A as his secret value.

Private key extract: Enter system parameters, user A's identity ID_A, secret value x_A and output user A's private key SK_A.

Public key extract: Enter system parameters, user A's identity ID_A, secret value x_A and output user A's public key PK_A.

Sign: Enter system parameters, user A's identity ID_A, the message M to be signed and the private key SK_A, generates a signature σ.

Verify: Input the system parameters params, the message M, the signature σ, the public key PK_A of signature user A and user A's identity ID_A. If the signature is true, output 1, otherwise output 0.

CLAS-BP Scheme

The Description of CLAS-BP Scheme

- System setup: Input security parameter k, the key generation center (KGC) outputs two large prime numbers p,q, and $q|(p-1)$. KGC randomly selects g from Z_p^* as an order for the generation of q, the g generated subgroup is G. KGC randomly selects $x\in Z_q^*$and computes $y= g^x$. KGC selects hash function: $H_1:\{0,1\}^*\times Z_p^*\rightarrow Z_q^*$, $H_2:\{0,1\}^*\times Z_p^*\times Z_p^*\rightarrow Z_q^*$. The public system parameters are: params= $\{p,q,g,y,H_1,H_2\}$, master key msk= x and x $\in Z_q^*$.
- Partial key extract: The user i input identity ID_i to KGC, KGC selects r_i from Z_q^* randomly and computes R_i=g^{ri}, $Q_i=H_1(ID_i,R_i)$, $D_i=r_iH_1(ID_i,R_i)=r_iQ_i$. KGC return D_i, Q_i to user i through the security channel and put D_i as partial private key of user i.
- Set secret value: User i randomly selects x_i from Z_q^* as long-term secret value.
- Private key extract: User i input params, partial private key D_i and the client output the private key S_i, S_i=x_i. And generates complete private key SK_i=<S_i, D_i>.
- Public key extract: User i selects secret value x_i to compute $X_i=g^{xi}$, and generates public key PK_i=<X_i,R_i>.
- Single signature: The message required signing of the user i is M_i, $h_i=H_2(X_i,ID_i,M_i)$, $U_i=g^{xi}=X_i$, $V_i=r_i+h_i+x_i$, generates signature $\sigma_i=(U_i,V_i)$.
- Aggregate signature: Compute $U=U_1U_2\ldots U_n$, $V= (V_1, V_2,\ldots,V_n)$. So the $\sigma=(U,V)$ is the aggregate signature of the messages $M_1, M_2,\ldots,M_n$.
- Single signature verification: The verifier received the signature compute $U_i^{'}=X_i^{'}=g^{Vi}/(R_ig^{hi})$, verifies $U_i^{'}=U_i$.
- Aggregate signature verification: The verifier received the signature will compute $X_i^{'}=g^{Vi}/(R_ig^{hi})$, $X=X_1X_2\ldots X_n$, $U^{'}=X$, if $U^{'}=U$, the verifier will accept, otherwise reject.

The validity of Signature

Proposition 3.1 The validity of signature σ: $U=U_1U_2\ldots U_n=X_1X_2\ldots X_n$.

Proof $$U=\prod_{i=1}^{n} g^{V_i}/(R_i\,g^{h_i})=\prod_{i=1}^{n} g^{r_i+h_i+x_i}/(R_i\,g^{h_i})$$

$$=\prod_{i=1}^{n} X_iR_ig^{h_i}/(R_i\,g^{h_i})$$

$$=\prod_{i=1}^{n} X_i$$

Security Analysis

The Uncomputability of Private Key

The security of private key is based on the KGC and the user and it is not to reveal the private key of system and users. The private key of system r_i and the private key of user xi is very important because the private key SK_i of signers depends on them. Only the private keys of system and users are all attacked that the entire system will be breached. However, if attackers compute the system and the user private key x_i, r_i, its difficulty is to solve elliptic curve discrete logarithm problem. So it is computationally infeasible.

The Non-forgeability of Single Signature

If an attacker u pretended as a signer to forge single signature $\sigma_u=(U_u,V_u)$. The U_u can be obtained by the public key but V_u cannot be calculated correctly. The reason is that $V_u=r_u+h_u+x_u$ and the r_u,x_u,h_u is unknown for the attacker u. So the σ_i cannot be forged correctly by the attacker. The attacker to obtain the r_u,x_u that the difficulty is to solve elliptic curve discrete logarithm problem.

The Non-forgeability of Aggregate Signature

The same as the non-forgeability of single signature that the attacker can forge U_u but cannot forge V_u. If an attacker wants to obtain the signatures that need to calculate all the private key of the signers and it is obviously impossible. Even if the attacker gained one or several private key, it is not possible to be validated. Assumed the attacker have obtained the n-1 signatures of signers but just is not getting the signature of u_n that it still cannot get the private key SK_n of u_n.

The Unrelatedness of Private Key

The private key is composed of the system private key and the user private key. The system private key is the hash value of identity and the random number selected by system and it is irrelevant to the other value. The attacker obtains the system and user private keys that are computationally infeasible. The hash value is secret for anyone except the signer and KGC. The user private key is selected by user that is irrelevant to other value. If the attackers want to deduce other users' private key from one user private key that is also computationally infeasible.

Performance Analysis

The efficiency of n signatures aggregation is mainly reflected in the key calculation, the generation and verification of signatures. The paring operation, exponentiation computation and scalar multiplication is major considered when assessment computational cost of the schemes in this paper. Where *Pa* denotes a paring operation, *Exp* denotes one exponentiation computation and *Sm* denotes one group of scalar multiplication. The computational cost comparison results are as in table1.

Table 1. The computational cost comparison

scheme	calculated price		
	signature	verification	total
Xu[9	2n*Sm*	(2n+1)*Pa*	(2n+1)*Pa*+2n*Sm*
Wen[10]	2n*Sm*	(n+1)*Pa*+n*Sm*	(n+1)*Pa*+3n*Sm*
Yu[11]	6n*Sm*	5n*Pa*	5n*Pa*+6n*Sm*
CLAS-BP	n*Exp*+n*Sm*	2n*Exp*+(n-1)*Sm*	3n*Exp*+(2n-1)*Sm*

The scheme of Xu total uses (2n+1)*Pa*+2n*Sm*, the Wen total uses (n+1)*Pa*+3n*Sm* and the Yu total uses 5n*Pa*+6n*Sm*. Our schemes total needs 3n exponentiation computations and 2n-1 scalar multiplication. However, the computational complexity of bilinear pairings is seven times than exponentiation computation [8]. So compared with the other schemes, our scheme has the higher efficiency.

Conclusion

In this paper, we propose a novel aggregate signature scheme based on the certificateless public key cryptography theory. This scheme solves the identity based aggregate signature schemes in the key escrow problem. The analysis shows that our scheme satisfies the security requirements of aggregate signature. Our scheme requires need 3n exponentiation computations and 2n-1 scalar multiplication. Compared to other aggregate signature schemes, it has more efficiency.

References

[1] B. Dan, C. Gentry, B. Lynn, H. Shancham: *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, in: Lecture Notes in Computer Science, vol.2656, no.1, 416-432 (2003).

[2] A. Lysyanskaya, S. Micali, L. Reyzin, H. Shacham: *Sequential aggregate signatures from trapdoor permutations*, in: Advances in Cryptography-Euro crypt 2004, 74 -90 (2004).

[3] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, B. Waters: *Sequential Aggregate Signatures and Multisignatures Without Random Oracles*, in: Advances in Cryptology-EUROCRYPT 2006, 465-485(2006).

[4] J. H. Cheon, Y. Kim, H. J. Yoon: *A New ID-based Signature with Batch Verification*, in: Trends in Mathematics, vol.8, no.1, 119-131(2005).

[5] J. Herranz: *Deterministic Identity-Based Signatures for Partial Aggregation*, in: The Computer Journal, vol.49, no.3, 322-330(2006).

[6] C. Gentry, Z. Ramzan: *Identity -based aggregate signatures*, in: Proceedings of PKC 2006, 257-273(2006).

[7] J. Camenisch, S. Hohenberger, M. Ø. Pedersen: *Batch Verification of Short Signatures*, in: Journal of Cryptology, vol.25, no.4, 723-747(2012).

[8] Z. P. Jia, H. Li, C. Song, and X. H. Zhang: *Efficient certificateless tripartite key agreement protocol*, in: Computer Engineering and Applications, vol.50, no.10, 105-107(2014). (In Chinses)

[9] J. Xu, Z. Zhang, D. Feng: *ID-Based Aggregate Signatures from Bilinear Pairings*, in: Proceedings of Cryptology and Network Security: 4th International Conference 2005, vol.3810, 110-119(2005).

[10] Y. L. Wen, J. F. Ma, C. Wang: *New ID-based Aggregate Signature Scheme*, in: Computer Science, vol.38, no.6, 54-57(2011). (In Chinses)

[11] X. Y. Yu, D. K. He: *New Certificateless Aggregate Signature Scheme*, in: Application Research of Computers, vol.31, no.8, 2485-2487(2014). (In Chinses)