Novel Efficient Certificateless Aggregate Signatures

Lei Zhang[1], Bo Qin[1,3], Qianhong Wu[1,2], and Futai Zhang[4]

[1] UNESCO Chair in Data Privacy
Department of Computer Engineering and Mathematics
Universitat Rovira i Virgili
Av. Països Catalans 26, E-43007 Tarragona, Catalonia
{lei.zhang,bo.qin,qianhong.wu}@urv.cat
[2] Key Lab. of Aerospace Information Security and Trusted Computing
Ministry of Education, School of Computer, Wuhan University, China
[3] Dept. of Maths, School of Science, Xi'an University of Technology, China
[4] College of Mathematics and Computer Science
Nanjing Normal University, Nanjing, China
zhangfutai@njnu.edu.cn

Abstract. We propose a new efficient certificateless aggregate signature scheme which has the advantages of both aggregate signatures and certificateless cryptography. The scheme is proven existentially unforgeable against adaptive chosen-message attacks under the standard computational Diffie-Hellman assumption. Our scheme is also efficient in both communication and computation. The proposal is practical for message authentication in many-to-one communications.

1 Introduction

The notion of newly introduced aggregate signatures [2] allows an efficient algorithm to aggregate n signatures of n distinct messages from n different signers into one single signature. The resulting aggregate signature can convince a verifier that the n signers did indeed sign the n original messages. These properties greatly reduce the resulting signature size and make aggregate signatures very applicable to message authentication in many-to-one communications.

The inception of certificateless cryptography [1] efficiently addresses the key escrow problem in ID-based Cryptography. In certificateless cryptosystems, a trusted Key Generation Center (KGC) helps each user to generate his private key. Unlike ID-based cryptosysems, the KGC in certificateless cryptosystems merely determines a partial private key rather than a full private key for each user. Then the user computes the resulting private key with the obtained partial private key and a self-chosen secret value. As for the public key of each user, it is computed from the KGC's public parameters and the secret value chosen by the user. With this mechanism, certificateless cryptosystems avoid the key escrow problem in ID-based cryptosystems.

The advantages of certificateless cryptosystems motivate a number of further studies. The first certificateless signature scheme was presented by Al-Riyami

M. Bras-Amorós and T. Høholdt (Eds.): AAECC 2009, LNCS 5527, pp. 235–238, 2009.

and Paterson [1]. A security definition of certificateless signature was formalized in [7] and the Al-Riyami-Paterson scheme was analyzed in this model. The security model of CLS schemes was further enhanced in [6,8,9]. Two Certificateless Aggregate Signature (CLAS) schemes were recently presented [5] with security proofs in a weak model similar to that in [7]. Subsequently, a new CLAS scheme was proposed in [10] and proven secure in a stronger security model. As for efficiency, the existing schemes require a relatively large number of paring computations in the process of verification and suffer from long resulting signatures.

Our Contribution. In this paper, we propose a novel CLAS scheme which is more efficient than existing schemes. By exploiting the random oracle model, our CLAS scheme is proven existentially unforgeable against adaptive chosen-message attacks under the standard CDH assumption. It allows multiple signers to sign multiple documents in an efficient way and the total verification information (the length of the signature), consists only 2 group elements. Our scheme is also very efficient in computation and the verification procedure need only a very small constant number of pairing computations, independent of the number of aggregated signatures.

2 Our Certificateless Aggregate Signature Scheme

In this section, we propose a new certificateless aggregate signature scheme. Our scheme is realized in groups which allowing efficient bilinear maps [3].

2.1 The Scheme

The specification of the scheme is as follows.

- Setup: Given a security parameter ℓ, the KGC chooses a cyclic additive group G_1 which is generated by P with prime order q, chooses a cyclic multiplicative group G_2 of the same order and a bilinear map $e : G_1 \times G_1 \longrightarrow G_2$. The KGC also chooses a random $\lambda \in Z_q^*$ as the master-key and sets $P_T = \lambda P$, chooses cryptographic hash functions $H_1 \sim H_4 : \{0,1\}^* \longrightarrow G_1$, $H_5 : \{0,1\}^* \longrightarrow Z_q^*$. The system parameter list is params $= (G_1, G_2, e, P, P_T, H_1 \sim H_5)$.
- Partial-Private-Key-Extract: This algorithm is performed by KGC that accepts params, master-key λ and a user's identity $ID_i \in \{0,1\}^*$, and generates the partial private key for the user as follows.
  1. Compute $Q_{i,0} = H_1(ID_i, 0)$, $Q_{i,1} = H_1(ID_i, 1)$.
  2. Output the partial private key $(D_{i,0}, D_{i,1}) = (\lambda Q_{i,0}, \lambda Q_{i,1})$.
- UserKeyGen: This algorithm takes as input params, a user's identity ID_i, selects a random $x_i \in Z_q^*$ and sets his secret/public key as $x_i / P_i = x_i P$.
- Sign: To sign a message M_i using the signing key $(x_i, D_{i,0}, D_{i,1})$, the signer, whose identity is ID_i and the corresponding public key is P_i, first chooses a one-time-use string Δ then performs the following steps.

1. Choose a random $r_i \in Z_q^*$, compute $R_i = r_i P$.
2. Compute $T = H_2(\Delta), V = H_3(\Delta), W = H_4(\Delta)$.
3. Compute $h_i = H_5(M_i||\Delta||ID_i||P_i)$.
4. Compute $S_i = D_{i,0} + x_i V + h_i(D_{i,1} + x_i W) + r_i T$.
5. Output $\sigma_i = (R_i, S_i)$ as the signature on M_i.

– Aggregation: Anyone can act as an aggregate signature generater who can aggregate a collection of individual signatures that use the same string Δ. For an aggregating set (which has the same string Δ) of n users with identities $\{ID_1, \cdots, ID_n\}$ and the corresponding public keys $\{P_1, \cdots, P_n\}$, and message-signature pairs $(M_1, \sigma_1 = (R_1, S_1)), \cdots, (M_n, \sigma_n = (R_n, S_n))$ from $\{U_1, \cdots, U_n\}$ respectively, the aggregate signature generater computes $R = \sum_{i=1}^{n} R_i, S = \sum_{i=1}^{n} S_i$ and outputs the aggregate signature $\sigma = (R, S)$.

– Aggregate Verify: To verify an aggregate signature $\sigma = (R, S)$ signed by n users with identities $\{ID_1, ..., ID_n\}$ and corresponding public keys $\{P_1, ..., P_n\}$ on messages $\{M_1, ..., M_n\}$ under the same string Δ, the verifier performs the following steps.
   1. Compute $T = H_2(\Delta), V = H_3(\Delta), W = H_4(\Delta)$, and for all $i, 1 \leq i \leq n$ compute $h_i = H_5(M_i||\Delta||ID_i||P_i), Q_{i,0} = H_1(ID_i, 0), Q_{i,1} = H_1(ID_i, 1)$.
   2. Verify $e(S, P) \stackrel{?}{=} e(P_T, \sum_{i=1}^{n} Q_{i,0} + \sum_{i=1}^{n} h_i Q_{i,1}) e(T, R) e(W, \sum_{i=1}^{n} h_i P_i)$ $e(V, \sum_{i=1}^{n} P_i)$. If the equation holds, output *true*. Otherwise, output *false*.

In our scheme, each user in an aggregating set must use the same one-time-use string Δ when signing. As mentioned in [4], it is straightforward to choose such a Δ in certain settings. For example, if the signers have access to some loosely synchronized clocks, Δ can be chosen based on the current time. Furthermore, if Δ is sufficiently long, then it will be statistically unique. By exploiting a approach similar to that presented in [4], the one-time-use restriction on common reference string Δ in the above scheme can also be removed to achieve better applicability.

2.2 Security Analysis

Two types of adversaries, who can access to services in addition to those provided to the attacker against regular signatures, are considered in CL-PKC – Type I adversary and Type II adversary. A Type I adversary is not allowed to access to the master-key, but he can replace the public key of any user with a value of his choice. A Type II adversary can access to the master-key but he cannot replace the public key of any user. In a secure CLAS scheme, it is infeasible for Type I adversary and Type II adversary to forge a valid signature.

Under the standard computational Diffie-Hellman assumption, the proposed CLAS scheme is provably secure against both types of adversaries in the random model. The formal security proof is in the full version of this paper.

3 Conclusion

We presented an efficient certificateless aggregate signature scheme. To verify an aggregate signature signed by n users on n messages under the same string, a verifier only needs to compute four pairing operations. The proposal is provably secure in the random oracle model assuming that the computational Diffie-Hellman problem is hard. Our CLAS scheme can be applied to authentication in bandwidth limited scenarios such as many-to-one communications.

Acknowledgments and Disclaimer

This paper is partly supported by the Spanish Government through projects CONSOLIDER INGENIO 2010 CSD2007-00004 ARES, TSI2007-65406-C03-01 E-AEGIS and by the national nature science foundation of China (No. 60673070). The views of the author with the UNESCO Chair in Data Privacy do not necessarily reflect the position of UNESCO nor commit that organization.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless Public Key Cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
2. Boneh, D., Gentry, C., Shacham, H., Lynn, B.: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 416–432. Springer, Heidelberg (2003)
3. Boneh, D., Franklin, M.: Identity-based Encryption from the Weil Pairing. SIAM J. Comput. 32, 586–615 (2003); a Preliminary Version Appeared. In: Kilian, J. (ed.): CRYPTO 2001. LNCS, vol. 2139, pp. 213-229. Springer, Heidelberg (2001)
4. Gentry, C., Ramzan, Z.: Identity-Based Aggregate Signatures. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.) PKC 2006. LNCS, vol. 3958, pp. 257–273. Springer, Heidelberg (2006)
5. Gong, Z., Long, Y., Hong, X., Chen, K.: Two Certificateless Aggregate Signatures from Bilinear Maps. In: Proc. of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 188–193 (2007)
6. Hu, B.C., Wong, D.S., Zhang, Z., Deng, X.: Key Replacement Attack Against a Generic Construction of Certificateless Signature. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058, pp. 235–246. Springer, Heidelberg (2006)
7. Huang, X., Susilo, W., Mu, Y., Zhang, F.: On the Security of Certificateless Signature Schemes from Asiacrypt 2003. In: Desmedt, Y.G., Wang, H., Mu, Y., Li, Y. (eds.) CANS 2005. LNCS, vol. 3810, pp. 13–25. Springer, Heidelberg (2005)
8. Huang, X., Mu, Y., Susilo, W., Wong, D.S., Wu, W.: Certificateless Signature Revisited. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 308–322. Springer, Heidelberg (2007)
9. Zhang, Z., Wong, D.: Certificateless Public-Key Signature: Security Model and Efficient Construction. In: Zhou, J., Yung, M., Bao, F. (eds.) ACNS 2006. LNCS, vol. 3989, pp. 293–308. Springer, Heidelberg (2006)
10. Zhang, L., Zhang, F.: A New Certificateless Aggregate Signature Scheme. Computer Communications (2009), doi:10.1016/j.comcom.2008.12.042