An Efficient Certificateless Signature from Pairings

Changji Wang[1,2], Dongyang Long[1,2], and Yong Tang[1]
(Corresponding author: Changji Wang)

Department of Computer Science, Sun Yat-sen University, Guangzhou, P.R.China[1]
Xingang West Road 135, Guangzhou 510275, China (Email: {isswchj}@mail.sysu.edu.cn)
Guangdong Province Information Security Key Laboratory, Guangzhou, P.R.China[2]
The State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences[3]
Beijing, P. R. China

(Received June 22, 2006; revised and accepted Sept. 19, 2006)

Abstract

A certificateless signature retains the efficiency of Shamir's identity-based signature while it does not suffer from the inherent private key escrow problem, which is first introduced by S. Al-Riyami and K. Paterson in Asiacrypt 2003. In this paper, we proposed a new certificateless signature scheme based on bilinear pairings. The proposed scheme is more efficient than those of previous schemes by pre-computing the pairing $e(P, P) = g$ and publishing as the system parameters, it needs not to compute the pairing in the `Sign` stage, and only needs to compute three pairings in the `Verify` stage. In addition, the proposed scheme does not need the special MaptoPoint hash function and the confidential channel between KGC and users. The proposed scheme is unforgeable under the hardness assumption of the q-strong Diffie-Hellman problem and Computational Diffie-Hellman problem.

Keywords: Bilinear Pairings, Certificateless Signature, q-Strong Diffie–Hellman Problem

1 Introduction

A digital signature is one of the most important security primitives in modern cryptography. In a traditional public key signature scheme, methods to guarantee the authenticity of a public key are required, since the public key of the signer is actually a type of random string. To provide the binding between a signer and his public key, the traditional public key signature uses a certificate that is a digitally signed statement issued by the CA (Certification Authority). The need for public key infrastructure (PKI) supporting certificates is considered the main difficulty in the deployment and management of public key signature schemes.

First proposed by Shamir [10], identity-based public key cryptography tackles the problems of authenticity of keys in a different way to traditional PKI. The identity-based signature scheme can dispense with certificates, the key escrow of a user's private key is inherent in the identity-based signature scheme [3, 5, 7]. A trusted third party called the PKG (Private Key Generator) manages the generation and distribution of the users' private keys.

In Asiacrypt 2003, Al-Riyami and Paterson introduced and made concrete the concept of certificateless public key cryptography [9]. A certificateless signature scheme does not require the use of certificates and yet does not have the inherent key escrow problem of the identity-based signature scheme [8, 12]. Unlike the PKG in an identity-based signature scheme, the KGC (Key Generating Center) in a certificateless signature scheme does not have access to the user's private key. The KGC derives a partial private key from the user's identity and the master key. The user then combines the partial private key with some secret information to generate the actual private signing key. The system is not identity-based, because the public key is no longer computable from a user identity. However, no authentication of the public key is necessary and no certificate is required.

In this paper, we proposes a new certificateless signature scheme based on bilinear pairings. The proposed scheme is more efficient than those of previous schemes by pre-computing the pairing $e(P, P) = g$ and publishing as the system parameters, thus it need not to compute the pairing in the `Sign` stage, and only need to compute three pairings in the `Verify` stage. In addition, the proposed scheme does not need the special MaptoPoint hash function. Finally, we proved the proposed scheme is unforgeable under the hardness assumption of the q-strong Diffie–Hellman problem and Computational Diffie-Hellman problem.

The rest of the paper is organized as follows. In Section 2, we describe background concepts on bilinear pairings and related mathematical problems. In Section 3, we

present a new certificateless signature scheme. The security and efficiency analysis are given in Section 4. Finally, we conclude the paper with Section 5.

2 Preliminaries

2.1 Bilinear Pairings

Bilinear pairing is an important cryptographic primitive. Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of the same prime order q. The bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$, which satisfies the following properties:

- `Bilinear:` $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in Z_q^*$.
- `Non-degenerate:` If P is a generator of G_1, then $e(P, P)$ is a generator of G_2. In other words, $e(P, P) \neq 1_{G_2}$.
- `Computable:` There exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

Typically, the map e will be derived from either Weil or Tate pairing on a elliptic curve over a finite field.

2.2 Diffie-Hellman Problems

We also introduce here the computational problems that will form the basis of security for the proposed certificateless signature scheme.

`Discrete Logarithm Problem (DLP):` Given two group elements P and Q in G_1, find an integer n, such that $Q = nP$ whenever such an integer exists.

`Computational Diffie-Hellman Problem (CDHP):` For any $a, b \in Z_q^*$, given (P, aP, bP), compute abP.

`Decisional Diffie-Hellman Problem (DDHP):` For any $a, b, c \in Z_q^*$, given (P, aP, bP, cP), decide whether $c = ab \mod q$.

`Gap Diffie-Hellman (GDH) Group:` We define G_1 as a GDH group if G_1 is a group such that DDHP can be solved in polynomial time, but no algorithm can solve CDHP with non-negligible advantage within polynomial-time.

`The` q`-Strong Diffie-Hellman problem (`q`-SDHP):` Given a $(q+2)$-tuple $(P, Q, \alpha Q, \alpha^2 Q, \cdots, \alpha^q Q)$, find a pair $(c, (c+\alpha)^{-1} P)$ with $c \in Z_q^*$.

3 An Efficient Certificateless Signature Scheme

At the AsiaCrypt 2003 conference, Al-Riyami and Paterson introduced and made concrete the concept of certificateless public key cryptography, a model for the use of public key cryptography which avoids the inherent escrow of identity-based cryptography and yet does not require certificates to guarantee the authenticity of public keys. Since then, several certificateless signature shcemes were presented [8, 12]. In this section, we propose a new certificateless signature scheme from bilinear pairings.

A certificateless signature scheme is a 7-tuple of polynomial time algorithms (Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Sign, Verify), where `Setup` and `Partial-Private-Key-Extract` are performed by a KGC. Since `Set-Secret-Value`, `Set-Private-Key`, and `Set-Public-Key` are executed by a user, the key escrow of the user's private key is not inherent in a certificateless signature scheme. The detailed descriptions of the proposed certificateless signature scheme are depicted as follows.

Setup:
This algorithm takes as input a security parameter k and returns the system parameters and master key. More specially, this algorithm runs as follows. Let G_1 be a cyclic additive group generated by P, whose order is a prime q, G_2 be a cyclic multiplicative group of the same order q, and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing.

1) Choose $s \in_R Z_q^*$ and set $P_{pub} = sP$ and compute $g = e(P, P)$.

2) Choose cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow Z_q^*$ and $H_2 : \{0,1\}^* \times G_2 \rightarrow Z_q^*$.

3) Set the system parameters as $\{G_1, G_2, q, P, P_{pub}, g, H_1, H_2\}$ and keep the master key s secret.

The system parameters are distributed to the users of the system through a secure authenticated channel.

Partial-Private-Key-Extract:
This algorithm takes as input the system parameters, the master key, and an identifiable information and returns its corresponding partial private key. More formally, to construct the partial private key for Alice with identifiable information ID_A, we adopt the blind technique as in [11] to remove the requirement of confidential and authentic channel between Alice and KGC in this stage.

1) Alice chooses a value $k \in_R Z_q^*$ to compute kP, then Alice sends his identity ID_A and kP to the KGC.

2) KGC checks that Alice has a claim to a particular online identifier ID_A. If they do, the KGC computes $D'_{ID_A} = (H_1(ID_A) + s)^{-1} P + s(kP)$, then sends it to Alice through an open channel.

3) Alice computes $D_{ID_A} = D'_{ID_A} - k(sP) = (H_1(ID_A) + s)^{-1} P$.

Alice		KGC
	$k \in_R Z_q^*$	
$ID_A \parallel kP$		
	$\xrightarrow{ID_A \parallel kP}$	
		$D'_{ID_A} = (H_1(ID_A)+s)^{-1}P + s(kP)$
	$\xleftarrow{D'_{ID_A}}$	

$$D_{ID_A} = D'_{ID_A} - kP_{pub} = (H_1(ID_A)+s)^{-1}P$$

Anyone else cannot get Alice's private key unless he can get ksP from kP and sP, which is a hard CDH problem. Alice can get his private key by $D'_{ID_A} - kP_{pub}$ because k is chosen by himself. Notice that Alice can verify the correctness of the `Partial-Private-Key-Extract` algorithm output by checking that $e(D_{ID_A}, H_1(ID_A)P + P_{pub}) = g$.

Set-Secret-Value:
This algorithm takes as input the system parameters and an identifiable information and returns its corresponding secret value. More specially, to set the secret value for Alice, choose $x_A \in_R Z_q^*$, and output x_A as her secret value.

Set-Private-Key:
This algorithm takes as input the system parameters, a partial private key, and a secret value and returns corresponding private key. More specially, to construct the private key for Alice, compute $SK_{ID_A} = x_A D_{ID_A} = x_A(H_1(ID_A)+s)^{-1}P$ as her private key.

Set-Public-Key:
This algorithm takes as input the system parameters and a secret value and outputs corresponding public key. More specially, to construct the public key for Alice, compute $X_A = x_A^{-1}P$, $Y_A = x_A^{-1}P_{pub}$, and set $PK_{ID_A} =< X_A, Y_A >$ as her public key.

Sign:
Given a message m and a private key SK_{ID_A}, perform the following steps.

1) Choose $a \in_R Z_q^*$.
2) Compute $r = g^a \in G_2$.
3) Set $v = H_2(m \parallel r) \in Z_q^*$.
4) Compute $U = (a+v)SK_{ID_A} \in G_1$.
5) Set $\sigma = (U, v) \in G_1 \times Z_q^*$ as the signature of the message m.

Verify:
To verify a signature $\sigma = (U, v)$ of a message m for Alice with public key $PK_{ID_A} =< X_A, Y_A >$, this algorithm runs as follows.

1) Check whether or not the equality $e(X_A, P_{pub}) = e(Y_A, P)$ holds. If not, stop and reject the signature. Otherwise, continue.
2) Compute $r = e(U, H_1(ID_A)X_A + Y_A)g^{-v}$
3) Check if $v = H_2(m \parallel r)$ holds. If it does, accept the signature. Otherwise, stop and reject the signature.

This completes the description of our proposed certificateless signature scheme. In the following section, we analyze the scheme from performance and security points of view.

4 Analysis of the Proposed Certificateless Signature Scheme

4.1 Correctness Analysis

Consistency of the proposed scheme is satisfied. In effect, if $\sigma = (U, v)$ is a valid signature of a message m for Alice with public key $PK_{ID_A} =< X_A, Y_A >$, then

$$e(X_A, P_{pub}) = e(X_A, sP) = e(sX_A, P) = e(Y_A, P) \quad (1)$$

$$\begin{aligned} r &= e(U, H_1(ID_A)X_A + Y_A)g^{-v} \\ &= e((a+v)SK_{ID_A}, H_1(ID_A)x_A^{-1}P + x_A^{-1}sP)g^{-v} \\ &= e((a+v)(H_1(ID_A)+s)^{-1}x_AP, (H_1(ID_A)+s)x_A^{-1}P)g^{-v} \\ &= e(P,P)^{a+v}g^{-v} \\ &= g^a \end{aligned} \quad (2)$$

4.2 Performance Analysis

According to the state-of-the-art results in [1] and [2], one bilinear pairing operation requires at least 10 times more multiplications in the underlying finite field than an elliptic curve point scalar multiplication does in the same finite field. In addition, most of the ID-based and Certificateless cryptosystems require a special hash function called map-to-point hash function ([3, 4, 9, 12]) for converting a user's identity to a point on the underlying elliptic curve. This operation is also time consuming and cannot be treated as a conventional hash operation which is commonly ignored in performance evaluation. A map-to-point hash function, on the other hand, is usually implemented as a probabilistic algorithm and is more expensive than a point scalar multiplication in terms of computation time.

In the proposed scheme, the pairing $e(P, P) = g$ can be pre-computed and published as the system parameters. Thus, it not need to compute pairing in the `Sign` stage, and it only needs to compute three pairings in the `Verify`

Table 1: Performance comparison of CLS schemes

		Pairing Operation	Scalar Multi in G_1	Add in G_1	Exponentiation in G_2	MaptoPoint Operation
[9]	Sign	1	2	1	1	need
	Verify	4	0	0	1	
[8]	Sign	0	2	0	0	need
	Verify	4	1	1	0	
Our scheme	Sign	0	1	0	1	don't need
	Verify	3	1	1	0	

stage. In addition, the proposed scheme does not need the special MaptoPoint hash function. In Table 1, we summarize the number of different operations of some well-known certificateless signature schemes and our scheme proposed above. We ignore the time taken by conventional hash operations and point addition operations as they are much more efficient when compared with pairings, scalar multiplications, and map-to-point hash operations. From Table 1, we can conclude that our scheme is a little more efficient than Al-Riyami and Paterson's certificateless signature scheme [9] and X. Li, K. Chen and L. Sun's certificateless signature scheme [8].

4.3 Security Analysis

The proposed scheme is unforgeable under the hardness assumption of the q-strong Diffie–Hellman problem and Computational Diffie–Hellman problem.

On the one hand, even the KGC who knows the master key s, the partial private key of Alice, and the public key $< X_A, Y_A >$ of Alice, cannot compute a valid signature. If he can compute x_A from the equalities $X_A = x_A P$ or $Y_A = x_A sP$, then he can forge BLS signatures [5] which are proven to be unforgeable based on the CDH assumption.

On the other hand, any third party may try to compute a valid signature via two ways.

- In the first place, he randomly chooses the value U and tries to compute v such that $v = H_2(m \parallel e(U, H_1(ID_A)x_A + Y_A)g^{-v})$ holds.
- Secondly, the adversary can choose v at random and try to compute U such that the equation $v = H_2(m \parallel e(U, H_1(ID_A)x_A + Y_A)g^{-v})$ holds.

However, due to the hardness of the q-strong Diffie–Hellman problem, computational Diffie–Hellman problem and the one-way property of cryptographic hash function, the adversary can not forge a valid signature by this two ways.

Theorem 1. *Let us assume that there exists an adaptively chosen message and identity attacker $\digamma$ making q_{h_i} queries to random oracles $H_i (i = 1, 2)$ and q_s queries to the signing oracle. Assume that, within a time t, $\digamma$ produces a forgery with probability $\epsilon \geq 10(q_s+1)(q_s+q_{h_2})/2^k$. Then, there exists an algorithm $\mathfrak{B}$ that is able to solve the q-SDHP for $q = q_{h_1}$ in an expected time*

$$t \leq 120686 q_{h_1} q_{h_2} (t+O(q_s, \tau_p))/(\epsilon(1-q/2^k))+O(q^2\tau_{mult}). \quad (3)$$

where τ_{mult} and τ_p respectively denote the cost of a scalar multiplication in G_2 and the required time for a pairing evaluation.

The formal security analysis is the same as Barreto et al.'s provably-secure identity-based signatures [3], we refer to [3] for more details.

5 Conclusions

In order to avoid the inherent escrow of identity-based cryptography and yet not requiring certificates to guarantee the authenticity of public keys, Certificateless public key cryptography was first introduced by Al-Riyami and Paterson in Asiacrypt 2003, and has received a significant attention in recent years. In this paper, we proposed a new certificateless signature scheme based on bilinear pairings, the proposed scheme is more efficient than those of previous schemes by pre-computing the pairing $e(P, P) = g$ and publishing as the system parameters. The scheme is proved to be secure under under the hardness assumption of the bilinear pairing inversion problem and Computational Diffie-Hellman problem.

Acknowledgements

This work is supported by National Natural Science Foundation of China under Grant (No.60503005, No.60673135 and No.60573039) and the Natural Science Foundation of Guangdong Province under Grant (No.05200302 and No.5003350).

References

[1] P. Barreto, H. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proceedings of Crypto'2002*, LNCS 2442, pp. 354-368, Springer-Verlag, 2002.

[2] P. Barreto, B. Lynn, and M. Scott, "On the selection of pairing-friendly groups," in *Selected Areas in Cryptography (SAC 2003)*, LNCS 3006, pp. 17-25, Springer-Verlag, 2003.

[3] P. S. L. M. Barreto et al., "Efficient and provably-secure identity-based signatures and signcryption from ilinear maps," in *Proceedings of Asiacrypt'2005*, LNCS 3788, pp. 515-532, Springer-Verlag, 2005.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proceedings of Crypto'01*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairings," in *Proceedings of Asiacrypt'01*, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[6] Y. J. Choie, E. Jeong, and E. Lee, "Efficient identity-based authenticated key agreement protocol from pairings," in *Applied Mathematics and Computation*, vol. 162, no. 1, pp. 179-188, 2006.

[7] F. Hess, "Efficient identity based signature scheme based on pairings," *Selected Areas in Cryptography-SAC 2002*, LNCS 2595, pp. 310-324, Springer-Verlag, 2003.

[8] X. Li, K. Chen, and L. Sun, "Certificateless signature and proxy signature schemes from bilinear pairings," *Lithuanian Mathematical Journal*, vol. 45, no. 1, pp. 95-103, 2005.

[9] S. A. Riyami, and K. Paterson, "Certificateless public key cryptography," in *Proceedings of Asiacrypt'03*, LNCS 2894, pp. 452-473, 2003.

[10] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Crypto'84*, LNCS 196, pp. 47-53, Springer-Verlag, 1985.

[11] G. Xie, *An ID-Based Key Agreement Scheme from Pairing*, Cryptology ePrint Archive: Report 2005/093, 2005. (http://eprint.iacr.org/2005/093)

[12] D. Yum and P. Lee, "Generic construction of certificateless signature," in *Proceedings of ACISP'04*, LNCS 3108, pp. 200-211, 2004.

Changji Wang, received the BS degree from Jishou University in 1994, MS degree from Sun Yat-sen University in 1997, PHD degree from USTC (University of Science and Technology of China) in 2002. And he finished his postdoctor research at Network Research Center in Tsinghua University in 2004. At present, he is a associate professor in Department of Computer Science, Sun Yat-sen Univesity. His research interests are information and network security.

Dongyang Long, received the BS degree from Huan Normal University in 1982, MS degree from Lanzhou University in 1986 and PHD degree from City University of Hong Kong in 2002. At present, he is a professor in Department of Computer Science, Sun Yat-sen Univesity. He is a member of IEEE and a member of American Mathematical Society, Reviewer of Mathematical Reviews. His research interests are information theory and coding theory.

Yong Tang, received the BS, MS degrees in from Wuhan University, and PHD from USTC (University of Science and Technology of China) in 1985, 1990 and 2001, respectively. At present he is a professor in Department of Computer Science, Sun Yat-sen Univesity. His research interests are database, knowledge base and cooperative software.