An Effective Certificateless Signature Scheme Based on Bilinear Pairings*

M. Choudary Gorantla, Raju Gangishetti, Manik Lal Das and Ashutosh Saxena

Institute for Development and Research in Banking Technology
Castle Hills, Masab Tank, Hyderabad 500057, INDIA.

Abstract. In this paper we propose a certificateless signature scheme based on bilinear pairings. The scheme effectively removes secure channel for key issuance between trusted authority and users and avoids key escrow problem, which is an inherent drawback in ID-based cryptosystems. The scheme uses a simple blinding technique to eliminate the need of secure channel and user chosen secret value to avoid the key escrow problem. The signature scheme is secure against adaptive chosen message attack in the random oracle model.

1 Introduction

In traditional public key cryptosystems (PKC), the public key of a signer is essentially a random bit string picked from a given set. This leads to a problem of how the public key is associated with the signer (for signature schemes). In these cryptosystems the binding between public key and identity of the signer is obtained via a digital certificate. The trusted third party verifies the credentials of the entity before issuing a digital certificate. The traditional PKC also requires huge efforts in terms of computing time and storage to manage the certificates.

To simplify this tedious certificate management process, Shamir [20] introduced the concept of ID-based cryptosystem wherein, a user's public key is his identity or derived from his identity. The user's private key is generated by a trusted third party called Private Key Generator (PKG). Unlike traditional PKCs, ID-based cryptosystems require no public key directories. The encryption and verification processes require only user's identity along with some system parameters which are one-time computed and available publicly. These features make ID-based cryptosystems advantageous over the traditional PKCs, as key distribution and revocation are not required. Moreover, the signer's public key need not be published or sent along with the message. A verifier can verify a signature just by using the signer's identity. But an inherent problem of ID-based cryptosystems is key escrow, i.e., the PKG knows the user's private key. Therefore, the PKG can decrypt any ciphertext or forge signature for any message and thus there is no user privacy and authenticity in the system. After Shamir's proposal, several ID-based cryptosystems [6, 13, 14, 17, 19] have been proposed. However, most of the

* This work is supported in part by the Ministry of Communications and Information Technology, Govt. of India, under the grant no. 12(35)/05-IRSD.

Choudary Gorantla M., Gangishetti R., Lal Das M. and Saxena A. (2005).
An Effective Certificateless Signature Scheme Based on Bilinear Pairings.
In *Proceedings of the 3rd International Workshop on Security in Information Systems*, pages 31-39
DOI: 10.5220/0002572500310039

schemes require a secure channel between users and the PKG to deliver private keys. Due to these inherent problems, ID-based cryptosystems are considered to be suitable for private networks [20]. Thus, eliminating these problems in ID-based cryptosystems is essential to make them more applicable in the real world.

Recently, Al Riyami and Paterson [1] introduced the concept of certificateless cryptosystem, which is intermediate between traditional PKC and ID-based cryptosystem. Like the ID-based cryptosystem, certificateless cryptosystem does not require the use of certificates to guarantee the authenticity of public keys. In this paper, we propose a certificateless signature scheme based on bilinear pairings. We use a simple blinding technique and user chosen secret value to eliminate secure channel and the key escrow problem respectively. The trusted authority (TA) issues a partial private key to the user in a blinded manner through which the user creates his own private key. Thus, the TA neither knows the user's private key nor uses secure channel for key issuance. The signature scheme is secure against adaptive chosen message attack in the random oracle model assuming that the CDHP is computationally hard.

1.1 Previous Work

In 1984, Shamir[20] proposed an ID-based signature scheme based on the difficulty of factoring integers. Hess [14] proposed an efficient ID-based signature scheme based on pairings and Cha et.al [6] proposed an ID-based signature from Gap Diffie-Hellman groups. But, all these schemes [6, 14, 20] suffer from key escrow problem and require a secure channel for key issuance.

Boneh and Franklin [5] proposed a solution for the key escrow problem in ID-based cryptosystem, where a user's private key is computed in a threshold manner by multiple authorities. But, multiple identity verifications of a user by multiple authorities are quite a burden. Generating a new private key by adding multiple private keys is another approach [7], but in this scheme the key generation centers have no countermeasure against the user's illegal usage of his private key. Gentry [11] proposed a scheme that eliminates the key escrow and secure channel requirement using some user chosen secret information, but it is certificate-based. Later, Al-Riyami and Paterson [1] introduced the concept of certificateless PKC to eliminate the key escrow problem. Their original scheme requires a secure channel between the users and the trusted authority to transmit partial private keys. Recently, a secure key issuing protocol in ID-based cryptosystem was proposed by Lee et al [15], wherein private key is issued by a key generation center and its privacy is protected by multiple key privacy authorities. However, its computational complexity is high and efficiency is poor in terms of communication requirements.

1.2 Organization

The rest of the paper is organized as follows: Section 2 gives the background concepts on bilinear pairings and some related mathematical problems. Section 3 presents the model of our scheme. Section 4 presents the signature scheme and its security analysis. We conclude the paper in Section 5.

2 Background Concepts

In this section, we briefly review the basic concepts on bilinear pairings and some related mathematical problems.

2.1 Bilinear Pairings

Let G_1 be an additive cyclic group of prime order q, G_2 be a multiplicative cyclic group of the same order and P be a generator of G_1. A bilinear map is defined as $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

Bilinear: $e(aR, bS) = e(R, S)^{ab}$ $\forall R, S \in G_1$ and $a, b \in Z_q^*$. This can be restated as $\forall$ $R, S, T \in G_1$, $e(R + S, T) = e(R, T)e(S, T)$ and $e(R, S + T) = e(R, S)e(R, T)$.
Non-degenerate: There exists $R, S \in G_1$ such that $e(R, S) \neq I_{G_2}$ where I_{G_2} denotes the identity element of the group G_2.
Computable: There exists an efficient algorithm to compute $e(R, S)$ $\forall R, S \in G_1$.

In general implementation, G_1 will be a group of points on an elliptic curve and G_2 will denote a multiplicative subgroup of a finite field. Typically, the mapping e will be derived from either the Weil or the Tate pairing on an elliptic curve over a finite field. We refer to [5] for more comprehensive description on how these groups, pairings and other parameters are defined.

2.2 Mathematical Problems

Here we discuss some mathematical problems, which form the basis of security for our scheme.

Discrete Logarithm Problem (DLP): Given q, P and $Q \in G_1^*$, find an integer $x \in Z_q^*$ such that $Q = xP$.

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 $c \equiv ab \bmod q$.

Bilinear Diffie-Hellman Problem (BDHP): For any $a, b, c \in Z_q^*$, given $< P, aP, bP, cP >$, compute $e(P, P)^{abc}$.

Gap Diffie-Hellman Problem(GDHP): A class of problems where CDHP is hard while DDHP is easy.

Weak Diffie-Hellman Problem(WDHP): For $S \in G_1$ and for some $a \in Z_q^*$, given $< P, S, aP >$ compute aS.

3 The Model for the Proposed Scheme

We assume that the public keys of the users are placed in a public directory maintained by a trusted authority (TA) that issues partial private keys to the users. We put no further

security on the public key directory and allow an active adversary to replace any public key with a public key of his own choice. We say that even though an adversary replaces a public key, the innocent user can not be framed of repudiating his signature. Hence the users have the same level of trust in the TA as they would in a CA in the traditional PKC. The trust assumptions made in our scheme are greatly reduced compared to ID-based schemes where the PKG knows the private keys of every user.

There are two types of adversaries who can replace the public keys kept in the directory. The adversaries who do not have access to the master key and the adversaries with the master key. We discuss the adversarial actions in the security analysis part.

The proposed signature scheme consists of four algorithms, namely **Setup**, **Key Generation**, **Sign** and **Verify**.

Setup: The TA selects a `master-key` and keeps it secret. It then specifies the system parameters `params`, which include description of the bilinear map, hash functions, the TA's public key, message space $\mathcal{M}$ and signature space $\mathcal{S}$. The TA publishes the `params`.

Key Generation: This algorithm generates the public key and private key of the user as follows:

- The user *A* chooses two secret values, calculates the user parameters `user-params` and sends them to the TA over a public channel along with his identity.
- The TA verifies *A*'s identity and checks the validity of `user-params.`
- On successful verification, the TA calculates user's public key P_A and partial private key D_A.
- The TA publishes P_A and sends D_A to the user *A* over a public channel.
- The user checks the validity of D_A and extracts his private key S_A from it.

Sign: The user *A* signs on a message M using his private key S_A and produces a signature $Sig \in \mathcal{S}$.

Verify: To verify a signed message from a user *A*, a recipient performs the operation using *A*'s identifier ID_A and public key P_A after checking P_A's correctness.

3.1 Chosen Message Attack

Here, we present the formal security model for our signature scheme. Security against chosen message attack is the standard notion of security for a signature scheme. It is defined through the following game between a challenger and an adversary $\mathcal{A}$.

Setup: The challenger takes a security parameter k and runs the **Setup** algorithm. It gives to $\mathcal{A}$ the resulting system parameters `params` and keeps `master-key` with itself.

Query Phase: $\mathcal{A}$ issues signing queries $M_1, ..., M_n$ where $M_i \in \{0,1\}^*$. These queries can be made adaptively. The challenger responds by first running the **Key Generation** algorithm to generate the private key. It then works through the **Sign** algorithm with the private key and returns the resulting signature to $\mathcal{A}$.

Guess: $\mathcal{A}$ outputs a message-signature pair $\langle M, Sig \rangle$ where M is the one that did not appear in the query phase. The adversary wins if *Sig* is a valid signature on M. The

advantage of an adversary $\mathcal{A}$ against a signature scheme is defined to be the probability that $\mathcal{A}$ produces a valid message-signature pair in the game.

We say that our signature scheme is secure against adaptive chosen message attack if no polynomially bounded adversary has non-negligible advantage in this game.

4 Proposed Scheme

In this section, we present a signature scheme, which is based on the ID-based signature scheme of [14]. The proposed signature scheme involves three entities the trusted authority (TA), the signer and the verifier.

4.1 The Signature Scheme

Setup: The TA performs the following steps.

1. Specifies $\langle G_1, G_2, e\rangle$ where G_1 and G_2 are groups of some prime order q and $e : G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing.
2. Chooses an arbitrary generator $P \in G_1$.
3. Selects a `master-key` t uniformly at random from Z_q^* and sets TA's public key Q_{TA} as $Q_{TA} = tP$.
4. Chooses two cryptographic hash functions $H : \{0,1\}^* \times G_2 \rightarrow Z_q^*$ and $H_1 : \{0,1\}^* \rightarrow G_1^*$.

The system parameters are `params` $= \{G_1, G_2, q, e, n, P, Q_{TA}, H, H_1\}$, the message space is $\mathcal{M} = \{0,1\}^*$ and the signature space is $\mathcal{S} = G_1 \times Z_q^*$.

Key Generation: In this algorithm the user A first calculates his parameters `user-params` and sends them to the TA along with his identifier ID_A. The TA verifies ID_A and `user-params`, calculates partial private key D_A and public key P_A for A, sends D_A to A and publishes P_A. Then the user A calculates his private key S_A on his own from the received D_A. The algorithm is described in the following steps.

1. A chooses two secret values $s_1, s_2 \in Z_q^*$, calculates his user parameters as `user-params` $= \{s_1 s_2 Q_A, s_1 Q_A, s_2 P, s_1 s_2 P\}$ where $Q_A = H_1(ID_A)$ and sends them to the TA. A also sends his identifier ID_A along with the `user-params`.
2. TA verifies ID_A, calculates Q_A and checks whether the equalities

$$e(P, s_1 s_2 Q_A) = e(s_1 s_2 P, Q_A) = e(X_A, s_1 Q_A)$$

   hold good, where $X_A = s_2 P$. If not it aborts the process.
3. TA calculates D_A as $D_A = t s_1 s_2 Q_A$ and P_A as $P_A = \langle X_A, Y_A\rangle$ where $Y_A = tX_A = t s_2 P$.
4. TA sends D_A to A and publishes P_A.
5. A verifies the correctness of D_A by checking $e(D_A, P) = e(s_1 s_2 Q_A, Q_{TA})$. A also verifies whether the published public key component X_A is equal to $s_2 P$ and calculates S_A as $S_A = s_1^{-1} D_A$ after successful verification.

Note that the step 2 is performed by the TA to see whether the `user-params` are associated with the identity of the user.

In our scheme the secret value s_1 serves as a blinding factor and has been used to avoid the secure channel between the user and the TA. The user A extracts his private key S_A by unblinding the partial private key D_A. The user's chosen secret value s_2, which has been used to eliminate the key escrow problem, binds the private key S_A and the public key P_A.

Sign: To sign a message $M \in \mathcal{M}$ using the private key S_A, the signer A performs the following steps.

1. Chooses a random $l \in Z_q^*$.
2. Computes $r = e(lP, P) \in G_2$.
3. Sets $v = H(M, r) \in Z_q^*$.
4. Computes $U = vS_A + lP$.

Then A sends $\langle U, v \rangle \in \mathcal{S}$ as the signature along with the message M to the verifier.

Verify: On receiving a signature $Sig =< U, v > \in \mathcal{S}$ on a message M from user A with identifier ID_A and public key P_A, the verifier performs the following steps.

1. Checks that the equality $e(X_A, Q_{TA}) = e(Y_A, P)$ holds good. If not aborts the verification.
2. Computes $r' = e(U, P)e(Q_A, -Y_A)^v$.
3. Checks if $v = H(M, r')$ holds. Accepts the signature if it does and rejects otherwise.

4.2 Security Analysis

As given in the security model in previous section, the adversary's goal is to produce an existential forgery of a signature scheme by a signer's ID and public key of its choice. For a target identity ID_t, we allow the adversary to query four oracles.

Identity Hash Oracle: For any given identity ID this oracle will produce corresponding hash value $H_1(ID)$.

Extraction Oracle: For any given identity ID and public key, this oracle will produce the corresponding secret key.

Message Hash Oracle: For any given message M and $r \in Z_q^*$, this oracle will produce the corresponding hash value $H(M, r)$.

Signature Oracle: For any given message M, identity ID and public key this oracle will produce a signature of user with identity ID on the message M.

As stated in the security model, the output of the adversary $\mathcal{A}$ should not be a signature such that the secret key or signature of the target identity ID_t have been asked of the oracles.

Chosen Message Security: In the random oracle model, suppose that an adaptive adversary $\mathcal{A}$ exists which makes at most $n_1 \geq 1$ queries of the identity hash and the

extraction oracle, at most $n_2 \geq 1$ queries of the message hash and signature oracle and which succeeds within the time T_A of making an existential forgery with probability

$$\varepsilon_A \geq \frac{an_1n_2^2}{q}$$

for some constant $a \in Z^{\geq 1}$. Then there is another probabilistic algorithm $\mathcal{C}$ and a constant $c \in Z^{\geq 1}$ such that $\mathcal{C}$ solves the CDHP with respect to

$$(P, Y_A, R)$$

on input of any given $R \in G_1^*$, in expected time

$$T_C \leq \frac{cn_1n_2T_A}{\varepsilon_A}.$$

The detailed proof of the above statement can be found in [14].

Apart from formal security, we now discuss some possible attacks during the **Key Generation** phase. we show that our scheme can successfully resist following attacks.

User Private Key Forgery: An attacker trying to forge the signature by calculating the private key of a participating user in the scheme is computationally infeasible because given `params` and the publicly transmitted information Q_A, `user-params` $\{s_1s_2Q_A, s_1Q_A, s_2P, s_1s_2P\}$ and P_A, calculating the private key S_A (i.e. ts_2Q_A) is as hard as WDHP, which is assumed to be computationally hard. Forgery attacks can also be performed by replacing the public keys in the directory as discussed earlier. But, the adversaries who replace public keys and do not have access to the master key can not calculate the corresponding private key. Thus, assuming that the TA does not involve in such type of actions, our scheme achieves trust level 2 as per the terminology describe in [12]. By applying the alternate key generation technique given in [1], where Q_A is calculated as $H_1(ID_A||P_A)$, even the TA can not perform forgery by replacing the public keys without being detected. Thus, our scheme enjoys trust level 3 which is the same for conventional PKC.

Man-in-the-middle Attack: An attacker can eavesdrop on the communication between the user and the TA and alter the `user-params` which are communicated through a public channel. A possible attack might be changing the `user-params` $\{s_1s_2Q_A, s_1Q_A, s_2P, s_1s_2P\}$ to $\{s_1s_2Q_A, s_1Q_A, as_2P, a^{-1}s_1Q_A\}$. As the user checks the X_A component before calculating his private key, such an attack can always be detected.

Collusion Attack: Another possible attack can be the collusion attack where the users collude among themselves to extract the TA's master key or collude with the TA to forge a valid signature. Calculating the TA's master key by collusion among users is as hard as the DLP and forging a valid signature by colluding with the TA is equivalent to WDHP, which are assumed to be computationally hard.

5 Conclusions

In this paper, we presented a certificateless signature scheme based on bilinear pairings. We used a simple blinding technique to avoid the necessity of a secure channel for

key issuance between the participating entities and the trusted authority. Moreover, we eliminated the key escrow problem, which is an inherent drawback of ID-based cryptosystems, by using user chosen secret value. We showed that the scheme is secure in random oracle model against adaptive chosen message attack assuming that the CDHP is computationally hard.

References

1. Al-Riyami, S., and Paterson, K.: Certificateless Public Key Cryptography. In: Advances in Cryptology-ASIACRYPT 2003, Lecture Notes in Computer Science, Vol. 2894, Springer-Verlag, (2003) 452-473.
2. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., and Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Advances in Cryptology-CRYPTO 2002, Lecture Notes in Computer Science, Vol. 2442, Springer-Verlag, (2002) 354-368.
3. Bellare, M., Desai, A., Pointcheval, D., and Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Advances in Cryptology-CRYPTO 98, Lecture Notes in Computer Science, Vol. 1462, Springer-Verlag, (1998) 26-45.
4. Boldyreva, A.: Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman-Group Signature Scheme. In: Proceedings of PKC 2003, Lecture Notes in Computer Science, Vol. 2567, Springer-Verlag, (2003) 31-46.
5. Boneh, D., and Franklin, M.: Identity-based Encryption from the Weil pairing. SIAM J. of Computing, 32(3), (2003) 586-615. Extended abstract in Proceedings of CRYPTO 2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, (2001) 213-229.
6. Cha, J., and Cheon, J.H.: An Identity-Based Signature from Gap Diffie-Hellman Groups. In: Proceedings of Public Key Cryptography-PKC 2003, Lecture Notes in Computer Science, Vol. 2567, Springer-Verlag, (2003) 18-30.
7. Chen, L., Harrison, K., Smart, N. P., and Soldera, D.: Application of multiple trust authorities in pairing based cryptosystems. In: Proceedings of INFRASEC 2002, Lecture Notes in Computer Science, Vol. 2437, Springer-Verlag, (2002) 260-275.
8. Dolev, D., Dwork, C., and Naor, M.: Non-malleable cryptography. SIAM J. of Computing, 30(2), (2000) 391-437.
9. Dutta, R., Barua R., and Sarkar, P.: Pairing-Based Cryptographic Protocols: A Survey. In: Cryptology ePrint Archive, Report 2004/064, (2004). http://eprint.iacr.org/2004/064/.
10. Fiat, A., and Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Advances in Cryptology-CRYPTO 86, Lecture Notes in Computer Science, Vol. 0263, Springer, (1986) 186-194.
11. Gentry, C.: Certificate-Based Encryption and the Certificate Revocation Problem. In: Advances in Cryptology-EUROCRYPT 2003, Lecture Notes in Computer Science, Vol. 2656, Springer-Verlag, (2003) 272-293.
12. Girault, M.: Self-certified public keys. In: Advances in Cryptology-EUROCRYPT'91, Lecture Notes in Computer Science, Vol. 0547, Springer-Verlag, (1991) 490-497.
13. Guillou, L., and Quisquater, J.-J.: A "Paradoxical" Identity-Based Signature Scheme Resulting From Zero-Knowledge. In: Advances in Cryptology-CRYPTO 88, Lecture Notes in Computer Science, Vol. 0403, Springer, (1988) 216-231.
14. Hess, F.: Efficient Identity Based Signature Schemes Based on Pairings. In: Selected Areas in Cryptography-SAC 2002, Lecture Notes in Computer Science, Vol. 2595, Springer- Verlag, (2003) 310-324.

15. Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J., and Yoo, S.: Secure Key Issuing in ID-based Cryptography. In: Proceedings of the Second Australian Information Security Workshop-AISW 2004, ACSW Frontiers 2004, ACS Conferences in Research and Practice in Information Technology, Vol. 32, (2004) 69-74.
16. Libert, B., and Quisquater, J.-J.: What is Possible with Identity Based Cryptography for PKIs and What Still Must Be Improved. In: Proceedings of EUROPKI 2004, Lecture Notes in Computer Science, Vol. 3093, Springer-Verlag, (2004) 57-70.
17. Paterson, K.G.: ID-based signatures from pairings on elliptic curves, In: Cryptology ePrint Archive, Report 2002/004, (2002). http://eprint.iacr.org/2002/004/
18. Pointcheval, D., and Stern, J.: Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 13(3), Springer-Verlag (2000) 361-396.
19. Sakai, R., Ohgishi, K., and Kasahara, M.: Cryptosysytems based on pairing. In: Proceedings of Symposium on Cryptography and Information Security, SCIS 2000, 2000.
20. Shamir, A.: Identity-based Cryptosystems and Signature Schemes. In: Advances in Cryptology-CRYPTO 84, Lecture Notes in Computer Science, Vol. 0196, Springer-Verlag, (1984) 47-53.
21. Yum, D.H., and Lee, P.J.: Identity-Based Cryptography in Public Key Management. PKI 2004, Lecture Notes in Computer Science, Vol. 3093, Springer-Verlag, (2004) 71-84.