

# Short Signature Scheme From Bilinear Pairings

Sedat Akleylek <sup>\*</sup>, Barış Bülent Kırlar <sup>\*\*</sup>, Ömer Sever, and Zaliha Yüce <sup>\*\*\*</sup>

Institute of Applied Mathematics, Middle East Technical University, 06531, Ankara,  
Turkey

{akleylek,kirlar}@metu.edu.tr, severomer@yahoo.com, zyuce@stm.com.tr

**Abstract.** The Boneh, Lynn, Shacham (BLS) scheme, the first short signature scheme, proposed by Boneh, Lynn, and Shacham [7] has the shortest length among signature schemes in classical cryptography. The main problem in BLS is the use of special hash function [3, 4, 7]. To deal with this problem, many cryptographic schemes were proposed with cryptographic hash functions such as MD5, SHA-1 [8]. We construct a new and efficient short signature scheme from the bilinear pairings. Our scheme is constructed by Bilinear Inverse-Square Diffie-Hellman Problem (BISDHP) and does not require any special hash function. We give the implementation and comparison results of the BLS scheme.

**Key words:** short signature, bilinear pairings

## 1 Introduction

Digital signatures are the most important cryptographic primitive for the daily life. Short signatures are needed in environments with space and bandwidth constraints. Upto pairing-based cryptography, the best known shortest signature was obtained by using the Digital Signature Algorithm (DSA) [1] over a finite field  $\mathbb{F}_q$ . The length of the signature is approximately  $2\log q$ . On the other hand, when the pairing-based cryptographic protocol is used the length of the signature is about  $\rho \log q$ , where  $\rho = \log q / \log r$  and  $r$  is the largest prime divisor of the number of the points in the elliptic curve. For example, if one uses RSA signature 1024 bit modulus, ECDSA signature is 320 bit long for the same security level. However, short signature provides the same security level only for 160 bits for the best choice.

In 2001 Boneh, Lynn and Shacham [7] proposed the idea of short signature scheme by using bilinear pairings. This scheme is based on Weil pairing and needs a special hash function. Over the last years, there are various applications

---

<sup>\*</sup> S. Akleylek is also with the Department of Computer Engineering, OnDokuz Mayıs University, Samsun, Turkey

<sup>\*\*</sup> B. B. Kırlar is also with the Department of Mathematics, Süleyman Demirel University, Isparta, Turkey

<sup>\*\*\*</sup> Z. Yüce is a software engineer in STM A.Ş

of bilinear pairings in short signature schemes to construct new efficient schemes [5], [6], [8]. The main improvement in short signature schemes is the use of cryptographic hash function instead of special hash function called map to point hash operation. It is known that short signature scheme with cryptographic hash function is more efficient than others since map to point hash operation is still probabilistic.

In this note, we describe a new short signature scheme in a similar setting in the ZSS scheme. Our system is based on Bilinear Inverse-Square Diffie-Hellman Problem a combination of Bilinear Inverse Diffie-Hellman Problem (BIDHP) and Bilinear Square Diffie-Hellman Problem (BSDHP). The main advantage of our scheme is that it can be used with any cryptographic hash function such as MD5, SHA-1. We give the comparison of our scheme with the BLS scheme and ZSS scheme. According to the comparison results, our scheme is more efficient than BLS scheme.

## 1.1 Bilinear Pairings

**Definition 1.** Let  $(G_1, +)$  and  $(G_2, +)$  be abelian groups of order  $n$ . Let  $(G_3, \cdot)$  be a cyclic group of order  $n$ . A bilinear pairing is an efficiently computable map  $e : G_1 \times G_2 \rightarrow G_3$  which satisfies the following additional properties:

1. (bilinearity) For all  $P, R \in G_1$  and all  $Q, S \in G_2$ , we have  $e(P + R, Q) = e(P, Q)e(R, Q)$  and  $e(P, Q + S) = e(P, Q)e(P, S)$ .
2. (non-degeneracy) For all  $P \in G_1$ , with  $P \neq Id_{G_1}$ , there is some  $Q \in G_2$  such that  $e(P, Q) \neq 1$ . For all  $Q \in G_2$ , with  $Q \neq Id_{G_2}$ , there is some  $P \in G_1$  such that  $e(P, Q) \neq 1$ . When  $G_1 = G_2$  and  $n$  is prime,  $e(P, P)$  is a generator of  $G_3$  for all  $P \neq Id_{G_1}$ .

## 1.2 The Bilinear Diffie-Hellman Problem (BDHP)

Security of the some of the applications of bilinear pairings in cryptography relies on the difficulty of bilinear Diffie-Hellman problem which was first stated in [4].

**Definition 2.** Let  $G$  be a finite cyclic group of order  $n$  with a generator  $g$ , and let  $a, b, c$  be integers. The BDHP is to compute the value of the bilinear pairing  $e(g^{abc}, g)$ , whenever  $g^a, g^b$  and  $g^c$  are given.

There are variants of BDHP.

- **Bilinear Inverse Diffie-Hellman Problem (BIDHP)** : For  $a, b \in \mathbb{Z}_n^*$ , given  $P, aP, bP$  to compute  $e(P, P)^{a^{-1}b}$ .
- **Bilinear Square Diffie-Hellman Problem (BSDHP)** : For  $a, b \in \mathbb{Z}_n^*$ , given  $P, aP, bP$  to compute  $e(P, P)^{a^2b}$ .

It is not hard to obtain Bilinear Inverse-Square Diffie-Hellman Problem as a combination of BIDHP and BSDHP:

- **Bilinear Inverse-Square Diffie-Hellman Problem (BISDHP)** : For  $a, b \in \mathbb{Z}_n^*$ , given  $P, aP, bP$  to compute  $e(P, P)^{a^{-2}b}$ .

**Theorem 1.** *BDHP, BIDHP, BSDHP and BISDHP are polynomial time equivalent.*

## 2 New Short Signature Scheme From Bilinear Pairings

Let  $(G_1, +)$  and  $(G_2, \cdot)$  be cyclic groups of prime order  $n$ ,  $P \in G_1$ ,  $G_1 = \langle P \rangle$  and  $e : G_1 \times G_1 \rightarrow G_2$  be a bilinear map. Let  $H(x)$  be cryptographic hash function such as MD5, SHA-1. Suppose that  $A$  wants to send a signed message to  $B$ .

A signature scheme consists of four steps.

- **Parameters** :  $\{G_1, G_2, e, n, P, H\}$
- **Key Generation** :  $A$  randomly selects  $x \in \mathbb{Z}_n$  and computes  $P_{pub1} = x^2P$  and  $P_{pub2} = 2xP$ . In this structure,  $P, P_{pub1}$  and  $P_{pub2}$  are the public keys,  $x$  is the secret key.
- **Signing** : Given a secret key  $x$  and a message  $m$ ,  $A$  computes the signature,  $s = (H(m) + x)^{-2}P$ .
- **Verification** : Given the public keys  $P, P_{pub1}$  and  $P_{pub2}$ , a message  $m$  and a signature  $s$ ,  $B$  verifies the signature if

$$e(H(m)^2P + P_{pub1} + P_{pub2}H(m), s) = e(P, P) \text{ holds.}$$

*Proof.* By using Bilinear Inverse-Square Diffie-Hellman Problem,

$$e((H(m) + x)^2P, (H(m) + x)^{-2}P) = e(P, P)^{(H(m)+x)^2(H(m)+x)^{-2}} = e(P, P)$$

### 2.1 Efficiency

We compare our signature scheme with the BLS scheme and ZSS scheme from the implementation point of view.  $PO, SM, PA, Squ, Inv, MTP$  and  $H$  denote the pairing operation, scalar multiplication in  $G_1$ , point addition in  $G_1$ , squaring in  $\mathbb{Z}_n$ , inversion in  $\mathbb{Z}_n$ , map to point hash operation and hash operation in  $\mathbb{Z}_n$ , respectively. Table 1 summarizes the result.

**Table 1.** Comparison of our scheme with the BLS scheme and ZSS scheme

	BLS	ZSS	Proposed
Key Generation	1 $SM$	1 $SM$	2 $SM$
Signing	1 $MTP$ , 1 $SM$	1 $H$ , 1 $Inv$ , 1 $SM$	1 $H$ , 1 $Squ$ , 1 $Inv$ , 1 $SM$
Verification	1 $MTP$ , 2 $PO$	1 $H$ , 1 $SM$ , 1 $PO$	1 $H$ , 1 $Squ$ , 1 $SM$ , 2 $PA$ , 1 $PO$

We implemented proposed signature scheme by using Pairing-Based Cryptography (PBC) Library [2]. It should be noted that computation of pairing is the most time-consuming part in short signature schemes. According to the implementation results, our new scheme is more efficient than BLS scheme since it requires less pairing operation.

### 3 Conclusion

In this note, we proposed a new short signature scheme not requiring any special hash function. The security of this signature scheme depends on a new problem called Bilinear Inverse-Square Diffie-Hellman Problem (BISDHP). It is shown that this problem and BDHP are polynomial time equivalent.

### References

1. FIPS 186. Digital Signature Algorithm, 1994.
2. The Pairing-Based Cryptography (PBC) Library available at <http://crypto.stanford.edu/pbc/>
3. P.S.L.M. Barreto and H.Y. Kim, "Fast hashing onto elliptic curves over fields of characteristic 3", Cryptology ePrint Archive, Report 2001/098, available at <http://eprint.iacr.org/2001/098/>.
4. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Cryptology CRYPTO01, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.
5. D. Boneh and X. Boyen, "Short Signatures without Random Oracles", Advances in Cryptology - EUROCRYPT'04, Vol.3027 of LNCS, pp.56-73, Springer-Verlag, 2004.
6. D. Boneh, X. Boyen and H. Shacham, "Short Group Signatures", Advances in Cryptology - CRYPTO'04, Vol.3152 of LNCS, pp.41-55, Springer-Verlag, 2004.
7. D. Boneh, B. Lynn and H. Shacham, "Short Signatures from the Weil Pairing", Advances in Cryptology - ASIACRYPT01, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.
8. F. Zhang, R. Safavi-Naini and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications", PKC 2004, Singapore. LNCS, Springer-Verlag, 2004.