New Short Signature Scheme with Weil Pairing

Neetu Sharma
(Corresponding Author)
School of Studies in Mathematics
Pt. Ravishankar Shukla University
Raipur (C.G) 492010, India

Birendra Kumar Sharma
School of Studies in Mathematics
Pt. Ravishankar Shukla University
Raipur(C.G) 492010, India

ABSTRACT
Short signature is an essential component in cryptography. Short digital signatures are needed in environments where a human is asked to manually key in the signature.. In this paper we propose a new short signature scheme with weil pairing. Also we analyze security and efficiency of our scheme. Security of our scheme is based on expressing the torsion point of curve into linear combination of its basis points; it is more complicated than solving ECDLP(Elliptic Curve Discrete Logarithm Problem). We claim that our new short signature scheme is more secure and efficient than the existing scheme of SedatAkleylek et al. based on bilinear pairing.

General Terms
2000 AMS Subject Classification No. 94A60

Keywords
Cryptography, Short signature scheme, Elliptic curve cryptosystem, Chosen message attack, Weil Pairing.

1. INTRODUCTION
Digital signature schemes have found numerous practical applications such as electronic mail, office automation, and electronic funds transfer. 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 Fq. The length of the signature is approximately$2logq$. On the other hand, when the pairing-based cryptographic protocol is used the length of the signature is about $r\,logr$, where $r = logq/logr$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, the output of elliptic curve digital signature algorithm (ECDSA) 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 the last couple of years, the bilinear pairing has become flourishing area in cryptography, namely Weil pairing and Tate pairing are important tools for construction of ID-based cryptographic scheme.

The first cryptographic treatment on short signature scheme was proposed by Boneh, Lynn, and Shacham [2] in the year 2001 which has the shortest length among signature schemes in classical cryptography. The main problem in BLS is the use of special hash function [1, 3, 4]. To deal with this problem, many cryptographic schemes were proposed with cryptographic hash functions such as MD5, SHA-1 [5]. In 2004,Fangguo Zhang [3] et al. proposed a new short signature scheme from the bilinear pairings that unlike BLS, uses general cryptographic hash functions such as SHA-1 or MD5, and does not require special hash functions. Furthermore, the scheme requires less pairing operations than BLS scheme and so is more efficient than BLS scheme. In 2011, Sedat Akleylek et al.[6] proposed a new short signature scheme in a similar setting in the ZSS scheme whose security was based on Bilinear Inverse-Square Diffie-Hellman Problem a combination of Bilinear Inverse Diffie-Hellman Problem (BIDHP) and Bilinear Square Diffie-Hellman Problem (BSDHP).

In this paper, we propose a new short signature scheme with weil pairing, the security of our scheme is based on expressing the torsion point of curve into linear combination of its basis points, it is more complicated than solving ECDLP.

The rest of this paper is as follows: In section 2, we discuss some basic preliminaries of our scheme. In section 3, we propose new short signature scheme with the weil pairing and in section 4, we analyze the security properties of our new scheme. In section 5, we give efficiency of our scheme. Finally we conclude our work in last section.

2. PRELIMINARIES
Definition 2.1.Elliptic Curve

Let $K = F_q$ be a finite field, where q is a power of some prime number The Weierstrass equation of an elliptic curve over K can be written in the following form:-

$$y^2 + cxy + dy = x^3 + ax + b$$

$$where\ a, b, c, d \in K$$

If $q > 3$ then by a linear change of variables above equation can be reduced in simpler form

$$y^2 = x^3 + ax + b\ with\ a, b \in GF\ (q)\ and$$

$$4a^3 + 27b^2 \neq 0,$$

An elliptic curve over K is the set of solutions of the Weierstrass equation with a point O, called point at infinity. An adding operation can be defined over the elliptic curve, which turns the set of the points of the curve into a group. The adding operation between two points is defined as follows.

In affine coordinates let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the elliptic curve, neither being the point at infinity over$GF\ (q)$. The inverse of a point P_1 is$-P_1 = (x_1, -y_1)$.If $P_1 \neq P_2$ then $P_1 + P_2 = P_3 = (x_3, y_3)$ with

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

Where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \text{ if } P_1 \neq P_2$$

$= \frac{3x_1^2+a}{2y_1}$, if $P_1 = P_2$ (doubling)

Definition 2.2.Torsion Points and Basis Points

Let $m \geq 1$ be an integer. A point $P \epsilon E$ satisfying $= O$(point at infinity) is called point of order m in the group$E$. The set of points of order m is denoted by

$$E[m] = \{P \in E;\ mP = O\}$$

Such points are called points of finite order or torsion points. If P and Q are in $E[m]$ then $P + Q$ and $-P$ are also in$E[m]$, so $E[m]$ is subgroup of E.

Proposition2.1. Let $m \geq 1$ be an integer

(1) Let E be an elliptic curve over. Then

$$E(K)[m] \cong \frac{Z}{mZ} \times \frac{Z}{mZ}$$

(2) Let E be an elliptic curve over F_q and assume that $p$does not divide m then there exists a value $k$such that

$$E(F_{p^{jk}})[m] \cong \frac{Z}{mZ} \times \frac{Z}{mZ} for all j \geq 1$$

Proof. For the proof of proposition refer [9], Corollary III 6.4.

According to proposition, if we allow points with coordinates in a sufficiently large field, then $E[m]$looks like a 2-dimensional vector space over the field Z/mZ.Let'schoose basis P_1, P_2in $E[m]$. Then any element $P \in E[m]$can be expressed in terms of the basis elements as $P = aP_1 + bP_2$ for unique a, binZ/mZ. Expressing a point in terms of the basis points P_1, P_2 is more complicated than solving ECDLP [10].

Definition2.3.Weil pairing [9]:- Weil pairing $e_m : E[m] \times E[m] \rightarrow G$, where G is a multiplicative group of m^{th}roots of unity. Weil pairing is denoted bye_m, takes as input a pair of points $P, Q \in E[m]$ and gives as output an m^{th} root of unity $e_m(P, Q)$. The bilinearity of the Weil pairing is expressed by the equations

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$$

$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$$

The weil pairing has many useful properties:-

a) The values of the Weil pairing satisfy $e_m(P, Q)^m = 1$ for all $P, Q \in E[m]$.

b) The Weil pairing is alternative, which means that $e_m(P, P) = 1$ for all $P \in E[m]$.

c) The Weil pairing is non degenerate, which means that if $e_m(P, Q) = 1$ for all $Q \in E[m]$ then $P = O$.

3. A NEW SHORT SIGNATURE SCHEME

Our new scheme involves the one-to-one interactions to execute the system initialization phase, the key generation phase, the signature generation phase and the signature verification phase, as follows.

3.1. System initialization Phase

In the system initialization phase, the following commonly required parameters are generated to initialize the scheme.

a) A field size q, which is selected such that, q = p if p is an odd prime, otherwise,$q = 2^n$, as q is a prime power.

b) Two parameters $a, b \in F_q$ that define the equation of elliptic curve E over F_q ($y^2 = x^3 + ax + b(mod q)$ in the case$q > 3$, where$4a^3 + 27b^2 \neq 0(mod q)$).

c) A large prime number m, and basis points P_1 and P_2 of $E[m]$.

d) Weil pairing$e_m : E[m] \times E[m] \rightarrow G$, where G is a multiplicative group of m^{th}roots of unity.

e) $H(,)$a secure hash function.

3.2. Key generation

The signer U compute secret and public key pair using two basis point $P_1,\ P_2 \in E[m]$.

a) Randomly select integers a, b from the interval $[1, 2, \ldots, n - 1]$ as the secret key.

b) Compute the corresponding public key as $P = aP_1 + bP_2$, where $P_1,\ P_2 \in E[m]$ be two basis point.

3.3. Signing

To sign the message m, the original signer needs to perform the operations as follows:-

a) Convert the message $m$and the value P into one integer using hash operation$h = H(m, P)$.

b) Then original signer computes $y = ha - bmodn$, and sends (h, y) to verifier.

3.4. Verification phase

For verifying the correctness the verifier has to perform the following operations

a) Compute $h = H(m, P)$ and

$$e_m(P_1, P_2)^y = e_m(P, P_2)^h e_m(P, P_1)$$

Checks whether the equation holds. If so, the verifier accepts the signature (h, y); otherwise rejects it.

3.5. Correctness of scheme

Theorem3.1. The equation
$e_m(P_1, P_2)^y = e_m(P, P_2)^h e_m(P, P_1)$ is correct.

Proof:- $e_m(P, P_2)^h e_m(P, P_1)$

$= e_m(aP_1 + bP_2, P_2)^h e_m(aP_1 + bP_2, P_1)$

$= e_m(aP_1, P_2)^h e_m(bP_2, P_1)$

$= e_m(P_1, P_2)^{ah} e_m(P_2, P_1)^b$

$= e_m(P_1, P_2)^{ah} e_m(P_1, P_2)^{-b}$

$= e_m(P_1, P_2)^{ah-b}$

$= e_m(P_1, P_2)^y$

4. SECURITY ANALYSIS

We use the following lemma and other security properties to discuss the security of our scheme. We shall show some possible attacks by which an adversary (Adv) may try to take down the new developed identification scheme. The difficulties associated with the attacks are based on expressing the torsion point of curve into linear combination of its basis points, it is more complicated than solving ECDLP. For every attack, we define the attacks and give reason why this attack would be failed.

Lemma4.1. If one can express a point of elliptic curve into linear combination of basis points then he can easily solve ECDLP.

Proof. Solving the ECDLP for P means that if Q is a multiple of, then find m so that$Q = mP$. If Q is any point of elliptic curve then expressing Q in terms of the basis means finding $m_1$and m_2, so that $Q = m_1P_1 + m_2P_2$. If we can solve the former, then given $P$and$Q$, write$P = n_1P_1 + n_2P_2$ and $Q = m_1P_1 + m_2P_2$. Since $P_1$and P_2 are independent, if $Q = kP$, then

$$1 = k * n1 mod(orderP1)$$

$$m2 = k * n2 mod(orderP2).$$

From this one can solve for k modulo the order of P.

Attack I. Suppose eavesdropper is able to solve ECDLP. Since P_1 and P_2 are independent. So Pcan not be expressed as scalar multiple of P_1 and P_2. Hence Adv cannot use ECDLP to find the values of a and b from $P = aP_1 + bP_2$.

Attack II. Adv wishes to obtain secret key (a, b) using all information that available from the system. Adv needs to solve $P = aP_1 + bP_2$ which is clearly infeasible because the difficulty is based on expressing the torsion point of curve into linear combination of its basis points, it is more complicated than solving ECDLP.

Attack III. The case when the Adv wishes to forge an individual signature (h, y) for message, m. To forge a valid signature for a message m, the Adv needs to solve$h = H(m, P)$, and calculate y. The method of finding all these is also based on expressing the torsion point of curve into linear combination of its basis points, which is more complicated than solving ECDLP.

5. EFFICIENCY

Table 1 defines our notation. The time complexity of the proposed protocol and some other protocol in terms of modular multiplication operation, modular weil pairing operation, modular inverse operation, and modular scalar multiple scalar multiplication and one way hash function is shown in table 1.

Table 2 shows the efficiency comparison of our newly propose scheme with the scheme of BLS[2] ,ZSS[3]and Sedat Akleylek et al[6]scheme.

Table1. Time complexity of various operations

Notation	Definition
T_{BP}	Time complexity for the execution of a bilinear pairing.
T_{EC-MUL}	Time complexity for the execution of an elliptic curve multiplication.
T_{SM}	Time complexity for the execution of a scalar multiple scalar multiplication.
T_{EXP}	Time complexity for the execution of a exponentiation.
T_{IN}	Time complexity for the execution of an inversion.
T_h	Time complexity for the execution of a hash function.
T_{MUL}	Time complexity for the execution of a modular multiplication.
T_{EC-ADD}	Time complexity for the execution of an elliptic curve addition.
T_{ADD}	Time complexity for the execution of an addition.
T_{SQU}	Time complexity for the execution of an square.
T_{MTP}	Time complexity for the execution of map to point hash function.

Table 2:- Comparison of efficiency

	Key generation	Signature generation	Signature verification
BLS [2]	$1T_{EC-MUL}$	$1T_{MTP}$ $+1T_h$	$2T_{BP}$ $+1T_{MTP}$
ZSS [3]	$1T_{EC-MUL}$	$1T_{EC-MUL}$ + $+1T_{IN}$ + $1T_h$	$1T_{EC-MUL}$+ $1T_{BP}$ + $1T_h$
SedatAkleylek et al[6]	$2T_{EC-MUL}$	$1T_h$+ $1T_{SQU}$+ $1T_{EC-MUL}$ $+1T_{INV}$	$1T_{EC-MUL}$ + $1T_h$ $+1T_{SQU}$ + $2T_{BP}$+ $2T_{EC-ADD}$
Our's scheme	$1T_{SM}$	$1T_{MUL} + 1T_h$	$2T_{BP} + 1T_h$ $+2T_{EXP}$

6. CONCLUSION

Security of our scheme is based on expressing the torsion point of the curve into linear combination of its basis points, it is more complicated than solving ECDLP. So our scheme is more secure than all based on ECDLP and as compare to other existing schemes it is efficient also.

7. REFERENCES

[1] FIPS 186. Digital Signature Algorithm, 1994.

[2] D. Boneh, B. Lynn and H. Shacham, 2001, "Short Signatures from the Weil Pairing", Advances in

Cryptology - ASIACRYPT01, LNCS 2248, Springer-Verlag, pp. 514-532.

[3] F. Zhang, R. Safavi-Naini and W. Susilo, 2004, "An efficient signature scheme from bilinear pairings and its applications", PKC 2004, Singapore. LNCS, Springer-Verlag.

[4] 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/.

[5] D. Boneh and M. Franklin, 2001, "Identity-based encryption from the Weil pairing", Advances in Cryptology CRYPTO01, LNCS 2139, Springer-Verlag, pp. 213-229.

[6] SedatAkleylek, Barıs Bulent Kırlar,2011, ¨Omer Sever, and ZalihaY¨uce, Short Signature Scheme From Bilinear Pairings.Journal of telecommunication and information technology.

[7] V.S.Miller,1986 Use of elliptic curves in cryptography, Advances in Cryptology-Proceedings of Crypto85, LNCS, vol. 218, Springer.

[8] J.H.Silverman, 1986, The arithmetic of elliptic curves, volume 106 of graduate texts in mathematics, springer-verlag,Newyork 1986.

[9] J. Hoffstein, J. Pipher., and J. H. Silverman, An introduction to mathematical cryptography, springer.