# A New Short Signature Scheme from Weil Pairing

Subhas Chandra Sahana
Department of Information Technology
North Eastern Hill University
Shillong, India

Somen Debnath
Department of Information Technology
Mizoram University
Mizoram, India

Bubu Bhuyan
Department of Information Technology
North Eastern Hill University
Shillong, India

## ABSTRACT
Currently, short signature is receiving significant attention since it is particularly useful in low-bandwidth communication environments. In this paper, a short signature scheme is proposed from weil pairing. The proposed scheme is efficient as lesser number of cost effective pairing operations involved. We analyze security and efficiency comparison of the proposed scheme with other short signature schemes.

## General Terms
Cryptography and network security

## Keywords
short signature; elliptic curve cryptosystem; weil pairing

## 1. INTRODUCTION
Digital signatures are the most important cryptographic primitive for the daily life. Short signature is a variant of digital signature which can provide a high security level with relatively shorter signature length. As an example, BLS [1] short signature has half the size of a DSA [2] signature but gives a same security level. Short signatures have many applications in real life. For instance, as said in Bellare and Neven (2006), wireless devices have a short battery life. Communicating even one bit of information uses essentially more power than executing one 32-bit instruction (Barr and Asanovic, 2003). Consequently, diminishing the number of bits in communication saves power and increase the battery life. Also, in numerous settings, communication channels are not reliable. So with the short signature, it reduces the number of bits to be sent over a communication channel. Recently, short signatures have been investigated intensively and many short signature schemes have been proposed [1][3][4][5].

Recently, bilinear paring mainly Weil pairing and Tate pairing are used as tools to construct variant signature schemes. There are some cryptographic schemes which can only be constructed by bilinear pairing, for example ID-based encryption, non-trivial aggregate signature, tripartite one round Diffie-Hellman key exchange, etc. Besides these, some primitives which can be constructed using other techniques, but for which pairings provides improved functionality and makes the cryptographic schemes simple and efficient.

The Digital Signature Algorithm (DSA) [2] over a finite field $F_q$ gives the best known shortest signature. The length of the signature is about 2 log q. But using bilinear pairing as a tool the signature length is approximately $\alpha$logq where $\alpha$= logq/logr and r is chosen in such a way that it is the largest prime divisor of the total number points on the elliptic curve.

The rest of this paper is as follows: In section 2, some basic preliminaries of our scheme are discussed. In section 3, a new short signature scheme inspired by Neetu et al.[5] is proposed from weil pairing and in section 4, security analysis of the proposed scheme is done. In section 5, the efficiency of our scheme is given. Finally, we conclude our work in section 6.

## 2. PRELIMINARIES
In this section, some mathematical concepts are introduced related to the proposed scheme.

### 2.1 Elliptic curve
The elliptic curve over field K=$F_q$ where $q$ is a power of some prime number and $q$ >3 is the set of all pairs (x, y) ∈ $F_q$ which fulfils

$$y^2 \equiv x^3 + ax + b \quad (1)$$

together with an imaginary point at infinity $O$, where $a, b \in F_q$ and with the condition

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

The set of points satisfying the equation 1 forms a group.

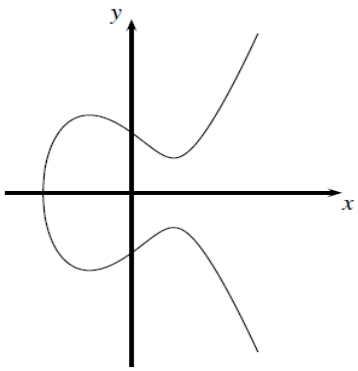


**Fig. 1. An Elliptic Curve**

#### *2.1.1 EC operations*
There are two basic Elliptic Curve operations: point addition and point doubling.

1) ***Point Addition*:** Let P and Q be two points on the elliptic curve with affine coordinates P=($x_1$, $y_1$) and Q=($x_2$, $y_2$). Point Addition refers to the addition of two points on the curve resulting in a third point. R=P+Q with R=($x_3$, $y_3$). Graphically, to get a point R on the curve, a line is drawn through P and Q and the third point of intersection on the curve is mirrored.

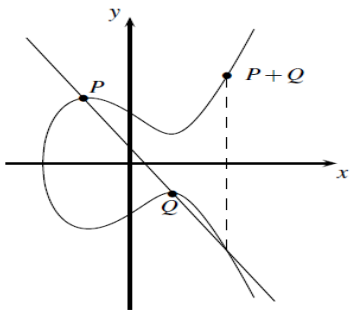


**Fig.2. ECC point addition**

However, the coordinates of the point resulting as a sum of two points can be calculated using the algorithm 1 [6][7][8].

**Algorithm 1. Point Addition**

*Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ be two different points on a curve.*

*If either points is O then the result is the other point.*

*If P=Q, use the double algorithm.*

*If $x_1 = x_2$ and $y_1 \neq y_2$, $P + Q = O$.*

*If $P \neq Q$ then $P + Q = R(x_3, y_3)$, where*

$\lambda = (y_1 + y_2)/(x_1 + x_2)$

$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$

$y_3 = \lambda(x_1 + x_3) + x_3 + y1$

2) ***Point Doubling*:** Point doubling is a ECC operation where a point P is added to itself. Graphically a tangent is drawn through the point and the intersection of the tangent on the curve is mirrored to get the result.

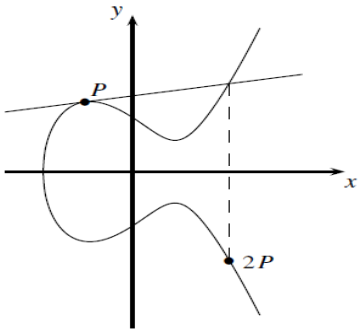


**Fig. 3 Point Doubling**

The coordinates of R=2P can be found using the algorithm 2 [6][7][8].

**Algorithm 2. Point Doubling**

*Let $P(x_1, y_1)$ be a point on the curve.*

*If $x_1=0$, then the result of 2P is O.*

*If $x_1 \neq 0$, $2(x_1, y_1) = R(x_3, y_3)$, where*

$x_3 = \lambda^2 + \lambda + a$

$y_3 = x_1^2 + (\lambda+1)x_3$

$\lambda = x_1 + y_1/x_1$

## 2.2 Weil pairing

Let $n \geq 1$ be an integer. A point $P \in E$ satisfying $nP = O$ (point at infinity) is called a point of order $n$ on the elliptic curve group E. The set of points of order $n$ formed a subgroup of E is denoted by

$$E[n]=\{P \in E;\ nP = O\}$$

Let $n \geq 1$ be an integer. Let E be an elliptic curve over the finite field K. Then there are $n^2$ points in the mentioned subgroup.

$$E(K)[n] \equiv Z_n \times Z_n$$

If $K=F_q$ and assume that p does not divide n then there exists a value k such that

$$E(Fp^{jk})[n] \equiv Z_n \times Z_n \text{ for all } j \geq 1$$

The proof of the above equation is given in [9] Corollary III6.4.

According to the above equation, if it is allowed the points with coordinates in $Fp^{jk}$ field, then $E[n]$ looks like a 2-dimensional vector space over the field $Z_n$. Let's choose basis $P1, P2 \in E[n]$. Then every point $P \in E[n]$ can be expressed in terms of the basis points as $P = aP1 + bP2$ for unique choice of $a, b \in Z_n$ . But it is more difficult to express a point in terms of the basis points $P_1, P_2$ than solving ECDLP problem.

Weil pairing is a map $e_n$: $E[n] \times E[n] \rightarrow G$ , where G is a multiplicative group. The $e_n$ takes as input a pair of points from $E[n]$ and gives as output an $n^{th}$ root of unity in the multiplicative group. The weil pairing used in our proposed scheme is alternating because we do not use any distortion map [6] which is a map $\emptyset$: E→E to get independent curve points from linearly dependent curve points.

The weil pairing has many useful properties:

a) Bilinearity

$e_n(aP, bQ) = e_n(P, Q)^{ab}$ where $P, Q \in E[n]$ and $a, b \in Z_n$

b) The Weil pairing is alternating, which means

$$e_n(P, P) = 1 \text{ for all } P \in E[n].$$

c) The Weil pairing is non degenerate, which means

$$\text{if } e_n(P, Q) = 1 \text{ for all } Q \in E[n] \text{ then } P = O.$$

# 3. THE PROPOSED SCHEME

Actually, our proposed scheme is a variant of the Neetu et al. [5] from weil pairing with alternating property. Just like other signature scheme, it consists of the system initialization phase, the key generation phase, the signature generation phase and the signature verification phase.

## 3.1. System initialization Phase

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

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

b) Two co-efficient parameters $a, b \in F_q$ that define the equation (1) in section 2 of elliptic curve $E$ over $F_q$

c) A large prime number $n$, and basis points $P_1$,$P_2 \in E[n]$

d) The Weil pairing $e_n$: $[n] \times E[n] \rightarrow G$ , where $G$ is a multiplicative group.

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

## 3.2 Key generation

a) The signer computes secret and public key pair using two basis points $P_1$,$P_2 \in E[n]$.

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

c) The corresponding public key is computed as $P = aP_1 + bP_2$ where $P_1, P_2 \in E[n]$ be two basis points.

## 3.3 Signing

For signing a message $m$, in this proposed scheme, it is sufficient to use one secret key value. The originan signer needs to perform the following operations to get the signature $S$.

a) Calculate the hash function over the message $m$ and the value $P$ and get hashed integer value $h$=H$(m, P)$.

b) Calculate $S = a^{-1}hP_2$

After signature calculation, the signer sends the signature $S$ and message $m$ to the verifier.

## 3.4 Verification phase

For verifying the correctness the signature $S$ with respect to the massage $m$, the verifier has to perform the following operations:

a) Calculation of the hashed integer value

$$h = \mathrm{H}(m, P)$$

b) Checking whether the following equation holds

$$e_n(h^{-1}P, S) = e_n(P_1, P_2)$$

If the equation holds, then verifier accepts the signature $S$, otherwise rejects.

## 3.5 Correctness

$$e_n(h^{-1}P, S) = e_n(P, S)^{h^{-1}}$$

$$= e_n(aP_1 + bP_2, S)^{h^{-1}}$$

$$= e_n(aP_1 + bP_2, a^{-1}hP_2)^{h^{-1}}$$

$$= e_n(aP_1, a^{-1}hP_2)^{h^{-1}} e_n(bP_2, a^{-1}hP_2)^{h^{-1}}$$

$$= e_n(aP_1, a^{-1}hP_2)^{h^{-1}}$$

$$= e_n(P_1, P_2)^{ah^{-1}a^{-1}h}$$

$$= e_n(P_1, P_2)$$

# 4. SECURITY ANALYSIS

The security of the scheme is based on the difficulty of expressing a point $P \in E[n]$ in term of linear combination of basis points as

$$P = aP1 + bP2$$

where $P_1, P_2 \in E[n]$ and $a \neq 0$ and $b \neq 0$.

But it is more complicated than solving ECDLP problem. If $a = 0$, then $P = bP_2$ and if $b = 0$ then $P = aP_1$ which just like solving an ECDLP problem. To avoid that situation the values of $a$ and $b$ are chosen from the interval $[1,2 \ldots . n-1]$ as secret keys.

**Attack I.** The signature $S$ is just a point on the on the elliptic curve. To get the value of the private key $a$ from the known signature $S$ of a message $m$, the Adv has to solve ECDLP [6] problem which is a hard problem.

**AttackII**. Adv wishes to find out the secret key value $a$ from the known information of the system. So, Adv needs to solve the equation $P = aP_1 + bP_2$. Finding the value of the secret keys from this equation is completely infeasible problem because it is more difficult than solving ECDLP [6] problem.

# 5. EFFICIENCY

The various notations for time complexity of the operations are given in the table 1. The efficiency comparison of our enhanced proposed scheme with the scheme BLS [1],ZSS[3] and Sedat Akleylek et al. [4] and Neetu et al. [5] is shown in table 2. It is clear that, the signature verification process of the proposed scheme is constructed with lesser number of cost effective pairing operations. So the scheme presented in this paper is efficient.

**Table 1. Time complexity of various operations**

| Notation | Description |
|---|---|
| $\tau_{bp}$ | *Execution of a bilinear pairing* |
| $\tau_{inv}$ | *Execution of an inversion* |
| $\tau_h$ | *Execution of a hash function* |
| $\tau_{mul}$ | *Execution of a modular multiplication* |
| $\tau_{exp}$ | *Execution of an exponentiation* |
| $\tau_{add}$ | *Execution of an addition* |
| $\tau_{squ}$ | *Execution of a square* |
| $\tau_{mtp}$ | *Execution of map to point hash function* |
| $\tau_{ec-mul}$ | *Execution of an elliptic curve multiplication* |
| $\tau_{sm}$ | *Execution of scalar multiple scalar multiplication* |
| $\tau_{ec-add}$ | *Execution of a elliptic curve point addition* |

**Table 2. Comparison of efficiency**

| | BLS[ 1] | ZSS[ 3] | Sedat Akley lek et al[ 4] | Neetu et al.[5] | Proposed scheme |
|---|---|---|---|---|---|
| Key generation | $1\tau_{ec-r}$ | $1\tau_{ec-mul}$ | $2\tau_{ec-mul}$ | $1\tau_{sm}$ | $1\tau_{sm}$ |

| | BLS[ 1] | ZSS[ 3] | Sedat Akley lek et al[ 4] | Neetu et al.[5] | Proposed scheme |
|---|---|---|---|---|---|
| Signing | $1\tau_{mtp}$ + $1\tau_h$ | $1\tau_{ec-mul}$ + $1\tau_{inv}$+ $1\tau_h$ | $1\tau_{ec-mul}$ + $1\tau_{inv}$+ $1\tau_h$+ $1\tau_{squ}$ | $1\tau_{mul}$ + $1\tau_h$ + $1\tau_{inv}$ + $1\tau_{add}$ | $1\tau_{ec-mul}$ $1\tau_h$+ $1\tau_{mul}$ $+1\tau_{inv}$ |
| Verification | $2\tau_{bp}$ + $1\tau_{mtp}$ | $1\tau_{ec-mul}$ + $1\tau_{bp}$+ $1\tau_h$ | $1\tau_{ec-mul}$ + $2\tau_{bp}$+ $1\tau_h$+ $1\tau_{squ}$+ $1\tau_{ec-add}$ | $2\tau_{exp}$ + $2\tau_{bp}$+ $1\tau_h$ | $1\tau_{inv}$+ $1\tau_{bp}$+ $1\tau_h$ |

## 6. CONCLUSION

The scheme presented in this paper is based on weil pairing which is alternating as the distortion map is not used. Actually, the distortion map makes curve points independent from linearly dependent curve points. The security of the scheme depends on the solving ECDLP problem. The proposed scheme does not require any special kind of hash function such as map-to-point hash function. The hash function used in our proposed scheme is a general cryptographic hash function. More important, our proposed scheme is efficient as compared to other existing schemes as it takes a lower number of pairing operations.

## 7. REFERENCES

[1] Boneh, Dan, Ben Lynn, and Hovav Shacham. "Short signatures from the Weil pairing." *Advances in Cryptology—ASIACRYPT 2001*. Springer Berlin Heidelberg, 2001. 514-532.

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

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

[5] Sharma Neetu, and Birendra Kumar Sharma. "New Short Signature Scheme with Weil Pairing." *International Journal of Computer Applications* 94.10 (2014): 25-28..

[6] Hoffstein, Jeffrey, et al. *An introduction to mathematical cryptography*. New York: Springer, 2008.

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

[8] Washington, Lawrence C. Elliptic curves: number theory and cryptography. CRC press, 2008.

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