Volume: 05, Issue: 02, Pages:1893-1897 (2013) ISSN : 0975-0290

ID-Based Signature Scheme with Weil Pairing

Neetu Sharma
School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.) 492010 India
Email: neetusharma524@gmail.com
Hemlal Sahu
School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.) 492010 India
Email: hemlalsahu@gmail.com
Birendra Kumar Sharma
School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur (C.G.) 492010 India
Email: sharmabk07@gmail.com

ABSTRACT

Digital signature is an essential component in cryptography. Digital signaturesguarantee end-to-end message integrity and authentication information about the origin of a message. In this paper we propose a new identification based digital 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 identification based digital signature scheme is more secure and efficient than the existing scheme of Islam et al(S. K. Hafizul Islam, G.P. Biswas, An Efficient and Provably-secure Digital signature Scheme based on Elliptic Curve Bilinear Pairings, Theoretical and Applied Informatics ISSN 18965334 Vol.24, no. 2, 2012, pp. 109-118) based on bilinear pairing.

Keywords –Cryptography, Digital signature scheme, Identification scheme, Elliptic curve cryptosystem, Chosen message attack.

Date of Submission: August 07, 2013 Date of Acceptance: September 27, 2013

I. INTRODUCTION

Digital signature schemes have found numerous practical applications such as electronic mail, office automation, and electronic funds transfer. Digital signatures is being increasingly demanded to ensure the integrity and authenticity of digital messages and documents. A secure digital signature scheme can be constructed using an interactive identification scheme and a hash function. When the identification scheme is converted to a signature scheme, the verifier's role is replaced by the hash function. A digital signature scheme resulting from the above paradigm has equal complexity as identification scheme. Public-key identification schemes prevent online systems or electronic cash from unauthorized access and unauthorized transfer. In 1984, Shamir[1] introduced the concept of ID-based cryptosystem. In 1987, Fiat-Shamir[2] introduced the method of transforming identification schemes into signature schemes, and is thus very popular.

In 1988, Shao[3] proposed a digital signature scheme based on IFP(Integer Factorization Problem) and DLP(Discrete Logarithm Problem). In 1988,Li and Xiao[4] presented a simple attack and proved that Shao's scheme is insecure. In 1994, Harn[5] developed a new signature scheme based on two different cryptographic assumptions IFP and DLP, however, the scheme is not secure as demonstrated by Hwang[6] in 1996. In 2000, Nyang and Song [7], proposed an efficient digitalsignature scheme using a zero-knowledge based identification (ZKI) scheme and hash function. The ECC(Elliptic curve cryptography) was initated by Koblitz[8]and Miller[9], where the security was established on the discrete logarithm problem over the points on an elliptic curve, called ECDLP. In 2004, Tzeng and Hwang[10] proposed digital signature with message recovery and its variants based on ECDLP. In 2007, Chung et al.[11] proposed another ZKI-based signature scheme using ECC, however, the scheme is not secure as demonstrated by Yang and Chang[12]. In 2013, Ismail et al.[13] modified the scheme of Chung et al.[11].

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. In 2010, Islam et al.[14] proposed secure digital signature scheme based on elliptic curve bilinear pairing whose security is based on ECDLP. In this paper, we propose a new identification based digital 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 ID-based signature scheme from 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.

Volume: 05, Issue: 02, Pages:1893-1897 (2013) ISSN : 0975-0290

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 addingoperation 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

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \text{ if } P_1 \neq P_2$$
$$= \frac{3x_1^2 + a}{3y_1}, \text{ if } P_1 = P_2 \text{ (doubling)}$$

Definition 2.2.Torsion Points and Basis Points
Let $m \geq 1$ be an integer. A point $P \epsilon E$satisfying $mP = O$(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.

Proposition 2.1. Let $m \geq 1$ be an integer

(1) Let E be an elliptic curve over Ror C. 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 [15], 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's choose basis P_1, P_2 in $E[m]$. 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, bin Z/mZ. Expressing a point in terms of the basis points P_1, P_2 is more complicated than solving ECDLP [16].

Definition2.3.Weil pairing [15]:- 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 by e_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 nondegenerate, which means that if $e_m(P, Q) = 1$ for all $Q \in E[m]$then $P = O$.

3. A NEW DIGITAL SIGNATURE SCHEME

Using a one-way hash function, the identification scheme developed by Popescu [17], based on zero-knowledge protocol, can be transformed into a digital multi-signature scheme. A one-way hash function is designed herein with two characteristics: the output is of a fixed length, unlike the input, which is of variable length; also the length of the signed message can be reduced by applying the hash function, so that the chosen-message attack, as defined by E1Gamal [18] and Harn [5], can be resisted. 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 ($y^2 = x^3 + ax + b(modq)$ in the case $q > 3$, where $4a^3 + 27b^2 \neq 0(modq)$).
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.
f) A positive integer t, which is the secure parameter, say $t \geq 72$[7].

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 $y = ha - bmodn, \sigma = e_m(P_1,\ P_2)^y$and sends$(\sigma, h, y)$ 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
$$g = e_m(P, P_2)^h e_m(P, P_1)$$
b) Checks whether the equation $g = \sigma$ holds. If so, the verifier accepts thesignature(σ, h, y); otherwise rejects it.

3.5. Correctness of scheme:-

Theorem 3.1. The equation $g = \sigma$ is correct.
Proof :-

$$\begin{aligned} g &= e_m(P, P_2)^h e_m(P, P_1) \\ &= e_m(aP_1 + bP_2, P_2)^h e_m(aP_1 + bP_2, P_1) \\ &= e_m(aP_1, P_2)^h e_m(bP_2, P_1) \\ &= e_m(P_1, P_2)^{ha} e_m(P_2, P_1)^b \\ &= e_m(P_1, P_2)^{ha} e_m(P_1, P_2)^{-b} \\ &= e_m(P_1, P_2)^{ha-b} \\ &= e_m(P_1, P_2)^y \\ &= \sigma \end{aligned}$$

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.

Lemma 4.1. 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$P$, 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

$$m_1 = k * n_1 mod(order P_1)$$
$$m_2 = k * n_2 mod(order P_2)$$

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 Advcannot 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 $(\sigma, h, y)$for message$m$. To forge a valid signature for a message m, the Adv needs to solve $= e_m(P_1,\ P_2)^y,\ h = H\ (m, P\ )$, 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, modularweil pairing operation, modular inverse operation, 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 Islam et al's [14]and Ismail et al's [13]scheme.

Table 1. 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

Volume: 05, Issue: 02, Pages:1893-1897 (2013) ISSN : 0975-0290

	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.

Table 2:- Comparison of efficiency

	Key generation	Signature generation	Signature verification
Ismail's scheme [13]	$1T_{EC-MUL}$	$1T_{EC-MUL}$+ 1 _ + 1 +1	2 _ + 2 _ + 1
Islam et.al's scheme [14]	1 _	2 _ + 1 + 1 + 1	1 _ +1 + 1
Our's scheme	1	1 + 1 + 1 +1	2 + 1 + 1

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.

REFERENCES

[1] A. Shamir, Identity-Based cryptosystems and signature schemes. Vol. 196 of Lecture Notes in Computer Science, Springer 1984, pp. 47-53.

[2] A. Fiat, A. Shamir, How to prove yourself: practical solutions to identification and signature problems, Advances in CryptologyProceedings of Crypto '86, LNCS, vol. 263, Springer, 1987, pp. 186-194.

[3] Z. Shao: Signature schemes, based on factoring and discrete logarithms, IEE Proceedings of the Computers and Digital Techniques, 145 (l), 1988, pp. 33-36.

[4] J. Li, X. Xiao: Remarks on new signature scheme based on two hard problems, IEE Proceedings of the Computers and Digital Techniques, 34 (25), 1988, pp. 2401.

[5] L. Harn: Public-key cryptosystem design based on factoring and discrete logarithms, IEE Proceedings of the Computers and Digital Techniques, 141(3), 1994, pp. 193-195.

[6] N-Y. Lee, T. Hwang: Modified Harn signature scheme based on factorizing and discrete logarithms, IEE Proceedings of the Computers and Digital Techniques, 143 (3), 1996.

[7] D. H. Nyang, J. S. Song. Knowledge-proof based versatile smart card verification protocol,ACM SIGCOMM Computer Communication Review 30(3), 2000, pp. 39-44.

[8] N. Koblizt, Elliptic curve cryptosystem, Mathematics of Computation 48(177), 1987, pp. 203-209.

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

[10] S. F. Tzeng, M. S. Hwang, Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem, Comput. Standards and Interfaces 26(2), 2004, pp. 61-71.

[11] Yu Fang Chung, KuoHsuan Huang, Feipei Lai, TzerShyong Chen, ID-based digital signature scheme on the elliptic curve cryptosystem, Computer Standards and Interfaces 29, 2007, pp. 601-604.

[12] J.H. Yang, C.C. Chang: Cryptanalysis of ID-based digital signature scheme on elliptic curve cryptosystem, In: Proceedings of the International Conference on Intelligent Systems Design and Applications (ISDA08), 2008, pp. 3-5.

[13] E. S. Ismail, W. S. Wan-Daud, , ID-based digital signature scheme using elliptic curve cryptosystem, Applied Mathematical Sciences, Vol. 7, no. 73, 2013, 3615 - 3624.

[14] S. K. Hafizul Islam, G.P. Biswas, An Efficient and Provably-secure Digital signature Scheme based on Elliptic Curve Bilinear Pairings, Theoretical and Applied Informatics ISSN 18965334 Vol.24, no. 2, 2012, pp. 109-118.

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

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

[17] C. Popescu, An identification scheme based on the elliptic curve discrete logarithm problem, The 4th International Conference on High-Performance Computing in the Asia-Pacific Region, vol. 2, 2000, pp. 624-625.

[18] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transaction on Information Theory, IT-31(4), 1985, 469-472.

Authors Biography

Neetu Sharma received M.Sc and M.Phil degree in mathematics from Pandit Ravishankar Shukla University Raipur, Chhattisgarh (India) in 2010 and 2012. She is doing research in Bilinear Pairing within the domain of cryptography for Ph.D degree in S.o.S in mathematics, ofPandit Ravishankar Shukla University Raipur, Chhattisgarh (India).

HemlalSahu holdsdegree of B.Sc and M.Sc in Mathematics from Pandit Ravishankar Shukla University Raipur,Chhattisgarh (India). He iscurrently an Assistant Professor in mathematics at Govt. P.G. College Dantewada Chhattisgarh. His scientific interests lie in the fields of elliptic curve based asymmetric key cryptosystems.

*Birendra Kumar Sharma*Professor, School of Studies in Mathematics, Pandit Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical Society and the Ramanujan Mathematical Society.