A New Zero Knowledge Identification Scheme based on Weil Pairing

B. K. Sharma
School of Studies in Mathematics
Pt. Ravishankar Shukla University
Raipur (C.G.) 492010 India

Hemlal Sahu
School of Studies in Mathematics
Pt. Ravishankar Shukla University
Raipur (C. G.) 492010 India

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

ABSTRACT
Many identification schemes have been proposed in which security are based on the intractability of factoring or DLP (Discrete Logarithm Problem). In 2009, Massoud et.al gave identification scheme whose security was based on solving ECDLP (Elliptic Curve Discrete Logarithm Problem). The security of this scheme is improved in order to propose a more secure and efficient scheme. The security of proposed scheme is based on expressing torsion point of elliptic curve into linear combination of basis points. This is more complicated than solving ECDLP and thus provides a higher level of security. Also proposed scheme is more efficient with respect to encryption and decryption since it requires only minimal operations in both algorithms.

Keywords
Identification, Elliptic Curve, Weil Pairing, Challenge-Response, Zero-Knowledge Proof.

1. INTRODUCTION
Zero-knowledge proof was introduced by Goldwasser, Micali, and Rackoff in 1985 [5]. It plays important role in cryptography. Zero knowledge proof can be used for identification. In an identification protocol, the prover(Alice), proves to the verifier (Bob), that she is really Alice who is communicating to Bob. Alice introduces herself to Bob in a challenge-response system. Fiat-Shamir protocol [3] is the first practical zero knowledge protocol with cryptographic application and was based on difficulty of factoring. A more common variation of the above scheme was the Fiege-Fiat-Shamir [4] zero knowledge proofs of identity. Guillou and Quisquater [8] further improved Fiat and Shamir's protocol in terms of memory requirements and interaction. Schnorr identification protocol is an alternative to the Fiat - Shamir and Guillou and Quisquater protocols. Its security was based on the intractability of the DLP. Public-key systems are based on either the discrete logarithm problem or the integer factoring problem. The modular exponent operation is time consuming in these protocols. To reduce such computation cost, the elliptic curve cryptography becomes a best choice, because it reduces the computational cost at the same security level. In 2009, Massoud Hadian et.al.[9] introduced identification scheme. The security of their scheme was based on solving ECDLP. The security of [9] is modified in proposed paper to gain more security and enhanced efficiency. This paper is organized into five sections. The next section briefly introduces some mathematical backgrounds. In the section 3, a new scheme is proposed. In the section 4 and 5, the security and efficiency of the new scheme is analyzed. Last section is conclusion.

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

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

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

Definition 2.2.Torsion Points
Let $m \geq 1$ be an integer. A point $P \in E$ 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.
(1) Let $m \geq 1$ be an integer. Let E be an elliptic curve over R or 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

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

Proof. For the proof of proposition refer [12], 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, b in Z/mZ. Expressing a point in terms of the basis points P_1, P_2 is more complicated than solving ECDLP.

Definition2.3.Weil pairing

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 as below

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 $P = O$.
For detail refer [6].

Now a Zero Knowledge Identification Scheme is proposed whose security depends upon expressing a point of elliptic curve in terms of the basis points.

3. PROPOSED SCHEME

The implementation of the proposed new Zero Knowledge Identification Scheme involves the system initialization, commitment, challenge, response and verification phases as below

3.1. System Initialization Phase

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

a) A field size q, 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 $a, b \in F_q$ 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) Security parameter t, where $2^t < m$.

3.2. Scheme.

a) Commitment: Alice selects randomly two numbers a and b from $[1\ to\ m-1]$ and calculate $P = aP_1 + bP_2$. She then sends P to the verifier Bob.
b) Challenge: Bob chooses a random number $d \in \{1, 2, \ldots\ldots, 2^t\}$ and sends it to Alice.
c) Response: Alice computes $y = da - b$ and sends it back to Bob.
d) Verification: Bob accepts Alice's identity if and only if
$$e_m(P_1, yP_2) = e_m(P, P_1)e_m(P, P_2)^d$$
The correctness of the scheme is shown as below.

Lemma 3.1. The scheme has completeness property.

Proof. $e_m(P, P_1)e_m(P, P_2)^d$

$$\begin{aligned} &= e_m(aP_1 + bP_2, P_1)\ e_m(aP_1 + bP_2, P_2)^d \\ &= e_m(bP_2, P_1)e_m(aP_1, P_2)^d \\ &= e_m(P_2, P_1)^b e_m(P_1, P_2)^{ad} \\ &= e_m(P_1, P_2)^{-b} e_m(P_1, P_2)^{ad} \\ &= e_m(P_1, P_2)^{ad-b} \\ &= e_m(P_1, P_2)^y = e_m(P_1, yP_2) \end{aligned}$$

Lemma 3.2. The scheme has soundness property.

Proof. We assume that eavesdropper can compute values d_1, d_2, y_1, y_2 such that

$$e_m(P_1, P_2)^{y_1} = e_m(P, P_1)e_m(P, P_2)^{d_1}$$
$$e_m(P_1, P_2)^{y_2} = e_m(P, P_1)e_m(P, P_2)^{d_2}$$

It follows that

$$e_m(P_1, P_2)^{y_1 - y_2} = e_m(P, P_2)^{d_1 - d_2}$$

$$= (aP_1 + bP_2, P_2)^{d_1 - d_2}$$

$$= e_m(P_1, P_2)^{a(d_1 - d_2)}$$

Since $e_m(P_1, P_2)$ has order m therefore

$$y_1 - y_2 = a(d_1 - d_2)\ mod\ m$$

If gcd $((d_1 - d_2), m) = 1$ then eavesdropper can compute private key a as follows

$$a = (y_1 - y_2)(d_1 - d_2)^{-1} mod\ (m)$$

Otherwise $gcd(d_1 - d_2), m) = h$ then

$$\gcd\left(\frac{d_1 - d_2}{h}, \frac{m}{h}\right) = 1$$

4. SECURITY ANALYSIS

Lemma 4.1. If one can express a point of elliptic curve into linear combination of basis points then he can easily solve ECDLP. But converse is not true.

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 for given P and Q, we write $P = n_1P_1 + n_2P_2$ and $Q = m_1P_1 + m_2P_2$. Since P_1 and P_2 are independent, and if $Q = kP$, then

$$m_1 = kn_1\ mod(order P_1)$$

$$m_2 = kn_2 \, mod(orderP_2)$$

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

Conversely, suppose Oscar (eavesdropper) is able to solve ECDLP. Since P_1 and P_2 are independent. So P can not be expressed as scalar multiple of P_1 as well as P_2. Hence he cannot use ECDLP to find the values of a and b from $P = aP_1 + bP_2$.

Lemma 4.2. The private key for prover could be revealed by verifier if in the commitment stage a is a constant.

Proof. To obtain Alice's private key, Bob could compute the difference of two integers y_1, y_2 which are corresponding to k and $k+1$ respectively (d and $d+1$ selected in challenge stage by Bob). Now Bob computes

$$y_2 - y_1 = da - b + a - (da - b) = a.$$

Therefore he obtains the value a (Alice's private key) thus the zero knowledge proof property of our protocol will be vanished.

Lemma 4.3. In the scheme if the cheater (Oscar) guess the correct value of challenge (d), then Oscar cannot introduce himself as the prover (Alice) to the verifier (Bob).

Proof. Since Oscar could guess the correct value of d to impersonate Alice, he should compute value y of

$$A^y = e_m(P_1, yP_2) = e_m(P, P_1)e_m(P, P_2)^d = B$$

Where $A^y = B$ is DLP in G.

5. EFFICIENCY

Table 1 defines our notation The time complexity of the proposed protocol and some other protocol in terms of modular multiplication operation, Weil 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 Massoud Hadian et.al. [9] Zero Knowledge Identification Scheme.

Table 1. Time complexity of various operations

Notation	Definition
TG_e	Time complexity for execution of a bilinear pairing.
T_{EC-MUL}	Time complexity for execution of an elliptic curve multiplication.
T_{SM}	Time complexity for execution of a scalar multiple scalar multiplication.
T_{EXP}	Time complexity for execution of a exponentiation.
T_{MUL}	Time complexity for execution of a modular multiplication.
T_{EC-ADD}	Time complexity for execution of an elliptic curve addition.
T_{ADD}	Time complexity for execution of an addition.

Table 2:- Comparison of efficiency

Phases	Massoud Hadian's scheme[9]	Our scheme
Key generation	$1T_{EC-MUL}$	$0T_{EC-MUL}$
Commitment	$1T_{EC-MUL}$	$1T_{SM}$
Response	$1T_{MUL}$	$1T_{MUL}$
Verification	$1T_{EX} + 1T_{EC-MUL} + 3TG_e$	$1T_{EX} + 1T_{EC-MUL} + 3TG_e$

6. CONCLUSION

The security of our scheme depends on expressing a torsion point of elliptic curve into linear combination of basis points which is more complicated than solving ECDLP. Thus our scheme has a higher level of security. It is more efficient since it requires only minimal operations in both algorithms.

7. REFERENCES

[1] Diffie W., Hellman M., 1976. New directions in cryptography. IEEE trans .Inf. Theory, 22(6), 644-654.

[2] E1Gamal T., 1985.A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory, IT-31(4): 469-472.

[3] Fiat A., Shamir A., 1986. How to prove yourself: practical solutions to identification and signature problems. proceedings of crypto 86, Santa Barbara 181-187.

[4] Fiege, U., Fiat, A., Shamir, A., 1987. Zero knowledge proofs of identity. Proc. of STOC.

[5] Goldwasser,S., Micali, S., and Rackoff, C., 1989.The Knowledge Complexity of Interactive Proofs Systems. SIAM Journal on Computing, Vol. 18, pages 186-208, 1989.Preliminary version in 17th ACM Symposium on the theory of computing, 1985.Earlier version date to 1982.

[6] Hoffstein, J.,Pipher, J., Silverman, J. H., An Introduction to mathematical Cryptography. Springer.

[7] Koblitz, N., 1987, Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.

[8] Guillou, L.C.,Quisquater, J. J., 1988.A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. Advances in Cryptology EUROCRYPT 88 Lecture Notes in Computer Science Volume 330, pp 123-128.

[9] Massoud, H. D., and Reza, A., 2007. Zero-Knowledge Identification Scheme Based on Weil Pairing. ISSN 1995-0802, Lobachevskii Journal of Mathematics, Vol. 30, No. 3, pp. 203-207.

[10] Miller, V. S., 1986. Uses of elliptic curves in cryptography. in: Advances in Cryptology- Crypto'85, Lecture Notes in Computer Science, 218, Springer-Verlag, Berlin, pp. 417-426.

[11] Rivest, R.L., Shamir, A., Adleman, L., 1978. A method for obtaining digital signatures and public key cryptosystems. Communication of the ACM, 21,120-126.

[12] Silverman, J. H., 1986. The Arithmetic of elliptic curves. Volume 106 of Graduate Texts in Mathematics, Springer-Verlag New York.