ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An efficient authentication protocol using zero knowledge property and pairing on elliptic curves

Manoj Kumar
Department of Mathematics and Statistics,
Gurukul Kangri Vishwavidyalaya,
Haridwar (Uttrakhand) 249404, India

***Abstract*:** The systematic introduction to zero knowledge proof protocol has important theoretical guidance and practical significance on attracting more scholars involved in research as well as expanding application fields. Zero-knowledge proofs were first conceived in 1985 by Shafi Golwasser, Silvio Micalli and Charles Rackoff in a draft of the knowledge complexity of interactive proof systems. The goal of the present paper is to introduce a new identity based scheme which is a combination of zero-knowledge interactive proof and weil pairing on elliptic curves. The concept of weil pairing was first introduced by Andre Weil in 1940. It plays an important role in the theoretical study of the arithmetic of elliptic curves and Abelian varieties. It has also recently become extremely useful in cryptologic constructions related to these objects

2010 Mathematical Subject Classification: Primary 94A55, Secondary 11T71, 68P25.

***Keywords* and phrases:** Elliptic Curves, Identification, Zero Knowledge Proofs, Weil Pairing.

I. INTRODUCTION

Efficient and secure public-key cryptosystems are essential in today's age of rapidly growing Internet communications. Elliptic curve scalar multiplication in particular, which refers to the operation of multiplying a large integer by a point on an elliptic curve, is crucial for both data encryption technology as well as testing the security of cryptographic systems. An identification protocol (also known as authentication scheme) is an interactive protocol between a prover and a verifier by which a prover may prove his/her identity to a verifier without revealing essential knowledge. An identification scheme enables a prover holding a secret key to identify itself to a verifier holding the corresponding public key. The primary objectives of an identification protocol are completeness, in the case of honest parties the prover is successfully able to authenticate itself to the verifier, and soundness- a dishonest prover has a negligible probability of convincing a verifier. Identity based protocol is a new development of public key cryptography. Nowadays identity based cryptography has become a very active field of research. The concept of identity based protocol was first proposed by Shamir [19]. Identity based schemes have been extensively studied for last three decades and a lot of literature exist on the topic [2, 3, 4, 5, 6, 10, 13, 14, 18, 19, 20].

Recent years have brought a host of identification schemes that make use of bilinear pairings [17] on elliptic curves. In the world of elliptic curve cryptography [1, 8, 11], the pairing was initially considered as negative property. This is because it reduces the discrete logarithm problem on some elliptic curves (e.g. super singular curves) to the discrete logarithm problem in a finite field, thus diminishing the strength and practicability of super singular curves in cryptography. Until a tripartite key agreement protocol proposed by Joux in ANTS 2000 [9], the pairing for the first time became beneficial and favorable to cryptographic research and applications. Later Boneh and Franklin [2] proposed an identity based encryption scheme based on the modified weil-pairing and gave thorough analysis about its properties, security and performance. In the present paper we proposed a new zero knowledge identification scheme based on weil pairing on an elliptic curve, and prove its security given certain computational assumptions. The whole paper is organized into six sections. Section first is introductory in nature. Section second consists of basic definitions and notations used in the paper. Section third presents the basic identification scheme which proposed. Section fourth analyzes the security facts of the scheme. In section five we compare the efficiency of our scheme with Massoud et al [14] scheme. Finally the last section ends with the conclusion and future work.

II.NOTATIONS AND BASIC DEFINITIONS

A. Zero-knowledge proofs: Zero-knowledge proofs were invented by Goldwasser, Micali and Rackoff in 1982[7]. Zero knowledge protocols are instances of an interactive

proof system, where claimant and verifier exchange messages (typically depending on random events). A zero knowledge protocol must satisfy the following properties [4]**:***i). Completeness:* If the statement is true, the verifier will be convinced of this fact by an honest prover.
*ii). Soundness***:** If the statement is false, no cheating prover can convince the verifier that it is true.
iii). Zero-knowledge: If the statement is true, no cheating verifier learns anything than this fact.

***B. Elliptic Curve Cryptography*:** The use of elliptic curve cryptography was initially suggested by Koblitz [12] and Miller [16]. For $n \geq 1$ and a prime p let F_q be a finite field with $q = p^n$ elements. An elliptic curve E over F_q can be given by the Weierstrass equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in F_q$, $i = 1,2,...,6$ together with the condition that curve has no singular points.

If $q \neq 2,3$ then an easier representation of elliptic curve E is given by

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

where $qa = 0 \forall\, a \in F_q$ and the discriminant $\Delta = 4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, q)$.

Thus an elliptic curve E is defined as the set of points (x, y) satisfying the equation (1) and including a point O called point at infinity.

The following properties hold on an elliptic curve E:

i). If $P(x, y)$ is a point on an elliptic curve E then inverse (reciprocal or opposite) point of P is $-P(x,-y)$.

ii). IF $P(x_1, y_1)$ and $Q(x_2, y_2)$ are two different points on the curve E, then their sum $R(x_3, y_3)$ is given by

$$x_3 = \lambda^2 - x_1 - x_2$$

and $y_3 = \lambda(x_1 - x_3) - y_1$,

where $\lambda = (y_1 - y_2)/(x_1 - x_2)$.

iii). If $P = Q$ then $R(x_3, y_3) = 2P$ is given by

$x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = (3x_1^2 + a)/2y_1$.

C. Torsion points of an elliptic curve E**:** As we know that every point on an elliptic curve E is one of two types (i) a point of finite order i.e. there exists a positive integer n such that $nP = O$ (ii) a point of infinite order i.e. there exist no such n. The points of first type are known as torsion points. Thus the set of torsion points P on an elliptic curve E denoted by $E[n]$ is defined as

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

It can be easily verified that $E[n]$ is a finite subgroup of E i.e. $(P_1 - P_2) \in E[n]$ for all $P_1, P_2 \in E[n]$.

***D.Weil Pairing[15*]:** Let n belongs to the set of positive integers N and G_n be a multiplicative group of nth roots of unity. Then weil pairing on an elliptic curve E over the field F_q, is family of maps

$$w_n : E[n] \times E[n] \rightarrow G_n$$

Having the following properties:

i)Bilinearity: If $P, Q, R \in E[n]$ then

$$w_n(P + Q, R) = w_n(P, R).w_n(Q, R)$$

and

$$w_n(P, Q + R) = w_n(P, Q).w_n(P, R)$$.

ii) Alternating: If $P \in E[n]$ then $w_n(P, P) = 1$.

Consequently using bilinearity we get $w_n(Q, P) = [w_n(P, Q)]^{-1}$ for all $P, Q \in E[n]$ which is known as skew-symmetry or anti-symmetry.

iii) Non-degeneracy: If $P \in E[n]$ with $P \neq O$ then there exists $Q \in E[n]$ such that $w_n(P, Q) \neq 1$.

iv)Compatibility: If $P \in E[nk]$ and $Q \in E[n]$ then $w_{nk}(P, Q) = w_n(kP, Q)$.

v) Galoic Invariance: If $P, Q \in E[n]$ and $k \in Gal(\overline{F_q} / F_q)$ then $w_n(P^k, Q^k) = [w_n(P, Q)]^k$.

Besides the above definitions we will also use the following notations:

- $\mathbf{T_{EC\text{-}MUL}}$**:**Time complexity for execution of an elliptic curve multiplication.
- $\mathbf{T_{EX}}$**:** Time complexity for execution of an exponentiation.
- $\mathbf{T_{MUL}}$**:** Time complexity for execution of a modular multiplication.
- $\mathbf{T_{SM}}$**:** Time complexity for execution of a scalar multiplication.
- $\mathbf{TG_w}$**:** Time complexity for execution of a bilinear pairing.

III. OUR SCHEME

The identification schemes based on classical cryptography use public key cryptosystems for establishing the common key. Some of them have been proven to be secure but they need high amount of resources and they require large keys for encryption / decryption. In this section we propose a

secure zero knowledge identification protocol based on torsion points of an elliptic curve. Applying this technique the memory and the power consumption are lower for the proposed protocol. Another advantage is that this kind of protocols are secure enough even if a small key size is used for encryption / decryption. The proposed protocol is based on expressing torsion points of an elliptic curve as the linear combinations of basis points.

1). Initial Setup: To implement the proposed protocol we have to make some assumptions first as:

i). To select field size q , we choose a prime number $p > 3$ such that $q = p$ if p is an odd prime otherwise $q = 2^k$ where $k \geq 2$.

It is obvious that $q > 3$.

ii) Choose two parameters a and b in F_q to define the Weierstrass equation of an elliptic curve E over F_q as

$$y^2 = (x^3 + ax + b)(\mathrm{mod}\, q)$$

iii) Select a very large prime n and two base points P and Q in $E[n]$.

iv) Define a multiplicative group G_n of n[th] roots of unity then a weil pairing is given by $w_n : E[n] \times E[n] \to G_n$.

v) Choose a security parameter s such that $2^s < n$.

2). Protocol Description: The different phases of proposed protocol are described below

i) Commitment: Prover selects two random numbers a and b between 1 and $(n-1)$, calculates $R = aP + bQ$ and sends R to the verifier.

ii) Challenge: Verifier selects a random number r from the set $\{1, 2, ..., 2^s\}$ and sends it to the prover.

iii) Response: Prover calculates $y = ra - b$ and sends it to the verifier.

iv) Verification: Verifier accepts prover's identity if and only if $w_n(P, yQ) = w_n(R, P).[w_n(R, Q)]^r$.

3) Verification of zero knowledge properties: The correctness of our scheme can be shown by proving the following zero knowledge properties namely completeness and soundness properties:

i) Completeness: We have

$$\begin{aligned} & w_n(R,P).[w_n(R,Q)]^r \\ &= w_n(aP+bQ,P).[w_n(aP+bQ,Q)]^r \\ &= w_n(aP,P).w_n(bQ,P) \\ &\quad \times [w_n(aP,Q)]^r.[w_n(bQ,Q)]^r \\ &\qquad \text{(using bilinearity property)} \\ &= w_n(bQ,P).[w_n(aP,Q)]^r \text{ (using alternating, compatibility and Galoic invar. property)} \\ &= [w_n(Q,P)]^b.[w_n(P,Q)]^{ar} \text{ (using compatibility and Galoic invariance property)} \\ &= [w_n(P,Q)]^{-b}.[w_n(P,Q)]^{ar} \\ &\qquad \text{(using antisymmetric property)} \\ &= [w_n(P,Q)]^{ar-b} \\ &= [w_n(P,Q)]^{y} \\ &= [w_n(P,yQ)] \end{aligned}$$

Thus completeness property holds in our proposed scheme.

ii) Soundness: By completeness property, for two integers y_1 and y_2 , we have

$$[w_n(P,Q)]^{y_1} = w_n(R,P).[w_n(R,Q)]^{r_1}$$

and $$[w_n(P,Q)]^{y_2} = w_n(R,P).[w_n(R,Q)]^{r_2}$$

Dividing above relations, we get

$$\begin{aligned} [w_n(P,Q)]^{y_1-y_2} &= [w_n(R,Q)]^{r_1-r_2} \\ &= [w_n(aP+bQ,Q)]^{r_1-r_2} \\ &= [w_n(P,Q)]^{a(r_1-r_2)} \end{aligned}$$

(using bilinearity, alternating, compatibiltyand Galoic Invariance property)

which implies that $y_1 - y_2 = a(r_1 - r_2)(\mathrm{mod}\, n)$.

If $(r_1 - r_2)$ and n are relatively prime then private key a can be computed as

$$a = (y_1 - y_2).(r_1 - r_2)^{-1}(\mathrm{mod}\, n)$$

If $(r_1 - r_2)$ and n are not relatively prime then $\gcd(r_1 - r_2, n) = k$ i.e. $\gcd\left(\frac{r_1 - r_2}{k}, \frac{n}{k}\right) = 1$.

IV. SECURITY OF THE SCHEME

In this section we shall prove the security of our proposed scheme. The security of our scheme is based on representing torsion point of an elliptic curve into linear combination of basis points. This is more complicated than solving elliptic curve discrete logarithm problem (ECDLP) and hence our protocol provides a higher level of security. We shall explain the security facts in three steps. First we shall show that if we are able to represent a point R on an elliptic curve E as $R = mP + nQ$ where P and Q are basis points of E and $m, n \in F_q$, then we can easily solve ECDLP. This is a one way implication result and its converse is not true. As we know that an ECDLP is said to be solvable for R on an elliptic curve E , whenever S is a multiple of R, we can always find a positive integer k such that $S = kR$. If S is any point on E then we can write S as a linear combination of basis points P and Q i.e. $S = m_1 P + n_1 Q$.

Since R is on E therefore we can write $R = m_2P + n_2Q$. But P and Q are independent and $S = kR$ therefore we get

$$m_1 = km_2 \bmod(orderP)$$

and $$n_1 = kn_2 \bmod(orderQ)$$

These two relations together with help us to find k modulo the order of R. Conversely suppose we are able to solve ECDLP. Solving our protocol means that for given basis points P, Q and a torsion point R on E, we are able to find two positive integers m and n such that $R = mP + nQ$. Since P and Q are independent therefore we cannot represent R as a scalar multiple P of as well as scalar multiple of Q.This implies that R cannot be represented as a linear combination of P and Q i.e. we are unable to find m and n such that $R = mP + nQ$. This proves the correctness of the above result. Second fact related to the security of our scheme is private key for prover could be revealed by the verifier if a is constant in the commitment phase. To find the prover's private key verifier could calculate the difference of integers y_1 and y_2 i.e. $y_1 - y_2 = ra - b + a(ra - b) = a$ .This implies that zero knowledge property of our scheme will be vanished in obtaining prover's private key by the verifier. The third fact about the security of our scheme is that even cheater guesses the accurate value of r in challenge phase, he/she cannot introduce himself/herself as prover to the verifier. Suppose cheater could guess the accurate value of r to impersonate prover, then he/she should compute the value of y from

$$X^y = w_n(P, yQ) = w_n(R, P).[w_n(R, Q)]^r = Y \quad ,$$

where $X^y = Y$ is called discrete logarithm problem (DLP). Thus our proposed protocol provides higher level of security.

V. COMPARISION

Most of the identification schemes have been proposed in which security are based on intractability of factoring or DLP. In this section we compare the efficiency of our protocol with Massoud [14] identification scheme whose security was based on solving ECDLP. The following table (5.1) comprises the efficiency of our scheme with Massoud et al scheme.

(Table 5.1)

Stages	**Our Scheme**	**Massoud et al Scheme**
Key generation	0 $T_{EC\text{-}MUL}$	1 $T_{EC\text{-}MUL}$
Commitment	1 T_{SM}	1 $T_{EC\text{-}MUL}$
Response	1 T_{MUL}	1 T_{MUL}
Verification	1 T_{EX} + 1$T_{EC\text{-}MUL}$ + 3TG_w	1 T_{EX} + 1$T_{EC\text{-}MUL}$ + 3TG_w

It is obvious from the above table that the security of our scheme is improved in order to propose a more secure and efficient scheme. As we have discussed earlier that the security of proposed protocol is based on representing torsion points on an elliptic curve as linear combinations of basis points. Since it is not easy to represent a torsion point as a linear combination of basis points of an elliptic curve, therefore to solve our scheme is more complicated than solving ECDLP. Further as clear from the table, our scheme is more efficient as it requires minimal operations in encryption/decryption algorithms.

VI. CONCLUSION AND FUTURE WORK

In the present paper we presented a relatively more secure and efficient protocol which is based on expressing torsion point on an elliptic curve as a linear combination of basis points. The protocol has low complexity because identification is made through zero knowledge property. Using the concept of weil pairing on elliptic curve it provides a methodology for obtaining high speed implementation of authentication protocol as it requires minimal operations in encryption/decryption algorithms. We believe that weil pairing based cryptography can still bring efficiency to many well known applications and we intend our future work to be driven by this idea.

REFERENCES

[1] Afreen R. and S.C. Mehrotra S. C., A review on elliptic curve cryptography for embedded systems, International Journal of Computer Science & Information Technology (IJCSIT), Vol. 3, No. 3, 84-103, 2011. doi : 10.5121/ijcsit.2011.3307 84

[2] Boneh D. and Franklin M., Identity-based Encryption from the weil-pairing, SIAM J. of Computing, Vol. 3, No. 3, 586-615, 2003.

[3] Cha J. C. and Cheon J. H., An identity based signature from gap Diffie-Hellman groups, in Proceedings of International workshop on Practice and teory in Public Key Cryptography-PKC, Springer-verlag, 18-30, 2003.

[4] Constantinescu N., Authentication protocol based on elliptic curve cryptography, Anals of the University of Craiova, Mathematics and Computer Science Series, Vol. 37(2), 83-91, 2010.

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

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

[7] Goldwasser S., Micali S. and Rackoff C., 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.

[8] Iyengar V. S., Novel elliptic curve scalar multiplication algorithm for faster and safer public key cryptosystems, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, 57-66, 2012. doi:10.5121/ijcis.2012.2305 57

[9] Joux A., A one round protocol for tripartite Diffie-Hellman, In springer-verlag, Algorithm Number Theory Symposium, ANTS-IV, Vol. 1838, Lecture notes in computer science, 385-394, 2000.

[10] Joye M. and Neven G., Identity based cryptography, IOS Press, 2009.

[11] Kar J., ID-based Deniable Authentication Protocol based on Diffie-Hellman Problem on Elliptic Curve, International Journal of Network Security, Vol.15, No.5, 357-364, 2013.

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

[13] Kumar M., A secure and efficient authentication protocol based on elliptic curve diffie-hellman algorithm and zero knowledge property, I. J. S. C. E., Vol. 3, Issue-5, 137-142, 2013.

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

[15] Miller V. S., The weil pairing and its efficient calculation, J. Cryptography, 17:235-261, 2004.

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

[17] Moody D., Peralta R., Perlner R., Regenscheid A., Roginsky A., and Chen L., Report on Pairing-based Cryptography, Journal of Research of the National Institute of Standards and Technology 11, Vol. 120, 11-27, 2015. http://dx.doi.org/10.6028/jres.120.002

[18] Paterson K. G., ID based signature from pairings on elliptice curves, Electron Lett. 38(18), 1025-1026, 2002.

[19] Shamir A., Identity based cryptosystems and signature schemes, in CRYPTO , 47-53, 1984.

[20] Zhang F. and Kim K., ID based blind signature and ring signature from pairings, in Advances in Cryptology-ASIACRYPT, springer-verlag, 533-547, 2002.