IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-9 E-ISSN: 2347-2693

A Tripartite Zero Knowledge Authentication Protocol based on Elliptic Curve Weil Pairing

Parthajit Roy

Dept. of Computer Science, The University of Burdwan, Bardhaman, India

*Corresponding Author: roy.parthajit@gmail.com, Tel.: +91-94747-87711

Available online at: www.ijcseonline.org

Received: 21/Aug/2017, Revised: 30/Aug/2017, Accepted: 19/Sep/2017, Published: 30/Sep/2017

***Abstract*—** Secret sharing is an important cryptographic protocol having many striking applications in reality. In a fraudulent model, it is even more difficult to compute because, fraud will also know the secrets and will impersonate as a valid secret share holder thereafter. This paper proposes a model for zero knowledge identification of authentic secret shareholders based on Elliptic curves. The model considers Chinese remainder theorem based secret sharing scheme for oblivious computations. The proposed model uses Weil pairing based tripartite Diffie-Hellman model on Elliptic curves and the model only says whether the participating parties are true shareholders or not without reviling any secret information. The paper also discusses the computational aspects the proposed models and possible weaknesses of the model.

***Keywords*—**Weil Pairing, Zero Knowledge Authentication, Secret Computing, Chinese Remainder, Elliptic Curve

I. INTRODUCTION

Secret sharing is a concept where a piece of secret information is divided and shared among n users in such a way that for any combination of less than n shareholders it is impossible to guess slightest idea about the piece of information or any part of the same. However, if n persons agree to disclose their secrets, the complete information can be reviled. The first secret sharing model was proposed by Shamir [1]. In his model, polynomials on modulo primes have been proposed for computation of secrets. The scheme was such that any k out of n shareholders can revile the complete information and any combination less then k shareholders do not get any information about the secret. Such type of secret sharing scheme is called threshold secret sharing where a threshold number, k out of n, shareholders have to jointly agree to recover the secret.

After the first proposal by Shamir, there were several proposals on the same line. Instead of polynomials, a set of n linear equations on a k- dimensional hyper-plane and the threshold sharing based on that was proposed by Blakley [2]. A matrix multiplication based secret sharing scheme was proposed by Kernin et al [3]. A good discussion on classical secret sharing can be found in the book of Schneier [4]

Chinese Remainder Theorem (CRT) was first proposed by a Chinese mathematician, Sun Tse, in the first century. CRT has its application in cryptography in speeding up the RSA computation [5]. The early proposals on CRT based secret sharing was given by Asmuth-Bloom [6] and Mignotte [7]. Some recent works on CRT based secret sharing has been done by Singh et al [8] where a sequential secret sharing model has been proposed whereas dual threshold secret sharing has been proposed by Shi et al [9]. Some application of secret sharing in Wireless sensor network has been proposed in [10].

Oblivious computation is a cryptographic process where multiple parties compute some cryptographic protocols without reviling the piece of information they possess. Cryptographic secure computation is mainly used in secret sharing. This is because there may be a fraud inside the system. In a secret sharing model, if a fraud takes part into computations, the fraud will know the secret shares of the other persons. Secure computation for groups in a distributed system has been proposed by Castiglione et al [11] whereas the same in a cloud setup has been proposed by Bilakanti et al [12]. Secure computation has successfully been applied in social fields also. In the domain of health science, it has been applied by Tso et al [13].

Zero knowledge proof of ownership is another important branch of cryptography. In zero knowledge proof model, a person proves that he knows an information without reviling the actual one. A good explanation of zero knowledge proof has been given by Quisquater et al [14] and Schneier [4].

This paper proposes a fusion of zero knowledge proof and secure computing for Chinese Remainder based secret sharing model. The proposed work computes the zero knowledge on Elliptic curve based groups. Especially the

Weil pairing of Elliptic curve has been introduced in a novel way to both secure computing as well as for zero knowledge proof.

The rest of the paper is organized as follows. Section II discusses the Elliptic curves, Weil pairing and a brief of the Chinese Remainder Theorem. Section III presents the proposed model and analyses various aspects of computing and efficiencies. Section IV discusses the security and drawbacks of the proposed model. Section V concludes the paper and references come at the end.

II. ELLIPTIC CURVE MATHEMATICS

Elliptic curves are curves of the form $y^2 = x^3 + ax^2 + bx + c$ in two dimension but the Elliptic curves that we consider for cryptographic protocols are Elliptic curves over a Gallios field $GF(p)$ and are known as finite Elliptic curve. Formally, a Finite Elliptic curve is defined as follows.

Given a prime p, let $Z(p)$, be a finite Gallois field realized on addition modulo over prime p. An Elliptic curve over $Z(p)$ is the set of all ordered pairs (x, y), $s.t.\ x \in Z_p$ & $y \in Z_p$ and (x, y) satisfy the equation of the form $E(p)$: $y^2 = x^3 + ax + b \ mod\ p$. To make it a group, we incorporate an extra point at infinity Θ and an extra condition (Condition of smoothness) $4a^3 + 27b^2 \neq 0 \ mod\ p, \forall a, b \in Z(p)$.

A finite elliptic curve over a prime p is a group structure. Given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, the addition of the points is defined as the mirror image of the line through P_1, P_2 and the curve E at the point P_3 whose slope is given by equation 1

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & if\ P_1 \neq P_2 \\ \frac{3x^2 + a}{2y_1} & if\ P_1 = P_2 \end{cases} \quad (1)$$

And $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $(x_3, y_3) = p_3 = P_1 + P_2$. The inverse of any point $P = (x, y)$ is $P' = (x, -y)$. The addition of any point on the Elliptic curve E with the unit element Θ is defined as $P + \Theta = \Theta + P = P$ and the addition of P and its inverse P' is defined as $P + P' = \Theta$, which is point at infinite.

Elliptic curve arithmetic forms a group with finite elements. Such finite groups have generators. If $Q = (x_k, y_k)$ is a generator, then all of the points on the Elliptic curve E can be generated by repeated addition operation of the generator with itself as $Q, 2Q, 3Q, \cdots$. A good discussion on Elliptic curve is given in the work of Hoffstein [5]. A practical and computational approach for designing Elliptic curve based crypto systems has been given by Hankerson, Menezes and Vanstone [15].

The discrete logarithm over Elliptic curve was first proposed by Neal Koblitz [16] and Victor Miller [17] independently. Discrete logarithm on Elliptic curves can be stated as follows.

Given an elliptic curve E: $y^2 = x^3 + ax + b \ mod\ p$ for some known public p and a generator of the elliptic curve points $Q = (x_k, y_k)$, the discrete logarithm problem on Elliptic curve is the problem of computing $n \in Z_p$, for which $(x_i, y_i) = \mathrm{B} = n \times Q$ for some public $\mathrm{B} = (x_i, y_i)$. It is believed that the discrete logarithm problem on Elliptic curves is even harder than the discrete logarithm problem in the finite multiplicative modulo groups.

A point of finite order with respect to a group is the smallest +ve integer $m \geq 1$, such that for $P \in E, m \times P = \Theta$. For any elliptic curve, the set of torsion points is defined as

$$T^m_{E(p)} = \{P,\ \forall\ P \in E\ \&\ m \times P = \Theta \quad (2)$$

Where $E(p)$ is the Finite Field Elliptic curve over p, over which the torsion set is defined. If T^m is the set of torsion points, then T^m forms a group.

Given a set of torsion points over an Elliptic curve $E(p)$, if we consider a torsion point set $T^m_{E(p)}$ in such a way that $m \neq 0\ mod\ p$, then there exits another Elliptic curve over $p\hat{}k$ define as $E(p^k)$ for some k, in such a way that the set of torsion points of order m has an equivalence with the Cartesian product of two cyclic group of order m. Formally, this relationship can be defined as,

$$T^m_{E(p^k)} = Z_m \times Z_m \quad (3)$$

Where Z_m is the field over modulo m.
It is a fact that if m is a prime, $T^m_{E(p^k)} = Z_m \times Z_m$ forms a vector space of dimension 2.

The Weil pairing $T^m_{E(p^k)} = Z_m \times Z_m$ is the bilinear mapping that returns a scalar from two points on the vector space $T^m_{E(p^k)}$ which is similar to dot product in a vector space. The Weil pairing of dot product over the Elliptic curve torsion points $T^m_{E(p^k)}$ is denoted as $\tau_m(.)$ and is defined in the following way,

$$\tau_m(P_1 + P_2, Q) = \tau_m(P_1, Q) \times \tau_m(P_2, Q) \quad (4)$$
$$\tau_m(P, Q_1 + Q_2) = \tau_m(P, Q_1) \times \tau_m(P, Q_2) \quad (5)$$

$$\tau_m(P, P) = 1\ \forall P \in T^m_{E(p^k)} \quad (6)$$

A good discussion on Weil pairing is given in [5]. There exists a practical algorithm for Weil pairing due to Miller [18].

A distortion map over an Elliptic curve is the mapping $\psi: E(p) \rightarrow E(p)$, such that,

$$\begin{aligned} & \tau\big(a \times P, b \times \psi(P)\big) \\ = \ & \tau\big(a \times P, \psi(b \times P)\big) \\ = \ & \tau(P, \psi(P))^{ab} \end{aligned} \quad (7)$$

It can be noted that two points on the Elliptic curve are multiplied by two integers and the Weil pairing gives the exponentiation of the two numbers. This a beautiful property of Weil pairing and has successfully been applied for Diffie-Hellman key exchange among three parties by Joux [19].

Now we shortly introduce Chinese Remainder Theorem. If $s_1, s_2, \cdots, s_m$ are m pairwise co-prime integers, then for any x in the range $1 \leq x \leq \Pi_{i=1}^{m} s_i$, x can uniquely be written as a set of linear equations as,

$$x = a_i \ mod \ s_i \ \ \forall i = 1,2,3, \cdots, m \quad (8)$$

It is clear that knowing a_i and s_i one can recover the value x and the concept has been used by researchers in the field of secret sharing [6] [7].

III. PROPOSED ZERO KNOWLEDGE PROOF MODEL

The proposed model is a three person authentication model. The model works as follows. Let there is a supreme authority S who wants to share a secret among three persons namely Alice(A), Bob(B) and Charlie(C). The method of secret sharing that the supreme authority has adapted is secret sharing using Chinese Remainder in non-threshold mode, i.e. all the three persons Alice, Bob and Charlie have to agree to recover the secret. The model can further be extended to a threshold based model also. The working principle of the proposed model is as follows.

A. Secret generation

Let the supreme authority wants to share a secret x. In our case x is an integer in the range $2^{512} \leq x \leq 2^{3\times512}$. This a stringent requirement for the success of the proposed model. Let Supreme authority has decided to share it among three persons. For this, he will select three large primes p_1, p_2, p_3 each of which is at least 512 bits (this is why x is less than $2^{3\times512}$. He then computes the remainders using equation (9), (10) and (11) for CRT.

$$x = a_1 \ mod \ p_1 \quad (9)$$

$$x = a_2 \ mod \ p_2 \quad (10)$$

$$x = a_3 \ mod \ p_3 \quad (11)$$

Clearly all the conditions of CRT has been satisfied. i.e. p_1, p_2, p_3 are prime and hence pairwise co-prime and $x \leq 2^{3\times512} => x \leq p_1 \times p_2 \times p_3$. The supreme authority then transfer the pair (a_1, p_1) to Alice, (a_2, p_2) to Bob and (a_3, p_3) to Charlie. Table 1 shows the computation of the supreme authority.

Table 1 The computation and Sharing of Secrets.

Supreme Authority's Computation	**Transferring Secrets through secure channel**
1. Selects a secret x.	
2. Computes three large primes p_1, p_2, p_3 of size at least 512 bits.	
3. Computes the Chinese Remainders as,	
3.1. $x = a_1 \ mod \ p_1$	3.1.1 Sends(a_1, p_1) to Alice
3.2. $x = a_2 \ mod \ p_2$	3.1.2 Sends (a_2, p_2) to Bob
3.3. $x = a_2 \ mod \ p_2$	3.1.3 Sends (a_3, p_3) to Charlie

B. Public parameter generations for reconstruction and authentication

The Supreme authority then, does the following thing. He selects a large prime p. Large means greater than $p \geq p_1 p_2 p_3$ and selects an elliptic curve $E: y^2 = x^3 + ax + b \ mod \ p$ over the finite field $F(p)$. He then identifies a point $P \in E_{F(p)}$ and a corresponding suitable distortion map $\psi(.)$ for the for P of prime order m. He then publishes all the parameters. The Initial setup and parameter generations are summarized in table 2.

Table 2 Public parameter generation (By the Supreme Authority).

Supreme Authority's Public parameter Generation	**Making public**
1. Computes a large prime p $(p \geq p_1 p_2 p_3)$	A. Make p public
2. Choose Elliptic curve $E_{F(p)}: y^2 = x^3 + ax + b$ over $F(p)$.	B. Make $E_{F(p)}$ public.
3. Choose a point $P \in E_{F(p)}$ of order m.	C. Make P public
4. Choose distortion map $\psi(.)$ for P.	D. Make $\psi(.)$ public.
5. Compute Distortion Weil pairing $c = \tau(P, P)^{p_1 p_2 p_3}$	E. Publish c.

It can be noted that making c public is safe. Because this is equal to Elliptic curve discrete logarithm problem.

Once the parameters are generated and have made public, the secret distribution becomes complete. This is enough to identify the right persons without reviling their information.

C. Authentication using zero knowledge proof

Let us discuss now the most important part of our model. The zero knowledge proof of valid share holder.

Let Alice is a valid share holder and she does not know who the other shareholders are. Let some person P_1 and P_2 comes to Alice and says that they are the other shareholders. If she believes them and explores her information, they will learn it. If it turns out that one of them is (or both are) fraud, then they will know about Alice's share and later can impersonate as Alice. This is dangerous. Instead of that, Alice performs the following tasks. She computes $A_1 = p_1 \times P$ and announces A_1 to P_2 and P_3. Similarly, P_2 and P_3 will also compute the similar thing as A_2 and A_3 and will revile them. Alice will then compute $K_1 = \tau(A_2, A_3)^{p_1}$.

By Weil pairing Alice is actually computing the following.

$$\begin{aligned}\tau(A_2, A_3)^{p_1} &= \tau(p_2 \times P, p_3 \times P)^{p_1} \\ &= \tau(P, P)^{p_1 p_2 p_3} \\ &= K_1\end{aligned}$$

Clearly, K_1 will be equal to c, which is already computed by the authority if the actual p_2 and p_3 are supplied by the persons P_2 and P_3. i.e. they are truly Bob and Charlie. There is nothing special about Alice. Anybody can test others.

While this is going to work if all of the persons are correct, if one of them is fraud he can still do wrong things. Suppose person P_3 is a fraud, he then knows the value $A_1 = p_1 \times P$ and later can impersonate as Alice and will supply A_1 for his identification.

For this we need a different setup. Alice, P_2 and P_3 will supply most of the time a wrong information and occasionally will supply the correct information. Every time whenever Alice will get A_2, A_3, she will compute $\tau(A_2, A_3)^{p_1}$ for actual p_1. And will announce "Yes" or "No" depending upon whether she is getting the public parameter c or not. So, if by chance P_2 and P_3 supplies correct values, Alice will be able to generate c and she will be sure about the identity of the others and she will stop the process and will disclose her value A_1. Others will be able to immediately check the identity of Alice and the process will stop. This implies that everybody knows the prime number of the CRT. Table 3 summarizes the rounds of Zero knowledge proof.

Table 3 Secret holder's computation for proof of Identity

Shareholder's computation
For round j= 1,2,3,….
1. Every ith shareholder says $A_i[j]$ as her Weil pair output.
2. Every person P_i computes $\tau(A_{i-1}, A_{i+1})^{p_i}$ and says "yes" or "no".
3. If somebody recovers the value c, she discloses her A value.
4. Other persons verifies it and the process stops.

It can be noted that a fraud will never be able to say "yes" because he will never be sure whether the other two have supplied the correct values or not.

Once they will be convinced, they will revile their shares (a_1, p_1), (a_2, p_2) and (a_3, p_3) respectively and will recover the secret using CRT.

IV. SECURITY AND DRAWBACKS

The security of the proposed model is based on assumption of hardness of the underlying discrete logarithm problem on Elliptic curves. First of all, the supreme authority publishes the value $c = \tau(P, P)^{p_1 p_2 p_3}$. This is safe. Because there are two step security. Firstly, from $E_{F(p)}, P, \psi, p$ and c, it is infeasible (computationally) to compute the product $p_1 p_2 p_3$. Even if it is leaked, from the product $p_1 p_2 p_3$ it is again computationally impossible to recover individual factors p_1, p_2, p_3 because it is large prime factorization problem and large prime factorization problem is hard. Obviously, some care should be taken in choosing the prims.

Secondly, all the computations done by Alice, Bob and Charlie are simply $p_i \times P$ for some known $P \in E_{F(p)}$ and for some secret p_i. This is Elliptic curve discrete logarithm problem and Elliptic curve discrete logarithm problems are also hard. So, from this products, nobody gets any information of the value p_i. So, the overall the model is secure against the intruder who is listening the communications among Alice, Bob and Charlie.

Finally, if one or more of Alice, Bob and Charlie is fraud, then process never stops. So, after a sufficient number of trials the actual shareholders will be convinced that there are frauds in the system. The fraud person, on the other hand, cannot say "yes", because in that case he has to publish his A_i. Which he cannot generate because he does not know p_i. Secondly, for a fraud, it is very hard to guess, when the others are computing the value of A_i for their actual prime numbers. So, he will not get any slightest idea about the values A_i for other shareholders. So, he cannot impersonate at later phase.

The only drawback of the system is that there are many rounds of expensive computations for proving the knowledge with zero information.

V. CONCLUSION

This paper proposed a Weil pairing based tripartite zero knowledge identification of actual shareholders for Chinese remainder based secret sharing method. The model uses Weil pairing technique on Elliptic curves. The model is secure against outside intruders as well as inside frauds. The model also shows practical importance because of its computational efficiencies.

Some of the problems, however, like many rounds of computations for proving the authenticity of the persons, is a drawback of the system. Some other problems are, if the system has a fraud, the detection is hundred percent accurate. But sometimes even if all the persons are true shareholders,

the system may not become conclusive. This is because if in every round at least two persons supply wrong information then the third person will never be sure about their actuality. These two drawbacks can be rectified with more sophisticated techniques in future. Overall, the applicability of the proposed model is robust and satisfactory.

REFERENCES

[1] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 24, no. 11, pp. 612-613, 1979.

[2] G. Blakley, "Safeguarding Cryptographic Keys," *Proceedings of the National Computer Conference, 1979*, vol. 48, pp. 313-317, 1979.

[3] E. Kernin, J. Greene and M. Hellman, "On Sharing Secret Systems," *IEEE Transactions on Information Theory*, Vols. IT-29, pp. 35-41, 1983.

[4] B. Schneier, Applied Cryptography, Protocols, Algorithms, and Source Code in C, 2nd ed., New Delhi: John Wiley & Sons, 2001.

[5] J. Hoffstein, J. Pipher and J. Silverman, Introduction to Mathematical Cryptography, New York: Springer+Business Media, 2008, pp. 81-84.

[6] C. Asmuth and J. Bloom, "A Modular Approach to Key Safeguarding," *IEEE Transaction on Information Theory*, Vols. IT-29, no. 2, pp. 208-210, 1983.

[7] M. Mignotte, "How to Share a Secret," in *Lecture Notes in Computer Science*, 1983.

[8] N. Singh, A. N. Tentu, A. Basit and V. C. Venkaiah, "Sequential Secret Sharing Scheme based on Chinese Remainder Theorem," *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai*, pp. 1-6, 2016.

[9] G. Shi, Y. Ci, R. Xie, H. Wang and J. Zeng, "A Dual Threshold Secret Sharing Scheme among Weighted Participants of Special Right," *IEEE First International Conference on Data Science in Cyberspace (DSC), Changsha*, pp. 104-108, 2016.

[10] M. Karanam, "Shared Secret Key with Random Value Authentication Scheme in Wireless Sensor Networks," *International Journal of Computer Sciences and Engineering*, vol. 4, no. 5, pp. 21-24, 2016.

[11] A. Castiglione, P. D'Arco, A. D. Santis and R. Russo, "Secure Group Communication Schemes for Dynamic Heterogeneous Histributed Computing," *Future Generation Computer Systems*, vol. 74, pp. 313-324, 2017.

[12] A. Bilakanti, N. Anjana, A. Divya, K. Divya, N. Chakraborty and G. K. Patra, "Secure computation over cloud using fully homomorphic encryption," *2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore*, pp. 633-636, 2016.

[13] Raylin Tso, Abdulhameed Alelaiwi, S. Rahman, Mu-En Wu and M. Shamim Hossain, "Privacy-Preserving Data Communication Through Secure Multi-Party Computation in Healthcare Sensor Cloud," *Journal of Signal Processing Systems*, vol. 89, no. 1, pp. 51-59, 2016.

[14] Quisquater, J. Jacques, G. Louis and B. Thomas, "How to Explain Zero-Knowledge Protocols to Your Children," *Proceedings of the Advances in Cryptology – CRYPTO '89:*, vol. 435, pp. 628-631, 1990.

[15] D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, New York: Springer, 2004.

[16] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 177, no. 48, pp. 203-209, 1987.

[17] V. Miller, "Use of elliptic curves in cryptography," *Lecture Notes in Computer Science*, vol. 85, pp. 417-426, 1985.

[18] V. Miller, "The Weil pairing, and its efficient calculation," *Journal of Cryptology*, vol. 17, no. 4, pp. 235-261, 2004.

[19] A. Joux, "A one rou d protocol for tripartite Diffie-Hellman," *Journal of Cryptography*, vol. 17, no. 4, pp. 263-276, 2004.

Authors Profile

Parthajit Roy has received his Bachelor of Science from Burdwan Raj College under The University of Burdwan and subsequently has received his Masters in Computer Applications from The University of Burdwan. He is currently working as an Assistant Professor in the Department of Computer Science at The University of Burdwan. He has published several papers in the field of Pattern Recognition and graph based clustering. He has submitted his PhD thesis from University of Kalyani. His research interest is pattern recognition, clustering, cryptography and graph theory.

