I. J. Mathematical Sciences and Computing, **2021, 2, 24-30**
Published Online June 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2021.02.03

A Verifiable Ring Signature Scheme of Anonymous Signcryption Using ECC

Pratik Gupta
Department of Mathematics, Mandsaur University, Mandsaur-458001, India
E-mail: pratikgupta1810@gmail.com

Manoj Kumar
Department of Mathematics, Gurukul Kangri University, Haridwar-249404, India
E-mail: sdmkg1@gmail.com

Received: 28 January 2021; Revised: 18 February 2021; Accepted: 26 March 2021; Published: 08 June 2021

Abstract: The ring signature does hide the member of actually signature in the all possible signer. This technique was introduced by Rivest, Tauman and Shamir in 2001. This paper presents elliptic curve cryptosystem using signcryption algorithm with the anonymity feature. In the present paper, combines ring signature scheme with signcryption method to produce the anonymity feature for the signcryption scheme and discuss the characteristic of the security. Because elliptic curve cryptosystem yields like as small bandwidth requirements, low computation load, and high security and methodology of ring signature gives without revealing the actual signer to all possible signers. Combining the benefits of these two methodologies, the result is an efficient anonymous signcryption algorithm and highly secure.

Index Terms: Elliptic Curve, signcryption, digital signature, authentication, anonymous.

1. Introduction

Now days, cryptography is a tool to access information security on the Internet. The important character of information security is based on encryption scheme and digital signature scheme which assure confidentiality, authenticity, and integrity of message broadcast. The digital signature is generally applied in the internet society on behalf of traditional handwritten signatures. Various types of digital signature had been developed in such a manner ring signature, blind signature, threshold signature, proxy signature, signcryption. The application of ring signature and signcryption are use simultaneously in the presented research paper.

In the year 2001, Firstly Rivest et al. [1] developed a new idea of ring signature and implemented in article "How to leak a secret". The main purpose of ring signature technique is parallel to the group signature scheme but with some changes. In a group signature protocol, the management of group administrator can access the original identity of the real message signer and retract the anonymity of misbehaving signers. In addition, a group signature considered as identical to verifier only but not to the management of group administrator. To resolve these issues in ring signature protocol, it does not need to management of group administrator to define set of ring members so the real message signer only need randomly choosing a portion of the all ring members and generating a ring signature through the private key of actual message singer.

2. Mathematical Background of ring signature and ECC

Ring signature using RSA [5]: Let $M_1, M_2, M_3, ..., M_n$ be the ring members with public and private key pairs $(Pb_i, \Pr_i : 1 \le i \le n)$. It involves two methods, namely ring-sign and ring-verify which is described under below:

A ring sign methods is a probabilistic method which is defined under below as a following stages:

(i) A actual message signer $M_s, 1 \le s \le n$ uses a hash function of the message m. It gives a output and consider as the symmetric key

$$k = h(m, Pb_1, Pb_2, ..., Pb_n) \text{ or } k = h(m)$$

(ii) The actual message signer M_s uniformly and independently selects random values x_i in the length of $\{0,1\}^b$ and computes the value

$$z_i = f_i(x_i),\ i \neq s$$

where

$$f_i(x_i) = \begin{cases} q_i k_i + g_i(r_i); & (q_i+1)k_i \leq 2^b \\ x_i \quad\quad\quad\quad\ ; & otherwise \end{cases},$$

$$g_i(x_i) = x_i^{e_i} \bmod p_i \text{ and } Pb_i = (p_i, e_i).$$

(iii) To find z_s, Firstly determine the ring equation by the actual message signer M_s, we get

$$C_{k,x_s}(z_1, z_2, z_3, ..., z_n) = x_s$$

where C_{k,x_s} is a combining functions and in practice it is very difficult to determine the above ring equation for an oscar.

(iv) The message signer M_s computes $x_s = f_s^{-1}(y_s)$

(v) After that, ring signature is given by as the $(2n+1)$-tuple $(Pb_1, Pb_2, ..., Pb_n, x_s, x_1, x_2, ..., x_n)$.

Now, we can apply a ring verify method which is a deterministic method and it involves some stages:

(i) The verifier M_v, computes $z_i = f_i(x_i),\ 1 \leq i \leq n$.

(ii) The verifier M_v uses a hash function on the message *i.e.* $k = h(m)$ and M_v considers as a symmetric key k.

(iii) The verifier M_v tests the ring equation for z_i $(1 \leq i \leq n)$, we get

$$C_{k,x_s}(z_1, z_2, z_3, ..., z_n) = x_s$$

Here, the above ring equation is fulfilled according to the verifier then the verifier gets the valid signature, otherwise deny the signed message.

In the above mention ring signature scheme, it have required security components such as unforgeability and anonymity of actual message singer. Here, anonymity of message signer is that a verifier can find the probability of a ring signature is $1 \backslash n$. On the other hand unforegeability of message signer is the influence of a unknown member which can produce negligible of a ring signature.

Mathematical background of ECC: The elliptic curve was first proposed by Neil and Koblitz separately, the authors produced mathematically concept on elliptic curve which are useful to explain the introduced algorithm. Mathematical concept on elliptic curve is existing on the various literatures [6-10]. A easier and simple mathematically concept on elliptic curves is given by the following [1]:

The definition of elliptic curve E is express a mathematically way

$$E = \left\{(x, y) : \left(y^2 = x^3 + ax + b\right) \bmod p\right\} \cup \{O\}.$$

Where (x, y) is a point on E and O is point at infinity.

Addition of two distinct points on an Elliptic Curve: Here, we define addition of two given distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on an elliptic curve E and denoted as $R(x_3, y_3)$ on E [5]

i.e.

$$R = P + Q$$

where

$$x_3 = \left(\lambda^2 - x_1 - x_2\right), \quad y_3 = \lambda\left(x_1 - x_3\right) - y_1$$

and

$$\lambda = \frac{\left(y_2 - y_1\right)}{\left(x_2 - x_1\right)}$$

A geometrical representation for adding two given distinct points P and Q on E is shown in the below figure 1

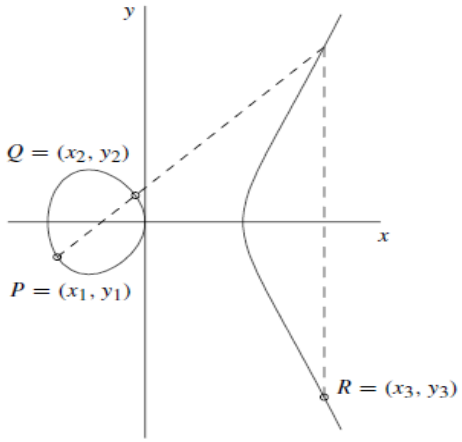


Fig 1. The addition of P and Q is R [5]

Doubling of a point on an Elliptic Curve: Doubling of a point P is nothing but it consider same *point i.e.* a single point $2P = P + P$. Algebraically, the point 2 P is defined as:

$$2P = P + P = R(x_3, y_3)$$

where

$$x_3 = \left(\lambda^2 - 2x_1\right), \quad y_3 = \lambda\left(x_1 - x_3\right) - y_1$$

and

$$\lambda = \frac{\left(3x_1^2 + a\right)}{2y_1}$$

A geometrical representation for doubling of a point P on E which is represent in the following figure 2.

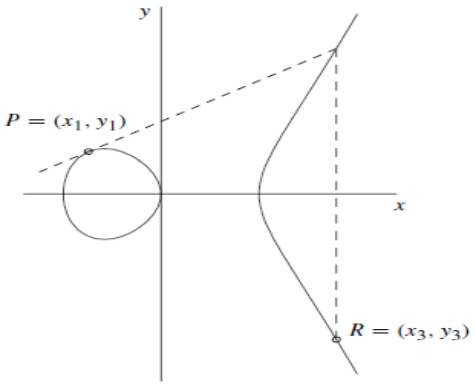


Fig 2. Doubling of P is P+P = 2P [5]

3. Proposed Ring Signature Scheme

In The proposed schemes consists of the following phases

***Phase-I: System parameters generation*:**

q	a large prime number $> 2^{160}$.
F_q	Finite field
a, b	$a, b \in F_q$ such that $4a^3 + 27b^2 \bmod q \neq 0$
O	a point of E at infinity.
$E_{k_1}(.) / D_{k_1}(.)$	symmetric encryption/decryption function along with symmetric key k_1 such as AES or DES.
Hash	a one-way hash function for resisting collision
E	Elliptic curve over F_q such that $y^2 = (x^3 + ax + b) \bmod q \cup O$
G	a base point of order n, on elliptic curve E.
n	a prime number such that $n.G = O$ which is greater than 2^{160}

Let $M_1, M_2, M_3, ..., M_i, ..., M_n$ be the members of ring signature. If d_i with $i = 1, 2, ..., n$ is the secret key of M_i then associated public key can be calculated as $P_i = d_i G$ respectively.

Phase-II: Ring generation of signcrypted text:

In this phase, a ring member M_i forward the signcrypted content of message m to the verifier $M_v, v \neq i$. After that M_i can generating of signcryption text and executed in the following steps.

(i) Randomly select α and β in $[1, q-1]$;

(ii) Calculate $K_i = \alpha G = (x_i, y_i)$, $K_e = \beta P_v = (k_1, k_2)$;

(iii) Calculate $c = E_{k_1}\left(m \| E_{d_i}(Hash(m)\right)$, $h = Hash(c \| k_2)$;

(iv) Compute $s = \frac{\beta}{h + d_i} (\bmod q)$, $R = hG$;

(v) Again randomly select $r_t \in [1, q-1]$

where $t = \begin{cases} n+1 & ; t = 1 \\ 1, 2, ..., i-1, i, i+1, ...n & : otherwise \end{cases}$

(vi) Campute $\gamma_t = Hash(c \| x_{t-1})$ and $K_t = r_t G + \gamma_t P_t = (x_t, y_t)$,

where $t = \begin{cases} n+1 & ; t = 1 \\ 1, 2, ...i-1, i, i+1, ...n; & otherwise \end{cases}$

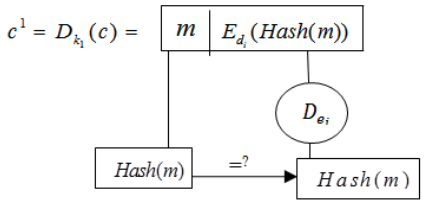
(vii) Compute $\gamma_i = Hash(c \| x_{i-1})$ and $r_i = \alpha - d_i \gamma_i (\bmod q)$;

(viii) Send the encrypted text $\chi = (c, R, \gamma_1, r_1, r_2, ..., r_n, s)$ to the verifier M_v.

Phase-III: Ring verification of signcrypted text:

After receiving the encrypted text $\chi = (c, R, \gamma_1, r_1, r_2, ..., r_n, s)$, the verifier M_v performs the following steps to verify it.

(i) Compute $(k_1, k_2) = d_v s R + d_v s P_i$, $h = Hash(c, k_2)$ and



(ii) For $t = 1, 2, ..., n-1$, calculate $K_t = r_t G + \gamma_t P_t = (x_t, y_t)$ and $\gamma_{t+1} = Hash(c^1 \| x_t)$;

(iii) Calculate $K_n = r_n G + \gamma_n P_n = (x_n, y_n)$ and $\gamma_1^1 = Hash(c^1 \| x_n)$;

(iv) With $\gamma_1^1 = \gamma_1$ and $R = hP_i$, confirm that the anonymous signcryption text $\chi = (c, R, \gamma_1, r_1, r_2, ..., r_n, s)$ is a valid from the ring member $M_i, 1 \le i \le n$, otherwise deny the signcrypted text.

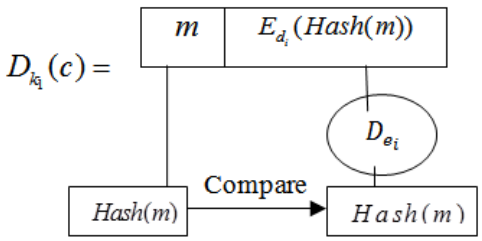
4. Discuss the Security of the Above Introduced Algorithm

In this section, we study the security components which introduced algorithm should require. The introduced algorithm associates the ring signature, ECC-based system and signcryption using symmetric encryption. In the security algorithms, the main two problems are solving the ECDLP and ECDHP which is hard problem to the current security algorithms. We discussed in the below:

ECDLP(Elliptic Curve Discrete Logarithm Problem)*:* Given $P, Q \in E$ such that Q is multiple of P where E denotes set of all points an elliptic curve over the finite field F_q. ECDLP says that evaluate $t \in Z$ such that $tP = Q$. It is a hard problem *i.e.* computationally infeasible to find t. [12].

***ECDHP (Elliptic Curve Diffie–Hellman Problem)*:** Let E denotes set of all points an elliptic curve over the finte field F_q and G is generator of E. The given relation is $P = c.G$ and $Q = d.G$ where $P, Q \in E$. Evaluate $t \in Z$ such that $t = c.d \times G$. This problem is known as ECDHP. It is a hard problem *i.e.* computationally infeasible to find t. [12].

Authentication: It is a technique for verification to identify the certify user through in a proper verification method. In this proposed scheme, the authenticity process is fulfilled by the below verification equation



The above equation shows that if the comparison is hold then the introduced algorithm fulfils the authenticity process.

Confidentiality: It is a technique to handle of securing the information from untrusted parties. In the introduced algorithm, if the adversary access the private key k_1 where k_1 is a member of K_e. It is impossible to evaluate k_1 because to solve k_1 is equivalent to the ECDHP or ECDLP problems.

Integrity: An integrity is a method to verify the original information by the recipient and also check whether received information is the original one that was sent by the sender or not. In the proposed scheme, ring member calculate h, s of the signcryption phase sends to the recipient. After that the adversary wants to replace the cipher text C by C^1 then automatically replaced the message M^1. Here, Use of one-way hash function to check the replace message in the verification process and automatically deny the original message. This shows that our proposed algorithm fulfil the condition of integrity.

Forward secrecy: Forward secrecy is characteristic of security to verify by signcryption. In this case, the adversary cannot decrypt the computation to gets the plaintext. In the proposed algorithm, The message signer knowing

for the verifier, to using long-term secret key of signer, communicated signcryption text χ. Because key x_e of the encrypted plaintext is produced a uniformly number β, a decryption key is produced every time. Hence, A signer M_i is disclose own long-term secret key d_i, old information remain secure, so, it has fulfil forward secrecy.

Unforgeability: It is a procedure to verify the adversary cannot generate a new signature by an older signed message. In the proposed algorithm, the recipient is the dynamic attacker to forge signcrypted message, because the recipient have secret key d_B to automatically verify message from sender. So, the recipient can easily decrypt the cipher text c using the his secret key d_B and generate c^1. In this case, ECDSA is unforgeable against adaptive attack. This shows that our proposed algorithm fulfil the condition of unforgeability.

Anonymity: The anonymity is holds only signer and verifier. In this case, on getting the signcryption documents, then a receiver can verify the time slot of the signcryption documents but not access to identify the actual sender. The difference between all the existing protocol and introduced protocol is lies in anonymity of a signer. In the sender and another party checked all signcryption documents which already generated to actual message signer, another party can only check the signature belongs to or not. If signature is issue by any member of that group then the another party cannot establish the actual identity of the signer. So, the verifier and another party cannot identify a sender using the signcryption documents.

Undeniability: If a dispute appears then receiver can change the original signcryption content which already generated a ring signature. After that, party can check this ring signature, and authenticate the original of the signature and the third party cannot determined the real identity of the signer. The signcryption could not be produced by a non-member and not be forged by the verifier. This shows that our proposed algorithm fulfil the condition of undeniability.

Table 1. The provided security analysis of different signcryption schemes

Signcryption Schemes	Confidentiality	Undeniability	Unforgeability	Anonymity	Forward Secrecy
Zheng[4]	✓	✓	✓	X	X
Zheng and Imai[2]	✓	✓	✓	X	X
Bao and Deng[5]	✓	✓	✓	X	X
Gamage et. al.[6]	✓	✓	✓	X	X
Jung et.al.[5]	✓	✓	✓	X	X
Our scheme	✓	✓	✓	✓	✓

5. Conclusions

The proposed scheme in the present paper, combines ring signature scheme with signcryption method to produce the anonymity feature for the signcryption scheme. The use of ECC provides the advantages like high security, less power consumption, low memory space. In this protocol includes the symmetric encryption processes and digital signature. Various applications of this ring signature scheme such as employee feedback systems, voting machine. This results in the reduced transmission load. Thus efficiency of performance and transmission enhanced.

References

[1] Kumar, Manoj and Gupta, Pratik, "Cryptographic schemes based on Elliptic Curve over the Ring Zp[i]", Applied Mathematics, vol. 7, no. 3, pp. 304-312, 2016.

[2] Chaum, David, "Group signatures", Davies D W, ed. In: Proceedings of EUROCRYPT'91, Lecture Notes in Computer Science, Berlin: Springer-Verlag, Vol. 547, pp. 257–265, 1991.

[3] Rivest, Ronald and Shamir, Adi and Tauman, Yael "How to leak a secret", In: Proceedings of ASIACRYPT'01, Lecture Notes in Computer Science, Berlin: Springer-Verlag, vol. 2248, pp. 552–565, 2001.

[4] Zheng, Yuliang, "Signcryption and Its Applications in Efficient Public Key Solutions", Proceedings of 1997, Information Security Workshop (ISW'97), 1997. (http://www.sis.uncc.edu/~yzheng/papers/).

[5] Rivest, Ronald and Shamir, Adi and Adleman, Leonard, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[6] Gupta, Pratik and Kumar, Manoj and Kumar, Ajay, "A Novel and Secure Multi-party Key Exchange Scheme Using Trilinear Pairing Map Based on Elliptic Curve Cryptography", *International Journal of Pure and Applied Mathematics*. Vol. 116, no. 1, 2017.

[7] Hankerson, Darrel and Menezes, Alfred and Vanstone, Scott, "Guide to Elliptic Curve Cryptography", Springer-Verlag, Germany, 2004.

[8] Silverman, Joseph, "The Arithmetic of Elliptic Curves", Springer, New York, 1986. (http://dx.doi.org/10.1007/978-1-4757-1920-8).

[9] Stinson, Douglas, “Cryptography Theory and Practice”, Chapman and Hall/CRC, United Kingdom, 2006.
[10] Washington, Lawrence, “Elliptic Curves Number Theory and Cryptography”, *Chapman and Hall/CRC, United Kingdom*, 2008. (http://dx.doi.org/10.1201/9781420071474). (1971).
[11] Boneh, Dan and Lipton, Richard, “Algorithms for black-box fields and their application to cryptography”, *In: Advances in Cryptography*, pp. 283-297, 1996.
[12] Johnson, Don and Menezes, Alfred and Vanstone, Scott, “The elliptic curve digital signature algorithm (ECDSA)”, *International Journal of Information Security*. Vo. 1, no. 1, pp. 36-63, 2001.
[13] Rosalina, Nur Hadisukmana," An Approach of Securing Data using Combined Cryptography and Steganography ", *International Journal of Mathematical Sciences and Computing(IJMSC)*, Vol.6, No.1, pp.1-9, 2020. DOI: 10.5815/ijmsc.2020.01.01

Authors’ Profiles

Dr. Pratik Gupta is working as an assistant professor in the department of Mathematics at Mandsaur University, Mandsaur (India). Areas of interest are Cryptography, and Network Security. He has been published more than seven research papers in reputed national and international Journals.

Dr. Manoj Kumar is working as an assistant professor in the department of Mathematics and Statistics, Gurukul Kangri Vishwavidyalaya, Haridwar, Uttarakhand (India). His research areas are Elliptic Curve Cryptography, Quantum Cryptography and Approximation Theory. He has been published more than fifteen research papers in reputed national and international Journals.

How to cite this paper: Pratik Gupta, Manoj Kumar," A Verifiable Ring Signature Scheme of Anonymous Signcryption Using ECC ", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.7, No.2, pp. 24-30, 2021. DOI: 10.5815/ijmsc.2021.02.03