International Journal of Applied Science and Engineering

Efficient and secure multiple digital signature to prevent forgery based on ECC

Sarvesh Tanwar[1], Sumit Badotra[2*], Medini Gupta[1], Ajay Rana[1]

[1] Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida, India
[2] Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India

ABSTRACT

Adversary can be able to perform selective forgery where valid signature on message are created by someone else, with a significant probability and existential forgery, in which a pair of message and valid signature is created by him. For a signature scheme to be perfectly secured, it should be secured computationally. We present an ID based multiple signatures scheme secure against selective forgery attack based on ECC. The objective of the work carried out is to design and implement multi digital signature based on ECC against selective forgery attack.

Keywords: Signature, Secure, ECC, Selective forgery.

1. INTRODUCTION

The foremost and ancient cryptographic primitive is digital signature. Digital signature serves to verify that signer of the document has created and signed that document and that record is tamperproof (David et al., 1999). It is used for non-repudiation, authentication and data integrity. It is generated using public key cryptography.

Digital signatures guarantees the following information security properties (badotra, et al., 2020):- authenticity, integrity, non-repudiation, credibility, non-reusable and unalterable.

It is important to protect information when two parties exchanging it, so that the ultimate recipient have knowledge about the information being created by sender and it remains unaltered. According to the IT act, 2000, digital signatures on a document ensure the authenticity and security. To obtain a digital signature, first computing a hash of the biological information provided by the entities, encipher the hash values with the private key of the sender, and affixing the encipher hash to the digital records. Signed records usually carries a duplicate copy of signer's certificate. Digital signature paves the way to verify that signer of the record has created and signed that document and that record is not modified and trustworthy (David et al., 1999). It is generated using public key cryptography to ensure the authentication non-repudiation, credibility, integrity, non-reusable and unalterable (badotra, et al., 2019).

Digital signature can be implemented using RSA, ECC (Elgamal and Elliptic Curve Cryptography). ECC has the advantage of shorter key and higher efficiency over RSA.

If A want to send a signed message to B, then the digital signature would be as follows:- A generates a unique fingerprint using one way hash function then encrypts message dist with his secret key. A message or document alongwith obtained signature is transmitted to the receiving party and that receiving party calculates the message digest using the same hashing algorithm that of sender. The signature is then decrypted with signer's public key and computed message digest is compared with the decrypted signature. If the condition is satisfy, receiver validates the signature and accept the message or document otherwise reject the same. Fig. 1 depicted the working of digital

OPEN ACCESS

Received: May 13, 2021

Accepted: May 25, 2021

Corresponding Author:
Sumit Badotra
sumit.26152@lpu.co.in

Publisher:
Chaoyang University of Technology
ISSN: 1727-2394 (Print)
ISSN: 1727-7841 (Online)

https://doi.org/10.6703/IJASE.202109_18(5).010

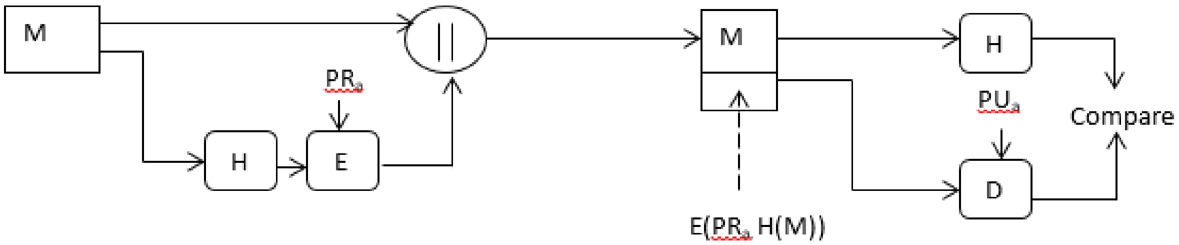


Fig. 1. Generation and verification of digital signature

signature.

The remaining paper comprises the following sections - literature review presented in Section 2. Section 3 present the proposed scheme supported by performance and evaluating security parameters in section 4 and section 5 and finally section 6 is the conclusion of the paper.

2. LITERATURE REVIEW

Bi et al. (2018) proposed an algorithm for MECCDSA (Multiple Elliptic Curves Digital Signature) which allows crating elliptic curves depending on security requirement along with updating parameters of each elliptic curves. Performance analysis is based on three factors- validity, efficiency and security. It is difficult to manage the algebraic logarithm problem in elliptic curve digital signature. MECDSA have a positive result in solving ECDLP (Elliptic Curve Discrete Logarithm Problem). The processing cost is identified by inverse function in finite prime series and multiplication and division function in elliptic curve.

Saritha (2020) discussed about using Digital Signature Algorithm (DSA) that is an asymmetric key cryptography where public and secret keys are applied for enciphering and deciphering sensitive information. The two-factor authentication that takes password and other credentials such as face recognition is less secure than ECC (Elliptic Curve Cryptography). ECC is a public key cryptography that uses less key size for enhanced security. ECC coupled with DSA will be more beneficial for authentication in Blockchain technology. Algorithms for signature generation and verification are used. Bitcoin is a digital cryptocurrency that has implemented ECCDSA for maintaining integrity of records and secured transactions.

Tsai and Su (2017) proposed a scheme for blind signature in digital information based on elliptic curve cryptography. ECC has higher computational speed. Focused on ECDLP, this scheme integrates signcryption for verification of multiple digital records. Small key values in ECC and complex ECDLP has resulted in high security and low communication overhead. Various features such as blindness, confidentiality, integrity, forgery-proof, untrace ability, authentication is embedded in the system. The scheme involves less multiplication operations as compared to previous work. Large number of digital messages can be carried out with efficient and greater security.

Mehibel and Hamadouche (2021) discussed about the challenges of Elliptic curve Diffie-Hellman (ECDH) which doesn’t validate secret session key thus prone to man-in middle attack. ECC is widely used for limited memory devices because computational time is low with high security. Authors developed a low cost authenticated secret session key scheme using ECCDSA where two arbitrary values are taken. Performance is evaluated based on computational difficulty and security where the system have better results than other two works mentioned. Security of the proposed scheme is higher than of A-ECDH. There is similarity in security features of Biswas scheme and the proposed scheme.

Singh et al. (2020) designed a protocol for smart cards using Elliptic Curve Signcryption. Protocol is divided into different phases and three actors are smart card user, registration center and service provider. User and service provider have to get registered in register center respectively. No third party can interrupt the communication. Mutual authentication based on signcryption takes places where user and service provider mutually authenticate each other. The security protocol is effective with brute force attack, man in the middle attack, masquerade attack, replay attack. Protocol utilizes low communication bandwidth and less computing cost.

In 1983 Itakura and Nakamura first proposed the concept of multiple signatures (Gangishetti et al., 2006). In multiple signature a group of members need to sign the message for approval using a single compact signature (Tanwar, et al., 2019). In multiple signature n random secret keys k1, k2, kn and public key t is generated such that:
(k_1+k_2+..k_n)*t = 1 mod Ø(n)

In 1984, Shamir proposed identity (ID) based cryptosystem. In ID based signature public key is derived from the user’s identity and private key generated by PKG. There is no need to transmit public key as it is efficiently derived from the receiver’s identity information such as name, email address, IP address and mobile number (Sharma, et al., 2014).

Devi et al. (2015) has proposed an efficient digital multiple signature schemes that is vulnerable to inside and forgery attack. As receiver can verify signer’s identity by comparing the received one with the actual identities.

Authors proposed an efficient multiple signature based on discrete logarithm problem. Signature verification time and length are fixed but suffers modulus clashing problem (Harn and Ren, 2008).

Miller (1985); Koblitz (1987) proposed Elliptic Curve Discrete Logarithm Problem (ECDLP) which plays significant role in cryptographic techniques. In 1998 ECC digital signature was accepted as an ISO standard. Negi et al. (2015) proposed scheme to improve the security by using multiple integers (e_1, e_2, e_n) to primary integer number and increase difficulty of decryption key. But they do not allow storing digital signature. Nia et. al. (2016) explained different type of digital signature such as batch scheme, forward secure scheme, blind scheme and proxy scheme. Tianhuang and Xiaoguang (2010) proposed algorithm for the improvement of DSA to solve ecommerce security issues. Shamir et al. (1984) explained two basic categories of digital signature- direct and arbitrated. Direct signature involved two parties- sender and the receiver whereas in arbitrated signature scheme every signed message go through arbiter.

Many other authors (Wang et al., 2015; Harn and Ren, 2008; Yang, 2013; Buenasmañanas Domínguez et al., 2011; Gangishetti et al., 2006; Bellare and Neven, 2006) proposed multiple digital signature based on RSA and ECC.

In this paper, we proposed an efficient and secure ID based digital multiple signatures based on ECC which has a setup phase, key generation phase multi-signature generation and verification phase.

2.1 Preliminary Notes

In this section we will summarizes some fundamental concepts on bilinear pairing and necessary hard problems. In cryptography, bilinear pairing is an important primitive. Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group with same order q (prime). A map $\hat{e} = G_1 \times G_1 \rightarrow G_2$ be a bilinear if satisfies the following properties:-

- Bilinear: for all $a, b \in Z_r$, it holds that $\hat{e}(P^a, Q^b) = \hat{e}(P, Q)^{ab}$.
- Non-degeneracy: There exists a $P \in G_1$ and $Q \in G_2$ such that $\hat{e}(P, Q) \neq 1$.
- Computable: if $P, Q \in G_1$, $e(P, Q) \in G_2$ can be computable in polynomial time using an efficient algorithm.

2.2 Mathematical Hard Problem and Assumptions

The security of ECC depends on the difficulty of solving the elliptic curve logarithm problem.

- Computational Diffie-Hellman Problem (CDHP): Given $P, aP, bP \in G_1$ for some $a, b \in Z_q^*$ and $\in G_1$, the CDHP problem is to compute $abP \in G_1$.
- Computational Bilinear Diffie-Hellman Problem (CBDHP): Given $P, aP, bP, cP \in G_1$ for some $a, b, c \in Z_q^*$ and $\in G_1$, the CBDHP problem is to compute $\hat{e}(P, P)^{abc} \in G_2$.

2.3 Proposed Scheme for Multi Digital Signature Based on ECC Against Selective Forgery Attack

Adversary can be able to perform selective forgery where valid signature on message are created by someone else, with a significant probability and existential forgery, in which a pair of message and valid signature is created by him. A signature scheme can be perfectly secure if it is computationally secure. Now a day's ECC has become hotspot in the field of information security (Miller, 1985; Chen et al., 2004). ECC has the advantage of shorter key and higher efficiency over RSA. The author (Devi et al., 2015) has proposed an efficient and secure digital multiple signature protocol based on ECC that is vulnerable to inside and forgery attack. As the receiver can verify signer's identity by comparing the received one with the actual identities.

2.4 Implementation of ECC Based Digital Signature Along with a Timestamp

We presented an ID based multiple signatures scheme secure against selective forgery attack based on ECC. It has a setup phase, key generation phase multi-signature generation and verification phase. We implemented ECC based digital signature along with a timestamp. Fig. 6.1 shows time taken in digital signature generation and verification based on ECC.

a. Setup Phase

1. p = a large prime number, public to all
2. Q = a large prime factor of p-1, public to all
3. Define the equation $E_q = y^2 \ mod \ p = x^3 + ax^2 + b \ mod \ p$ for elliptic curve on a prime field E(Fp) where a and b are two parameters where$4a^3 + 27b^2 \neq 0$.

b. Key Generation Phase

1. Select random number r_i. And compute private key $d_i = H(ID_i|r)$.
2. Compute public key $X_i = d_i P$
3. Send Xi to other signers and clerk or group admin sums up all the Xi as follows:-

$$X = \sum_{i=1}^{N} X_i$$

c. Multi-Signature Generation Phase

Each signer follows the following steps to generate multi-signature:-

1. Choose a random number K_i.
2. Compute $h = (ID_i||U)$
3. Compute $Y_i = K_i hP$
4. Send Y_i to other signers and finally clerk or group admin sums up all the Y_i as follows:-
5. $Y = \sum_{i=1}^{N} Y_i$
6. Perform $e = H(M\|\text{r})$
7. Compute $S_i = K_i + ed_i$ mod n
8. Send S_i to other signers and finally clerk or group admin sums up all the S_i as follows:-
9. $s = \sum_{i=1}^{N} S_i \, mod \ \ n$

Send $\sigma(s, Y)$ to the receiver or verifier

d. Multi-Signature Verification Phase

We carried out ECC based digital signature inclusive of a timestamp. The time taken in digital signature generation and verification based on ECC. The receiver receives the multi-signed document. He performs the following steps to get the valid document:-

1. Compute $e = H(M||\mathrm{r})$
2. Compute $v1 = shP$
3. Compute $v2 = Y + eX$
4. Accepts the message if and only if $v1 == v2$ else reject it.

```
C:\Users\303950\Desktop\java programs\ecc>java
ECDSA
private key is:
edd6cf536758fcc24bcfb43593d1ba27c5c4011536403
3f09415325150b34e10
The private key is: [B@2f7a2457
x of public key is:
2707027307278111594562277269945288746908243
0945682425931237000257035762527895
y of public key is:
3268425681633395547168369688851131953479725
7588384881508206331602156419638864
Time started for Signature Generation:1619978545777
End Time for Signature Generation:1619978545821
Runing Time of singning in ECDSA:44000us
the value of R is:
6481969842109113757130364190535918021362478837
2242250497000172977107657729835
the value of S is:
2069866637831263279295733892895585667116557156
448639547820178116675238460349
Valid signature
Runing Time of verification: 41.00 ms.
```

3. PERFORMANCE ANALYSIS

The proposed scheme is compared with Yadav et al. (2013); Chen et al. (2004). Table 1 and Table 2 show the computational time of different operations and depicts the notations.

Table 3 describes the comparison between (Devi et al., 2015; Chen et al., 2004) and proposed scheme.

The proposed scheme is more efficient and secure than in (Devi et al., 2015; Chen et al., 2004) terms of authentication and security.

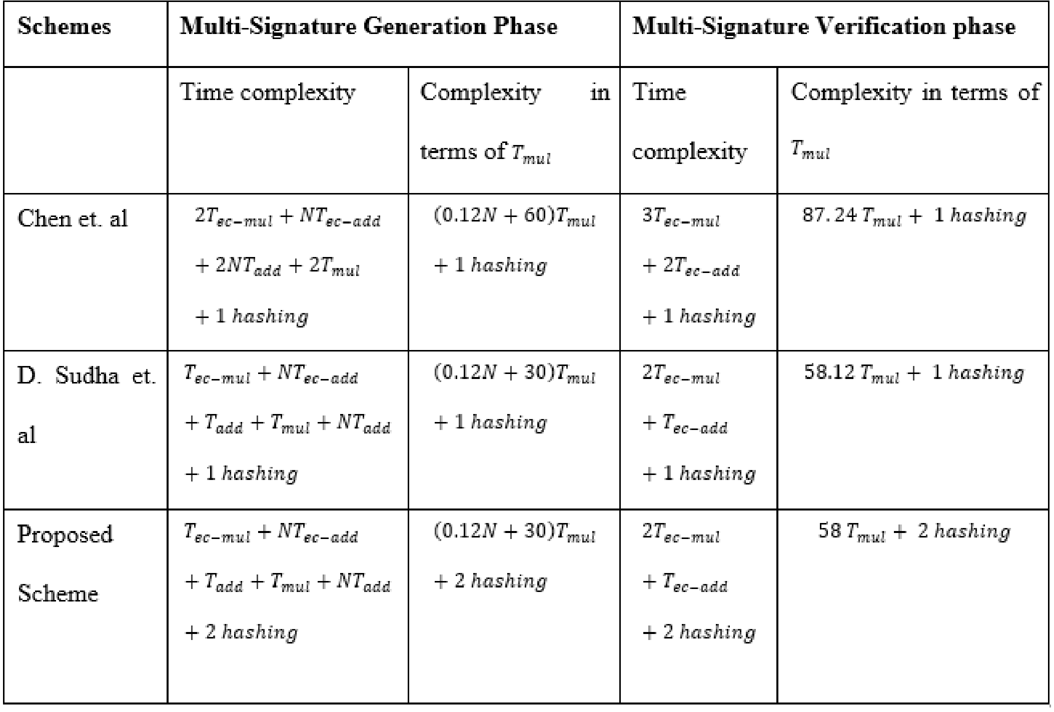
Table 1. Shows unit conversion of various operations in terms of T_{MUL} (THU, (Tanwar et al., 2019))

Time Complexity of an operation unit	Time complexity in terms of multiplication
T_{EXP}	240 T_{MUL}
T_{EC-MUL}	29 T_{MUL}
T_{EC-ADD}	0.12 T_{MUL}
T_{MUL}	0.12 T_{MUL}
T_{ADD}	Negligible
T_{INV}	0.073 T_{MUL}

Table 2. Various operation units converted into T_{MUL}

Notation	Description
T_{EXP}	Time required for executing modular exponentiation
T_{EC-MUL}	Time required for executing multiple multiplication
T_{EC-ADD}	Time required for executing addition of two points in an elliptic curve
T_{ADD}	Time required for executing modular addition
T_{INV}	Time required for executing modular inversion
T_{HASH}	Time required for executing hash function
T_{MUL}	Time required for executing modular multiplication

Table 3. Comparison of proposed scheme with Sudha et al. (2015); Chen et al. (2004)



Schemes	Multi-Signature Generation Phase		Multi-Signature Verification phase	
	Time complexity	Complexity in terms of T_{mul}	Time complexity	Complexity in terms of T_{mul}
Chen et. al	$2T_{ec-mul} + NT_{ec-add}$ $+ 2NT_{add} + 2T_{mul}$ $+ 1\ hashing$	$(0.12N + 60)T_{mul}$ $+ 1\ hashing$	$3T_{ec-mul}$ $+ 2T_{ec-add}$ $+ 1\ hashing$	$87.24\ T_{mul} +\ 1\ hashing$
D. Sudha et. al	$T_{ec-mul} + NT_{ec-add}$ $+ T_{add} + T_{mul} + NT_{add}$ $+ 1\ hashing$	$(0.12N + 30)T_{mul}$ $+ 1\ hashing$	$2T_{ec-mul}$ $+ T_{ec-add}$ $+ 1\ hashing$	$58.12\ T_{mul} +\ 1\ hashing$
Proposed Scheme	$T_{ec-mul} + NT_{ec-add}$ $+ T_{add} + T_{mul} + NT_{add}$ $+ 2\ hashing$	$(0.12N + 30)T_{mul}$ $+ 2\ hashing$	$2T_{ec-mul}$ $+ T_{ec-add}$ $+ 2\ hashing$	$58\ T_{mul} +\ 2\ hashing$

4. SECURITY ANALYSIS

We proposed scheme that comes up with a wide range of security features such as:-

1. Confidentiality: For making sensitive information more secure, it must be hidden from the unauthorized access. An attacker Eve wants to derive d_i from d_iP which is infeasible to solve ECDLP. Suppose he is able to get $h(m)$ and knows the seed value of curve, which is public to all still it is quiet infeasible to solve it.
2. Authentication: Authentication ensures that message received by user is the exact same sent by the sender and verifies the participants are who really claim to be. With regards to message authentication, the proposed scheme can prove the authenticity that is able to protect from malicious or unauthorized modification through a checksum at the receiver side. In this identities of the both the participating parties are verified by verifying the checksum $h = (ID_i\ ||U)$.
3. Integrity: In the proposed scheme, the receiver can very whether the message is sent by the sender or not. If the attacker change the cipher text $s\ to\ s'$. It is infeasible to obtain same digest for the two messages.
4. Unforgeability: It is difficult to forge the signature $\sigma(s, Y)$ for a message. In ECC, attacker selects random number k and prove multiple signature $(k + ed)P = Y + eX$.
5. Non-repudiation: The target of non-repudiation is to prevent the sender from denying the signature, he has done. Unforgeability implies non-repudiation.
6. Secure against forgery: The proposed scheme is secure against forgery attack as (David, 1999) scheme does not. For the attacker it is not possible to derive the private key $d_i = H(ID_i|r$. Because two different messages have different message digest. Due to ECDLP it is not possible to derive public key $X_i = d_iP$. When message signed by multiple signers, is received along with hash of senders and receiver identities prevent modification in the message.
7. Public verifiability: Multi signatures are valid only if $v1 == v2$. To forge the signature with equation $v1 = shp$, attacker has to solve the ECDLP, which is not possible.
$$v1 = shP$$
$$= \left(s = \sum_{i=1}^{N} S_i \ \ mod\ \ n \right) hP$$
$$= \ \ (\sum_{i=1}^{N} K_i\ )hP + e(\sum_{i=1}^{N} d_i\ )hP\ //S_i = K_i + ed_i$$
$$= (\sum_{i=1}^{N} Y_i\ \ ) + e\sum_{i=1}^{N} X_i\ \ )\ \ h\ //Y_i = K_ihP$$
$$= Y + eX$$
$$= \text{v2}$$
8. Forward Secrecy: Forward secrecy implies that regardless of the possibility that a private key of the sender gets compromised, still it won't be conceivable for someone to unsigncrypt the message that were signcrypted beforehand by the user. If the adversary $\mathcal{A}$ is able to possess private key d_i, still he is not able to retrieve previously send signed messages. For

https://doi.org/10.6703/IJASE.202109_18(5).010

accessing those messages, he needs value of r_i and its very difficult to retrieve value of k due to the ECDLP.

5. CONCLUSION

Digital signature refers to an electronic signature that have its usage to authenticate identity for online transaction like e-commerce (badotra, et al., 2020, Shobha et al.,2021) . In this paper we have proposed ECC based ID with multiple signature, which is more secure than (Devi et al., 2015; Chen et al., 2004). Forgery can be detected in the proposed scheme as secret key is derived from the hash of identity and a random number 〖d〗 _i=H(〖ID〗 _i |r). This can be extended by applying blind signature on message and signcryption. And it can be designed for multiple receivers.

REFERENCES

Badotra, S., Panda, S.N. 2019. Evaluation and comparison of OpenDayLight and open networking operating system in software-defined networking. Cluster Computing, 1–11.

Badotra, S., Panda, S.N. 2020. A survey on software defined wide area network. International Journal of Applied Science and Engineering, 17, 59–73.

Badotra, S., Panda, S.N. 2020. Experimental comparison and evaluation of various OpenFlow software defined networking controllers. International Journal of Applied Science and Engineering, 17, 317–324.

Badotra, S., Singh, J. 2017. A review paper on software defined networking. International Journal of Advanced Research in Computer Science, 8.

Badotra, S., Singh, J. 2017. Open daylight as a controller for software defined networking. International Journal of Advanced Research in Computer Science, 8

Badotra, S., Singh, J. 2019. Creating firewall in transport layer and application layer using software defined networking. In Innovations in Computer Science and Engineering, 95–103. Springer, Singapore.

Badotra, S., Nagpal, D., Panda, S.N., Tanwar, S., Bajaj, S. 2020. IoT-enabled healthcare network with SDN. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 38–42. IEEE.

Bi, W., Jia, X., Zheng, M. 2018. A secure multiple elliptic curves digital signature algorithm for blockchain. arXiv preprint arXiv:1808.02988.

Buenasmañanas Domínguez, F.J., Encinas, A.H., Queiruga Dios, A., Hernández Encinas, L. 2011. Digital identity-based multisignature scheme implementation. The First International Conference on Advanced Communications and Computation (INFOCOMP 2011), 42–45.

Chen, T.S., Huang, K.H., Chung, Y.F. 2004. Digital multi-signature scheme based on the elliptic curve cryptosystem. Journal of Computer Science and Technology, 19, 570–573.

Devi, D.S., Thilagavathy, K., Krishnan, P.S. 2015. An efficient and secure digital multi-signature protocol based on ECC. International Journal on Cryptography and Information Security (IJCIS), 5.

Devi, D.S., Sudendar, S. 2015. Privacy preserving analytics in outsourced healthcare system. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9.

Gangishetti, R., Gorantla, M.C., Das, M.L., Saxena, A. 2006. Identity based multisignatures. Informatica, 17, 177–186.

Harn, L., Ren, J. 2008. Efficient identity-based RSA multisignatures. computers & security, 27, 12–15.

ISO/IEC 14888-3, 1998. Information technology – securitytechniques – digital signatures with appendix. Part 3: Certificatebased-mechanisms, International Organization for Standardization, Geneva.

Koblitz, N. 1987. Elliptic curve cryptosystems. Mathematics of computation, 48, 203–209.

Mehibel, N., Hamadouche, M.H. 2021. Authenticated secret session key using elliptic curve digital signature algorithm. Security and Privacy, 4, p.e148.

Miller, V.S. 1985. Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques, 417–426. Springer, Berlin, Heidelberg.

Negi, A., Sharma, P., Chaudhary, P., Gupta, H. 2015. New method for obtaining digital signature certificate using proposed RSA algorithm. International Journal of Computer Applications, 121, 24–29.

Nia, M.A., Sajedi, A., Jamshidpey, A. 2014. An introduction to digital signature schemes. arXiv preprint arXiv:1404.2820.

Saritha, K. 2020. Block chain authentication using elliptic curve digital signature algorithm.

Shamir, A. 1984. Identity-based cryptosystems and signature schemes. In Workshop on the theory and application of cryptographic techniques, 47–53. Springer, Berlin, Heidelberg.

Shobha, G., Rana, A., Kansal, V., Tanwar, S. 2021. Code clone detection—A systematic review. Emerging Technologies in Data Mining and Information Security, 645–655.

Sharma, R., Mogha, M., Tanwar, S., Rana, A. 2020. Emerging part of industry 4.0: The digital and physical technology. In 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) (149–154). IEEE.

Singh, A.K., Solanki, A., Nayyar, A., Qureshi, B. 2020. Elliptic curve signcryption-based mutual authentication protocol for smart cards. Applied Sciences, 10, 8291.

Tanwar, S. 2017. A new pairing free ID based certificate less digital signature (CL-DS) scheme using elliptic curve cryptography. International Journal of Computer Science and Information Security (IJCSIS), 15.

Tanwar, S., Kumar, A. 2019. An efficient and secure identity based multiple signatures scheme based on RSA. Journal of Discrete Mathematical Sciences and Cryptography, 22, 953-971.

Thu, A.A., Mya, K.T. 2014. Implementation of an efficient blind signature scheme. International Journal of Innovation, Management and Technology, 5, 443.

Tianhuang, C., Xiaoguang, X. 2010. Digital signature in the application of e-commerce security. In 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT), 1, 366–369. IEEE.

Tsai, C.H., Su, P.C. 2017. An ECC-based blind signcryption scheme for multiple digital documents. Security and Communication Networks.

Wang, X., Bai, Y., Hu, L. 2015. Domain based certification and revocation. In Proceedings of the International Conference on Security and Management (SAM), 272–278. The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Yadav, N., Tanwar, S. 2013. Implementation of white-box cryptography in credit card processing combined with code obfuscation. International Journal of Computer Applications, 70.

Yang, F.Y., Lo, J.H., Liao, C.M. 2013. Improving an efficient ID-based RSA multisignature. Journal of Ambient Intelligence and Humanized Computing, 4, 249–254.