Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **3**, May **2017**

Mixed Symmetric Key and Elliptic Curve Encryption Scheme Used for Password Authentication and Update Under Unstable Network Environment

Wencui Chang[1], Haifeng Li[2,*] and Shou-Lin Yin[3]

[1]School of Information Technology and Engineering,
Jinzhong University
Jinzhong 030600, Shanxi, China

[2]School of Software
Dalian University of Technology
Dalian 116620, China
*Corresponding author:lihaifeng8848@mail.dlut.edu.cn

[3]Software College
Shenyang Normal University
Shenyang 110034, China

Received December, 2016; revised February, 2017

Abstract. *Data encryption scheme has been used widely in network communication. It mainly contains two encryption schemes: symmetric key encryption and asymmetric key encryption. Symmetric key encryption has the fast encryption character, while it cannot transmit key in unsafe channel due to the same encryption key and decryption key. On the contrary, asymmetric key encryption has the different encryption key and decryption key. But its encryption speed is too slow. Especially, the above schemes cannot effectively conduct secure password authentication and password update under unstable network environment when user logins remote management. To solve this question, we propose a mixed symmetric key and elliptic curve encryption scheme for password authentication and update. Our new scheme is composed of four stages: registration, password authentication, password update and session key distribution. In addition, it provides defence to answer various attack such as password guessing attack, server spoofing attack, data eavesdropping and replay attack. What's more, the new method generates a common symmetric key encryption, which needs less convergence time than traditional asymmetric key encryption. Finally, we give the performance and efficiency analysis for this new scheme. Also there are comparison experiments with the latest encryption schemes to demonstrate the effectiveness of our new method.*
Keywords: Symmetric key encryption, Asymmetric key encryption, Secure password authentication, Password update, Elliptic curve encryption

---

1. **Introduction.** Network is used for users to acquire various online services. However, lots of network systems are easily attacked by virous Hackers under this open environment. Therefore, secure password authentication and update[1-5] is introduced which can make server distinguish user in the unsafe communication channel. But it runs into many attack challenges. How to design a safe and effective password authentication and update scheme is an urgent problem. So many schemes are proposed by researchers. Islam [6] designed a dynamic identity-based three-factor password authentication scheme

using extended chaotic map in the random oracle model. The proposed scheme was provably secure based on the intractability assumption of chaotic map-based DiffieCHellman problem. Chen et al.[7] proposed a generic framework for designing four-party password-based authenticated key exchange (4PAKE) protocols. This new framework took a different approach from previous work, where the users were not required to have public key certificates, but they simply reused their login passwords, which they shared with their respective domain authentication servers. Meanwhile, the authentication servers, assumed to be part of a standard PKI, acted as ephemeral CAs that certified some key materials that the users could subsequently use to exchange and agree on as a session key. Moreover, he adopted a compositional approach. That is, by treating any secure two party password-based key exchange (2PAKE) protocol and two-party asymmetric-key/symmetric-key-based key exchange (2A/SAKE) protocol as black boxes, he combined them to obtain generic and provably secure 4PAKE protocols. Yin[8] presented a new certificateless aggregate signcryption(NCAS) scheme based on Exclusive OR(XOR). NCAS improved computation efficiency by reducing the computation number of bilinear pairings. Tang[9] proposed a public key scheme to defence password guessing attack, server spoofing attack, data eavesdropping etc. Yoon E J[10] presented an improved public key scheme to prevent from some weaknesses (i.e. replay attack, DoS attack) and distribute private key between user and server. However, the disadvantages in[10] are obvious. 1) Attacker steals password validator from the database of server and uses the offline guessing attack to acquire the correct password. 2) Attacker may use the same password and identifier to visit other servers, and begin internal attack by the user's password. 3) Attackers can use the server private key to decrypt data and get the original password of user. Then they directly start to imitation attack. 4) Attackers acquire the same ¡identifier, password¿ pair, then they can login server and have access to one account. Zhu[11] stated a new robust biometrics-based one-time identity-password (OTIP) authenticated key agreement protocol. Yie and Liu[12] proposed a new Map-Reduce model with k-means clustering of differential privacy protection, which adopted distributed computing functions provided by MapReduce model to improve clustering analysis efficiency in social network privacy protection. Mun[13] presented a new enhanced scheme that uses Elliptic Curve DiffieCHellman (ECDH) to overcome disadvantage with failing to achieve anonymity and perfect forward secrecy, and disclosing of legitimate user's password and improve performance.

The weakness of above schemes can be summarized as :

- Cannot defend data eavesdropping attack.
- Lack key distribution mechanism.
- User cannot freely select or set password.
- Remote authentication fails, because it is difficult to remember long-bit distance.
- It easily suffers from offline guessing attack with a short password.

Therefore, we propose a mixed symmetric key and elliptic curve encryption scheme for password authentication and update in this paper. New scheme combines the advantage of symmetric key and elliptic curve encryption. It can realize the mutual authentication and ensure forward, backward security. In addition, it defends various attack such as password guessing attack, internal attack, fake attack, server spoofing attack, data eavesdropping and replay attack. The followings are the structures of this paper. In section2, we give some preliminaries. Section3 detailed introduces the mixed symmetric key and elliptic curve encryption scheme. We give the security analysis and performance analysis in section4 and section5. There is a conclusion in section6.

2. **Preliminaries.**

2.1. **Ellipse curve cryptography.** In this paper, our scheme is based on ellipse curve group[14-16], and its security is based on computational Diffie-Hellman problem.

Supposing that F_p is a p element finite field. There are two elements a and b in F_p satisfying discriminant $\Delta = 4a^3 + 27b^2 \neq 0$. So ellipse curve can be written as $E(F_p)$ and it denotes the set of all the points (x, y) and infinity point O meeting Weierstrass equation $y^2 = x^3+ax+b$. Namely $E(F_p) = ((x, y)|x, y \in F_p \quad and \quad y^2 = x^3 + ax + b) \cup O$. Obviously, all the points in ellipse curve $E(F_p)$ consist of commutative group.

2.2. **Symmetric key encryption.** As we all know, symmetric key algorithm encrypt[17-18] and decrypt data using a single key. As shown in Figure1, the key and the plaintext message are passed to the encryption algorithm, generating a ciphertext. The result can be sent across an insecure medium, allowing only a recipient who has the original key to decrypt the message, which is done by passing the ciphertext and the key to a decryption algorithm. Obviously, the key must remain secret for this scheme to be effective.

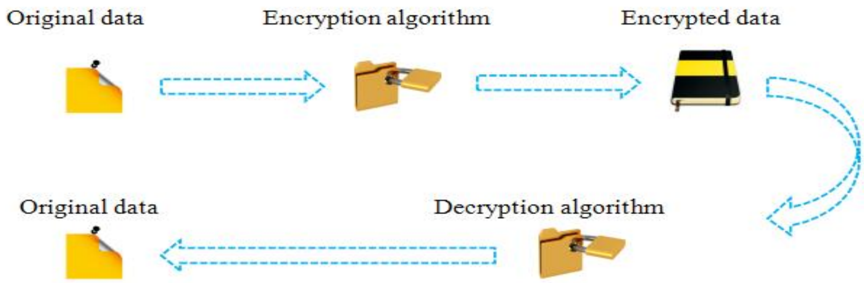

FIGURE 1. Symmetric key encryption

3. **Mixed symmetric key and elliptic curve encryption scheme.** In this paper, we use some symbols as in table1. New scheme includes four aspects: registration, password authentication, password update and session key distribution. Then we detailed introduce them respectively as follows.

TABLE 1. Parameters

Symbol	Explanation
ID_A	Identifier of user A
pw_A	Password of A
d_s	Private key of server S
$U_s = d_s \cdot G$	Public key of server S
$U_A = pw_A \cdot G$	Password validator of user A
K_s	Private key calculated by $K = pw_A \cdot U_s = (K_x, K_y)$
G	Base point of $n - order$ elliptic curve group, meet $n \cdot G = 0$
$H(\cdot)$	Anti-Collision one-way secure hash function
r_A and r_s	user and server randomly select number from $[1, n-1]$
$+$ and $-$	Addition and subtraction of Elliptic curve points

1. Registration stage. First, user A must use identifier ID_A and password validator U_A to register in server S. And A can get public key of server S. Then server storages identifier and password validator of each legal user and writes the state-bit of protection files. Where state-bit indicates the state of user(i.e. when user logins the server, it set the position of state-bit as 1. Otherwise, it is 0.). Table2 is the verification table.

Table 2. Verification table

Identifier	Password validator	State-bit	Identifier	Password validator	State-bit
ID_A	$U_A = pw_A \cdot G$	0/1	ID_C	$U_C = pw_C \cdot G$	0/1
ID_B	$U_B = pw_B \cdot G$	0/1	$\cdots$	$\cdots$	$\cdots$

2. Password authentication stage. This stage contains four steps.
   - From agent interface to server $ID_A, E_{K_x}(ID_A, R_A, W_A)$. User A puts the identifier ID_A and password pw_A into terminal services. User randomly selects a number r_A from $[1, n-1]$. Compute $R_A = r_A \cdot U_S$ and $W_A = (r_A \cdot pw_A) \cdot G$. Then user uses symmetric key K_x to encrypt (ID_A, R_A, W_A) and sends it to server. Encryption key K_x is the x-coordinate of $K = pw_A \cdot U_s = pw_A \cdot d_S \cdot G = (K_x, K_y)$.
   - From server to user $(W_A + W_S), H(W_S)$. Server uses $K = d_S \cdot U_A = pw_A \cdot d_s \cdot G = (K_x, K_y)$ to calculate decryption key K_x. Then server uses K_x to decrypt $E_{K_x}(ID_A, R_A, W_A)$. Server will compare the decrypted $ID_A, \hat{e}(R_A, U_A)$ to acquired $ID_A, \hat{e}(W_A, U_S)$. If the results meet all conditions, then server will randomly select a number r_S and compute $W_S = r_S \cdot U_S = r_S \cdot d_S \cdot G$. $(W_A + W_S), H(W_S)$ will be sent to user.
   - From agent interface to server $ID_A, H(W_A, W_S)$. User uses (W_A, W_S) to subtract W_A and gets W_S. If $W_S = H(W_S)$, user executes the hash operation $H(W_A, W_S)$ and sends it to server.
   - From server to user(we use symmetric key to encrypt the data): Access authorization or rejected. Server extracts hash value of W_S and W_A in step2. Compare it to acquired $H(W_A, W_S)$. If all the conditions meet requirement, it allows user to login.
3. Password update stage (Assuming that old password pw_A is absolute security).
   - From agent interface to server $ID_A, E_{K_x}(ID_A, R_A, W_A)$.
   - From server to user $(W_A + W_S), H(W_S)$.
   - From agent interface to server $ID_A, H(W_A, W_S), W_A + U'_A, H(W_S, U'_A)$.
   - From server to user: Password update authorization or rejected.

   If user wants to modify the password pw_A as pw'_A, then user needs to calculate corresponding password validator $U'_A = pw'_A \cdot G$. In step3, if password authorization $H(W_A, W_S)$ is verified, then server uses $W_A + U'_A$ to subtract W_A and gets new password validator U'_A. If hash value of (W_S, U'_A) is equal to $H(W_S, U'_A)$. Then U_A will be replaced by U'_A.
4. Session key distribution stage.
   - From agent interface to server $ID_A, E_{K_x}(ID_A, R_A, W_A)$.
   - From server to user $(W_A + W_S), H(W_S)$.
   - From agent interface to server $ID_A, H(W_A, W_S)$.
   - From server to user: Session key distribution authorization or rejected.

   In this protocol, user and server select a random number r_A and r_S from $[1, n-1]$ respectively. User computes the final session key and server calculates $SK = (r_S \cdot d_S) \cdot W_A = r_A \cdot r_S \cdot pw_A \cdot d_S \cdot G$.

3.1. **Correctness of new scheme.** Our scheme follows the bilinear pairings rule, which guarantees the correctness of new scheme. To proof $\hat{e}(R_A, U_A) = \hat{e}(W_A, U_S)$,

$$\hat{e}(R_A, U_A) = \hat{e}(r_A \cdot d_S \cdot G, pw_A \cdot G) = \hat{e}(G, G)^{r_A pw_A d_S}. \tag{1}$$

$$\hat{e}(W_A, U_S) = \hat{e}(r_A \cdot pw_A \cdot G, d_S \cdot G) = \hat{e}(G, G)^{r_A pw_A d_S}. \tag{2}$$

Therefore, $\hat{e}(R_A, U_A) = \hat{e}(W_A, U_S)$.

4. **Security analysis.** In this section, we analyze the security of new scheme. New scheme can defend various known password attacks and provide many security attributes.

1. Replay attack. Replay attack can be defined that attacker masquerades legal user to attack network through repeated using acquired information in previous protocol. In protocol, it encrypts W_A by symmetric key K_x. Only server and legal user can calculate it. If attacker wants to reuse old session information $(ID_A, E_{K_S}(ID_A, R_A, W_A))$ to masquerade a legal user, but he cannot acquire W_A and W_S and compute symmetry key $K = pw_A \cdot U_S = d_S \cdot U_A = (K_x, K_y)$. Because the key can be calculated from private key d_S of server, password validator U_A of user, user password pw_A and public key U_S of server. If attacker offers wrong information $H(W_A^*, W_S^*)$, then server can detect the information by comparing to $H(W_A, W_S)$. Therefore, this new scheme can defend the replay attack.
2. Password guessing attack. Password guessing attack is an important problem in the remote user authentication scheme based on password access. In fact, user always uses the low intensity password which is easily remembered. Low intensity password is usually cracked by attacker. So attacker can masquerade a legal user. In the proposed protocol, server uses write-protected file to storage password validator $U_A = pw_A \cdot G$. Attacker cannot get password pw_A from U_A. Therefore, this new scheme can defend the password guessing attack.
3. Imitation attack. Assuming that attacker makes a try to masquerade server to change the session key of legal user. Before intercepting data, attacker would run protocol message $E_{K_x}(ID_A, R_A, W_A)$. But attacker cannot acquire W_A from message, in that (ID_A, R_A, W_A) is only encrypted by symmetric key K_x only known by user and server. Then attacker uses the wrong message $(W_A^* + W_S^*, H(W_S^*))$ (where W_A^* and W_S^* are randomly selected by attacker.) to respond to user. After receiving message $(W_A^* + W_S^*, H(W_S^*))$, users compare the $H(W_A^* + W_S^* - W_A)$ with $H(W_S^*)$, the comparison result is inequality. Therefore, user stops the key distribution protocol. This new scheme can defend the imitation attack.
4. Attack of denial service. When user logins the account,he inputs wrong password. If the number of input password exceeds the limit value, then the server closes system logon session. However, account still can continuely arise login request until user provides correct password. In the process of password changing protocol, supposing that attacker uses (ID_A), $H(W_A, W_S)$, X and $H(W_S, U'_A)$ to replace (ID_A), $H(W_A, W_S)$, $W_A + U'_A$ and $H(W_S, U'_A)$ and sends it to server. Where X is the random elliptic curve point. After receiving (ID_A), $H(W_A, W_S)$, X and $H(W_S, U'_A)$, server computes $X - W_A$ and $H(W_S, X - W_A)$ and compares $H(W_S, X - W_A)$ with acquired $H(W_S, U'_A)$. But they are inequality. Therefore, server sends the wrong message of denial password update to user. So the new scheme can detect attack of denial service.
5. Multiple logged-in users. Assuming that several attackers have got the password pw and login identifier ID_A of user. In our scheme, only one attacker can login remote server and server sets its state position as 1. If other attackers try to use the same password and login identifier to login server at the same time, server will reject this request due to it state.
6. Server spoofing attack. In this attack, attacker may be disguised as one server to attain user's password and server's private key. Without $K = pw_A \cdot U_S = d_S \cdot U_A = (K_x, K_y)$ or password pw_A, it cannot calculate symmetry key d_S. In the first step of password authentication protocol, attacker cannot decrypt $ID_A, E_{K_x}(ID_A, R_A, W_A)$ to get W_A by using wrong key, so attacker will fail in third step. If attacker knows the

W_A accidentally, it still does not know the password due to the complex of ECDLP. Therefore, our scheme can defend server spoofing attack.

7. Perfect forward secrecy. In perfect forward secrecy, if private key of server and password of user are damaged, security of previous established session key should not be affected. Assuming that attacker obtains pw_A and d_S, he can calculate $K = pw_A \cdot U_S = d_S \cdot U_A = (K_x, K_y)$ and get W_A and W_S from message $ID_A, E_{K_x}(ID_A, R_A, W_A)$ and $(W_A + W_S), H(W_S)$ respectively. But attacker cannot obtain session key $SK = r_A \cdot r_S \cdot pw_A \cdot d_S \cdot G$. In order to get key SK, attacker tries to directly calculate $(W_A, W_S) = (r_A \cdot pw_A \cdot G, r_S \cdot d_S \cdot G)$. Due to the complex of DIffie-Hellman problem, attacker cannot get SK. In other words, although current session key is leaked, it depends on random number r_A and r_S, attacker cannot obtain old session key. So our scheme provides perfect forward secrecy.
8. Internal attack. Attacker steals the password identifer from server's verification table. Internal privileged users in server use legal login request to access to other server. Our scheme can maintain the password verification table including identifer ID_A and password identifer $U_A = pw_A \cdot G$. Attacker cannot get pw_A by computing. So attacker cannot generate symmetry key K_x.

   The internal privileged users can't pretend to be legitimate users. Due to without key K_x, privileged users are unable to authenticate identity through the remote server. So internal attack is infeasible with our new scheme.

5. **Performance analysis.** In this paper, we make a comparison to elliptic curve cryptography(ECC)[19], cyclic elliptic curve points sequence(CECPS)[20], Elliptic Curve Cryptography with Symmetric Algorithm(ECCSA)[21] with our scheme(SKECE) to demonstrate the security of our new scheme as table3. A_1 to A_8 are the security attribute descried in above section. Y denotes that scheme can prevent attack. N denotes that scheme cannot prevent attack.

Table 3. Security comparison with different schemes

Scheme	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
ECC	Y	N	N	N	Y	N	Y	N
CECPS	N	Y	N	Y	N	Y	Y	N
ECCSA	Y	Y	N	Y	Y	N	Y	N
SKECE	Y	Y	Y	Y	Y	Y	Y	Y

From table3, we can know that the new scheme can prevent any attack. Table4 is the comparison of calculation cost. In this paper, we compute total number of virtual operating and virtual computing time for each scheme. An asymmetric operation calculation is equivalent to one point operation (namely, 10^3 symmetric operation and 10^4 Hash operation). Setting one virtual operation is equivalent to one point operation (namely, 1 asymmetric=1 point=10^3 symmetric=10^3 virtual operation=10^4 Hash). So the executing time for asymmetric operation, symmetric operation and Hash operation are $5 \times 10^{-1}s$, $5 \times 10^{-4}s$ and $5 \times 10^{-5}s$ respectively. One virtual operating is equivalent to symmetric operation, so $1T = 5 \times 10^{-4}s$ virtual computing time. Asymmetric operation and symmetric operation are used in ECC, CECPS, ECCSA, which increase the calculation cost. But new scheme dose not use asymmetric operation and symmetric operation. Its virtual operating time is very low. Where H denotes Hash operation number. XOR denotes exclusive or operation number. S, A and P denote the asymmetric operation number, symmetric operation number and point operation number respectively.

Table 4. Calculation cost comparison with different schemes

Scheme	Total number of operation	virtual operating time
ECC	12H+7XOR+3S+4P	2.0014
CECPS	10H+5XOR+4S+5A	2.0621
ECCSA	12H+7XOR+4S+5A	2.3452
SKECE	17H+8XOR+3P	2.0003

6. **Conclusions.** In this paper, we propose a mixed symmetric key and elliptic curve encryption scheme for password authentication and update. This new scheme can effectively solve the imitate attack and clock synchronization etc. It can generate symmetric key and make reliable message exchange, in addition, it has low calculation cost. In the future, we will further improve the security of our scheme and reduce the calculation cost.

Acknowledgment. This work is supported by the Natural Science Foundation of China No.61472010,61602080.

REFERENCES

[1] C. L. Lin, T. Hwang A password authentication scheme with secure password updating, *Computers & Security*, vol. 22, no. 1, pp. 68-72, 2003.

[2] S. K. H. Islam, M. K. Khan, M. S. Obaidat, et al, Provably Secure and Anonymous Password Authentication Protocol for Roaming Service in Global Mobility Networks Using Extended Chaotic Maps, *Wireless Personal Communications,* vol. 84, no. 3, pp. 1-22, 2015.

[3] L. M. Surhone, M. T. Timpledon, S. F. Marseken Secure Password Authentication, *Betascript Publishing*, 2010.

[4] C. M. Chen, L. L. Xu, T. Y. Wu, and C. R. Li, On the Security of a Chaotic Maps-based Three-party Authenticated Key Agreement Protocol, *Journal of Network Intelligence*, vol. 1, no. 2, pp. 61-66, May 2016.

[5] C. M. Chen, W. Fang, K.H. Wang, T.Y. Wu, Comments on An improved secure and efficient password and chaos-based two-party key agreement protocol, *Nonlinear Dynamics*, vol. 87, no. 3, pp. 2073C2075, 2017.

[6] S. H. Islam Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps, *Nonlinear Dynamics*, vol. 78, no. 3, pp. 2261-2276, 2014.

[7] L. Chen, H. W. Lim, G. Yang, Cross-domain password-based authenticated key exchange revisited, *ACM Transactions on Information and System Security , no. TISSEC)*, vol. 16, no. 4, pp. 15, 2014.

[8] S. L. Yin, H. Li and J. Liu. A New Provable Secure Certificateless Aggregate Signcryption Scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1274-1281, November 2016.

[9] Q. Tang, H. Ma, X. Chen, Extend the Concept of Public Key Encryption with Delegated Search, *Computer Journal*, vol. 58, no. 4, pp. 724-734, , 2013.

[10] E. J. Yoon, E. K. Ryu, K. Y. Yoo Further improvement of an efficient password based remote user authentication scheme using smart cards, *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 612-614, 2004.

[11] H. Zhu, Y. Xia, H. Li, An Efficient and Secure Biometrics-Based One-Time Identity-Password Authenticated Scheme for E-Coupon System Towards Mobile Internet, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 6, no. 3, pp. 444-457, , 2015.

[12] S. L. Yin and J. Liu, A K-means Approach for Map-Reduce Model and Social Network Privacy Protection, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, November 2016.

[13] H. Mun, K. Han, S. L. Yan, et al. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks, *Journal Mathematical & Computer Modelling* , vol. 55. no.(1C2), pp. 214-222, 2012.

[14] S. Kamienny, F. Najman, Torsion groups of elliptic curves over quadratic fields, *Revista de la Real Academia de Ciencias Exactas, Fsicas y Naturales. Serie A. Matemáticas*, vol. 152, no. 1), pp. 291-305, 2016.

[15] V. Chandee, C. David, D. Koukoulopoulos, et al., The frequency of elliptic curve groups over prime finite fields, *Canadian Journal of Mathematics*, 2014.

[16] T. Fisher, R. Newton, Computing the CasselsCTate pairing on the 3-Selmer group of an elliptic curve, *Mathematics*, vol. 10, no. 7, pp. 1881-1907, 2014.

[17] K. Sindhuja, S.Pramela Devi, A Symmetric Key Encryption Technique Using Genetic Algorithm, *International Journal of Computer Science & Information Technolo*, 2014.

[18] S. Ahmad, K. M. R. Alam, H. Rahman, et al., A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets, *International Conference on NETWORKING Systems and Security. IEEE*, pp. 1-5, 2015.

[19] S. H. Islam, G. P. Biswas Design of improved password authentication and update scheme based on elliptic curve cryptography, *Mathematical & Computer Modelling*, vol. 57, no. 11C12, pp. 2703-2717, 2013.

[20] S. Sowmya, S. V. Sathyanarayana Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)*International Conference on Contemporary Computing and Informatics. IEEE*, pp. 137-150, 2014.

[21] Y. S. Lee, E. Alasaarela, H. J. Lee, An Efficient Encryption Scheme using Elliptic Curve Cryptography (ECC) with Symmetric Algorithm for Healthcare System, *International Journal of Security & Its Applications*, vol. 8, no. 3, pp. 63-70, 2014.