Journal of Computer Sciences

Original Research Paper

A CAE Scheme Using ECC Based Self Certified PKC

[1,2]Manoj Kumar Chande, [3,4]Cheng-Chi Lee and [5]Chun-Ta Li

[1]School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur, 492010, Chhattisgarh, India
[2]Shri Shankaracharya Institute of Professional Management and Technology Raipur, 492015, Chhattisgarh, India
[3]Department of Library and Information Science, Fu Jen Catholic University No. 510, Jhongjheng Road, New Taipei City 24205, Taiwan, R.O.C., Taiwan
[4]Department of Photonics and Communication Engineering, Asia University No. 500, Lioufeng Road, Taichung City 41354, Taiwan, R.O.C., Taiwan
[5]Department of Information Management, Tainan University of Technology No. 529, Zhongzheng Road, Tainan City 71002, Taiwan, R.O.C., Taiwan

Article history
Received: 30-04-2016
Revised: 26-11-2016
Accepted: 22-12-2016

Corresponding Author:
Cheng-Chi Lee
Department of Library and Information Science, Fu Jen Catholic University No. 510, Jhongjheng Road, New Taipei City 24205, Taiwan, R.O.C., Taiwan and
Department of Photonics and Communication Engineering, Asia University No. 500, Lioufeng Road, Taichung City 41354, Taiwan, R.O.C., Taiwan
Email: cclee@mail.fju.edu.tw

Abstract: The Convertible Authentication Encryption (CAE) scheme, allows the signer to generate an authentic ciphertext signature, which can be recuperated and validated by a specific recipient only. In case of any kind of dispute the recipient is capable enough to convert the ciphertext signature as a normal signature and that can be validated publicly. The CAE schemes are used for transformation of confidential information over insecure networks, because they provide confidentiality, authenticity and integrity for the transmitted message or information. We propose a new CAE scheme by integrating the concepts of ECC- based self-certified public keys and encryption scheme. The security analysis shows that the proposed CAE scheme fulfill the basic security conditions such as indistinguishability of ciphertext signature, unforgeability and non-repudiation. The performance analysis shows that our proposed CAE scheme has little advantage over Wu and Lin scheme regarding computational complexity and timings.

Keywords: Convertible Authentication, Elliptic Curve, Elliptic Curve Discrete Logarithm Problem, Self-Certified Key

Introduction

Diffie and Hellman (1976), introduced the public key cryptosystem (PKC) and cryptographic security of their PKC rely on the intractability of the Discrete Log Problem (DLP). In this system, every participant compute a public key, corresponding to his secret key. This system is not safe, because, an adversary can attack by replacing a forge public key. To avoid such attacks, a certificate-based approach is used, in which the Certifying Authority (CA) can generate a certificate and authenticate public keys of each user. This approach is costly due to additional communication and computation costs. Shamir (1984), introduced the Identity based (ID-based) PKC. In this approach every users public key is his public identity, so no need to put extra efforts for checking certificates. In this ID-based approach private key of user is derived by the Private Key Generator (PKG). No one has the valid secret key, without the secret trapdoor value from PKG. One of the negative aspects of this approach is, the PKG can masqueraded as a legal user without being detected, because he has the control over secret key of each user. To eliminate was of the previous approaches, Girault (1991), proposed a novel system for public keys, which is known as Self-Certified Public Key (SCPK) system. In SCPK system, the tasks of the public key validation and the signature validation can be done in only one step, which cut down the computation as well as communication cost. SCPK approach is cost optimizing and more efficient than certificate and identity based approach.

Koblitz (1987) and Miller (1985), independently introduced Elliptic Curve Cryptosystem (ECC). The significant difference from the other traditional PKC is that, much shorter keys provide similar security. This will help in faster execution of algorithms and also requirement of bandwidth is reduced. ECC is useful in such situation where the storage space and computational power is limited. Tsaur (2005), presented an effectual ECC based SCPK cryptosystem.

The presented cryptosystem combine the merits of ID-based SCPK and ECC.

The confidentiality of the transmitted message in any electronic communication or transaction is very crucial. At the same time it is also important that the message is being received by only the designated receiver. No other entity is able to recuperate the original message and check the genuineness of the signature attached with the message. Horster *et al*. (1994), introduced the concept of Authenticated Encryption (AE) scheme which encrypt and authenticate message simultaneously in a very efficient manner. One of the draw backs of their scheme is non - repudiation, because, the message recipient is not able to prove that the message he receives is sent by the specified user only. Zheng (1997), in his paper gave a new method for AE called signcryption. In his approach the parties involved (Message signer, Message receiver and Third party) have more interaction than the Horster *et al*. (1994). In this way the problem of non-repudiation is removed. This method of Zheng (1997), is a little costly regarding both computational and communication cost. Petersen and Michels (1998), found that there is lack of confidentiality in the Zheng (1997), scheme and then proposed an improved scheme. He and Wu (1999), showed that, the scheme of Petersen and Michels (1998), failed to satisfy unforgeability property and improve their scheme further. Araki *et al*. (1999), presented a signature scheme equipped with convertibility, which differ from usual AE. In their scheme the process of signature conversion requires some extra information from the actual signer. This approach is not successful, if the signer doesn't want to co-operate. Wu and Hsu (2003), proposed an efficient CAE scheme, in which the conversion procedure is very easy and only recipient can solely manage this process, without any heavy computation. Huang and Chang (2003), point out that Wu and Hsu (2003), scheme is not safe, since the adversary is capable of signature conversion, if he has the knowledge of the actual message and project an improvised scheme. Unfortunately, Wang *et al*. (2004), scheme given by Huang and Chang (2003), is also insecure against known plain text attack. They analyzes that a new ciphertext can be decrypted by an adversary, if he has an idea of some of the of previous valid ciphertext. Lv *et al*. (2005), finds security was in Wu and Hsu (2003) and Huang and Chang (2003), schemes and presented better schemes based on SCPK. Shao (2006), realize the weakness of Lv *et al*. (2005), scheme and then puts forward a new scheme. Wu and Lin (2008), presented an ECC based new CAE scheme using SCPK. Next year Lee *et al*. (2009), presented a new CAE scheme, on the basis of ElGamal cryptosystem, but unfortunately Lin *et al*. (2011), have demonstrated that their scheme fail, to resist the chosen plain text attack and then presents a better variant with provable security. Further in recent years other variants (Hsu and Lin, 2014; Huang *et al*., 2015; Lin, 2015; Liu *et al*., 2015; Wu *et al*., 2013), of CAE scheme, based on different assumption and mathematical problems are proposed by researchers.

In this study using the merits of ECC-based SCPK we design a new CAE scheme. The rest of the paper is structured as: Next section, is about the prerequisite mathematical background. Our proposed CAE scheme is given in section 3. The discussion regarding security of the proposed scheme and its performance is given in section 4 and at last, the final section concludes our paper.

Mathematical Background

Our CAE scheme is based on ECC and security of the our scheme rely on ECDLP and OWHF, therefore these preliminaries are precisely defined as follows:

Elliptic Curve (EC)

The elliptic curve denoted by E, is of the form:

$$y^2 = c^3 + ax + b,\ a,b \in F_p$$

Provided $4a^3+27b^2 \neq 0$: The points on EC, together a special point O at infinity form a cyclic group under addition operation. The order of group G is n. Let us consider two points $P = Q \in G$, on the straight line L, this line becomes tangent line if $P = Q$. If $P = Q$ or $P \neq Q$, in both the situation point addition formulaes are defined. Scalar multiplication for the points on E is also defined. For elliptic curve algebra interested readers may refer (Stallings, 2011).

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let us consider an elliptic curve E, which is defined over a finite field F_p, where p is a large prime. Suppose a point P of prime order n on E and the other point Q is such that $Q = \alpha P$ for some integer α. The ECDL problem is that, if Q, is given then find α. Select p, E and P, such that the solution of ECDLP is infeasible.

One Way Hash Function (OWHF)

The OWHF defined as:

$$h:\{0,1\}^* \rightarrow \{0,1\}^n$$

The input for h may be of variable length, but its output is of fixed length. The resultant hash of the message is known as hash value or message digest (Stallings, 2011). Characteristics of OWHF are as follows:

- The hash function can be used for any arbitrary length of message

- For any particular value x, the value of $h(x)$, can be calculate effortlessly. But from known value of $h(x)$, to find x is mathematically infeasible, that's why it is called OWHF
- The hash function takes strings of arbitrary length as input and gives output of fixed length strings by using the mapping defined
- For a particular input value x, finding different value y, is mathematically infeasible, for which $h(y)$ and $h(x)$, are equal
- Computationally is not possible to find distinct elements x and y, for which $h(x) = h(y)$

Proposed CAE Scheme

The System Setup Phase

The system parameters generated by System Authority (SA) and their notations are as follows:

Notation	Description
F_p	A finite field, where field size p is prime and typically very large.
E	Represents an elliptic curve, over finite field F_p.
P	Represents the base point of $E(F_p)$, with order q, where q is prime and very large.
$h(\cdot)$	A secure OWHF, for which input may vary in length, but output is of a static length $l \in [2, q\text{-}2]$.
γ	The private key of SA.
Q	The public key of SA and $Q = \gamma P$.
U_i	Represents the user.
x_i	Denote the private key of U_i.
Y_i	Denote the public key of U_i.
ID_i	The identity information associated with user U_i.
$\|\|$	Concatenation of two strings.

All the above system parameters are published, but secret key of each user and SA, should be kept secret. Hash $h(P)$, of an elliptic curve point P, means $h(P_x \| P_y)$, where $P = (P_x, P_y)$.

User Registration (UR) Phase

Let the user U_i, along with his identity information ID_i, would like to register with SA. For this every user performs the following steps:

The user U_i, first select $t_i \in [2, q\text{-}2]$, as the master key and compute:

$$V_i = h\left(t_i \| ID_i P\right) \tag{3.1}$$

Then transmit (V_i, ID_i), to SA.

Now SA selects an integer $z_i \in [2, q\text{-}2]$ and calculates a public key Y_i and corresponding witness w_i for each U_i respectively as:

$$Y_i = V_i + \left\{z_i - h\left(ID_i\right)\right\}.P = \left(Y_{ix}, Y_{iy}\right) \tag{3.2}$$

$$w_i = z_i + \gamma.\left\{\left(Y_{ix} + h\left(ID_i\right)\right) \bmod q\right\} \tag{3.3}$$

The send (Y_i, w_i) to U_i.

Every user U_i, computes his secret key x_i and check its validity as:

$$x_i = w_i + h\left(t_i \| ID_i\right) \bmod q \tag{3.4}$$

$$x_i P = Y_i + h\left(ID_i\right)P + \left[\left\{Y_{ix} + h\left(ID_i\right)\right\} \bmod q\right] \cdot Q \tag{3.5}$$

If the above equation holds then, U_i accepts (x_i, Y_i) as his secret and public key.

Theorem 1

The secret key xi and public key Y_i of the user U_i satisfy the Equation 3.5.

Proof

We have from the Equation 3.5:

$$\begin{aligned}
RHS &= Y_i + h\left(ID_i\right)P + \left[\left\{Y_{ix} + h\left(ID_i\right)\right\} \bmod q\right] \cdot Q \\
&= V_i + \left\{z_i - h\left(ID_i\right)\right\} \cdot P + h\left(ID_i\right)P + \left[\left\{Y_{ix} + h\left(ID_i\right)\right\} \bmod q\right] \cdot Q \\
&= V_i + z_i P + \gamma\left[\left\{Y_{ix} + h\left(ID_i\right)\right\} \bmod q\right] \cdot P \\
&= h\left(t_i \| ID_i\right)P + z_i P + \gamma\left[\left\{Y_{ix} + h\left(ID_i\right)\right\} \bmod q\right] \cdot P \\
&= h\left(t_i \| ID_i\right)P + \left[z_i + \gamma\left\{Y_{ix} + h\left(ID_i\right)\right\} \bmod q\right] \cdot P \\
&= h\left(t_i \| ID_i\right)P + w_i P \bmod q \\
&= x_i P
\end{aligned}$$

The Signature Generation and Verification (SGV) Phase

Suppose a user U_a wants to transmit U_b an authenticated ciphertext for the message M with embedded redundancy. To do this U_a, chooses first an integer $k \in [2, q\text{-}2]$ and computes:

$$C = k \cdot \begin{Bmatrix} Y_b + h\left(ID_b\right) \cdot P \\ + \left[\left\{Y_{bx} + h\left(ID_b\right)\right\} \bmod q\right] \cdot Q \end{Bmatrix} = \left(C_x, C_y\right) \tag{3.6}$$

$$r_1 = M \cdot h\left(C\right)^{-1} \bmod q \tag{3.7}$$

$$r_2 = h\left(M, h\left(k \cdot P\right), C\right) \bmod q \tag{3.8}$$

$$S = k - x_a \cdot r_2 \bmod q \tag{3.9}$$

The tuple (r_1, r_2, S), is the signature for M and is then send to U_b, after receiving this signature (r_1, r_2, S), U_b compute:

$$K = r_2 \cdot \begin{Bmatrix} Y_a + h\left(ID_a\right) \cdot P \\ + \left[\left\{Y_{ax} + h\left(ID_a\right)\right\} \bmod q\right] \cdot Q + S \cdot P \end{Bmatrix} \tag{3.10}$$

$$= \left(r_2 \cdot x_a + S\right) \cdot P \tag{3.11}$$

$$C_1 = x_a \cdot K = \left(K_x, K_y\right) \tag{3.12}$$

The message M, can be recovered as:

$$M = h\left(C_1\right) \cdot r_1 \bmod p \tag{3.13}$$

Next, U_b can verify the signature (r_1, r_2, S) through the equation:

$$r_2 = h\left\{M, h\left(K\right), C_1\right\} \bmod q \tag{3.14}$$

If this equation holds then only the signature is valid, simultaneously the public key Y_a of signer U_a is also authenticated.

Theorem 2

The signature recipient U_b, can recover the message M, with the embedded redundancy with Equation 3.13.

Proof

We have from the Equation 3.13:

$$\begin{aligned}
RHS &= h\left(C_1\right) \cdot r_1 \bmod q \\
&= h\left(x_b \cdot K\right) \cdot r_1 \bmod q \\
&= h\left(x_b \cdot r_2 \cdot \begin{Bmatrix} Y_a + h\left(ID_a\right) \cdot P \\ + \left[\left\{Y_{ax} + h\left(ID_a\right)\right\} \bmod q\right] \cdot Q + S \cdot P \end{Bmatrix} \cdot r_1 \right) \bmod q \\
&= h\left\{\left(x_b \cdot \left(r_2 \cdot x_a \cdot P + S \cdot P\right)\right)\right\} \cdot r_1 \bmod q \\
&= h\left\{\left(x_b \cdot \left(k - S\right) \cdot P + S \cdot P\right)\right\} \cdot r_1 \bmod q \\
&= h\left(x_b \cdot k \cdot P\right) \cdot r_1 \bmod q \\
&= h\left(C\right) \cdot r_1 \bmod q \\
&= M \\
&= LHS
\end{aligned}$$

Theorem 3

The signature (r_1, r_2, S), must satisfy the Equation 3.14, through this equation the public key Y_a automatically get authenticated.

Proof

We have from the Equation 3.14:

$$\begin{aligned}
RHS &= h\left\{M, h\left(K\right), C_1\right\} \bmod q \\
&= h\left[M, h\left\{\left(r_2 \cdot x_a + S\right) \cdot P\right\}, x_b \cdot K\right] \bmod q \\
&= h\left[M, h\left(k \cdot P\right), x_b \cdot K\right] \bmod q \\
&= h\left[M, h\left(k \cdot P\right), x_b \cdot \left(r_2 \cdot x_a + S\right) \cdot P\right] \bmod q \\
&h\left[M, h\left(k \cdot P\right), x_b \cdot \left(k \cdot P\right)\right] \bmod q \\
&= h\left[M, h\left(k \cdot P\right), C\right] \bmod q \\
&= LHS
\end{aligned}$$

The Signature Conversion (SC) Phase

In circumstances of some dispute or disagreement, U_b the signature receiver can simply release the converted signature (r_2, S, C_1) and the recuperated M. Suppose someone is validating the signature, first he will have to calculate K, through Equation 3.10, then check the signature through Equation 3.14. If Equation 3.14, holds then only he assures that the signature is generated by U_a only.

The Signature Recipient Proof (RP) Phase

Let the signature recipient U_b, is looking to convince some other user U_c, that he is the actual recipient, to do this U_b perform the following computations:

- The user U_b, sends the converted signature (r_2, S, C_1) to U_c
- The other user U_c, calculate K through Equation 3.10, then check the signature through Equation 3.14. If this equation holds, then only U_c proceed further
- U_c, chooses an integer d randomly and compute:

$$E = d \cdot K$$

  and then send E to U_b.

- After receiving E, U_b computes:

$$Q = x_b \cdot E$$

  and send back Q to U_c.

- Now U_c computes $Q' = d \cdot C_1$ and compare Q with Q', if $Q = Q'$, then only U_c accept of the that U_b is the specified recipient

Security and Performance Analysis

This section is divided into two subsection, in the first the cryptographic security of the proposed CAE scheme is analyzed and in the second, performance of our scheme is analyzed.

Security Analysis

First of all we show that our scheme is secure against some active attacks. The safety of our scheme is due to ECDLP and OWHF. We focus on the three security properties namely: Confidentiality, non-repudiation and unforgeability.

Confidentiality

The confidentiality of the secret key (γ) of SA, is maintained due to ECDLP. If some attacker is looking to get secret key γ, through public key $Q = \gamma P$, of SA, or from Equation 3.3 of the registration phase, then the attacker will have to encounter the intractability of the ECDLP. It is difficult to obtain from Equation 3.3, because of random value z_i, which is also secured due to ECDLP through Equation 3.2. Same level of difficulty will have to faced to obtain from Equation 3.4.

To break the confidentiality of recovered message M, the attacker has to retrieve the key Y_{ab}, from the Equation 3.10 and 3.12, but again he will have to solve ECDLP to achieve this goal.

The proposed CAE, keep indistinguishability of the confidentiality. The attacker cannot distinguish the particular message from the two messages M_1,M_2. To distinguish the messages attacker will have to verify the Equation 3.14 and it is not mathematically feasible for him, due to unavailability of secret key x_b. So in this way the authenticated encryption messages are indistinguishable.

Non-Repudiation

The designated signature recipient U_b, can only validate the signature tuple (r_1, r_2, S) generated by the signer U_a only. In the circumstances of some dispute, the receiver can transmit the tuple (r_2, S, C_1) to a particular one whom the recipient would like to convince that the signature is generated by U_a. From signature generation phase it is clear that the signature is generated using the secret key of U_a and U_b, that's why it is not possible for them to deny their participation.

Unforgeability

To forge a genuine signature (r_1, r_2, S), for a random message of his choice M_0, an adversary will have to select randomly (r'_2, S'), then compute K', which satisfy the Equation 3.10. After this he will have to choose a new value C'_1, using this value he can compute r'_1 which satisfy the Equation 3.13. The randomly selected values chosen (r'_2, S'), cannot satisfy the Equation 3.14. Due to the intractability of ECDLP, it is not feasible to find out the secret key (x_b), of the signer to forge a genuine signature.

Forgery of the public key from Equation 3.5, is impossible for an adversary because of the secured assumptions of the OWHF and ECDLP.

Performance Analysis

To describe the algorithmic complexity of our scheme, we use the subsequent notations.

Notation	Description
T_h	The time taken for hashing.
T_m	The time taken to compute modular multiplication.
T_i	The time taken to compute modular inversion.
T_{EA}	The time taken to perform modulo addition over elliptic curve.
T_{EM}	The time taken to perform scalar multiplication to a point on elliptic curve.

The Table 1, shows the time complexity of our proposed scheme is less than the Wu and Lin (2008) scheme. The communication costs are same for both schemes.

The Table 2, shows the computational timings. The computational timing calculation is based on (Ramasamy and Prabakar, 2011). The communication costs are same for both schemes.

As it is clear from the Table 2, that every stage of our scheme is cost efficient than the corresponding stages of Wu and Lin (2008) scheme. Overall time consumption of our scheme is reduced by approximately 6% than Wu and Lin (2008) scheme.

Table 1. Comparison of computational complexity

Phase	User	Wu and Lin (2008)	Our
UR	U_i	$3T_h + 2T_{EA} + 4T_{EM}$	$2T_h + 2T_{EA} + 4T_{EM}$
	SA	$2T_h + T_i + T_m + T_{EA} + 2T_{EM}$	$T_h + T_m + T_{EA} + T_{EM}$
SGV	U_a	$5T_h + 2T_i + 3T_m + T_{EA} + 4T_{EM}$	$4T_h + 2T_m + T_i + 2T_{EA} + 4T_{EM}$
	U_b	$5T_h + T_m + 2T_{EA} + 5T_{EM}$	$4T_h + T_m + 3T_{EA} + 5T_{EM}$
SC	U_b	0	0
RP	U_b	T_{EM}	T_{EM}
	U_c	$4T_h + 2T_{EA} + 6T_{EM}$	$4T_h + 2T_{EA} + 6T_{EM}$
Grand Total		$19T_h + 3T_i + 5T_m + 8T_{EA} + 22T_{EM}$	$15T_h + 4T_m + T_i + 10T_{EA} + 21T_{EM}$

Table 2. Comparison of computational timings (In ms)

Phase	User	Wu and Lin (2008)	Our	Difference
UR	U_i	182.109414	180.595688	1.513726
	SA	95.960177	47.515748	48.444429
SGV	U_a	194.797950	189.299679	5.498271
	U_b	230.974826	229.625162	1.349664
SC	U_b	0.0	0.0	0.0
RP	U_b	44.310028	44.310028	0.0
	U_c	272.243196	272.243196	0.0
Grand Total		1020.395591	963.589501	56.806090

Conclusion

In this study a new CAE scheme based on ECC and self-certified PKC is proposed. This scheme is computationally indistinguishable and security is based on ECDLP and OWHF. This scheme has advantage over certificate based approach, since no extra efforts are required to verify certificates. The task of signature verification and authentication of the public key can be performed in single step. If there will be some dispute then the signature recipient is able to prove his genuineness to this third party. The receiver of signature is also able to transform the signature into a usual signature with very little computational efforts. The previous section shows that the proposed scheme satisfies the basic security properties. The performance analysis shows that the proposed CAE scheme has little advantage over Wu and Lin ECC- based CAE scheme, regarding time complexity. The use of ECC gives an advantage, if availability of storage and computational resources is limited like personalized digital gadgets.

Acknowledgment

The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other author have read and approved the manuscript and no ethical issues involved.

References

Araki, S., S. Uehara and K. Imamura, 1999. The limited verifier signature and its application. IEICE Trans. Fundamentals, E82-A: 63-68.

Diffe, D. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654. DOI: 10.1109/TIT.1976.1055638

Girault, M., 1991. Self-certified public keys. Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques, Apr. 08-11, Springer, Brighton, UK, pp: 491-497. DOI: 10.1007/3-540-46416-6_42

He, W.H. and T.C. Wu, 1999. Cryptanalysis and improvement of Petersen-Michels signcryption scheme. IEE Proc. Comput. Digital Tech., 146: 123-124. DOI: 10.1049/ip-cdt:19990198

Horster, P., M. Michel and H. Peterson, 1994. Authenticated encryption schemes with low communication costs. Electron. Lett., 30: 1212-1213. DOI: 10.1049/el:19940856

Hsu, C.L. and H.Y. Lin, 2014. Convertible authenticated encryption scheme with hierarchical access control. Applied Math. Inf. Sci., 8: 1239-1246. DOI: 10.12785/amis/080338

Huang, H.F. and C.C. Chang, 2003. An efficient convertible authenticated encryption scheme and its variant. 5th International Conference on Information and Communications Security, Oct. 10-13, Springer, Huhehaote, China, pp: 382-392. DOI: 10.1007/978-3-540-39927-8_35

Huang, H.F., P.H. Lin and M.H. Tsai, 2015. Convertible multi-authenticated encryption scheme for data communication. IJ Netw. Security, 17: 40-8.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209. DOI: 10.1090/S0025-5718-1987-0866109-5

Lee, C.C., M.S. Hwang and S.F. Tzeng, 2009. A new convertible authenticated encryption scheme based on the elgamal cryptosystem. Int. J. Foundat. Comput. Sci., 20: 351-359. DOI: 10.1142/S0129054109006607

Lin, H.Y., 2015. RPCAE: A novel revocable proxy convertible authenticated encryption scheme. Int. J. Inform. Security, 14: 431-441. DOI: 10.1007/s10207-014-0269-2

Lin, H.Y., C.L. Hsu and S.K. Huang, 2011. Improved convertible authenticated encryption scheme with provable security. Inform. Process. Lett., 111: 661-666. DOI: 10.1016/j.ipl.2011.03.021

Liu, G., Y. Liu, C. Liu and Z. Shi, 2015. Improved convertible multi-authenticated encryption scheme. J. Inform. Comput. Sci., 12: 3231-3240. DOI: 10.12733/jics20105853

Lv, J., X. Wang and K. Kim, 2005. Practical convertible authenticated encryption schemes using self-certified public keys. Applied Math. Comput., 169: 1285-1297. DOI: 10.1016/j.amc.2004.10.057

Miller, V., 1985. Use of elliptic curves in cryptography. Proceedings of the Advances in Cryptology, Aug. 18-22, Springer, London, UK., pp: 417-426. DOI: 10.1007/3-540-39799-X_31

Petersen, H. and M. Michels, 1998. Cryptanalysis and improvement of signcryption schemes. IEE Proc. Comput. Digital Tech., 145: 149-151. DOI: 10.1049/ip-cdt:19981862

Ramasamy, R.R. and M.A. Prabakar, 2011. Digital signature scheme with message recovery using knapsack-based ECC. Int. J. Netw. Security, 12: 7-12.

Shamir, A., 1984. Identity-based cryptosystems and signature schemes. Proceedings of the Advances in Cryptology, Aug. 19-22, Springer, Santa Barbara, California, USA., pp: 47-53. DOI: 10.1007/3-540-39568-7_5

Shao, Z., 2006. Cryptanalysis and improvement of practical convertible authenticated encryption schemes using self-certified public keys. Informatica, 17: 577-586.

Stallings, W., 2011. Cryptography and Network Security: Principles and Practice. 5th Edn., Prentice Hall, Boston, ISBN-10: 0136097049, pp: 719.

Tsaur, W.J., 2005. Several security schemes constructed using ECC-based self-certified public key cryptosystems. Applied Math. Comput., 168: 447-454. DOI: 10.1016/j.amc.2004.09.010

Wang, G., R.H. Deng, D. Kwak and D. Moon, 2004. Security analysis of two signcryption schemes. Proceedings of the 7th International Conference on Information Security, Sept. 27-29, Springer, USA, pp: 123-133. DOI: 10.1007/978-3-540-30144-8_11

Wu, T.S. and C.L. Hsu, 2003. Convertible authenticated encryption scheme. J. Syst. Software, 62: 205-209. DOI: 10.1016/S0164-1212(01)00143-1

Wu, T.S. and H.Y. Lin, 2008. ECC based convertible authenticated encryption scheme using self-certified public key systems. Int. J. Algebra, 2: 109-117.

Wu, T.S., H.Y. Lin, S.H. Tsao and P.Y. Ting, 2013. On the construction of DL-based convertible authenticated encryption scheme with message linkages. Information, 16: 7983-7994.

Zheng, Y., 1997. Signcryption and its applications in efficient public key solutions. Proceedings of the 1st International Workshop on Information Security, Sept. 17-19, Springer, Japan, pp: 291-312. DOI: 10.1007/BFb0030430