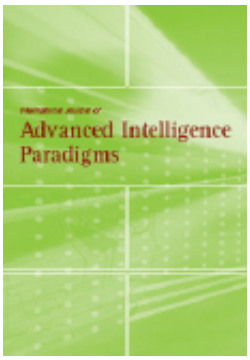


International Journal of Advanced Intelligence Paradigms

ISSN online: 1755-0394 - ISSN print: 1755-0386
https://www.inderscience.com/ijaip

Advanced cryptography technique in certificateless environment using SDBAES

C.G. Naveen Kumar, C. Chandrasekar

DOI: 10.1504/IJAIP.2018.10021467

Article History:

Received:	11 May 2018
Accepted:	03 June 2018
Published online:	22 February 2024

Advanced cryptography technique in certificateless environment using SDBAES

C.G. Naveen Kumar*

Department of Computer Science,
Bharathiar University,
Coimbatore, 641046, India
Email: navecg@gmail.com
*Corresponding author

C. Chandrasekar

Department of CS&E,
Government Arts College,
Udumalpet, Tamilnadu, 642126, India
Email: chandrasekar2000@gmail.com

Abstract: Certificateless encryption is a kind of public key encryption which is used to eliminate the disadvantage of traditional PKI-based public key encryption scheme and identity-based encryption scheme. The existing certificateless environment contains the lack of security which leads to the numerous security issues. Also the existing system does not provide the efficient certificateless environment in terms of time and performance. To reduce such issues, the proposed work used the SDBAES algorithm which is used to reduce the maximum of the security threats in the cloud. It is also used to increase the efficiency of the system by reducing the time and improving the performance. The experimental results show that the proposed work provides higher security and efficiency than the existing technique.

Keywords: EMV-CLSC; CLSC; IBAS; SDBAES.

Reference to this paper should be made as follows: Naveen Kumar, C.G. and Chandrasekar, C. (2024) 'Advanced cryptography technique in certificateless environment using SDBAES', *Int. J. Advanced Intelligence Paradigms*, Vol. 27, No. 1, pp.61–71.

Biographical notes: C.G. Naveen Kumar is a research scholar in Bharathiar University, Coimbatore. Currently, he is working as a faculty in the Department of Computer Science in Government CPC Polytechnic. His interest in research includes computer networks, cryptography, data security and cloud computing.

C. Chandrasekar is working as an Assistant Professor in Government Arts College, Udumalpet, Tamilnadu. He has more than 15 years of experience and published papers in reputed international and national journals. He has good number of publications in various reputed journals. His research interests includes computer networks, data mining, cloud computing and data security.

1 Introduction

Ceritificateless public key cryptography: a CL-PKC scheme is similar with the identity-based cryptography (IBC) scheme in the respect that it relies on the existence of a trusted third party which possesses a master key, the scheme also uses the identity of the user. These ideas were formally developed by Al-Riyami and Paterson (2003) and were derived from the scheme presented by Boneh and Franklin (2001) by making simple modifications. The authors suggested an intermediate between public key cryptography and IBC as certificateless public key cryptography and it eliminates the key escrow associated with the IBE schemes without the need of certificates. In principle there are three parties involved in a CL-PKC scheme, the trusted third party called key generation centre (KGC), the party sending the message called Sender and the party who receives the sent message called Receiver. The KGC uses his master private key along with the receiver's identity to generate a partial private key which the receiver then combines with a secret value to derive his full private key. Thus this key is known only to the receiver and key escrow is avoided. The receiver needs to authenticate his identity to the KGC who must then securely transmit the partial private key. Meanwhile, the receiver also computes his public key by combining the same secret value with the public parameters published by the KGC and distributes it freely. The generation of private key and public key is independent of each other and just requires the use of the same secret value. The sender can thus obtain the public key related to a certain identity and use it to send encrypted messages to the receiver.

To authorise a secure system in Public key cryptography, the public key infrastructure for managing certificates are needed. But the identity component used in the certificate is to find the entity owned by public/private key pair. Public key cryptosystem is used to reduce high cost of symmetric key in key management. Open system interface (OSI) model adds advantage in designing the network that offers modularity, flexibility, comfort of use and standardisation of protocol. While data transfer from one to another node occurs, it is possible to get attacked by the hackers. The hackers get the data and decode it to include the fake data into it. So the security for the network is not a fully established procedure. A technique for key escrow issue which is possible on identity-based cryptosystem (Au et al., 2007).

The concept of CL-PKC was first introduced by Al-Riyami and Paterson they presented a scheme which was structurally similar and borrowed ideas from self-certified keys presented by Petersen and Horster (1997), Girault (1991) and Saeednia (1997) and more recently CBE scheme proposed by Boneh et al. (2003). In their work the authors specified certificateless encryption, signature and key exchange schemes and demonstrated how to support certificateless hierarchical schemes. Later in 2008 the first concrete and efficient construction for CLE secure in the standard model against strong adversaries was presented by Dent et al. (2008). This model is secure from strong type I attacker and strong type II attacker.

The secret key of a user is defined by KGC always. The user impersonation occurs, if the KGC be malicious. A model for security scheme for certificate less encryption and certificate less signatures are produced. The certificate less signatures and encryption have key generation system algorithm of same set. Third party maintains the message decipher, where key pair binds with an entity. But, some third party does malicious actions. Hence, certificate less public key cryptography used to reduce this kind of issue, involving the private key to be KGC and also generates the random numbers formed by

the user. While encoding and decoding, the public key acts as identity to an entity so that KGC could not access to entities.

Shi and Li (2007) presented a way for overcoming the key escrow in certificate less public key cryptography (CL-PKE). Here, the protocol for key agreement of CL-PKE along with the security related issues are provided. The existing various certificate less public key signature and encryption schemes is combined with this protocol to form certificate less public key cryptosystem. The efficiently secured certificate less authenticated key agreement for two parties had been proposed in such a way that, KGC produces public key of the user in public directory known as LDAP server (Mohamed et al., 2012).

The LDAP certificate is an identity to the user's communication, which uses symmetric key that are same were kept secret. It provides solutions for the issue of a key escrow and also for man-in-the-middle attack. It produces for other security related issues to make the protocol fully secure maintaining KGC to be honest party where the secret values are to be protected by those parties. The key management system issues of integrated certificate less public key infrastructure are proposed in this paper (Hassouna et al., 2013). In case of device theft in private key, a two factor authentication is used for private key to be protected. The private information is accessed and private key calculates in two factor authentication. Here it addresses the problem for revocation of public key, where message authentication code (MAC) provides portability for private key.

Seo et al. (2014) proposed a solution for sensitive information that has been shared, the mediated certificate less public key encryption (mCL-PKE) without the pairing operations is used. For each data that has to be shared, should be of same access control policy, which are encrypted by data owner and uploading it into cloud to decrypt partially if authorised rightly. Using private keys, users now fully decrypt data that was decrypted partially by the cloud. The approach mCL-PKE scheme is defined for confidentiality of a data and encrypts the efficient data for every user. This improves the encryption's efficiency, thereby evaluating security and performance.

Comparing with symmetric key algorithm, this manages the keys and revocations of the user, so the user's private key could not be changed. Cheng and Wen (2015) proposed a certificateless partially blind signature (CLPBS) technique in electronic cash system. Security problems and few schemes were proposed for it and the approach of improved CLPBS schemes proved a better security performance and efficiency. The signature on any message with the information given along with the identity, a public/private key where they communicate with requester. The requester then chooses messages for signing the information of identity to signer, hence signer communicate with the KGC.

A revocable certificateless public-key encryption (RCL-PKE) and the problem of revocation is been addressed (Tsai and Tseng, 2015). The syntax was defined and the security related problems of RCL-PKE are proposed. This is secured against the cipher text attacks by determining using the prediction of bilinear Diffie-Hellman and computational Diffie-Hellman assumptions.

The client verification and key assention convention utilising bilinear blending was proposed. Under computational CDH and k-CCA1 presumption and in arbitrary prophet demonstrate takes framework parameters, ace key and a client's identifier ID as sources of info, produces halfway private key. The Schnorr's mark plot is the mark conspires in light of the discrete logarithm issue, which can be demonstrated secure against picked message assaults in the arbitrary prophet display (He, 2012).

Security and utilisation of less vitality control was bolstered to handheld the cell phones in the meantime with less calculation cost and correspondence cost, for remote client verification benefits through uncertain remote correspondence channel, another ID-based confirmation convention utilising bilinear pairings was made. The convention has common verification property and opposes to surely understood security dangers in portable client condition (Hassan et al., 2017).

2 Contributions

The proposed work enhances the certificate less environment using cryptographic technique. The KGC or the Certificate authority provides the public/private key to the users. They act as a trusted third party, but some third party does malicious actions to take the necessary data and misuse it. In order to avoid such situations the proposed work contributes an algorithm as discussed below:

- the proposed work provides the secure dynamic bits advance encryption standard (SDBAES) algorithm
- it generates the secret key in the random manner to reduce the security issues
- it can able to remove Brute-Force attack, SQL injection attack, collision attack and birthday attacks.

3 Overview of architecture

The file owner uploads the data to cloud in the form of cipher text. The encryption of the data is carried out through SDBAES algorithm. It generate the random key bit (from 128, 192, 256) size for encrypting the data. The encrypted cipher text is stored into the cloud. For decrypting the file, the user needs to send the request to cloud admin to get the private key. After obtaining the private key the user can decrypt the file. In this technique the key database is assumed to be the authenticated database. The entire encryption and decryption technique is monitored through cloud admin.

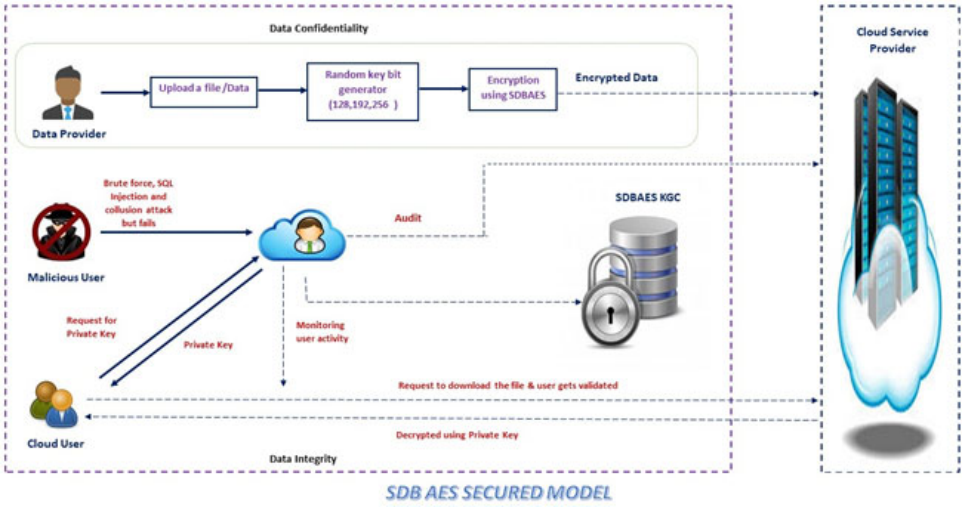
3.1 Overview of architecture

Fact of distinguishing among the legal liability of the network and the attacker are usually scanned through key which are managed by the service providers. The risks for security in cloud are different from risks of the conventional IT infrastructure due to intensity or nature. The process of communication resulted in the transmission of communication/data in the cloud applications among user and cloud. The file owners outsource their data and applications to cloud with a trust in such that assets of them will be secured in a cloud server.

The process of SDBAES ensures the data confidentiality, privacy and integrity. The process can be proceeded through random key generator which selects the key size from the 128, 192, 256 bits. Cloud service providers manage these resources for every individual user. It is carried out through access of right authentications for same resources at same time by increasing the utilisation of resources. The services of uploading the file to the cloud are automatically updating as per the file owner provides the generated data to the cloud server.

Key management is performed by the file owners and authenticated users. Since private key is depending on user's password, a user authenticated with secret key stored as a first authenticated factor. There is a necessity of entering the right password to decrypt the data and this is calculated as a full private key as second authenticated factor. As a private key is used for decryption of data by the user. The proposed scheme is protective against device theft, since the third party or the attackers are blocked by the cloud service provider while monitoring the activity of users.

Figure 1 SDBAES architecture (see online version for colours)



3.2 Security analysis

A security services involved in SDBAES are:

1 Confidentiality: confidentiality makes sure that none of them able to read what information is sent between authenticated parties. For achieving this, encryption algorithms are used. With asymmetric algorithms, a public key and also a private key are used. The public key is available to public while private key is available for the self-user. The data encryption can be done using public key and for decryption of data, private key is used. Asymmetric encryption key transfers the symmetric key and makes sure of other authenticated party.

2 Integrity: integrity is an assurance for non-alteration. Data in transit or at rest is not been altered undetectably. This assurance is essential for business or electronic environment and also for many other environments. The integrity level is achieved by the mechanisms such as parity bits and cyclic redundancy codes or by Hash techniques involved in it. These are designed to detect the proportions of bit errors that tend to be powerless to a thwart manipulation of data whose goal is in modifying the data content.

3 Authentication: identification served in identifying the specific entities that are involved, essentially in isolation from any other activity that the entity might want to perform. The identification of entity produces the concrete results that are used in enabling other communications or activities. For example, process of the identification of entity resulted in the symmetric key that is used in file to decrypt for reading or for modification. It establishes the secure communications channel with any other trusted entity. Once an identity key is authenticated, it is associated with the set of privileges on access control list for making access control decisions.

3.3 Algorithm

```
Byte in [n] <- input of n bytes
Key_Size <- size of the key
Begin
Byte state [16];
State = in;
AddRoundKey (state, round_key[0]);
For i = 1 to random (Key_Size (128, 192, 256)) stepsize 1 do
SubBytes (state);
SheftRows (state);
MixColumns (state);
AddRoundKey (state, round_key [i]);
End for
SubBytes (state);
ShiftRows (state);
AddRoundKey (state, round_key [random (1Key_Size (128, 192, 256))]);
Return encrypted data;
End
```

3.4 Description of algorithm

The AES contains the 3 bit levels which are 128 bits, 192 bits, and 256 bits. In the same manner, the proposed work contains the 128 bits, 192 bits, and 256 bits. The data should be in encrypted format, when the file owner uploads their file into the cloud. The encryption is carried out through SDBAES by random key size generation technique. During decryption, the file is decrypted through the private key, which is generated using random key bit provided by the SDBAES.

4 Comparison of proposed scheme with existing schemes

Table 1 Technical comparisons

Approach	*Computational cost*	*Forward secrecy*	*No key escrow problem*	*Removal of Brute force and collision attack*	*Key exchange*
He et al. (2012)	Client: 3TM + 3TH + T Server: Te + 2TM + 2TA + 3TH = |ID| + 2|Z * q| + 3|$\mathbb{G}$1| = 10 + 2 × 20 + 3 × 65 = 245 bytes	No	No	No	Yes
Tsai and Tseng (2015)	Client: 2TM + 3TH + T Server: Te + 5TM + 2TA + 5TH = 2|Z * q| + 3|$\mathbb{G}$1| = 2 × 20 + 3 × 65 = 235 bytes	Yes	No	No	Yes
Hassan et al. (2017)	Client: 5TM + TA + 4TH Server: 2Te + 4TM + 2TA + 6TH = |ID| + 2|Z * q| + 2|$\mathbb{G}$1| = 10 + 2 × 20 + 2 × 65 = 180 bytes	Yes	Yes	No	Yes
Proposed scheme	Client: 6TM + TA + 5TH Server: 3Te + 4TM + 2TA + 5^{TH} = |ID| + 1|Z * q| + 2|$\mathbb{G}$1| = 10 + 1 × 20 + 2 × 65 = 160 bytes	Yes	Yes	Yes	Yes

5 Results and discussions

5.1 Secured data

The secured data distribution is calculated by the ratio of number of data received properly and the number of data sent properly. The formula for calculating the secured data transmission is depicted below:

$$SM = \frac{Number\ of\ data\ received}{Number\ of\ data\ sent} * 100$$

Table 2 depicts the SM value of different research models.

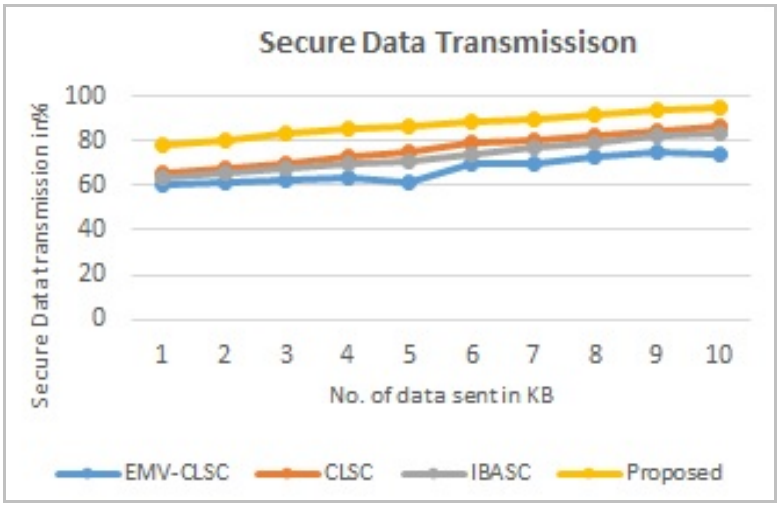
The pictorial representation of Table 2 is depicted in Figure 2.

Figure 2 depicted the secured data transmission rate of the different number of data. From the depicted figure, it is clear that the proposed technique will provide better results than the existing techniques.

Table 2 SM values of different research models

Number of data sent	*Secured data transmission rate (%)*			
	EMV-CLSC	*CLSC*	*IBASC*	*Proposed*
5	60	65.36	63.25	78.52
10	61.12	68.15	65.31	80.12
15	62.8	70.10	67.85	83.65
20	63.32	72.52	69.65	85.10
25	61.72	74.68	70.54	86.65
30	69.55	78.65	73.52	88.36
35	70.02	80.10	76.85	90.10
40	72.45	82.45	79.65	91.65
45	75.13	84.65	82.10	93.32
50	74.32	86.65	83.36	95.10

Figure 2 Secured message (see online version for colours)



5.2 Computational cost

Computational cost is described that the time taken to evaluate the certificate less algorithm. It is measured through the milliseconds.

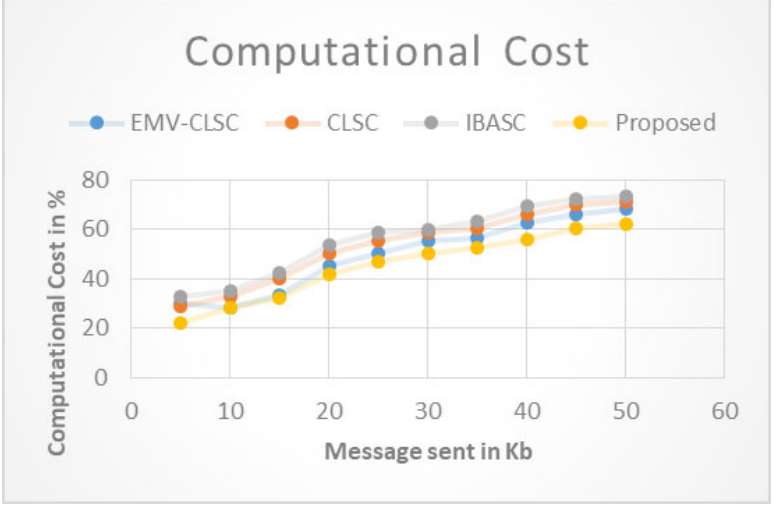
$$CC = Time(run\ certificateless\ SDBAES\ algorithm)$$

Figure 3 depicted the computational cost of the different size of data. From the depicted figure, it is clear that the proposed technique will provide better computational cost than the existing techniques.

Table 3 Comparison of computational cost with the proposed system

Message size in KB	*Computational cost (ms)*			
	EMV-CLSC	*CLSC*	*IBASC*	*Proposed*
5	30.00	28.9	32.7	22.3
10	28.13	32.8	34.9	28.4
15	33.17	40.1	42.6	32.1
20	45.34	50.2	53.6	41.8
25	50.32	55.3	58.9	46.7
30	55.27	58.6	60.1	50.1
35	56.38	60.3	63.4	52.6
40	62.47	66.1	69.7	55.7
45	65.98	69.8	72.3	60.4
50	68.34	71.2	73.6	62.3

Figure 3 Computational cost (see online version for colours)



5.3 Memory consumption

Memory consumption is described that the difference between the total memory required for storing the data and the unused memory. The formula for the memory consumption is depicted below:

$$Memory = Total\ memory\ for\ storing\ data - unused\ memory$$

The memory consumption rate of different data size is represented in Table 4.

Table 4 Comparison of memory consumption levels with the proposed system

Message size (KB)	*Memory consumption rate*			
	EMV-CLSC	*CLSC*	*IBASC*	*Proposed*
15	180	148	172	131
30	199	155	190	145
45	218	178	210	159
60	245	220	239	201
75	262	235	251	210
90	292	247	282	218
105	312	260	300	243
120	322	280	310	261
135	335	296	321	282
150	356	312	345	290

The pictorial representation of Table 4 is in Figure 4.

Figure 4 Memory consumption (see online version for colours)

6 Conclusions

The novel of SDBAES algorithm is proposed for the data encryption and decryption through the process of security enhanced with integrity, confidentiality and privacy. This algorithm manages to provide data from the data provider and upload the data which are encrypted to store in the cloud server. The cloud service provider acts on the data and managed in such that, the file size and updated data by the data provider can be achieved in terms of authentication. This is viewed by the cloud service provider for denoting authorised and unauthorised users to access the data that are stored in the database. This tends frequent random user to require data re-encryption with the exchange of keys in order to avoid leakage of data to revoked user. Thus, advanced methods will be

considered for key exchange in a certificateless public key cryptography with relevant system related basis in future.

References

Al-Riyami, S.S. and Paterson, K.G. (2003) 'Certificateless public key cryptography', in *Asiacrypt*, November, Vol. 2894, pp.452–473.

Au, M.H., Mu, Y., Chen, J., Wong, D.S., Liu, J.K. and Yang, G. (2007) 'Malicious KGC attacks in certificateless cryptography', in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, March, pp.302–311, ACM.

Boneh, D. and Franklin, M. (2001) 'Identity-based encryption from the Weil pairing', in *Advances in Cryptology – CRYPTO 2001*, Springer, Berlin/Heidelberg, pp.213–229.

Boneh, D., Gentry, C., Lynn, B. and Shacham, H. (2003) 'Aggregate and verifiably encrypted signatures from bilinear maps', in *Eurocrypt*, May, Vol. 2656, pp.416–432.

Cheng, L. and Wen, Q. (2015) 'Cryptanalysis and improvement of a certificateless partially blind signature', *IET Information Security*, Vol. 9, No. 6, pp.380–386.

Dent, A.W., Libert, B. and Paterson, K.G. (2008) 'Certificateless encryption schemes strongly secure in the standard model', in *International Workshop on Public Key Cryptography*, Springer, Berlin, Heidelberg, March, pp.344–359.

Girault, M. (1991) 'Self-certified public keys', in *Advances in Cryptology – EUROCRYPT'91*, Springer Berlin/Heidelberg, pp.490–497.

Hassan, A., Eltayieb, N., Elhabob, R. and Li, F. (2017) 'An efficient certificateless user authentication and key exchange protocol for client-server environment', *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 4 pp.1–15.

Hassouna, M., Barri, B., Mohamed, N. and Bashier, E. (2013) 'An integrated public key infrastructure model based on certificateless cryptography', *International Journal of Computer Science and Information Security*, Vol. 11, No. 11, p.1.

He, D. (2012) 'An efficient remote user authentication and key agreement protocol for mobile client–server environment from pairings', *Ad Hoc Networks*, Vol. 10, No. 6, pp.1009–1016.

Mohamed, N., Hassouna, M. and Bashier, E. (2012) 'A secure and efficient key agreement protocol based on certificateless cryptography', *International Journal of Intelligent Computing Research (IJICR)*, Vol. 3, No. 4, pp.1–8.

Petersen, H. and Horster, P. (1997) 'Self-certified keys-concepts and applications', in *Proc. Communications and Multimedia Security*, September, Vol. 97, pp.102–116.

Saeednia, S. (1997) 'Identity-based and self-certified key-exchange protocols', in *Information Security and Privacy*, Springer Berlin/Heidelberg, pp.303–313.

Seo, S.H., Nabeel, M., Ding, X. and Bertino, E. (2014) 'An efficient certificateless encryption for secure data sharing in public clouds', *IEEE Transactions on Knowledge and Data Engineering*, Vol. 26, No. 9, pp.2107–2119.

Shi, Y. and Li, J. (2007) 'Two-party authenticated key agreement in certificateless public key cryptography', *Wuhan University Journal of Natural Sciences*, Vol. 12, No. 1, pp.71–74.

Tsai, T.T. and Tseng, Y.M. (2015) 'Revocable certificateless public key encryption', *IEEE Systems Journal*, Vol. 9, No. 3, pp.824–833.