# Identity-based Signcryption for Big Data Using Forward Secrecy

Adoubara K.*, Daniel M. and Anireh V.I.E

*Department of Computer Science, Faculty of Science, Rivers State University*
*Port Harcourt, Nigeria.*

***Abstract***

*Identity-based cryptography is a form of public-key cryptography that does not require users to pre-compute key pairs and obtain certificates for their public keys. Instead, public keys can be arbitrary identifiers such as email addresses. This means that the corresponding private keys are derived, at any time, by a trusted private key generator. The idea of signcryption is to provide a method to encrypt and sign data together in a way that is more efficient than using an encryption scheme combined with a signature scheme. The research also proposes a method to implement the ID Based signcryption with forward secrecy using sessions so as to provide an extra layer of security against eavesdropping; the proposed system encrypts the random message encryption key using the assigned receiver's public key and then sends the message to the receiver. The main aim of this research work is to simulate the process using a program written in python programming language which implements forward secrecy using sessions. Also the proposed system aims to verify if IBE and IBS can be used in conjunction to achieve greater efficiency. The implementation language used to prove this approach is Python, which is an interpreted high-level, general-purpose programming language. The results achieved show a great reduction in signcryption time as compared to sign and encrypt method which proves the proposed concept of increasing efficiency and reducing response time to identity theft cases.*

**Keywords) —** *cryptography, encryption, identity-based, signcryption*

## I. INTRODUCTION

The ever increasing size of data increases the need for data security and data privacy. Data security is a major requirement for the big data. The leakage of sensitive user data to unauthorized users and other security threats can be of extreme loss to the individual in concern as well as the organization, thus drastically eroding the confidence of the users. The data should only be accessible by an authorized user.

Security solutions design for big data needs to be scalable, and should also consider the V's of Big Data (volume, veracity, velocity and variety). Of the many goals which the study of cryptography sets out to achieve, Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. Traditionally, these goals have been studied separately and can be summarized into encryption and digital signature; these are the two fundamental cryptographic tools that can guarantee the availability, integrity, and confidentiality of communications.

Public key encryption schemes aim at providing confidentiality whereas digital signatures must provide authentication and non-repudiation. Nowadays, noticeably, many real-world cryptographic applications require those distinct goals to be simultaneously achieved. A traditional approach to achieve these requirements is to sign-then-encrypt the message. For instance, in order to send a confidential letter in a way that it cannot be forged, it has been a common practice for the sender of the letter to sign it, put it in an envelope and then seal it before handing it over to be delivered. Discovering Public key cryptography has made communication between people who have never met before over an open and insecure network, in a secure and authenticated way possible (Anirvan et al, 2018). The rise of cyber-attacks has put a major concern on the safety of data in a big data environment. Companies, including Uber and Facebook have been victims of cyber-attacks. In September 2018, cyber-attack exposed Uber's data of 57 million customers and drivers costing the company about $100,000 paid to the hackers so that the stolen data could be deleted (Newcomer, 2019). Facebook also had its share of cyber-attack in 2018 as 90 million Facebook user accounts were exposed by a security breach in the UK (Tech world, 2018). The researcher has identified the following constrains to the effective implementation of a seamless process:

- Inadequate implementation of the use of an Identity based signcryption techniques
- Lack of ID Based techniques that fulfil forward secrecy security property at its core so as to optimize the security of data and further reduce and prevent future occurences of identity theft

## II. LITERATURE REVIEW

### *A. Signcryption*:

Signcryption was first proposed by Zheng (Zheng, 1997). It is a new paradigm in public key cryptography that simultaneously fulfils both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly lower than that required by the traditional "signature followed by encryption". In simple words signcryption is a cryptographic primitive that fulfils both the functions of digital signature and public key encryption simultaneously, at a cost significantly lower than that required by the traditional signature-then-encryption approach. The performance advantage of signcryption over the signature-then-encryption method makes signcryption useful in many applications, such as electronic commerce, mobile communications and smart cards thereby improving speed of data processing. As a cryptographic primitive, signcryption combines the functions of digital signature and public key encryption simultaneously, but at lower costs of computation and communication than those required by the traditional signature-then-encryption approach. Indeed, shorter signcryptext is preferable in the real application environment. For example, wireless communication is an essential component of mobile computing, but the energy required for transmission of a single bit has been measured to be over 1000 times greater than for a single 32-bit computation (Barr et al, 2003).

Thus, if the researcher can compress the data transmit, by even 1 bit, energy would be saved. From this point of view, it is more desirable for us to design a secure IBSC scheme that can reduce the signcryptext expansion as small as possible. It is also of significance if the researcher can reduce the computation complexity at the same time. Although Li and Takagi's IBSC scheme (Li et al, 2011) achieves confidentiality and unforgeability simultaneously without random oracles, it inherits the inefficiency from Zhang's scheme (B. Zhang, 2010).

More exactly, larger signcryptext expansion and more exponentiation computation are inevitable because of using the same design techniques from (B. Zhang, 2010), compared with Yu et al.'s first standard model-based IBSC scheme (Yu et al, 2009). A natural question is whether there exists a secure IBSC scheme in the standard model that not only preserves the efficiency of Yu et al.'s scheme, but also achieves provable security. (Xiangxue Li, et al, 2013) paper answers the open problem by presenting an IBSC scheme which achieves the following desired features simultaneously.

### *B. Identity Based Signcryption*

Identity (ID)-based encryption, or IBE for short, is an exciting alternative to public-key encryption, which eliminates the need for a Public Key Infrastructure (PKI) that makes publicly available the mapping between identities, public keys, and validity of the latter (Anirvan Chkraborty et al, 2018). The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, because the identities (e.g. emails or IP addresses) together with common public parameters are sufficient for encryption. The private keys of the users are issued by a trusted third party called the private key generator (PKG).

ID-based signcryption is potential solution for the secure communication in a big data environment. In the public key infrastructure the revocation is achieved by broadcasting certificate in the revocation function. The non-revoked users are able to obtain short term secret keys in the current time interval by incorporating their own long-term private keys and key update information distributed by the Private Key Generator (PKG). Due to the need to support large scale data processing, it is important that the revocation function is also scalable without incurring significant computational overheads.

Extending the concept of Identity-Based Encryption (IBE), (Sahai et al, 2005) provides flexible and different types of access control over encrypted data by enabling one-to-many encryption based on user attribute .To annihilate the decryption overhead on the user side, (Green et al., 2011) proposed on Attribute-Based Encryption (ABE) paradigm equipped with outsourced decryption based on a key blinding technique . By applying the transformation key which is provided by user, a semi-trusted cloud server is able to convert any ABE ciphertext into an ELGamal-style ciphertext without accessing the data or secrete keys. With the transformed ciphertext from the cloud server, the user can perform the complete decryption with a small computational overhead at the clients end. To determine correctness of the conversion carried out by the semi-trusted cloud server, (Lai et al, 2013) imported verifiability of the clouds decryption service and contingent accurate construction using a parallel encryption technique. For correctness checking, a redundancy ciphertext is applied to the original ciphertext. Observing the bulky bandwidth and computation cost in (Lai et al, 2013), (Lin et al, 2015) and (Mao et al, 2015) provide alternative approaches to construct ABE equipped with verifiable outsourced decryption by incorporating the idea of commitment independently. (Ma et al, 2015) proposed an ABE paradigm that support both outsourced decryption and encryption, and defined a new security notion of exculpability for the outsourced decryption to guarantee the user cannot "accuse" the cloud server of incorrect translation, while the cloud server performs the transformation honestly. To realize the strongest from of access policy, (Xu et al, 2016) put forward a circuit ABE scheme with verifiable decryption outsourcing based on the multi linear map.

### C. Bilinear Pairing

Assume, (G1, G2) is the same order p cyclic groups pair. In addition, g, a random generator is chosen from group G1. Therefore, e maps as e : G1 × G1 → G2 has three characteristics (McCullagh et al):

1. Bilinearity: Always, e maps as e(gx, hy) = e (g, h)xy for any two integers (x, y) ∈_R(Z_p^*)
2. Non-degeneracy: For identity element 1 in G2, always e(g, g)≠ 1.
3. Computability: At least one algorithm exists to calculate e (g, h) efficiently for some (g, h) ∈ (G1)2.

Note that e(·, ·) is symmetric by its nature as e(gx , hy ) = e(g, h)xy= e(gy, hx ).

### D. Mathematical Definitions

Now, the researcher discuss few DH-based assumptions which are assumed to be intractable for every PPT algorithm A. Let, g is a generator of G1. Also i, j and k are randomly chosen fromZ_p^*.

Definition 1:

(Computational Diffie-Hellman Assumption). Computation of Z =gij for given (gi, gj) is hard. It can be defined as

$$|Pr (A(gi, gj) = gij)| \geqslant s \quad (1)$$

Definition 2:

(Decisional Diffie-Hellman Assumption). Taking decision of X = gij for given (gi, gj, gij) and (gi,gj,X) is hard. It can be defined as

$$|Pr(A(gi, gj, gij)) - Pr ( A(gi, gj, X))| \geqslant s \quad (2)$$

Definition 3:

(Bilinear Diffie-Hellman Assumption). Computation of Z = e(g, g)ijkfor given (gi, gj, gk) is hard. It can be defined as

$$|Pr(A(gi, gj, gk) = e(g, g)ijk)| \geqslant s \quad (3)$$

### E. Formal Structure of the IBSC Scheme

The structure of IBSC (An, 2002) is considered as four algorithms.

1. Setup (1λ): Takes a security parameter λ as input and generates MSK, which is kept as secret, and params, which is known publicly to all users in the system.
2. Extract (params, MSK, IDi): Takes params, user's identity IDi and MSK as input parameter. After that, it sends the generated SKi securely to user through secure communication.
3. Signcrypt(M, params, IDA, SKA, IDB): Takes message M, the system parameter params, IDA, SKA, and IDB as input. Then it produces signcryptext σ which is then sent to the recipient through the public ⊥ (Special symbol used to indicate nothing returns channel).
4. Unsigncrypt( σ , params, IDB, SKB, IDA): Takes σ , params with recipient ' s (IDB, SKB) and sender ' s IDAas input parameter, and finally returns M, if the signcryptext σ is valid; otherwise, returns ⊥..

### F. Forward Secrecy

An encryption scheme provides forward secrecy when the exposure of public and private keys to an eavesdropper does not in any way compromise past session keys that have earlier been used. Forward secrecy is a security property of signcryption that make sure the encrypted data earlier existing are secured and cannot be accessed even if there is a breach of the protocol because the keys used for signcryption and unsigncryption are created for each session and frequently changes. The eavesdropper can only gain access to the current session and not past correspondences that existed between the sender and the receiver.

Forward secrecy, also known as perfect forward secrecy (PFS), is an important security property which guarantees that derived session keys cannot be revealed, even if the longterm private key is compromised in the future. Especially in the situation where Internet surveillance is a concern, forward secrecy lets enterprises argue that eavesdroppers simply cannot reveal secret data of past communications. However, in TLS, forward secrecy is not necessarily guaranteed. In particular, the RSA key exchange is only secure as long as the server can protect its private key. If the server's private key is ever revealed, an attacker can decrypt all recorded sessions by deriving the pre-master secret using the server's private key, and basically recover all past session keys. There are currently two key exchange methods in TLS that support forward secrecy, including ephemeral DiffieHellman (DHE) and ephemeral Elliptic Curve Diffie-Hellman (ECDHE).

When using DHE or ECDHE, the server's longterm secret key is used to sign a short-lived Diffie-Hellman key exchange message as the pre-master secret (that is discarded after the session). For example, when using DHE key exchange with RSA signatures, the server sends an additional Server Key Exchange message which contains an ephemeral Diffie-Hellman public key that is signed with server's RSA private key. Similarly, when using ECDHE with RSA signatures, an extra Server Key Exchange message contains the ephemeral elliptic curve Diffie-Hellman public key and its elliptic curve domain parameters, which are signed with the server's RSA private key. The server may also replace RSA signatures entirely with elliptic curve cryptography, by signing the ECDHE public key with its ECDSA private key.

## III. METHODOLOGY

As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap.

***Analysis of the Present System***

The researcher analyses the present system which was proposed by Zheng in 1996. The signcryption scheme was based on discrete logarithm problem (DLP) whereby the sender (Alice) generates a private key and further digitally sign and encrypt the data using the private key into cipher text before sending it to the receiver (bob) who in-turn verifies and decrypt the cipher text.

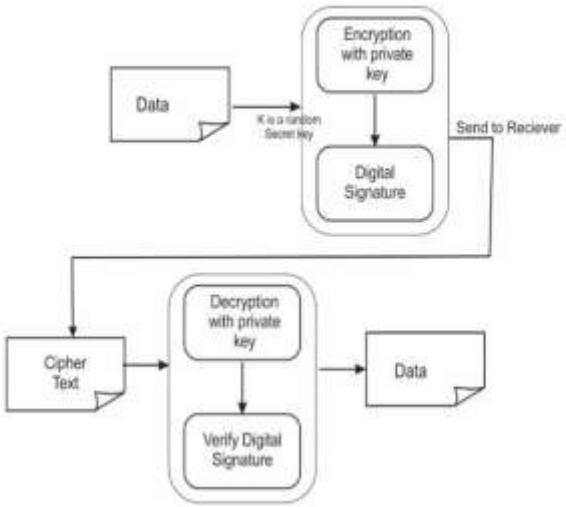


**Fig. 1: Existing architecture of the encryption and decryption model.**

***B. Strength and weakness of the present system***

***1. Ciphertext authentication***

A scheme offering ciphertext authentication provides the guarantee to the recipient of a signed and encrypted message that the message was encrypted by the same person who signed it. This means that the ciphertext must have been encrypted throughout the transmission and so it cannot have been the victim of a successful man-in-the-middle attack. It also implies that the signer chose the recipient for its signature.

***2. Message confidentiality***

The accepted notion of security with respect to confidentiality for public key encryption is in distinguishability of encryptions under adaptive chosen ciphertext attack, as formalized in ( Rackoff et al, 1992). The notion of security defined in the game below is a natural adaptation of this notion to the identity-based signcryption setting.

***3. Signature non-repudiation***

A signcryption scheme offering non-repudiation prevents the sender of a signcrypted message from disavowing its signature. Note that non-repudiation is not as straightforward for signcryption as it is for digital signature schemes since the researcher is dealing with encrypted data. As a consequence, by default, only the intended recipient of a signcryption can verify.

***4. Ciphertext anonymity***

Ciphertext anonymity is the property that ciphertexts contain no third-party extractable information that helps to identify the sender of the ciphertext or the intended recipient. It is defined via the following game.

Weakness of the present system

It was discovered that the present system failed some security properties which will provide strong encryption and guarantee data safety in the system such as forward secrecy and public verifiability as discussed the forward secrecy in the literature review.

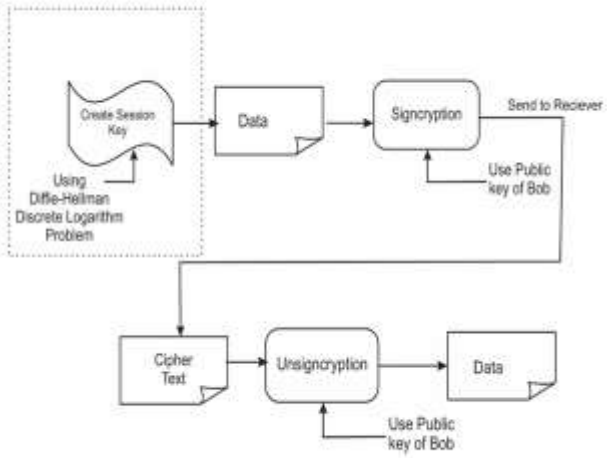


**Fig 2: The Proposed System Design**

## IV. ANALYSIS OF THE PROPOSED SYSTEM

The performances of the proposed system measuring the time taken to encrypt and decrypt specific character length of data and the time taken to signcrypt similar character length.

The researchers analyzed the performances of the proposed system measuring the time taken to encrypt and decrypt specific character length of data and the time taken to signcrypt similar character length.

**TABLE I**

**Analyses of the proposed scheme**

| Message Length | Encryption Time (sec) | Signcryption Time (sec) |
|---|---|---|
| 4 | 0.01397 | 0.00500 |
| 8 | 0.01400 | 0.00597 |
| 24 | 0.01501 | 0.00500 |
| 32 | 0.01397 | 0.00500 |
| 80 | 0.01500 | 0.00600 |
| 160 | 0.01403 | 0.00600 |
| 300 | 0.01553 | 0.00797 |
| 500 | 0.01697 | 0.00900 |
| 1000 | 0.04806 | 0.01399 |

Table 1 above shows the analyses of the between the encryption time and signcryption time (in seconds). The researcher analysed the time taken to encrypt/decrypt some message character length for both the encryption/decryption and signcryption/unsigncryption algorithms and discovered that the signcryption algorithm performed faster than the encryption algorithm. Fig. 3 below shows the graph.

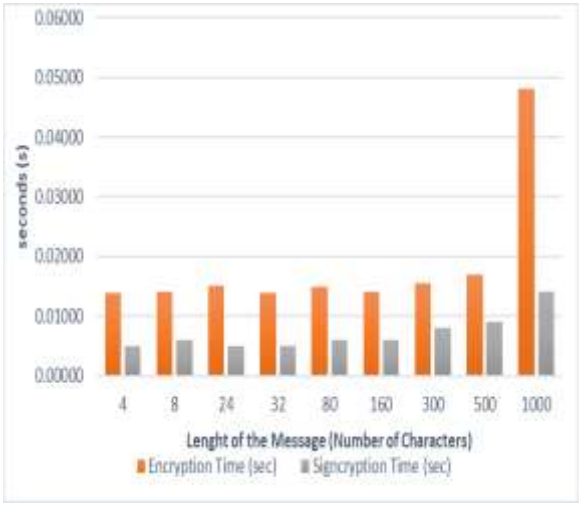


**Fig. 3: Graphical Analysis of the proposed system**

**TABLE 2**

**Analyses of the proposed scheme**

| Message Length | Zheng's Signcryption | Proposed Signcryption |
|---|---|---|
| 4 | 0.064 | 0.00500 |
| 8 | 0.068 | 0.00597 |
| 24 | 0.069 | 0.00500 |
| 32 | 0.071 | 0.00500 |
| 80 | 0.074 | 0.00600 |
| 160 | 0.074 | 0.00600 |
| 300 | 0.084 | 0.00797 |
| 500 | 0.093 | 0.00900 |
| 1000 | 0.107 | 0.01399 |

The researchers compared the proposed scheme with Zheng's scheme in table 6 above. It was further discovered that the proposed scheme also performed faster than the existing scheme. The graph is shown in fig. 4 below.

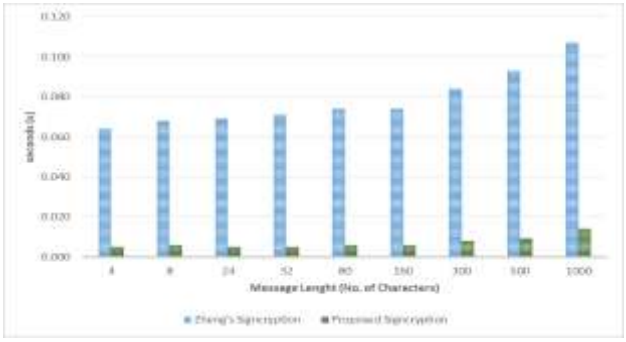

**Fig. 4: Graphical Comparison of Zheng's scheme and the proposed system**

## V. DISCUSSION

The proposed system suggests that the performance-based arguments against deploying forward secrecy are no longer valid. ECDHE-based key exchange, which provides forward secrecy, can be faster than basic RSA-2048 key exchange which does not. The reason for the performance improvement is the replacement of an expensive RSA-2048 decryption with faster secp256r1 elliptic curve operations. As we transition to longer RSA keys, such as RSA3072 or RSA-4096, the performance advantage of the forward secrecy techniques will become even more pronounced. These results suggest that sites should migrate to forward secrecy techniques (when possible) for both security and performance reasons

## VI. CONCLUSIONS AND RECOMMENDATIONS

### A. Conclusions

Identity based Signcryption is an approach that reduces the communication as well as computation cost and increase the efficiency of the system, together with forward secrecy, the security of a platform is highly assured. Here the researcher has proposed the new improved identity-based scheme that applies forward secrecy with the use of sessions and is more efficient as compared to some existing scheme. The proposed scheme admits a full security analysis as proposed in the model of Boyen (6). We have compared the complexity of our proposed scheme with existing work and proved that our scheme is efficient. Later we proposed the new certificateless signcryption scheme to avoid the key escrow problem that comes in identity-based cryptosystem and compared their efficiency with existing scheme and proved that our certificateless scheme is the improved version. In many applications where less time is required Identity based signcryption is the great solution like AD-hoc network, mobile computing and embedded system. This scheme combined with forward secrecy implementation further enhances the security of a system and can be applied in numerous sectors especially against identity theft.

### B. Recommendations

In light of the knowledge acquired from this research, the tremendous value contribution to academic research and to the security organizations even to smart home users, the researcher is recommending that this proposed scheme be further analysed and deployed as tertiary security parameter in security as well as private/corporate web mail and website log on to optimize system security. While the need for TLS forward secrecy has become more widely discussed over the recent years, it is critical that servers are configured and implemented correctly, and not otherwise, achieving a false sense of security.

## REFERENCES


[1] Y. Zheng, "*Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption),"* in Advances in CryptologyCRYPTO'97, pp. 165–179, Springer, 1997.

[2] D. Boneh and M. Franklin, "*Identity-based encryption from the weil pairing,"* in Advances in CryptologyCRYPTO 2001, pp. 213–229, Springer, 2001.

[3] S. S. Al-Riyami and K. G. Paterson, "*Certificateless public key cryptography,"* in Advances in Cryptology-ASIACRYPT 2003, pp. 452–473, Springer, 2003.

[4] K.G. Paterson. "*ID-based signatures from pairings on elliptic curves*". Cryptologye Print Archive, Report 2002/004, 2002. http://eprint.iacr.org/.

[5] F. Hess. "*Exponent group signature schemes and efficient identity based signatureschemes based on pairings*." Cryptology ePrint Archive, Report 2002/012, 2002.http://eprint.iacr.org/.

[6] J. C. Cha and J. H. Cheon. "*An identity-based signature from gap Diffie-Hellman groups"*. In Public Key Cryptography - PKC 2003, volume 2567 of LNCS, pages 18–30. Springer-Verlag, 2003.

[7] N.P. Smart. An identity based authenticated key agreement protocol basedon the Weil pairing.Cryptology ePrint Archive, Report 2001/111, 2001.http://eprint.iacr.org/.

[8] C. Gentry and A. Silverberg. "*Hierarchical ID-based cryptography. CryptologyePrint Archive"*, Report 2002/056, 2002. http://eprint.iacr.org/

[9] Sravan Kumar Nalla, Konni Srinivasarao, "*An Identity based Authentication and Data Encryption in Cloud Computing*" SSRG International Journal of Computer Science and Engineering 4.10(2017)

[10] Sahai A., Waters B. (2007) "*Fuzzy Identities and Attribute-Based Encryption*". In: Tuyls P., Skoric B., Kevenaar T. (eds) Security with Noisy Data. Springer, London

[11] Q. Yanfeng, T. Chunming, L. Yu, X. Maozhi, and G. Baoan, "*Certificateless proxy identity-based signcryption scheme without bilinear pairings,*" Communications, China, vol. 10, no. 11, pp. 37–41, 2013.

[12] Q. Xia and C. Xu, "*Cryptanalysis of two identity based signcryption schemes,*" in Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on, pp. 292–294, IEEE, 2009.

[13] X.-Y. Jia, B. Li, and Y.-M. Liu, "*Random oracle model,*" Ruanjian Xuebao/Journal of Software, vol. 23, no. 1, pp. 140–151, 2012.

[14] B. Libert and J.-J. Quisquater, "*New identity based signcryption schemes from pairings*.," IACR Cryptology ePrint Archive, vol. 2003, p. 23, 2003.

[15] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, *"Efficient and provably-secure identity-based signatures and signcryption from bilinear maps,*" in Advances in Cryptology-ASIACRYPT 2005, pp. 515–532, Springer, 2005.

[16] G. Chen and S. Wan, "*Analysis and improvement of identity-based designated verifier signature scheme,*" in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 2388–2391, IEEE, 2012.

[17] L. Chen and J. Malone-Lee. "*Improved identity-based sincryption. Cryptology ePrint Archive*", Report 2004/114, 2004. http://eprint.iacr.org/.

[18] Satyam Akunuri, Sanjeev Bandru, Chandu Naik Azmera "*Security Systems for DNS Using Cryptography*" International Journal of Computer Trends and Technology 68.4 (2020)

[19] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. "*Efficient algorithms forpairing-based cryptosystems*". InProc. Crypto '02, LNCS 2442, 2002

[20] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "*Efficient and provably-secure identity-based signatures and signcryption from bilinear maps,*" in Advances in Cryptology-ASIACRYPT 2005, pp. 515–532, Springer, 2005.

[21] G. Yu, X. Ma, Y. Shen, and W. Han, "*Provable secure identity based generalized signcryption scheme,"* Theoretical Computer Science, vol. 411, no. 40, pp. 3614–3624, 2010

[22] Q. Yanfeng, T. Chunming, L. Yu, X. Maozhi, and G. Baoan, "*Certificateless proxy identity-based signcryption scheme without bilinear pairings,*" Communications, China, vol. 10, no. 11, pp. 37–41, 2013.

[23] M. Bellare and P. Rogaway. "*Random oracles are practical: A paradigm for designing efficient protocols*". In 1st ACM Conference on Computer and Communications Security, pages 62–73, 1993.

[24] J. Malone-Lee. "*Identity-based signcryption*". Cryptology ePrint Archive, Report2002/098, 2002. http://eprint.iacr.org/.

[25] X. Boyen. "*Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography*." In Advances in Cryptology - CRYPTO 2003, volume 2729 of LNCS, pages 382–398. Springer-Verlag, 2003

[26] C. Rackoff and D. Simon. *"Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack*". In Advances in Cryptology - CRYPTO '91, volume 576 of LNCS, pages 433–444. Springer-Verlag, 1992.

[27] Nikhil B. Khandare "*Performance Analysis of Cryptographic Protocols to Enhance SMS and M-Commerce Security*". International Journal of Computer Trends and Technology (IJCTT) V44(2) 2017.

[28] S. Goldwasser, S. Micali, and R. Rivest. "*A digital signature scheme secure against adaptive chosen-message attacks*". SIAM Journal on Computing, 17(2):281–308, 1988.

[29] R. Sakai, K. Ohgishi, and M. Kasahara. "*Cryptosystems based on pairings*". In Symposium on Cryptography and Information Security, 2000