New Hierarchical Identity Based Encryption with Maximum Hierarchy

Dasari Kalyani[1], R. Sridevi[2]

(Corresponding author: D. Kalyani)

Department of Information Technology, VNR Vignana Jyothi Institute of Engineering and Technology[1]
Vigana Jyothi Nagar, Bachupally Road, Pragathi Nagar, Hyderabad, Telangana 500090, India
Department of Computer Science and Engineering, Jawaharlal Nehru Technological University Hyderabad[2]
Kukatpally, Hyderabad, Telangana 500085, India
(Email: kalyani_d@vnrvjiet.in)

(Received Oct. 9, 2017; revised and accepted Apr. 21, 2018)

Abstract

Identity Based Encryption (IBE) is a type of public-key encryption in which the public key of a user has some unique information about the identity of the user, and it is an important primitive of public cryptography. As far as Hierarchical Identity-Based Encryptions (HIBE) concern, it is rational to view the root PKG (Private Key Generator) as a trusted party or being unconditionally trusted, but those level PKGs should be treated suspiciously in hierarchical identity based setting. To achieve the full security, existing schemes suffers a security degradation exponential in the hierarchy depth. In this paper, we propose Hierarchical Identity-Based Encryption with maximum hierarchy extension to Boneh IBE under Decisional Bilinear Diffie-Hellman (DBDH) assumption in standard security model. To overcome key escrow problem challenge in HIBE, we proposed a new method that overcomes key escrow by having maximum Hierarchy length. This is due to sequential manner in the key generation, means that level PKGs does not have the ability of determining valid private keys without other level private keys. Correctness and security analysis of the scheme is also discussed.

Keywords: Ciphertext; IBE; HIBE; Key Escrow; Public Key Cryptography; Random Oracle

1 Introduction

Identity-Based Encryption (IBE) [24] is a public-key encryption scheme where ones public key can be unreservedly set to any unique identity (for example, one's identity). An authority that holds a master secret key can take any arbitrary identifier and extract a secret key corresponding to this identifier. Anyone can then encrypt messages using the identifier as a public encryption key, and only the holder of the corresponding secret key can decrypt these messages. This idea was presented by Shamir [27], an prototype solution was proposed in [5,6], and the primary completely IBE framework were portrayed by Boneh and Franklin [27] and Cocks [7]. IBE frameworks can enormously disentangle the general population key foundation for encryption arrangements, yet they are still not as general as one might want. Numerous associations have a various hierarchical structure, maybe with one trusted authority, a few sub-authorities and numerous individual clients, each have a placing with a little piece of the association tree.

We might want to have an answer where every specialist can assign keys to its sub-authorities, who can continue appointing keys additionally down the hierarchy to the clients. The length of the hierarchy order can run from a few in little associations, up to at least ten in huge ones. An IBE framework [14] that permits lower authorities as above is called Hierarchical Identity-Based Encryption (HIBE). In HIBE [15,16], messages are encoded for character vectors, noting as nodes in the hierarchy chain. This idea was presented by Horwitz and Lynn [8], who likewise depicted a partial solution for it, and the primary fully functional HIBE framework was portrayed by Gentry and Silverberg [33].

In traditional hierarchical identity based cryptosystems, non-leaf entities as level Private Key Generators (PKG) are usually capable of deriving private keys for their descendants with use of their private keys. The non-leaf entities can therefore act (decrypt or sign) on the behalf of their arbitrary descendants. This is called key escrow problem of HIBC. In [18], the authors proposed a secure key issuing protocol for IBE which is also extends to key generation of HIBE with coalition of other threshold [22,29] and multi level access structures [28,30] to distribute the decryption key to the receiver.

The dual system technique has been successfully used to obtain adaptive security for not only (H)IBE [3,32] but also more expensive Fully Encryption (FE) [8,20,34]. Recently, the dual system technique helped us to go further. Chen and Wee [9, 10] applied the dual system technique in a novel way and gave an IBE with security loss only related to system parameters.

Initial idea and motivation of identity-based encryption introduced by Shamir [27] where a public key can be the identity string of a user such as an e-mail address. Although practical solutions proposed by different authors for IBE, Key escrow is well known problem in an identity based encryption. In order to resolve key escrow problem in IBE, Gentry and Silverburg [33] given construction of HIBE [19, 26] is which the security is based on the random oracle model. Subsequently, Boneh and Boyen [4] presented a HIBE without random oracles in the selective-ID model. One inherent limitation of previous HIBE schemes [17,21] is that the maximum hierarchy depth should be fixed in the setup phase. In this paper, we address this problem and propose a hierarchical identity based encryption scheme, that is a modification to the Boneh *et al.* [12] HIBE. In this scheme, we included our proposed distributed key issuing protocol [18] to achieve maximum hierarchy with threshold secret key recovery. We also present correctness and security analysis of the proposed scheme.

The rest of the paper is organized as follows: Section 2 presents related work and Section 3 gives an overview of preliminaries and Identity Based Cryptography and their extensions. In Section 4, discussed overview of distributed key issuing protocol. In Section 5, we present Hierarchical Identity Based Encryption scheme and their correctness. Security assumptions, analysis and comparative analysis is presented in Section 6. Section 7 we explore possible applications of proposed scheme and other IBE schemes. Concluding remarks are in Section 8.

2 Related Work

The concept of IBE [27] initially proposed by Adi Shamir in 1984 and it remained an open problem for almost two decades to come up with a satisfying construction for it. In 2001, Boneh and Franklin [5] proposed formal security notions for IBE systems and designed a fully functional secure IBE scheme using bilinear maps. Since the pioneering work of Boneh and Franklin [5], many IBE schemes [4, 11, 13, 14, 33] were proposed in bilinear maps.

Identity-based encryption (IBE) is a kind of public key encryption (PKE) that uses any bit-string (e.g., e- mail address, phone number, or identity) as a public key of a user. Identity-based PKI [12] is the binding between the public/private keys and the individual. In IBE, a single key generation center (KGC) should issue private keys and establish secure channels to transmit private keys of users. To reduce the cost of private key generation of the KGC in IBE, the concept of hierarchical IBE (HIBE) [7] was introduced such that the KGC delegates the key generation functionality to a lower level KGC [22, 29] using sequential and threshold manner.

The first construction of HIBE is due to Gentry and Silverberg [12] where the security is based on the random oracle model. Subsequently, Boneh and Boyen [4] presented a HIBE without random oracles in the selective-ID model [25]. The best known HIBE constructions, both with and with- out random oracles, are based on bilinear maps (Boneh *et al.*, 2005; Boyen and Waters, 2006; Gentry and Halevi, 2009; Waters, 2009). More recent HIBE schemes are built over lattices proposed by Agrawal *et al.* [1,2]. In all these constructions, the sizes of ciphertexts and private keys, as well as the decryption cost, grow linearly with the identity depth. Boneh *et al.* [12] proposed the first HIBE system with constant size ciphertext and without random oracles, whereas the provable security is under the selective-ID model.

3 Preliminaries

We briefly review bilinear maps and bilinear map groups.

3.1 Bilinear Pairings

Let n be a prime number. Let $(\mathbb{G}_1, +)$ be an additive $(+)$ cyclic group of order q, where q is the prime and $(\mathbb{G}_2, x)$ be an multiplicative (x) group of order q. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ with the following properties [31]:

- **Bi-linearity:** $e(aP, bQ) = e(P, Q)^{ab}$ where $P, Q \in \mathbb{G}_1, a, b \in \mathbb{Z}_q^*$
- **Non-degeneracy:** $e(G, G) \neq 1$. Therefore, it is a generator of $\mathbb{G}_2$.
- **Computability:** There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

For any $a \in Z_q$ and $P \in G_1$, we write aP as the scalar multiplication of group element P by integer a. Typically, G_1 is obtained as a subgroup of the group of points on a suitable elliptic curve over a finite field, and G_2 is obtained from a related finite field.

For simplicity, we define ID-based encryption systems in the below.

3.2 Identity Based Encryption

The main motivation for Identity Based Encryption is to help the deployment of a public key infrastructure. Boneh and Franklin [5] were the first to propose a feasible IBE system based on the Weil pairing in 2001. After shamir's proposal in 1984 [27], it was proposed nearly two decades in 2001.

An identity based encryption (IBE) algorithm is a tuple of algorithms $(Setup, KeyDer, Encrypt, Decrypt)$ provides the following features. The trusted third party runs $Setup$ to create a master key (MSK). It outputs public parameters mpk which are kept public and keeps the master secret key MSK private. At the point when a client with identity ID would like participate in the framework, the trusted authority produces a decryption key $d_{ID} \leftarrow KeyDer(msk, ID)$, and sends this key over a protected and validated channel to the client. To send a scrambled message m to the client with identity ID, the sender processes the ciphertext $C \leftarrow Encrypt(mpk, ID, m)$, which can be decrypted by the client as $m \leftarrow Decrypt(d_{ID}, C)$.

3.3 Hierarchical Identity Based Encryption

A HIBE system consists of the following five algorithms *HIBE = (Setup,Extract, Derive, Encrypt, Decrypt)*. The root PKG runs the Setup algorithm to output public and private parameters for HIBE setting, including a bilinear pairing as HIBE context, public parameters and master key only known to the root PKG (at level 0). The Extract algorithm generates private keys for all identities in hierarchy with master key, public parameters and identities as input, and distributes private keys to their owners via trusted channel. Algorithm Derive functions alike to Extract. It is used by ancestor entities to generate private keys for their descendants, or delegate private keys along hierarchy. The Encrypt algorithm encrypts a message on the intended recipient's identity. Algorithm Decrypt uses the intended recipient private key to decrypt a cipher text.

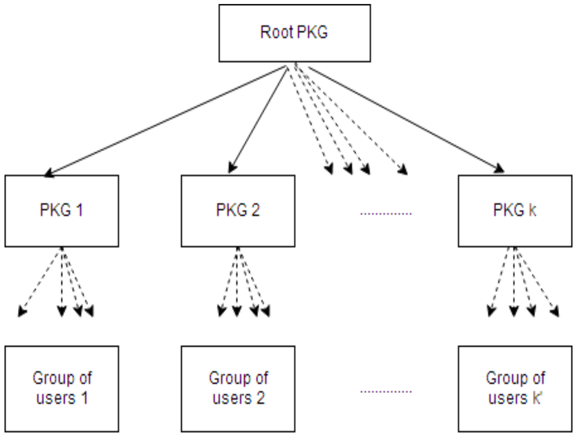

Figure 1: Hierarchical ID based encryption

3.4 Security Assumptions

In this subsection we present the complexity assumptions [3, 34] required for our construction.

Computation Diffie-Hellman Problem (CDH) - Given $(g, g^a, g^b) \in \mathbb{G}^3$ for unknown $a, b \in \mathbb{Z}^*$, where $G$is a cyclic prime order multiplicative group with g as a generator and q the q order of the group, the CDH problem in G is to compute g^{ab}.

The advantage of any probabilistic polynomial time algorithm A in solving the CDH problem in $\mathbb{G}$ is defined as $Adv_A^{CDH} = Pr[A(g, g^a, g^b) = g^{ab} | a, b \in \mathbb{Z}_q^*$.

The CDH Assumption is that, for any probabilistic polynomial time algorithm A, the advantage Adv_A^{CDH} is negligibly small.

Decisional Diffie-Hellman Problem (DDH) - Given $(g, g^a, g^b, h) \in_R \mathbb{G}^4$ for unknown $a, b \in \mathbb{Z}^*$, , where G is a cyclic prime order multiplicative group with g as a generator and q the order of the group, the DDH problem in G is to check whether $h = g^{ab}$.

The advantage of any probabilistic polynomial time algorithm A in solving the DDH problem in G is defined as

$Adv_A^{DDH} = |Pr[A(g, g^a, g^b, g^{ab}) = 1] - Pr[A(g, g^a, g^b, h) = 1]||a, b \in \mathbb{Z}_q^?$.

The DDH Assumption is that, for any probabilistic polynomial time algorithm A, the advantage $AdvA$ is negligibly small.

4 Distributed Key Issuing Protocol

In this section, we present our proposed distributed key issuing protocol [18] using threshold cryptography. It will be useful for increasing the hierarchy with maximum number of level and recovery of decryption secret is with threshold number of participants.

A distributed PKG, KPAs (Key Privacy Authorities) and the user (receiver) have the partial private key of the decryption secret key (S). An HIBE scheme with an (t, n)- distributed PKG along with KPAs and User consists of the following components:

4.1 Overview

The proposed protocol divided into five sub phases namely **Setup, System public key setup, Key is -suing, Key securing, and Private Key reconstruction**. Throughout this algorithm we use KGC - is a PKG, KPAs - intermediate trusted authorities and User is a private key receiver.

Setup: (run by KGC) The KGC selects initial parameters such as hash functions, groups under addition and multiplication, bilinear maps, master key and calculate the public key.

System public key setup: (run by KGC and KPAs) Here the KPAs run the Asmuth bloom (t,n) threshold scheme and generates the shares for the common secret. KGC collect shares from KPAs and calculate the system public key.

Key issuing: (run by KGC and User) In this phase, new user joins and interact with KGC to collect partial private key from KGC. Here User registration and

KGC response provides partial private key to the user.

Key securing: (run by User and KPAs) User selects any pair of $t+1$out of $n(n > 2t)$ or $n = 2t+1$) KPAs and run the robust secret sharing algorithm which gives even t of KPAs corrupted the user able to reconstruct partial private key with a random value.

Private Key reconstruction: (run by User) Finally, user combines the partial private keys issued by KPAs and KGC along with his partial private key for the re- construction of original private key which can be used for decryption of cipher-texts.

5 Proposed Hierarchical Identity Based Encryption

Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ be a bilinear map, where $\mathbb{G}$ is a group of prime order P. An identity is defined as $ID = (I_1, \cdots, I_k) \in (\mathbb{Z}_p^*)^k$, where k is the depth of the hierarchy that the ID belongs to. There are four algorithms: Setup, Keygen, Encryption and Decryption. l is the maximum depth of the hierarchy allowed.

- **Setup**(1^λ)**:** It runs a probabilistic polynomial time (PPT) algorithm which takes a security parameter λ as input and outputs $mastersecretkey(MSK)$ and $I = \{0,1\}^\lambda$ be the identity space.
  - Select a generator $g \in \mathbb{G}$, $\mathbb{G}$ is a group of prime order P and obtains a bilinear group;
  - Choose $f_1, f_2 \in \mathbb{G}$ and randomly $x, y \in \mathbb{Z}_P$;
  - Compute $u = g^x$ and $v = g^y$;
  - Pick randomly $h_1, h_2, \cdots, h_l \in \mathbb{G}$;
  - Calculate MSK $= g^\alpha$, where $\alpha = x.y$;
  - Publish public parameters $params = (g, f_1, f_2, h_1, h_2, \cdots, h_l)$.
- **Keygen**$(ID_{|k}, MSK, Params)$**:** It runs a probabilistic polynomial time (PPT) algorithm which takes an identity $ID_{|k} = (I_1, \cdots, I_k) \in I^k$, MSK and *params* as input and outputs private key $SK_{ID_{|k}}$ for k^{th} level identity ID in sequential manner to avoid Key escrow problem.
  - Choose random exponents $r_1, \cdots, r_k \in \mathbb{Z}_p$;
  - Compute $SK_{ID_{|k}} = (b_0 = g^\alpha.(\prod_{i=1}^{k-1} h_{ij}^{I_j}.g_3)^r, b_1 = g^r)$ and $b_k, \cdots b_l = h_k^r, \cdots, h_l^r$
  - Generation of K^{th} level private key:
    - Select a random $t \in \mathbb{Z}_P$;
    - Compute private key for $SK_{ID_k} = (b_0.b_k^{I_k}.(\prod_{j=1}^{k} h_j^{I_j}.f_2)^t, b_1.g^t, h_{k+1}^t, \cdots, h_l^t)$.
- **Encrypt**$(ID_{|k}, M, Params)$**:** It runs a probabilistic polynomial time (PPT) algorithm which takes public key $ID_{I_l} = (I_1, \cdots, I_l) \in I^l$, message (or plain text) $M \in \mathbb{M}$, and the *params* as input along with $t, s_1, \cdots, s_k \in \mathbb{Z}_p$ and outputs cipher text C.

  Cipher text is $C = (C_1, C_2, C_{i,3}, C_{i,4})$, where
  - $C_1 = e(f_1, f_2)^{t.\alpha}.M$
  - $C_2 = g^t$
  - $C_{i,3} = g^{s_i}$;
  - $C_{i,4} = \{(h_1^{I_1}, \cdots, h_k^{I_k}.f_2)\}_{i=1}^t$.
- **Decrypt**$(C, SK_{ID_{|k}}, Params)$
  It runs a deterministic algorithm which takes cipher text C for $ID_{|l}$, private keys of $SK_{ID_{|k}}$ for $ID_{|k}$ and *params* as input and outputs message M as follows:

$$M = \frac{C_1.(C_2, SK_{ID_{i,1}})^{-1}}{\prod_{i=1}^{k} e(C_{i,3}, SK_{ID_{|k}}).e(C_{i,4}, SK_{ID_{|k}})}.$$

5.1 Correctness

With cipher text C encrypted with private key $SK_{ID_{|k}}$ for each identity $ID_k = ((I_1, \cdots, I_k))$, the $\prod_{i=1}^{k} e(C_{i,3}, SK_{ID_{|k}}).e(C_{i,4}, SK_{ID_{|k}})$ is calculated as $M.C_1.(C_2, SK_{ID_{i,1}})^{-1}$ provides consistency of our proposed HIBE scheme.

6 HIBE Security Analysis

In this section, we present security analysis and efficiency of proposed modified HIBE scheme. The security of (unbounded) HIBE is defined via the following experiment between a challenger C and an adversary A, denoted by $Exp_A^{HIBE}(\lambda, n)$.

Setup. C runs Setup and sends master public key mpk to A.

Phase 1. A is capable of acquiring secret keys for any identity vector by making key extraction queries. C answers the query by invoking **KeyGen**.

Challenger. A submits two messages (m_0^*, m_1^*) of equal length and a challenge identity vector x^* with the restriction that no prefix of x^* has been requested in Phase 1. C flips a coin toss $\beta \leftarrow \{0,1\}$ and encrypts m_β^* under x^*. The resulting challenge ciphertext $CT_{x^*}^*$ is sent back to A.

Phase 2. A can make more key extraction queries with the restriction above.

Guess. A outputs its guess $\beta' \in \{0,1\}$.

An adversary A wins iff $\beta = \beta$. We use $Exp_A^{HIBE}(, n) = 1$ to denote this event. The probability space is defined by all randomness used by C and A. We define the advantage function of an adversary A as

$$Adv_A^{HIBE}(, n) = |Pr[Exp_A^{HIBE}(, n) = 1] = 1/2|.$$

6.1 Security in Standard Oracle Model

We define the security of our scheme equivalent to that of HIBE schemes, but with the adversary choosing a challenge pattern instead of an identity to which the challenge ciphertext will be encrypted.

More formally, the IND-CPA (Indistinguishability under Chosen Plaintext Attack) security model is defined through the following game, played between an adversary $A = (A_1, A_2)$ and a challenger:

- The challenger generates a master key pair $(mpk, msk) \leftarrow Setup$.
- The adversary runs A_1 on mpk. The adversary is given access to a key derivation oracle that, on input of an identity $ID = (ID_1, ..., ID_l)$, returns the secret key $d_{ID} \leftarrow KeyDer(msk, ID)$ corresponding to that identity. The adversary outputs two equal-length messages (m_0, m_1) and a challenge pattern P, along with some state information state.
- The challenger chooses a bit $\beta \leftarrow \{0, 1\}$ and computes the ciphertext $C \leftarrow Encrypt(mpk, P, m\beta)$.
- The adversary runs A_2 on the input C and the state information state. The adversary is given access to a key derivation oracle as before. The adversary outputs a bit $\beta^{'}$.

The adversary wins the game if $\beta = \beta^{'}$ and it never queries the decryption oracle on any identity ID which matches the pattern P, *i.e.* any identity $ID \in P$. The adversary's advantage is defined as $|2Pr[Awins] - 1|$.

6.2 Efficiency

The proposed HIBE method having the fixed constant ciphertext size, private keys sk, l for Hierarchical path in the distributed manner. And our scheme achieves public keys $O(k)$ and private key achieve $O(l)$ size. We have presented comparison efficiency of the existing schemes with our proposed scheme in Table 1.

Table 1: Comparison efficiency

Schemes	Cipher text size	sk size	pk size
[27]	$O(k)$	$O(k)$	$O(l)$
[14]	$O(1)$	$O(l-k)$	$O(l)$
[15]	$O(k)$	$O(k)$	$O(l)$
[34]	$O(1)$	$O(l-k)$	$O(l)$
[21]	$O(klnd^2)$	$O(k^2l^2n^2d^2)$	$O(kn^2d^3)$
[23]	$O(lnd^2)$	$O(l^2n^2d^2)$	$O(n^2d^3)$
Our method	$O(1)$	$O(l)$	$O(k)$

7 Applications

Identity-based encryption (IBE) [13, 27], an important primitive that can be used to ensure the data confidentiality for secure communication in several domains.

7.1 Public key Infrastructure (PKI)

In the identity-based setting, the public key is bound to the transmitted data while the binding between the private key and the individual is managed by the TA (Trusted Authority). Boneh and Franklin suggested in [5] that key escrow can be circumvented by using multiple TAs and threshold cryptography. On the other hand, because of this built-in feature, the user always needs to set up an independent secure channel with his TA for retrieving private key material.

7.2 Private Messaging

The system of a PKI comprises of security and operational arrangements, security administrations, and interoperability conventions supporting the utilization of open key cryptography for the administration of keys and certificates. A PKI empowers the foundation of a trust hierarchy. These interesting properties of IBC show the likelihood of building up an option security framework that gives more prominent adaptability to substances in- side an public environment.

We discuss proposed PKI structure [11] as follows: A client in this framework is a client who has an arrangement of different clients enlisted with it as contacts. This client enrolment is bi-directional. As it were when client A turns into a contact of client B, client B turns into a contact of client A. A client expects to send messages to every one of its contacts. These messages are to be conveyed to the client contacts by then of time. This is like the idea of microblogging. (Illustration: Facebook and Twitter). Such a message is identified as an update.

We present the problem of a contact obtaining an update that it missed anonymously with the following requirements:

- A user P should be able to simply send its update M_P only to those contacts who are available online at the point of time it sends the update using direct connections to those users. We denote the set of online contacts as $C^+ \subseteq C$ where $|C^+| \geq 1$.
- All the contacts of P who were off-line at when P sent M_P should be able to obtain M_P when they are available online. List those contacts as $C^- \subset C$. Any $C_{P_i} \in C^-$ can publish a query requesting an update of P that is called Q_P.
- Any $C_{P_i} \in C^+$ will have the capacity to distribute a response to a Q_P. This response is denoted by S_P and an eavesdropper with polynomially bounded resources should not be able to compute the original M_P using S_P.

- The contact who provides S_P should not be able to learn who generated Q_P. The contact who generates Q_P and gets the relating S_P should be able to extract M_P but should not be able to learn who generated S_P.
- At the point when the creation of C changes to new arrangement of clients C', P should be able to update private setup of the members of C' with the issue of a public message.
- After such an update those clients in the set $C - C'$ should not be able to obtain an update of P.

Users in the HIBPKI setting do not need to obtain short-term private keys from their respective PKGs. This is because the users themselves act as PKGs for their local proxy clients.

8 Conclusion

An Identity-Based Encryptions (HIBE) are concerned, it is rational to viewed the root PKG (Private Key Generator) as a trusted party or being unconditionally trusted, but those level PKGs should be treated suspiciously in hierarchical identity based encryption. In order to resolve key escrow problem in HIBE, in this paper, we propose a new efficient hierarchical identity based encryption scheme standard security model, a modification to the proposed by Boneh *et al.*by avoiding key escrow problem with maximum hierarchy. Details of the scheme is provided with level evaluation with encryption privacy and correctness of the scheme. Security analysis of the scheme along with comparative analysis are discussed. At end, we presented applications of HIBE in public key infrastructure and private message communication.

References

References

[1] S. Agrawal, D. Boneh, X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proceedings of 30th Annual Cryptology Conference*, pp.98-115, 2010.

[2] S. Agrawal, X. Boyen, Vaikuntanathan, "Functional encryption for threshold functions (or fuzzy IBE) from lattices," in *Proceedings of 15th International Conference on Practice and Theory in Public Key Cryptography*, pp. 280-297, 2012.

[3] O. Blazy, E. Kiltz, J. Pan, "Identity-based encryption from affine message authentication," in *Advances in Cryptology*, pp. 408425, 2014.

[4] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *ACM Conference on Computer and Communications Security*, pp. 417-426, 2008.

[5] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'01)*, vol. 2139, pp. 213-229, 2001.

[6] D. Boneh and X. Boyen, "Efficient selective id secure identity-based encryption without random oracles," in *Advances in Cryptology*, vol. 3027, pp. 223-238, 2004.

[7] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *Advances in Cryptology*, vol. 3494, pp. 440-456, 2005.

[8] X. Boyen and B. Waters, "Anonymous hierarchical identity based encryption (without random oracles)," in *Advances in Cryptology*, vol. 4117, pp. 290-307, 2006.

[9] J. Chen, H. Wee, "Fully tightly secure IBE and dual system groups," in *Advances in Cryptology*, pp. 435460, 2013.

[10] J. Chen, H. Wee, "Dual system groups and its applications compact HIBE and more," in *IACR Cryptology ePrint Archive*, pp. 265, 2014.

[11] R. Fnado, B. Bharat, "Mark L - Private anonymous messaging," in *IEEE International Symposium on Reliable Distributed Systems*, pp. 430–435, 2012.

[12] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *Advances in Cryptology*, vol. 2501, pp. 548-566, 2002.

[13] C. Gentry, "Practical identity based encryption without random oracles," in *Advances in Cryptology*, vol. 4004, pp. 445-464, 2006.

[14] C. Gentry and S. Halevi, "Hierarchical identity based encryption with polynomially many levels," in *Theory of Cryptography (TCC'09)*, vol. 5444, pp. 437-456, 2009.

[15] C. Gentry, "Practical identity-based encryption without random oracles," in *Proceedings of the Advances in Cryptology*, vol. 4004, pp. 445464, 2006.

[16] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in *Advances in Cryptology*, vol. 2332, pp. 466-481, 2002.

[17] S. Jahid, P. Mittal, N. Borisov, "EASiER: encryption-based access control in social networks with efficient revocation," in *ACM (ASIACCS'11)*, pp. 411415, 2011.

[18] D. Kalyani and R. Sridevi, "Robust distributed key issuing protocol for identity based cryptography," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI'16)*, pp. 821-825, 2016.

[19] B. Lee, E. Boyd, E. Daeson, K. Kim, J. Yang and S. Yoo, "Secure key issuing in ID-based cryptography," in *proceedings of the Second Australian Information Security Workshop (AISW'04)*, pp.69-74, 2004.

[20] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," in *Theory of Cryptography*, vol. 5978, pp. 455-479, 2010.

[21] A. B. Lewko, B. Waters, "Unbounded HIBE and attribute-based encryption," in *Advances in Cryptology*, pp. 547567, 2011.

[22] D. K. Pattipati, A. N. Tentu, V. Ch. Venkaiah, "Sequential secret sharing scheme based on level ordered access structure," *International Journal Network Security*, pp. 874-881, 2016.

[23] Y. L. Ren and D. W. Gu, "Efficient hierarchical identity based encryption scheme in the standard model," *Wuhan University Journal of Natural Sciences*, vol. 32, no. 2, pp. 207-211, 2008.

[24] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*, vol. 3494, pp. 457-473, 2005.

[25] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*, vol. 3494, pp. 457-473, 2005.

[26] J. H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in *Cryptology (CT-RSA'13)*, vol. 7779, pp. 343-358, 2013.

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, vol. 196, pp. 47-53, 1984.

[28] A. N. Tentu, A. Basit, K. Bhavani, V. Ch. Venkaiah, "Multi-secret sharing scheme for level-ordered access structures," *Number-Theoretic Methods in Cryptology*, pp. 267-278, 2017.

[29] A. N. Tentu, P. Paul, V. Ch. Venkaiah, "Computationally perfect compartmented secret sharing schemes based on MDS codes," *International Journal of Trust Management in Computing and Communications*, pp. 353-378, 2014.

[30] A. N. Tentu, V.Ch. Venkaiah, V. K. Prasad, "CRT based multi-secret sharing schemes: Revisited," *International Journal of Network Security*, vol. 16, no. 4, pp. 249-255, 2018.

[31] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[32] X. Wang and X. Yang, "Cryptanalysis of two efficient HIBE schemes in the standard model," *Cryptology ePrint Archive*, vol. 109, no. 2, pp. 189-200, 2011.

[33] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology*, vol. 3494, pp. 114-127, 2005.

[34] B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions," in *Advances in Cryptology*, vol. 5677, pp. 619-636, 2009.

Biography

D. Kalyani is working as Assistant Professor in Department Information Technology at VNRVJIET, Hyderabad, and also pursuing her Ph.D in Computer Science and Engineering from JNTU Hyderabad. where she teaches Information Security Management and Standards for post graduates. Her research interests focus on the Cryptography and Information Security.

R. Sridevi is a Professor and heading Computer Science and Engineering Department at JNTUH College of Engineering Hyderabad, Jawaharlal Technological University Hyderabad. She received her Ph.D in 2010. Her research interests include Steganography, Steganalysis, Network security and Cryptography, Computer Networks. She has published more than twenty research papers in reputed journals and eight international and national conferences.