Identity Based Encryption and Identity Based Signature Scheme: A Research on Security Schemes

Maitri Patel, Rajan Patel

Abstract— In computer based system, key for the problem of identification, authentication and secrecy can be found in the field of cryptography. Dependence on public key infrastructure and to receive certificates signed by Certificate Authority (CA) to authenticate oneself for exchange of encrypted messages is one of the most significant limitation for the widespread adoption of Public Key Cryptography (PKC) as this process is time engrossing and error prone. Identity based cryptography (IBC) aspires to reduce the certificate and key management overhead of PKC. IBC's important primordial is Identity-based Encryption (IBE). IBE provided emergent for perception of Identity based signature (IBS) schemes. In this paper, overview of IBE and IBS schemes has been given. Also, a survey on various IBE and IBS schemes has been performed to review different problems related to them. Finally, feasibility and applicability of IBC in current and future environments has been discussed.

Keywords: Certification Authority, Identity Based Cryptography, Public Key Cryptography, Identity Based Encryption, Security, Identity Based Signature

I. INTRODUCTION

Cryptography has mainly five elements named plain text, cipher text, keys, and encryption & decryption algorithm. In PKC, public private key pairs has been maintained. Everyone will know public key and private key has been kept secret with user. One form of public-key cryptography (PKC) is IBE. Main idea behind introducing IBE was to reduce the overhead of certificate management and thus debar CA and its need. [1]

1.1 Identity-based Encryption (IBE)

In 1984, A.Shamir has introduced perception of IBC. [2] In suggested scheme, for encryption or signature verification, user's identity like email or IP address is being utilised in place of digital certificates. Thus, the scheme remarkably reduces the complication and expense for certificate management of public key infrastructure (PKI).

In cryptography field, IBC has attracted the researcher's attention [3] as Shamir's [2] IBE scheme was persisted as an open issue till 2001. Initially, D.Boneh and M.Franklin [4] put up practical IBE scheme secured in random oracle model. [5] After that, Boneh and Boyen [6], suggested fully secure scheme without random oracle. The fully secure scheme introduced by Boneh and Boyen [6] was improved and simplified by Water [7]. Coke [8] has also provided the solution for the open problem related to IBC.

Overview of Cryptographic Operations [5]

IBE relies on reliable arbitrator called Private Key Generator (PKG). PKG produces master public/private key pair (pk_{PKG} and sk_{PKG}) respectively. pk_{PKG} is publicly accessible to all the users.

Encipher and decipher process for IBC is described as follows:

1. User A obtains cipher text C by encrypting plaintext message M with ID_B (User B's identity) and pk_{PKG} (master public key) and sends C to User B. Note that User A does not require any prior communication on User B's part to encrypt message M.
2. After receiving cipher text C from User A, User B authenticates to PKG with adequate proof that ID_B owned by him. After successful authentication, PKG sends User B's private key sk_{IDB} through secure channel.
3. User B retrieves plaintext message M by decrypting C using his private key sk_{IDB}.

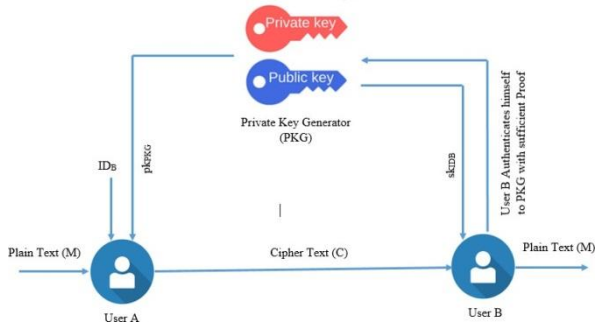

Figure 1. Identity Based Encryption

One variant of IBE described above is also available. In that variant, PKG is authorised to decrypt C for User B and transmits decrypted text securely after successful authentication.

1.2 Identity-based Signature (IBS)

When Shamir [2] has proposed IBE scheme, he has also suggested IBS scheme by utilising existing RSA function. IBS scheme, mirror image of IBE can be described as follows [3, 5]:

Revised Manuscript Received on April 22, 2019.

Maitri Patel, Research Scholar, Faculty of Engineering & Technology Sakalchand Patel University, Visnagar, Gujarat, India (Email: maitru1487288@gmail.com)

Rajan Patel, Associate Professor, Department of Computer Engineering, Gandhinagar Institute of Technology, Moti-Bhoyan, Gandhinagar. Gujarat, India (Email: rgpce21@gmail.com)

1. User A receives private key sk_{IDA} after successful authentication to PKG.
2. By using sk_{IDA}, User A generates the signature σ for plain text message M and transmits it to User B.
3. After obtaining M, User B verifies σ by using User A's identity ID_A and pk_{PKG}. If the signature is genuine, User B returns "Accepted". Otherwise, User B returns "Rejected". Here, there is no need for User B to get the certificate form User A.

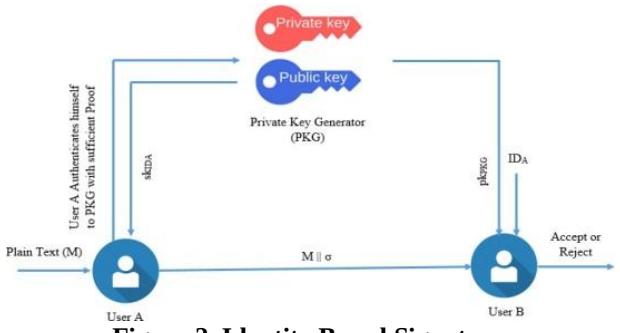

Figure 2. Identity Based Signature

Following is formation of the remaining paper: Section 2 examines open problems associated to IBE and IBS in detail. Section 3 presents survey on existing security systems implemented using IBE to provide security and their vulnerabilities against various type of attacks. In Section 4, survey on existing security systems implemented using IBS to provide authentication and their vulnerabilities against various type of attacks has been discussed. Section 5 contains information related to implementation details. Conclusions are being presented in Section 6.

Open Problems related to IBE and IBS:

2.1 Key Escrow

In IBE and IBS scheme [3], any message can be decrypted and signed by PKG as it issues private key to user using master secret key. In IBE, this may be helpful where user has forgot his or her private key. When analysing IBC system security this consideration should be taken into account as it will be depend on IBC adopter's choice. But in IBS, it infringes the most essential need of digital signature scheme i.e. "non- repudiation" property. Boneh and Franklin [9] suggested solution for this problem but the solution enforces big communication and computational cost. [3] Hence, to build IBE or IBS scheme without key escrow problem is still resides as an open question.

2.2 Non-Repudiation

In IBC system, it is assumed that PKG is not signing messages or it signs messages only on user's request. Failure of this assumption causes the violation of non-repudiation property.

2.3 Key Revocation

Suppose user's private key associated with its mail id has been compromised, then what does he/she need to do? Does he/she has to create or change the mail address? What if, he/she has used his biometric data as a part of private key? Again, Boneh and Franklin [9] suggested the solution for this problem to add timestamp to the public key. But it raises new problems like what will be the time format or validity of that time-stamp? Hence, it still remains the open problem to build key revocation free IBC system.

2.4 Other Open Problem

To provide high level security to PKG and availability of PKG to send private keys to users, make PKG more vulnerable to attack. Also, to construct IBE scheme without bilinear pairing and efficient compared to Coke's scheme. [3]

1. Results & Discussions

The table 1 gives the overview of IBE systems related to security services provided by the system. Also, it provides information about the type of attack which has been detected or prevented by the system.

Sr No	Proposed Method	Security Services	Attack Detection	Attack Prevention	Type Of Attack/ Problem	Remarks
1	Identity Based Online/ Offline Encryption [10] (IBOOE)	Confidentiality	Yes	Yes	Chosen Plaintext Attack	Works on polynomial time algorithm and Diffie-Hellman algorithm
2	Identity Based Online/ Offline Key Encapsulation Management [10] (IBOOKEM)	Confidentiality	Yes	Yes	Chosen Cipher Text Attack	Works on polynomial time algorithm and Diffie-Hellman algorithm
3	mKDM-sID-CPA [11] IBE Scheme	Confidentiality	Yes	Yes	Chosen Plaintext Attack	The master public key and cipher text sizes rely on number of challenge queries or number of users n

4	Intrusion Detection Sensor(IDS) using [12] IBE	Authentication and Confidentiality	Yes	Yes	Man-in-the- middle attack	Suggested system includes change in supported and widely-known implementations like OpenSSL
5	New biometric IBE scheme based on BIO-IBE[13]	Confidentiality	Yes	Yes	Denial of Service (DoS) attack	Security of the proposed method is not provided compared to earlier system in standard model
6	An efficient RIBE with a public channel[14]	Confidentiality	Yes	Yes	Adaptive chosen plaintext attacks and adaptive chosen cipher text attacks	Works on Diffie–Hellman Algorithm
7	Mediated Identity Based Encryption scheme[15]	Confidentiality	Yes	Yes	Known Message Attack	Uses online mediator to provide privacy sessions. Not secure if KGC or online mediator is compromised
8	Communication protocol based on IBE[16]	Confidentiality	Yes	Yes	Known Message Attack	Improves the key escrow capabilities compare to original IBE. Less efficient compare to original IBE.
9	Revocable Key IBC Without Key Escrow[17]	Confidentiality	Yes	Yes	Replay attack, Private Key Recovery by an Attacker, Key escrow Attack, Compromised Key Attack	Uses E-mail id for generating public key. Needs to update secret value whenever informed by Key Generation Centre(KGC)
10	Revocable Identity Based Encryption Scheme[18]	Confidentiality	No	Yes	Decryption Key Exposure	Uses complete binary tree for key revocation and KUnode algorithm to reduce key cost. Security proven only in their security model.
11	LV-RIBE scheme[18]	Confidentiality	No	Yes	Decryption Key Exposure	Proves that proposed scheme is not safe against Decryption Key Exposure attack
12	BGK-RIBE scheme[18,19]	Confidentiality	No	Yes	Decryption Key Exposure	Security guarantees offered only in the relaxed selective-ID model where target identity must be chosen ahead of time by adversaries Proves that proposed scheme is not safe against Decryption Key Exposure attack
13	Improved Identity Based signcryption (IBSC) Scheme[20]	Confidentiality and Authentication	No	Yes	Adaptively Chosen Plain Text and Identity Attack	Scheme is secured by considering intractability of DBDH assumption as a base in standard model
14	Revocable Hierarchical Identity-Based Encryption (RHIBE) scheme[21]	Confidentiality	No	Yes	Identity Attack	Tries to resolve open question of Libert and Vergnaud IBE system. Considers BBHIBE scheme as a base for construction and only selective security under DBDH assumption has been proven in the standard model for construction.

15	IDGSC[22]	Confidentiality and Authentication	No	Yes	Identity Attack	Proposed complete security model is more comprehensive than existing model. The proposed scheme has less implementation complexity and comparable computational complexity compare to existing normal signcryption schemes.

Table 1. Survey on IBE Security Systems

2. Survey on Existing IBS Security Systems based on various type of attacks:

The table 2 gives the overview of IBS systems related to security services provided by the system. Also, it provides information about the type of attack which has been detected or prevented by the system.

Sr No	Proposed Method	Security Services	Attack Detection	Attack Prevention	Type Of Attack/ Problem	Remarks
1	Escrow free IBS scheme[23]	Authentication	Yes	No	Known Message Attack	Key escrow problem of IBS has been solved without requiring multiple PKGs
2	Efficient escrow free IBS scheme[24]	Authentication	Yes	No	Known Message Attack	Efficient and practical solution compared to earlier system
3	Key escrow free IBS scheme[25]	Authentication	Yes	Yes	Unregistered Identity Attack	Solves the key escrow problem More efficient compare to Das signature scheme
4	Identity-based signature scheme using bilinear pairings[26]	Authentication	Yes	Yes	Chosen Message Attack	Need for secure channel has been eliminated between user and KGC. Not secured against unregistered identity attack
5	Identity Based Authenticated Key Exchange[27]	Authentication	No	Yes	Man in the Middle (MITM) Attack	MITM attack is possible if someone behaves like authenticated PKG
6	Strongly Unforgeable Revocable Identity Based Signature Scheme[28]	Authentication	No	Yes	Adaptive Chosen Message Attack	Secured in standard model under Computational Diffie-Hellman (CDH) and Collision resistant hash (CRH) assumption
7	Improved Identity Based signcryption (IBSC) Scheme[29]	Confidentiality and Authentication	No	Yes	Adaptively Chosen Message and Identity Attack	Scheme is secured based on intractability of the Decisional Bilinear Diffie- Hellman (DBDH) assumption in standard model.

8	IBS scheme Based on Water's ID- based encryption scheme[30]	Authentication	No	Yes	Chosen Message Attack	CDH assumption has been used as a base for the proposed scheme. Drawback of proposed scheme is large size public parameters.
9	Lightweight Identity Based Signature Scheme[31]	Authentication	No	Yes	Adaptively Chosen Plain Text and Identity Attack	Secured in random oracle model under discrete logarithm assumption. Larger bit complexity compare to existing system
10	IBKIS-NOKE[32]	Authentication	No	Yes	Man-in-the- middle (MITM) attack	Solves key escrow and Key update problem Not secure if the key stored in user device is being compromised
11	IBS-1 and IBS-2 By Rossi and Schmid[33]	Authentication	No	Yes	Adaptively Chosen Message and Key Disclosure Attack	Security proof has been given for the proposed IBS schemes that they are not secure against Adaptively Chosen Plain Text and Key Disclosure Attack
12	EIBS[34]	Authentication	No	Yes	Identity Attack	Probably secure in random oracle model under the CDH assumption.
13	IDGSC[35]	Confidentiality and Authentication	No	Yes	Identity Attack	Proposed complete security model is more Comprehensive than existing model. The proposed scheme has less implementation complexity and has comparable computational complexity compare to existing normal signcryption schemes.
14	Forward-secure identity-based signature scheme[36]	Authentication	No	Yes	Key Exposure Attack	Introduces forward security in IBS scheme. Suggested scheme's security has been proven by considering l + 1- computation Diffie– Hellman assumption as a base without random oracles
15	Leakage-free IBS scheme[37]	Authentication	Yes	Yes	Ephemeral Secret Leakage, Adaptive Chosen Plain Text and ID Attack	Security of suggested scheme has been proven in random oracle model by considering CDH assumption as a base under defined security notion.

Table 2. Survey on IBS Security Systems

3. Related Works(Implementation)[3,5]:

D.Boneh and M.Franklin had suggested the IBE scheme called "Stanford IBE system" was implemented in C++ under Debian GNU/Linux. [9] The implementation code can be obtained at http://crypto.stanford.edu/ibe/download:html.

IBE email system which provides plugins for Outlook, hotamail etc. was developed by Voltage Security is the most noticeable real world application of IBE. Proofpoint, Inc. provides licensed value add-ons to Voltage's software. Hewlett Packard Lab in Bristol, UK has implemented health care information system with IBE capability.

Till now, there is not any java implementation of IBE exist in public domain. According to Naor's observation, a secure (public key) signature can be obtain through conversion of any IBE system [38] under same assumption and IBS schemes are mirror image of the corresponding IBE systems [2]. Also, as per our knowledge and based on survey performed, there is not any DNS security system which is implemented using IBE.

Sr No.	System Name	Type (Open Source/ Licensed/ Free)	Platform	Implementation Language	Developed by	Remarks
1	Stanford IBE System[3, 5,9]	Open Source	GNU/ Linux	C++	Boneh and Franklin, 2003	System security has been proved through random oracle model. At present, constructing a chosen cipher text secure IBE in the standard model is an open question.
2	Voltage Identity-Based Encrypti on (IBE) system[39, 40]	Licensed	GNU/Lin ux/MS Windows	C++	Voltage Security, 2007	Uses the IBE system which was implemented by Boneh and Franklin.
3	Proposed IBE System[41]	Open Source	MS Windows /Linux	C/Java(For GUI)	Anastasios Kihidis, Konstantino s Chalkias, and George Stephanides , 2010	The system's stability is currently being tested.
4	IBE System[42]	Licensed	MS Windows /Linux	Java	Louise Owens, Adam Duffy, Tom Dowling	IBE system can be extended to include features like public key revocation, IBE signature schemes and Key-escrow problem.

Table 3. Survey on Implementation of IBE Systems

II. CONCLUSION

According to survey performed, IBE makes things simpler compare to PKI. IBE and IBS schemes are less time consuming as they do not require CA and key distribution for message exchange. Also, IBE is cost effective compare to PKI as the need to exchange the certificates for authentication has been removed. There are various IBE and IBS security systems available to provide confidentiality and authentication respectively. But, these security system are vulnerable against security attacks and also does not provide perfect solution for the open problems related to IBE and IBS. Also, most of the systems are implemented in C++. Thus, there is a need of security system that can provide solution to the open problems related to IBE and IBS.

REFERENCES

1. Hussain, Mehdi, and Mureed Hussain. "Advance Applications of Identity Based Encryption."
2. Shamir, Adi. "Identity-based cryptosystems and signature schemes." In *Workshop on the theory and application of cryptographic techniques*, pp. 47-53. Springer, Berlin, Heidelberg, 1984, DOI: https://doi.org/10.1007/3-540-39568-7_5.
3. Newmarch, Joonsang Baek1 Jan, Reihaneh Safavi-Naini, and Willy Susilo. "A Survey of Identity-Based Cryptography." *Sign Verify IO-Sign IO-Verify* (2004).

4. Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." In Annual international cryptology conference, pp. 213-229. Springer, Berlin, Heidelberg, 2001, DOI: https://doi.org/10.1007/3- 540-44647-8_13.
5. Youngblood, Carl, "An Introduction to Identity-Based Cryptography", CSEP 590TU, pp. 1-7, 2005.
6. Boneh, Dan, and Xavier Boyen. "Secure identity based encryption without random oracles." In Annual International Cryptology Conference, pp. 443-459. Springer, Berlin, Heidelberg, 2004, DOI: 10.1007/978- 3-540-28628-8_27.
7. Waters, Brent. "Efficient identity-based encryption without random oracles." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 114-127. Springer, Berlin, Heidelberg, 2005, DOI: https://doi.org/10.1007/11426639_7.
8. Cocks, Clifford. "An identity based encryption scheme based on quadratic residues." In IMA International Conference on Cryptography and Coding, pp. 360-363. Springer, Berlin, Heidelberg, 2001, DOI: https://doi.org/10.1007/3-540-45325-3_32.
9. Boneh, Dan, and Matthew Franklin. "Identity-based encryption from the Weil pairing." SIAM journal on computing 32, no. 3 (2003): 586-615, DOI: https://doi.org/10.1007/3-540-44647-8_13.
10. Chow, Sherman SM, Joseph K. Liu, and Jianying Zhou. "Identity-based online/offline key encapsulation and encryption." In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, pp. 52-60. ACM, 2011, DOI: 10.1145/1966913.1966922
11. Galindo, David, Javier Herranz, and Jorge Villar. "Identity-based encryption with master key-dependent message security and leakage-resilience." In European Symposium on Research in Computer Security, pp. 627-642. Springer, Berlin, Heidelberg, 2012, DOI: https://doi.org/10.1007/978-3-642-33167-1_36.
12. Roschke, Sebastian, Luan Ibraimi, Feng Cheng, and Christoph Meinel. "Secure communication using identity based encryption." In IFIP International Conference on Communications and Multimedia Security, pp. 256-267. Springer, Berlin, Heidelberg, 2010, DOI: https://doi.org/10.1007/978-3-642-13241-4_23.
13. Sarier, Neyire Deniz. "A new biometric identity based encryption scheme secure against DoS attacks." Security and Communication Networks 4, no. 1 (2011): 23-32, DOI: https://doi.org/10.1002/sec.162.
14. Tseng, Yuh-Min, and Tung-Tso Tsai. "Efficient revocable ID-based encryption with a public channel." The Computer Journal 55, no. 4 (2012): 475-486, DOI: https://doi.org/10.1093/comjnl/bxr098.
15. Oh, JoongHyo, KyungKeun Lee, and SangJae Moon. "How to solve key escrow and identity revocation in identity-based encryption schemes." In International Conference on Information Systems Security, pp. 290-
16. 303. Springer, Berlin, Heidelberg, 2005, DOI: 10.1007/11593980_22.
17. Das, Manik Lal. "A key escrow-free identity-based signature scheme without using secure channel." Cryptologia 35, no. 1 (2010): 58-72, DOI: 10.1080/01611194.2010.515905.
18. Gupta, Swati, and Vipul Gupta. "Revocable key identity based cryptography without key escrow problem." In 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 443-448. IEEE, 2016, DOI: 10.1109/CCAA.2016.7813817.
19. Seo, Jae Hong, and Keita Emura. "Revocable identity-based encryption revisited: Security model and construction." In International Workshop on Public Key Cryptography, pp. 216-234. Springer, Berlin, Heidelberg, 2013, DOI: https://doi.org/10.1007/978-3-642-36362-7_14.
20. Libert, Benoît, and Damien Vergnaud. "Adaptive-ID secure revocable identity-based encryption." In Cryptographers' Track at the RSA Conference, pp. 1-15. Springer, Berlin, Heidelberg, 2009.
21. Jin, Zhengping, Qiaoyan Wen, and Hongzhen Du. "An improved semantically-secure identity-based signcryption scheme in the standard model." Computers & Electrical Engineering 36, no. 3 (2010): 545- 552, DOI: https://doi.org/10.1016/j.compeleceng.2009.12.009.
22. Seo, Jae Hong, and Keita Emura. "Efficient delegation of key generation and revocation functionalities in identity-based encryption." In Cryptographers' Track at the RSA Conference, pp. 343-358. Springer, Berlin, Heidelberg, 2013, DOI: https://doi.org/10.1007/978-3-642-36095-4_22.
23. Yu, Gang, Xiaoxiao Ma, Yong Shen, and Wenbao Han. "Provable secure identity based generalized signcryption scheme." Theoretical Computer Science 411, no. 40-42 (2010): 3614-3624, DOI: https://doi.org/10.1016/j.tcs.2010.06.003.
24. Yuen, Tsz Hon, Willy Susilo, and Yi Mu. "How to construct identity-based signatures without the key escrow problem." International Journal of Information Security 9, no. 4 (2010): 297-311, DOI: https://doi.org/10.1007/s10207-010-0110-5.
25. Zhang, Yunmei, Joseph K. Liu, Xinyi Huang, Man Ho Au, and Willy Susilo. "Efficient escrow-free identity- based signature." In International Conference on Provable Security, pp. 161-174. Springer, Berlin, Heidelberg, 2012, DOI: https://doi.org/10.1007/978-3-642-33272-2_11.
26. Sahana, Subhas Chandra, Bubu Bhuyan, and Manik Lal Das. "An Efficient Key Escrow-Free Identity-Based Signature Scheme." Int J Appl Eng Res 12, no. 19 (2017): 8964-8971.
27.
28. Das, Manik Lal. "A key escrow-free identity-based signature scheme without using secure channel." Cryptologia 35, no. 1 (2010): 58-72., DOI: 10.1080/01611194.2010.515905.
29. Cakulev, Violeta, and Ganapathy S. Sundaram. "IBAKE: Identity-based authenticated key exchange." (2012).
30. Hung, Y-H., T-T. Tsai, Y-M. Tseng, and S-S. Huang. "Strongly secure revocable id-based signature without random oracles." Information Technology and Control 43, no. 3 (2014): 264-276, DOI: http://dx.doi.org/10.5755/j01.itc.43.3.5718.
31. Jin, Zhengping, Qiaoyan Wen, and Hongzhen Du. "An improved semantically-secure identity-based signcryption scheme in the standard model." Computers & Electrical Engineering 36, no. 3 (2010): 545- 552, DOI: https://doi.org/10.1016/j.compeleceng.2009.12.009.
32. Paterson, Kenneth G., and Jacob CN Schuldt. "Efficient identity-based signatures secure in the standard model." In Australasian Conference on Information Security and Privacy, pp. 207-222. Springer, Berlin, Heidelberg, 2006, DOI: https://doi.org/10.1007/11780656_18.
33. Galindo, David, and Flavio D. Garcia. "A Lightweight Identity Based Signature Scheme."
34. Li, Chenghua, Jianxin Zhu, Junjun Wu, Xinfang Zhang, and Qian Deng. "A practical identity-based signature scheme." Wuhan University Journal of Natural Sciences 13, no. 6 (2008): 692-696, DOI: https://doi.org/10.1007/s11859-008-0611-5.
35. Qin, Zhen, Chen Yuan, Yilei Wang, and Hu Xiong. "On the security of two identity-based signature schemes based on pairings." Information Processing Letters 116, no. 6 (2016): 416-418, DOI: https://doi.org/10.1016/j.ipl.2016.02.003.
36. Shim, Kyung-Ah. "An ID-based aggregate signature scheme with constant pairing computations." Journal of Systems and Software 83, no. 10 (2010): 1873-1880, DOI: https://doi.org/10.1016/j.jss.2010.05.071.

37. Yu, Gang, Xiaoxiao Ma, Yong Shen, and Wenbao Han. "Provable secure identity based generalized signcryption scheme." Theoretical Computer Science 411, no. 40-42 (2010): 3614-3624, DOI: https://doi.org/10.1016/j.tcs.2010.06.003.
38. Yu, Jia, Rong Hao, Fanyu Kong, Xiangguo Cheng, Jianxi Fan, and Yangkui Chen. "Forward-secure identity- based signature: Security notions and construction." Information Sciences 181, no. 3 (2011): 648-660, DOI: https://doi.org/10.1016/j.ins.2010.09.034.
39. Tseng, Yuh-Min, Tung-Tso Tsai, and Sen-Shan Huang. "Leakage-free ID-based signature." The Computer Journal 58, no. 4 (2013): 750-757, DOI: 10.1093/comjnl/bxt116.
40. Park, Jong Hwan, and Dong Hoon Lee. "A New Practical Identity-Based Encryption System." IACR Cryptology ePrint Archive 2013, no. 23 (2013).
41. Martin, Luther, and Mark Schertler. "Using the Boneh-Franklin and Boneh-Boyen identity-based encryption algorithms with the Cryptographic Message Syntax (CMS)." (2009).
42. Micro Focus, “The Identity-Based Encryption Advantage”.
43. Kihidis, Anastasios, Konstantinos Chalkias, and George Stephanides. "Practical Implementation of Identity Based Encryption for Secure E-mail Communication." In 2010 14th Panhellenic Conference on Informatics, pp. 101-106. IEEE, 2010, DOI: 10.1109/PCI.2010.48.
44. Owens, Louise, Adam Duffy, and Tom Dowling. "An identity based encryption system." In Proceedings of the 3rd international symposium on Principles and practice of programming in Java, pp. 154-159. Trinity College Dublin, 2004, DOI:10.1145/1071565.1071594

Authors Biography

Ms. Maitri Patel: Ms. Maitri Patel is a Ph.D Scholar in Computer Engineering Department of Sankalchand Patel College of Engineering, Visnagar. She completed her B.E. in Computer Engineering from Gujarat University and M.Tech in Computer Science and Engineering from Jodhpur University. She published and presented research articles in International/National level of Conferences and Journals. Chaired a technical session for two days international conference on “ICT for Sustainable Development” Organized jointly by ASSOCHAM (India-Gujarat Chapter), GESIA, and ACM Chapter.

Dr. Rajan Patel: Dr. Rajan Patel is an Associate Professor in Computer Engineering, Department of Gandhinagar Institute of Technology, Gandhinagar. Dr. Patel has more than 14 professional memberships. He completed his B.E. in Computer Engineering from Saurashtra University and M.Tech in Computer Engineering from NIT, Surat. He did his Ph.D. in Computer Engineering in the domain of MANET Security from RK University. Dr. Patel published and presented research and survey articles in International/National level of indexing Conferences and Journals including IEEE, Science Direct, Springer, Elsevier. Dr. Patel received more than 11 Award/Honored/Excellence/Appreciation from academic bodies such as Certificate of Excellence as a coordinator for conduction of sponsored ICT (MHRD)