Survey on Identity based and Hierarchical Identity based Encryption Schemes

D. Kalyani
Assistant professor
VNR Vignana Jyothi
Institute of Engineering and
Technology, Hyderabad, India

R. Sridevi, PhD
Professor
JNTUHCE, Hyderabad, India

ABSTRACT

In this paper, we present a comprehensive picture and the state of the art of Identity Based Cryptography (IBC) and their security implications with applications. First, we introduce the basic concepts of security and principles of cryptography and then move into identity-based cryptography, an overview of its development process and research progress. We explain identity-based encryption (IBE) schemes and identity-based signature (IBS) schemes and their security analysis. Later, we discuss the hierarchical identity-based encryption (HIBE) present in standard model as well as in random oracle model. We also discuss Revocable Identity Based Encryption (RIBE) schemes from the view point of security models and constructions.

We review several encryption schemes and their advantages and disadvantages along with their efficiency and security considerations

General Terms

Cryptography, Security.

Keywords

Identity based Encryption, Hierarchical IBE, Signature, Pairings, Fuzzy IBE, Revocation IBE.

1. INTRODUCTION

Cryptography encryption techniques are basically has two categories i.e. symmetric key based and asymmetric key based cryptography. In symmetric based cryptography, plain text and cipher text will use same key for encryption and decryption. Symmetric key based system gives efficient encryption and some integrity based applications. Asymmetric based cryptography uses separate keys i.e., Public key and Private key for encryption and decryption. Asymmetric cryptosystems are more secure than symmetric cryptosystems when the length of message is less in size. This also provides efficient digital signatures and key management. Traditional asymmetric cryptosystem used in internet that relies on Public key Infrastructure (PKI). The PKI is depends on availability and security of certificate authority (CA). Identity-based cryptography schemes are in the category of Asymmetric Key based" cryptography. Identity-based cryptography[1,2] specifies a cryptosystem in which both public and private keys are based on the identities of the users.

1.1 Security Services

Security of digital information over communication channels can be achieved using cryptographic protocols. A collection of cryptographic primitives used to provide security services is called cryptosystem. The security services in network security are not altogether different than those of other network communication paradigms. The goal is to protect the information and the resources from attacks and misbehavior. In dealing with network security, we shall explain the

Following requirements that an effective security paradigm must ensure:

Confidentiality: is a core security primitive for network security, It ensures that a given message cannot be understood by anyone else than its desired recipient(s). Data confidentiality is typically enabled by applying cryptography.

Integrity: denotes the authenticity of data sent from one end to another end. That is, it ensures that a message sent from sender A to receiver B was not modified by a malicious party, C, during transmission. If a robust confidentiality mechanism is employed, ensuring data integrity may be as simple as adding one-way hashes to encrypted messages.

Availability: ensures that the desired network services are available whenever they are expected, in spite of attacks. Systems that ensure availability seek to combat denial of service.

Authentication: ensures communication from one end to another is genuine. It ensures that a malicious party cannot masquerade as a trusted network.

Non-repudiation: ensures that the origin of the message is legitimate. i.e when one node receives a false message from another, non-repudiation allows the former to accuse the later of sending the false message and enables all other nodes to know about it. Digital signature may be used to ensure non-repudiation.

Public-key encryption, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentiality.

In public key Cryptography, the sender and receiver must generate encryption and signature key pairs, then submit certificate request along with the proof of identity to Certificate Authority (CA) and then used to authenticate one another to exchange encrypted messages, but it is time consuming and error prone.

Public-key on the other hand, introduces another concept involving key pairs: one for encrypting, the other for decrypting. This concept, as you will see below, is very clever and attractive, and provides a great deal of advantages over symmetric-key:

- Simplified key distribution
- Digital Signature
- Long-term encryption

To overcome Key storage and generation of key pairs, Shamir [1] in 1984, introduced a new concept of Identity based Cryptography, in which the users will be identified based on identifier information such as E-mail, IP address, unique identity, phone number etc, instead of digital certificates used as public key for Encryption or digital Signatures. This reduces complexity of existing public key encryption schemes. Shamir proposed identity based signature (IBS) scheme using RSA function, but not solved problem of identity based Encryption (IBE). Then in 2001 Boneh, Franklin [2] and Cocks introduced a solution for this problem.

In Identity Based Cryptographic Schemes for Bilinear Pairing, "Admissible Bilinear pairing " is a mathematical primitive, which plays a crucial role in current identity Based Cryptography[7], but it is inefficient in plain-text message, since it is encrypted bit-by-bit and hence the length of the output (cipher text) become long. Due to this new idea has been introduced i.e., pairing based identity Based Cryptographic schemes. These problems are solved by Bilinear Diffie-Hellman Assumption (BDH). Security of many identity based Cryptographic schemes in current literature depends on BDH assumptions only.

Hess [5] also constructed IBS scheme based on bilinear pairing [10]. Identity based blind signature and ring signature was introduced by Zhang et.al [6]. Other non-Identity based Later other variations of IBE have proposed like HIBE [15,16], Fuzzy based IBE, and revocation identity based encryption schemes [20,22].

1.2 Organization of the paper

The rest of the paper is organized as follows: Section 2 presents history of the public key cryptography and identity based cryptography. Section 3 explains the overview identity based encryption and signature scheme models. Hierarchical Identity based encryption schemes were described in section 4. Section 6 provides brief about revocation IBE and Fuzzy IBE. In section 6, some of the applications of identify based encryption schemes provided and conclusions are in section 7. References are listed in section 8.

2. BACKGROUND

2.1 Public Key Cryptography

Two basic types of public-key schemes emerged in the 1970s: Diffie-Hellman for key agreement in 1975, and key transport and digital signing schemes proposed by Rivest, Shamir and Adleman (RSA) in 1977.

The Diffie-Hellman key agreement scheme based discrete logarithm problem: given p, g, and ga, find a. The security of Diffie-Hellman Key agreement is depends on the hardness of discrete logarithm problem. The RSA encryption algorithm is based on the integer factorization problem: given a number n that is the product of two primes, p and q, find p and q. he security of RSA algorithm is depends on the hardness of integer factorization problem

In 1980s, cryptographers realized that except the hardness of these problems, the function used in cryptography itself did not provide sufficient security. Later researchers are carefully observed and realized that protocol design was needed together with a methodology for defining precisely the security objective and proving that a protocol met that objective.

Until the mid-1990s that provably secure protocols actually began to be efficient and that provided enough security to the practical application. Later other developments like most prominently, the ElGamal public-key encryption and signature schemes was proposed based on integer factorization in 1984 to rival those of RSA, then later ElGamal techniques were based on the discrete logarithm problem. So too, in 1995 elliptic curve cryptography (ECC), which appeared on the scene.

2.2 Public Key Encryption: Model

A public key encryption PKE is a tuple of polynomial time algorithms

KeyGen(1^λ): A randomized key generation algorithm run by a private key generator (PKG) that takes a security parameter 1^λ as input and outputs secret key SK and public key PK.

Encryption(m, PK): A randomized encryption algorithm that takes a message m, the sender's public key PK as input and Outputs cipher text 'C'.

Decryption(C,SK): A deterministic polynomial time algorithm that takes a cipher text C, secret key SK of receiver as input and outputs cipher text 'C'.

2.3 Identity-based Cryptography

To eliminate the certificate management and public key infrastructure, Shamir [1] proposed the ID-based cryptosystem in 1984. ID-based cryptosystem has become most required system for a secure communication of digital information. There are many ID-based cryptographic primitives exists i.e. digital signature, encryption and key agreement. An ID-based encryption (IBE) system is form of public key system where public key can be user's identity such that emails address etc.

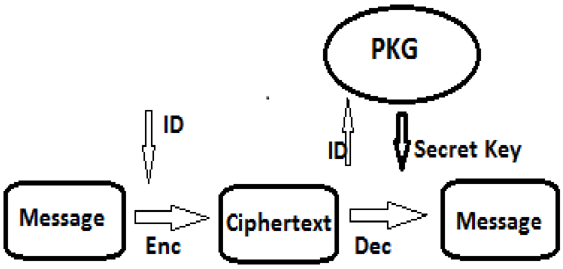

Fig.1 Identity based Cryptography

Encryption Scheme: Model

The following first three algorithms may be randomized but the last is not, it is deterministic. An Identity Based Encryption (IBE) scheme consists of four algorithms:

Setup(1^λ) : A randomized polynomial time algorithm run by a private key generator (PKG) that takes a security parameter 1^λ as input and outputs a master secret key MSK and public parameters Params.

- **Setup**(1^λ) : A randomized polynomial time algorithm run by a private key generator (PKG) that takes a security parameter 1^λ as input and outputs a master secret key MSK and public parameters $Params$
- **KeyGen**$(ID, MSK, Params)$: A randomized polynomial time algorithm run by PKG which takes identity ID_{Rec}, master secret key MSK and public parameters $Params$ as input and outputs a secret key $SK_{ID_{Rec}}$ associated to the identity ID_{Rec}.

- **Encryption**$(m, pk_{PKG}\ , ID_{Rec}, Params)$: A randomized Polynomial time algorithm that takes a message m, the sender's public key pk_{PKG} , the sender's identity ID_{Rec} and public parameters $Params$ as input and Outputs cipher text 'C'.
- **Decryption**$(C, SK_{ID}, Params\ )$: A deterministic polynomial time algorithm that takes a cipher text C, secret key $SK_{ID_{Rec}}$, of receiver, and public parameters $Params$ as input and outputs plaintext 'm' (message).

The above figure1 shows the work flow of ID-based cryptosystem. Between PKG and receiver we need a secure channel is required for private key exchange. If we provide like traditional PKC, we need verification of authorized user is required while giving private key.

Signature Scheme: Model

Identity-based signatures (IBS) (figure 2) also seem to be much easier to implement than identity-based encryption (IBE), of which only few instantiations are known.

An Identity Based Signature (IBS) scheme consists of four algorithms:

Setup(1^λ) : A probabilistic polynomial time algorithm run by a private key generator (PKG) that takes a security parameter 1λ as input and outputs a master secret key MSK and public parameters Params.

KeyGen(ID,MSK,Params) : A probabilistic polynomial time algorithm run by PKG which takes identity ID, master secret key MSK and public parameters Params as input and outputs a secret key SKID associated to the identity ID.

Sign(m, SK_{IDSen}, ID_{Sen}, Params) : A probabilistic polynomial time algorithm that takes a message m, the sender's secret key SK_{IDsen}, the sender's identity ID_{Sen} and public parameters Params as input and outputs a signature σ.

Verify(m, σ, ID_{Sen}, Params) : A deterministic polynomial time algorithm that takes a message m, a signature σ, sender's identity ID_{Sen} and public parameters Params as input and outputs true if σ is a valid signature of the message m, else outputs ⊥(false).

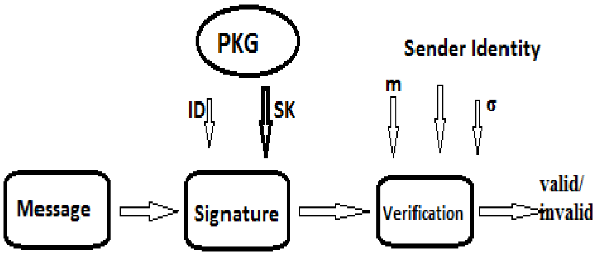

Fig.2 Identity based Signature

In 1984, Shamir [1] proposed first ID-based signature (IBS) scheme. Proposed signature scheme is based on integer factorization problem. Later, Guillou et.al [9] proposed a new paradoxical Identity Based Signature based on interactive zero knowledge protocol. Sakai et.al [3,4] proposed first pairing based Identity Based Signature scheme. This scheme could not prove its security analysis. To overcome the drawback of sakai ,Paterson [11] proposed Identity Based Signature scheme based on pairing along with security proof of the scheme. Hess[12] came up with secure IBS and based on Gap Diffie-hellman cha-cheon et.al [8,13] proposed an IBS scheme. Cheon et.al[14, 15] proposed IBS scheme that gives secure batch verification. Chen et. Al [16] presented an IBS without private key generator.

3. IDENTITY BASED CRYPTPGRAPHY

3.1 Encryption Schemes

The main motivation for Identity Based Encryption is to help the deployment of a public key infrastructure. Boneh and Franklin were the first to propose a feasible IBE system based on the Weil pairing in 2001. After shamir's proposal in 1984, It was proposed nearly two decades in 2001. Boneh and Franklin proposed a new algorithm for IBE systems as follows:

Algorithm:

Setup: PKG runs this algorithm. Selects the master secret key as $s \in Z_q^*$ and calculates the public key $P_{pub} = sP$. A map-to-point hash function $H_1 : \{0,1\}^* \to G_1^*$ and another hash function $H_2 : G_2^* \to \{0,1\}^n$

params: $\left(G_1, G_2, e, P, P_{pub}, H_1, H_2\right)$ master-key: (s)

KeyExtract: Input $ID \in \{0,1\}^*$ the PKG verifies the identity and does the following

1. Computes $Q_{ID} = H_1(ID) \in G_1^*$

2 . Calculate the private key $S_{ID} = sQ_{ID}$

The component acts Q_{ID} as a public key corresponding to the identity ID.

Encrypt: Choose message $m \in \{0,1\}^n$ for a user with the identity ID then sender:

1. Compute $Q_{ID} = H_1(ID) \in G_1^*$

2. Choose a random $r \in Z_q^*$

3. Calculate cipher text:

$C = \left(rP, M \oplus H_1\left(g_{ID}^r\right)\right)$ where

$g_{ID} = e\left(Q_{ID}, P_{pub}\right)$

Cipher text: $C = \left(U = rP, V = M \oplus H_1\left(g_{ID}^r\right)\right)$

$$\in G_1^* \times \{0,1\}^n$$

Decrypt: To decrypt a cipher text $C = (U, V)$;

Compute $V \oplus H_2\left(e\left(d_{ID}, U\right)\right) = M$

Correctness:

$$V \oplus H_2\left(e\left(d_{ID},U\right)\right) = V \oplus H_2\left(e\left(sQ_{ID},rP\right)\right)$$

$$= V \oplus H_2\left(e\left(Q_{ID},P\right)^{sr}\right) = V \oplus H_2\left(e\left(Q_{ID},P_{pub}\right)^{r}\right)$$

$$= V \oplus H_2\left(g_{ID}^{r}\right) = M$$

Security Implications:

i. IBE scheme is computationally efficient, based on mathematical function called bilinear non degenerate maps.

ii. Security of IBE is based on the assumption that the particular bilinear maps chosen are one-way functions.

iii. One-way function means easy to calculate results, but hard to calculate the inverse, this property often referred to as Bilinear Diffie-Hellman Assumption.

Advantages of IBE:

i. Any preparation is not required on the part of the recipient to receive an encrypted message.

ii. Public key infrastructure maintenance is not required.

iii. The features possible in IBE those are not possible in PKI-based systems like signatures

iv. It can improve he user-friendliness by not having client side initialization and having the PKG handle cryptographic operations for the user

v. Sometimes if the receiver does not receive private, having with PKG is higher security than a user's workstation.

Disadvantages of IBE:

i. In IBE, we are giving Major preference in terms holding all private keys. This requires a higher level of assurance and availability from PKG side. This is drawback of IBE System .

ii. Key escrow inherent feature in IBE, i.e., In the server itself decryption and signature will take place. Mainly in IDS because it eliminates non-repudiation in most cases

4. HIERARCHICAL IDENTITY BASED CRYPTOGRAPHY

The first HIBE [16] cryptosystem has been proposed by Boneh, Boyen, and Gho. In this the size of the cipher text as well as the cost of the decryption algorithm are independent of depth of the hierarchy. In HIBE scheme, Cipher texts are always just three group elements and requires only two bilinear map computations are required for decryption.

Let G be a bilinear group of p where p is the prime order and let e: $G \times G \to G_1$ be a bilinear map. Assume that public keys (ID) at depth k are vectors of elements in $(Z_p*)^k$.

ID=$(I_1 \ldots I_k) \in (Z_p*)^k$.

The j^{th} component corresponds to the identity at level j, then extend the construction to public keys over {0, 1}* by first hashing each component I_j using a collision resistant hash

H : {0, 1}* → Z^*p .

Assume that the messages to be encrypted are elements in G_1. Hierarchical Identity Based Encryption (HIBE) system consists of four sub algorithms: Setup, KeyGen, Encrypt, and Decrypt.

Setup(l):

- To generate system parameters for an HIBE of

  maximum depth, select a random generator g ∈ G, a random $\alpha \in Z_p$, and set $g_1 = g^{\alpha}$.

  - Next, pick random elements $g_2 , g_3 , h_1 , \ldots , h_l \in G$.
  - Thepublic parameters and the master key are params = $(g, g_1 , g_2 , g_3 , h_1 , \ldots , h_l)$, master-key = g_2^{α}

Key Gen ($d_{ID|k-1}$, ID):

- To generate a private key d_{ID} for an identity ID = $(I_1,\ldots,I_k) \in (Z_p^*)^k$ of depth $k \leq l$, using the master secret, pick a random $r \in Z_p$ and output.

  $d_{ID}= (g_2^{\alpha} \cdot h_1^{I1} \cdots h_k^{Ik} \cdot g_3)^r, g^r , h^r_{k+1} , \ldots , h^r_l \in G^{2+l-k}$

  Note that d_{ID} becomes shorter as the depth of ID increases.

- The private key for ID can be generated incrementally, given a private key for the

  parent identity

  $ID_{|k-1} = (I_1 , \ldots , I_{k-1}) \in (Z_p*)^{k-1}$, as required. Indeed, let

  $d_{ID|k-1}= (g_2^{\alpha}\cdot h_1^{I1} \cdots h_{k-1}^{Ik-1} \cdot g_3)^{r'} , g^{r'} , h_k^{r'} , \ldots , h_l^{r'} = (a_0 , a_1 , b_k , \ldots , b_l)$ be the private key for $ID_{|k-1}$. To generate d_{ID} , pick a random $t \in Z_p$ and output

  $d_{ID} = (a_0 \cdot b_k^{Ik} \cdot (h_1^{I1} \cdots h_k^{Ik} \cdot g_3)^t, a_1 \cdot g^t , b_{k+1} \cdot h^t_{k+1} , \ldots , b_l \cdot h_l^t)$

- This private key is a properly distributed private key for ID = $(I_1,\ldots,I_k)$ for $r = r'+ t \in Z_p$.

Encrypt (params, ID, M):

- To encrypt a message $M \in G_1$under the public key ID $=(I_1 , .. . , I_k) \in (Z*_p)^k$, pick a random $s \in Z_p$ and

- Output

  CT = $(e(g_1 , g_2)^s \cdot M, g^s , (h_1^{I1} \cdots h_k^{Ik} \cdot g_3)^s) \in G_1 \times G_2$.

Decrypt (d_{ID}, CT):

- Consider an identity ID = $(I_1, \ldots , I_k)$. To decrypt a given cipher text CT = (A, B, C) using the private key $d_{ID} = (a_0 , a_1 ,b_{k+1} \ldots , b_l)$,
- Output = $A \cdot e(a_1 , C) / e(B, a_0) = M$.

Security Implications:

1. The HIBE scheme is selective identity secure (IND-sID-CPA) under the decisional Bilinear Diffie-Hellman Inversion assumption.

2. Chosen Ciphertext Security is also provided where Canetti et al. Show a general method of building an IND-sID-CCA secure -HIBE from a IND-sID-CPA

secure + 1-HIBE. A more efficient construction is given by Boneh and Katz. Applying either method to our HIBE construction results in a IND-sID-CCA secure -HIBE for arbitrary where the cipher text length is independent of the hierarchy height.

3. The HIBE system is selective-ID secure without random oracles. Thus, the system is secure when the adversary commits ahead of time to the identity he intends to attack.

Advantages of HIBE:

1. HIBE scheme supports limited delegation where users can be given restricted private keys that only allow delegation to bounded depth
2. The HIBE system can be modified to support sub linear size private keys at the cost of some cipher text expansion.

Limitations of HIBE:

1. In HIBE selective ID-proof of security is tight.
2. The proof of full security (either in the random oracle or standard model) degrades
3. Exponentially in the hierarchy depth and it is a main problem in all existing HIBE Systems.

5. REVOCABLE AND FUZZY IDENTITY BASED ENCRYPTION

In dynamic distributed system, efficient revocation capability is required in the sense that the overhead of the key generation center (KGC) should be reasonable. Boldyreva et.al [23] proposed the first revocation IBE scheme efficiently called Revocable IBE (RIBE). In this, overhead of the KGC is based on the number of users participating in the scheme logarithmically increased. Later subsequent scalable RIBE schemes have been studied in the literatures [18, 20, 22].

In the Identity-Based Encryption (IBE), there are only few works has been proposed. In the conventional key management scheme, based on publishing the revocation list, the revocation capability can be done. But, similar approach cannot apply the IBE method since such a method can have an adverse effect on the advantage of IBE over the conventional key manage schemes.

Revocation is performed by publishing key update information for each time period and allowing only non-revoked users to be able to generate short-term decryption keys for the current time period from their own long-term keys and public key updates.

Fuzzy identity based encryption proposed in [19, 23] by Sahai and Waters.. In fuzzy identity based encryption, identities are viewed as a set of descriptive attributes, instead of a string of characters. The basic idea of Fuzzy IBE is that private keys can decrypt messages encrypted with the public key, but also messages encrypted with the public key for a certain metric d and a fault tolerance value e. One valuable application of fuzzy identity based encryption is the use of biometric identities.

6. APPLICATIONS

Identity based encryption has many applications in secure communication, public and private networks and interaction of entities over the internet. IBE applications are E-mail system by voltage security provider plugging form Outlook, pine, and email encryptions like hotmail, Yahoo, electronic voting, mobile phone calls and web applications.

Some of the applications are listed below.

• Secure Email encryption

A practical secure email system based on Identity Based Encryption (IBE) which uses DNS as the infrastructure for public key exchange, a proxy service for encryption/decryption on behalf of user and a secure key token or fingerprint authentication system for user authentication.

• Web applications

Receiving public key is major issue in web applications. In the normal PKI sender will store the public key of the receiver in some database and get the information. In identity based encryption the sender will know only the receiver e-mail ID and this can be used as the public key.

• Electronic Voting

For efficient and practical implementation of Electronic voting, the ID-based signature schemes play important role in verification.

• Mobile Communication

Identity-based cryptography offers an approach to end-to end encryption for mobile telephone calls in which the telephone numbers of the call participants are used as the public keys to secure the communication channel, thus making the cryptographic security procedure as easy as making a telephone call.

• MANETs

These days fast development in technology and usage of interne, we believe that Identity Based Cryptography is a promising solution for MANET security issues.

i. Without any infrastructure requirement it is easy to deploy. This saves certificate distribution without any interaction between nodes.

ii. It uses less resource requirements, regarding process power, storage space, communication bandwidth.

HIBE gives very efficient forward secure public key and identity based cryptosystems. It converts the NNL broadcast encryption system into an efficient public key broadcast system.

7. CONCLUSIONS

This paper presents survey of Identity based cryptography and their applications. In this, start review with public key cryptography, moving into Identity based cryptography and its variations. We have explained Identity based encryption: algorithms, advantages, disadvantages, Hierarchical Identity based encryption: algorithms, advantages, disadvantages. Also we have discussed revocation Identity based encryption and dynamic key infrastructure for some applications. The following observations are found:

- We note that the public key infrastructure associated with standard public key cryptosystems also includes a trusted third party and allows a hierarchy of certificate authorities.
- The root certificate authority can issue certificates for other certificate authorities, who in turn can issue

certificates for users in their respective domains.

- The original system of Boneh and Franklin does not allow for such structure.
- However, a hierarchy of PKGs is desirable in an IBE system, as it greatly reduces the workload on master server(s) and allows key escrow at several levels.
- Although HIBE reduces Key escrow problem little extent but not completely. Overhead of KGC is increased if the numbers of users are increased. Exponentially in the hierarchy depth and it is a main problem in all existing HIBE Systems.

Further, we work on a dynamic key infrastructure for security application in Public key infrastructure. Our aim is to resolve the key escrow issue encountered with the fully hierarchical identity-based approach. Using this approach, most of the benefits that identity-based techniques offer can be preserved, while eliminating key escrow from the infrastructure.

8. REFERENCES

[1] A. Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO ’84, LNCS 196, pages 47–53, Springer-Verlag, 1984.

[2] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing, Proceedings of CRYPTO 2001, LNCS 2139, pages 213–229, Springer-Verlag, 2001.

[3] A. Joux, One Round Protocol for Tripartite Diffie-Hellman, Algorithmic Number Theory Symposium – Proceedings of ANTS 2002, LNCS 1838, pages 385–394, Springer-Verlag, 2000.

[4] J.Baek and Y.Zheng, Identity-Based Threshold Decryption, Public Key Cryptography – Proceedings of PKC 2004, LNCS 2947, pages 262-276, Springer-Verlag, 2004.

[5] F. Hess, Efficient Identity Based Signature Schemes Based on Pairings, Selected Areas in Cryptography – Proceedings of SAC 2002,LNCS 2595, pages 310–324, Springer-Verlag, 2002.

[6] F. Zhang and K. Kim, ID-based Blind Signature and Ring Signature from Pairings, Advances in Cryptology – Proceedings of ASIACRYPT 2002, LNCS 2501, pages 533–547, Springer-Verlag, 2002.

[7] Yacobi, Yacov, A Note on the Bi-Linear Diffie-Hellman Assumption, Cryptology, ePrint Archive, Report 2002/113.

[8] L.C. Guillou and J.-J. Quisquatar. A “paradoxical” identity-based signature scheme resulting from zero-knowledge. In Advances in Cryptology-Crypto’88 , LNCS 0403, pp. 216-231, Springer-Verlag, 1990.

[9] F. Hess. Efficient Identity Based Signature Schemes Based on Pairings. In Selected Areas in Cryptography-SAC’02, LNCS 2595, pp.310-324, Springer- Verlag, 2003.

[10] R. Sakai, K. Ohgishi and M. Kasahara. Cryptosysytems based on pairing. In Symposium on Cryptography and Information Security-SCIS’00, 2000.

[11] K. G. Paterson. ID-based signatures from pairings on elliptic curves, Cryptology ePrint Archive, Report 2002/004, 2002. http://eprint.iacr.org/2002/004.

[12] J. Cha and J.H. Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. In Public Key Cryptography-PKC’03, LNCS 2567, pp.18-30, Springer-Verlag, 2003.

[13] J. H. Cheon, Y. Kim, H. J. Yoon, A New ID-based Signature with Batch Verification, Cryptology ePrint Archive, Report 2004/131, 2004. http://eprint.iacr.org/2004/131.

[14] X. Yi, An Identity-Based Signature Scheme From the Weil Pairing, IEEE Communication Letters, 7(2):76-78, IEEE, 2003.

[15] X. Chen, F. Zhang, K. Kim, A New ID-based Group Signature Scheme from Bilinear Pairings, In Proceedings of WISA’03, LNCS 2908, pp.585-592, Springer-Verlag, 2003.

[16] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, “Identity-based hierarchical strongly key-insulated encryption and its application,” in ASIACRYPT (Lecture Notes in Computer Science), vol. 3788, B. K. Roy, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 495–514.

[17] R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-keyencryption scheme,” J. Cryptol., vol. 20, no. 3, pp. 265–294, Jun. 2007.

[18] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. 15th ACM CCS, 2008, pp. 417–426.

[19] B. Libert and D. Vergnaud, “Adaptive-ID secure revocable identity-based encryption,” in CT-RSA (Lecture Notes in Computer Science), vol. 5473, M. Fischlin, Ed. Berlin, Germany: Springer-Verlag, 2009, pp. 1–15.

[20] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, “Revocable identity-based encryption from lattices,” in Information Security and Privacy (Lecture Notes in Computer Science), vol. 7372, W. Susilo,Y. Mu, and J. Seberry, Eds. Berlin, Germany: Springer-Verlag, 2012, pp. 390–403.

[21] B. Waters, “Efficient identity-based encryption without random oracles,” in EUROCRYPT (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 114–127.

[22] J. M. González-Nieto, M. Manulis, and D. Sun, “Fully private revocable predicate encryption,” in Information Security and Privacy (Lecture Notes in Computer Science), vol. 7372, W. Susilo, Y. Mu, and J. Seberry, Eds. Berlin, Germany: Springer-Verlag, 2012, pp. 350–363.

[23] J. H. Seo and K. Emura, “Revocable identity-based encryption revisited: Security model and construction,” in Public-Key Cryptography (Lecture Notes in Computer Science), vol. 7778, K. Kurosawa and G. Hanaoka, Eds. Berlin, Germany: Springer-Verlag, 2013, pp. 216–234.