Identity-Based Cryptography and Comparison with traditional Public key Encryption: A Survey

Girish
Department of PGS-CEA
The National Institute of Engineering,
Manadavady Road,Mysore-570008, INDIA

Phaneendra H.D
Department of information science and Engineering,
The National Institute of Engineering,
Manadavady Road,Mysore-570008, INDIA

Abstract- **In this paper, we survey the state of research on identity-based cryptography(IBC) and compare it with the traditional public key encryption. IBC is an emerging area of public key cryptography. We first reviewing the basic concepts of IBE and identity based signature(IBS) schemes, and subsequently review some important IBE schemes based on the bilinear pairing, a computational primitive widely used to build up various identity-based cryptographic schemes in the current literature. We Compare IBE with the traditional public key encryption. Finally, we discuss advantages and disadvantages of IBC with applications of IBC**

Keywords- Identity based cryptography, Public key infrastructure.

I.INTRODUCTION

In 1984, Shamir [1] proposed a concept of identity-based cryptography. In this new paradigm of cryptography, user's identifier information such as email address, IP addresses, social security number, a photo, a phone number, postal address etc., instead of digital certificates can be used as public key for encryption or signature verification. As a result, identity-based cryptography significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework known as Public Key Infrastructure (PKI). Although Shamir [1] easily constructed an identity-based signature (IBS) scheme using the existing RSA [2] function, he was unable to construct an identity-based encryption (IBE) scheme, which became a long-lasting open problem. Only in 2001, Shamir's open problem was independently solved by Boneh and Franklin [3] and Cocks [4]. Thanks to their successful realization of identity-based encryption, identity-based cryptography is now hot area within the research community.

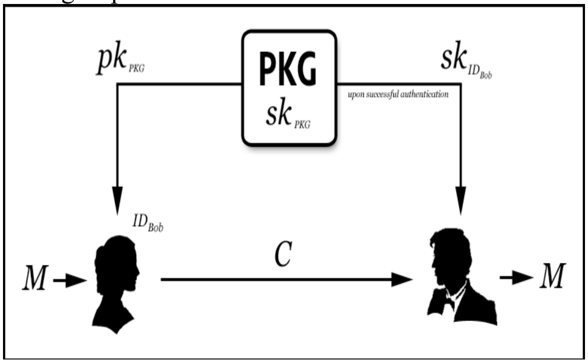
II BASIC CONCEPTS OF IDENTITY BASED ENCRPTION AND SIGNATURW

In this section we discuss the requirements of the Identity based encryption and Identity based signature

A. *Identity based signature*

As mentioned earlier, in the IBE scheme, the sender Alice can use the receiver's identifier information which is represented by any string, such email address, IP addresses, social security number, a photo, a phone number, postal address etc., to encrypt a message. The receiver Bob, having obtained a private key associated with his identity information from trusted third party called the "Private KeyGenerator (PKG)", can decrypt the ciphertext.

Summing up, we describe an IBE scheme using the following steps.



(Figure 1 illustrates a schematic outline of an IBE scheme).

Setup: The PKG creates its master (private) and public key pair, which we denote by *skPKG* and *pkPKG* respectively. (Note that *pkPKG* is given to all the interested parties and remains as a constant system parameter.)

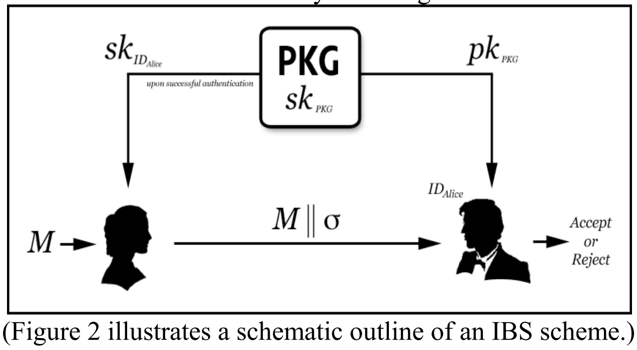
Private Key Extraction: The receiver Bob authenticates himself to the PKG and obtains a private key *sk*ID*Bob* associated with his identity ID*Bob*.

Encryption: Using Bob's identity ID*Bob* and the PKG's *pkPKG*, the sender Alice encrypts her plaintext message *M* and obtains a cipher text *C*.

Decryption: Upon receiving the cipher text *C* from Alice, Bob decrypts it using his private key *sk*ID*Bob* to recover the plaintext *M*.

B. *Identity based signature.*

As a mirror image of the above identity-based encryption, one can consider an identity-based the signature (IBS) scheme. In this scheme, the signer Alice first obtains a signing (private) key associated with her identifier information from the PKG She then signs a message using the signing key. The verifier Bob now uses Alice's identifier information to verify Bob's signature.



(Figure 2 illustrates a schematic outline of an IBS scheme.)

No needs for Bob to get Alice's certificate. More precisely, an IBS scheme can be described using the following steps.

Setup: The Private Key Generator (PKG),which is a trusted third party, creates its master (private) and public key pair, which we denote by *skPKG* and *pkPKG* respectively.

Private Key Extraction: The signer Alice authenticates herself to the PKG and obtains a private key *sk*ID*Alice* associated with her identity ID*Alice*.

Signature Generation: Using her private key *sk*ID*Alice* , Alice creates a signature σ on her message *M*.

Signature Verification: Having obtained the signature σ and the message *M* from Alice, the verifier Bob checks whether σ is a genuine signature on *M* using Alice's identity ID*Alice* and the PKG's public key *pkPKG*. If it is, he returns "*Accept*". Otherwise, he returns "*Reject*".

III Identity Based Cryptographic Schemes From Bilinear Paring

We first review the "admissible bilinear pairing", which is a mathematical primitive that has been playing a central role in current identity-based cryptography since it was used in Boneh and Franklin's identity-based encryption scheme [8].(Note that differently from Boneh and Franklin), Cocks [15] used a variant of "integer factorization" problem to construct his IBE scheme. However, the scheme is inefficient in that a plaintext message is encrypted bit-by-bit and hence the length of the output ciphertext becomes long. For this reason, we focus only on the pairing-based identity-based cryptographic schemes which are more widely used in practice.

A. Definition of the Bilinear Pairing

Let G_1, G_2 be two groups of the same prime order q. We view G_1 as an additive group and G_2 as a multiplicative group. Let P be an arbitrary generator of G1. (a.P denotes P added to itself a times). Assume that discrete logarithm problem(DLP) is hard in both G_1 and G_2. A mapping $e:G_1^2\text{-}>G_2$ satisfy the following properties is called a bilinear map from a cryptographic point of view:

Bilinearity: e(aP,bQ) = e(P,Q)ab for all P,Q $\in$G1 and a,b $\in Z^*_q$.

Non-degeneracy: if P is a generator of G1, then E(P,P) is a generator of G2. In other words e(P,P)$\neq$1.

Computable: There exists an efficient algorithm to compute e(P,Q) for all P,Q $\in$G1.

B. The Boneh-Franklin identity based encryption scheme

The first fully functional identity-based encryption scheme was given by Boneh and Franklin [5]. In the original paper the authors construct the system in stages. They first describe a simpler version of the scheme, BasicIdent, which is secure against chosen plaintext attacks in the random oracle model. The system is then transformed using a technique of Fujisaki and Okamoto [6] to a system FullIdent which is shown to be secure against adaptive chosen ciphertext attacks in the random oracle model, assuming the hardness of BDH in the groups and pairing involved.

IV. Other Identity Based Encryption Schemes

Following the Boneh-Franklin scheme, lots of other identity based encryption has been proposed.Some try to improve on the level of security, others try to adapt special types of publickey cryptosystems (e.g. hierarchical schemes, fuzzy schemes, etc.) to the setting of identity based encryption. In this section we give a short overview of some important systems that have been developed.

A. Identity based encryption without random oracles

Because the random oracle model is quite controversial, an important open problem after the construction of the Boneh-Franklin scheme was to develop an identity based encryption scheme which is provably secure in the standard model. As a first step towards this goal, Canetti et al. [7] create an identity based encryption scheme which is provably secure without random oracles, although in a slightly weaker security model. In this weakened model, known as selective identity security, an adversary needs to commit to the identity he wishes to attack in advance. In the standard identity based model, the adversary is allowed to adaptively choose his target identity. The security of the scheme depends on the hardness of the DBDH problem and the construction is quite inefficient. As an improvement, Boneh and Boyen [8] created two eficient identity based encryption schemes, both provably secure in the selective-identity model and also without resorting to random oracle methodology. The first system can be extended to an efficient hierarchical identity based encryption system (see next section) and its security is based on the DBDH problem. The second system is more efficient, but its security reduces to the non-standard DBDHI problem.

A later construction due to Boneh and Boyen [10] is proven fully secure without random oracles. Its security reduces to the DBDH problem. However, the scheme is impractical and was merely given as a theoretical construct to prove that there indeed exists fully secure identity based encryption schemes without having to resort to random oracles. Finally, Waters [11] improves on this result and constructs a modification of the scheme which is efficient and fully secure without random oracles. Its security also reduces to the DBDH problem.

B. Hierarchical identity based encryption

The concept of hierarchical identity based encryption was first introduced by Horwitz and Lynn [12]. In traditional public key infrastructures there is a root certificate authority, and possibly a hierarchy of other certificate authorities. The root authority can issue certificates to authorities on a lower level and the lower level certificate authorities can issue certificates to users. To reduce workload, a similar setup could be useful in the setting of identity based encryption. In identity based encryption the trusted party is the private key generator. A natural way to extend this to a two-level hierarchical based encryption is to have a root private key generator and domain private key generators. Users would then be associated with their own primitive identity plus the identity of their respective domain, both arbitrary strings. Users can obtain their private key from a domain private key generator, which in turn obtains its private key from the root private key generator. More levels can be added to the hierarchy by adding subdomains, subsubdomains, etc..

The first hierarchical identity based encryption scheme with an arbitrary number of levels is given by Gentry and Silverberg [13]. It is an extension of the Boneh-Franklin scheme and its security depends on the hardness of the BDH problem. It also uses random oracles. Boneh and Boyen managed to construct a hierarchical based encryption scheme without random oracles based on the BDH problem, but it is secure in the weaker selective-ID model [14].

In the aforementioned constructions, the time needed for encryption and decryption grows linearly in the hierarchy depth, thus becoming less efficient at complex hierarchies. In [15], Boneh, Boyen and Goh give a hierarchical identity based encryption system in which the decryption time is the same at every hierarchy depth. It is selective-ID secure without random oracles and based on the BDHE problem.

C. Fuzzy identity based encryption

In [16], Sahai and Waters give a fuzzy identity based encryption system. In fuzzy identity based encryption, identities are viewed as a set of descriptive attributes, instead of a string of characters.The idea is that private keys can decrypt messages encrypted with the public key ω, but also messages encrypted with the public key ω' if d(ω,ω') < e 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. Since two measurements of the same biometric (e.g. an iris scan) will never be exactly the same, a certain amount of error tolerance is required when using such measurements as keys. The security of the Sahai-Waters scheme reduces to the modified DBDH problem.

D. Identity based encryption schemes without pairings

Another identity based encryption scheme that was published around the same time as the Boneh-Franklin scheme (but turned out to be invented several years earlier) is due to Cocks. The security of the system is based on the quadratic residuosity problem modulo a composite N = pq where p, q ∈ Z are prime [17]. Unfortunately, this system produces very large ciphertexts compared to the pairing based systems and thus is not very efficient. Recently, Boneh et. al. constructed another identity based encryption system that is not based on

pairings [18]. It is related to the Cocks system since the security of it is also based on the quadratic residuosity problem. The system is space efficient but encryptions are slow. It is proven secure in the random oracle model[22]

V. COMPARASION OF PUBLIC KEY CRYPTOGRAPHY AND IDENTITY BASED CRYPTOGRAPHY.

In this section we compare the public key Infrastructure scheme and Identity-based key Cryptography

A. Public key cryptography

Public Key Infrastructures (PKIs) are currently the primary means of deploying asymmetric cryptography. In this paper, when discussing PKIs we are referring to infrastructures that support the deployment of traditional asymmetric cryptographic algorithms, such as RSA [19]. Because of the inherent public nature of the encryption or verification keys, the integrity of the public keys is usually protected with a certificate. The PKI is the infrastructure that supports the management of keys and certificates.

As well as the keys and certificates, the core components of a PKI are:

Certificate Authority (CA): The CA is the entity that generates the certificates. It is responsible for ensuring the correct key is bound to the certificate, as well as ensuring the certificate content.

Registration Authority (RA): The RA is responsible for ensuring that the user that receives the certificate is a legitimate user within the system. The functionality of the CA and RA is sometimes carried out by a single entity.

Certificate Storage: In most systems certificates (as well as update information such as Certificate Revocation Lists) are stored in a CA managed database.

Software : For the certificates to be of use, the software that is going to use the certificates need to be aware of what the certificate content represents within the scope of the system security policy.

Policies and Procedures: Although the core of a PKI is mainly technical, there is, by necessity, a strong requirement for ensuring that the mechanisms are used correctly. The Certificate Policy (CP) and Certification Practice Statements (CPS) define the how the certificates are generated and managed. They also define the role of the certificates within the broader security architecture.

In a traditional PKI, one can choose where the key pair is generated. The keys can either be generated by the CA for the client, or the client can generate the keys for itself and provide a copy of the public key to the CA to certify. The choice of mechanism will largely be dictated by the security policy of the system. It will also be influenced by the key usage. If a signature key is likely to be used to support non-repudiation, then it is better that the key is generated by the client. In the case of a decryption key that is used to keep company information confidential, it might be prudent to have the CA generate (or have access to) the key so that there is always a means of recovering encrypted information.

B. Identity/Identifier-Based Public Key Cryptography

One of the difficulties inherent in running a PKI is in the managing of the certificate and associated key. Identity – and subsequently identifier – based cryptography was created as a means of overcoming this problem. Shamir [20] was the first to propose such a scheme in which the key itself is generated from some publicly identifiable information, such as a person's e-mail address. His original scheme provided a signature algorithm, but could not be used for encryption. It is only recently that an efficient identity-based encryption system was proposed by Boneh and Franklin [21].

The core difference between an ID-PKC and a traditional asymmetric algorithm in the means of generating the keys. The difference is identifiable in two ways:

- As mentioned above, in both the signature and encryption variants, the public keys are generated from publicly identifiable information. This allows a client *A* to generate the public key of another client *B* without having to do a search in a directory or ask *B* for a copy of their key.
- Because of the mathematics that underpin the algorithms, the creation of the private key requires the knowledge of a master secret that is held by the Trusted Authority (TA), who is the analogue of the CA in a PKI.

Recently, it has been recognised that an identity need not be the only determinant of a client's public key. For example, information such as the client's position within an organisation, the validity period for the keys, etc. can be included in the data used to derive the key pair. This results in the broader concept of identifier-based public key cryptography.

Because the TA is directly responsible for the generation of the private key in an ID-PKC mechanism, there is an inherent escrow facility in the system. This may or may not be desirable. This forces a change in the role of the trusted third party within the system. In a PKI, the CA is concerned with validating the authenticity of the information present in the certificate, whereas, in an ID-PKC the TA is directly responsible for generating and distributing all keying material within the system.

There is also the requirement that TA and client are abl to set up an independent secure channel for the distribution of private key material. This channel needs to protect both the authenticity and confidentiality of the private key.

Although the idea of using a client's identity as the base for their key pair is very appealing, it does not come without consequences. The two main issues that will influence are as follows.

- Coping with the practicalities of implementation are not insignificant. If we take revocation as an example, because we cannot revoke a person's identity, there is a requirement for additional input to the key generation process. If we include validity dates, key usage, etc. then a push toward broader use of identifying information results, leading naturally to identifier-based cryptography.
- The authenticity of the information that is used as the identity or identifier is now crucial to the security of the system. In a PKI, the certificate is supposed to demonstrate the authenticity of identifying information. In ID-PKC, because a private key may be generated after the public key, the TA may not have validated the authenticity of the information relating to the key pair prior to the public key's use. For example, *A* might use information it thinks is valid to generate a public key for *B*, but the information *A* uses could either relate to the wrong *B*, or may be completely invalid in the eyes of the TA

VI. ADVANTAGES AND DISADVANTAGES OF IBE

In this section we will discuss the advantages and disadvantages of the identity based encryption

A. Advantages of IBE

- No certificates needed. A recipient's public key is derived from his identity
- No pre-enrollment required.
- Keys expire, so they don't need to be revoked. In a traditional public-key system, keys must be revoked if compromised.
- Enables postdating of messages for future decryption.

B. Disadvantages of IBE.

- Requires a centralized server. IBE's centralized approach implies that some keys must be created and held in escrow -- and are therefore at greater risk of disclosure.
- Requires a secure channel between a sender or recipient and the IBE server for transmitting the private key.

VII APPLICATION OF IDENTITY BASED ENCRYPTION

There are many applications in which the identity based encryption can be used in the growing communication in the internet. Some of the applications are listed below.

A. Email encryption

- Bob encrypts mail with pub-key = “alice@hotmai
  - Easy to use: no need for Bob to lookup Alice’s cert
  - Bob can send mail to Alice even if Alice has no cert.
- Bob encrypts with pub-key = “alice@hotmail || current-date”
  - Short lived private keys: revocation + mobility
  - Bob can send mail to be read at future date
- Credentials: embed user credentials in public key
  - Encrypt with: “alice@hotmail || date || clearance=secret”
  - Alice can decrypt only if she has secret clearance on given date
  - Easy to grant and revoke credentials at PKG

B. Web applications

The main problem in the web application is to get the get the receivers public key. 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-mailid[21] and this can be used as the public key.

C. Electronic Voting

The ID-based ring signature scheme can be used for electronic voting, which is more efficient and practical

D. Mobile Phone Calls.

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.

VIII. CONCLUSION

In this paper we survey the state of art of the identity based cryptography. Different cryptographic schemes using the identity based encryption. Comparison of the identity based encryption with the traditional public key encryption advantages and disadvantages and applications of the IBE. The area is still growing and many new applications of the IBE will be added. We believe our survey helps in providing knowledge of IBE and research work that has been carried out in the area of IBE for the recent years. The challenge is to make IBE is a useful technology for the real world application.

REFERENCES

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

[2] Ronald L. Rivest, Adi Shamir, and Leonard M.Adleman. A Method for Obtaining Digital Signatures and Public KeyCryptosystems, Communi cations of the ACM 21 (2), pages 120-126, 1978

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

[4] C. Cocks, An Identity Based Encryption Scheme Based on Quadratic Residues, Cryptography and Coding - Institute of Mathematics and Its Applications International Conference on Cryptography and Coding " Proceedings of IMA" 2001, LNCS 2260, pages 360-363, Springer-Verlag, 2001.

[5] Dan Boneh and Matt Franklin, Identity-based encryption from the Weil pairing, Lecture Notes in Computer Science 2139 (2001), 213

[6] Eiichiro Fujisaki and Tatsuaki Okamoto, Secure integration of asymmetric and symmetric en-cryption schemes, Lecture Notes in Computer Science 1666 (1999), 537-554.

[7] R. Canetti, S. Halevi, and J. Katz, A forward-secure public-key encryption scheme, Advances in Cryptology (Eurocrypt 2003). Lecture Notes in Computer Science, vol. 2656, Springer-Verlag,2003,pp.255-271

[8] D. Boneh and X. Boyen, E_cient selective-ID secure identity-based encryption without random oracles, Advances in Cryptology (EUROCRYPT 2004), LNCS, vol. 3027, Springer, 2004,pp.223-238.

[9] Secure identity based encryption without random oracles, Proceedings of Crypto 2004,Lecture Notes in Computer Science, Springer-Verlag, 2004.

[10] D. Boneh, X. Boyen, and E. Goh, Hierarchical identity based encryption with constant size ci-phertext, Proceedings of Eurocrypt '05, 2005.

[11] B. Waters, E_cient identity-based encryption without random oracles, Advances in Cryptology EUROCRYPT 2005, Lecture Notes in Computer Science, vol. 3404, 2005, pp. 114-127.

[12] Jeremy Horwitz and Ben Lynn, Toward hierarchical identity-based encryption, Theory and Application of Cryptographic Techniques, 2002, pp. 466-481.

[13] Craig Gentry and Alice Silverberg, Hierarchical id-based cryptography, ASIACRYPT '02: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security (London, UK), Springer-Verlag, 2002, pp. 548-566.

[14] D. Boneh and X. Boyen, E_cient selective-ID secure identity-based encryption without random oracles, Advances in Cryptology (EUROCRYPT 2004), LNCS, vol. 3027, Springer, 2004, pp. 223-238.

[15] D. Boneh, X. Boyen, and E. Goh, Hierarchical identity based encryption with constant size ciphertext, Proceedings of Eurocrypt '05, 2005.

[16] Amit Sahai and Brent Waters, Fuzzy identity based encryption, Lectures Notes in ComputerScience, vol. 3494, Springer, 2005, pp. 457-473.

[17] Cliford Cocks, An identity based encryption scheme based on quadratic residues, Proceedings of the 8th IMA International Conference on Cryptography and Coding. Lecture Notes in Computer Science, vol. 2260, 2001.

[18] Dan Boneh, Craig Gentry, and Michael Hamburg, Space-eficient identity based encryption without pairings, FOCS '07: Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (Washington, DC, USA), IEEE Computer Society, 2007, pp. 647-657.

[19] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the A.C.M., 21(2):120-126, February 1978.

[20] A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology CRYPTO '84, volume 196 of LNCS, pages 47-53. Springer-Verlag, 1984.

[21] Yanjiong Wang, Qiaoyan Wen, Hua Zhang, "A Single Sign-On Scheme for Cross Domain Web Applications Using Identity-Based Cryptography," Networks Security, Wireless Communications and Trusted Computing, International Conference on, pp. 483-485, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010

[22] Dennis Meffert "Bilinear Paring in Cryptography" Master Thesis May 2004.