COMPARATIVE ANALYSIS OF IDENTITY-BASED ENCRYPTION WITH TRADITIONAL PUBLIC KEY ENCRYPTION IN WIRELESS NETWORK

Ms. Priyanka Bubna[1], Prof. Parul Bhanarkar Jha[2]

[1]*Wireless Communication & Computing, TGPCET/RTM Nagpur University, Nagpur, (India)*

[2]*Head of Department, Information Technology, TGPCET/ RTM Nagpur University Nagpur, (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* – *Certificate Based Encryption, ID Based Encryption, ID Based Digital Signature, Public Key Infrastructure, Secure Data Transmission.

I INTRODUCTION

Identity Based Encryption (IBE) is a public cryptographic scheme where any piece of text can act as a valid public key. This is a powerful concept as it means that email addresses, dates or a combination of both can act as public keys.

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 [3] 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 [2]. 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

In this section we discuss the requirements of the Identity based encryption. 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 Key Generator (PKG)", can decrypt the cipher text. Summing up, we describe an IBE scheme using the following steps.

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 skIDBob associated with his identity IDBob.

Encryption: Using Bob's identity IDBob 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 skIDBob to recover the plaintext M.

III RELATED STUDY AND ACADEMIC RESEARCH

The most significant papers on Identity Based Encryption are by Shamir [1] and Boneh and Franklin [2]. In [1], Shamir proposed that a receiver’s public key be calculated mathematically from their identity. The key server calculates the private key. The IBE algorithm removes the need for public key queries or certificates. However, while Shamir constructed an Identity Based Signature (IBS) scheme he was unable to construct an IBE scheme. In [2] Boneh and Franklin solved this mathematical problem and constructed the first practical implementation of the IBE system.

While Boneh and Franklin’s implementation is perhaps the most well-known, there are in fact multiple implementations of the IBE system. Baek, Newmarch, Safavi-Naini and Susilo [4] point out that many IBE schemes are based on the Bilinear Diffie-Hellmann (BDH) assumption. BDH is a computational hardness assumption that is used to prove the security of cryptographic systems. Cha and Cheon have devised an IBS scheme based on bilinear pairing. Other schemes similar to IBE include a Certificate-Based Encryption (CBE) scheme, where a user needs both a private key and an up to date certificate from a CA, and the Public Key Encryption with Keyword Search (PEKS) where the body of the encrypted data contains a keyword so that, for example, an email gateway can test for this keyword without reading the rest of the message. Gagné [5] describes Authenticated ID-Based Encryption where message authentication is provided at no additional computational cost. In other words, the receiver verifies the identity of the sender and whether or not the message has been tampered with, thus removing the need for digital signatures when authentication is required. Thus, secure authenticated conversation is possible.

Gagné [5] also cites the Hierarchical ID-Based Encryption (HIBE) scheme. One disadvantage of IBE is that the private key generator (PKG) has a demanding task in a large network. With the Hierarchical ID-Based Encryption Scheme, however, a hierarchy of PKGs is used. Under this scheme, PKGs only compute private keys for entities immediately below them in the hierarchy. In an IBE system each user is represented by a string ID. In Figure 5 we see how, for example, the root PKG computes a private key for ID1 using the make key formula, mk. In this system the user is no longer represented by a string ID but by a tuple of IDs containing the IDs of the ancestors in the hierarchy. For example, in Figure 5 the user in the third level of the hierarchy below the root is not represented by a string ID3 but by a combination of strings ID1, ID2 and ID3.

Boneh, Goh and Boyen [6] present the HIBE scheme in more detail and cite its potential application in forward-secure encryption which provides a guarantee that all messages encrypted before a secret key is compromised remain secret. HIBE is also appropriate for broadcast encryption schemes where data can be broadcast efficiently to a dynamic group of users authorized to receive the data. Finally, Boneh, Goh and Boyen [6] outline the role HIBE can play in encrypting to the future where a trusted server publishes the private key corresponding to a particular day, thus enabling all messages encrypted for that day to be decrypted.

Boneh and Hamburg [7] propose a Generalized Identity Based and Broadcast Encryption Scheme (GIBE) where different encryption properties can be combined using a product rule.

This enables the construction of encryption schemes with multiple properties. For example, a multi-authority, forward-secure, broadcast encryption system can be derived using this product rule. Boneh and Hamburg [7] also outline a spatial encryption system, a specific instance of GIBE which enables the construction of encryption systems with specific properties.

Goyal [8] introduces the concept of Accountable Authority Identity Based Encryption (A-IBE) which attempts to overcome the key escrow problem inherent in IBE. Simply put, a PKG has to be completely trusted as it is able to compute the private key corresponding to any identity.

Goyal [8] cites arguments that, for this reason, IBE is still restricted to small closed groups where a trusted central authority is available. On the other hand, under the scheme proposed by Goyal [8], a user gets the decryption key from the PKG using a secure key generation protocol. Under this scheme the PKG has no knowledge of the key the user obtained. Ho Au, Huang, Liu, Susilo, Wong and Yang [9] extend the concept of A-IBE by having the PKG's master secret key retrieved automatically if more than one user secret key are released thus providing the user with concrete proof of misbehavior on the part of the PKG.

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 public key 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.

4.1 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. [10] 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 [11] created two efficient 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 nonstandard DBDHI problem. A later construction due to Boneh and Boyen [12] 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 [13] 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.

4.2 Hierarchical identity based encryption

The concept of hierarchical identity based encryption was first introduced by Horwitz and Lynn [14]. 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, sub subdomains, etc..

The first hierarchical identity based encryption scheme with an arbitrary number of levels is given by Gentry and Silverberg [15]. 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 [16]. 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 [17], 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.

4.3 Fuzzy identity based encryption

In [18], 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 ϕ, but also messages encrypted with the public key ϕ' if d (ϕ, ϕ') < 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.

4.4 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 = p, q where p, q ε Z are prime [19]. Unfortunately, this system produces very large cipher texts 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 [20]. 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.

V COMPARASION OF PUBLIC KEY AND IDENTITY BASED CRYPTOGRAPHY

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

5.1Public 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 [21]. 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.

5.2 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 [22] 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 [23].The difference between an ID-PKC and a traditional asymmetric algorithm is in the way of key generation.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 recognized 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 organization, 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 IDPKC 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 able 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

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

B. Disadvantages of IBE.

1. 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.
2. 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.Gagné [5] outlines several applications for IBE. These include:

1. The previously discussed forward-secure encryption.
2. The revocation of public keys whereby the current date can be included in the construction of the public key, thus providing a preset expiration date.

3. The management of user credentials where the inclusion of a clearance level in the public key means that a receiver will only be able to decrypt the message if he/she has the appropriate clearance level.
4. Delegations of decryption keys whereby management can give subordinates private keys corresponding to their responsibilities so that subordinates can only decrypt messages which fall within their responsibilities.

Here we have outlined how IBE provides better performance than its symmetric and asymmetric key management counterparts. With the former, the need for a central server to manage each transaction means that the server gets busier the more email users are added to the system and there is no offline capability. There is a similar lack of offline capability with asymmetric key management systems. Moreover, the performance of asymmetric key management systems is affected by the difficulties that can be encountered in locating certificates and the administrative problems in validating these certificates. By contrast, messages can be encrypted and decrypted using IBE even when offline.

Ad-hoc communication is also possible as no pre-enrolment of users is required. Penn and Sage expand on these advantages to explore how IBE is easier to integrate into other products and how better key usage and management is facilitated. IBE has other applications other than secure email. IBE would seem to be the only practical means of providing security for Wireless Sensor Networks (WSNs).

VIII CONCLUSION

Identity Based Encryption is a promising solution for overcoming the issues associated with symmetric and asymmetric key management schemes. While there are issues, the comparative simplicity of its architecture makes IBE an attractive proposition for diverse computer systems including mobile computing. In this paper we survey the 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] Adi Shamir, “Identity-based cryptosystems and signature schemes”, Advances in Cryptology—Crypto 1984, Lecture Notes in Computer Science, vol. 196, Springer-Verlag, pp. 47-53, 1984.

[2] D. Boneh and M. Franklin , “Identity based encryption from the Weil pairing”, SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003. Advances in Cryptology - Crypto 2001, Springer-Verlag, pp. 213-229, 2001.

[3] 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

[4] J Baek, J Newmarch, R Safavi-Naini and W. Susilo, “A Survey of Identity-Based Cryptography”, School of Information Technology and Computer Science, University of Wollongong.

[5] M. Gagné, “Identity Based Encryption: A Survey”, RSA Laboratories Crypto bytes Volume 6, No.1 — Spring 2003

[6] D Boneh, E. Goh and X. Boyen, “Hierarchical Identity Based Encryption with Constant Size Cipher text”, Advances in Cryptography- Euro crypt 2005, pp. 440-456

[7] D. Boneh and M. Hamburg, “Generalized Identity-Based and Broadcast Encryption Schemes”, Asia Crypt 2008.

[8] V. Goyal, “Reducing Trust in the PKG in Identity Based Cryptosystems”, Advances in Cryptology - Crypto 2007

[9] M. Ho Au, Q. Huang, J. K. Liu, W. Susilo, D. S. Wong and G. Yang,” Traceable and Retrievable Identity-Based Encryption”, Proceedings of Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008

[10] 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

[11] 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.

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

[13] 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.

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

[15] 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.

[16] 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.

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

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

[19] 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.

[20] 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.

[21] 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.

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

[23] 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.