Techniques Practiced in Identity-based Cryptography and Applications

Ms. Amrita Kungwani(*Author*)
Dept. of Computer Science and Engineering
Jhulelal Institute of Technology
Nagpur, India

Dr. C. S. Warnekar (*Author*)
Dept. of Computer Science and Engineering
Jhulelal Institute of Technology
Nagpur, India

***Abstract*— With regards to confidentiality, cryptography is used to encrypt data residing on storage devices or traveling through communication channels to avoid any illegal access. Also, cryptography is used to secure the process of authenticating the parties which attempt any function on the system. Since a party wishing be granted a certain functionality on the system must present something as a proof that they indeed who they say they are. That something is sometimes known as credentials and additional measures must be taken to ensure that these credentials are only used by their authorized owner. The most classic credential used is passwords. Passwords are stored in encrypted format to protect against illegal usage. Identity Based Cryptography is an important concept of public key cryptography. Elliptic Curve is now being used in designing many cryptographic protocols. Pairing based protocols are used in many protocols and pairing has found applications in the solution of ID – based Cryptographic schemes and short signature schemes. Pairing-based cryptography does pairing between elements of two cryptographic groups to a third group with a mapping e: G1 * Gs -> GT to construct or analyze cryptographic systems.**

Keywords*— *Identity based Cryptography, Public Key, Private key, authorisation, digital signature.

I. INTRODUCTION

Identity-Based (IB) cryptography is an emerging approach to public-key cryptography that does not require principals to pre-compute key pairs and obtain certificates for their public keys instead, public keys can be arbitrary identifiers such as email addresses, while private keys are derived at any time by a trusted private key generator upon request by the designated principals. Identity Based Cryptography is used to secure the process of authenticating the parties which attempt any function on the system. This technique is dependent on the identity of the user. The identifier information of the user i.e. IP Address, email or mobile number instead of digital certificates can be accepted and used as public key for signature verification or encryption. The previously available scheme like RSA is more complex because it requires two prime numbers with some conditions leading to difficulty in find a couple of numbers as initiator of keys for millions of users. This complexity and difficulties of public key encryption is reduced by the process called identity-based cryptography, which significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework. The idea of IB cryptography was emerged in 1984, although only an IB signature (IBS) scheme was then suggested, based on conventional algebraic methods in Zn. Other IBS and identification schemes were convenient to follow. However, it is only in 2001, a practical IB encryption (IBE) mechanism was Ultimately suggested, based on the much heavier machinery of bilinear pairings on elliptic curves, whose use in cryptography had slowly started to surface in the few years prior, e.g., for key exchange and IBS.

II. CONCEPT OF IDENTITY BASED CRYPTOGRAPHY SYSTEM

In the IBE scheme, the sender Alice can use the receiver's identifier information which is represented by any string, such as email or IP address, even a digital image, to encrypt a message. Bob(receiver), having obtained a private key associated with his identifier information from the trusted third party called the Private Key Generator (PKG)", can decrypt the cipher text.

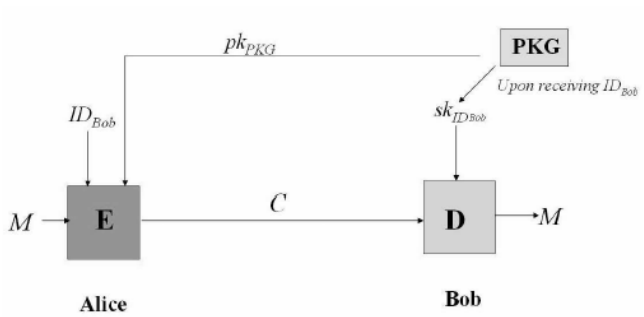

Fig 1: Identity-Based Encryption

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

1. Setup: The PKG generates its master (private) and public key pair, which we denote by skPKG and pkPKG respectively.

2. Private Key Extraction: Bob (receiver) authenticates himself to the PKG and obtains a private key skIDBob associated with his identity IDBob.

3. Encryption: Alice uses Bob's identity IDBob and the PKG's pkPKG to encrypt her plaintext message M and obtains a cipher text C.

4. Decryption: Upon receiving the cipher text C from Alice, Bob decrypts the cipher text using his private key skIDBob to recover the plaintext M.

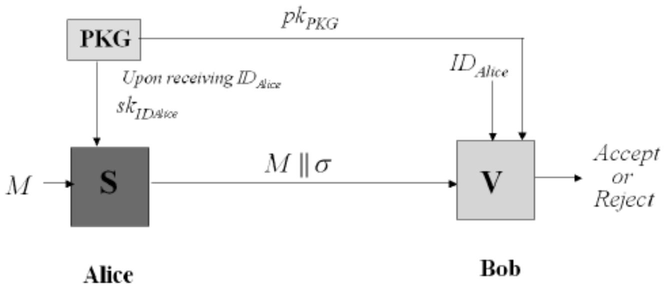

Fig 2: Identity-Based Signature

Similar to the identity-based encryption, one can consider an identity-based signature (IB) scheme. In this scheme, the signer Alice initially obtains a signing (private) key associated with her identifier information from the PKG. Alice then signs a message using the signing key. The verifier Bob uses Alice's identifier information to verify Bob's signature. An IBS scheme can be described using the following steps:

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

2. Private Key Extraction: The signer Alice authenticates herself to the PKG and obtains a private key skid.

3. Signature Generation: Using her private key skid Alice, Alice generates a signature ¾ on her message M.

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

III. IDENTITY BASED CRYPTOGRAPHY SCHEMES FROM BILINEAR PAIRING

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 cipher text 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 G1, G2 be two groups of the same prime order q. We view G1 as an additive group and G2 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 G1 and G2. A mapping e:G12->G2 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 € G1 and a, b

€ 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)≠1.

Computable: There exists an efficient algorithm to compute e(P,Q) for all P,Q € 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 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. 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 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 nonstandard DBDHI problem. A later construction due to Boneh and Boyen 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. 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. 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. In the aforementioned constructions, the time needed for encryption and decryption grows linearly in the hierarchy depth, thus becoming less efficient at complex hierarchies.

C. Fuzzy identity based encryption

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 $d(\omega, \omega') < e$ 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. 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. 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.

V. COMPARASION OF PUBLIC KEY CRYPTOGRAPHY AND IDENTITY BASED CRYPTOGRAPHY

In this area we look at the general population key Infrastructure plan and Identity-based key Cryptography.

A. Open key cryptography

Open Key Infrastructures (PKIs) are presently the essential method for sending hilter kilter cryptography. In this paper, when examining PKIs we are alluding to frameworks that backing the organization of customary hilter kilter cryptographic calculations, for example, RSA. In light of the inborn open nature of the encryption or confirmation keys, the trustworthiness of the general population keys is normally secured with a declaration. The PKI is the foundation that backings the administration of keys and testaments. And in addition the keys and declarations, the center segments of a PKI are:

Testament Authority (CA): The CA is the element that produces the declarations. It is in charge of guaranteeing the right key is sure to the authentication, and in addition guaranteeing the declaration content.

Enlistment Authority (RA): The RA is in charge of guaranteeing that the client that gets the testament is a genuine client inside the framework. The usefulness of the CA and RA is now and then completed by a solitary substance.

Endorsement Storage: In many frameworks declarations (and also overhaul data, for example, Certificate Revocation Lists) are put away in a CA oversaw database.

Programming: For the endorsements to be useful, the product that is going to utilize the declarations need to be mindful of what the endorsement substance speaks to inside the extent of the framework security strategy.

Strategies and Procedures: Although the center of a PKI is mostly specialized, there is, by need, a solid prerequisite for guaranteeing that the components are utilized effectively. The Certificate Policy (CP) and Certification Practice Statements (CPS) characterize the how the declarations are produced and oversaw. They likewise characterize the part of the declarations inside the more extensive security construction modeling. In a customary PKI, one can pick where the key pair is created. The keys can either be produced by the CA for the customer, or the customer can create the keys for itself and give a duplicate of general society key to the CA to confirm. The decision of system will to a great extent be directed by the security arrangement of the framework. It will likewise be affected by the key use. On the off chance that a mark key is prone to be utilized to backing non-revocation, then it is better that the key is produced by the customer. On account of a decoding key that is utilized to keep organization data private, it may be judicious to have the CA create (or have admittance to) the key so there is dependably a method for recouping scrambled data.

B. Identity/Identifier-Based Public Key Cryptography

One of the challenges intrinsic in running a PKI is in the overseeing of the endorsement and related key. Personality – and in this way identifier – based cryptography was made as a method for beating this issue. Shamir was the first to propose such a plan in which the key itself is created from some freely identifiable data, for example, an individual's email address. His unique plan gave a mark calculation, however couldn't be utilized for encryption. It is just as of late that an effective personality based encryption framework was proposed by Boneh and Frank

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 its 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.

- IDE 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.
- IDE 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 primary issue in the web application is to get the get the collectors open key. In the ordinary PKI sender will store general society key of the beneficiary in some database and get the data. In personality based encryption the sender will know just the beneficiary e-mailid and this can be utilized as general society key.

C. Electronic Voting

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

D. Mobile Phone Calls.

Character based cryptography offers a way to deal with end-to end encryption for cell phone brings in which the phone quantities of the call members are utilized as the general population keys to secure the correspondence station, in this way making the cryptographic security methodology as simple as making a phone call.

VIII. CONCLUSION

In this paper we review the condition of craft of the personality based cryptography. Diverse cryptographic plans utilizing the character based encryption. Examination of the character based encryption with the conventional open key encryption preferences and inconveniences and utilizations of the IBE. The zone is as yet developing and numerous new utilizations of the IBE will be included. We accept our study helps in giving learning of IBE and exploration work that has been completed in the zone of IBE for the late years. The test is to make IBE is a valuable innovation for this present reality application.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Dr. C. S. Warnekar, Ms. Mona Mulchandani and Ms. Nisha Balani for their supervision, guidance and support throughout the period of learning.

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 or 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. Girish et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5521-5525