ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A REVIEW: ON IDENTITY-BASED CRYPTOGRAPHY TECHNIQUES AND APPLICATIONS

Deepti Sangwan[1], Shailendra Soni[2] & Ritu Kadyan[3]
[1]M. tech Scholar, Department of Computer Science, Ganga Technical Campus, India
[2]Assistant Professor, Department of Computer Science, Ganga Technical Campus, India
[3]Assistant Professor, Department of Computer Science, Ganga Technical Campus, India

ABSTRACT

This paper contains a review on the state of research on the important topic in the field of information interchange that is identity-based cryptography which more or less extension of the public key cryptography field. The paper starts with analyzing the fundamental concepts of identity-based cryptographic techniques. These cryptographic techniques include encryption and digital signature technique for authentication, which is called as identity-based signature. Mainly, this paper contains analyses on various techniques and applications of identity-based cryptography which depends on the methods of bilinear pairing. Bilinear pairing is a computational method widely used to build up various identity-based cryptography systems in the current literature. Afterwards this paper reviews the identity-based encryption applications in the field of various networks such as ad-hoc networks, mobile networks and other wireless networks in the current era.

Keywords: *Cryptography; Information Security; ID-Base Cryptography.*

I. INTRODUCTION

Adi Shamir in 1984 introduced the idea and concept of identity-based cryptography. This technique is based on identity of the user. The identifier information of the user such as IP Address, email or phone number instead of digital certificates can be accepted and used as public key for signature verification or encryption. As previously available schemes like RSA is more complex because it requires two prime numbers with some conditions. This is difficult to find a couple of numbers as initiator of keys for millions of users. The complexity and difficulties of public key encryption is reduced, the output of this process is identity-based cryptography, which significantly reduces the system's complexity and the cost for establishing and managing the public key authentication framework. This framework is known as Public Key Infrastructure (PKI). There was a change in the conventional public key cryptography It was that, in place of a random couple of public key and secrete key generation, the user could be choose his identity like his name, IP address or his mobile number as his public key.

II. IDENTITY BASED CRYPTOGRAPHY

In the identity-based system, one person is authorized to generate a public key from their known identity value, may be a string. There is a third party in the environment to generate the corresponding private key; this system is called as Private Key Generator, responsible to generate the key. First the master public key is published by the PKG and then the master private key is retained. This master private key is referred as master key.

Say UID is the unique identity of a user like his email UID. For given master public key, any user, can compute a public key with reference to the identity UID by combining the identity value with the master public key. Now other user needs corresponding private key. Therefore, for obtaining this private key, this user recommends to use the identity UID and contact to PKG. The user is authorized to contact PKG. PKG uses the master private key to generate the private key for the identity UID.

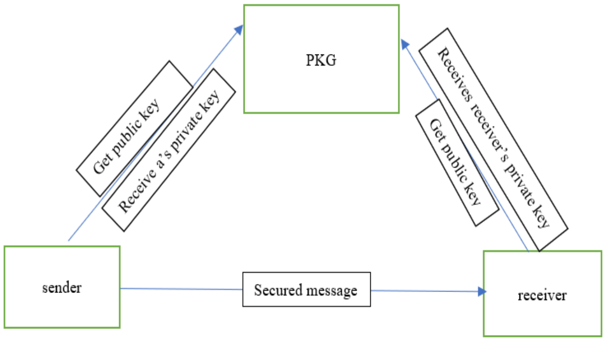

Figure: 1 Illustrates the offline steps of the ID based Encryption system.

We assumed that there is a sender at one end and a receiver on the other end. Both these parties trust a third party for secrecy, it is Private Key Generator (PKG).

PKG is responsible for creating the environment for the ID based encryption system. So 'sender' wants to send an encrypted message to receiver. First PKG creates an environment by providing the keys to 'receiver' and 'sender'. first of all 'sender' obtains the public master key using his own private ID, in this case 'sender' select his BANK ATM's PIN number. In place of its 'sender' can be choose his email address, phone number or Social Security number etc.

After this 'sender' is authenticated by the PKG and receive the private key of 'sender'. In place of it 'sender' can be choose his email address, phone number or Social Security number etc. After this 'sender' is authenticated by the PKG and receive the private key of 'sender'. After obtaining these keys 'sender' executes the encryption process and finally protected message is transferred to receiver 'receiver'. Before applying the decryption and verification process, 'receiver' obtained the master public key from PKG using his email id b@abc.in. PKG provides the master public key based on his ID then authenticate it and provide the private key to 'receiver'. Now his end 'receiver' applies the decryption and verification process to access the actual message.

III. SECURITY OF IDENTITY BASED CRYPTOGRAPHY

For identity-based cryptography a number of schemes have been proposed. All the schemes which are discovered so far in context with identity based cryptography are computationally efficient.These schemes are based on mathematical functions called *bilinear nondegenerate maps*. A bilinear nondegenerate map is a function pairing element from one cyclic group to another of the same prime order, where as the discrete log problem is hard in the first group.

The security of identity-based cryptography depends on the bilinear maps choosen.The bilinear maps chosen should be one-way functions, making it is easy to calculate the result with given pair of operands but hard to calculate the inverse. This property is often referred to as the *Bilinear Diffie-Hellman Assumption*, since the Bilinear Diffie-Hellman problem is reducible (algorithmically equivalent) to the discrete-log or inverse operation for these bilinear maps.

In simplify notation a bilinear map has the property:
Pair(a.X,b.Y)=Pair(a.Y,b.X)
Non degeneracy:Pair(X,Y)!=1

In two of the more well-known IDE systems, the Weil (pronounced vay, rhyming with the English word *way*) and Tate pairings, the · operator above refers to multiplication of a point on an elliptic curve by integers . Although the multiplication operation, such as calculating $a \cdot X$, is easy, finding a given X and $a \cdot X$ is computationally infeasible.

Both Franklin and Boneh were the first to propose a viable IDE system based on the Weil pairing in2001, nearly two decades after Shamir's original proposal. Since then a number of other pair- based IDE and IDS systems have been proposed. As we can see that most of the schemes are pairing-based, so identity-based cryptography is often called as Pairing based cryptography.
Cryptographic operations in the both Franklin and boneh IDE system are conducted as follows. Not that some details of the math involved in elliptic curves have been omitted for clarity's sake

Setup: The PKG picks an elliptic curve, a secret s and a point P on the curve using a random number generator. It then publishes P and $s \cdot P$ as the master public key.

Encryption: sender hashes the chosen identity attribute for receiver to a point $\mathrm{IDr}_{\mathrm{eceiver}}$ *on* the elliptic curve. He/She then picks a random r and calculates a key k:
K= pair $(r.ID_{bob,}s.p)$
Alice then sends E_k[M]and r.P to bob.

Decryption: Receiver may not yet have a private key. To get it, he authenticates with the PKG, which calculates s $\cdot$ $\mathrm{ID}_{\mathrm{receiver}}$ returns it to him over a secure channel. This is his private key. After receiving $E_k[M]$ and $r \cdot P$ from Sender, Receiver can recover the key k by calculating:
K= pair $(r.ID_{bob,}r.p)$

This is possible because of the properties of bilinear maps. Receiver can then use k to decrypt the message. No one else (besides the PKG) can calculate k because only Receiver knows $s \cdot IDreceiver$.

Even though Shamir had already provided one possible identity-based signature system based on RSA in his seminal proposal, other researchers have discovered pairing-based IBS systems to complement the pairing-based encryption systems**.**

IV. PROS AND CONS OF IDNTITY BASED CRYPTOGRAPHY

1. To receive an encrypted message no preparation is required on the part of the recipient . This is the most compelling feature of IDC.
2. There is no need of managing a public key infrastructure, including CRL management.
3. The IBC's inherent key escrow feature means that the decryption and signature can take place on the server. While this is a disadvantage (especially in IDS because it eliminates non-repudiation in most cases), it also makes certain other features possible that are not possible in PKI-based systems where the signer has the possession of his/her private key, such as:

i."Chameleon" signatures, in which only the designated recipient is capable of asserting a signature's validity.

ii.As the PKG is handling the cryptographic operations for the user and requiring no client-side installation we can say that this scheme is more user friendly. It can be especially powerful in case of an enterprise which wants to adopt a policy whereby all messages of a certain sensitivity level are automatically encrypted and/or signed. An administrator can specify the rules and regulations that govern whether a message will be signed or encrypted using tools like a keyword search of the message content, a time range, or a regular expression match on the sender or recipient, and email users do not need to modify their behavior.

iii. while the users are not keeping their private key, it can be kept on the PKG, which often has a much higher level of security than a user's workstation.

4. If there is no PKI it means there is less public information about your enterprise need be revealed to those who do not have a need to know. Every person or application connecting to an enterprise's certificate database could theoretically discover a great deal of information about a company's infrastructure or hierarchy. For the companies having large number of employees where some employees work on sensitive projects or where many

employees only interact with their close colleagues on a daily basis, not needing to access a certificate database could be beneficial.

The most notable disadvantage of IBC is its inherent key escrow property. While it has already been noted that this can be an advantage in some cases, most IDC adopters would like to be able to decide whether or not they want this feature. It should be noted that many organizations already employ encryption key escrow, to be able to recover a user's encrypted data in the event his or her private key is lost. This should be taken into account when analyzing the security of IBC systems. The practical difference, therefore, between IBC and most PKI systems is that PKI systems do not escrow users' signature keys. This allows for better non-repudiation, which is an essential feature of digital signature schemes. A number of IBC variants are also being developed that eliminate or mitigate the key escrow feature, including certificate-based encryption, secure key issuing cryptography and certificateless cryptography. In secure key issuing, for example, the PKG's level of trust is reduced by spreading the master keys across multiple PKGs. While this increases the system's security, it also decreases performance.

Another important drawback of IBC system is the high level of assurance required in the PKG. Since the PKG holds all private keys, it requires a higher level of assurance and availability than a CA. CAs may be kept disconnected from a network, but the PKG must be available to send users their private keys, further increasing its vulnerability to attack. For this reason, extra care must be taken to secure PKGs above and beyond the high level of security already required for Cas.

V. IMPLEMENTATIONS OF IDENTITY BASED CRYPTOGRAPHY

Boneh and Franklin, along with other researchers, developed a C++/based IBE implementation published under an MIT-style license, called the “Stanford IBE System”.

Shamus Software also developed another C++-based cryptographic library called “MIRACL”which follows Boneh and Franklin's IBE scheme.

The most notable commercial implementation of IBE is published by Voltage Security, Inc. They offer plug-ins for a number of popular mail clients, including Microsoft Outlook. Proofpoint, Inc. has licensed Voltage's software to provide value-addons, such as policy-based automatic outbound email encryption.

VI. CONCLUSION

As per above discussion on identity-based encryption, we can say it is better approach for the secure information exchange in any type of network and any scale of users. This technique has its benefit over the competent techniques. Because of this, the technique is acceptable for variety of applications. Apart from this, there are some open problems to solve in this related field like Key Escrow Problem, Revocation Problem and yet, we do not know whether it is possible to construct especially IBE schemes which are not based on the pairing but are more efficient than Cocks' IBE scheme.

REFERENCES

1. *Encryption Made Easy: The Advantages of Identity-Based Encryption, Proofpoint Inc.http://www.proofpoint.com/downloads/WP-Proofpoint-Encryption-Made-Easy.pdf.*
2. *Identity-basedencryption http://en.wikipedia.org/wiki/Identity_based_encryption.[3]Identity-basedencryption. http://www.voltage.com/technology/ibe.htm*
3. *A.Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO '84, LNCS 196, pages 47-53, Springer-Verlag, 1984.*
4. *J. Baek, J. Newmarch, R. Sfavi-Naini, W. Susilo, A Survey of Identity-Based Cryptography, http://jan.netcomp.monash.edu.au/publications/auug_id_survey.pdf.*
5. *BilinearPairings. http://rooster.stanford.edu/~ben/maths/ep/pairing.php*

6. *D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing, Proceedings of CRYPTO 2001, LNCS 2139, pages 213–229, Springer-Verlag,2001. http://crypto.stanford.edu/~dabo/papers/ibe.pdf.*
7. *D. Boneh, B. Lynn, H. Shacham, Short Signatures from the Weil Pairing, Asiacrypt, Lecture Notes in Computer Science, vol. 2248, pages 514+, 2001. http://citeseer.ist.psu.edu/boneh01short.html.*
8. *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. http://www.cesg.gov.uk/site/ast/idpkc/media/ciren.pdf.*