Identity Based and Attribute Based Cryptography: A Survey

Meenal Jain and Manoj Singh

Abstract— Changing scenario of cryptography has led to a change in paradigm of from certificate based public keys and keyrings to user-dependent keys which are based on identities of users or their attributes. This is termed as identity based cryptography or attribute based cryptography. Such encryption schemes are much relevant in current scenario of cloud computing and mobile computing where participation of user in transactions is partial, or user-based access control over an encrypted database is required. This paper presents a survey of identity based and attribute based cryptographic primitives.

Index Terms— Cryptography, Cryptosystem, Signcryption

I. INTRODUCTION

Identity-based cryptosystem was first conceived as an idea by Shamir[1] in 1984 as a means to get rid of public-key certificates by allowing the user’s public key to be an arbitrary string which is an information identifying the user in a non-ambiguous way (through identities like email address, social security number etc). The advantage was that cost of establishing and managing the public key authentication framework was reduced significantly. Also the system complexity public key infrastructure was reduced. The main problem here is that for every application or system a unique string identifier cannot exist. Rather users are generally identified by their attributes. Sahai et al [2] proposed attribute based encryption (ABE) as a problem to this solution. ABE views identity of any user as a set of attributes. The key-authority distributes the attributes and they are used to generate an identity. Then a scheme built on ideas from IBE [1, 3-5] can be used. In this paper we first review some important Identity based encryption, signature and signcryption schemes. Subsequently, we review a few important attribute based encryption and signature schemes.

II. IDENTITY BASED CRYPTOGRAPHY

Encryption keys derived from user identities are useful in avoiding trust problems which are generally faced in certificate based public key infrastructures (PKIs). This is so because there is no need of binding a public key to its owner, which is a single unique entity. These systems generally involve some trusted authorities, called private key generators, to compute users’ private key from their identity information (users do not generate their key pairs themselves). The idea was proposed first by Shamir[1] in 1984. Many practical identity based signature schemes [6-7] have been devised since then. The problem was again brought to surface by Boneh et al [3] in 2001. They presented the first identity-based encryption scheme based on use of groups for which there was an efficiently computable bilinear map. It was proved to be secure and practical. Ever since, a rapid development of IBE and IBS has taken place, and a series of research [4,5,8-14] have proposed newer notions of security which are stronger in the standard model. The first construction of IBE, called the Selective-ID model was proposed by Canetti et al [4]. Being a slightly weaker model in which the adversary declares the identity to be attacked before the global public parameters are generated; it is provably secure outside the random oracle model. Boneh et al [13] presented a space-efficient IBE without pairings. Gentry [15] proposed the first CCA2 secure IBE system without random oracles that has a tight reduction to decisional Bilinear Diffie-Hellman Exponent assumption. This scheme was extended as [16] to construct an adaptively-secure identity based broadcast encryption system without random oracles. Boyen [17] proposed a framework for constructing Hierarchical Identity-based Encryption (HIBE) systems from exponent-inversion IBE systems. The idea is to select pairing-based IBE systems having specific properties (also called parallel IBE and linear IBE). Authors [17] proved that an IBE system with these properties can be transformed into HIBE with comparable security. Identity based signcryption achieves the functionality of signcryption with the added advantages that IBE provides. Malone-Lee[18] proposed the first identity based signcryption scheme. Since then quite a few ID-based signcryption schemes have been proposed [19-23]. Out of these most efficient are those of Chen et al [23] and Barreto et al [22]. In 2008, Li et al [24] devised an identity based threshold signcryption scheme and proved the confidentiality of their scheme. Selvi et al [25] soon showed that in the scheme [24] the secret key of the sender is insecure in the presence of malicious insiders during signcryption. They proposed an improved scheme [25] in the same security model.

Basics of IBE

There are four functions in IBE: 1) setup - generates global system parameters and a master-key, 2) extract - uses the master key to generate the private key corresponding to an arbitrary public key string ID, 3) Encrypt – encrypts messages using the public key ID, 4) Decrypt – decrypts messages using the corresponding private key.

Manuscript received May 16, 2015.

Meenal Jain, M.Tech. Computer Science, Department of Computer Science, Gurukul Institute of Engineering & Technology, Kota, Rajasthan, India

Manoj Singh, Head of Department, Department of Computer Science, Gurukul Institute of Engineering & Technology, Kota, Rajasthan, India
A map \( \hat{\epsilon} : \mathcal{G}_1 \times \mathcal{G}_2 \to \mathcal{G}_2 \) is called a bilinear pairing if for all \( x, y \in \mathcal{G}_1 \) and all \( \alpha, \beta \in \mathbb{Z} \), we have \( \hat{\epsilon}(x^\alpha, y^\beta) = \hat{\epsilon}(x, y)^{\alpha \beta} \).

The Bilinear Diffie-Hellman problem for a bilinear map \( \hat{\epsilon} : \mathcal{G}_1 \times \mathcal{G}_2 \to \mathcal{G}_2 \) such that \( |\mathcal{G}_1| = |\mathcal{G}_2| = q \) is primarily defined as follows: To give \( g, g^a, g^b, g^c \in \mathbb{G}_1 \), compute \( \hat{\epsilon}(g, g)^{abc} \), where \( g \) is a generator and \( a, b, c \in \mathbb{Z} \). An algorithm \( A \) is said to solve the BDH problem with advantage \( \varepsilon \) if 
\[
\Pr[A(g, g^a, g^b, g^c) = \hat{\epsilon}(g, g)^{abc}] \geq \varepsilon ,
\]
where the probability is over the random choice of \( a,b,c,g \) and the random bits of \( A \).

Secret sharing scheme – Secret sharing schemes are used to divide a secret among a number of parties. The information given to a party is called the share (of the secret) for that party. Every SSS realizes access structure that defines the sets of parties who should be able to reconstruct the secret by using their schemes. Shamir and Blakley [26] were the first to propose a construction for (t,n) secret-sharing schemes where the access structure is a threshold gate. That is, if any \( t \) or more parties come together, they can reconstruct the secret by using their shares. However, any lesser number of parties does not get any information about the secret.

III. ATTRIBUTE- BASED CRYPTOGRAPHY

The concept of attribute-based encryption emerged from fuzzy–IBE proposed by Sahai[2]. The basic idea is user with secret key for identity \( \omega \) is able to decrypt a ciphertext encrypted with identity \( \omega' \) if and only if \( \omega \) and \( \omega' \) are close to each other as measured by the “set overlap” distance metric. In other words, in an ABE system, if the message is encrypted with a set of attributes \( \omega' \), a private key for a set of attribute enables decrypting that message, if and only if \( |\omega \cap \omega'| \geq d \), where \( d \) is fixed during the setup time. Thus, ABE achieves error tolerance making it suitable for use with biometric identities. One drawback of the Sahai approach is that their initial construction was limited to handling formulas consisting of one threshold gate.

Proper attribute-base schemes appeared in [27-29] as an improvement of these ideas. Further research can be divided into two categories: key policy ABE and ciphertext policy ABE. Goyal et al[30] further clarified these concepts of attribute-based encryption. In particular, they proposed two complimentary forms of ABE. Firstly, key-policy ABE (KPABE): in this the attributes are used to annotate the ciphertexts and formula’s over these attributes are ascribed to user’s secret keys. Goyal et al[30] provided a construction for KPABE that allowed keys to be expressed in terms of a monotonic formula over encrypted data. The system has been proved to be selectively secure under the Bilinear Diffie-Hellman assumption. The second type, ciphertext–policy ABE (CPABE) is a complimentary form. In this the attributes are used to describe the user’s credentials and the formulas over these credentials are attached to the ciphertext by the encrypting party.

The problem of CPABE was explicitly addressed in [31] by Bethencourt et al. The proposed system is efficient and expressive, analogous to the Goyal et al [30] construction. It allows an encryptor to express an access predicate \( f \) in terms of any monotonic formula over attributes. Cheung et al [32] proposed another CP-ABE scheme in which decryption policies are restricted to a single AND gate, but attributes are allowed to be either positive or negative. Goyal et al [33] provide a “bounded” CP-ABE construction; a general approach to construct a CP-ABE scheme from a KP-ABE system. The main drawback of this approach is that it needed to build a complete tree of depth \( d \) to cover all possible access trees. A new technique to realize cipher text-policy attribute encryption (CP-ABE) was proposed by Brent[34]. The proposal considers concrete and non-interactive cryptographic assumptions that allow any encryptor to specify access control in terms of an LSSS matrix, \( M \), over the attributes in the system. Chase[35] proposed a solution for multi-authority attribute-based encryption, provided that a trusted central authority is available.

Besides encryption, there have been several efforts towards constructing attribute based signatures. Yang et al. [36] proposed the notion of fuzzy identity-based signature (FIBS). In FIBS, the user can sign a message with some of its attributes. The verifier can check if the signature is signed by user with these attributes. Mazi et al. [37] tried to achieve attribute-based signature with signer privacy. But the proposal suffers from weak security; the security has been proved only in non-standard hardness assumption and generic group model. Khader[38] proposed another notion which was called attribute based group signature. It allows a verifier to request a signature from a member of a group who possesses certain attributes and the signature should prove ownership of certain properties. However, what the picture is currently missing is an algorithm that combines (existing or new) ABE and signature into practical and secure way.

Access structure

Let \( \mathcal{P} = \{P_1, P_2, ..., P_n\} \) be a set of parties. A collection \( \Gamma \subseteq 2^\mathcal{P} \) is monotone if
\[
\forall B, C \in \Gamma \text{ and } B \subseteq C \implies B \subseteq \Gamma.
\]
An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) \( A \) of non-empty subsets of \( \{P_1, P_2, ..., P_n\} \). i.e. \( \Gamma \subseteq 2^\mathcal{P} \setminus \{\emptyset\} \).

The sets in \( \Gamma \) are called the authorized sets and the sets not in \( \Gamma \) are called the unauthorized sets.

The initial ABE schemes were limited to expressing only monotonic access structures and there is no satisfactory method to represent negative constraints in a key’s access formula. Ostrovsky et al.[28] proposed the attribute-based encryption with non-monotonic access structure. Non-monotonic access structure can use the negative word to describe each attributes in the message, but the monotonic access structure cannot. The problem with Attribute-based Encryption Scheme with Non-Monotonic Access Structures is that there are many negative attributes in the encrypted data, but they don't relate to the encrypted data. It means that each attribute adds a negative word to describe it, but these are useless for decrypting the encrypted data. It can cause the encrypted data overhead becoming huge. It is inefficient and complex each ciphertext needs to be encrypted with \( d \) attributes, where \( d \) is a system-wise constant.

Hierarchical attribute-based encryption (HABE) is derived by Wang et al[39]. The HABE model consists of a root master (RM) that corresponds to the third trusted party (TTP), multiple domain masters (DMs) in which the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. This scheme used the property of hierarchical generation of keys in
To reduce the burden of authority and achieve immediate attribute revocation, two CP-ABE schemes with immediate attribute revocation were proposed by Ibrahim et al. [49] and Yu et al. [50]. They employ a semi honest service provider for this purpose. However, these too have failed to achieve fine-grained user access control in the data outsourcing environment. For this reason, Hur and Noh [51] proposed a CP-ABE scheme with fine-grained attribute revocation with the help of the honest-but-curious proxy deployed in the data service provider. Boldyreva et al. [43] proposed an efficient revocation method that uses a binary tree to represent revocation and each revocation is followed by reencryption of ciphertext. However, this scheme cannot resist the collusion attack. Aiming at reducing the computation overhead of data service manager, Xie et al. [52] proposed new CP-ABE construction with efficient user and attribute revocation. Compared with Hur and Noh’s [51], in the key update phase, the computation overhead of the data service manager will be reduced by half.

The direct revocation method enforces revocation directly by the sender who specifies the revocation list while encrypting the cipher text. A directly revocable KP-ABE scheme was first mentioned by Staddon et al. [57], but their scheme only works when the number of attributes associated with a ciphertext is exactly half of the size of the universe of real attributes. Attrapadung and Imai [54] suggested a user-revocable ABE scheme by combining broadcast encryption schemes with ABE schemes. However, the data owner should take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation. This scheme is not applicable to the data outsourcing architecture, because the data owner will no longer be directly in control of data distribution after outsourcing their data to the external data server. Liang et al. [55] proposed a CP-ABE scheme with efficient revocation. Their construction uses linear secret sharing and binary tree techniques, and can be proved secure in the standard model. In addition to the attribute set, each user is also assigned a unique identifier. Therefore, a user can be easily revoked by using his/her unique identifier. All the above schemes [53, 54, 55] support user revocation, but they have no effect on attribute revocation. Recently, Wu and Zhang [56] first formalized the notion of adaptively secure ABE scheme supporting attribute revocation under direct revocation mode.

V. CONCLUSION

Encryption mechanisms based on user identities and attributes hold a great promise for changing scenarios of computing, namely cloud computing and ubiquitous computing. These schemes relate a key with a set of attributes and thus alleviate the problem of key generation and distribution of PKI. Also, the concepts of such schemes can be used to further design trust and security mechanisms for data storage in cloud.

REFERENCES