Categorical Heuristic for Attribute Based Encryption in the Cloud Server

R. Brindha[1], **R. Rajagopal**[2]

[1](M.E , Dept of CSE, Vivekanandha Institutes of Engineering and Technology for Women, Tiruchengode, India)

[2](Assistant Professor , Dept of CSE, Vivekanandha Institutes of Engineering and Technology for Women, Tiruchengode, India)

ABSTRACT- *Attribute-based encryption (ABE) is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and Ciphertexts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. In ABE system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes or access policy into a simple ciphertext, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed ciphertext. However, it does not guarantee the correctness of the transformation done by the cloud. In the existing system, a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. In the proposed Categorical Heuristics on Attribute-based Encryption (CHAE) is an adaptation of Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance of the signed data, and moreover towards the anonymity of the signer. Finally, show an implementation of our scheme and result of performance measurements, which indicates a significant reduction on computing resources imposed on users.*

***KEYWORDS* - Attribute-based encryption, outsourced decryption, verifiability, CHABE, CABS.**

I INTRODUCTION

ABE is a new public key based one-to-many encryption that enables access control over encrypted data using access policies and ascribed attributes associated with private keys and Ciphertexts. There are two kinds of ABE schemes: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext.

CP-ABE: attributes sets are used to annotate the Ciphertexts and access polices over these attributes are associated with users' private keys. One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a ciphertext grows with the complexity of the access policy. In KP-ABE they encrypt the attributes along with the data and give the access structure to each user as part of their secret key.

Attribute based encryption is more applicable in the regular world if the access structure can be embedded in the cipher text and the users can have their attributes saved in their secret keys. CHAE is an adaptation of ABE for the purposes of providing guarantees towards the provenance of the signed data, and moreover towards the anonymity of the signer.

A digital signature scheme is a mathematical scheme for representing the authenticity of a digital message or document. A valid digital signature gives an assured reason to believe that the message was created by a known sender, and that it was not altered during data transfer. Categorical Attribute-based signature (CABS), which allows a signer to choose a set of attributes instead of a single string representing the signer's identity, under standard cryptographic assumption in the standard model is a challenging problem. Signatures in a CABS scheme describe a message and a predicate over the universe of attributes. A valid CABS signature attests to the fact that a single user, whose attributes satisfy the predicate, endorsed the message.

In this work emphasize the word single in this informal security guarantee CABS signatures, as in most attribute-based systems, require that colluding parties not be able to pool their attributes together. Furthermore, attribute signatures do not reveal more than the claim being made regarding the attributes, even in the presence of other signatures. A CABS assures the verifier that a signer, whose set of attributes satisfies a (possibly) complex predicate, has endorsed the message.

II LITERATURE REVIEW

1. Ciphertext-Policy Attribute-Based Encryption: an expressive, efficient, and provably secure realization

Waters at al., (2011) Public-Key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device. In this method the applications where the data provider knows specially which user he wants to share with, in many applications the provider will want to share data according to some policy based on the receiving user's credentials.

CP-ABE systems from a general set of access structures in the standard model under concrete and non-interactive assumptions. Both the cipher text overhead and encryption time scale with O(n) where n is the size of the formula. The decryption time scales with the number of nodes. CP-ABE under concrete and non interactive cryptographic assumptions in the standard model. This work allows any encryptor to specify access control in terms of any access formula over the attributes in the system. In most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula.

2. Fully secure functional Encryption: ABE and (hierarchical) inner product encryption

Allison Lewko at al., (2010) In a traditional public key encryption system, data is encrypted to be read by a particular individual who has already established a public key. Allison Lewko at al., Functional encryption is a new way of viewing encryption which opens up a much larger world of possibilities for sharing encrypted data. In this method have proposed two fully secure functional encryption schemes; a fully secure ABE scheme and a fully secure (attribute-hiding) predicate encryption (PE) scheme for inner-product predicates. In an ABE system, private keys distributed by an authority are associated with sets of attributes and cipher texts are associated with formulas over attributes. A user should be able to decrypt a cipher text if and only if their private key attributes satisfy the formula. In a predicate encryption scheme, secret keys are associated with predicates, and cipher texts are associated with attributes. A user should be able to decrypt a cipher text if and only if their private key predicate evaluates to 1 when applied to the cipher text attribute.

3. On cryptographic protocols employing asymmetric pairings-the role of revisited

Sanjit Chatterjee at al., (2008) Pairing-based cryptography, though anticipated only at the turn of the century, has witnessed a tremendous growth. The successful application of pairings in the design of novel cryptographic protocols and their potential use as a principal building block for many others fuelled this growth.

Many cryptographic protocols in the asymmetric setting rely on the existence of an efficiently-computable isomorphism for their security reduction while some use it in the protocol itself. For these reasons, it is believed that some of these protocols cannot be implemented with Type 3 pairings, while for some the security reductions either cannot be transformed to the Type 3 setting or else require a stronger complexity assumption. Contrary to these widely held beliefs, we argue that Type 2 pairings are merely inefficient implementations of Type 3 pairings, and appear to offer no benefit for protocols based on asymmetric pairings from the point of view of functionality, security, and performance.

4. Outsourcing the decryption of ABE cipher texts

Hohenberger at al., (2013) ABE is a public key encryption that allows users to encrypt and decrypt messages based on user attributes. ABE is currently being considered for many cloud storage and computing applications. However, one of the main efficiency drawbacks of ABE is that the size of the cipher text and the time required to decrypt it grows with the complexity of the access formula. In this method to implemented a new paradigm for ABE that largely eliminates this overhead for users. Suppose that ABE cipher texts are stored in the cloud. In this work have represented how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE cipher text satisfied by that user’s attributes into a (constant-size) cipher text, without the cloud being able to read any part of the user's messages. To precisely define and demonstrate the advantages of this approach.

This work provide new security definitions for both CPA and replayable CCA security with outsourcing, several new constructions, an implementation of this algorithms and detailed performance measurements. In a typical configuration, the user saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.

This work to use outsourcing as a tool to harden ABE implementations in platforms with code isolation. For example, in a system equipped with Trust Visor, implementers can embed the relatively simple key generation and Decrypt out routines in security-sensitive code and use outsourcing to push the remaining calculations into non-sensitive code. This not only reduces the size of the sensitive code base, it also simplifies parameter validation for the PAL. This technique as "self-outsourcing" and note that it can also be used in systems containing hardware security modules.

5. Decentralizing Attribute-Based Encryption

Lewko at al., (2011) Multi-Authority ABE system. In this system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities.

In constructing this system, largest technical hurdle is to make it collusion resistant. Multi-Authority ABE systems achieved collusion resistance when the ABE system authority tied together different components of a user's private key by randomizing the key. However, in this work each component will come from a potentially different authority, where assume no coordination between such authorities.

To new techniques to tie key components together and prevent collusion attacks between users with different global identifiers.

6. Improved proxy re-encryption schemes with applications to secure distributed storage

Bleumer at al., (2005) Proxy re-encryption allows a proxy to transform a cipher text computed under Alice's public key into one that can be opened by Bob's secret key. There are many useful applications of this primitive. For instance, Alice might wish to temporarily forward encrypted email to her colleague Bob, without giving him her secret key. In this method have proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plaintext. To predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks.

Following recent work of Dodis at al., (2010) new re-encryption schemes that realize a stronger notion of security, and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

7. Attribute-Based Encryption schemes with constant- size ciphertexts

ABE as introduced Sahai and Waters, allows for fine-grained access control on encrypted data. In its key-policy flavor (the dual cipher text-policy scenario proceeds the other way around), the primitive enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which cipher texts the key holder will be allowed to decrypt. In most ABE systems, the cipher text size grows linearly with the number of cipher text attributes and the only known exception only supports restricted forms of access policies. Herranz at al., (2012) First ABE schemes allowing for truly expressive access structures and with constant cipher text size. In this work the first result is a CP-ABE scheme with O(1)-size cipher texts for threshold access policies and where private keys remain as short as in previous systems. As a second result, show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model. The final contribution is a KP-ABE realization supporting non-monotonic access structures (i.e., that may contain negated attributes) with short cipher texts. As an intermediate step toward this result, This work describe a new efficient identity-based revocation mechanism that, when combined with a particular instantiation of our general monotonic construction, gives rise to the most expressive KP-ABE realization with constant-size cipher texts. The downside of our second and third constructions is that private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes.

8. Unbounded HIBE and Attribute-Based Encryption

Lewko at al., (2007) Hierarchical Identity-Based Encryption (HIBE) systems and ABE systems offer users more levels of flexibility in sharing and managing sensitive data than are provided by Identity-Based and Public Key Encryption systems. In a hierarchical identity-based encryption scheme, user identities are arranged in an organizational hierarchy. Anyone can encrypt a message to any identity in the system using the public parameters. An identity at level k in the hierarchy can use its secret key to delegate secret keys to its subordinates, but cannot decrypt any messages which are intended for recipients other than itself and its subordinates.

In a KP-ABE system, users have secret keys which are associated with access policies over a universe of attributes and cipher texts are associated with sets of attributes. A user can decrypt a message encrypted to a set of attributes S only if S satisfies the access policy of the user's key. Both HIBE and ABE systems are designed to accommodate certain changes in the needs of users over time, but current constructions have some inherent limitations. For instance, new users can enter an HIBE system and collect secret keys without requiring any change to the public parameters or the keys of users already present. However, for all previous constructions in the standard model, the identities of new users must fit within the hierarchy depth specified by the public parameters. More precisely, the size of the public parameters grows linearly with the maximum depth of the hierarchy, and it is impossible to add new levels to the hierarchy once the public parameters are fixed.

9. Divertible protocols and atomic proxy cryptography

Blaze at al., (1998) divertible protocols, The notion of divertibility as a protocol property as opposed to the existing notion as a language property. The important examples falling under the new definition are blind signature protocols. This work presents a sufficiency criterion for divertibility that is satisfied by many existing protocols and which, surprisingly, generalizes to cover several protocols not normally associated with divertibility. Next, Blaze have proposed atomic proxy cryptography, in which an atomic proxy function, in conjunction with a public proxy key, converts cipher texts for one key into cipher texts for another. Proxy keys, once generated, may be made public and proxy functions applied in untrusted environments. This work presents atomic proxy functions for discrete-log-based encryption, identification, and signature schemes. It is not clear whether atomic proxy functions exist in general for all public-key cryptosystems. This work introduced the notion of perfect and computational protocol divertibility, and have given a sufficiency criterion for the former. All existing diverted protocols are found in the literature turned out to satisfy this criterion.

V CONCLUSION

Attribute based encryption is more applicable in the regular world if the access structure can be embedded in the cipher text and the users can have their attributes saved in their secret keys. ABE is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. CHAE providing guarantees towards the provenance of the signed data, and moreover towards the anonymity of the signer. Digital signature scheme is a mathematical scheme for representing the authenticity of a digital message or document. A valid digital signature gives an assured reason to believe that the message was created by a known sender, and that it was not altered during data transfer. A Categorical attribute-based signature assures the verifier that a signer, whose set of attributes satisfies a (possibly) complex predicate, has endorsed the message.

REFERENCE

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Proc. EUROCRYPT*, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *Proc. ACM Conf. Computer and Communications Security*, 2006, pp. 89–98.

[3] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in *Proc. ACM Conf. Computer and Communications Security*, 2007, pp. 195–203.

[7] A. B. Lewko and B. Waters, “Unbounded HIBE and attribute-based encryption,” in *Proc. EUROCRYPT*, 2011, pp. 547–567.

[8] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in *Proc. IEEE Symp. Security and Privacy*, 2007, pp. 321–334.

[9] L. Cheung and C. C. Newport, “Provably secure ciphertext policy ABE,” in *Proc. ACM Conf. Computer and Communications Security*, 2007, pp. 456–465.

[10] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, “Attribute-based encryption schemes with constant-size ciphertexts,” *Theor. Comput. Sci.*, vol. 422, pp. 15–38, 2012. [11] S. Hohenberger and B. Waters, “Attribute-based encryption with fast decryption,” in *Proc. Public Key Cryptography*, 2013, pp. 162–179.

[11] M. Green, S. Hohenberger, and B.Waters, “Outsourcing the decryption of ABE ciphertexts,” in *Proc. USENIX Security Symp.*, San Francisco, CA, USA, 2011.

[12] M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols,” in *Proc. ACM Conf. Computer and Communications Security*, 1993, pp. 62–73.

[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in *Proc. Public Key Cryptography*, 2011, pp. 53–70.

[5] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in *Proc. EUROCRYPT*, 2010, pp. 62–91.

[6] T. Okamoto and K. Takashima, “Fully secure functional encryption with general relations from the decisional linear assumption,” in *Proc. CRYPTO*, 2010, pp. 191–208.