ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ABSTRACT BASED CRYPTOGRAPHY

Arun Kumar*, Mohit Verma, Anurag Chandna

* M. Tech Scholar, Dept. of Computer Science, Roorkee College of Engineering, Roorkee, UK, India

Assistant Professor, Dept. of Computer Science Engineering, Roorkee College of Engineering, Roorkee, UK, India

ABSTRACT

The issues of confidentiality, authenticity and anonymity have been known from long time in Security i.e. Cryptography , and the idea of provable security is the basic foundation for most, if not all, latest cryptographic research. With highly advance and improved technology, there is also a need to define these methods of security under various approaches. One such current approach of security is the attribute based view that has been established by the requirements in a distributed setting. Attribute based encryption and signature concept have been developed in order to give a more better grained access control. Currently attribute-based method have large area applicability in a number of new decentralized settings and address some already exciting problems. In this thesis we studied an efficient attribute-based encryption(ABE) method , with support for multi-level threshold predicates. We also discuss regarding the security of some attribute-based signature(ABS) schemes and give the implementation for a threshold ABS method based on a novel approach.

In this paper we first look at ABE. Anonymous access control is a highly required property in various applications, e.g. encrypted data in distributed Systems; and attribute based encryption method is a cryptographic methods that is targeted to achieve this property. ABE is an encryption mechanism that is helpful in settings where the list of users may not be known apriority. Here, all users may possess some credentials, and these are used to know access control and also give a reasonable degree of anonymity with respect to the user's identity. Cipher text policy attribute based encryption is a scheme that gives a natural way to separate the credentials from the access policy and cleverly combine them at a later stage to provide secure access to protected data. In most ABE schemes the size of the cipher text is quite large and is of the order of the number of attributes. In this work we present our approach for a multi-level threshold attribute based encryption which is independent of the number of attributes.

KEYWORDS: Cryptography, ABE, Encryption. etc

INTRODUCTION

Public-key cryptography, also known as asymmetric cryptography, It is a type of cryptographic protocols based on different algorithms that require two separate keys, one of which is *secret* (or *private*) and one of which is *public*. A public-key cryptosystem comprises of mechanisms to provide confidentiality, through public key encryption, and authenticity, through digital signatures. In this type of communication parties involved are - sender and receiver – both maintain a pair of keys each, in order to perform operations like encryption or signing. Depending on the requirement different types of different types of cryptographic system is proposed. Currently new approach is Attribute based system. Unlike in traditional cryptography where the intended recipient or the signer's identity is clearly known, in an attribute based systems one only needs to specify the attributes or credentials of the recipient(s) or the signer in the form of a predicate that is to be satisfied. This feature enables secure data sharing even in a decentralized setting, providing both fine-grained control on access and some degree of anonymity for the participants. In this thesis, we will look at attribute-based systems with special focus on those that support threshold predicates.

ATTRIBUTE-BASED ENCRYPTION

There are several settings where a user would want to provide access to the documents and lies on certain credentials or the position of a person. This can be comparable with 'Views' in a database. We would want different kind of users of the database to be able to see only those contents which is relevant to them in simple words we want access control on database. Similarly, in a distributed setting where all the data may be stored in a server, the server might

allow access to files and documents based on some predefined access control policy, for instance, clients may have to go through proper authentication process to retrieve particular files. In such cases, if the data(storage) in the database or server is compromised, then although it may be in the cipher text form, anyone who has access to the database or server may be able to retrieve all information as well as those documents or files that may not be relevant to them. To be more to the point, any normal user of the database who gets his/her hands on the compromised data may now be able to get those files which were restricted and whose access was determined by some application in the database or server.

ABE: The concept of attribute-based encryption was first proposed in a landmark work by Amit Sahai and Brent Waters in [SW05, GPSW06]. It provides a procedure by which we can ensure that even if the database is compromised, the loss of information will only be minimal. What attribute based encryption does is that, it effectively binds the access-control policy to the data and the users instead of having a server mediating access to files. To understand this better, we will take a closer look at what constitutes an attribute based system, with particular attention to ABE.

Access Policy: An access control policy would be a policy that defines the kind of users who would have permissions to read the documents. e.g In an academic setting, grade-sheets of a subject may be accessible only to a lecturer handling the course and some teaching assistants (TAs) of that course. We can repersent such a policy in terms of a predicate:

((Lecturer ^ ME dept.)V(P.hd student ^ ME-410 TA ^ ME dept.))

Motivation

In this paper we look at threshold ABE and ABS approach. The most appealing fact about threshold gates is that they are very elaborative and encompass the other common AND and OR gate access structures as well.

In mostly existing ABE schemes, the length of the cipher text is very large, it is usually in the sequence of the number of attributes under assumption. Most efficient schemes with expressive access control have cipher text length proportional to the number of attributes involved [Wat08]. There have also been works on constant size CP-ABE schemes. A good number of the constant size cipher text schemes are applicable only to some restricted access structures that use only AND gates [ZH10, EMN+09]; and those that support threshold and suitable only in the case where the predicate has a single gate(threshold or otherwise). This motivates us to analyze the more expressive, multi-level threshold CP-ABE whose cipher text-size is independent of the number of attributes.

Bilinear Pairing

Let G_1, G_2 be additive groups and G_T a multiplicative group, all of prime order p. Let $P \in G_1, Q \in G_2$ be generators of G_1 and G_2 respectively.
A pairing is a map: $e : G_1 \times G_2 \to G_T$
for which the following holds:
Bilinearity: $\forall a, b \in \mathbb{Z}_p^* : \ e\left(P^a, Q^b\right) = e\left(P, Q\right)^{ab}$
Non-degeneracy: $e\left(P, Q\right) \neq 1$
For practical purposes, e has to be computable in an efficient manner.

HARDNESS ASSUMPTIONS

Computational Diffie-Hellman Assumption

The CDH assumption is related to the discrete logarithm assumption, which holds that computing the discrete logarithm of a value base a generator g is hard. If taking discrete logs in $\mathbb{G}$ were easy, then the CDH assumption would be false: given

$$(g, g^a, g^b),$$

one could efficiently compute g^{ab} in the following way:

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

- compute a by taking the discrete log of g^a to base g;
- compute g^{ab} by exponentiation: $g^{ab} = (g^b)^a$;

5.2 Decisional Diffie-Hellman Assumption

Consider a (multiplicative) cyclic group G of order q, and with generator g. The DDH assumption states that, given g^a and g^b for uniformly and independently chosen $a, b \in \mathbb{Z}_q$, the value g^{ab} "looks like" a random element in G.

This intuitive notion is formally stated by saying that the following two probability distributions are computationally indistinguishable (in the security parameter, $n = \log(q)$):

- (g^a, g^b, g^{ab}), where a and b are randomly and independently chosen from $\mathbb{Z}_q$.
- (g^a, g^b, g^c), where a, b, c are randomly and independently chosen from $\mathbb{Z}_q$.

Computational Bilinear Diffie-Hellman Assumption.

Let e: G×G —>GT be an efficiently computable bilinear map, where G has prime order p. The computational bilinear diffie-hellman(CBDH) assumption is said to hold in G if, given elements {P; aP; bP; cP}, then no probabilistic polynomial-time adversary can compute $e(P; P)^{abc}$ with non-negligible advantage, where a,b, c Є R Zp *and generator P Є G are chosen independently and uniformly at random.

Decisional Bilinear Diffie-Hellman Assumption

Let e: G×G —>GT be an efficiently computable bilinear map, where G has prime order p. The decisional bilinear diffie-hellman(DBDH) assumption is said to hold in G if no probabilistic polynomial-time adversary is able to distinguish the tuples c0 = $(g,g^a,g^b, g^c,e(g, g)^{abc})$ and c1 = = $(g,g^a,g^b, g^c,e(g, g)^z)$ with non-negligible advantage, where a, b, c, z $Є_R$ Z^*p and generator g ЄG are chosen independently and uniformly at random.

Decision Linear Assumption

The **Decision Linear (DLIN) assumption** is a computational hardness assumption used in elliptic curve cryptography. In particular, the DLIN assumption is useful in settings where the decisional Diffie–Hellman assumption does not hold (as is often the case in pairing-based cryptography). The Decision Linear assumption was introduced by Boneh, Boyen, and Shacham.

Informally the DLIN assumption states that given (f, g, f^x, g^y), with f, g random group elements and x, y random exponents, it is hard to distinguish (h, h^{x+y}) (for random h) from (h, h') (for independently random h, h').

OBSERVATIONS

Our main observations are that, the specific attack we mention is possible when the following conditions are satisfied:

1. d is a constant and the universe of attributes U contains a large number of elements.
2. The signer possesses lot more than d attributes although (s)he might not have k out of the given set ω^* of attributes.

It is important here to note that the attack was made on the key construction and method of verification, and not on the signature itself. The primary flaw in the key construction is in using the idea of secret shares to distribute the master secret, and at the same time giving each person lot more shares than what is required for recovering the secret. These additional shares - in the form of dummies and other attributes the signer has which are not a part of ω^* - give the signer multiple ways to recover a derivative of the master secret key, which in turn leads to the attacks.

DISCUSSION.

We would like to remark here that, the concept of secret sharing when combined with Waters' signature seems to be vulnerable to the attack we have focused on, even when the number of keys are far fewer. We strongly feel that there does not exist a fix for this key-construct that can resist the mentioned attacks; however this direction is definitely worth exploring.

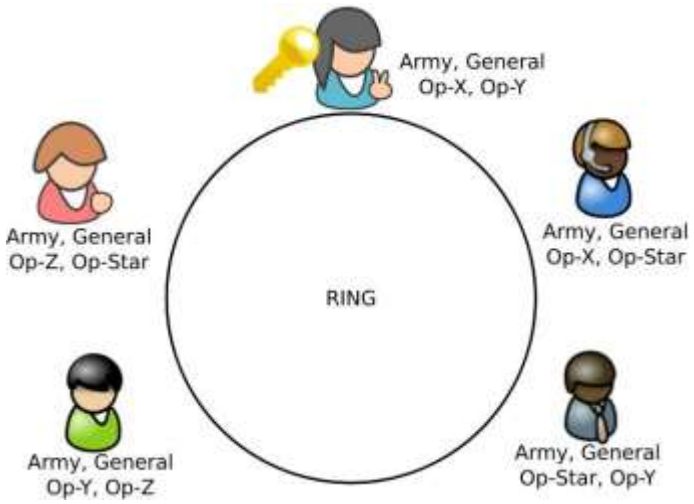

Figure 1: Ring ABS where each alleged member of the ring has 4 attribute

Advantages of the new approach

The proposed threshold scheme has a new property that we can call controlled partial anonymity which is not known to be present (to the best of the our knowl-edge) in any of the previous threshold attribute based signature schemes. This is a feature that would allow the signers to control their anonymity even if the signing policy is not determined by them. We will illustrate this feature with an example. Let us say Alice is signing a document which wants the signer to satisfy a threshold predicate, and she has sufficient attributes to satisfy the predicate. Say, one of the attributes of the signing policy is CIA officer. Now, Alice being a CIA officer among other things wishes to highlight this particular fact in the signature (although it may not be necessary).She can choose attribute sets $\{T_i\}_{i\pounds\{1,\ldots\ldots,n\}}$ with CIA officer being one of the attributes in each of these sets. By doing this, she has control over which of her attributes she wants to reveal. But if Alice does not wish to reveal anything about her credentials except that they satisfy the necessary threshold, then she will have to give all the (n^* to t) possible sets. If on the other-hand, Alice is completely indifferent about revealling all of her attributes, then she can give a signature and include a single subset of attributes. And that set should contain just the exact set of attributes used in the signature inorder to satisfy the given policy. Note that this will also be a constant size signature, since it will have only one T_i and U_i.

The power that this feature gives is that, even if the signing policy is specified by a different authority, the signer can choose to reveal more in the signature than what other schemes would normally allow. In a way, our approach allows the signer control over the signature size and privacy, although he/she may not have had the freedom to set the signing policy. If a signer does not care about privacy, then she can go for a constant size signature. On the other-hand if the size of the signature components is immaterial, then signer can choose to get complete privacy by choosing all the subsets of attributes satisfying the policy to be a part of the signature.

We also observe that this scheme can be extended to a multi-level threshold attribute based signature if each attribute is present only once in the predicate.

Conclusions and indication for Future Work

We wrap up our analysis on attribute-based cryptosystems in this chapter. We will early recap our effort on size dynamic attribute based schemes and coeval some of the objections in this area mannerism. We will then frequently visit the security of ABS schemes and draft our assumptions. We present some interesting directions for future work in the area of threshold attribute-based signatures with particular focus on our new approach. We also give some

intuitions for potential solutions to some of the problems we pose. Finally we'll end this chapter by summarizing our work and present the potential this field has in the emerging computing world.

REFERENCES

1. Xavier Boyen. Mesh signatures. In Proceedings of the 26th annual international conference on Advances in Cryptology, EUROCRYPT '07, pages 210–227, Berlin, Heidelberg, 2007. Springer-Verlag.
2. Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In ACM Conference on Computer and Communications Security, pages 168–177, 2004.
3. John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334, 2007.
4. Jan Camenisch. Efficient and generalized group signatures. In Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques, EUROCRYPT'97, pages 465–479, Berlin, Heidelberg, 1997. Springer-Verlag.
5. Ling Cheung and Calvin Newport. Provably secure ciphertext policy abe. In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 456–465, New York, NY, USA, 2007. ACM.
6. Sherman S. M. Chow, S. M. Yiu, and Lucas C. K. Hui. Efficient iden-tity based ring signature. In Applied Crypto and Network Security - ACNS 2005, LNCS 3531, pages 499–512. Springer, 2005.