A Survey Of Attribute-based Encryption Schemes

Qxx

***Abstract*—The abstract goes here.**

***Index Terms*—The keywords goes here[1].**

I. INTRODUCTION

Attribute-based encryption(ABE) play an important role in encryption scheme of cloud such us[**?**],[**?**],[**?**],[**?**],[**?**] due to that ABE is not only powerful mechanism for protecting the confidentiality of stored and transmitted information inheriting traditional public-key encryption but also achieves the stride from one-to-one model from previous encryption to one-to-many[**?**],and specifically implementing access control and supporting storing in untrusted storage server are the reasons for its achieving.Additionally,ABE has following concrete advantages:

1) High Efficiency: :The cost of encryption and decryption is only related with the length of ciphertext and the number of attributes,and has nothing to do with the number of users;

2) Dynamic: :decryption can be completed by user only when the attributes satisfy the policy,and has nothing to do with the time when the user join this systems.

3) Flexibility: :ABE supports various access structure such us threshold policy and boolean format.

4) Privacy: :when data owner encrypt,he or she has no need to know the specific identities of individuals who will authorised decrypt[**?**].

ABE is actually an extension of identified based encryption(IBE) and it can regard as a special IBE that multiply identities which meet a specific constraint can decrypt the ciphertext.In ABE,that constraint is just the access policy,and user can decrypt only when attributes satisfy the policy.For integrity,there is a simple division,which is only helpful on the application context and make little sense for the more heuristic research on ABE after it has formed,of ABE into ciphertext-policy attribute-Based encryption(CP-ABE) and key-policy attribute-Based encryption(KP-ABE).For CP-ABE,user keys are associated with sets of attributes,whereas ciphertexts are associated with policies,and for KP-ABE,the case is the contrary.

With the development of heuristic research on ABE,more and more ABE variants has been growing.However,there has been no integrated overview published that should not just concludes most of topics of ABE but also figure out the logical and clear clues or veins of development of ABE from pre-birth to now.[**?**]does the survey on ABE of access control,but just enumerate CP-ABE,KP-ABE,ABE Scheme with Non-Monotonic Access Structures,and Hierarchical ABE so from this article we can't find out the relationship among those schemes.From the aspect of difficulties of ABE,[**?**] analyzes the access structure,attribute revocation,key-abuse problem and multi-authority scheme,but those issues don't contain all of that in ABE.[**?**] points out the direction of development on concrete topics of ABE,however there is also no clear hierarchy of ABE schemes.

this is thanks

A. Motivation And Contributions

When everything occurs to us,the ultimate questions of which we would like to know the answer are always about past,now,and future.Now those happen to ABE.Detailedly,the three questions are:

- Where does ABE come from?
- Whats the essence of ABE?and how is it going?
- where will ABE go?

Our motivation is finding out the answers of these three questions.

As for our contributions,the first is figuring out the logical and clear clues of the development of ABE based on present ABE schemes,and the clues are helpful to that researchers get clear and integrated general view of ABE and can obtain some possible directions of exploration of ABE.Then we propose a taxonomy which contains all or most ABE schemes,and the taxonomy can be used by researchers to answer many important questions such us:

- what's the reasons for emergences of those kinds of ABE schemes?
- what's the relationship among ABE schemes?
- what's the more possible work along developed directions of ABE?

Additionally,this paper explores the design philosophy of classical ABE schemes,which can be a reference for researchers when he or she wants to find the principles of some schemes.After all above,we propose some foresight about the future of ABE.

B. Organization

In this paper,we survey some attribute-based encryption schemes,and propose clues and a taxonomy of the development of present ABE schemes and give some opinions about the future directions of ABE. The organization of the paper is organized as follows.In section 2,we review the key nodes of development of ABE,then draw its clues.Syntax of ABE schemes is introduced in section 3.In section 4,we consider the design philosophy of two classical ABE schemes.Access control,the most essential technology in ABE,are catched from most present ABE schemes in section 5.We propose a taxonomy of the development of present ABE schemes in section 6,and this taxonomy implies all or most direction along which ABE has developed.In section 6,we do some

comparisons,each comparison is made among schemes in a same category,and these targets,used by comparison,are just these purposes of schemes in the same category.extension in section 7 is about several interdiscipline of cryptography that hasn't been ripe so far,but that has the possibility to be a part of ABE as mature technologies used.

II. CLUES ON THE DEVELOPMENT OF ABE

In this section,we attempt to survey the existing literature and constructions for ABE schemes over the period 2005-2016 from the aspects of three trunk clues,function,efficiency and security.Then we explain how do we arrive at more logical and clear clues on the development of ABE.

A. the development Of ABE

1) the birth of ABE: Attribute-based encryption is firstly mentioned in[**?**],this idea originates from Hierarchical identity-based encryption schemes[**?**]and the schemes of [**?**] can be achieved due to the inspiration from threshold secret share technology by[**?**].After that,researchers pay much attention on general policy,which ties data owner with data user as a series of formalized constraint,compared with traditional point-to-point constraint(corresponding the privilege management infrastructure technology).So the access control technology is recalled,and ABE has perfectly formed just when this technology and the attribute as object of authorization are used in public-key scheme.When access control technology occurs to ABE,there are two types of models realized,i.e KP-ABE and CP-ABE.[**?**] is the first KP-ABE scheme and [**?**] is the first CP-ABE,so these two schemes proposed sign the perfect formation of ABE.After then,apart from research on more practical access policies,which are surveyed in section 5,the directions of development of ABE can be summarized those:fuction,efficiency and security.

2) function: survey on Multi-authority and Distributed ABE

survey on proxy re-encryption.

3) efficiency: survey on general technology

survey on specific technology

4) security: survey on theoretical security

survey on applied security

B. clues on the development of ABE

The surveys above clearly display the development of ABE due to the three main clues obtained.The reveal of how we find out more detail clues is shown in this subsection.In brief,focus on the purposes and process of all or most present ABE schemes.The detailed procedures are explained as followings.Firstly,pay our attention to the all parts of process on original ABE schemes i.e[**?**] and [**?**],and draw a picture containing three parts:components of specific scheme,participants and operations of process of these schemes,shown in Fig. **??**.We note that operations are actually not independent to components and participants,this division is just for discerning more clearly,and that mentioned clues above don't conclude access structure,so this method can also be used in other public-key encryption schemes.Secondly,we ligature each two parts which there are some responding relationships between,then the lines are labeled with relationships.For example,there is an "authorization" between "CA" and "user",so we line this two parts and label with "authorization".After finished lines of each existing relations,a new issue of ABE is added in this kind figure in the way concentrate attention to the purpose and the process.For example,constant ciphertext issue of ABE can be add as Fig. **??**,and proxy re-encryption ABE can be added as Fig. **??**.Finally,after surveyed the most issues of ABE,we obtain the Fig. **??**.All lines in Fig. **??** is called as detailed clues,We can clearly view the motivations or main process of present ABE schemes using our clues,so that a overview of ABE tend to be crystallized and visual.Besides,researchers also can get some possible directions of exploration of ABE though using this kind way to line parts which haven't lined in Fig. **??**.For example,we can construct called common constraint ABE(CCABE) through lining between plaintext and encryption.In CCABE,universal attributes is defined by some trusted authority.These attributes are divided into some groups,and each group contains arbitrary number attributes.Then according to the distributed attribute group every data owner holds,every owner in this system can define its own access policy which it wants user's attributes to satisfy in order to decrypt.And only when users attributes satisfy all or some other rules(such us threshold policy)from data owners' access policy.

III. SYNTAX OF ABE SCHEMES

Syntax of ABE Schemes goes here,and don't contain security.

IV. DESIGN PHILOSOPHY OF CLASSICAL ABE SCHEME

some introduction goes here

A. KP-ABE

Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data Vipul Goyal Omkant Pandeyy Amit Sahaiz Brent Waters in Proc of Acmccs- 2006

B. CP-ABE

Ciphertext-Policy Attribute-Based Encryption John Bethencourt Amit Sahai Brent Waters in 2007 IEEE Symposium on Security and Privacy 2007

V. ACCESS CONTROL IN ABE

some introduction

A. Access Structure

some introduction

1) Monotonictity: Monotonictity goes here

2) Expressive Formula: expressive formula goes here

B. Extension

hierarchy ABE introduction goes here

VI. Research On The Developed Direction Of ABE

some introduction

A. Function

some introduction

1) Proxy Re-encryption: proxy re-encryption ABE goes here

2) Multi-authority: multi-authority ABE and distributed ABE in here

B. Efficiency

some introduction

1) General Technology: outsource and constant ciphertext in ABE goes here

2) Specific Technology: Some examples of Specific Technology in here

C. Security

some introduction

1) Theoretical security: some introduction and security model goes here

2) Applied security: some introduction and collusion problem,abuse key problem,hidden-policy problem,revocation problem go here

VII. Comparison

comparison among some goes here

VIII. Extension

extension goes here. find some interdiscipline topics such as combined with searchable scheme.

IX. Conclusion

The conclusion goes here.

X. Future Of ABE

The future goes here.

References

[1] J. Donald and M. Martonosi, "Techniques for multicore thermal management: Classification and new exploration," in *Proc. Int. Symp. on Computer Architecture (ISCA)*, June 2006, pp. 78–88.

PLACE PHOTO HERE

aaa Biography text here.

PLACE PHOTO HERE

bbb Biography text here.

PLACE PHOTO HERE

ccc Biography text here.