A Survey Of Attribute-based Encryption Schemes

Qxx

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

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

I. INTRODUCTION

introduction goes here.

II. DEFINITION

introduction of framework and security model.

A. Framework Of ABE

Framework Of ABE goes here.

B. Security Model

introduction of security model.

1) Random Oracle And standard model: In a random oracle model, there exists an oracle which can be thought as a box. When taking a binary string as input, it will return a binary string as output. And everyone can not know or predict the internal workings of the oracle. A?random oracle?is an?oracle that is a theoretical?black box. When a query is performed, it responds?with a random?response which is chosen?uniformly?from its output domain. In detail, a random oracle can be thought as a perfect hash function:

1.For the same input, the output of the function must be the same.

2.The output of the function can be calculated in polynomial time.

3.The function is a one-way function.

4.The output of the function is uniformly distributed in the value of space and have the property of anti-collision.

The proof under this model needs to make a assumption that the adversary can not exploit the weakness of the hash function. In reality, however, the hash function is deterministic and its output can not be completely random and evenly distributed. Therefore, some schemes are not safe after using a real hash function instead of random oracle. Nevertheless, the security proof based on the random oracle model can meet the security requirements except for the hash function. Comparing with the standard model, the security proof based on random oracle model is easier to realize and the schemes based random oracle model usually have higher efficiency. So, most of encryption?schemes include attribute based encryption adopt random oracle model to construct their schemes.

In a standard model, the adversary is only limited by amount of time and computational power available. In other words, the formal security proof in the standard only relies on the difficulty provided by the one-way trap function (standard number theory hypothesis, such as the calculation of discrete logarithm) and the irreversibility of a one-way hash function, and some other properties of the hash function that can be implemented in the real world. Comparing to the random oracle model, standard model has higher security, so there are many researchers researching on the encryption schemes based on the standard model.In 1998, Cramer and Shoup [?] proposed the first efficient public key cryptography scheme that can be proved to be secure under the standard model. And the difficulty assumption in this paper is the Decisional Diffie-Hellman Assumption. In the field of attribute-based encryption research, there also exits some schemes based on the standard model[?][?].

2) Select Security And Full Security: Select Security And Full Security goes here.

3) CPA and CCA: CPA and CCA goes here.

III. DESIGN PHILOSOPHY OF CLASSICAL ABE SCHEME

some introduction goes here.

A. Access Structure

some introduction goes here.

1) Monotonicity: Monotonicity goes here.

2) Boolean Formula: Boolean Formula goes here.

B. Design philosophy of classical ABE scheme

some introduction goes here.

1) KP-ABE: analyze article: *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data* Vipul Goyal Omkant Pandeyy Amit Sahaiz Brent Waters in Proc of Acmccs- 2006

2) CP-ABE: analyze article: *Ciphertext-Policy Attribute-Based Encryption* John Bethencourt Amit Sahai Brent Waters in 2007 IEEE Symposium on Security and Privacy 2007

IV. STATE-OF-THE-ART OF THE ABE

A. 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

this is thanks

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.

B. efficiency

1:Survey on original ABE,and some efficient technology such us constant ciphertext and constant cost in decryption.

2:You describe these articles in time sequence.

3:And also need a table to compare efficiency among articles mentioned by you.

C. security

1:Survey on original ABE,and some articles,which have promoted in security,based on original ABE.

2:You describe these articles in time sequence.

3:Also need a table to compare security among articles mentioned by you.

D. function

1:Survey on original ABE,and some articles,which have promoted in function,based on original ABE.

2:You describe these articles in time sequence.

3:Also need a table to compare security among articles mentioned by you if possible.

V. Extension

some introduction goes here.

A. Key-abuse Problem

Key-abuse Problem goes here.

B. Outsource

Key-abuse Problem goes here.

C. Proxy Re-encrypton

Proxy Re-encrypton goes here.

D. Multi-authority And distributed ABE

Multi-authority And distributed ABE goes here.

E. Revocation

Revocation goes here.

F. hide-policy ABE

hide-policy ABE goes here.

VI. Related work

With the exploration on ABE from aspects of efficiency, security and function, more and more ABE variants has been growing. However, there has been no integrated overview published that contains not only various ABE schemes, but also analysis of design philosophy. [?] does the survey on ABE of access control, but just enumerate CP-ABE, KP-ABE, ABE Scheme with Non-Monotonic Access Structures and so on, so that we cannot obtain the clear relationship among those schemes from the paper, and also Boolean formula of LSSS and circuit do not be mentioned. From the standpoint of difficulties in ABE, [?] describes the access structure, attribute revocation, key-abuse problem and multi-authority scheme, but we cannot find the Non-Monotonic Access Structures and Boolean formula of circuit in the part of access structure from this article. Besides, the ABE variants such as proxy re-encryption, outsource ABE are not concluded. [?] points out the direction of development on hot topics of ABE, However the survey on the most essential access policy is not embodied.

VII. Future work

Future work goes here.

VIII. Conclusion

The conclusion goes here.

PLACE
PHOTO
HERE

aaa Biography text here.

PLACE
PHOTO
HERE

bbb Biography text here.

PLACE
PHOTO
HERE

ccc Biography text here.