A Survey Of Attribute-based Encryption Schemes

Qxx

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

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

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: Random Oracle And standard model goes here.

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

this is thanks

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 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.

VI. Related work

Related work goes here.

VII. Future work

Future work goes here.

VIII. Conclusion

The conclusion 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.