A Study of Identity Based Encryption Systems

Samuel Petit
3rd Year Integrated Computer Science student at Trinity College Dublin, the University of Dublin
Email: petits@tcd.ie

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

I. Introduction

Will be studying IBE. A type of Asymmetric paired keys encryption system. Charcterised with the fact that one of its keys identifies the recipient (email...phone no).

Makes a lot of sense to compare with classical systems currently in use such as RSA.

So let's compare both systems and try to explain why IBE is not as popular

A. What is public key encryption ?

Explain public / asymmetric key paired encryption

1) How it works: explain concepts of public key encryption

B. Different ways it is implemented

explain different implementations

1) Requirements for public key algorithms (key gen, encrypt and decrypt): explain Requirements here

2) Explain how RSA works: explain RSA systems - a typical implementation

3) Explain how IBE works: explain IBE systems

C. Math Systems at the core of Public Key Encryption

Explain that at the core of public key encryption, underlies many important mathematical concepts.

1) Extended euclidean algo to find gcd, coefficients: euclidean algo

2) Fermat's little theorem: fermats little thm, its place in public crypto

3) Prime numbers: prime numbers at the core of crypto

4) Discrete logarithms: discrete log problem

5) Chinese remainder theorem: chinese remainded thm at the core of decryption (or encryption)

6) Square and multiply: square and multiply to compute large exponents

D. What is identity based encryption ?

Explain what is exactly IBE now that we know more about public key encryption

1) IBE typical implementation: how is an IBE system implemented

2) What are its advantages and flaw?: pros and cons of IBE

E. IBE vs RSA

Compare the two

1) Attacks on IBE Public key systems: Go through possible attacks on Public key systems

2) Are these attacks all possible on IBE? is it better or worse with IBE?: go through how IBE protects from attacks differently than rsa systems

3) which is most safe?: expalin which system is safest

II. Conclusion

The conclusion goes here.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.