Optimized Identity-based Encryption From Bilinear Pairing For Lightweight Devices

Abstract

- Lightweight devices such as smart cards and RFID tags have a very limited hardware resource, which could be too weak to cope with asymmetric-key cryptography.
- It would be desirable if the cryptographic algorithm could be optimized in order to better use hardware resources.
- In this paper, we demonstrate how identity-based encryption algorithms from bilinear pairing can be optimized so that hardware resources can be saved.

- We notice that the identity-based encryption algorithms from bilinear pairing in the literature must perform both elliptic curve group operations and multiplicative group operations, which consume a lot of hardware resources.
- We manage to eliminate the need of multiplicative group operations for encryption. This is a significant discovery since the hardware structure can be simplified for implementing pairing-based cryptography.

Existing System

- Identity-based encryption (IBE) has attracted a lot of attention since Boneh and Franklin proposed the first fully secure IBE.
- In comparison with public-key encryption (PKE), the encryption of IBE exhibits nice features that an encryptor does not need to verify the authenticity of public keys, and the encryption can be conducted prior to the setup of public keys.
- Suppose sensitive data on lightweight devices will be encrypted via either PKE or IBE, and then sent over an insecure channel to a receiver.

- We found IBE is the only candidate encryption that can be adopted.
- This is because a public key of PKE must be checked to find whether it is expired or not prior to encryption. The expiry verification is based on certificate system which requires the device to knowthe current time.

Disadvantages

- Applying PKC to lightweight devices is always challenging due to the constraint of computation and hardware capacity

Proposed System

- In this paper, we propose a novel identity-based encryption scheme, which is provably secure in the random oracle model.
- For the optimization of hard-ware implementation, our encryption algorithm only requires the single group G1 for all group operations of encryption, while exponentiations in GT, pairing computations and group hashing operations are no longer required.
- In comparison with other pairing-based IBE schemes, our encryption algorithm saves the computation of exponentiations in GT

Advantages

- Our IBE scheme is useful for those applications in which lightweight devices need to implement the IBE encryption algorithm with a less hardware cost.

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net /java

Conclusion

- We have presented a novel identity-based encryp-tion scheme from bilinear pairings, aiming to re-duce the hardware cost of lightweight resource. It is provably secure against chosen-ciphertext attacks under the q-DDSDH assumption in the random oraclemodel. In comparison with traditional pairing-based
- IBE constructions, the encryption algorithm of our IBE scheme only requires group operations in G1
- Theother primitives associated with the pairing group(G1; G2; GT; e), such as exponentiations in GT and pairing computations are no longer required in the encryption part of scheme.