Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-12, (2017)
ISSN (O): 2454-1362

The Survey of Optimized Identity-Based Encryption from Bilinear Pairing

Miss. Nilima Balode D.[1], Mr. Gade Suraj A.[2], Miss. Shinde Maya R.[3], Prof. Kore K.S.[4]

[1, 2, 3,] Student, BE Computer, SPCOE, Department Of Computer Engineering, Dumbarwadi[1]
[4]Assistant Professor, SPCOE, Head of Computer Engineering Department, Dumbarwadi[2]

ARTICLE INFO

Received 25 November 2017
Accepted 9 December 2017
Published 14 December 2017

ABSTRACT

Since inception of internet security and privacy of are the critical issues faced by researchers. Thus researchers came up with use of encryption / decryption for data security, in which public-key cryptography is most celebrated type of cryptography. Key sizes also play vital role in modern cryptographic solution and thus pairing-based cryptography is preferred over other cryptographic solutions. Pairing based cryptography works on interesting properties of curves. And Wireless devices also 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 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 hard- ware 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.

Keywords*- Security, ABE, CP-ABE, PKC, IBE, Encryption algorithm*

1. Introduction

Since the development of computer the security of data came into existence and whole new branch is devoted for research into cryptography. Securing a data is critical for any business ranging from small firm or large organizations [04] [12]. Cryptography uses strong mathematics to convert data into some non-sense form called as 'cipher text' and anyone having valid key can decrypt the 'cipher text' [12].

These types of algorithms are useful in low bandwidth channels or devices with low processing powers. Bilinear pairing is used for All public-key cryptosystems can trace their roots to the Diffie-Hellman key exchange protocol [05] which uses cyclic groups with particular properties or RSA which works with acyclic groups. Cryptographic systems obtains their strength from mathematical properties of pairing which are efficient to calculate from one side and reverse engineering them is hard problem. Using interesting properties from bilinear maps various researchers developed different types of pairing based cryptographic systems. All of the pairing based cryptographic solutions exploits mapping between Gap group denoted as G1 and second group denoted as G2 [03].

In this paper detailed survey of pairing based cryptography is given, section II covers mathematics behind bilinear pairing and pairing based cryptography. Section III covers previous researches on pairing based cryptosystems, section IV covers how to build cryptosystem using pairing based cryptosystem and section V acknowledgment.

Goals and Objective

- Our encryption algorithm only requires the single group G1 for all group operations of encryption.
- In comparison with other pairing-based IBE schemes, our encryption algorithm saves the computation of exponentiations in GT.

2. Problem Statement

- The drawback of IBE is overhead computation at private key generator (PKG) during Revocation.
- Disadvantages of Asymmetric Encryption is Key Length, Encryption speed, Key management, Key Validation.

3. Mathematical Background

3.1. Cyclic Groups

A group G is called cyclic if G can be generated by a single element g called a generator (G can have many generators). All cyclic groups are Abelian (A group G is called Abelian iff elements commute i.e. AB =BA for all elements A and B) [02]. It is denoted as,

$$G = \langle g \rangle = \{ g^n \mid n \text{ is an integer } \}$$

gi gj = gj gi = g i+j = gj+i

As every cryptographic system is built around discrete logarithmic problem [11], given as

Discrete Log Problem. Given g, gx, compute x.

Computational Diffie-Hellman Problem. Given g, gx, gy, compute gxy.

Decisional Diffie-Hellman Problem. Given g, gx, gy, gz, determine if x.y = z.

DLP is believed to be intractable for certain (carefully chosen groups) of finite field, and this leads to the security of Diffie-Hellman protocol.

3.2. Group Generators

A set of generators g1,...,gn is a set of group elements such that repeated group operation (addition, multiplication) or inverse of gn on the generators on themselves is capable of producing all the elements in the group [01]. Typically G is elliptic curve, elliptic curve defined by y2=x3+1 over finite field Fp, it is super singular curve of abelian varieties having dimension 1.

3.3. Bilinear Maps

Bilinear maps is the most important part in pairing based cryptography, it gives additional properties to cyclic groups [04]. Initially it was found that these additional properties could be used by an attacker to break cryptosystem, but later it is discovered that it can be used to build new cryptosystem. Mathematically bilinear maps are function combining elements from two vector spaces that yields element in third vector space. Pairing based cryptography uses very complicated math that are non-trival to compute, but they are very secure. Pairing calculations and elliptic curve scaler multiplication are two major operations in pairing based cryptography and these operations dependent on arithmetic over prime fields Fp.

4. Related Work

This chapter covers survey of attribute based encryption, Bilinear Pairing Based Cryptography and integrity checking systems. It also covers basics of cryptography and elliptic curve cryptography also known as Bilinear pairing based cryptography is absolute choice for designing cryptographic systems. Cryptography is art of hiding data from unintended person. There are two types of cryptographic systems one is 'Symmetric Cryptography' and other one is called as 'Public-Key Cryptography' [08]. Symmetric cryptography uses single key for both encryption and decryption whereas public-key cryptosystems uses two keys that are mathematically linked (public key for encryption and private key for decryption). Symmetric cryptosystems are simple but it requires some secure key-sharing mechanism between two communicating parties. Whereas, public key cryptosystem releases burden of secure sharing of keys [04].

Applications of Pairing based cryptography are given as follows [12],

1. Identity Based Encryption
2. Hierarchical Identity Based Encryption
3. Attribute Based Encryption
4. Identity Based Encryption with Threshold
5. Searchable Encryption
6. Signatures

5. Proposed Work

The architecture of this multi-ABE scheme is shown in figure 3.1. The scheme consist of 4 player's main authority, local authority, intermediate storage node and one or many end user.

The role of each user discussed below,

Main Authorities: It's responsible for generating unique keys for end user by collaborating with local authorities. This guarantees collision will not take place between user attribute keys.

Authority: Local authorities are like part of organization that is responsible for managing its employees. It defines access policies and responsible for getting user in main flow.

Storage node: Node that temporarily stores data until it reaches to receiver in DTN environment. Storage node erases the data based on expiration time set for the data by data owner and it also helps users to verify the integrity of message.

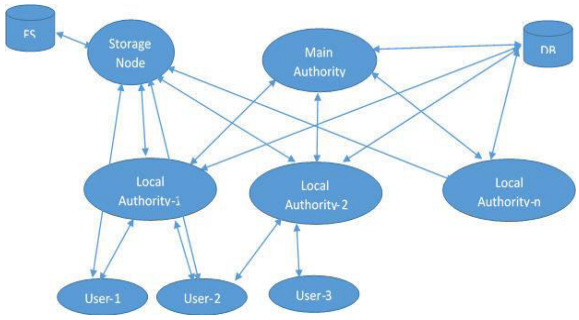

Figure 1. Example figure.

***User*:** Defines access structure tree for data to be shared and shares the data. There is no cleaver way by which user will know how many authorities are there, also how central authority will know how many local authorities are there. By getting all this initial information then only system will functions correctly.

Public Parameter Setup: During system setup trusted third party chooses a bilinear group G0 of prime order p with generator g and a hash function H. The public parameter is given by (G0, g, H).

Main Authority: Main authority chooses a random exponent βƐZp. It sets h = gβ. The public key is *h* and private key *β*.

Local Authority: Each local authority A*i* chooses αi from Zp. The public key is set to e (g, g) α and private key is α.

Key Generation: User keys in CP-ABE schemes are composed two components personal key that uniquely identifies user and prevents collision attacks and multiple attribute keys that defines access policies. The personalized key is alone generated by CA.
The intuitive way of sharing the information about user's and number of local authorities is to use single database. It is assumed that the database is managed independently by third party and is secure from unintended accesses.

Personalized key Generation: Main authenticates user ui and from each local authority Ai € m, then main authority chooses σi where i € m and finally it computes where ϒi is personalized key of user ui.

Attribute Key Generation: To generate attribute keys for user ui, main authority engages local authorities in two phase communication protocol. It first establishes component.

Encoding Message: When data owner wants share data with set of user's, then data owner defines access structure using access tree *T* and encrypts message.

Decoding Message: The message is broadcasted to all users with matching access structure and user can view the data in their dashboard. User decrypts the encoded message with its secret key SK.

6. Conclusion

Identity-based encryption scheme from bilinear pairings, aiming to reduce the hardware cost of lightweight resource. It is provably secure against chosen-ciphertext attacks under the q-DDSDH assumption in the random oracle model. In comparison with traditional pairing-based IBE constructions, the encryption algorithm of our IBE scheme only requires group operations in G1. The other 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. The implementation result shows that our encryption algorithm saves up to 47 percent memory (27,239 RAM bits) in FPGA implementation. Our IBE scheme is useful for those applications in which lightweight devices need to implement the IBE encryption algorithm with a less hardware cost.

7. Acknowledgements

I would like to thanks to my project guide **Prof**. **Kore K. S.** who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of computer department for their valuable guidance, suggestion and support through the paper work, who has given co-operation for the project with personal attention. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work.

8. References

[1] Fuchun Guo, Yi Mu, "Optimized Identity-Based Encryption from Bilinear Pairing for Lightweight Devices",in Proc. IEEE TRANSACTIONS ON DEPEND-ABLE AND SECURE COMPUTING, VOL. 14, NO. 2, MARCH/APRIL 2017.

[2] Atkin and F. Morain, "Elliptic curves and primality proving," Mathematics of Computation, vol. 19, 1993.

[3] P. Barreto, S. Galbraith, C. and M. Scott, "E_cient pairing computation on super singular abelian varieties," Designs, Codes and Cryptography, 2007.

[4] P. Barreto, H. Kim, B. Lynn and M. Scott, “Efficient algorithms for pairing- based cryptosystems," Advances in Cryptology CRYPTO 2002, Lecture Notes in Computer Science, 2002.

[5] Dan Boneh, “The decisional diffie-hellman problem," In Third Algorithmic Number Theory Symposium, pages 4863. Springer-Verlag, 1998.

[6] Whitfield Diffie and Martin E. Hellman, “new directions in cryptography,” IEEE Transactions on Information Theory, IT-22(6):644654, 1976.

[7] Adi Shamir, ‘Identity-based cryptosystems and signature schemes," In Crypto 84, Springer, 1985.

[8] W. Diffie and M. Hellman, “New directions in cryptography," IEEE Transactions on Information Theory, 1976.

[9] S. Galbraith,I. Blake, G. Seroussi and N. Smart , “Advances in Elliptic Curve Cryptography," Cambridge University Press , 2005.

[10] S. Galbraith, K. Harrison and D. Soldera, \ IEEE "Implementing the Tate pairing"," Algorithmic Number Theory: 5th International Symposium, 2002.