SURVEY OF PAIRING BASED CRYPTOSYSTEM

Mr. Walunj Pratap, Assistant Prof. Kore Bhagawan

[1] *PG Student, Dept. Of Computer, SPCOE, Maharastra, India*
[2] *Assistant Prof, Dept. Of Computer, SPCOE, Maharastra, India*

ABSTRACT

A Public-key cryptosystems, are the most celebrated contribution of modern cryptography. Pairing-based cryptography is a novel cryptosystems that works around a particular function with interesting properties. This paper contains detailed survey of pairing based crypto system and how they works. These types of cryptosystems are so secure that, if a key size in pairing based cryptosystem uses 256 bit key then to achieve same level of security RSA would require 1250 bits. 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 which uses cyclic groups with particular properties or RSA which works with acyclic groups.

Keyword: *Pairing based cryptography, Bilinear maps, Cyclic groups, Diffie-Hellman Key Exchange Protocol, Public Key Cryptosystem..*

1. INTRODUCTION

Almost every network security analysis is familiar with asymmetric cryptosystems which put given roadmap to modern cryptographic algorithms [07]. But traditional asymmetric algorithms having some limitations such as their key sizes, security, these factors motivates researchers to design new cryptosystems. Pairing-based cryptography is a novel cryptosystems that works around a particular function with interesting properties [01]. These types of cryptosystems are so secure that, if a key size in pairing based cryptosystem uses 256 bit key then to achieve same level of security RSA would require 1250 bits [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 concludes.

2. MATHEMATICAL BACKGROUND

1.1 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,

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

$$g^i g^j = g^j g^i = g^{i+j} = g^{j+i}$$

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

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

Computational Diffie-Hellman Problem. Given g, g^x, g^y, compute g^{xy}.

Decisional Diffie-Hellman Problem. Given g, g^x, g^y, g^z, 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.

1.2 Group Generators

A set of generators $g^1,...,g^n$ is a set of group elements such that repeated group operation (addition, multiplication) or inverse of g^n 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 $y^2=x^3+1$ over finite field F_p, it is super singular curve of abelian varieties having dimension 1.

1.2 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.

1.3 Vector Spaces

A vector space is collection of vectors which can be added/ multiplied/scaled together. Let V, W, X are three vector spaces over based field F then bilinear map is a function of form [08],

B: V * W -> X

Such that, for any w in W the map,

v – B(v,w)

is a linear map from V to X, and for any v in V the map. In other words, when we hold the first entry of the bilinear map fixed while letting the second entry vary, the result is a linear operator, and similarly for when we hold the second entry fixed.

3. LITERATURE SURVEY

In this section we will consider various attribute based encryption techniques that uses pairing based cryptography. Interestingly pairing based cryptography was initially used to break ECC crypto in 2005, Weil and Tate pairing were used. The idea behind it was reducing the problem of DLP in elliptic curves to DLP over finite fields. Pairing based encryption [13]. In ABE attributes play an important role for generating public key, encrypting data and defining access policies. Using ABE having multiple advantages are they reduce communication overhead and provide fine grained access control [06].

The idea of identity based encryption is brought by Shamir [00], it using user identity to easily calculate public key while user's private key is calculated by trusted authority (Private Key Generator). ID-based cryptosystem is alternative approach for certificate based public key infrastructure (PKI). Earlier bilinear maps uses Weil and Tate pairing for cryptography. Weil pairing can also be used for three party one round key agreement protocol, it is proved by Joux [09]. Public key cryptography become efficient using pairing based cryptography as receiver public key can be easily derived from his identity thus solving public key distribution problem.

BLS [04] scheme is the most efficient scheme, it has shortest length compared to others signature schemes. BLS allows user to verify singer is authentic. These signatures are elements over elliptic curve. A signature consist of key generation, singing and verification functions. The key generation algorithm selects x from interval [0, r-1], where x is private key and public key is g^x. Singing involves hashing the message bits m using some hash function such as h=H(m) and computing a signature sigma = h^x. Verification involves given a sigma and g^x, verify $e(\sigma,g)=e(H(m),g^x)$. BLS is short and simple.

Weil pairing [09] can be efficiently computed using Victor Miller algorithm. Weil pairing is pairing on points of order dividing n of elliptic curve E taking values in nth roots of unity. Suppose α is an endomorphism, and g is a

rational function. Then a natural construct is to compose g and α, i.e. g. α. For example, if α is translation by a point T, then g·α(P)=g(P+T). The map α also induces a map on the divisors α∗:Div(E)→Div(E) that takes the divisor of g to the divisor of g·α. For example, if α is translation by T, then α∗ takes a divisor ∑mP⟨P⟩ to ∑mP⟨P−T⟩. Then the function g^T in the Weil pairing may be defined as a function such that

$$\langle g^T \rangle = [m]_*(\langle T \rangle - \langle O \rangle)$$

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

3. CONCLUSION

Pairing based cryptography is very hot topic and is constantly growing at fast rate. In this paper we surveyed use of bilinear pairing for building cryptographic protocols that are far more efficient and secure than traditional techniques. For pairing based cryptography some researchers used hyper-elliptic curves, but hyper-elliptic curves are not efficient than elliptic curves. Hyper-elliptic curves are only suitable for protocols with few pairing based computations and higher number of operations on G1, as in hyper-elliptic curves we get speed up G_1 operations. Some questions need to considered while developing pairing based computations, like are there pairing friendly curves for efficient and secure computations and it is easy to construct equations for such curves. Whether user have fine grained control over such parameters. Finally super singular curves are pairing friendly curves.

4. REFERENCES

[1]. Atkin and F. Morain, "Elliptic curves and primality proving", Mathematics of Computation, 1993.
[2]. P. Barreto, S. Galbraith, C. and M. Scott, "Efficient pairing computation on super singular abelian varieties", Designs, Codes and Cryptography, 2007.
[3]. 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.
[4]. Dan Boneh. The decisional diffie-hellman problem. In Third Algorithmic Number Theory Symposium, pages 48–63. Springer-Verlag, 1998.
[5]. Whitfield Diffie and Martin E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644–654, 1976.
[6]. Adi Shamir. Identity-based cryptosystems and signature schemes. In Crypto '84, LNCS Vol. 196, pages 47–53. Springer, 1985.
[7]. W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, 22 (1976), 644–654.
[8]. S. Galbraith, "Pairings", Ch. IX of I. Blake, G. Seroussi and N. Smart, eds., Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005.
[9]. S. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", Algorithmic Number Theory: 5th International Symposium, ANTS-V, Lecture Notes in Computer Science, 2369 (2002), 324–337.
[10]. I. Niven, H. Zuckerman and H. Montgomery, An Introduction to the Theory of Numbers, 5th edition, Wiley, 1991.
[11]. J. Silverman, The Arithmetic of Elliptic Curves, Springer, 1986.
[12]. T. Okamoto and D. Pointcheval. The gap-problems: A new class of problems for the security of cryptographic schemes. In Public Key Cryptography, pages 104–118, 2001.
[13]. R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. Lecture Notes in Computer Science, 2248:552+, 2001.
[14]. F. Brezing and A. Weng. Elliptic curves suitable for pairing-based cryptography. http://eprint.iacr.org/2003/143.