International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 1 Issue: 7
ISSN: 2454-4248
12 – 14

Modified Elliptic Curve Discrete Log Problem: A New One-Way Function and its Cryptanalysis

N Anil Kumar, Chakravarthy
Mahatma Gandhi Institute of Technology,Gandipet, Hyderabad, Telangana, India.
Email: *anil230@gmail.com*

Abstract: In this paper we explain the concept of the one-way functions and their use in cryptography. We explain in detail the use of one-way function like Integer factorization and it use in RSA algorithm.
We describe its cryptanalysis. We explain the discrete log problem and its cryptanalysis. We introduce a novel one-way function called Modified Elliptic Curve discrete log problem (MECDLP). We explain its cryptanalysis also.

*****

I. INTRODUCTION

A one-way function f is one-way function if f is easy to evaluate and difficult to invert. An algorithm is said to be easy if its time complexity is expressed as polynomial function. An algorithm is said to be hard if its time complexity cannot be expressed as polynomial function.
Some one-way function are functions are

1. Integer factorization problem
2. The discrete log problem

In the section 2 we describe about Integer factorization problem. In section 3 we describe about the discrete log problem. In section 4 we introduce a novel one-way function MECD

II. INTEGER FACTORIZATION

RSA invented by Rivest, Shamir and Adleman [2]is the first public key cryptosystem. RSA can be used for encryption/decryption, digital signing and key exchange. The security of the RSA cryptosystem is based on the hardness of integer factorization problem. We briefly describe the RSA algorithm.
Choose two large prime number p,q
We compute n=p q, Compute Ø(n)=(p-1)(q-1)
Choose e coprime with Ø(n)
Compute d such that ed ☰1 mod Ø(n)
Let m be a message. Encryption of the message is c=m^e mod n; where c is ciphertext.
The decryption of the message is c^d mod n which gives the message m.
p, q, Ø(n) are deleted after calculations are done.
e, and n are public parameters. d is the private parameter. For signing we compute the hash of the message and sign on the hash.

2.1 Attacks on RSA [3]

To break the cryptosystem we have to find the private key d from the public parameters. If we know Ø(n) we can find d easily from the equation ed ☰1 mod Ø(n). If we know p and q we can calculate Ø(n) easily. So now the problem is to find p and q from the given n i.e factoring the given n. Algorithms for factoring can be classified into two broad categories.

1. Group order methods
2. Fermat's method of factorization

2.1.1 Group order methods:

The main algorithms in this category are pollard p-1 method, pollard rho method, elliptic curve factorization method.

Pollard p-1 method

We select a large number take the product of prime numbers below that number. Let us say the number be M. Randomly pick a number r coprime to n. Compute f=gcd(r^M-1, n);
If f is not a trivial factor of n return f else repeat the same process.

Pollard rho method

We select a random nonlinear function g(x) mod n. Get g1=g(x) mod n, g2=g(g(x)) mod n and so on. We compute gcd(g1-g2,n) and check whether got a non trivial factor or not. If we get a non trivial factor we are done, else we need to repeat for gcd(g_i-g_2i,n).

III. DISCRETE LOG PROBLEM [6]

An ordinary logarithm log_g (b) is a solution of the equation g^x =b over the real or complex
numbers. Similarly, if g and b are elements of a finite cyclic group G then a solution x of
the equation g^x = b is called a Discrete Logarithm Problem (DLP) in group G.
We define discrete log problem over Z_p^*, let g be the generator of the group Z_p^*
We select a number x and compute g^x mod p let it be b. Given g,x and p it is easy to calculate b, but given g, b, p it is difficult to calculate x. This is a one way function. Many cryptosystems are designed based on this hard problem.

 ISSN: 2454-4248
12 – 14

The cryptanalysis for this problem is to find the x given g, b and p. Popular algorithm are

1. Shanks algorithm
2. Pohlig-Hellman algorithm
3. Pollard's rho method
4. Pollard lambda method
5. Index calculus method

3.1 Shanks algorithm

This is also called baby step giant step algorithm. The equation is g^x=b mod p. We write x as s*i+t; where s=ceil (sqrt(p)); we vary i,t from 0 to s.

g^(s*i+t)=b mod p

g^(s*i) g^t =b mod p

(g^s)^i =b *g^(-t) mod p

(g^s)^i =b *(g^-1)^(t) mod p

We calculate (g^s)^0 mod p, (g^s)^1 mod p, (g^s)^2 mod p, … , (g^s)^(s-1) mod p and store them in a table.

We next calculate b *g^(-0) mod p, b *g^(-1) mod p, ... and check whether there is a match or not.

If there is a match we can get i and t from them. We can calculate x as s*i+t.

Pollard's rho method

Pollards rho method tries to find x by generating random numbers r1, r2 and compute g^r1 *b ^r2 mod p and store. We keep on generating random numbers and compute g^r1 *b ^r2 and check with the earlier generated numbers. If there is a match we can compute x as follows

IV. MODIFIED ELLIPTIC CURVE DISCRETE LOG PROBLEM

Simplified Weierstrass equation for elliptic curve is y^2 = x^3 + ax + b where a, b, x and y belong to some field with 4a^3 + 27b^2 ≠ 0. For detailed discussion refer [7].

Let P and Q be two points on the elliptic curve. Let the line joining the two points intersect

the curve at a third point say R. The addition of points is defined as P + Q + R = identity

Identity is defined as a point at infinity denoted by O. A line is said to pass through

point at infinity when it is vertical. It may easily be seen that the elliptic curve forms a group

under addition.

Scalar multiplication is defined a repeated addition. Let n be integer.

nP = P + P + · · · n times

The following holds when P, Q and R are points on the elliptic curve.

- P + Q will be point on the curve (Closure)
- P + Q = Q + P (Commutativity)
- (P + Q) + R = P + (Q + R) (Associativity)
- P + O = O + P = P (Existence of an identity element)
- There exists (−P) such that −P + P = P + (−P) = O (Existence of inverse)

Similar to ordinary DLP we can define elliptic curve discrete log like xP=Q. Where P is a point on the elliptic curve we choose x and calculate xP as Q. Given x and P finding Q is easy but given P and Q finding x is hard. So this is a one way function.

We propose modified elliptic curve discrete log problem.

We take two points P, Q and take random elements x and y. We calculate xP+yQ=R. Given P, Q, x and y we can easily calculate R. Given P, Q, R it is difficult to calculate x and y. To estimate the time complexity to calculate x and y we devise an algorithm. Let the order of P be n1 and Q be n2.

```
Input: P, Q, R
Output: x, y
n1=order of P;
n2=order of Q;
For i from 1 to n1 do
  For j from 1 to n2 do
    temp=i*P+j*Q;
    if(temp==R)
      x=i;
      y=j;
      Return x, y;
    End if;
  End for;
End for;
```

The time complexity of the algorithm is O(n1*n2); So the Modified Elliptic curve discrete log problem is hard problem.

V. CONCLUSION

In this paper we have described various one-way function like integer factorization, Discrete log problem. We have explained cryptosystems associated with the one-way function. We have proposed a new one-way function and named it as the Modified Elliptic curve discrete log problem.

We have developed an algorithm and find that the time complexity of the modified Elliptic curve discrete log problem is O(n1*n2). We come to the conclusion that this is hard problem.

REFERENCES

[1] John M Pollard. Kangaroos, monopoly and discrete logarithms. Journal of cryptology, 13(4):437–447, 2000.

[2] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). *Communications of the ACM*. **21** (2): 120–126

[3] Boneh, Dan. "Twenty years of attacks on the RSA cryptosystem." *Notices of the AMS* 46.2 (1999): 203-213.

[4] Pollard, J. M. (1974). "Theorems of factorization and primality testing". *Proceedings of the Cambridge Philosophical Society*. **76** (3): 521–528 **(p-1) method**

ISSN: 2454-4248
12 – 14

[5] Pollard, J. M. (1975), "A Monte Carlo method for factorization", *BIT Numerical Mathematics*, **15** (3): 331–334**(rho)**

[6] Hoffstein, Jeffrey, Jill Catherine Pipher, Joseph H. Silverman, and Joseph H. Silverman. An introduction to mathematical cryptography. Vol. 1. New York: springer, 2008.

[7] Blake, Ian, GadielSeroussi, and Nigel Smart. Elliptic curves in cryptography. Vol. 265. Cambridge university press, 1999.