Advances in Computer Science and Engineering

http://www.pphmj.com
http://dx.doi.org/10.17654/CS017010001
Volume 17, Number 1, 2018, Pages 1-10 **ISSN: 0973-6999**

STRENGTH ANALYSIS OF FIGHTING BIRTHDAY ATTACK BASED ON FINITE CYCLIC GROUP

Yinghui Luo

Department of Computer Science
Guangdong University of Education
Guangzhou, 510303
P. R. China

Abstract

Birthday attack can reduce half of the effective key length of public key cryptosystem based on the finite cyclic group theory and get 63.2% attack success rate. ElGamal cryptograms and elliptic curve cryptography (ECC) based on discrete logarithms can also be expressed in the form of finite cyclic groups, which are vulnerable to birthday attacks. There are two ways to solve this problem: one is to increase the complexity of the addition operation in the group and the other is to increase the order n of the group.

1. Introduction

Public key cryptography known also as asymmetric cryptography is the critical technology for digital signature. The electronic certificate based on this technique is the key to e-commerce. Therefore, its security is important.

Commonly used algorithms for digital signatures are RSA [1] and ECC (elliptic curve) [2]. It is generally accepted that the latter has better security

Received: March 1, 2018; Accepted: April 5, 2018
Keywords and phrases: finite cyclic Abelian group, asymmetric encryption, birthday attack.
Communicated by Yangming Li; Editor: JP Journal of Algebra, Number Theory and Applications; Published by Pushpa Publishing House, Allahabad, India.

in the case of the same code length. For example, some documents think that the security of 160-bit ECC is comparable to 1024-bit RSA [3]. However, there are arguments about it among academics. Because the current RSA is more widely used than ECC, RSA security vulnerabilities are also well known, but ECC have not been tested extensively.

Group theory is widely used in the field of cryptography. Permutation groups are often used in symmetric encryption algorithms, and finite cyclic groups can be used to implement asymmetric encryption algorithms. Both ElGamal cryptosystems based on discrete logarithms [4] and elliptic curve cryptosystems [5, 6] can be expressed in the form of a finite cyclic group. These two cryptosystems can be considered as two applications of a finite cyclic group. Therefore, it has more universal meaning to study the encryption system security of a finite cyclic group.

The birthday paradox has made brilliant achievements in attacking Hash functions, such as MD5 message digest. The digest length is 128 bits, the effective security length with birthday attack is only 64 bits, while the length of 64 bits enables it under high probability of success in violent attacks during an effective length of time. At present there are countless websites on Internet that provide services to crack MD5. People can use birthday attacks to pretend message digests, in order to forge digital signatures.

In this article, we focus on the subject that birthday attacks reduce the effective encryption strength on a finite cyclic group encryption system.

2. Principle of Birthday Attack

2.1. Birthday paradox

The essence of birthday attack is to exploit the probability nature for random attacks. Suppose there are 23 people in a room, then the probability of two people sharing the same birthday is slightly bigger than 50%.

If there are 30 people, then the probability of the same birthday of two is about 70%. To generalize, assume that there are n objects, r individuals, each one selects an object (allow repetition of the selection, it may happen that

more than 1 person choose the same object). Then the probability that the second information is different from the first one is $(n-1)/n$, the probability of the third one being different from the previous two is $(n-2)/n$, and so on. If p is the probability of at least 2 same objects, then

$$p = 1 - \frac{n * (n-1) * \cdots * (n-r+1)}{n^r}. \tag{1}$$

Substituting $n = 365$ and $r = 23$ into equation (1), the probability of same birthday comes out to be $1 - 0.493 = 50.7\%$.

2.2. Probability of same birthday in two rooms

When cracking a password, it is often necessary to calculate the probability of having the same birthday in two different rooms. Suppose there are two rooms, each with 30 people. Then what is the probability that a person in the first room shares same birthday with someone in the second room? For example, suppose there are n objects and two groups of people, r people in each group, each person in each group chooses one object (repeatable). What is the probability that the first group and the second group choose same objects? It is easy to deduce the following formula:

$$p \approx 1 - e^{-\lambda}, \tag{2}$$

where

$$\lambda = r^2/n. \tag{3}$$

For example, if n is 365, $r = 30$, then $\lambda = 2.466$,

$$p \approx 1 - e^{-2.466} = 1 - 0.0849 = 0.915.$$

That means, when there are 30 people in each of the two rooms, it is about 91.5% possibility that a person in the first room shares the same birthday with someone in the second room.

When two keys in two different rooms have the same key value, it is considered that a collision has occurred. The birthday attack is to use the collision to achieve its attacks.

3. Use of a Finite Cyclic Group to Realize Asymmetric Encryption

3.1. Abelian group structure

What kind of Abelian group can be applied to asymmetric encryption system? If algebraic system $\langle G, \odot \rangle$ is a group, it needs to meet the following conditions:

(1) The algebraic system must be closed and discrete, and the elements in G are derived from the finite field $GF(n)$. For security reasons, n is a large prime number greater than 160 bits.

(2) Binary operation $\odot$ meets the combination law and exchange law, and complex enough.

(3) There exists unitary $e \in G$.

(4) All the elements in the group have inverse elements.

(5) Except unitary e, any element in a group G is a generator, so that G is a cyclic group.

Example 1. Structure of the ElGamal group.

ElGamal cryptosystem achieves asymmetric cryptography by difficult questions of discrete logarithm. Now we discuss how to generate a group to implement ElGamal cryptosystem:

To construct the algebraic system $\langle G, \odot \rangle$, where n is a prime number, a is a positive integer different from n, a is the primitive element of modulo n, the binary operation $\odot$ in algebraic system is modular multiplication, namely:

$$a^i \odot a^j \equiv a^i * a^j \pmod{n} \equiv a^{i+j} \pmod{n}.$$

The algebraic system can be proved to be a group as long as it meets cohesion law and there exists a unitary element and every element has an inverse.

(1) Structure of the group G:

$$G = \{a^0, a^1, a^2, a^3, a^4, ..., a^{n-1}\}.$$

(2) a^0 is unitary.

(3) Inverse of the element a^i is a^{n-i-1}.

This is because:

$$a^i \odot a^{n-i-1} \equiv a^{n-1} \bmod n,$$

a and n are mutually prime. From Euler's theorem or Fermat's little theorem

$$a^i \odot a^{n-i-1} \equiv a^{n-1} \bmod n \equiv 1 \bmod n \equiv a^0 \bmod n.$$

At the same time it can be concluded that the group is closed and circular.

(4) Except for unitary a^0, any element a^i can be used as the generator of this group.

Example 2. Structure of elliptic curve group.

The structure of the elliptic curve group is relatively more complicated. The authors in [3, 5, 6] described in detail the description that how to use the elliptic curve to construct a finite cyclic group $\langle G, + \rangle$. Below, we provide a brief introduction.

The elements, except for unitary e, in the group G are Weierstrass equations:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (4)$$

All groups of discrete solutions use infinity e as the unit of the unitary. The "+" operation in the group G is defined by the relation of three discrete solutions on the same line of equation (4). The square operation is defined by a straight line and tangent to elliptic curve (4). In group G, except for e, any element can be used as the generator element of group G, so that the group is a cyclic group.

3.2. Password generation

The asymmetric cryptosystem has a pair of passwords made of public key and private key. The order of the group $\langle G, \odot \rangle$ is n (n is a large prime number). The steps to generate this pair of passwords in group G are as follows:

(1) Take a point B in G as the generator of the group, and use B as the starting point.

(2) Randomly take a natural number d (meeting the condition: $0 < d < n - 1$) as the user's encrypted private key.

(3) Q is a point in group G, using it as the key, Q can be obtained by the following formula:

$$Q \equiv dB. \tag{5}$$

It is easy to get Q from d and B, while it is hard to get d from B and Q. (B, Q, d) is the group's cryptographic system, B and Q are public, and d is secret.

Note. Base point B and public key Q are points in the group G, and key d is a natural number.

3.3. Encryption process

Alice sends the message to Bob. Alice first encrypts it with Bob's public key Q, then sends the ciphertext to Bob, and Bob decrypts it with his own key d after he receives the ciphertext:

(1) Alice chooses a random positive integer k, uses the generator B and Bob's public key Q to calculate:

$$C_1 \equiv kB,\ C_2 \equiv kQ.$$

(2) Alice encrypts the data with C_2 and sends the encrypted data with C_1 to Bob.

(3) Bob receives C_1 and ciphertext, but C_1 cannot decrypt the data. Must

need C_2 to decrypt. C_2 can be obtained by calculating C_1. And Bob has key d, he can find C_2 by calculating the key d and C_1:

$$dC_1 \equiv d(kB) \equiv k(dB) \equiv kQ \equiv C_2.$$

Now through C_2, the decryption can be done. When the value of n is large enough, we can prove that the calculation of C_2 is relatively easy when d, B and C_1 are known. If d and k (k is a random number) are not known, it is more difficult to calculate C_2 from C_1 directly.

4. Birthday Attack Algorithm to Find the Key

As long as the key d is calculated by the generator B and the public key Q, the decoding of the cyclic group is completed.

There are two ways to calculate the subset P_1 and the subset P_2 of the group G, which are generated by the generator B and the public key Q respectively, where Z is a set of natural numbers.

Way 1: Through the generator B,

$$P_1 = \{P \mid xB \wedge x \in Z\}. \tag{6}$$

Way 2: Through the public key Q,

$$P_2 = \{P \mid yQ \wedge y \in Z\}. \tag{7}$$

P_1 and P_2 are subsets of the group G, and the number of elements in P_1 and P_2 is r. When there exists an element p belonging to both subsets P_1 and P_2, a collision happens. Larger the value of r, greater is the probability of collision between the elements of these two subsets. The decryption can be completed in the event of a collision. Suppose the order of group $\langle G, + \rangle$ is n, then

$$\exists p(p \in P_1 \wedge p \in P_2).$$

So, for natural numbers x and y:

$$xB \equiv yQ. \tag{8}$$

Again by the formula (5),

$$xB \equiv yQ \equiv (yd)B,$$

and hence

$$yd \equiv x \bmod(n-1). \tag{9}$$

Solving equation (9) of a congruence, find the key d.

Decryption is successful!

5. Birthday Attack Time Complexity Analysis

The complexity of the time of the birthday attack depends on the size of r, the elements in subsets P_1 and P_2 of the calculation group. Larger is r, larger is the workload of computing subsets P_1 and P_2, greater is the possibility of collisions to occur, and higher is the rate of attacks success.

Obviously, the value of r is small when the decrypt success rate is only 10% of the value of r in the decrypt success rate of 90%. When $r = n$, it is to obtain all elements in the group with 100% success rate of cracking, it means a violent attack. So when the value of r is far less than n, the birthday attack makes sense. However, if the value of r is too small, the probability of successful attack p is very low, the birthday attack is equally meaningless.

When the attack success rate $p \geq 50\%$, the minimum value of r is called the effective security length of the key. The value of r has also become a measure for the strength of an encryption system against birthday attack.

Suppose that there are n elements in the group $\langle G, + \rangle$, then generate r elements by B and Q. According to the probability of same birthday in two rooms, the relation between r and n is deduced from formula (2) as

$$\lambda = \ln\left(\frac{1}{1-p}\right). \tag{10}$$

Then by the formula (3),

$$r = \sqrt{n} * \sqrt{\ln(1/(1-p))}. \tag{11}$$

As seen from equation (11), r and n are square roots, that is, if n is a 160-bit integer, then r is only 80-bit binary, and the value of $\sqrt{\ln(1/(1-p))}$ does not change much, 0.325 at $p = 10\%$ and 1.52 at $p = 90\%$. In particular, when $p = 63.2\%$, $\sqrt{\ln(1/(1-p))} = 1$, r equals $\sqrt{n}$. That is to say that the probability of cracking password is 63.2%, and the effective password length r is exactly half of n.

Table 1. Relation of effective password length and cracking success rate

The effective password r size	$1.52\sqrt{n}$	$\sqrt{n}$	$0.83\sqrt{n}$	$0.33\sqrt{n}$
Success rate	90%	63%	50%	10%

If the cracking success rate decreases, the effective password length r of the attacking decreases, not proportionally, but significantly. By choosing a smaller value of r to attack multiple accounts, get a higher probability of cracking one of the accounts.

As seen from Table 1, for the success rate of cracking reduction, effective password length reduction is not obvious, 90% to 10% reduction in the success rate, it is 9 times, while the value of r decreases by only 4.68 times. From this, we can conclude that not worth the candle to choose a smaller value of r to attack multiple accounts in order to obtain a higher probability of cracking one of the accounts.

6. Conclusion

Birthday attack can reduce by half the valid password length of a finite cyclic group encryption system and obtain a successful cracking rate of 63.2%, which challenges the security of a non-symmetric cryptosystem based on the group theory. Since both ElGamal and ECC based on discrete

logarithms can be expressed as a finite cyclic group, birthday attacks can also have their effective password length.

In order to enhance the strength of a finite cyclic group against birthday attacks, it is necessary to reduce the probability of collisions of elements in the subset P_1 generated by the generator B and the subset P_2 generated by the public key Q. As long as collision occurs, it is easy to find out key d. To reduce the probability of collision, the most direct way is to increase the order of the group to improve its security.

In order to improve the effectiveness of fighting birthday attack, the addition operation in the group $\langle G, + \rangle$ can be more complicated. As long as the addition operation in the group is defined sufficiently complex, it takes more time to generate the subsets P_1 and P_2, so greatly improves the security against birthday attacks.

References

[1] Luo Yinghui and Chen Yiqun, Macro modeling algorithm for fast realization of digital signature, Computer Engineering and Applications 4 (2007), 238-241.

[2] A. Menezes, Elliptic Curve Public Key Crytosystem, Kluwer Academic Publishers, 1993

[3] Luo Yinghui and Jiang Hong, The conditions to construct public cryptosystem and encryption intensity with finite cyclic groups, Computer Science 35(8) (2008), 101-103 (special issue).

[4] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory 31 (1985), 469-472.

[5] Yinghui Luo, A public key cryptography based on a finite cyclic group, JP J. Algebra Number Theory Appl. 11(1) (2008), 129-136.

[6] Luo Yinghui and Li Yangming, The construction of a finite cyclic group applied in asymmetric encryption, Journal of Foshan University (Natural Science) (2008), Issue 3, 6-8.