

**New Public Key Cryptosystem  
Using Discrete Logarithms over  $GF(p)$**

Masakatu MORII and Masao KASAHARA

愛媛大学工学部紀要 12 卷 2 号 pp. 433~439 別刷 平成 3 年 2 月

Reprinted from

Memoirs of the Faculty of Engineering, Ehime University

Vol. XII, No. 2, pp. 433~439 February 1991

## New Public-Key Cryptosystem Using Discrete Logarithms over $GF(p)$

Masakatu MORII\* and Masao KASAHARA\*\*

This paper discusses a public key cryptosystem over finite fields. The important result is the proposition of a new public key cryptosystem using discrete logarithms over finite fields as one way trapdoor function. It is very interesting that the proposed cryptosystem is strongly related to Merkel-Hellman multiplicative knapsack cryptosystem and RSA cryptosystem. The features of this cryptosystem are that it can be enciphered very fast with precomputed tables, and that the parallel processing techniques can be very easily applied when enciphering.

*Key words:* cryptography, public-key cryptosystem, number theory, finite fields, discrete logarithms

### 1. INTRODUCTION

The techniques of information security become more and more important for the society in the present age with modern computer and communication systems. Especially the cryptographic systems, that provide secrecy by use of transformations, are the basic systems of data security.

In 1976 W. Diffie and M. Hellman<sup>1)</sup> proposed a concept of new cryptographic system for data security, which is called "Public Key Cryptosystem". In the public key cryptosystem, the enciphering key is different from the deciphering key, and it is very hard that anyone, which does not know the deciphering key, can compute the deciphering key based on the knowledge of the enciphering key. Therefore the enciphering key can be published, and it can clear up the difficulties of the key distribution and the key management. However they gave no method of the realization for the public key cryptosystem. In 1978 R. Rivest, A. Shamir and L. Adleman<sup>2)</sup> proposed the method of the realization for that system. Later the some other methods have been proposed.

In this paper a new public key cryptosystem using discrete logarithms over prime field  $GF(p)$  is proposed. The features of this cryptosystem are that it can be enciphered very fast with precomputed tables, and that the parallel processing techniques can be very easily applied when enciphering. It is very interesting that this cryptosystem has strong relations to Merkle and Hellman's Multiplicative Knapsack Cryptosystem<sup>3)</sup> and Rivest-Shamir-Adleman cryptosystem.

\*Department of Computer Science, Ehime University

\*\*Department of Electronics and Information Science, Kyoto Institute of Technology

原稿受理 平成2年9月3日

## 2. CIPHER AND DECIPHER SYSTEMS

### 2.1 Construction of Public Key Cryptosystem

Let

$$a_1, a_2, \dots, a_n \quad (1)$$

be relatively prime numbers and choose two prime numbers  $p$  and  $e$  satisfying the following equations:

$$p > \prod_{i=1}^n a_i \quad (2)$$

and

$$\gcd(e, p-1) = 1. \quad (3)$$

Furthermore compute  $d$  satisfying the following equation:

$$e \cdot d \equiv 1 \pmod{p-1}. \quad (4)$$

A Euclidean algorithm is very useful for that computation. Next compute  $c_i$  satisfying the following equation:

$$c_i \equiv a_i^e \pmod{p} \quad (5)$$

where  $i = 1, 2, \dots, n$ . A new public key cryptosystem has  $c_i$  and  $p$  as the enciphering key (public key), and has  $a_i, e$  and  $d$  as the deciphering key (secret key).

(Enciphering)

Let the plain text be the bit sequence as follows:

$$x_1, x_2, \dots, x_n, \quad (6)$$

where  $x_i \in \text{GF}(2)$ , for  $i = 1, 2, \dots, n$ . The cipher text,  $F$ , can be transformed from the plain text as follows:

$$F = \prod_{i=1}^n (c_i)^{x_i} \pmod{p}. \quad (7)$$

(Deciphering)

Using  $F, p,$  and  $d,$  compute  $\tilde{F}$  by the following equation:

$$\tilde{F} = \prod_{i=1}^n (a_i)^{x_i} \equiv F \pmod{p}. \quad (8)$$

The plain text,  $x_i,$  can be transformed from  $\tilde{F}$  and  $a_i$  as follows:

$$x_i = \begin{cases} 1 & \text{if } \tilde{F} \equiv 0 \pmod{a_i} \\ 0 & \text{if } \tilde{F} \not\equiv 0 \pmod{a_i} \end{cases} \quad (9)$$

where  $i = 1, 2, \dots, n$ .

### 2.2 Example

Let  $n$  be 4, and choose the public keys and the secret keys as table 1. Now let the plain text,  $x_i,$  be

$$(x_1, x_2, x_3, x_4) = (1, 1, 0, 1). \quad (10)$$

(Enciphering)

The cipher text  $F$  can be transformed from the plain text as follows:

$$F \equiv \prod_{i=1}^4 (c_i)^{x_i} \pmod{211}$$

$$= 124. \tag{11}$$

(Deciphering)

Using the secret keys, compute  $\tilde{F}$  by the following equation:

$$\tilde{F} \equiv 124^{199} \pmod{211}$$

$$= 42. \tag{12}$$

Using Eq.(9), the plain text can be transformed from  $\tilde{F}$ , i. e. it can be verified that

$$\tilde{F} = 2 \cdot 3 \cdot 7. \tag{13}$$

Therefore the plain text satisfies

$$(x_1, x_2, x_3, x_4) = (1, 1, 0, 1). \tag{14}$$

Table 1 Example ( $n = 4$ )

Keys	The values giving in the toy example	The equation number in this paper
Secret keys	$(a_1, a_2, a_3, a_4) = (2, 3, 5, 7)$	(1)
	$e = 19$	(3)
	$d = 199$	(4)
Public keys	$(c_1, c_2, c_3, c_4) = (164, 39, 114, 85)$	(5)
	$p = 211$	(2)

### 3. DISCUSSIONS

#### 3.1 Properties of the Proposed Cryptosystem

Table 2 shows the properties of the cryptosystem proposed in this paper.

Table 2 Properties of the proposed cryptosystem

Length of plain text (bits)	$n$
Length of cipher text (bits)	$\log_2 p$
Public key (bits)	$(n+1) \log_2 p$
Secret key (bits)	$\sum_{i=1}^n \log_2 a_i + 2 \log_2 p$
Computation of enciphering	$O(np^2)$
Computation of deciphering	$O(p^2)$

#### 3.2 Relation to Merkle-Hellman Knapsack Cryptosystem

R. C. Merkle and M. E. Hellman proposed the two interesting public key cryptosystem based on the NP complete problem of knapsack packing. One has the trapdoor function using a super-increasing sequence, and it is very efficient system for its speed of the enciphering and deciphering. However it is well known that A.

Shamir<sup>4)</sup> discovered the efficient cryptanalysis of that system. The other is called "Multiplicative Knapsack Cryptosystem". Comparing the new cryptosystem proposed in this paper to the multiplicative knapsack cryptosystem, the interesting properties of the both system can be made clearly. Hereinafter the multiplicative knapsack cryptosystem is described simply, and the difference between the both systems is described clearly.

*Multiplicative Knapsack Cryptosystem* : Let

$$a_1, a_2, \dots, a_n \quad (15)$$

be the relatively prime and positive number, and choose a prime number satisfying the following equation :

$$p > \prod_{i=1}^n a_i \quad (16)$$

Furthermore  $b$  which is the primitive element over  $GF(p)$  is chosen, and  $c_i$  is computed with following equation :

$$a_i \equiv b^{c_i} \pmod{p}, \quad (17)$$

where  $i = 1, 2, \dots, n$ . Now the multiplicative knapsack cryptosystem has the public key,  $c_i$ , and has the secret keys,  $p, b$  and  $a_i$ , where  $i = 1, 2, \dots, n$ .

(Enciphering)

Let the plain text be the bit sequence :

$$x_1, x_2, \dots, x_n, \quad (18)$$

where  $x_i \in GF(2)$  and  $i = 1, 2, \dots, n$ . Then cipher text,  $F$ , is construct as followings :

$$F = \sum_{i=1}^n (x_i c_i). \quad (19)$$

(Deciphering)

Using  $F, p$  and  $b$ , compute  $\hat{F}$  as following equation :

$$\hat{F} = \prod_{i=1}^n a_i^{x_i} \equiv b^F \pmod{p}. \quad (20)$$

The plain text,  $x_i$ , can be transformed from  $\hat{F}$  and  $a_i$  as follows :

$$x_i = \begin{cases} 1 & \text{if } \hat{F} \equiv 0 \pmod{a_i} \\ 0 & \text{if } \hat{F} \not\equiv 0 \pmod{a_i} \end{cases} \quad (21)$$

where  $i = 1, 2, \dots, n$ .

Table 3 presents the relationship between the equations for the multiplicative knapsack cryptosystem and the new cryptosystem proposed in this paper.

In the multiplicative knapsack cryptosystem, letting  $n$  be 100, and each  $a_i$  be about 100 bits, then the sizes of  $b, p$  and each  $c_i$ , where  $i = 1, 2, \dots, 100$ , are about 10,000 bit from Eqs. (16) and (17). Therefore the information rate, which is defined by the ratio of the lengths between the plain text and the cipher text, is about 0.01. In order to improve this value of the information rate, each  $a_i$  should be made small as possible. Then the sizes of  $p$  and each  $c_i$  are both about 730 bits, and the information rate is improved to about 0.14. However A. M. Odlyzko

Table 3 The relationship between Merkle-Hellman's multiplicative knapsack cryptosystem (MH-PKCS) and the proposed cryptosystem in this paper (Proposed PKCS)

Proposed PKCS	Eq.	MH-PKCS	Eq.
$a_1, a_2, \dots, a_n$	(1)	$a_1, a_2, \dots, a_n$	(5)
$p > \sum_{i=1}^n a_i$	(2)	$p > \sum_{i=1}^n a_i$	(6)
$\gcd(e, p-1) = 1$	(3)		
$e \cdot d = 1 \pmod{p-1}$	(4)		
$c_d = a_i^e \pmod{p}$	(5)	$a_i = b^{c_i} \pmod{p}$	(7)
(Enciphering)		(Enciphering)	
$x_1, x_2, \dots, x_n$	(6)	$x_1, x_2, \dots, x_n$	(8)
$x_i \in GF(2), i = 1, 2, \dots, n$		$x_i \in GF(2), i = 1, 2, \dots, n$	
$F = \prod_{i=1}^n (c_i)^{x_i} \pmod{p}$	(7)	$F = \sum_{i=1}^n x_i c_i$	(9)
(Deciphering)		(Deciphering)	
$\tilde{F} = F^d \pmod{p}$		$\tilde{F} = b^F \pmod{p}$	
$= \prod_{i=1}^n (a_i)^{x_i} \pmod{p}$	(8)	$= \prod_{i=1}^n (a_i)^{x_i}$	(10)
$x_i = 1$ if $\tilde{F} = 0 \pmod{a_i}$		$x_i = 1$ if $\tilde{F} = 0 \pmod{a_i}$	
$x_i = 0$ if $\tilde{F} \neq 0 \pmod{a_i}$	(9)	$x_i = 0$ if $\tilde{F} \neq 0 \pmod{a_i}$	(11)

discovered<sup>5)</sup> the efficient cryptanalysis only in this case.

Comparing the new cryptosystem proposed in this paper to the multiplicative knapsack cryptosystem, it is clear that the remarkable difference is in Eqs. (17), (18) and (20). Consequently Eq. (17) means the solution for the problem of discrete logarithms over GF(p).<sup>6)</sup> Therefore it needs for the designer of the multiplicative knapsack cryptosystem to solve the problem of the discrete logarithms over GF(p), where the value of the p is about 10,000 bits. It means that, for example, p-1 should have the small factor.<sup>6)</sup> However it also implies that this cryptosystem has a very weak point. In more detail, when making conditions that p-1 has several small factors, p must be restricted. Therefore there is a great possibility of leaking out the value of p. Furthermore it should make each a\_i very large in order to keep secret of the value of b. However, when each a\_i has very large value, the information rate becomes very low from the condition of Eq. (16).

In the new cryptosystem proposed in this paper, the equations corresponding to the Eq. (17) are Eqs. (3), (4) and (5). In other words, the designer of this cryptosystem need not solve the problem of the discrete logarithms over GF(p). Therefore it requires no condition on p, and it is not necessary to make the value of each a\_i very large. Furthermore it mentions that the cryptanalysis proposed by Odlyzko cannot be applied to the new cryptosystem. In that cryptanalysis, when knowing each a\_i and c\_i in Eq. (17), the value delta satisfying the following equation:

$$1 = \sum_{i=1}^n \delta_i c_i \tag{22}$$

can be computed using  $L^3$  algorithm,<sup>7)</sup> and the both  $b$  and  $p$  are given from the  $\delta$ . However cryptanalyst must compute the value of  $e$  in Eq. (5) based on the knowledge of each  $c_i$ ,  $a_i$  and  $p$  in order to break this system. It means that the solving for the problem of discrete logarithms over  $GF(p)$  is necessary. It has not been reported that the problem can be solved using  $L^3$  algorithm. Therefore it becomes very difficult problem, when the value of  $p$  is about 500 bits. The above discussion shows the security of the cryptosystem proposed in this paper.

### 3.3 Remarks

In this cryptosystem, when trying to derive the secret keys from the public keys, it is equal to solve the problem of discrete logarithms over  $GF(p)$ . Furthermore it becomes very difficult problem that the plain text is guessed from the cipher text without the knowing the value of  $e$  or  $d$ . Hereinafter, when the cryptanalyst has the part of the secret keys, the security of this cryptosystem is considered.

#### I. In the case of leaking out the $a_i$ , where $i = 1, 2, \dots, n$ :

It is needed for this cryptosystem that each  $a_i$  is made as small as possible in order to increase the information rate. Therefore this cryptosystem has the great possibility of leaking out the part or all of  $a_i$ . However when the cryptanalyst ever has  $c_i$  corresponding to each  $a_i$ , he cannot know the transmitted information  $x_i$  on this cryptosystem. Moreover, in order to know the  $e$ , he must solve the problem of discrete logarithms over  $GF(p)$  as follows:

$$c_k \equiv a_k^e \pmod{p}, \quad (23)$$

where  $k = 1, 2, \dots, n$ . Consequently when the value of  $p$  is about 500 bits, it is difficult problem for the cryptanalyst to break this cryptosystem without the knowledge of the value of  $e$  or  $d$ .

#### II. In case of leaking out the $e$ :

The cryptanalyst can easily compute the value of  $d$  applying the Euclidean algorithm to Eq. (4). Then he can obtain the  $\hat{F}$  in Eq. (8) from the cipher text  $F$  only, and have each  $a_i$  from the factorization for  $F$ , where  $i = 1, 2, \dots, n$ . Consequently, this cryptosystem is perfectly broken in this case since he can get the all secret keys.

## 4. CONCLUSION

This paper has presented the public key cryptosystem using discrete logarithms over  $GF(p)$  as one way trapdoor function, and has discussed the properties and securities.

The information rate of the cryptosystem proposed in this paper is larger than that of the Merkle-Hellman's multiplicative knapsack cryptosystem. Furthermore

the techniques of parallel processing on arithmetic operations can be applied to the enciphering on the cryptosystem proposed in this paper. Therefore there exists the interesting relationship of the trade-off between the time of encoding and the memory of storing of data.

### REFERENCES

- 1) H. Diffie and M. Hellman: New directions in cryptography, *IEEE Trans. Info. Theory*, **IT-22**, pp. 644-654, 1976.
- 2) R. Rivest, A. Shamir and L. Adleman: On digital signatures and public key cryptosystems, *Comm. of the ACM*, **21**, pp. 120-126, 1978.
- 3) R. C. Merkle and M. Hellman: Hiding informations and signatures in trapdoor knapsacks, *IEEE Trans. Info. Theory*, **IT-24**, pp. 525-530, 1978.
- 4) A. Shamir: A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem, *IEEE Trans. Info. Theory*, **IT-30**, pp. 699-704, 1984.
- 5) A. M. Odlyzko: Cryptanalytic attacks on the multiplicative knapsack cryptosystem and Shamir's fast signature schema, *IEEE Trans. Info. Theory*, **IT-30**, pp. 594-601, 1984.
- 6) S. C. Pohlig and M. Hellman: An improved algorithm for computing logarithms over  $GF(p)$  and its cryptographic significance, *IEEE Trans. Info. Theory*, **IT-24**, pp. 106-110, 1978.
- 7) A. K. Lenstra, H. W. Lenstra and L. Lovasz: Factoring polynomials with rational coefficients, *Math. Ann.*, **261**, pp. 515-534, 1982.