942

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

June 1991

P1 INFORMAL No. 6, MATH #6

A New Public-key Cryptosystem based on k^{th} -power Residues

By: [redacted]
P12

LIBRARY No. S-237,204

A9585A.3-79

11

A New Public-key Cryptosystem Based on k^{th}-power Residues

This paper, by the number theorist (and sometime reviewer for Mathematical Reviews) CAO Zhen-Fu (Assistant Professor, Department of Mathematics, Harbin Institute of Technology, PRC), is part of the continuing P1 effort to make more accessible foreign literature which may have cryptologic implications. Translation from the Chinese has been carried out by [redacted] *of P12. The paper appeared in the Journal of the China Institute of Communications, vol. 11, March 1990, p. 80-83. Another article by the same author has previously appeared in this series. There can be no doubt that the author is tied into the Chinese cryptologic community (see bibliographic reference no. 9).*

Abstract: Using some results on k^{th}-power residues, we propose in this paper a new type of public-key cryptosystem based on the difficulty of factoring large integers. The Goldwasser-Micali probabilistic encryption system is a special case of the new system, and the new system has the additional property that it is impossible to use the solvability of $x^k \equiv a \bmod m$ to break the system.

1. Introduction

Since Diffie and Hellman [1] proposed the use of trapdoor one-way functions to construct public-key cryptosystems, many authors have studied them, with the principal work concentrated on the factorization of large integers and on the knapsack problem. The major systems based on factorization of large integers are the Rivest-Shamir-Adleman system [2] and the Goldwasser-Micali system [3]; the chief systems to use the knapsack problem are the Merkle-Hellman system [4] and others which are transforms of it [6]. Because most of the systems based on the knapsack system have been broken [6], systems based on the difficulty of factoring large integers have been receiving more and more attention.

In 1982, Goldwasser and Micali [3] proposed their well-known probabilistic encryption system based on the factorization of large integers. They

considered two properties which a trapdoor one-way function should have in the construction of a public-key cryptosystem:

(1) if $f(x)$ is an appropriate trapdoor one-way function then, unless n of of some very special form, $f(n)$ is easily computed from n.

(2) if $f(x)$ is an appropriate trapdoor one-way function then given $f(n)$ it is not possible to compute easily any information about n.

As we recently [7] showed, the Goldwasser-Micali system is in fact based upon a special type of trapdoor one-way function. However, the work of Goldwasser and Micali has shown us that a study of public-key cryptosystems should be launched with the following two characteristics:

(1) to encipher the information n (called the complete encryption of n), each individual part (that is, each individual digit) should be enciphered;

(2) the encryption function should have the properties of a trapdoor one-way function.

In this paper we use k^{th}-power residues to propose a new type of public-key cryptosystem based on the factorization of large integers. We will prove that the new system is at least as secure as the Goldwasser-Micali system. If $k > 2$, without any extra conditions on the large prime factor q of the large integer $m = pq$ we can prove that it is impossible to break the cryptology by using the solution of the congruence $x^k \equiv a \bmod m$. If $k > 2$, the new system may be regarded as a generalization of the Goldwasser-Micali system, and if we add a suitable condition on q we can also prove that it is impossible to break the cryptology by determining a solution of the congruence $x^2 \equiv a \bmod m$ (because it is impossible to solve efficiently the congruence $x^k \equiv a \bmod m$, $k > 1$, except by use of a probabilistic method), a property which the Goldwasser-Micali system does not enjoy. As discussed also in [9], if the factorization of large integers is difficult, this type of cryptosystem is secure.

2. The composition of the new system

Write Z for the set of integers, N for the set of positive integers. If $m \in N$, $m > 1$, then we use Z_m, Z_m^* respectively to represent the sets of, respectively, the smallest nonnegative residues and the smallest residues in absolute value mod m, so $Z_m = \{0, 1, \ldots, m-1\}$, $Z_m^* = \{-[\frac{m}{2}], \ldots, -1, 0, 1, \ldots, [\frac{m}{2}]\}$. For

a fixed $k \in N$, $k > 1$, let $p = kp_1 + 1$ be a fixed large prime number, where $p_1 \in N$. Then for $a \in Z$ the k^{th}-power residue symbol mod p, $(\frac{a}{p})_k$, is defined by

$$(\frac{a}{p})_k \triangleq (a^{p_1})_p, \quad p_1 = \frac{p-1}{k},$$

where $(\cdot)_p$ denotes the smallest absolute value mod p, so that $(\cdot)_p \in Z_p^*$. As a varies through Z_p, $(\frac{a}{p})_k$ assumes k different values in general (one of which is the value 1), thus in Z_p we can choose d $(1 < d \leq k)$ different numbers $a_0, a_1, \ldots, a_{d-1}$ such that

$$(\frac{a_i}{p})_k \neq (\frac{a_j}{p})_k, \; i \neq j. \tag{1}$$

Moreover, if $1 < d < k$, we can choose the a_i such that $(\frac{a_i}{p})_k \neq 1$, $(i = 0, 1, \ldots, d-1)$.

Now choose another large prime q. If $k > 2$, q may be chosen arbitrarily; if $k = 2$ then d must be 2, and we must choose q to satisfy

$$(\frac{a_0}{m}) = (\frac{a_1}{m}), \tag{2}$$

where $m = pq$ and $(\frac{\cdot}{m})$ denotes the Jacobi symbol for $\cdot$ mod m.

Then the new system consists of the following parts.

Secret key: p, q.

Public key: $m, k, (a_0, a_1, \ldots, a_{d-1})$, where $k << p$.

Plain text: $n = b_0 + b_1 d + \cdots + b_{t-1} d^{t-1}$, $b_i \in Z_d$.

Encryption: $\{E(x_i)\}_{i=0}^{t-1}$, where $\{x_i\}_{i=0}^{t-1}$, satisfying $(x_i, m) = 1$, $(i = 0, 1, \ldots, t-1)$ is an arbitrary sequence of integers, and if $b_i = j$, the encryption function is defined by

$$E(x_i) = < a_j x_i^k >_m, \; i \in Z_t, \; j \in Z_d, \tag{3}$$

where $< \cdot >_m$ denotes the smallest nonnegative residue of $\cdot$ mod m. Thus $< \cdot >_m \in Z_m$.

Decryption: knowing the secret key, decryption is convenient. Write $(\frac{a_i}{p})_k = c_i$, $(i = 0, 1, \ldots, d-1)$. Since

$$(\frac{E(x_i)}{p})_k = (\frac{a_j}{p})_k = c_j,$$

we need only compute the value $(\frac{E(x_i)}{p})_k$ and determine $b_i = j$ by finding $(\frac{E(x_i)}{p})_k$ among the $(c_0, \ldots, c_{d-1})$.

From number theory [8] we know that for a fixed $a \in N$ and prime $p \equiv 1 \bmod k$, $(\frac{a}{p})_k$ may be computed very easily. For example, for $a \equiv b \bmod p$ we know $(\frac{a}{p})_k = (\frac{b}{p})_k$. If $b = b_1 b_2 \cdots b_u$, we know that $(\frac{b}{p})_k \equiv \prod_{i=1}^{u} \left(\frac{b_i}{p}\right)_k \bmod p$. Therefore in the new system both encryption and decryption are very simply and easily accomplished.

In the new system we could take the case $k = 3$ for common use. Next we illustrate the encryption and decryption method of the new system for the case $k = 3$.

Let $p \equiv 1 \bmod 3$ be a large prime. Since $k = 3$ we have $1 < d \leq 3$. Thus to represent information we could use either 2 or 3 in the system. Choose in Z_p 2 or 3 different numbers a_0, a_1 or a_0, a_1, a_2 such that (1) holds, and in the former case we also require $(\frac{a_i}{p})_3 \neq 1$, (i=0,1). Also choose a large prime q and set $m = pq$. Then publish either $m, (a_0, a_1)$ or $m, (a_0, a_1, a_2)$, taken to be the enciphering keys, while the deciphering keys p and q are kept strictly secret.

Enciphering method. If the enciphering keys are $m, (a_0, a_1)$, then $d = 2$, and thus the plain text n used in the system is represented by

$$n = b_0 + b_1 \cdot 2 + \cdots + b_{t-1} \cdot 2^{t-1}, \ b_i \in Z_2.$$

Choose a sequence $\{x_i\}_{i=0}^{t-1}$ of integers satisfying $(x_i, m) = 1$, $(i = 0, 1, \ldots, t-1)$, and substitute into the enciphering function (3) to get

$$E(x_i) = \begin{cases} < a_0 x_i^3 >_m, & \text{if } b_i = 0 \\ < a_1 x_i^3 >_m, & \text{if } b_i = 1. \end{cases} \tag{4}$$

If the enciphering keys are $m, (a_0, a_1, a_2)$, then $d = 3$. Thus the plain text used in the system is represented by

$$n = b_0 + b_1 \cdot 3 + \cdots + b_{t-1} \cdot 3^{t-1}, \ b_i \in Z_3.$$

Therefore, with the sequence $\{x_i\}_{i=0}^{t-1}$ of integers relatively prime to m, we encipher as follows:

$$E(x_i) = \begin{cases} < a_0 x_i^3 >_m, & \text{if } b_i = 0 \\ < a_1 x_i^3 >_m, & \text{if } b_i = 1 \\ < a_2 x_i^3 >_m, & \text{if } b_i = 2. \end{cases} \tag{5}$$

Deciphering method. The intended receiver from $\{E(x_i)\}_{i=0}^{t-1}$ computes $(\frac{E(x_i)}{p})_3$. If the $E(x_i)$ are as in (4), then we have

$$b_i = \begin{cases} 0, & \text{if } (\frac{E(x_i)}{p})_3 = c_0 \\ 1, & \text{if } (\frac{E(x_i)}{p})_3 = c_1. \end{cases}$$

If the $E(x_i)$ are as in (5), then we have

$$b_i = \begin{cases} 0, & \text{if } (\frac{E(x_i)}{p})_3 = c_0 \\ 1, & \text{if } (\frac{E(x_i)}{p})_3 = c_1 \\ 2, & \text{if } (\frac{E(x_i)}{p})_3 = c_2. \end{cases}$$

3. A Security Analysis of the new System

The security of the new system is still based on the difficulty of factoring large integers. Below we shall prove that from m, k, and $(a_0, a_1, \ldots, a_{d-1})$, and knowing the construction of the new system, with the addition of the extra condition, it will be impossible to determine the factor p of m.

1. Immediately from m we know that there is a prime factor $kp_1 + 1$ with $p_1 \in \mathcal{N}$, but we would need to do $\pi(\frac{p-1}{k})$ trial divisions to obtain p, where $\pi(x)$ denotes the number of primes not exceeding x. But since $\pi(x) \sim \frac{x}{\log x}$ as $x \to \infty$ [8], for fixed k and very large p the very large number of trial divisions is difficult to accomplish.

2. Starting from $(\frac{a_i}{p})_k \neq (\frac{a_j}{p})_k, (i \neq j)$, with $(\frac{a_i}{p})_k \in Z_p^*$, we are also unable to obtain p. A prospective attacker may use a probabilistic method to test different primes p of the form $kp_1 + 1$ to see which satisfy the aforementioned conditions. But this is a very complicated test and a prime p which satisfies the conditions is not sure to be a factor of m. Using such a test, only a small percentage of primes will satisfy the above conditions and again one could try to find p by trial division, but this is not practical.

3. Since it is difficult to factor m directly, we might try instead to solve $x^k \equiv E(x_i) \bmod m$. Such a method is very effective in breaking the Goldwasser-Micali system, but for the new system it is of no avail. We see this as follows:

First, there may be no efficient method to solve $x^k \equiv E(x_i) \bmod m$, but then we would obviously be unable to recover the plain text.

Next, even if there were an efficient method to solve $x^k \equiv E(x_i) \bmod m$, if $k > 2$, the attacker does not know how to find the value of $(\frac{a_i}{p})_k$, so even from $x^k \equiv E(x_i) \bmod m$ it is impossible to determine b_i, and thus impossible to recover the plain text n. Thus if $x^k \equiv E(x_i) \bmod m$ can be solved it must be that $(\frac{a_i}{p})_k = 1$. Since if $d < k$, all a_i satisfy $(\frac{a_i}{p})_k \neq 1$, we must have $d = k > 2$. Knowing $(\frac{a_i}{p})_k = 1$, we can determine only those b_i in $(b_0, b_1, \ldots, b_{t-1})$ which are equal to j. Note that, because $(\frac{a_i}{p})_k = 1$ for only one value in $a_0, a_1, \ldots, a_{d-1}$, it follows that $j \in Z_d$ is fixed. For example, without loss of generality we can assume that a_0 satisfies $(\frac{a_0}{p})_k = 1$, $(\frac{a_i}{p})_k \neq 1$ for $i = 1, \ldots, d-1$, but this determines which of the $b_0, b_1, \ldots, b_{t-1}$ have value 0. Since $d > 2$, those b_i which are nonzero number at least $d - 1 \geq 2$, so we are unable to evaluate $b_i \neq 0$. Using $d > 2$ in the system is obviously advantageous.

If $k = 2$, the new system becomes the following generalized form of the Goldwasser-Micali system:

Let p be a fixed large prime, and choose $a_0, a_1 \in N$ such that $(\frac{a_0}{p}) \neq (\frac{a_1}{p})$, where $(\frac{a}{p})$ denotes the Legendre symbol for the modulus p (the k^{th}-power residue symbol when $k = 2$). Choose a large prime q such that $(\frac{a_0}{m}) = (\frac{a_1}{m})$, where $m = pq$. Publish m and the ordered pair (a_0, a_1) as the enciphering key, and use p, q as the deciphering key.

Enciphering: if the plain text $n = b_0 + b_1 \cdot 2 + \cdots + b_{t-1} \cdot 2^{t-1}$, $b_i \in Z_2$, $(i = 0, 1, \ldots, t-1)$, then choose an enciphering sequence $\{x_i\}_{i=0}^{t-1}$, $x_i \in Z$, such that $(x_i, m) = 1$, $(i = 0, 1, \ldots, t-1)$, and encipher to get

$$E(x_i) = \begin{cases} < a_0 x_i^2 >_m, & \text{if } b_i = 0 \\ < a_1 x_i^2 >_m, & \text{if } b_i = 1. \end{cases}$$

Deciphering: knowing the factor p of m, one can compute the values $(\frac{E(x_i)}{p})$, and we have $(\frac{E(x_i)}{p}) = (\frac{a_j}{p}) \iff b_i = j$ for $j = 0, 1$.

If in this system we take $a_0 = 1$ we have the Goldwasser-Micali system. If $a_0 > 1$, the conditions $(\frac{a_0}{p}) \neq (\frac{a_1}{p})$ and $(\frac{a_0}{m}) = (\frac{a_1}{m})$ can without loss of generality be written as the two conditions:

(1) $(\frac{a_0}{p}) = 1, (\frac{a_0}{q}) = -1$ and $(\frac{a_1}{p}) = -1, (\frac{a_1}{q}) = 1$;

(2) $(\frac{a_0}{p}) = 1, (\frac{a_0}{q}) = 1$ and $(\frac{a_1}{p}) = -1, (\frac{a_1}{q}) = -1$.

Here condition (2) generalizes the Goldwasser-Micali system, and it is not possible to carry out an attack by using the solvability of $x^2 \equiv E(x_i) \bmod m$: since by condition (1) we cannot in general solve $x^2 \equiv E(x_i) \bmod m$, so it is impossible to break the cryptology using the solvability of $x^2 \equiv E(x_i) \bmod m$. Note that it is required that $(\frac{a_0}{m}) = (\frac{a_1}{m})$ be impossible, for if not we could compute directly $(\frac{E(x_i)}{m}) = (\frac{a_j}{m})$ and break the system that way.

For $k > 2$, since the the k^{th}-power residue symbol $(\frac{a}{m})_k$ for a composite modulus $m \equiv 1 \bmod k$ is defined by

$$(\frac{a}{m})_k \triangleq ((\frac{a}{p})_k (\frac{a}{q})_k)_m,$$

to compute $(\frac{a}{m})_k$ one must first factor m, thus the other prime factor q of m is unrestricted. In addition, in the new system, if we choose q to satisfy the condition $q \not\equiv 1 \bmod k$, then the k^{th}-power residue symbol modulo a composite number is a generalization of the quadratic residue symbol.

4. Concluding Remarks

According to the previous discussion, we have proposed, based on k^{th}-power residues, a comparatively good public-key cryptosystem based on the difficulty of factoring large integers. It has the following characteristics:

1. As is the Goldwasser-Micali system, it is a probabilistic encryption system (which we can take as a special type of trapdoor one-way function [7]), so the new system retains the advantages of the Goldwasser-Micali system.

2. In contrast to the Goldwasser-Micali system, it is impossible to break the cryptologic by solving $x^k \equiv E(x_i) \bmod m$.

3. Using the system parameter d, $(1 < d \leq k)$, to represent the plain text, we know the security and adaptability are strengthened. Moreover, there exists a $d > 2$ representing the plain text in the system for which (2) is achieved.

4. If $k = 2$, we still have obtained a probabilistic encryption system different from the Goldwasser-Micali system. Such a system has the ability to deflect an attack based on the solvability of $x^2 \equiv E(x_i) \bmod m$.

At the same time, we also note that, using Eisenstein's Law of Reciprocity [8], we can propose some public-key cryptosystems based on the k^{th}-power residue over certain rings of algebraic integers. For example, in [9] we proposed a type of public-key cryptosystem using a cubic reciprocity law over the Eisenstein ring $Z[\omega]$, whose security is based on the difficulty of factoring "integers" over the ring of algebraic integers. Since the problem of factorization of "integers" over the ring of algebraic integers includes the problem of factoring rational integers, it generalizes the systems which are based on the factorization of large integers and thus has increased security.

Because the factorization into rational primes over the ring of algebraic integers is also very complicated in general, there can be said to be no effective method (by comparison with the already known difficulty of factoring rational integers) to break the more general system based on the factorization of large integers over the ring of algebraic integers.

Bibliographic References

1. W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Info. Theo. 22 (1976), 644-645.

2. R. L. Rivest, A. Shamir, and L. Adleman, A Method for obtaining digital signature and public-key cryptosystems, Commun. ACM 20 (1978), 120-126.

3. S. Goldwasser and S. Micali, Probabilistic encryption and how to play mental poker keeping secret all partial information, Proc. 14th ACM Symp. on the Theo. of Computing (1982), 365-377.

4. R. C. Merkle and M. E. Hellman, Hiding information and signatures in trapdoor knapsacks, IEEE Trans. Info. Theo. 24 (1978), 525-530.

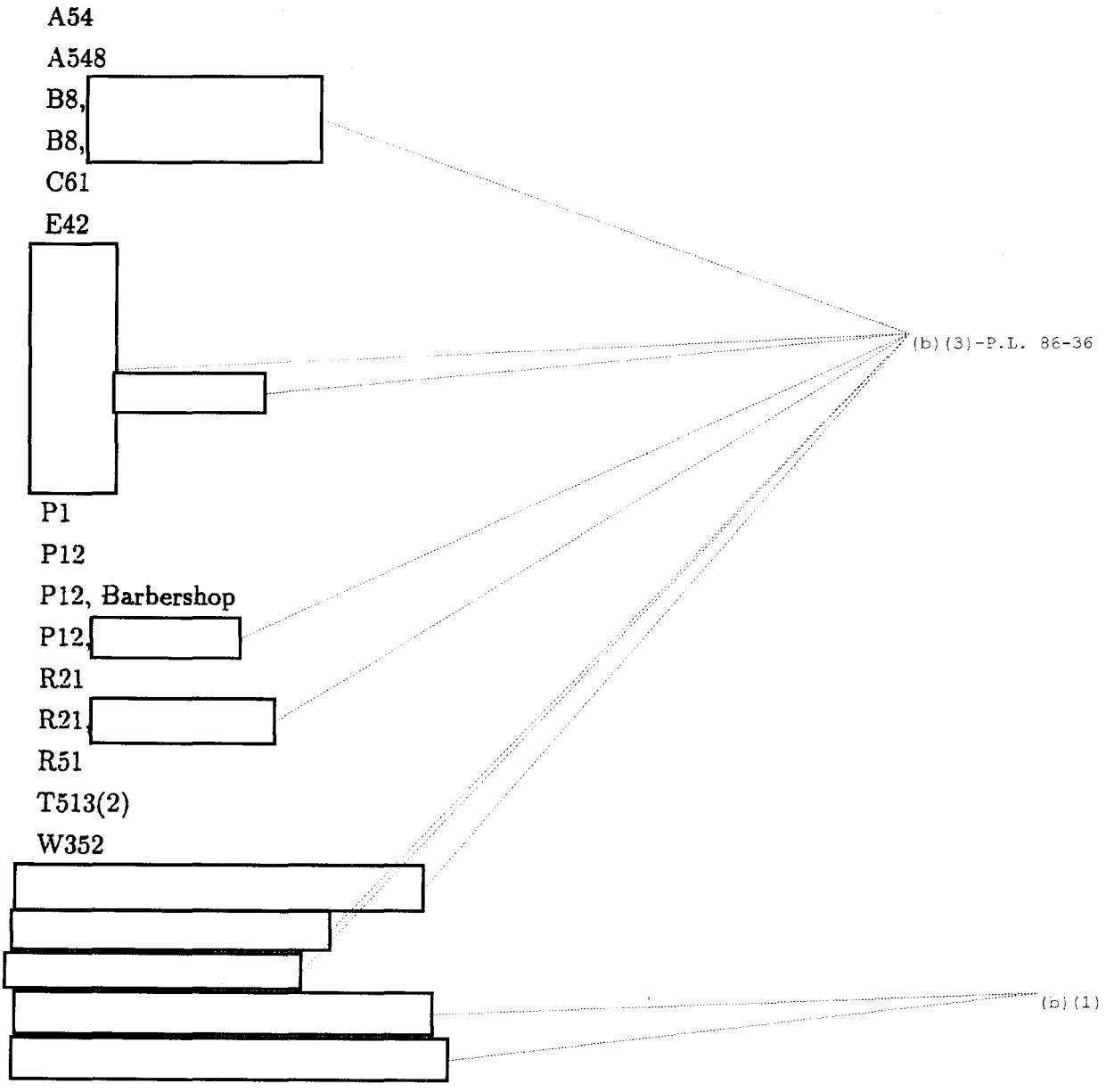
5. Zhen-fu CAO, Rui LIU, Breaking NP knapsack systems, High School Applied Math. J. 4 (1989), 1-5 (in Chinese).

6. A. Shamir, A Polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem, Proc. IEEE Symp. Found. of Compu. Sci. 23 (1982), 145-152.

7. Zhen-fu CAO, Some new types of public-key cryptosystems, Electronics Journal 16 (1988), 120-121 (in Chinese).

8. K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer-Verlag, 1982.

9. Zhen-fu CAO, A type of public-key cryptosystem over the Eisenstein ring $Z[\omega]$, Proc. Third National Cryptologic Study Convention (1988, Xian), 178-186.


A54
A548
B8,
B8,
C61
E42
P1
P12
P12, Barbershop
P12,
R21
R21,
R51
T513(2)
W352
(b)(3)-P.L. 86-36
(b)(1)