Trapdoor Rings And Their Use In Cryptography.

V.Varadharajan

Dept. of Elec. and Electronic Eng.,

Plymouth Polytechnic,

Drake Circus, PLYMOUTH PL4 8AA,

U.K.

Abstract

This paper examines possible trapdoor structures which can be used to design public key cryptosystems based on the factorization problem.Some examples of such finite trapdoor systems which might serve as a basis for an extended RSA cryptosystem are proposed.

Introduction

Recently much research work has been carried out in the field of asymmetric or public key cryptosystems [1,2,3],which allow two users to communicate securely over an insecure channel without any prearrangement.They are classified as asymmetric because the sender and the receiver employ two different keys to encrypt and decrypt a message. Separating the enciphering and deciphering capabilities allows secrecy to be maintained without keeping the encrypting key hidden as it is no longer used in deciphering.The decrypting key is kept private and there is no need for anyone to communicate his decryption key to anyone else.The concept of a public key cryptosystem is illustrated in figure 1.User i

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 369-395, 1986.

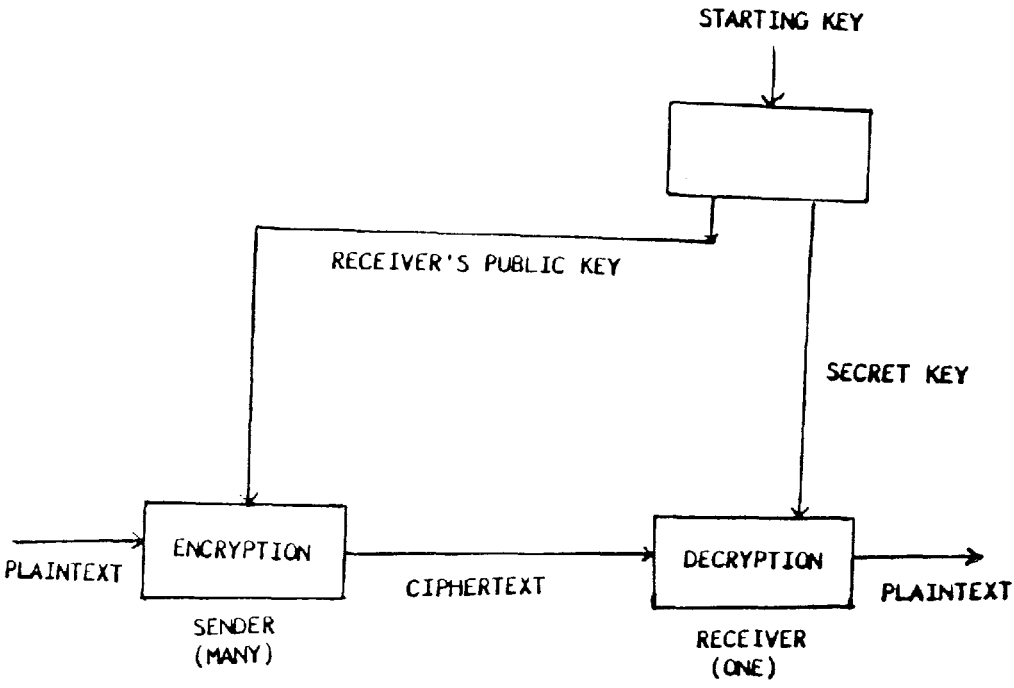

Fig.1 - Public key cryptosystem

encrypts the message M using the publicly known encrypting key of user j and sends the cipher to user j over an insecure channel.Only the user j will be able to decrypt the cipher to recover M as he is the only one who knows his secret decryption key.

The encryption (E) and decryption (D) algorithms in such a system have,in general,the following properties:

a. Deciphering the enciphered form of a message M yields M,that is, D(E(M))=M.

b. Both E and D are easy to compute.

c. By publicly revealing E,the user does not reveal an easy way to compute D.This means that only the receiver can decrypt the messages encrypted with E or compute D efficiently.

A major implication of the public key cryptosystem is that it eliminates the need for a secret transferral of keys as in the case of conventional symmetric cryptographic algorithms which employ the same key for both encryption and decryption.Furthermore,the public key algorithms can be used in conjunction with the symmetric algorithms to distribute the secret key.This can be seen as follows:
User i can encrypt the secret key in a symmetric system using the public key of user j and then send it to user j over an insecure channel.Because the deciphering key is only known to user j, he is the only one who can decrypt the cipher and obtain the secret key.Now users i and j can have a secure conversation using a symmetric algorithm with the transferred secret key.
Note that in this arrangement the sole purpose of the public key system is to distribute the secret key required for the symmetric algorithm.

Another implication of the public key cryptosystem is that it is possible to 'sign' messages in a way that is unforgeable but easily verifiable.This can be accomplished provided the enciphering and deciphering procedures can be used in either order.To sign a message, a user i operates first on the message with his secret decryption key and then with the public key of user j to produce the cipher.The user j recovers the message by operating on the cipher,first with his secret decryption key and then with the public key of user i.Since only user i knows his secret decryption key, only user i could have created the cipher which produces the correct message when his public key is applied to it.Thus it is possible to obtain a digital signature feature [3] provided the encryption and decryption algorithms satisfy an additional property (d) given by

d. Enciphering the deciphered form of a message M yields M,that is,E(D(M))=M.

For a public key system to be secure, it should be computationally infeasible for the cryptanalyst to determine the secret decryption key from the publicly known parameters of the encryption and decryption procedures and the encryption key.Such systems are constructed using 'trapdoor one-way functions'

Definition: A function f is said to be a one-way function if it is easy to compute $y=f(x)$ for all x but difficult to compute $x=f^{-1}(y)$ for almost all y.

Note that the phrase 'almost all y' is necessary because a table of some of the values of f(x) can be stored and if y happens to belong to this table the corresponding x can be easily determined.The above definition does not provide an absolute sense in which a function is one-way as it depends on the computational resources available.A precise definition of a one-way function depends on a specific measure of complexity as the difficulty of computing the inverse function varies with time and technology.The complexity measures are often defined in terms of time or storage required to compute the inverse.Computational tasks which require of the order of 10^{50} operations or 10^{50} storage elements are generally considered to be infeasible [4].It is possible to construct one-way functions $y=f(x,k)$ where the difficulty of computing y increases linearly with k but that of computing x increases exponentially with k.In such a case it is possible to increase k to such an extent that computation of the inverse requires the limits mentioned above.However one-way functions cannot be used directly to design a public key system as the legal receiver needs to decrypt the cipher y easily for all y.

Definition: A 'trapdoor one-way function' is a one-way function with the additional property that if certain specific information (the trapdoor) employed in the design of the function is known then it is easy to compute the inverse function.

That is,given the secret decryption key (trapdoor) $f^{-1}(y)$ can be easily calculated.

A well known public key cryptosystem which has survived many cryptanalytical attacks is the Rivest-Shamir-Adleman system (RSA) [2], which is based on the difficulty of factoring a large rational integer into its primes.The system designer chooses two distinct primes p and q and publishes the product m=pq.The product m is assumed to be so large that factoring it is beyond all projected computation capabilities.For instance,if m is chosen to be 200 digit decimal integer,then it will require of the order of 10^{23}operations using the best known factoring algorithm [2].The encryption procedure raises the message x,1<x<m, to the e-th power modulo m and the decryption is performed by raising the cipher y to the d-th power modulo m.

Encryption : $y \equiv x^e \pmod m$

Decryption : $x \equiv y^d \pmod m$

The public encryption key is (e,m) and the secret decryption key is (d,m).The coding exponents e and d are chosen to be multiplicative inverse of each other modulo $\phi(m)$, where ϕ is the Euler totient function.

$$ed = 1 \pmod{\phi(m)} \qquad (1)$$

If the cryptanalyst can determine $\phi(m)$,then he can obtain the decoding exponent d by solving (1).If m can be easily factorized to p and q, then the cryptanalyst can find $\phi(m)$ and d and hence crack the system.

In this article, some algebraic structures suitable for use in the design of RSA type factorization-based, trapdoor systems are investigated.

Trapdoor Rings

Assume R is a finite ring with unity which is associative but not necessarily commutative. Suppose that members of the ring R are used as messages and that $r \in R$ is enciphered as r^e where e is the published encrypting exponent.

The trapdoor property can be stated as follows:

there exists some integer $n>0$ such that $r^{n+1} = r$ for all $r \in R$.

These rings are to be referred to as trapdoor rings.

For instance, in the ring of integers modulo a prime number p, $R = Z/pZ$, $r^p = r$ for all $r \in R$. More generally, if $R = F_q = GF(q)$, the field of q elements where q is a prime power (p^k), then $r^q = r$ for all $r \in R$.

Consider any two such trapdoor rings R and S and construct the direct sum $R \oplus S$ consisting of vectors (r,s) with $r \in R$ and $s \in S$. These vectors are added and multiplied componentwise. That is, (r,s) + (r',s') gives (r+r',s+s') and (r,s) . (r',s') is (rr',ss'). These rules make $R \oplus S$ into another trapdoor ring, say T. The number of elements of T is equal to the product of the number of elements in rings R and S. Suppose that $r^{m+1} = r$ for all $r \in R$ and $s^{n+1} = s$ for all $s \in S$. Then $r^{m+N} = r^N$ for all $N \geq 1$. Similarly, $s^{n+N} = s^N$ for all $N \geq 1$. In particular, $r^{1+km} = r$ for all $k \geq 1$ and $s^{1+kn} = s$ for all $k \geq 1$. Hence $r^{1+lmn} = r$ and $s^{1+lmn} = s$ for all $l \geq 1$. Hence $t^{1+lmn} = t$ for all $t \in T$, $l \geq 1$, and so T is a trapdoor ring.

This above process can be applied repeatedly by taking vectors of

arbitrarily many components, each taken from some finite field.Considering finite fields F_{q_i} for $1 \leq i \leq j$ where q_i's can be the same or different,the trapdoor ring R consists of all vectors $x = (x_1,\ldots,x_j)$ where $x_i \in F_{q_i}$, $1 \leq i \leq j$. The ring consists of $q_1 \ldots q_j$ elements and the equality $r^{n+1} = r$ is obeyed for all $r \in R$,where n is equal to $(q_1-1)\ldots(q_j-1)$ or any multiple of it.

There are many finite rings which are not trapdoor rings.Consider,for instance,$R = Z/p^2Z$ where p is a prime. Then $p^2 = 0 = p^3 = \ldots$ in ring R but $p \neq 0$ in R.So the property that $p^{n+1} = p$ is not satisfied for any $n > 0$. However if we take an integer k to be a square free positive integer,say, $k = p_1 \ldots p_j$ where all p_i's are distinct primes then the ring $R = Z/kZ$ is a trapdoor ring and in fact it can be regarded as a direct sum of $F_{p_1} \oplus \ldots \oplus F_{p_j}$ as described above. If $j = 2$, then this becomes the standard trapdoor ring used by the RSA cryptosystem.

Classification Theorem

Let R be any trapdoor ring.Then

a. R has a 1.

b. R is commutative.

c. R is isomorphic to $F_{q_1} \oplus \ldots \oplus F_{q_j}$ for certain finite fields.

(Two rings R and S are isomorphic to each other if there exists a function $f : R \longrightarrow S$ which is one-to-one and onto and satisfies $f(r_1+r_2) = f(r_1) + f(r_2)$, $f(r_1r_2) = f(r_1)\,f(r_2)$ for all $r_1, r_2 \in R$.)

The proof relies on the use of Wedderburn's structure theory [5] for semisimple rings.The main steps of the argument are as follows :

1. The ring R is trapdoor implies that R has no nilpotent elements except 0.(An element x is said to be nilpotent if $x^a = 0$ and $x^{a-1} = 0$ for some $a > 0$)

2. A finite ring without non-zero nilpotent elements must have a 1 [5].

3. A finite ring with 1 and lacking nilpotents ($\neq 0$) is a direct sum of matrix rings with entries in a division algebra (skew field) - Wedderburn's theorem.

4. If any of these matrices is not 1x1,then there will be non-zero nilpotent elements in R.

5. Hence R is a direct sum of finite skew fields.

6. A finite skew field is necessarily commutative (Wedderburn-Witt theorem).

Hence the only finite trapdoor rings are of the type described above upto isomorphism.

Other possible trapdoor structures

Instead of using rings,we only need a system S in which an associative multiplication is defined,satisfying

1. For all $a,b \in S$, $ab \in S$

2. For all $a,b,c \in S$, $a(bc) = (ab)c$

Such a system is called a semigroup.If S is a semigroup with a 1 satisfying $a.1 = 1.a = a$ for all $a \in S$ then S is said to be a monoid. Further if a monoid S has the additional property that there is a unique corresponding $b \in S$ such that $ab = ba = 1$ then S is said to be a group.In a finite group G with n elements,every $g \in G$ satisfies $g^n = 1$, $g^{n+1} = g$.

Hence a finite group of order n can be used to construct trapdoor

systems.On the other hand,not all semigroups can be used to form trapdoor systems. Semigroups with the property that $a^{n+1} = a$ for all $a \in S$ are possible candidates.A more formal way of expressing this constraint would be : a semigroup S can be used provided it is completely regular.
Let us now consider some examples of finite systems that might serve as a basis for a generalized RSA cryptosystem.

Ring of Matrices

If the ring of all nxn matrices M_n over the ring R=Z/mZ , where $m = \prod_{i=1}^{s} p_i^{r_i}$,(p_i's are primes), is considered, then the ring M_n contains nilpotent elements when n > 1. This problem can be overcome by restricting the message space thereby avoiding nilpotent elements. In this paper, we consider three such subsets namely, the set of non-singular matrices over Z/mZ,the set of upper triangular matrices over Z/mZ and the set of orthogonal matrices over Z/mZ.

Let us first consider the multiplicative group formed by the non-singular matrices of order n over Z/mZ. The order of the group, N_m, is given by

$$N_m = \prod_{i=1}^{s} N_{p_i^{r_i}} \qquad (2)$$

where $N_{p_i^{r_i}}$ denotes the order of the group formed by non-singular matrices over $Z/p_i^{r_i}Z$.
It is well known [6] that the order of the group formed by non-singular matrices over Z/pZ is given by

$$N_p = (p^n-1)(p^n-p) \ldots (p^n-p^{n-1}) \qquad (3)$$

To evaluate N_{p^r}, in general, let θ be the homomorphism mapping an nxn matrix A over $Z/p^{r+1}Z$ to A', a matrix over Z/p^rZ, via $a_{ij} \pmod{p^{r+1}} \longrightarrow a_{ij} \pmod{p^r}$. This induces a surjective homomorphism θ' between the linear groups formed by these matrices. That is,

$$\theta' : GL_n(Z/p^{r+1}Z) \longrightarrow GL_n(Z/p^rZ)$$

Using group theory [7],

$$\frac{GL_n(Z/p^{r+1}Z)}{\text{Kernel } \theta'} \cong GL_n(Z/p^rZ)$$

where $\cong$ denotes isomorphic to.

The kernel consists of the set of matrices which are mapped to the identity matrix I (mod p^r), i.e.

$$a_{ii} \equiv 1 \pmod{p^r} \quad \text{for } 1 \leq i \leq n \tag{4}$$

$$a_{ij} \equiv 0 \pmod{p^r} \quad \text{for } i \neq j \tag{5}$$

There are p possibilities for each of the equations (4) and (5) giving rise to p^{n^2} possibilities. Therefore using group theory, the order (denoted by symbol #) is given by

$$\begin{aligned} \# GL_n(Z/p^{r+1}Z) &= p^{n^2} \# GL_n(Z/p^rZ) \\ &= p^{rn^2} \# GL_n(Z/pZ) \\ &= p^{rn^2} N_p \end{aligned}$$

Thus using (3),

$$N_{p_i^{r_i}} = p_i^{(r_i-1)n^2}(p_i^n-1) \ldots\ldots (p_i^n - p_i^{n-1}) \qquad (6)$$

Substituting (6) into (2) gives the order N_m.

Now as in the RSA cryptosystem, if m is made to be the product of two distinct primes p and q, then the expression for N_m simplifies to

$$N_m = N_p \; N_q$$
$$=(p^n-1)\ldots(p^n-p^{n-1})(q^n-1)\ldots(q^n-q^{n-1})$$

A public key system can therefore be constructed using (e,m,n) as the public encryption key and (d,m,n) as the secret decryption key. The coding exponents e and d are determined using

$$ed \equiv 1 \pmod{N_m} \qquad (7)$$

A message $M \in GL_n(Z/mZ)$ obeys

$$M^{N_m} \equiv I \pmod{m}$$

The encryption and decryption procedures can therefore be given by

$$C \equiv M^e \pmod{m}$$

and

$$M \equiv C^d \pmod{m}$$

respectively, where $M, C \in GL_n(Z/mZ)$.

Although the order N_m can be used in finding e and d as in (7), in practice, it is often desirable to find the exponent, EXP, of the group, that is, the least integer greater than zero such that

$$M^{EXP} \equiv I \pmod{m} \qquad M \in GL_n(Z/mZ)$$

The exponent of the group can be shown to be [8,9].

$$\left.\begin{aligned} &\text{EXP} = \text{lcm}\ \{v_1, \ldots\ldots, v_s\} \\ &\text{where} \\ &\qquad v_i = p_i^{r_i - 1}\ (w_i) \\ &\text{and} \quad w_i = p_i\ \text{lcm}\ (p_i - 1, p_i^2 - 1, \ldots\ldots, p_i^n - 1) \end{aligned}\right\} \qquad (8)$$

(assuming p_i is greater than n for all i).

As the expression for the order N_m (and the exponent EXP) depend on the prime factors of m, it can be used to design a public key cryptosystem by choosing m to be a large integer.

Alternatively, let us now consider the set of upper triangular matrices as a possible choice for the message space. If the diagonal entries are made unity, to ensure that the matrix is invertible over any modulus, then the order of the group formed by such matrices over Z/mZ is equal to ord = $m^{n(n-1)/2}$. That is, the order does not depend on the prime factors of m and hence this cannot be used as a public key system. A conventional cyrptosystem can be designed where the secret key is (e,d,m,n) and the exponents e and d are calculated using $ed \equiv 1 \pmod{\text{order}}$.

However, if the message space is altered to contain upper triangular matrices with diagonal entries relatively prime to m, then such matrices are again invertible modulo m. Further, in practice, as m is a product of large prime numbers, the choice of diagonal elements is almost arbitrary provided they are chosen to be realtively small integers.

The order of the group formed by such matrices is determined as follows:-

Considering a nxn matrix, it is required that all the n diagonal entries must be coprime to m. The number of integers less than m and coprime to m is given by the Euler totient function $\phi(m)$. The remaining $n(n-1)/2$ superdiagonal entries of the matrix may take any value modulo m. Therefore, the order is equal to $m^{n(n-1)/2}\{\phi(m)\}^n$. The vital difference between this order and the one calculated above is that now the order of the group is dependent on the prime factors of m. Hence the modulus m needs to be factorized before the decryption exponent d can be calculated using $ed \equiv 1 \pmod{\text{order}}$. As for the set of non-singular matrices, the exponent of the group formed by such upper triangular matrices can be used instead of the order in finding e and d. The exponent of the group is shown to be equal to [8,9].

$$EXP' = \text{lcm}\ \{\phi(p_1^{r_1})p_1^{r_1}, \ldots\ldots\ldots, \phi(p_s^{r_s})p_s^{r_s}\}$$

where

$$m = \prod_{i=1}^{s} p_i^{r_i}$$

Finally, one can also use the special set of non-singular matrices, namely the set of orthogonal matrices, as the message space of the matrix based RSA system. The order of the group formed by nxn orthogonal matrices over Z/pZ has been worked out by MacWilliams [10].

For odd n, i.e. $n = 2a + 1$ for some integer a, the order is given by

$$2p^a \prod_{i=0}^{a-1} (p^{2a} - p^{2i})$$

For even n, i.e. n = 2a, the order is given by

$$2(p^a-1)\prod_{i=0}^{a-1}(p^{2a} - p^{2i}) \qquad \text{if } -1 \text{ is a square (mod p)}$$

and

$$2(p^a + (-1)^{a+1})\prod_{i=1}^{a-1}(p^{2a} - p^{2i}) \qquad \text{if } -1 \text{ is a non-square (mod p)}$$

Using the Chinese Remainder Theorem, the order of the group formed by orthogonal matrices over Z/mZ where m=pq, a square free integer is equal to the product.

(order of orthogonal matrices over Z/pZ) x (order of orthogonal matrices over Z/qZ).

As the factorization of the modulus m is required to calculate the order, this set can be used in the matrix based public key system.

Thus it can be seen that the RSA system can be generalised to matrix rings provided the message space is restricted to avoid nilpotent elements. From a practical implementation point of view, the upper triangular matrices with invertible diagonal elements seems to be the better candidate as the messages can be constructed in an almost arbitrary manner. In the case of non-singular matrices, an additional procedure to find the determinant of the message matrix is required. However, this problem can be overcome by constructing the message matrix as a product of upper triangular and lower triangular matrices as follows:

Let U be an upper triangular matrix and L be a lower triangular matrix with unit diagonal over Z/mZ. The elements other than the diagonal ones in U and L can be arbitrarily chosen modulo m. As both U and L

are invertible over Z/mZ, their product M=LU is also invertible over Z/mZ. Further, the non-commutativity property of matrices ($LU \neq UL$ in general) ensures that the crytpanalyst still needs to factorize m to be able to calculate the decrypting exponent d. This is in contrast to the case of just the upper triangular matrices with unit diagonal mentioned earlier. This is because $M^e = (UL)^e \neq U^eL^e$. Thus although $U^{ed_1} \equiv U \pmod{m}$ and $L^{ed_1} \equiv L \pmod{m}$ where $ed_1 \equiv 1 \pmod{ord}$, $M^{ed_1} \not\equiv M \pmod{m}$ but $M^{ed} \equiv M \pmod{m}$ where $ed \equiv 1 \pmod{N_m \text{ or } E \times P}$. The receiver can recover the matrices L and U uniquely given the matrix M. Furthermore, the above procedure also applies if one of U or L is a triangular matrix with invertible diagonal elements and the other triangular matrix with unit diagonal.

This extended RSA system using matrix messages has been simulated on a Prime Computer [8]. The encryption and the decryption of message matrices have been performed using the Square and Multiply technique [11].

Two points are worth mentioning regarding this extended system. Firstly, it is seen that a non-square free modulus can be used with this system which is not possible with the RSA system over integers. That is, powers of primes can be used to form the modulus m. Secondly, the use of a matrix as a message allows large amounts of data to be processed within one encryption/decryption cycle. Whether this is an advantage depends upon the ease with which matrix manipulation can be carried out in real time.

Ring of Polynomials

Consider the factorization trapdoor system in another ring of special interest, namely the ring of polynomials R[x], which consists of polynomials with coefficients in an arbitrary ring R.

Let $R \cong Z/pZ$ and $f(x)$ be a polynomial in $Z/pZ[x]$ of degree s whose factorization is given by

$$f(x) = g_1(x) \ldots g_r(x) \pmod{p}$$

where $g_i(x)$, $1 \leq i \leq r$, are distinct irreducible polynomials over Z/pZ of degree s_i respectively.

Consider the multiplicative group formed by polynomials over Z/pZ of degree less than s and relatively prime to $f(x)$. The order of the group, denoted using the Euler function $\phi_p(f(x))$ is evaluated as follows:

$\phi_p(f(x))$ is equal to the number of invertible elements, that is, units in the residue ring $\frac{Z/pZ[x]}{f(x)}$. This ring is isomorphic to $Z[x]/(p,f(x))$ and can be regarded as a direct sum of finite fields as

$$Z[x]/(p,f(x)) \cong Z[x]/(p,g_1(x)) \oplus \ldots\ldots \oplus Z[x]/(p,g_r(x))$$

where $Z[x]/(p,g_i(x))$ is the finite (Galois) field $GF(p^{s_i})$, s_i being the degree of $g_i(x)$.

Hence

$$\text{units of } \left(\frac{Z[x]}{(p, f(x))}\right) = \text{units of } \left(\frac{Z[x]}{(p, g_1(x))}\right) \times \ldots \quad \times \text{units of } \left(\frac{Z[x]}{(p, g_r(x))}\right)$$

$$= (p^{s_1} - 1) \ldots\ldots (p^{s_r} - 1)$$

Hence

$$\phi_p(f(x)) = \prod_{i=1} (p^{s_i} - 1) \qquad (9)$$

A public key system in $Z[x]/(p,f(x))$ can therefore be designed as follows [12] : The message space consists of polynomials $\{m(x)\}$ of degree less than s over Z/pZ. The public encryption key is $(e,p,f(x))$ and the secret decryption key is $(d,p,f(x))$ where the coding exponents e and d are calculated using

$$ed \equiv 1 \pmod{\phi_p(f(x))} \qquad (10)$$

The encryption procedure raises the message polynomial $m(x)$ to the power e using

$$c(x) \equiv (m(x))^e \mod (p,f(x))$$

The decryption procedure is given by

$$m(x) \equiv (c(x))^d \mod (p,f(x))$$

As the order $\phi_p(f(x))$ is dependent on the degrees of the irreducible factors of the modulus polynomial $f(x)$, this scheme provides the trapdoor property.

However, the above scheme is not as secure as the RSA system over rational integers or the matrix based RSA system proposed earlier. This is because the security of this system is dependent on the difficulty of factorizing a composite polynomial into its irreducible factors over a finite field, which in general is not a hard problem in sharp contrast with the factorization problem of a large integer.

Berlekamp [13] proposed an efficient algorithm for factoring polynomials in Z/pZ. For large primes p, Knuth [11] has suggested some modifications to the Berlekamp's procedure. Once the degrees of the irreducible factors are found, the crtypanalyst can determine the order $\phi_p(f(x))$ and then calculate the secret decoding exponent using (10). Furthermore with this scheme, the same decoding exponent d works for all sets of $g_i(x)$ for i = 1 to r, with same degrees s_i.

The security of this system can be increased if it is implemented in the ring Z[x]/(m,f(x)) where m is the product of distinct prime integers $m = \prod_{i=1}^{t} p_i$ and f(x) is a square free composite polynomial as before.

The message space then consists of polynomials {m(x)} of degrees less than s with coefficients in Z/mZ. Using the Chinese Remainder Theorem, the ring Z[x]/(m,f(x)) is isomorphic to the direct of sum of rings given below

$$\frac{Z[x]}{(m, f(x))} \cong \frac{Z[x]}{(p_1, f(x))} \oplus \cdots \oplus \frac{Z[x]}{(p_t, f(x))}$$

The order of the multiplicative group formed by polynomials of degrees less than s and relatively prime to f(x) is equal to the number of units in Z[x]/(m,f(x)) and is given by $\phi_m(f(x))$

$$\phi_m(f(x)) = \text{units of } \left(\frac{Z[x]}{(m, f(x))}\right)$$

$$= \text{units of } \left(\frac{Z[x]}{(p_1, f(x))}\right) \times \cdots \times \text{units of } \left(\frac{Z[x]}{(p_t, f(x))}\right)$$

Hence

$$\phi_m(f(x)) = \prod_{i=1}^{t} \phi_{p_i}(f_i(x))$$

where

$$f_i(x) \equiv f(x) \pmod{p_i} \qquad 1 \leq i \leq t \ .$$

Let the factorization of $f_i(x)$ be

$$f_i(x) = \prod_{j=1}^{n_i} g_{ij}(x) \pmod{p_i} \qquad (11)$$

where the degree of irreducible polynomial $g_{ij}(x)$ over Z/p_iZ is s_{ij}. The upper limit in the product term in (11) goes up to n_i as it is a function of to which prime p_i the polynomial $f(x)$ is being factored. This is because in general $f(x)$ mod p_i will have some n_i distinct irreducible factors as i varies.

But using (9)

$$\phi_{p_i}\left(f_i(x)\right) = \prod_{j=1}^{n_i} \left(p_i^{s_{ij}} - 1\right)$$

Hence,

$$\phi_m\left(f(x)\right) = \prod_{i=1}^{t} \prod_{j=1}^{n_i} \left(p_i^{s_{ij}} - 1\right)$$

The order now depends not only on the degrees of the irreducible factors but also on the prime divisors of modulus m. Thus the cryptanalyst needs to factorize both m and f(x) and this gives rise to a system which is at least as strong as the corresponding RSA system over the integers. Furthermore, from cryptography point of view, it is required that both f(x) and m must be square free to avoid nilpotent elements and enable proper decryption. In this respect, it differs from the matrix RSA system described earlier. This system has also been simulated on the Prime Computer[8].

Ring of Algebraic Integers

We now consider the design of public key systems in some algebraic number fields based on factorization trapdoor.

A number θ is said to be an algebraic number [14] if it satisfies a polynomial equation

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

where the coefficients a_i are rational numbers, Q.
If the equation has rational integer coefficients and it is monic, then θ is said to be an algebraic integer. If θ is algebraic over Q, then the field $K = Q(\theta)$ is defined to be the smallest extension field containing both Q and θ. That is, it consists of numbers of the form

$$a_0 + a_1\theta + a_2\theta^2 + \ldots + a_n\theta^n$$

where a_i are rational numbers.

The subset of the field K consisting of algebraic integers forms a ring D, called the ring of algebraic integers in K. In general, D is not a unique factorization domain. Factorization of elements in D is unique if and only if every irreducible in D is also a prime, that is, if and only if D is a principal ideal domain (PID). The rings where unique factorization of integers fails correspond to non-principal ideal domains. In such domains, there are irreducibles which are not primes and they generate principal ideals which are not prime ideals but factorize into non-principal ideals [15]. We only consider the design of the factorization trapdoor systems in PIDs. Unless otherwise stated, from now on D is assumed to be a PID.

Let m be a square free integer in some ring D and its factorization be

$$m = \prod_{i=1}^{r} \pi_i$$

where π_i are irreducibles or primes in D.

Then, using the Chinese Remainder Theorem, the residue class ring is isomorphic to the direct sum of finite fields as

$$D/\langle m \rangle \cong D/\langle \pi_1 \rangle \oplus \cdots \oplus D/\langle \pi_r \rangle$$

where $\langle \pi \rangle$ denotes the principal ideal generated by π. The order of the group formed by invertible residue classes modulo the ideal $\langle m \rangle$ is given by $\Phi \langle m \rangle$, which is similar to the Euler function ϕ for rational integers.

$$\Phi\langle m \rangle = \Phi\langle \pi_1 \rangle \cdots \Phi\langle \pi_r \rangle \qquad (12)$$

For a prime π_i,

$$\Phi\langle \pi_i \rangle = N\langle \pi_i \rangle - 1 \qquad (13)$$

where $N\langle \pi_i \rangle$ denotes the norm of the ideal $\langle \pi_i \rangle$, the number of residue classes modulo the ideal $\langle \pi_i \rangle$.

A public key system is therefore possible as the order depends on the prime factors of m. Such a scheme is illustrated by considering a simple quadratic field K = Q(i). The ring of integers D = Z[i] consists of elements of the form $\{a + bi \mid a,b \in Z\}$ and is commonly known as the ring of Gaussian integers. Now m is a composite integer in Z[i] and its factors π_i, $1 \leq i \leq r$, are primes in Z[i]. To be able to calculate $\Phi\langle m \rangle$, it is necessary to find $N\langle \pi_i \rangle$, $1 \leq i \leq r$, (see (12) and (13)).

The norm $N\langle\pi_i\rangle$ is a rational integer and is equal to

$$N\langle\pi_i\rangle = \pi_i \overline{\pi_i}$$

where $\overline{\pi_i}$ is the complex conjugate of π_i .

Let the prime decomposition of $N\langle\pi_i\rangle$ in Z be

$$N\langle\pi_i\rangle = p_1 \cdots p_t$$

where p_i are distinct primes in Z.

Then, as $\pi_i \mid N\langle\pi_i\rangle$, $\pi_i \mid p_1 \ldots . p_t$. That is, π_i divides one of the primes p_j. It cannot divide two primes p_j and p_k. If so, then it is possible to find two integers a and b using Euclid's algorithm such that $ap_j + bp_k = 1$. As $\pi_i \mid p_j$ and $\pi_i \mid p_k$, $\pi_i \mid 1$. So π_i is a unit, not a prime which is contrary to the assumption. Thus every Gaussian prime π_i divides only one rational prime p_i. Hence $N\langle\pi_i\rangle$ divides Np_i. But $Np_i = p_i^2$. Therefore, $N\langle\pi_i\rangle = p_i$ or p_i^2. It can be shown that [14], if $p_i \equiv 1 \pmod 4$ then $N\langle\pi_i\rangle = p_i$ whereas if $p_i \equiv 3 \pmod 4$ then $N\langle\pi_i\rangle = p_i^2$. Thus the order $\phi\langle m\rangle$ is given by

$$\phi\langle m\rangle = \prod_{i=1}^{r} N\langle\pi_i\rangle - 1$$

where

$$N\langle\pi_i\rangle = \begin{cases} p_i & p_i \equiv 1 \pmod 4 \\ p_i^2 & p_i \equiv 3 \pmod 4 \end{cases}$$

The encryption and decryption coding exponents e and d can be calculated using

$$ed \equiv 1 \pmod{\varphi\langle m\rangle} \qquad (14)$$

The messages are represented using the residue classes modulo the ideal $\langle m\rangle$ and there are $N\langle m\rangle$ such residue classes.

Case 1

First consider the case where the primes π_i which form m divide rational primes p_i of the form $p_i \equiv 1 \pmod 4$. Then the norm is a square free rational integer given by

$$N\langle m\rangle = \prod_{i=1}^{r} N\langle \pi_i\rangle$$

$$= \prod_{i=1}^{r} p_i$$

The residue class ring $Z[i]/_{\langle m\rangle}$ is isomorphic to the direct sum of finite fields $Z[i]/_{\langle \pi_i\rangle}$, $1 \le i \le r$. The field $Z[i]/_{\langle \pi_i\rangle}$ contains p_i elements. Therefore, one standard method of representing the messages mod $\langle m\rangle$ would be to use the integers in the ring $Z/N\langle m\rangle Z$, that is, 0 to $N\langle m\rangle - 1$. This is similar to the message space of the RSA system over rational integers. The encryption and decryption processes are carried out using $C \equiv M^e \pmod{N\langle m\rangle}$ and $M \equiv C^d \bmod N\langle m\rangle$ and $(e, N\langle m\rangle)$ is the public key.

Now consider the situation where the message space still consists of the integers in $Z/N\langle m\rangle Z$ but the encryption and decryption procedures are calculated modulo m, $m \in Z[i]$. Let $m = a+bi$ and the message be M in $Z/N\langle m\rangle Z$. Then encryption gives, say,

$$C \equiv M^e \equiv g + hi \pmod{(a+bi)}$$

Decryption produces

$$(g+hi)^d \equiv k + li \pmod{(a+bi)}$$

That is, the recovered message M is equal to k + li

$$M \equiv k + li \pmod{(a+bi)} \qquad (15)$$

Conjugating both sides of (15)

$$M \equiv k - li \pmod{(a-bi)}$$

Using Chinese Remainder Theorem, the original M can be obtained as

$$M \equiv \alpha_1(k-li) + \alpha_2 (k+li) \pmod{(a+bi)(a-bi)}$$

where $\alpha_1 + \alpha_2 = 1 \qquad \alpha_1, \alpha_2 \in Z[i]$.

Case 2

If the primes Π_i which form m divide rational primes p_i of the form $p_i \equiv 3 \pmod 4$, then the N<m> is a non-square free rational integer given by

$$N\langle m\rangle = \prod_{i=1}^{\tau} p_i^2$$

In this case, although $Z[i]/_{\langle \Pi_i \rangle}$ is a finite field of p_i^2 elements, one cannot represent the residue classes modulo $\langle \Pi_i \rangle$ using the integers Z/p_i^2Z as the latter does not form a finite field. On the other hand, one can represent the messages in the form M = x+iy where $0 < x,y \leq \left|\sqrt{N\langle m\rangle}\right| - 1$, thus giving rise to N<m> distinct residue classes modulo <m>.

Encryption is performed by raising the message M to the power e and reducing the coefficients modulo $\left|\sqrt{N\langle m\rangle}\right|$. That is, if M = x + iy, then

$$C \equiv M^e \equiv (x+iy)^e \pmod{\langle m\rangle}$$
$$\equiv g \left(\bmod \left|\sqrt{N\langle m\rangle}\right|\right) + h \left(\bmod \left|\sqrt{N\langle m\rangle}\right|\right) i$$

A similar procedure is carried out in decryption.

Case 3

If m factorizes into primes π_i some of which divide rational primes $p \equiv 1 \pmod 4$ and others divide rational primes $p \equiv 3 \pmod 4$, then it can be shown [8] that the cryptanalyst can easily partly factorize m and hence reduce the difficulty of breaking the system. Therefore from cryptography point of view, this case should not be used.

The security of the public key system in Z[i] again depends on the difficulty of factorizing a large rational integer into its primes; in Case 1, the rational integer $N\langle m\rangle = p_1 \ldots p_r$ needs to be factored whereas in Case 2, the rational integer $\left|\sqrt{N\langle m\rangle}\right| = p_1 \ldots p_r$ needs to be factored. In both cases, once the primes p_1 to p_r are found, then the order $\phi\langle m\rangle$ can be easily determined using $\phi\langle m\rangle = \prod_{i=1}^{r} N\langle \pi_i\rangle - 1$ where $N\langle \pi_i\rangle = p_i$ or p_i^2. Then, the secret coding exponent d can be calculated using (14). Note that the cryptanalyst does not need to know the Gaussian primes π_1 to π_r but only needs to know their respective norms. In other words, the cryptanalyst will be working over Z and not over Z[i].

The design of factorization trapdoor system as described above can be extended to other quadratic fields which are principal ideal domains.

Discussion

A generalization of the RSA cryptosystem in the ring of matrices over Z/mZ where m is a composite integer is proposed. It is shown that

factorization of the modulus m is needed to compute the order of the group formed by non-singular matrix messages, upper triangular matrix messages with non-unity invertible diagonal elements and orthogonal matrix messages thus offering a similar level of security as the RSA system.

An extension of the RSA system to polynomial rings has been considered The difficulty of factorization of a polynomial into its irreducible factors over a finite field does not in itself provide a secure public key cryptosystem. However if the difficulty of factorizing a polynomial is compounded with the difficulty of factorizing an integer then a secure RSA type cryptosystem in the ring of polynomials is seen to be possible.

The design of public key system in some quadratic algebraic number fields using factorization trapdoor concept has been presented. The security of such systems is found to be dependent on the difficulty of factoring the norm of the modulus.

The investigation of such extensions of RSA cryptosystem indicates that rings other than the ring of rational integers can be used to construct public key systems based on factorization trapdoor property. From a practical point of view, however it seems that the complexity of such systems may favour the implementation of the factorization trapdoor in the ring of rational integers.

References

1. Diffie,W. and Hellman,M.E., 'New Directions in Cryptography',IEEE Trans. on Inf. Theory, Vol.IT-22, 1976, pp 644-654.
2. Rivest,R.L.,Shamir,A. and Adleman,L., 'A method for obtaining Digital Signatures and Public Key Cryptosystems',Comm. ACM, Vol.21, No.2, 1978, pp 120-126.
3. Diffie,W. and Hellman M.E., 'Privacy and Authentication : An Introduction to Cryptography, Proc.IEEE, Vol.67, NO.3, 1979.
4. Davies,D., 'Limits to Computations', NPL note, London.
5. Van der Waerden,B.L., Modern Algebra : Vol. 1 and 2, 1949.
6. Dickson,L.E., Linear Groups with an Exposition of the Galois Field Theory, Dover Pub., 1958.
7. Albert,A.A., Fundemental Concepts of Higher Algebra, The Univ. of Chicago Press, 1956.
8. Varadharajan,V., Some Cryptographic Techniques for Secure Data Communication, Ph.D. Thesis, CNAA, 1984.
9. Varadharajan,V. and Odoni,R., 'Extension of RSA cryptosystem to Matrix Rings', Cryptologia, Accepted for Publication Aug.1984.
10. MacWilliams,J., 'Orthogonal matrices over Finite Fields', American Mathematical Monthly, Feb.1969.
11. Knuth,D.E., The Art of Computer Programming, Vol.2 : Seminumerical Algorithms, Second Edition, Addison-Wesley, 1981.
12. Kravitz,D.W. and Reed,I.S., 'Extension of RSA Cryptostructure : A Galois Approach, IEE Electronic Letters, Vol.18, No.6, 1982, pp255-256
13. Berlekamp,E.R., 'Factoring Polynomials over large Finite Fields', Maths. of Computation, Vol.24, No.111, 1970, pp 713-735.
14. Pollard,H., The Theory of Algebraic Numbers, The Carus Math. Monographs, No.9, Pub. by Math. Assoc. of America, John Wiley, 1950.
15. Rosen,M. and Ireland,K., A Classical Introduction to Modern Number Theory, Springler-Verlag, 1980

Acknowledgements

The author would like to acknowledge the help of Prof.R.Odoni, Dept. of Maths., Exeter University, for valuable discussions on the subject.