ALGEBRAICAL STRUCTURES OF CRYPTOGRAPHIC TRANSFORMATIONS

Józef P. Pieprzyk
Institute of Telecommunication
Technical Academy of Bydgoszcz
Bydgoszcz, POLAND

In the paper, application of idempotent elements to construction of cryptographic systems has been presented. The public key cryptosystem based on idempotent elements and the cryptographic transformation that preserves elementary arithmetic operations have been described.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 16-24, 1985.

1. Introduction

Various methods are being applied to design cryptographic systems. There is, however, a cryptosystem class which can be defined by means of peculiar algebraical structures. They are injected in a vector space which is spanned over idempotent elements of an algebraical ring.

The purpose of the work is presentation of mathematical tools which may be adapted to project a wide class of cryptosystems. Let Z_N be a ring with addition and multiplication modulo N where $N=p_1 \ldots p_n$ and p_i is prime for $i=1,\ldots,n$. Now, let us take into account an integer $x \in Z_N$ Then, we can determine the sequence of integers in the form

$$(x_1,\ldots,x_n) \qquad (1)$$

while $x_i=x \pmod{p_i}$ for $i=1,\ldots,n$ and $p_i \neq p_j$ for $i \neq j$. On the other hand, we define the integer

$$\mathrm{LCM}(x_1,\ldots,x_n)=\mathrm{LCM}\big(x_1 \pmod{p_1},\ldots,x_n \pmod{p_n}\big) = [\![x_1; \ldots ;x_n]\!] \qquad (2)$$

where LCM stands for the least common multiple. The vector $[\![x_1;\ldots;x_n]\!]$ belongs to the ring $\bigoplus_{i=1}^{n} Z_{p_i}$ in which addition and multiplication are given as follows:

$$[\![x_1;\ldots;x_n]\!] + [\![y_1;\ldots;y_n]\!] = [\![x_1+y_1 \pmod{p_1};\ldots;x_n+y_n \pmod{p_n}]\!]$$

$$[\![x_1;\ldots;x_n]\!]\,[\![y_1;\ldots;y_n]\!] = [\![x_1y_1 \pmod{p_1};\ldots;x_ny_n \pmod{p_n}]\!]$$

As is known [2], the rings Z_N and $\bigoplus_{i=1}^{n} Z_{p_i}$ are isomorphic, so

$$Z_N \approx \bigoplus_{i=1}^{n} Z_{p_i}$$

Example 1:

Let us take into account the ring Z_{30} and $p_1=2$, $p_2=3$, $p_3=5$. If $x=17$, then

$$x=[\![17 \pmod 2;17 \pmod 3;17 \pmod 5]\!] = [\![1;2;2]\!] \in Z_{30}$$

The original value of x can be calculated according to the following expression:

$$\mathrm{LCM}\big(1,3,5,7,9,11,13,15,17,\ldots ;2,5,8,11,14,17,\ldots ;2,7,12,17,\ldots\big)=17$$

For the elements $x=17$ and $y=22$, we can find

$$x+y = 17+22 = 9 \pmod{30}=[\![1;2;2]\!] + [\![0;1;2]\!] =[\![1;0;4]\!]$$

$$xy = 17\cdot 22 = 14 \pmod{30}=[\![1;2;2]\!]\,[\![0;1;2]\!]=[\![0;2;4]\!]$$

From all elements of the ring $\bigoplus_{i=1}^{n} Z_{p_i}$, we choose

$$\begin{aligned} e_1&=[\![1;0;0; \;\ldots\; ;0;0]\!]\\ e_2&=[\![0;1;0; \;\ldots\; ;0;0]\!]\\ &\vdots\\ e_n&=[\![0;0;0; \;\ldots\; ;0;1]\!] \end{aligned} \qquad (3)$$

Vectors e_i $(i=1,\dots,n)$ are also called basic idempotent elements. They have the following properties:

PR1. $\underset{i=1,\dots,n}{\forall} \quad e_i^2 = e_i$

PR2. $e_1+\dots+e_n = 1 \pmod N$

PR3. $\underset{\substack{i,j\\ i\neq j}}{\forall} \; e_ie_j = 0 \pmod N$

PR4. $x = [\![x_1;\dots;x_n]\!] = \sum_{i=1}^{n} x\, e_i = \sum_{i=1}^{n} x_i e_i \pmod N$

PR5. A sum of arbitrarily chosen basic idempotent elements is an idempotent one.

<u>Example 2:</u>

There are three basic idempotent elements in the ring Z_{30}, namely

$e_1 = [\![1;0;0]\!] = 15$

$e_2 = [\![0;1;0]\!] = 10$

$e_3 = [\![0;0;1]\!] = 6$

2. Algebraical structure of public key cryptosystems

In this point, we present two public key cryptosystems, namely the Rivest-Shamir-Adleman cryptosystem (RSA system) and the cryptosystem based on the knapsack problem (Merkle-Hellman cryptosystem). Both cryptosystems are being designed by means of suitable algebraic rings.

Authors of the RSA system [5] proposed the cryptographic functions in the form

$$c = E_k(m) = m^k \pmod N \tag{4}$$

$$m = D_{k'}(c) = c^{k'} \pmod N \tag{5}$$

where m,c,k,k' represent a message, a cryptogram, a public key, and a secret key, respectively, and $N=p_1\dots p_n$ (p_i are different primes for $i=1,\dots,n$) determines the ring in which cryptographic transformations are being carried out. In order to find the original message at the receiver's side, the following congruence must be fulfilled:

$$D_k(c) = D_{k'}(E_k(m)) = c^{k'} = m^{kk'} = m \pmod N \tag{6}$$

As a result, we get the congruence in the shape

$$m^{kk'-1} = 1 \pmod N \tag{7}$$

Transforming (7), we obtain

$$[\![m_1;\dots;m_n]\!]^{kk'-1} = [\![1;\dots;1]\!] \tag{8}$$

Thus, we have the sequence of congruences given by

$$m_i^{kk'-1} = 1 \pmod{p_i} \text{ for } i=1,\dots,n \tag{9}$$

As is known [2], the sequence of congruences has a solution when

$$\underset{i=1,\ldots,n}{\forall} \quad (kk'-1)\,|\,(p_i-1) \tag{10}$$

So the integer $(kk'-1)$ must fulfill the equation

$$kk'-1 = LCM(p_1-1,\ldots,p_n-1)=\lambda(N) \tag{11}$$

Since, in the RSA system, the integer k is chosen randomly from all the elements of set Z_N, the integer k' is calculated at the receiver's side according to the following congruence

$$kk' = 1\left(\mathrm{mod}\ \lambda(N)\right) \tag{12}$$

Now, let us take into account an unauthorized user (UU) who observes both a cryptogram and a public key, and additionally knows the the cryptographic transformations and the value of integer N. When he wants to obtain the message from the cryptogram, he may employ two approaches. The first one relies on the factorization of N into primes as the UU can find $\lambda(N)$ and finally decipher the cryptogram. If the UU additionally knows that $n \geqslant 3$, then he may use the Pollard method [4] to carry out the factorization of N. This method requires $O(p^{1/2})$ elementary processing operations where p is the smallest among all the primes p_i, $i=1,\ldots,n$. Hence, in the RSA system, one chooses the integer N in the form $N=p_1p_2$ where p_1 and p_2 are of the same order since the Pollard method turns out to be not efficient for N of the order of a decimal integer composed of 200 digits. Thus, $\lambda(N)$ may be written as

$$\lambda(N)= LCM(p_1-1,p_2-1) \tag{13}$$

At last, let us notice that difficulties in breaking the cipher for the RSA system result from the fact that the ring $\bigoplus_{i=1}^{n} Z_{p_i}$ cannot be determined easily by the UU when he knows only the ring Z_N.

We are now going to describe a cryptographic system that is based on idempotent elements. This cryptosystem similarly to the Merkle-Hellman system [1] (MH system) is used to encipher binary messages. Let us assume that the initial condition of that system has been defined by the choice of n primes $p_1,\ldots,p_n$ and let $N=p_1\ldots p_n$. Thus, in the ring Z_N, there exist n basic idempotent elements of the form

$$e_1=[\![1;0;\ldots;0]\!] \quad \ldots \quad e_n=[\![0;0;\ldots;1]\!]$$

Similarly as in the MH system, we convert elements e_i according to the congruence

$$k_i = e_i a(\mathrm{mod}\ q)\ ;\ i=1,\ldots,n \tag{14}$$

where $q>\sum_{i=1}^{n} e_i$ (q is a prime), integer a is randomly chosen from the set Z_q, and the sequence $k=(k_1,\ldots,k_n)$ represents the public key. At the transmitter, there is generated a cryptogram for a message m=

$(m_1,\dots,m_n)$. It is generated according to the expression

$$c = \left| \sum_{j=1}^{u} m_{i_j} k_{i_j} - \sum_{j=u+1}^{n} m_{i_j} k_{i_j} \right| \tag{15}$$

where the subset $\{m_{i_j};\ j=1,\dots,u\}$ is create arbitrarily by the sender. At the receiver's side, the cryptogram is processed as follows:

$$c' = c\, a^{-1} \pmod q \tag{16}$$

Substituting (15) into (16), we get

$$c' = \left| \sum_{j=1}^{u} m_{i_j} e_{i_j} - \sum_{j=u+1}^{n} m_{i_j} e_{i_j} \right| \pmod q \tag{17}$$

Since under the sign of absolute value, we may have both the positive and negative values, we get two integers c' and c'' obeying the congruence (17), where

$$c'' = q - c' \tag{18}$$

Using c' and c'', we find two sequences

$c' \rightarrow (c_1',\dots,c_n')$ where $c_i' = c' \pmod{p_i}$; $i=1,\dots,n$

$c'' \rightarrow (c_1'',\dots,c_n'')$ where $c_i'' = c'' \pmod{p_i}$; $i=1,\dots,n$

One of the sequences given above is the message we are looking for. As it has been proved in [3], one can find such a transformation (14) that one of these sequences will already be rejected at the beginning of deciphering process.

It is noteworthy that the cipher considered is based, similarly to the MH system, on the knapsack problem. Hence, it has advantages and drawbacks similar to that system. Nevertheless, compared to the MH system, the cryptosystem based on idempotent elements has two additional advantages, namely it:

- decreases the redundancy of cryptograms,
- makes the knapsack problem much more difficult to solve.

We should also point to the flexibility of the considered system as it allows to encipher messages represented not only by binary sequences.

Giving our attention to algebraic properties, we may state that constructions of two rings Z_N and $\bigoplus_{i=1}^{n} Z_{p_i}$ are kept secret since their disclosure may allow to discover the clear message. In order to protect the rings, we have injected idempotent elements into the field Z_q.

Of course, the cryptosystem with idempotent elements can be treated as modification of the MH cryptosystem. Nevertheless, considering these cryptosystems, we may notice what influence over quality of a cryptosystem has determination of its algebraic structure. In the MH system, a vector of integers $(d_1,\dots,d_n)$ (where $\sum_{i=1}^{j-1} d_i < d_j$ for $j=2,\dots,n$) creates the initial condition (the vector space) of the cryptosystem.

But this simple vector space stands in the way of flexible creation of cryptograms. Situation is quite different when we deal with the cryptosystem based on idempotent elements.

3. Algebraic structure of cryptographic transformations which preserve arithmetic operations

In many situations, processing tasks may be performed using only two elementary arithmetic operations (addition and multiplication). Also input messages (integers) are required not to be accessible to the UU while they are being not only transmitted over the channel but processed in the computer system as well (see Fig.1). So the cryptographic transformation which preserves the arithmetic operations (also called cryptomorphism) has to fulfill the following conditions:

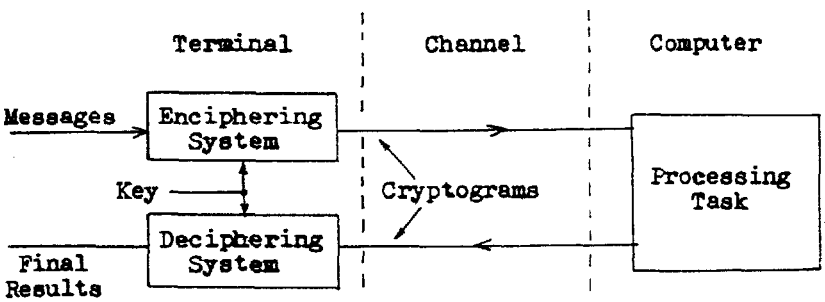

Fig.1. Application of cryptomorphisms

C1. $\forall_{m',m''\in M} \; f(m'+m'',k)= f(m',k) + f(m'',k)$

C2. $\forall_{m',m''\in M} \; f(m'm'',k)= f(m',k) \cdot f(m'',k)$

C3. $\forall_{d\in Z^+} \; \forall_{m\in M} \; f(dm,k)= d\, f(m,k)$

for a fixed key $k\in K$, where M,K and Z^+ are sets of messeges, keys, and positive integers, respeetively, and f is a cryptomorphism. The simplest form of such a cryptomorphism takes the shape

$$c = f(m,k)= mk \tag{19}$$

while $m\in M$, $k\in K$, $c\in C$ (C is the set of cryptograms), and $M,K,C\subset Z_N$ ($N=p_1\cdots p_n$; p_i are primes for $i=1,\dots,n$ and $p_i\neq p_j$ for $i\neq j$). Moreover, the key set is exclusively composed of idempotent elements of the ring Z_N .

Example 3:
For the ring Z_{12}, the set of keys contains three elements, namely $K=\{1,4,9\}$.

A key is an idempotent element of Z_N so there are two integers N^0 and N^1 which fulfill the following congruences:

$$k = 0 \pmod{N^0} \tag{20}$$

$$k = 1 \pmod{N^1} \tag{21}$$

whereas $N=N^0N^1$. As a result, we have that the cryptographic function of deciphering system is determined by the formula

$$m = f^{-1}(c,k) = c \pmod{N^1} \tag{22}$$

where $m \in M$, $c \in C$, $k \in K$, and k assigns one and only one value of N^1 while N is fixed. Furthermore, in order to find the correct message, it has to fulfill inequality in the form

$$0 \leqslant m \leqslant N^1-1 \tag{23}$$

Example 4:
Let the ring Z_N be determined for $N=3\cdot 5\cdot 7=105$ and we assume that the key $k=[\![1 \pmod 3; 0 \pmod 5; 1 \pmod 7]\!] = 85 \pmod{105}$. If $k=85$, then $N^1=21$. Thus, for $m=20$, we have the cryptogram $c=mk=1700$. To obtain the original message, we apply (22) as follows

$$m = c \pmod{N^1} = 1700 \pmod{21} = 20$$

After having examined the cryptomorphism in detail, we obtain their properties as follows:

P1. For fixed ring Z_N, there is one-to-one mapping between keys (idempotent elements) and pairs (N^0,N^1), where $N=N^0N^1$.

P2. The enciphering and deciphering transformations are defined according to the following formulae:

$$f(m,k) = mk$$

$$f^{-1}(c,k) = c \pmod{N^1}$$

P3. For any message $m \in Z_{N^1}$, there are m different cryptograms in the shape

$$c = m' + f(m'',k)$$

where $m'+m''=m$ and $m'=0,\dots,m-1$

P4. If an integer m has its inverse m^{-1} $\left(m,m^{-1} \in Z_{N^1}\right)$, then cryptograms of m and m^{-1} satisfy the following congruence:

$$f(m,k)\ f(m^{-1},k) = 1 \pmod{N^1}$$

Taking into account the properties, we can formulate four restrictions which have to be imposed to ensure a correctness of computations. These are:

R1. All message which are necessary to execute a program should satisfy the inequality

$$0 \leqslant m \leqslant N^1 - 1 \quad ; \quad m \in M \tag{24}$$

R2. A final result which would be obtained without using a cryptographic protection also has to fulfill (24).

R3. The execution of a processing task must be possible using only four basic arithmetic operations and all intermediate results have to have the form of either integers or fractions.

R4. Cryptograms of a numerator and a denominator should be determined when both the message and the anticipated final result are fractions.

Example 5:

Suppose that the expression $a = \frac{4+m}{2m^2-4}$ should be calculated for m=3. Of course, if we perform the calculations for clear message m=3, we shall get a=0,5. Let us assume that $N=3\cdot5\cdot7$ and key $k=\mathrm{LCM}\big(1\,(\mathrm{mod}\ 3), 1\,(\mathrm{mod}\ 5), 0\,(\mathrm{mod}\ 7)\big)=91$. In order to simplify our computations, instead of the cryptogram c=mk=273, we accept the cryptogram $c=m'+m''k=2+91=93$ for $m'+m''=3$ and $m'=2$. Thus, we have

$$f(a,k) = \frac{4+f(m,k)}{2\,f^2(m,k)-4} = \frac{4+93}{2\cdot8649-4} = \frac{97}{17294} = \frac{f(a',k)}{f(a'',k)}$$

For cryptogram $f(a',k)$, we obtain the clear form of the numerator

$$a' = f^{-1}(97,k) = 97\,(\mathrm{mod}\ 15) = 7$$

However, for $f(a'',k)$, we get

$$a'' = f^{-1}(17294,k) = 17294\,(\mathrm{mod}\ 15) = 14$$

Whence, we have the final result a=0,5. As any fraction can be presented in different ways, special precautions should be undertaken in case of fraction calculations. In order to illustrate difficulties, we take the expression

$$f(a,k) = \frac{97}{17294} = \frac{194}{34588}$$

After having deciphered cryptograms of the numerator and the denominator we get the wrong final result.

4. Conclusions

Cryptographic transformations in public key cryptosystems depend on determination of suitable algebraic structures. In the RSA system, such a structure is defined by means of only two basic idempotent elements. Next, in the cryptosystem with idempotent elements, the algebraic structure of a ring is based on many basic idempotent elements. Moreover, the more idempotent elements are applied the higher quality of the system (opposite to the RSA system).

Also, we have presented how an algebraic structure can be applied for construction of cryptomorphisms. Only the simplest case has been considered and the cryptographic transformation relies on multiplying a message by a cryptographic key which is an idempotent element. It is possible to notice that cryptomorphisms can be defined by the aid of a matrix of idempotent elements.

5. References

[1] Merkle R., Hellman M.E., Hiding Information and Receits in Trapdoor Knapsack, IEEE Trans. Inf. Theory, IT-24, September 1978, pp. 525-530

[2] Narkiewicz W., The Numbers Theory, PWN, Warsaw, 1977

[3] Pieprzyk J.P., Rutkowski D.A., Application of Public Key Cryptosystems to Data Security, Rozprawy Elektrotechniczne to be published

[4] Pollard J.M., A Monte Carlo Method for Factorization, BIT 15, 1975, pp.331-334

[5] Rivest R.L., Shamir A., Adleman L., A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM, Vol.21, February 1978, pp.120-126