ON PUBLIC-KEY CRYPTOSYSTEMS BUILT USING POLYNOMIAL RINGS

Józef P. Pieprzyk
Institute of Telecommunication
Technical Academy of Bydgoszcz
85-763 Bydgoszcz, Poland

Abstract

In the paper, a public-key cryptosystem that is, as a matter of fact, a modification of the Merkle-Hellman system has been described. However, unlike the Merkle-Hellman system, it has been built using a polynomial ring. Finally, its quality has been given.

1. Introduction

Although several solutions of public-key cryptosystems (PKC) have already been published, intensive studies are still pursued to gain new cryptosystems which couple advantages of existing ones while some of their drawbacks are removed. In the work, a variation of the public-key cryptosystem based on idempotent elements [5] is presented.

The variation relies on inserting idempotent elements into a polynomial ring. Clearly, operations defined in a polynomial ring over a finite field are more tractable than in an integer ring.

2. Description of the PKC

Presented in [5], the cryptosystem like the Merkle-Hellman cryptosystem (MH system) is based on the NP-complete knapsack problem. The best known algorithm [2] for solving the knapsack problem of size n requires $O(2^{\frac{n}{2}})$ time. So, $n=100$ what was originally suggested by Merkle and Hellman [4] seems to be too small. However for $n=200$, $2^{100} \approx 10^{30}$ and the algorithm is computationally infeasible.

On the other hand, the design of the PKC with idempotent elements over an integer ring proves to be somewhat burdensome. Difficulties will be removed applying polynomial algebraic structures. Moreover, the quality of the PKC based on a polynomial ring will be given taking into account steps needed to carry out cryptographic processes.

First of all, necessary notations are now introduced. A cryptosystem is known to be described by five components [2]:

$\mathcal{M}$ - a message space,

$\mathcal{C}$ - a ciphertext space,

$\mathcal{K}$ - a key space,

$E_K: \mathcal{M} \rightarrow \mathcal{C}$ - a family of enciphering transformations, where $K \in \mathcal{K}$,

$D_K: \mathcal{C} \rightarrow \mathcal{M}$ - a family of deciphering transformations, where $K \in \mathcal{K}$.

Let us assume that the PKC is used to encipher a message $M = (m_1(x), \dots, m_n(x))$, where $M \in \mathcal{M}$ and $m_i(x)$ is a binary polynomial for $i=1, \dots, n$. Furthermore at the receiver's side, the polynomial ring $R = R[x]/\varphi_1(x) \dots \varphi_n(x)$ over $GF(2)$ is created, where $\varphi_i(x)$ is irreducible and $\deg \varphi_i(x) = \deg m_i(x) + 1$ for $i=1, \dots, n$. Also, idempotent polynomials $p_i(x)$ ($i=1, \dots, n$) of R are calculated. Therefore

$$\forall_{i=1, \dots, n} \quad p_i^2(x) = p_i(x) \pmod{\varphi(x)} \quad (1)$$

whereas $\varphi(x) = \varphi_1(x) \dots \varphi_n(x)$.

Notice that, for the message $M = (m_1(x), \dots, m_n(x))$, the polynomial

$$\sum_i p_i(x) m_i(x) \quad (2)$$

can be computed. In order to get back $m_j(x)$ from (2), the following congruence is applied:

$$m_j(x) = \sum_i m_i(x) p_i(x) \pmod{\varphi_j(x)}; \quad j=1, \dots, n. \quad (3)$$

The public key $K = (k_1(x), \dots, k_n(x))$ is created as follows:

$$\forall_{i=1, \dots, n} \quad k_i(x) = p_i(x) a(x) \pmod{\varphi(x)}, \quad (4)$$

while $\varphi(x)$ is randomly selected and it generates a Galois field $GF(2^u)$ ($u = \deg \varphi(x) = \sum_i \deg \varphi_i(x) + \max_i \deg m_i(x)$), whereas $a(x)$ is an arbitra-

rily chosen element of $GF(2^u)$.

At the sender's side, for the message $M=(m_1(x), \dots, m_n(x))$, the ciphertext $C \in \mathcal{C}$ is created according to the equation

$$C = \sum_i m_i(x) k_i(x) \quad (5)$$

and it is sent to the receiver. On receipt, the ciphertext is transformed in $GF(2^u)$ so that

$$C' = C a^{-1}(x) \pmod{\psi(x)}. \quad (6)$$

By (4) and (5), (6) may be converted into the form

$$C' = \sum_i m_i(x) p_i(x) \pmod{\psi(x)}. \quad (7)$$

Next by applying (3), the message M can be recreated.

Example: Let us consider a cryptosystem defined by the ring $R = R[x]/\varphi_1(x)\varphi_2(x)$ over $GF(2)$ where $\varphi_1(x)=x+1$, $\varphi_2(x)=x^3+x+1$ and $\psi(x)=\varphi_1(x)\varphi_2(x)=x^4+x^3+x^2+1$. For the message $M=(m_1(x), m_2(x))$, the following equalities have to be fulfilled:

$$\deg m_1(x) = \deg \varphi_1(x) - 1 = 0,$$

$$\deg m_2(x) = \deg \varphi_2(x) - 1 = 2.$$

At the receiver's side, idempotent polynomials are also calculated and they are:

$$p_1(x) = x^3 + x + 1,$$

$$p_2(x) = x^3 + x.$$

As $\deg \sum_i p_i(x) m_i(x) = 5$, $\deg \psi(x) = 6$. We are now looking for $\psi(x)$.

Although it should be chosen randomly, we take into account the cyclotomic polynomial $Q^{(9)}(x)$ and accept $\psi(x) = Q^{(9)}(x) = x^6 + x^3 + 1$ (see [1]).

Now, we select the polynomial $a(x) = x^3 + 1$ and calculate its inverse $a^{-1}(x) = x^3$ in the field $GF(2^6)$. Then, the public key consists of two polynomials, namely:

$$k_1(x) = p_1(x) a(x) = x^4 + x^3 + x \pmod{x^6 + x^3 + 1},$$

$$k_2(x) = p_2(x) a(x) = x^4 + x + 1 \pmod{x^6 + x^3 + 1}.$$

At the sender's side, $K=(k_1(x), k_2(x))$ is used to create a ciphertext. For instance, for the message $M=(1, 1, 0, 1) = (1, x^2+1)$, the ciphertext takes on the form

$$C = (x^4 + x^3 + x) + (x^2 + 1)(x^4 + x + 1) = x^6 + x^2 + 1.$$

At the receiver's side, the ciphertext is transformed and

$$C' = C a^{-1}(x) = (x^6 + x^2 + 1)x^3 = x^5 + x^3 + 1 \pmod{x^6 + x^3 + 1}.$$

The message M can be easily recreated as

$$m_1(x) = C' \pmod{\varphi_1(x)} = x^5 + x^3 + 1 = 1 \pmod{x+1} \quad \text{and}$$

$$m_2(x) = C' \pmod{\varphi_2(x)} = x^5 + x^3 + 1 = x^2 + 1 \pmod{x^3 + x + 1}.$$

3. Determination of the polynomial ring

As is known, the algebraic ring ought to be defined by the polynomial $\varphi(x)$ whose factorization gives n different irreducible polynomials ($n > 200$). In Table 1, numbers of irreducible polynomials over $GF(2)$ for successive degrees are shown. Suppose that a designer of the cryptosys-

Table 1

polynomial degree	number of irreducible polynomials over $GF(2)$
1	2
2	1
3	2
4	3
5	6
6	9
7	18
8	30
9	56
10	99
11	186
12	335
13	630

tem chooses randomly a hundred irreducible polynomials from among all ones of degree 11 and a hundred irreducible polynomials of degree 12 as well. These polynomials are multiplied to get the polynomial $\varphi(x)$. Obtaining $\varphi(x)$ ($\deg \varphi(x) = \sum_{i=1}^n d_i$, where $d_i = \deg \varphi_i(x)$) needs $O(dn^2)$ elementary operations while d is the average degree of $\varphi_i(x)$ ($i=1, \dots, n$). Clearly, the probability of $\varphi(x)$ disclosure by an enemy observer is less than 2^{-200} . As the knowledge of all irreducible polynomials of degrees 11 and 12 is needed at the receiver's side, their list has to be given and stored all the time.

Knowing $\varphi(x)$, we can determine idempotent polynomials $p_i(x)$, $i=1, \dots, n$. Any polynomial $p_i(x)$ fulfills the two following congruences:

$$\forall_{i=1, \dots, n} \quad p_i(x) \equiv 1 \pmod{\varphi_i(x)}, \quad (8)$$

$$\forall_{i=1, \dots, n} \quad \forall_{j \neq i} \quad p_i(x) \equiv 0 \pmod{\varphi_j(x)}. \quad (9)$$

The congruence (9) implies that

$$p_i(x) = \alpha_i(x) \varphi_1(x) \dots \varphi_{i-1}(x) \varphi_{i+1}(x) \dots \varphi_n(x). \quad (10)$$

Of course, $\alpha_i(x)$ is unknown. Let us denote

$$\beta_i(x) = \varphi_1(x) \dots \varphi_{i-1}(x) \varphi_{i+1}(x) \dots \varphi_n(x) \pmod{\varphi_i(x)} \quad (11)$$

Applying (11) to (8), we get

$$\alpha_i(x) \beta_i(x) = 1 \pmod{\varphi_i(x)} \quad (12)$$

Otherwise

$$\alpha_i(x) = \beta_i^{-1}(x) \pmod{\varphi_i(x)} \quad (13)$$

So, finding $\alpha_i(x)$ relies on the calculation of the inverse element in $GF(2^{d_i})$. As is known [1], reckoning the inverse element requires $O(4d_i)$ units of time. Thus, in order to calculate all elements $\{\alpha_i(x); i=1, \dots, n\}$, we need $O(4nd)$ steps. Having the set $\{\alpha_i(x); i=1, \dots, n\}$, we can compute $\{p_i(x); i=1, \dots, n\}$ in time $O(n^2)$.

We now assume that $d_i=d$ for $i=1, \dots, n$. Next, we pay our attention to determine an irreducible polynomial that defines $GF(2^{(n+1)d})$. The most obvious solution of the problem would be a random choice of a polynomial of a required degree and verification of its irreducibility. Probability of choosing an irreducible polynomial from among all polynomials of degree $(n+1)d$ is known to be $\frac{1}{(n+1)d}$ [1].

On the other hand, to test if a polynomial is reducible or not, we may adapt Berlekamp's factoring algorithm [1] that requires $O((n+1)^3 d^3)$ units of time. Clearly, it can be considerably simplified for it sometimes ends at the beginning when, for example, a polynomial is not squarefree.

Irreducible polynomials may be pointed out by applying well-known properties of Galois fields. For instance, cyclotomic polynomials may be used as their forms can be easily computed even for high degrees [1]. Now assume that an irreducible polynomial $g(x)$ has been found ($\deg g(x) = (n+1)d$). If w is a root of $g(x)$ ($w \in GF(2^{(n+1)d})$), any element $v \in GF(2^{(n+1)d})$ may be presented as a polynomial for w of degree at most $(n+1)d$ and, moreover, it is a root of some minimal polynomial whose degree divides $(n+1)d$.

Therefore, we propose to fix the irreducible polynomial $\psi(x)$ by random choice of a binary polynomial $\xi(x)$ which defines the relation between elements w and v in the form

$$v = \xi(w)$$

whereas the irreducible polynomial $g(x)$ assigns $GF(2^{(n+1)d})$ ($w, v \in GF(2^{(n+1)d})$) and w is a primitive element. Hence, $\psi(x)$ is the minimal polynomial of v . Described in [1], the algorithm gives minimal polynomials in $O(\frac{1}{3}(n+1)^3 d^3)$ steps.

The rest operations needed to get both a public key and a message from a ciphertext requires $O((n+1)d)$ units of time.

4. Conclusions

The breaking of the cryptosystem may rely upon either the message disclosure by solving the suitable knapsack problem or determination of the algebraic ring R by searching the public key. Of course, the knapsack problem is NP-complete and, in general, it is shown [2] to be solvable in time $O(2^{n/2})$, where n is the size of the problem.

On the other hand, Brickell [3] has shown in his presentation at this conference that determination of the ring R is possible in polynomial time. It is due to modular multiplications which are used to disguise the shape of idempotent elements.

5. Bibliography

- [1] Berlekamp E.R., Algebraic Coding Theory, McGraw-Hill Book Company, New York, 1968
- [2] Denning D.E., Cryptography and Data Security, Addison-Wesley Publishing Company, Reading, Massachusetts, 1982
- [3] Brickell E.F., Attacks on Generalized Knapsack Schemes, EUROCRYPT 85, Linz, Austria, 1985
- [4] Merkle R.C., Hellman M.E., Hiding Information and Signatures in Trapdoor Knapsack, IEEE Trans. on Inf. Theory, Vol. IT-24, September 1978, pp.525-530
- [5] Pieprzyk J.P., Rutkowski D.A., Design of Public-Key Cryptosystems Using Idempotent Elements, Proc. of EUROCON, Brighton, UK, 26-28 September, 1984, pp.64-8