On a polynomial transformation and its application to the construction of a public key cryptosystem

A. Pethö *

Abstract. Generalizing results of Kovács and Pethö [5] we study when a certain map is injective (or bijective). Based on this map we propose a to the Merkle-Hellman knapsack scheme related cryptosystem.

1 Introduction

Let $g(t) = t^n + g_{n-1}t^{n-1} + \ldots + g_0 \in \mathbb{Z}[t]$ and $\mathcal{N}$ a finite subset of $\mathbb{Z}$. We denote by $\mathbb{Z}$ as usual the ring of integers. Let us define the sequence $\underline{x}_i \in \mathbb{Z}^n$, $i = 0, 1, \ldots$ by

$$\underline{x}_0 = (1, 0, \ldots, 0), \qquad \underline{x}_{i+1} = \underline{x}_i G \quad \text{if} \quad i \geq 0, \tag{1.1}$$

where the nxn matrix G is given by

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -g_0 & -g_1 & -g_2 & \cdots & \cdots & -g_{n-1} \end{pmatrix}. \tag{1.2}$$

Let $\mathcal{A}_{\mathcal{N}}$ be the set of all finite words $w = w_0 \ldots w_l$ over $\mathcal{N}$ with the convention that if $0 \in \mathcal{N}$ then either $w_l \neq 0$ or $l = 0$ and $w_0 = 0$. We call $l(w) = l + 1$ the length of w.

The pair $\{g(t), \mathcal{N}\}$ will be called *(weak) number system (WNS) NS* if the map $T : \mathcal{A}_{\mathcal{N}} \to \mathbb{Z}^n$, which is defined by

$$T(w_0, \ldots w_l) = w_0\underline{x}_0 + \ldots + w_l\underline{x}_l \tag{1.3}$$

is (injective) bijective.

In the special case $g(t) = t + g_0$ with $g_0 \geq 2$ and $\mathcal{N} = \{0, \ldots, g_0 - 1\}$ (1.3) defines the g_0-adic radix representation of the integers. You find results about the

*Research supported in part by Hungarian National Foundation for Scientific Research Grant No. 273/86

Computational Number Theory

radix representation of integers with extensive literature in Knuth [2]. Kovács and Pethö [4] proved that there exist infinitely many finite subsets $\mathcal{N}$ of $\mathbb{Z}$ such that $\{t+g_0, \mathcal{N}\}$ is a number system in $\mathbb{Z}$. They proved moreover in [5], that if $g(t)$ is irreducible then it is decidable whether the pair $\{g(t), \mathcal{N}\}$ is a number system in the ring $\mathbb{Z}[t]/g(t)\mathbb{Z}[t]$. We generalize their results for arbitrary polynomials in sections 6. and 7.

If T is injective then we can use it in a private key cryptosystem. Such a system is described in section 3.

Merkle and Hellman proposed in [6] a public key cryptographic scheme based on the knapsack problem. Starting from a superincreasing sequence $m_0, m_1, \ldots, m_n$ of integers, they chosed suitable integers w and k with $(w,k)=1$ and took

$$\overline{m}_i \equiv w m_i \pmod{k} \quad i = 0, \ldots, n.$$

The numbers $\overline{m}_0, \ldots, \overline{m}_n$ were proposed for apply as public keys. Shamir [7] proved that knowing the public keys it is possible to compute under natural conditions in polynomial time w, k and $m_0, \ldots, m_n$. Cryptosystems based on the knapsack problem are extensively studied in Horster [1].

We propose in section 4 a to the Merkle-Hellman cryptosystem related public key cryptographic scheme based on weak number systems. For a WNS we choose a suitable integer M and an nxn invertible matrix C in $\mathbb{Z}_M$ which do not commute with G. For public keys we use $\underline{x}_n C, \ldots, \underline{x}_{n+l} C \pmod{M}$ and $\mathcal{N}$, however C^{-1}, $g(t)$ and M remain secret.

2 Preliminary results about the map T

Let $\mathcal{N}[t]$ denote the set of polynomials in t with coefficients from $\mathcal{N}$ and let $T_1 := \mathcal{A}_{\mathcal{N}} \to \mathcal{N}[t]$, defined by

$$T_1(w) = w_0 + w_1 t + \ldots + w_l t^l$$

for any $w_0 \ldots w_l = w \in \mathcal{A}_{\mathcal{N}}$. Let T_2 be the natural ring homomorphism $T_2 : \mathbb{Z}[t] \to \mathbb{Z}[t]/g(t)\mathbb{Z}[t] = R_g$. By the definition of $g(t)$ it is clear that R_g is a commutative ring which is as a $\mathbb{Z}$-module isomorphic to $\mathbb{Z}^n$. Putting $\phi = T_2(t)$ we may write the elements of R_g uniquely in the form

$$\sum_{i=0}^{n-1} y_i \phi^i \text{ , with } y_i \in \mathbb{Z} \text{ for } i = 0, \ldots, n-1.$$

Let T_3 be the $\mathbb{Z}$-module isomorphism $R_g \to \mathbb{Z}^n$.

Proposition 2.1. *We have with the above notations*

$$T = T_3 \circ T_2 \circ T_1. \tag{2.1}$$

Furthermore, T is bijective iff the restriction of T_2 to $\mathcal{N}[t]$ is bijective.

Proof. We have $g(\phi) = 0$ in R_g, hence

$$\phi^n = (-g_0, -g_1, \ldots, -g_{n-1})\Phi^T,$$

where Φ^T denotes the transposition of the vector $\Phi = (1, \phi, \ldots, \phi^{n-1})$. Using this identity and (1.1) it is easy to prove

$$\phi^i = \underline{x}_i \Phi^T, \qquad i = 0, 1, \ldots.$$

Therefore, if

$$T(w_0 \ldots w_l) = (y_0, \ldots, y_{n-1}),$$

then

$$\begin{aligned} T(w_0 \ldots w_l)\Phi^T &= \sum_{i=0}^{l} w_i \underline{x}_i \Phi^T = \sum_{i=0}^{l} w_i \phi^i \\ &= (y_0, \ldots, y_{n-1})\Phi^T = T_3^{-1}(y_0, \ldots, y_{n-1}). \end{aligned}$$

We know that T_3 is a $\mathbb{Z}$-module isomorphism, thus (2.1) is proved. The second assertion follows easily from (1.3). □

Proposition 2.2. *Let $|g_0| > 1$ and assume that the elements of $\mathcal{N}$ are pairwise incongruent modulo g_0. Then $\{g(t), \mathcal{N}\}$ is a WNS.*

Proof. We need to prove that T is injective. By Proposition 2.1 it is enough to show that the restriction of T_2 to $\mathcal{N}[t]$ is injective. Assume contrary that there exist polynomials $p_i(t) = p_{i0} + \ldots + p_{im_i} t^{m_i} \in \mathcal{N}[t]$, $i = 1, 2$ such that

$$T_2(p_1) = T_2(p_2), \tag{2.2}$$

and p_1 has the smallest degree among such polynomials. There exists by (2.2) a polynomial $h(t) \in \mathbb{Z}[t]$ with

$$p_1(t) = p_2(t) + h(t)g(t). \tag{2.3}$$

Comparing the constant terms in (2.3) we get

$$p_{10} \equiv p_{20} \pmod{g_0}.$$

By the assumption on $\mathcal{N}$ this is possible only if $p_{10} = p_{20}$, thus $h(t) = th_1(t)$. Hence

$$T_2(p_{11} + \ldots + p_{1m_1} t^{m_1 - 1}) = T_2(p_{21} + \ldots + p_{2m_2} t^{m_2 - 1}),$$

which contradicts the choice of $p_1(t)$. □

3 Private key cryptosystem

Let $g(t) = t^n + g_{n-1}t^{n-1} + \ldots + g_0 \in \mathbb{Z}[t]$ with $|g_0| > 1$ and assume that the elements of $\mathcal{N}$ are pairwise incongruent modulo g_0, then it is possible to define a private key cryptosystem based on the WNS $\{g(t), \mathcal{N}\}$.

Assume that the individual A will send a message $w = w_0 \dots w_l \in \mathcal{A}_{\mathcal{N}}$ to the individual B. He chooses integers $u \leq v$ and random integers $l_1, l_2, \dots$ from the interval $[u, v]$. He cuts then w into consecutive blocks $W_1, W_2, \dots$ of length $l_1, l_2, \dots$ such that the last letters of the blocks are not 0, and send the encrypted message $T(W_1), T(W_2), \dots$ to the individual B. Knowing the polynomial $g(t)$ and the set $\mathcal{N}$, B is able to decrypt the original message w from $T(W_1), T(W_2), \dots$. We describe the method formally in the following two algorithms.

Algorithm 3.1.

Input: $w_0 \dots w_l \in \mathcal{A}_{\mathcal{N}}$; $u, v \in \mathbb{Z}$ *with* $0 \leq u \leq v$.

Output: $\underline{y}_0 \dots \underline{y}_h \in \mathcal{A}_{\mathbb{Z}^n}$.

(1) *Set* $W = w_0 \dots w_l$, $h = -1$.

(2) *Repeat until* $l < 0$

Set $h = h + 1$ *and* $i = random[u, v]$. *If* $l < i$ *then set* $i = l$.

While $w_i = 0$ *and* $i > 0$ *do* $i = i - 1$.

Set $\underline{y}_h = T(w_0 \dots w_i)$; $W = w_{i+1} \dots w_l$ *and* $l = l - i - 1$.

The individual B can decrypt the message $\underline{y}_0 \dots \underline{y}_h \in \mathcal{A}_{\mathbb{Z}^n}$ using the following algorithm.

Algorithm 3.2.

Input: $\underline{y}_0 \dots \underline{y}_h \in \mathcal{A}_{\mathbb{Z}^n}$ *with* $\underline{y}_i \in T(\mathcal{A}_{\mathcal{N}})$.

Output: $W_0 \dots W_h = w_0 \dots w_l \in \mathcal{A}_{\mathcal{N}}$.

(1) *Set* $s = 0$.

(2) *Repeat until* $s > h$

(3) *Put* $l(s) = n - 1$, $p(t) = \underline{y}_s(1, t, \dots, t^{n-1})^T = z_0 + \dots + z_{l(s)} t^{l(s)}$; $j = 0$.

(4) *Repeat until* $j > l(s)$

If $z_j \notin \mathcal{N}$ *then determine* $x_j \in \mathcal{N}$ *such that* $z_j \equiv x_j \pmod{g_0}$

and set $p(t) = p(t) - g(t)t^j(z_j - x_j)/g_0$, *set* $l(s) = n + j$,

if $z_i = 0$ *for* $j + 1 \leq i \leq l(s)$ *then set* $l = j$, $j = l(s)$.

Set $j = j + 1$.

(5) *Set* $j = l$.

(6) *While* $z_j = 0$ *and* $j > 0$ *do* $j = j - 1$.

(7) *Set* $W_s = z_0 \dots z_j$. $s = s + 1$.

Theorem 3.1. *The Algorithms 3.1 and 3.2 terminate successfully after* $c_1 nl$ *operations on integers, where* c_1 *is a constant depending only on the size of* $\mathcal{N}$.

Proof. The most time consuming operation in Algorithm 3.1 is the computation of y_j in the repeat loop. We have

$$\underline{y}_j = w_0\underline{x}_0 + \dots + w_i\underline{x}_i$$

by the definition of T, where the vectors $\underline{x}_i$ are defined by (1.1). Hence $\underline{y}_j$ can be computed by $2n(i+1)$ arithmetical operations. Summing up these numbers we get that Algorithm 3.1 terminates after $O(nl)$ operations.

In the inner repeat loop of Algorithm 3.2 the inverse of the map T_2 is computed. The vectors $\underline{y}_s$ have by the assumption preimages, and by Proposition 2.2 they are unique. Hence Algorithm 3.2 terminates also. If the length of W_s is $j+1$, then the inner repeat loop must be performed at most $j+2$ times, and the computation of $p(t)$ requires each times at most $g_0 + n + 2$ operations. This proves the upper bound for the number of operations needed in Algorithm 3.2. □

Remark 1. For a binary message, i.e. for a message consisting of 0's and 1's, it is most convenient to choose g_0 a power of 2, say $g_0 = 2^m$, and $\mathcal{N}$ a complete residue system modulo g_0. In this case we split the message into consecutive blocks of length m, change each block with that element of $\mathcal{N}$, which it is congruent modulo g_0 and then apply Algorithm 3.1 for the encryption. In order to decrypt the message one must apply naturally the inverse change.

Remark 2. Theorem 3.2 gives information about the time complexity of the encryption/decryption algorithm, but we have said nothing about their space complexity. If $g(t)$ is squarefree and its roots are of absolute value larger then 1, we examine the space complexity of Algorithms 3.1 and 3.2 in Theorem 6.3.

Remark 3. We have freedom in Algorithm 3.1 for the choice of the integers u and v. It is convenient to choose $u > n$ because otherwise we get the same words after the transformation as in the plaintext.

4 The public key cryptosystem

We shall now modify the cryptosystem described in the previous section so that the parameters required for the encryption are public, but for the efficient decryption one needs further secret parameters. The idea behind our cryptosystem is similar to that used by Merkle and Hellman [6].

Let $\{g(t), \mathcal{N}\}$ be a WNS. If for a $w = w_0 \dots w_l \in \mathcal{A}_{\mathcal{N}}$ we have $T(w) = (y_0, \dots, y_{n-1}) \in \mathbb{Z}^n$, then $m(w) = \max\{|y_0|, \dots, |y_{n-1}|, 1\}$ will be called the height of w.

Let $\mathcal{A}_{\mathcal{N}}^L$ denote the set of all words from $\mathcal{A}_{\mathcal{N}}$ with length at most $L+1$, and let M be an integer with

$$M > 2 \max\left\{ m(w) \ : \ w \in \mathcal{A}_{\mathcal{N}}^{L+n} \right\}. \tag{4.1}$$

Denote $\mathbb{Z}_M$ the residue class ring modulo M, and $\mathbb{Z}_M(n,m)$ the ring of nxm matrices over $\mathbb{Z}_M$.

Let $C \in \mathbb{Z}_M(n,n)$ be invertible which does not commute with G, i.e. $GC \neq CG$ in $\mathbb{Z}_M(n,n)$. Let

$$\hat{\underline{x}}_i \equiv \underline{x}_{n-i} C \pmod{M} \quad \text{for } i = 0, \dots, L, \tag{4.2}$$

and let the map $\hat{T} : \mathcal{A}_{\mathcal{N}}^L \to \mathbb{Z}^n$ be defined by

$$\hat{T}(w_0 \dots w_l) = w_0 \hat{\underline{x}}_0 + \dots + w_l \hat{\underline{x}}_l \quad (l \leq L). \tag{4.3}$$

The individual B, who creates the public key system publishes $\mathcal{N}$, $\hat{\underline{x}}_0, \dots, \hat{\underline{x}}_L$ but not $g(t)$, C, and M. The individual A can send messages to B using Algorithm 3.1 with $u = 0$, $v = L$ and computing $\hat{T}(w_0 \dots w_i)$ instead of $T(w_0 \dots w_i)$. Knowing C and M, the individual B is able to compute C^{-1} and so decrypt the message. We have namely by (4.3) and (4.2)

$$\hat{T}(w_0 \dots w_l) = w_0 \hat{\underline{x}}_0 + \dots + w_l \hat{\underline{x}}_l \equiv (w_0 \underline{x}_n + \dots + w_l \underline{x}_{n+l}) C \pmod{M},$$

hence

$$\hat{T}(w_0 \dots w_l) C^{-1} = (\hat{y}_0, \dots, \hat{y}_{n-1}) C^{-1} \equiv w_0 \underline{x}_n + \dots + w_l \underline{x}_{n+l} \pmod{M}.$$

Therefore

$$(y_0, \dots, y_{n-1}) = T(O^n w_0 \dots w_l) \equiv \hat{T}(w_0 \dots w_l) C^{-1} \pmod{M}. \tag{4.4}$$

We have $|y_i| < M/2$ by (4.1), hence (4.4) determines the integers $y_0, \dots, y_{n-1}$ uniquely performing the computations in the absolute smallest residue system modulo M. Knowing $(y_0, \dots, y_{n-1})$ the individual B is able to compute $w_0 \dots w_l$ applying Algorithm 3.2 to $(y_0, \dots, y_{n-1})$ and dropping the first n invaluable letters from the result.

5 Remarks about the parameters

We have in the public key cryptosystem defined in the previous section two important parameters: the polynomial $g(t)$ and the matrix C.

It is convenient to choose $L < n^2 + n - 1$ because otherwise taking $g_1, \dots, g_{n-1}$ and the entries of C as unknowns we would get at least as many equations by (4.2) and (1.1) as we have unknowns.

There exist in $\mathbb{Z}_M(n,n)$ at least $M^{n-1}o(M)$ invertible elements. It is easy to prove that if M is prime then the exact number of invertible elements in $\mathbb{Z}_M(n,n)$ is $(M^n-1)*\ldots*(M^n-M^{n-1})$.

The most important assumption in our cryptosystem is

$$GC \neq CG. \tag{5.1}$$

Suppose namely that (5.1) is not satisfied, i.e. $GC = CG$. Then we get by (4.2) and (1.1)

$$\underline{\hat{x}}_i = \underline{x}_{n+i}C = \underline{x}_{n-i-1}GC = \underline{x}_{n-i-1}CG = \underline{\hat{x}}_{i-1}G,$$

from which G is easy to compute. Knowing G it is possible to compute C from equation (4.2).

Hence it is important to know how many matrices from $\mathbb{Z}_M(n,n)$ satisfy (5.1). The next proposition shows that at least half of the invertible elements of $\mathbb{Z}_M(n,n)$ satisfy (5.1).

Proposition 5.1. *Let $\mathbb{Z}_M^*(n,n)$ be the group of the invertible elements of $\mathbb{Z}_M(n,n)$ and G the matrix defined by (1.2). Denote $C(G)$ the set of elements of $\mathbb{Z}_M^*(n,n)$ which do not satisfy (5.1). Then*

$$|\mathbb{Z}_M^*(n,n)| \geq 2\,|C(G)|\,.$$

Proof. By the definition $C(G)$ is the centralizer of G in $\mathbb{Z}_M^*(n,n)$, which is a subgroup. We have $|C(G)| \mid |\mathbb{Z}_M^*(n,n)|$ by Lagrange's theorem, hence it is enough to prove that there exists at least one element of $\mathbb{Z}_M^*(n,n)$ which does not commute with G.

Let P be the following permutation matrix

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & E_{n-2} & \\ 0 & 0 & & & \end{pmatrix}$$

where E_{n-2} denotes the $(n-2)$x$(n-2)$ unit matrix. Then PG differs from G such that the first two rows are exchanged, while GP such that the first two columns are exchanged. Hence $P \notin C(G)$ except when $n=2$, $g_0 \equiv -1$ and $g_1 \equiv 0 \pmod{M}$. In the exceptional case taking $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ one can prove by an easy computation that $P \notin C(G)$. The proposition is proved. □

6 Characterisation of number systems

We have given in section 2 a general sufficient condition for $\{g(t), \mathcal{N}\}$ to be a WNS. In the following theorem we are given a characterization of number systems when $g(t)$ is squarefree, i.e. without multiple roots. Denote in the sequel $A = \max\{|a| : a \in \mathcal{N}\}$, D_g the discriminant of g and $|\bar{g}|$ the maximum of the absolute values of the roots of g.

Theorem 6.1. *Let $g(t) = t^n + g_{n-1}t^{n-1} + \ldots + g_0 \in \mathbb{Z}[t]$ be squarefree. Then $\{g(t), \mathcal{N}\}$ is a number system if and only if*

(i) *Any roots α_i $(i = 1, \ldots, n)$ of $g(t)$ satisfy $|\alpha_i| > 1$.*

(ii) *$\mathcal{N}$ is a complete residue system modulo $|g_0|$ containing 0,*

(iii) *Any $\underline{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{Z}^n$ with $|y_i| < c_2$, $(i = 1, \ldots, n)$ has a unique preimage under the map T, where*

$$c_2 = \left|D_g^{-2}\right| (n|\bar{g}|^{n-1})^{n/2} A \max_{1 \le i \le n} \frac{|\alpha_i|}{(|\alpha_i| - 1)}$$

Remark. This is the generalization of Theorem 3 of Kovács and Pethö [5].

Proof. We shall use the notations of section 2. Let $w = w_0 \ldots w_l \in \mathcal{A}_{\mathcal{N}}$ and $T(w) = (z_0, \ldots, z_{n-1}) \in \mathbb{Z}^n$. We shall prove first the necessity of the conditions.

(i) Let α be a complex root of $g(t)$. Then we have

$$T_1(w)_\alpha = w_0 + w_1\alpha + \ldots + w_l\alpha^l = z_0 + z_1\alpha + \ldots + z_{n-1}\alpha^{n-1}. \tag{6.1}$$

If $|\alpha| < 1$, then the absolute value of the number staying on the left hand side of (6.1) is bounded independently of w, while the supremum of the right hand side is infinite, hence $|\alpha| \ge 1$. Assume now that $|\alpha| = 1$. Then α must be a root of unity (see the proof of Theorem 3. in Kovács and Pethö [5]). Let m be the smallest positive integer with $\alpha^m = 1$ and let $g_1(t) = g(t)/\gcd(g(t), t^m - 1)$. The degree of $g_1(t)$ is less then n and

$$g_1(t) \equiv g_1(t)t^m \pmod{g(t)}. \tag{6.2}$$

Suppose that

$$(T_3 \circ T_2)^{-1} g_1(\phi) = w_0 + x_1 t + \ldots + w_l t^l$$

with $w_i \in \mathcal{N}$, $w_l \neq 0$. Then we have

$$(T_3 \circ T_2)^{-1} g_1(\phi)\phi^{hm} = w_0 t^{hm} + \ldots + w_l t^{hm+l}$$

by (6.2) for any $h = 0, 1, \ldots$, hence T can not be bijective.

(ii) Let $\underline{x}_i = (x_{i0} \ldots x_{i,n-1})$, $i = 0, 1, \ldots$, where $\underline{x}_i$ is defined by (1.1). It follows $g_0 | x_{i0}$ immediately from (1.1), hence $z_0 \equiv w_0 \pmod{g_0}$ thus $\mathcal{N}$ contains a complete residue system modulo g_0.

Assume that $0 \neq w = w_0 \ldots w_l \in T^{-1}(0)$. Then $T_2 \circ T_1(w) = 0$ and $T_2 \circ T_1(ww) = T_2 \circ T_1(w) + t^{l+1} T_2 \circ T_1(w) = 0$, hence $T(w) = T(ww)$ and T is not even injective, so $0 \in \mathcal{N}$.

Assume finally that there exist $n_1, n_2 \in \mathcal{N}$ with $n_1 \equiv n_2 \pmod{g_0}$ but $n_1 \neq n_2$. Let $n_1 = n_2 + sg_0$ with an integer s. If $T^{-1}(sg_0) = h_0 \ldots h_l$, then $h_0 \equiv sg_0 \equiv 0 \pmod{g_0}$, hence $h_0 = 0$ and so

$$n_1 = (T_2 \circ T_1)^{-1}(n_1) = (T_2 \circ T_1)^{-1}(n_2 + sg_0) = n_2 h_1 \ldots h_l$$

which contradicts the bijectivity of T.

(iii) is obviously necessary for $\{g(t),\mathcal{N}\}$ to be an NS.

We shall now prove the sufficiency of (i),(ii) and (iii). If (i) and (ii) hold, then T is injective by Proposition 2.2. For a polynomial $p(t) = p_0 + p_1 t + \ldots + p_{n-1}t^{n-1} \in \mathbb{Z}[t]$ let

$$\begin{aligned} R(p(t)) &= w_{p(t)} = w, \quad \text{with } w \in \mathcal{N} \text{ and } w \equiv p_0 \pmod{g_0}, \\ S(p(t)) &= (p(t) - (p_0 - w)g(t)/g_0 - w)/t. \end{aligned}$$

The polynomial $S(p(t))$ has integer coefficients, it is of degree at most $n-1$ and it satisfies

$$p(t) = w_0 + w_1 t + \ldots + w_k t^k + S^{k+1}(p(t))t^{k+1} \tag{6.3}$$

for any $k = 0, 1, \ldots$, where $w_i = R(S^i(p(t)))$.

Let $\varepsilon > 0$ and choose $k = k(\varepsilon)$ so large that

$$|p(\alpha_i)/\alpha_i^{k+1}| < \varepsilon$$

hold for $i = 1, \ldots, n$. This is possible because of (i). We have by (6.3)

$$p(\alpha_i) = \sum_{j=0}^{k} w_j \alpha_i^j + S^{k-1}(p(t))_{\alpha_i}\alpha_i^{k+1},$$

which implies

$$|S^{k+1}(p(t))_{\alpha_i}| < \frac{|\alpha_i|}{|\alpha_i| - 1}A + \varepsilon. \qquad i = 1, \ldots, n. \tag{6.4}$$

Let $S^{k+1}(p(t)) = p_{k+1.0} + \ldots + p_{k-1.n-1}t^{n-1}$, where $p_{k+1,j} \in \mathbb{Z}$. The matrix (α_i^j) $i = 1, \ldots, n$; $j = 0, \ldots, n-1$ is invertible , because the roots of $g(t)$ are distinct. Hence there exists only finitely many possibilities for the polynomials $S^{k+1}(p(t))$. We may take ε arbitrarily small, hence choosing k large enough we get

$$|S^{k-1}(p(t))_{\alpha_i}| \leq \frac{|\alpha_i|}{|\alpha_i| - 1}A. \tag{6.5}$$

Considering (6.5) as a system of linear inequalities in $p_{k+1.0}, \ldots, p_{k+1,n}$ and using Hadamard's inequality we get $|p_{k+1,j}| \leq c_3$. The polynomial $S^{k+1}(p(t))$ has therefore a preimage under $T_1 \circ T_2$ by (iii). Inserting the resulting word into (6.3) we get the preimage of $p(t)$ which proves the theorem. □

In the sequel let

$$|\underline{g}| = \min\{|\alpha| \ : \ \alpha \text{ a root of the polynomial } g(t)\}.$$

Theorem 6.2. *Let $g(t)$ be a squarefree polynomial such that $|\underline{g}| > 1$ and let $\{g(t),\mathcal{N}\}$ be a WNS. Then there exists a constant c_4 depending only on $n, g(t)$ and A such that*

$$m(w) \leq An^{n/2}|\overline{g}|^{l(w)-1+n(n-1)/2}(|\underline{g}| - 1)^{-1} \tag{6.6}$$

and

$$l(w) \leq \frac{\log\ m(w)}{\log\ |\underline{g}|} + c_4 \tag{6.7}$$

hold for any $w \in \mathcal{N}$.

Proof. Let $\alpha_1, \ldots, \alpha_n$ denote the roots of $g(t)$, let $w = w_0 \ldots w_l$ and $T(w) = (y_0, \ldots, y_{n-1})$. Then we have

$$y_0 + \ldots + y_{n-1}\alpha_i^{n-1} = w_0 + \ldots + w_l\alpha_i^l\ . \qquad i = 1, \ldots, n.$$

Hence

$$\left|y_0 + \ldots + y_{n-1}\alpha_i^{n-1}\right| \leq \frac{|\alpha_i|^{l+1} - 1}{|\alpha_i| - 1}.$$

Using again Hadamard's inequality we get

$$m(w) = \max_{1 \leq i \leq n} |y_i| \leq An^{n/2}|\bar{g}|^{l(w)+1+n(n-1)/2}(|\underline{g}| - 1)^{-1}.$$

For $w = 0$ the inequality (6.7) is obviously true with $c_4 = 1$, hence we may assume $w \neq 0$ in the following. Take

$$k = \left\lceil \frac{\log\ m(w)}{\log\ |\underline{g}|} - \min_{1 \leq i \leq n} \frac{\log(|\alpha_i| - 1)}{\log\ |\alpha_i|} \right\rceil + n + 1.$$

then

$$\frac{1}{|\alpha_i|^k}\left|y_0 + \ldots + y_{n-1}\alpha_i^{n-1}\right| \leq \frac{m(w)|\alpha_i|^n}{|\alpha_i|^k(|\alpha_i| - 1)} < 1$$

holds for any $i = 1, \ldots, n$. This inequality implies (6.4) with $\varepsilon = 1$. There exists only finitely many polynomials in $\mathbb{Z}[t]/g(t)\mathbb{Z}[t]$ for which (6.4) holds. Let c_5 denotes the maximum of the length of the preimages of this polynomials. Then

$$l(w) \leq k + c_5 = \frac{\log\ m(w)}{\log\ |\underline{g}|} + c_4,$$

and the theorem is proved. □

The quantity $\mu(w) = n \log\ m(w)$ is a natural measure for the size of $w \in \mathcal{A}_{\mathcal{N}}$. Theorems 3.1 and 6.2 implies immediately the following

Theorem 6.3. *Let* $\{g(t), \mathcal{N}\}$ *be as in Theorem 6.2. Then the Algorithms 3.1 and 3.2 terminate successfully after* $O(\mu(w))$ *operations on integers of size* $O(\mu(w))$ *where the O-constant depends only on the choice of the number system, namely on* $g(t)$ *and* $\mathcal{N}$.

7 A special case

Let a polynomial $g(t) = t^n + g_{n-1}t^{n-1} + \ldots + g_0 \in \mathbb{Z}[t]$ with $|g_0| \geq 2$ and a finite subset $\mathcal{N}$ of $\mathbb{Z}$ be given. To verify that T is injective, which is most important for the applications in cryptography, $O(|g_0|^2)$ operations are needed by Proposition 2.2. In Theorem 6.1 we proved necessary and sufficient conditions for $\{g(t), \mathcal{N}\}$ to be an NS. It is easy to check whether $g(t)$ is squarefree as well as the conditions (i) and (ii), but to verify (iii) generally extensive computations are needed. The example $g(t) = x^3 - 2x^2 - x - 4$, $\mathcal{N} = \{0, 1, 2, 3\}$ shows that $\{g(t), \mathcal{N}\}$ is a WNS for which (i) and (ii) hold, but it is not an NS because for example -1 does not have a preimage. Hence (iii) is necessary too.

For a wide class of pairs $\{g(t), \mathcal{N}\}$ we are able to prove however that it is an NS. The idea goes back to Kovács [3]. We assume in the sequel that $0 < g_{n-1} \leq \ldots \leq g_0$, $g_0 \geq 2$ and none of the roots of $g(t)$ are roots of unity. We take finally $\mathcal{N} = \{0, \ldots, g_0 - 1\}$. We are given now a variant of the decryption Algorithm 3.2, however, for simplicity, only for a single input block.

Algorithm 7.1.

Input: $\underline{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n$.

Output: $w = w_0 \ldots w_{l(w)} \in \mathcal{A}_{\mathcal{N}}$

(1) *Put* $l(w) = n - 1$, $w_i = x_i$ $(0 \leq i \leq l(w))$, $p(t) = \sum_{i=0}^{l(w)} w_i t^i$, $j = 0$.

(2) *Set* $\hat{p}(t) = p(t) = p(t)\lambda g(t)$ *with* $\lambda = \max\Big\{\big[-\min_{0 \leq i \leq n-1} w_i/g_i\big], 0\Big\}$.
If $\lambda \neq 0$ *then set* $l(w) = l(w) + 1$. *Set* $\lambda = 0$.

(3) *Repeat until* $j > l(w)$

if $w_j \notin \mathcal{N}$ *then set* $\hat{p}(t) = p(t) + \lambda g(t)t^j$, *and determine*

$y_j \in \mathcal{N}$ *such that* $y_j \equiv w_j \pmod{g_0}$ *and set* $\lambda = (w_j - y_j)/g_0$,

$p(t) = \hat{p}(t) - \lambda g(t)t^j$, $l(w) = n + j$.

Set $j = j + 1$.

(4) *While* $l(w) > 0$ *and* $w_{l(w)} = 0$ *do* $l(w) = l(w) - 1$.

Remark. We used in Algorithm 7.1 the polynomial $\hat{p}(t)$ only for the convenience of the proof of the next theorem. One can easily modify Step 3 without using $\hat{p}(t)$.

Theorem 7.1. *Algorithm 7.1 terminates successfully i.e* $\{g, \mathcal{N}\}$ *is a NS. If* $g(t)$ *is squarefree then it takes* $O(\mu(w))$ *operations on numbers if size* $O(\mu(w))$ *where*

the O-constant depends only on the choice of the polynomial $g(t)$. More precisely, we have on every stage of the algorithm

$$\sum_{j=0}^{l(w)} |\hat{w}_j| < (n+1)(1+g_0)m(w), \tag{7.1}$$

where $\hat{p}(t) = \sum_{j=0}^{l(w)} \hat{w}_j t^j$.

Proof. After stage 2. all the coefficients of $p(t)$ and $\hat{p}(t)$ are non–negative and an easy computation shows that for the coefficients of $\hat{p}(t)$ (7.1) holds. We shall show that in the repeat loop the coefficients of $\hat{p}(t)$ remain always non–negative and their sum can not increase. In the sequel we set $g_n = 1$ and $g_{n+1} = g_{n+2} = \ldots = 0$.

Of course if $w_j \in \mathcal{N}$ then nothing else as an increment of j is done. Assume that $w_j \notin \mathcal{N}$. At the first occurrence of this event $\lambda = 0$, hence $\hat{p}(t)$ remains unchanged and the assertion is true. Otherwise, assume that $j_1 < j$ was the last index when $w_{j_1} \notin \mathcal{N}$ occurred. At this stage the algorithm sets $\lambda \neq 0$ and

$$p(t) = \hat{p}(t) - \lambda g(t) t^{j_1} = \sum_{i=0}^{j_1-1} \hat{w}_i t^i + \sum_{i=0}^{n} \left(\hat{w}_{j_1+i} - \lambda g_i \right) t^{j_1+i}. \tag{7.2}$$

Between the occurrence $w_{j_1} \notin \mathcal{N}$ and $w_j \notin \mathcal{N}$ the data $p(t)$ and λ do not change, which means that $w_i = \hat{w}_i$, $i = 0, \ldots, j_1$ and $w_{j_1+1} = \hat{w}_{j_1+1} - \lambda g_1, \ldots, w_{j-1} = \hat{w}_{j-1} - \lambda g_{j-1-j_1}$ are all non–negative. When $w_j \notin \mathcal{N}$ occurs then the algorithm sets

$$\hat{p}(t) = p(t) + \lambda g(t) t^j = \sum_{i=0}^{j} w_i t^i + \sum_{i=0}^{n} \left(w_{j+i} + \lambda g_i \right) t^{j+i}.$$

Using (7.2) we get

$$w_{j+s} + \lambda g_s = \hat{w}_{j+s} - \lambda g_{j-j_1+s} + \lambda g_s \geq \hat{w}_{j+s} \geq 0$$

for $s = 0, \ldots, n$ by the monoton decreasing property of the coefficients of $g(t)$.

The sum of the coefficients of the modified $\hat{p}(t)$ is

$$\sum_{i=0}^{j+n} w_i + \lambda \sum_{i=0}^{n} g_i = \sum_{i=0}^{j+n} \hat{w}_i - \lambda \sum_{i=0}^{n} g_i + \lambda \sum_{i=0}^{n} g_i = \sum_{i=0}^{j+n} \hat{w}_i.$$

So we proved (7.1).

Take $\hat{p}(t) = \hat{w}_0 + \ldots + \hat{w}_{l(w)} t^{l(w)}$ and $S_j(\hat{p}(t)) = \hat{w}_j + \ldots + \hat{w}_{l(w)} t^{l(w)}$. Then

$$\hat{p}(t) = \hat{w}_0 + \ldots + \hat{w}_{j-1} t^{j-1} + t^j S_j(\hat{p}(t))$$

holds. The coefficients of $S_j(\hat{p}(t))$ are non–negative and their sum is bounded, there exists so only finitely many possibilities for $S_j(\hat{p}(t))$. If Algorithm 7.1 would be non–finite, then there would exist integers $0 \leq j_1 \leq j_2$ such that $S_{j_1}(\hat{p}(t)) = S_{j_2}(\hat{p}(t))$. This means that there exists a polynomial $q(t) \in \mathcal{N}[t]$ with

$$S_{j_1}(\hat{p}(t)) = q(t) + t^{j_2-j_1} S_{j_2}(\hat{p}(t)). \tag{7.3}$$

We have $q(t) = 0$ because it has non–negative coefficients and the sum of the coefficients on both sides of (7.3) is equal. Hence

$$S_{j_1}(\hat{p}(t))\ (t^{j_2-j_1} - 1) = 0$$

holds in $\mathbb{Z}[t]/g(t)\mathbb{Z}[t]$. The assumption that none of the roots of $g(t)$ are roots of unity and the last equality implies $g(t)|S_{j_1}(\hat{p}(t))$. Hence $p(t) = w_0 + \ldots + w_{j_1-1}t^{j_1-1} + 0t^{j_1} + \ldots + 0t^{l(w)}$ holds after $j = j_1$ in the repeat loop, we have therefore in the remaining steps always $w_j \in \mathcal{N}$ and the algorithm terminates.

The second statement follows immediately from Theorem 6.2 and (7.1). □

References

[1] P. Horster. *Kryptographie*. Reihe Informatik **47** (1985). Bibliographisches Institut, Mannheim. Wien. Zürich.

[2] D.E. Knuth. *The art of computer programming. Vol. 2 Seminumerical algorithms*, Second edition. Addison-Wesley Publ. Co.. 1981.

[3] B. Kovács. *Canonical number system in algebraic number fields*. Acta Math. Acad. Sci. Hungar. **37** (1981). 405-407.

[4] B. Kovács and A. Pethö. *Canonical systems in the ring of integers*. Publ. Math Debrecen **30** (1983). 39-45.

[5] B. Kovács and A. Pethö. *Number systems in integral domains especially in orders of algebraic number fields*. to appear (Acta Sci. Math. Szeged).

[6] R.C. Merkle and M.E. Hellman. *Hiding information and signatures in trapdoor knapsacks*. IEEE IT **24** (1978). 525-530.

[7] A. Shamir. *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem*. FOCS **23** (1982). 145-152.