Generalized Number Systems and Secure Electronic Elections

Ph.D. Thesis

Andrea Huszti

Supervisor: Prof. Attila Pethő

University of Debrecen
Doctoral Committee of Natural Sciences
Doctoral School of Computer Sciences

Debrecen, 2008

Contents

Summary **1**

Összefoglaló (Hungarian summary) **16**

Bibliography **32**

Appendix **38**

Summary

The present dissertation is based on two more or less independent topics, dealing with generalized number systems and cryptographically secure electronic elections. In the first part we investigate Canonical Number Systems in quartic algebraic number fields, then we characterize three-dimensional Symmetric Shift Radix Systems. In the second part of the dissertation two secure election schemes are described, one of them is based on blind signatures the other one uses homomorphic encryptions.

Canonical Number Systems can be viewed as natural generalizations of radix representations of ordinary integers (Grünwald [19]) to algebraic integers. An example of a canonical number system was first studied by Knuth [30], [31]. They showed that the complex number $b = -1 + \sqrt{-1}$ can be used as a base for a number system which admits finite representations for each Gaussian integer. This observation has been generalized and studied extensively in the last decades.

CNS have connections to the theories of finite automata (see e.g. K. Scheicher [46], J. M. Thuswaldner [51]) and fractal tilings (see e.g. S. Akiyama and J. M. Thuswaldner [7]). S. Akiyama et al. [2] put Canonical Number Systems (CNS) into a more general framework thereby opening links to other areas, e.g. to a long-standing problem on Salem numbers.

In [2] a dynamical system called Shift Radix System (SRS) has been introduced. SRS are related to number systems as β-expansions (*cf.* for instance [15, 40, 44]) or Canonical Number Systems. Indeed they form a unification and generalization of these notions of number systems. More details about SRS and their relation to β-expansions and CNS can be found in [2], [3], [48]. We deal with an important variant of SRS, the so-called Symmetric Shift Radix Systems (SSRS), which was introduced in [6].

Cryptographic protocols, for example secure voting schemes, are as strongly related to number theory as generalized number systems. Security of constructions of cryptographic primitives are based on problems from number theory which seem to be computationally intractable. The most well-known of these problems are calculating discrete logarithms and factoring composite integers. Electronic election schemes according to the applied

cryptographic techniques can be categorized into three main models:

The mix-net model. Chaum [11] introduces the concept of a mix-net that is built up from several linked servers called mixes. Each mix randomizes input messages and outputs the permutation of them, such that the input and output messages are not linkable to each other. Several schemes based on mix-nets are proposed in the literature ([39], [45], [25]).

The blind signatures model. The concept of blind signatures was introduced by Chaum [12]. During the Authorizing stage a voting authority authenticates a token, (usually an encrypted vote) without knowing the contents. This way of authentication is achieved by applying blind signatures. Even if later the (un-blinded) signature is made public, it is impossible to connect the signature to the signing process, *i.e.* to the voter. For further schemes see [16], [22], [37], [38], [43].

The homomorphic encryption model. Schemes based on homomorphic encryptions employ s authorities in order to manage Voting and Tallying stages. These schemes use secret sharing scheme either to share the decryption key, or to share the vote itself. Models based on homomorphic encryption are [13], [32], [8], [14] and [20].

The concept of *receipt-freeness* and *uncoercibility* were introduced by Benaloh and Tuinstra [9]. Roughly speaking, receipt-freeness is the inability of a voter to prove an adversary that he voted in a particular manner, even if the voter wishes to do so. Several receipt-free and uncoercible voting schemes are designed with applying untappable channels or voting booths, that are unpractical [38] or employ an extra tamper-resistant hardware [34].

Generalized Number Systems

In the second chapter we deal with **Canonical Number Systems**. CNS bases are explicitly known for some quadratic, cubic and quartic fields ([26],[27],[17],[18],[51],[5],[29],[4],[42]). Our main result is the characterization of CNS bases in algebraic number fields including quartic cyclotomic fields, simplest quartic fields and two families of orders in quartic number fields. The results of this chapter are contained in our paper [10]. This paper is a joint work with Horst Brunotte and Attila Pethő.

In the sequel we denote by $\mathbb{Q}$ the field of rational numbers, by $\mathbb{Z}$ the set of integers and by $\mathbb{N}$ the set of nonnegative integers. For an algebraic integer γ we let $\mu_\gamma \in \mathbb{Z}[X]$ be its minimal polynomial and $\mathcal{C}_\gamma$ the set of all CNS bases for $\mathbb{Z}[\gamma]$.

Definition 1 *Let* $P(X) = X^d + p_{d-1}X^{d-1} + \cdots + p_1X + p_0 \in \mathbb{Z}[X]$, $N = \{0, 1, \ldots, |p_0| - 1\}$ *and* $\mathcal{R} := \mathbb{Z}[X]/P(X)\mathbb{Z}[X]$ *and denote the image of* X

under the canonical epimorphism from $\mathbb{Z}[X]$ to $\mathcal{R}$ by x. If every non-zero element $A(x) \in \mathcal{R}$ can be written uniquely in the form $A(x) = a_0 + a_1 x + \cdots + a_l x^l$ with $a_0, \ldots, a_l \in N, a_l \neq 0$, we call (P, N) a canonical number system (CNS for short). $P(X)$ is called CNS polynomial, to N we refer as the set of digits.

We denote by $\mathcal{C}$ the set of CNS polynomials, and α is a CNS basis for $\mathbb{Z}[\alpha]$ if and only if μ_α is a CNS polynomial. It can algorithmically be decided whether a given integral polynomial is a CNS polynomial or not (see [1]).

Lemma 1 *(B. Kovács – A. Pethő) For every nonzero algebraic integer α the following constants can be computed effectively:*

1. $k_\alpha = \min\{k \in \mathbb{Z} \,|\, \mu_\alpha(X + n) \in \mathcal{K} \text{ for all } n \in \mathbb{Z} \text{ with } n \geq k\}$,
2. $c_\alpha = \min\{k \in \mathbb{Z} \,|\, \mu_\alpha(X + k) \in \mathcal{C}\}$.

Definition 2 *The algebraic integer α is called a fundamental CNS basis for R if it satisfies the following properties:*

1. *$\alpha - n$ is a CNS basis for R for all $n \in \mathbb{N}$.*
2. *$\alpha + 1$ is a not CNS basis for R.*

Theorem 1 *Let γ be an algebraic integer. Then there exist finite effectively computable disjoint subsets $\mathcal{F}_0(\gamma), \mathcal{F}_1(\gamma) \subset \mathcal{C}_\gamma$ with the properties:*

(i) For every $\alpha \in \mathcal{C}_\gamma$ there exists some $n \in \mathbb{N}$ with $\alpha + n \in \mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma)$.

(ii) $\mathcal{F}_1(\gamma)$ consists of fundamental CNS bases for $\mathbb{Z}[\gamma]$.

By a theorem of B. Kovács [28] there exists CNS in an order if and only if there exists power integral bases. For finding CNS bases a modified version of the algorithm given by B. Kovács and A. Pethő [29] is applied. This algorithm finds sets $\mathcal{F}_0(\gamma)$ and $\mathcal{F}_1(\gamma)$ with properties (i) and (ii) of Theorem 1..

Algorithm is as follows:
Input: A nonzero algebraic integer γ and a (finite) set $\mathcal{B}$ of representatives of the equivalence classes of generators of power integral bases of $\mathbb{Z}[\gamma]$.
Output: The sets $\mathcal{F}_0(\gamma)$ and $\mathcal{F}_1(\gamma)$.

1 [Initialize] Set $\{\beta_1, \ldots, \beta_t\} = \mathcal{B} \cup (-\mathcal{B})$, $F_0 = F_1 = T = \emptyset$ and $i = 1$.

2 [Compute minimal polynomial] Compute $P = \mu_{\beta_i}$.

3 [Element of $F_0 \cup F_1$ found?] If there exist $k \in \mathbb{Z}, \delta \in \{0, 1\}$ with $(P, k, \delta) \in T$ insert $\beta_i - k$ into F_δ and go to step 11.

4 [Determine upper and lower bounds] Calculate k_{β_i} and c_{β_i}.

5 [Insert element into F_1?] If $k_{\beta_i} - c_{\beta_i} \leq 1$ insert $\beta_i - c_{\beta_i}$ into F_1, $(P, c_{\beta_i}, 1)$ into T and go to step 11, else perform step 6 for $l = c_{\beta_i} + 1, \ldots, k_{\beta_i} - 1$, put $p_{k_{\beta_i}} = 1, k = c_{\beta_i}$ and go to step 8.

6 [Check CNS property] If $P(X + l) \in \mathcal{C}$ set $p_l = 1$, otherwise set $p_l = 0$.

7 [Check CNS basis condition] If $p_k = 0$ then go to step 9.

8 [Insert element into $F_0 \cup F_1$] If $p_{k+1} = \cdots = p_{k_{\beta_i}} = 1$ insert $\beta_i - k$ into F_1, $(P, k, 1)$ into T and go to step 11, else insert $\beta_i - k$ into F_0 and $(P, k, 0)$ into T.

9 [Next value of k] Set $k \leftarrow k + 1$.

10 [CNS basis check finished?] If $k \leq k_{\beta_i} - 1$ then go to step 7.

11 [Next generator] Set $i \leftarrow i + 1$.

12 [Finish?] If $i \leq t$ then go to step 2.

13 [Terminate] Output $\mathcal{F}_0(\gamma) = F_0$ and $\mathcal{F}_1(\gamma) = F_1$ and terminate the algorithm.

Now we will treat the cyclotomic fields of degree 4.

Theorem 2 *Let $\zeta_5, \zeta_8, \zeta_{12}$ be a primitive fifth, eighth and twelfth root of unity respectively. Then we have $\mathcal{F}_0(\mathbb{Q}(\zeta_i)) = \emptyset$ for $i \in \{5, 8, 12\}$ and*
$\mathcal{F}_1(\mathbb{Q}(\zeta_5)) = \{-2 + \zeta_5, -3 - \zeta_5, -2 + \zeta_5 + \zeta_5^3, -3 - \zeta_5 - \zeta_5^3\}$.
$\mathcal{F}_1(\mathbb{Q}(\zeta_8)) = \{-3 \pm \zeta_8^k \mid k = 1, 3, 5, 7\}$.
$\mathcal{F}_1(\mathbb{Q}(\zeta_{12})) = \{-3 + \zeta_{12}, -3 - \zeta_{12}, -3 + \zeta_{12}^{-1}, -3 - \zeta_{12}^{-1}, -1 - \zeta_{12}^2 + \zeta_{12}^{-1}, -2 + \zeta_{12}^2 - \zeta_{12}^{-1}\}$.

Let us consider a family of orders in a parameterized family of quartic number fields, where all power integral bases are known. Let $t \in \mathbb{Z}$, $t \geq 0$, and $P(X) = X^4 - tX^3 - X^2 + tX + 1$. Denote by α one of the zeros of $P(X)$. In the following we deal with the order $\mathcal{O} = Z[\alpha]$ of $Q(\alpha)$. Based on paper of M. Mignotte, A. Pethő and R. Roth [35] we give the following result.

Theorem 3 *Let $t \geq 4$. We have $\mathcal{F}_0(\mathbb{Q}(\alpha)) = \emptyset$ and $\mathcal{F}_1(\mathbb{Q}(\alpha)) = \mathcal{G}_4 \cup \mathcal{G}_t$ where*

$$\begin{aligned} \mathcal{G}_4 &= \left\{209\alpha + 140\alpha^2 - 49\alpha^3 + 350, 209\alpha - 312\alpha^2 + 64\alpha^3 - 71\right\} \\ \mathcal{G}_t &= \big\{\alpha + t + 1, \alpha + t\alpha^2 - \alpha^3 + t + 2, t\alpha + (t-1)\alpha^2 - \alpha^3 + 8, \\ &\quad t\alpha - (t+1)\alpha^2 + \alpha^3 + 2, \alpha - \alpha^3 + 2, \\ &\quad \alpha - t(t^2+1)\alpha^2 + t^2\alpha^3 - t + 1\big\}. \end{aligned}$$

For $t \in \mathbb{Z} \setminus \{0, \pm 3\}$ let $P_t(X) = X^4 - tX^3 - 6X^2 + tX + 1$. Let $\vartheta = \vartheta_t$ be a root of $P_t(X)$, then the infinite parametric family of number fields $K_t = K = Q(\vartheta_t)$ is called *simplest quartic fields*. Power integral bases in the polynomial order $\mathbb{Z}[\alpha]$ of K_t were described by G. Lettl and A. Pethő [33].

Theorem 4 *Let $t \in \mathbb{N} \setminus \{0, 3\}$ and ϑ denote a root of the polynomial $X^4 - tX^3 - 6X^2 + tX + 1$. Then we have $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$ and $\mathcal{F}_1(\mathbb{Q}(\vartheta)) = \mathcal{G} \cup \mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_4$ where*

$$\mathcal{G} = \begin{cases} \{-3-\vartheta, -t-2+\vartheta, -2-6\vartheta-t\vartheta^2+\vartheta^3, \\ -t-3+6\vartheta+t\vartheta^2-\vartheta^3\}, \text{ if } t \geq 5, \\ \emptyset \text{ otherwise}, \end{cases}$$

$$\mathcal{G}_1 = \begin{cases} \{-4+\vartheta, -4-\vartheta, -5+6\vartheta+\vartheta^2-\vartheta^3, \\ -3-6\vartheta-\vartheta^2+\vartheta^3, -23+3\vartheta^2-\vartheta^3, -1-3\vartheta^2+\vartheta^3, \\ -14+25\vartheta+2\vartheta^2-4\vartheta^3, -10-25\vartheta-2\vartheta^2+4\vartheta^3\}, \\ \text{if } t = 1, \\ \emptyset \text{ otherwise}, \end{cases}$$

$$\mathcal{G}_2 = \begin{cases} \{-5+\vartheta, -3-\vartheta, -5+6\vartheta+2\vartheta^2-\vartheta^3, \\ -3-6\vartheta-2\vartheta^2+\vartheta^3\}, \text{ if } t = 2, \\ \emptyset \text{ otherwise}, \end{cases}$$

$$\mathcal{G}_4 = \begin{cases} \{-6+\vartheta, -3-\vartheta, 1+9\vartheta-22\vartheta^2+4\vartheta^3, \\ -78-9\vartheta+22\vartheta^2-4\vartheta^3, -7+6\vartheta+4\vartheta^2-\vartheta^3, \\ -3-6\vartheta-4\vartheta^2+\vartheta^3, -62+74\vartheta+30\vartheta^2-9\vartheta^3, \\ -15-74\vartheta-30\vartheta^2+9\vartheta^3\}, \text{ if } t = 4, \\ \emptyset \text{ otherwise}. \end{cases}$$

P. Olajos [36] proved that K_t admits a power integral bases if and only if $t = 2$ and $t = 4$, moreover he found all generators of power integral bases in these fields. Using his result we are able to compute all CNS bases in such fields.

Theorem 5 *We have $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$, $\mathcal{F}_1(\mathbb{Q}(\vartheta_2)) = \mathcal{G}_2$ and $\mathcal{F}_1(\mathbb{Q}(\vartheta_4)) = \mathcal{G}_4$, where $\mathcal{G}_2$ and $\mathcal{G}_4$ contains 19 and 12 elements, respectively.*

The sets mentioned above are explicitly given in the dissertation.

Chapter three is devoted to **Symmetric Shift Radix Systems**. Two dimensional SSRS is treated in [6] by Akiyama and Scheicher, we will deal with three-dimensional SSRS.

The results of this chapter are based on [24], that is a joint work with Klaus Scheicher, Paul Surer and Jörg M. Thuswaldner.

Definition 3 (*cf.* [6]) *Let $d \geq 1$ be an integer, $\mathbf{r} \in \mathbb{R}^d$, and let*

$$\tau_{\mathbf{r}} : \mathbb{Z}^d \to \mathbb{Z}^d, \quad \mathbf{a} = (a_1, \ldots, a_d) \mapsto \left(a_2, \ldots, a_d, -\left\lfloor \mathbf{ra} + \frac{1}{2} \right\rfloor \right). \tag{1}$$

Then $\tau_{\mathbf{r}}$ is called a symmetric shift radix system (SSRS for short), if $\forall \mathbf{a} \in \mathbb{Z}^d \quad \exists n \in \mathbb{N} : \tau_{\mathbf{r}}^n(\mathbf{a}) = \mathbf{0}$.

Let

$$\mathcal{D}_d := \left\{ \mathbf{r} \in \mathbb{R}^d \,\middle|\, \forall \mathbf{a} \in \mathbb{Z}^d \, \exists n, l \in \mathbb{N} : \tau_{\mathbf{r}}^k(\mathbf{a}) = \tau_{\mathbf{r}}^{k+l}(\mathbf{a}) \; \forall k \geq n \right\} \text{ and}$$
$$\mathcal{D}_d^0 := \left\{ \mathbf{r} \in \mathbb{R}^d \,\middle|\, \tau_{\mathbf{r}} \text{ is an SSRS} \right\}.$$

As a new result we prove that $\mathcal{D}_3^0$ is an union of four polyhedra and a polygon, by employing the algorithm that is established for SSRS in [6]. In [6] it has been shown that

$$\mathcal{E}_d(1) \subset \mathcal{D}_d \subset \overline{\mathcal{E}_d(1)}. \tag{2}$$

For $\mathbf{r} = (r_1, \ldots, r_d) \in \mathcal{D}_d$, an element $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d \setminus \{0\}$ is a *non-zero periodic point of τ_r of period L*, if $\mathbf{a} = \tau_{\mathbf{r}}^L(\mathbf{a})$. From the definition of $\mathcal{D}_d^0$ it follows that the existence of such a periodic point is necessary and sufficient for $\mathbf{r} \notin \mathcal{D}_d^0$. Suppose that the period defined by $\mathbf{a}$ runs through the orbit

$$\tau_{\mathbf{r}}^j(\mathbf{a}) = (a_{1+j}, \ldots, a_{d+j}) \quad (0 \leq j \leq L-1),$$

where $a_{L+1} = a_1, ..., a_{L+d-1} = a_{d-1}$. We denote such a period by

$$(a_1, \ldots, a_d); a_{d+1}, \ldots, a_L$$

and say that it is a period of $\tau_{\mathbf{r}}$ or just a *period of $\mathcal{D}_d$*.

Let a non-zero period $\pi := (a_1, \ldots, a_d); a_{d+1}, \ldots, a_L$ be given. We may ask for the set $P(\pi)$ of all $\mathbf{r} \in \mathcal{D}_d$ for that π occurs as a period of $\tau_{\mathbf{r}}$. By the definition of $\tau_{\mathbf{r}}$, an element $\mathbf{r} \in P(\pi)$ has to satisfy the system of L double inequalities

$$-\frac{1}{2} \leq r_1 a_{1+i} + r_2 a_{2+i} + \cdots + r_d a_{d+i} + a_{d+1+i} < \frac{1}{2}. \tag{3}$$

Here i runs from 0 to $L-1$ and $a_{L+1} = a_1, \ldots, a_{L+d} = a_d$. Such a system characterizes a convex polyhedron, which is possibly degenerated or equal to the empty set. Therefore we will call $P(\pi)$ a *cutout polyhedron*. Since each point $\mathbf{r} \in P(\pi)$ has π as a period of the associated mapping $\tau_{\mathbf{r}}$ the set $P(\pi)$ has empty intersection with $\mathcal{D}_d^0$. Thus we get the representation

$$\mathcal{D}_d^0 = \mathcal{D}_d \setminus \bigcup_{\pi \neq \mathbf{0}} P(\pi),$$

where the union is extended over all non-zero periods π. Since the set of periods is infinite, this expression is not suitable for calculations. The following theorem shows how to reduce the set of possible periods to a finite

set and gives an efficient algorithm for a closed subset H of $\operatorname{int}\mathcal{D}_d = \mathcal{E}_d(1)$ to determine $H \cap \mathcal{D}_d^0$. Let $\mathbf{e}_i$ be the i-th canonical unit vector. For an $\mathbf{r} = (r_1, \ldots, r_d) \in \operatorname{int}\mathcal{D}_d$, denote by $\mathcal{V}(\mathbf{r}) \subset \mathbb{Z}^d$ the smallest set with the properties

1. $\pm\mathbf{e}_i \in \mathcal{V}(\mathbf{r}), i = 1, \ldots, d$,
2. $(a_1, \ldots, a_d) \in \mathcal{V}(\mathbf{r}) \Rightarrow (a_2, \ldots, a_{d+1}) \in \mathcal{V}(\mathbf{r})$ where a_{d+1} satisfies

$$-1 < r_1a_1 + r_2a_2 + \cdots + r_da_d + a_{d+1} < 1.$$

$\mathcal{V}(\mathbf{r}) \subset \mathbb{Z}^d$ is called a *set of witnesses* for $\mathbf{r}$. Additionally define $\mathcal{G}(\mathcal{V}(\mathbf{r})) = V \times E$ to be the graph with set of vertices $V = \mathcal{V}(\mathbf{r})$ and set of edges $E \subset V \times V$ such that

$$\forall \mathbf{a} \in V : (\mathbf{a}, \tau_{\mathbf{r}}(\mathbf{a})) \in E.$$

Theorem 6 (*cf.* [6]) *Let $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_k \in \mathcal{D}_d$ and let $H := \square(\boldsymbol{r}_1, \ldots, \boldsymbol{r}_k)$ be the convex hull of $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_k$. Assume that $H \subset \operatorname{int}\mathcal{D}_d$ and sufficiently small in diameter. Then there exists an algorithm to construct a finite directed graph $G(H) = V \times E$ with vertices $V \subset \mathbb{Z}^d$ and edges $E \subset V \times V$ which satisfies*

1. *$\pm\boldsymbol{e}_i \in V$ for all $i = 1, \ldots, d$,*
2. *$\mathcal{G}(\mathcal{V}(\boldsymbol{x}))$ is a subgraph of $G(H)$ for all $\boldsymbol{x} \in H$,*
3. *$H \cap \mathcal{D}_d^0 = H \setminus \bigcup_\pi P(\pi)$, where π runs through all periods induced by the nonzero primitive cycles of G.*

Our aim is to characterize $\mathcal{D}_3^0$. We already know that

$$\mathcal{E}_3(1) \subset \mathcal{D}_3 \subset \overline{\mathcal{E}_3(1)}.$$

From [47, 49] we calculate

$$\mathcal{E}_3(1) = \{(x, y, z) \in \mathbb{R}^3 |\ |x| < 1, |y - xz| < 1 - x^2, |x + z| < |y + 1|\}.$$

Let

$$\begin{aligned}\mathcal{E}_3' := \big\{(x, y, z) \in \mathbb{R}^3 \big|\ |x| \le 1 \wedge |y - xz| \le 1 - x^2 \\ \wedge |x + z| \le |y + 1| \wedge |y - 1| \le 2 \wedge |z| \le 3\big\}\end{aligned}$$

and consider the intersection of $\mathcal{E}_3'$ with the hyperplane

$$A_c := \big\{(x, y, z) \in \mathbb{R}^3 \mid x - c = 0\big\}$$

for constant c.

Lemma 2 *For any $|c| < 1$ the intersection of $\mathcal{E}_3'$ with the plane A_c yields the closed triangle $\triangle(A_c^{(1)}, A_c^{(2)}, A_c^{(3)})$ with $A_c^{(1)} = (c, -1, -c), A_c^{(2)} = (c, 1 - 2c, c - 2), A_c^{(3)} = (c, 2c + 1, c + 2)$.*

Theorem 7 $\overline{\mathcal{E}_3(1)} = \mathcal{E}_3'$.

The number of inequalities can be reduced, we gain

$$\overline{\mathcal{E}_3(1)} = \left\{(x, y, z) \,\middle|\, |x + z| \leq 1 + y \wedge y - xz \leq 1 - x^2 \wedge |z| \leq 3\right\}.$$

For giving the complete description of $\mathcal{D}_3^0$ we define the sets

$$\begin{aligned}
S_1 := \{(x,y,z) \mid\ & 2x - 2z \geq 1 \wedge 2x + 2y + 2z > -1 \wedge 2x + 2y \leq 1 \\
& \wedge 2x \leq 1 \wedge 2x - 2y + 2z \leq 1\}, \\
S_2 := \{(x,y,z) \mid\ & x - z \leq -1 \wedge 2x - 2y + 2z \leq 1 \wedge -2x + 2y \leq 1 \\
& \wedge 2x > -1\}, \\
S_3 := \{(x,y,z) \mid\ & x - z > -1 \wedge 2x - 2y + 2z \leq 1 \wedge -2x + 2y < 1 \\
& \wedge 2x > -1 \wedge 2x - 2z < -1 \wedge 2x + 2y + 2z > -1\}, \\
S_4 := \{(x,y,z) \mid\ & 2x - 2y + 2z \leq 1 \wedge -2x + 2y \leq 1 \\
& \wedge 2x - 2z = -1, \wedge 2x + 2y + 2z > -1\}, \\
S_5 := \{(x,y,z) \mid\ & -1 < 2x \leq 1 \wedge -1 < 2x - 2z \leq 1 \\
& \wedge 2x + 2y + 2z > -1 \wedge 2x - 2y + 2z \leq 1 \\
& \wedge 2x + 4y - 2z < 3 \wedge 2y \leq 1\}
\end{aligned}$$

and denote their union by

$$\mathcal{S} := \bigcup_{i \in \{1,\ldots,5\}} S_i.$$

Note that S_1, S_2, S_3, S_5 are polyhedra while S_4 is a polygon.

Theorem 8 $\mathcal{D}_3^0 = \mathcal{S}$

We give an outline of the proof. In a first step we will use Theorem 6. in order to show that

$$\mathcal{S} \subseteq \mathcal{D}_3^0. \tag{4}$$

For showing the opposite inclusion we need a set of nonzero periods Π such that for $\mathcal{P} := \bigcup_{\pi \in \Pi} P(\pi)$ we have

$$\mathcal{S} \cup \mathcal{P} \supseteq \mathcal{D}_3.$$

From (4) we can deduce $\mathcal{S} \cap \mathcal{P} = \emptyset$. Thus,

$$\mathcal{S} \supseteq \mathcal{D}_3 \setminus \mathcal{P} \supseteq \mathcal{D}_3^0.$$

Since $\mathcal{D}_3 \subset \overline{\mathcal{E}_3(1)}$ we are done if we can cover $\overline{\mathcal{E}_3(1)}$ with $\mathcal{P} \cup \mathcal{S}$. By calculations we can show that

$$\mathcal{P} \cup \mathcal{S} \supseteq \overline{\mathcal{E}_3(1)}.$$

Cryptographically Secure Electronic Elections

In chapter four we detail all the protocol building blocks that we applied in our election schemes. In chapter five after describing requirements and participants of voting schemes two new secure election protocols are detailed. Both of them possess all basic requirements and can be implemented in practice.

Results of this chapter are based on [22] and [23].

Requirements we intend to fulfill in an electronic voting scheme are as follows: eligibility, privacy, unreusability, fairness, robustness, individual and universal verifiability, receipt-freeness, uncoercibility and protects against randomization, forced-abstention and simulation attacks.

A scheme is called *coercion-resistant* if it offers not only receipt-freeness, but also defense against randomization, forced-abstention and simulation attacks.

In the first part of the chapter we present **a coercion-resistant voting scheme based on blind signatures**. There are several election protocols using blind signatures that possess all basic requirements including verifiability, eligibility, unreusability, privacy etc., but not receipt-freeness ([16],[37]). Most of the receipt-free schemes in literature apply untappable channels or voting booths([38]), that are not practical. Our scheme satisfies besides eligibility, privacy, unreusability, fairness, robustness, individual and universal verifiability, coercion-resistance as well. The voting scheme based on blind signatures, requires only two authorities, practical and does not employ complex primitives like zero-knowledge proofs or threshold cryptosystems. It is offered to be employed in an environment, where authorities participating do not collude and the Voting Authority does not collaborate with adversaries.

Let denote P, Q large primes, where $Q|(P-1)$ and $g \in \mathbb{Z}_P^*$ of order Q. Let us define the candidate list as $C_1, C_2, \ldots, C_n$. The three functions applied in the scheme: *vote*, *ifeligible* and *verify* are as follows.

1. $vote(V_{ID}, SK_V, x, a, C_i) \rightarrowtail ballot$, where V_{ID} is the voter's identification number, SK_V is the voter's secret key, x, a are random parameters and C_i is the selected candidate. The form of the ballot is $(V_{ID}||r||y, V_{ID}||v)$, where

$$\begin{aligned} r &= E_{SK_V}(g) \\ y &\equiv g^{-x} \pmod{P} \\ v &\equiv y^a \cdot C_i \pmod{P} \end{aligned}$$

   and $||$ is the notation of concatenation.

2. $ifeligible(PK_V, r) \rightarrowtail \{0, 1\}$, where PK_V is the voter's public key, r is a received value. It returns 1 if $D_{PK_V}(r) = g$ and 0 if this congruence is not satisfied.

3. $verify(PK_V, z, s, y) \rightarrowtail \{0, 1\}$ calculates if $PK_V^z \equiv g^s \cdot y \pmod{P}$ congruence holds. It outputs 1 if it is correct and 0 otherwise. This function verifies if s sent by the voter is calculated well and by the same voter who previously *voted* with value y and public key PK_V, where element z is randomly generated by the Voting Authority.

It consists of three distinctive stages: *Authorizing*, *Voting* and *Tallying*. Participants besides voters are Registry that is manages the Authorizing stage and the Tallying stage, as well, and Voting Authority that is responsible for the Voting stage.

During the Authorizing stage the voter authenticates himself and receives his credentials(SK_V,V_{ID}) and the ElGamal public key of the Voting Authority(PK_A). Voting Authority gets the voter roll containing the corresponding ElGamal public keys(V_{ID}, PK_V) and all system parameters are generated(P,Q,g).

During the Voting stage voters create their ballots with function *vote*. Ballots contain the selected candidate and blind signature is applied to hide it from the Voting Authority (construction of value v). Voting Authority checks eligibility of the voters with function *ifeligible* and if they have already voted before. Voting Authority sends an encrypted random number(z) to the voter. Voters send encrypted values s and V_{ID}, where $s \equiv x + z \cdot SK_V \pmod{Q}$, then Voting Authority runs function *verify*. Voters receive their encrypted ballots signed by the Voting Authority($Sig(v, s)$), if a fraud is detected the voter makes a claim. At the end voters pass the corresponding decrypting keys of the encrypted ballots (a,s) to the Registry. Ballots and bulletin board information are passed through an anonymous channel.

During the Tallying stage the Voting Authority sends encrypted ballots (s,v) to the Registry. The ballots are being decrypted and the final results with the votes are listed on the bulletin board (s,C_i). Voters confirm that their ballots are on the bulletin board. If his ballot is not listed correctly, he makes a claim. During the voting process public and anonymous channels are employed and ElGamal encrypted messages are sent, hence it can be implemented in practice.

In the second part of the chapter we deal with **a receipt-free homomorphic election scheme**. Our protocol is based on homomorphic encryptions, it assumes existence of several authorities and it uses distributed ElGamal encryption [41]. This scheme is based on [13] that is not possessing the property of receipt-freeness or uncoercibility. There are two models based on [13] that are designed to be receipt-free in the literature: [32] and [20]. First one applies an honest verifier, the second one uses an untappable channel. Our scheme does not employ voting booths or untappable channels, it requires an anonymous return channel, hence it can be implemented in practice. We do not have an honest verifier, either. The only assumption is that among the Voting Authorities participating in distributed key generation and decryption there is at least one authority that is honest. The scheme satisfies eligibility, privacy, unreusability, fairness, robustness, individual and universal verifiability, receipt-freeness, uncoercibility and protects against randomization and forced-abstention attacks. The participants of the protocol are m voters, a Registry $\mathcal{R}$, an authority called Verifier Authority (*VA*) and s Voting Authorities.
Before describing our election scheme let us detail $ProofGenEG$ generator and $ProofVerEG$ verifier algorithms:

ProofGenEG
Input: signature: $s_m \in \mathbb{Z}_Q, R \in \mathbb{Z}_Q, \tilde{l} \in \mathbb{Z}_Q$
Output: $\overline{s_m} \in \mathbb{Z}_Q, \overline{R} \in \mathbb{Z}_P, \overline{T} \in \mathbb{Z}_Q$
1. The voter chooses random number: $\tilde{v} \in \mathbb{Z}_Q$
2. $R' \equiv (R \pmod P) \pmod Q$
3. $\overline{s_m} \equiv \frac{s_m}{\tilde{l}} \pmod Q$
4. $\overline{R} \equiv R^{\frac{\tilde{v}}{\tilde{l}}} \pmod P$
5. $\overline{T} \equiv \frac{R'}{\tilde{v}} \pmod Q$

ProofVerEG
Let denote EPK_{VA} Verifier Authority's ElGamal public key.
Input: $m \in \mathbb{Z}_P$, $\overline{s_m} \in \mathbb{Z}_Q, \overline{R} \in \mathbb{Z}_P, \overline{T} \in \mathbb{Z}_Q$
Output: true, false

1. $m' \equiv (m \pmod P) \pmod Q$
2. Verifies: $EPK_{VA}^{\overline{s_m}} \cdot \overline{R}^{\overline{T}} \equiv g^{m'} \pmod P$

During the Authorizing stage voters authenticate themselves in person and receive their credentials. All system parameters, sufficient private and public keys are generated. Let P and Q be large primes so that $Q|(P-1)$. G_Q denotes $\mathbb{Z}_P^*$'s unique multiplicative subgroup of order Q, and let g an arbitrary element such that $g \in G_Q$. Voting Authorities generate jointly the public (g, $h \equiv g^K \pmod P$) and private ($K \in \mathbb{Z}_Q$) keys using distributed ElGamal key generation method [41]. $\mathcal{R}$ randomly chooses $v_i \in \mathbb{Z}_Q^*$, $i = 1, \ldots, n$ elements $C_i \equiv g^{v_i} \pmod P$ where C_i represents candidate i from the voter roll and a one-way hash function $M()$ is chosen. All private and public keys are generated RSA keys of $\mathcal{R}$ (private: $RSK_{\mathcal{R}}, P_{\mathcal{R}}, Q_{\mathcal{R}}$, public: $RPK_{\mathcal{R}}, N_{\mathcal{R}}$) and *VA* (private: $RSK_{\mathcal{VA}}, P_{\mathcal{VA}}, Q_{\mathcal{VA}}$, public: $RPK_{\mathcal{VA}}, N_{\mathcal{VA}}$), ElGamal keys of *VA* (private: ESK_{VA}, public: (EPK_{VA}, P, g)). The voter gets his credential in a way that he generates his random reference number ($id_k^{\mathcal{R}}$), and $\mathcal{R}$ signs it blindly, hence $\mathcal{R}$ cannot connect the credential to the voter. During key-generation $\mathcal{R}$ does not learn anything about private keys either.

During the Voting stage voters create their ballots. *VA* checks eligibility of the voters and if they have already voted before by verifying signature of $\mathcal{R}$ on $id_k^{\mathcal{R}} \pmod{N_{\mathcal{R}}} \,||\, (M(id_k^{\mathcal{R}}))^{RSK_{\mathcal{R}}} \pmod{N_{\mathcal{R}}}$. Voter receives an identification value used only in vote validation phase, in order to follow if a voter has already run the zero-knowledge proof. Voter V_k initiates a blind signature algorithm in order to get his identification number authorized and possesses $id_k^{VA} \pmod{N_{VA}}||(M(id_k^{VA}))^{RSK_{VA}} \pmod{N_{VA}}$. Then V_k sends $id_k^{VA} \pmod{N_{VA}}||(M(id_k^{VA}))^{RSK_{VA}} \pmod{N_{VA}}$ through an anonymous return channel to *VA*. *VA* verifies the signature and if the corresponding voter has not been processed before, sends z_k back through the same channel, where $z_k \in \mathbb{Z}_Q$ random. Since id_k^{VA} signed blindly and anonymous return channel is used, *VA* cannot learn the sender. V_k chooses a candidate i and the corresponding $C_i^{(k)}$ from $\mathcal{BB}$. In order to create his ballot randomly chooses $\alpha_k, \beta_k, \gamma_k \in \mathbb{Z}_Q$ and computes $G_k \equiv g^{\alpha_k+\beta_k} \pmod P$, $H_k \equiv h^{\alpha_k+\beta_k} \pmod P$ and $Y_k \equiv g^{z_k \cdot \gamma_k} \pmod P$. Following V_k runs a non-interactive zero-knowledge proof to prove that he has constructed the ballot correctly, such that he has chosen the value $C_i^{(k)}$ from the voter roll listed on $\mathcal{BB}$. He chooses $r_j, d_j, w_k \in \mathbb{Z}_Q$ random numbers, where $1 \leq j \leq n$ and $j \neq i$, then calculates $(\mathsf{A}, \mathsf{B}) = (a_1, b_1), (a_2, b_2), \cdots, (a_n, b_n)$, where

$$a_i \equiv g^{w_k} \pmod P,$$

$$b_i \equiv h^{w_k} \pmod P,$$

for the elected candidate i and

$$\begin{aligned} a_j &\equiv g^{r_j} \cdot G_k^{d_j} \pmod{P}, \\ b_j &\equiv h^{r_j} \cdot \left(\frac{H_k \cdot C_i^{(k)}}{C_j^{(k)}} \right)^{d_j} \pmod{P} \end{aligned}$$

for all candidates $j \neq i$. Further, the voter calculates
$c_k = M(a_1||..||a_n||b_1||..||b_n||G_k||H_k \cdot C_i^{(k)}||g||h||id_k^{VA}||(M(id_k^{VA}))^{RSK_{VA}})$ challenge and $(\mathsf{D}, \mathsf{R}) = (d_1, r_1), (d_2, r_2), \ldots, (d_n, r_n)$,
where for candidate i

$$\begin{aligned} d_i &\equiv c_k - \sum_{j=1, i \neq j}^{n} d_j \pmod{Q} \\ r_i &\equiv w_k - (\alpha_k + \beta_k) \cdot d_i \pmod{Q}. \end{aligned}$$

V_k sends the following encrypted randomized ballot and parameters to *VA* through an anonymous return channel:

$$(\mathsf{A}, \mathsf{B})||G_k||H_k \cdot C_i^{(k)}||c_k||(\mathsf{D}, \mathsf{R})||id_k^{VA}||(M(id_k^{VA}))^{RSK_{VA}}||\tilde{r} \cdot Y_k,$$

where $\tilde{r} \in \mathbb{Z}_P$ is random. After receiving all necessary information *VA* checks whether the voter with id_k^{VA} has already run the zero-knowledge proof, whether id_k^{VA} is signed correctly and calculates the following congruences.

$$\begin{aligned} c_k &\equiv \sum_{j=1}^{n} d_j \pmod{Q}, \\ a_j &\equiv g^{r_j} \cdot G_k^{d_j} \pmod{P},\ j = 1, \ldots, n \\ b_j &\equiv h^{r_j} \cdot \left(\frac{H_k \cdot C_i^{(k)}}{C_j^{(k)}} \right)^{d_j} \pmod{P},\ j = 1, \ldots, n \end{aligned}$$

If the verification congruences hold, then *VA* signs all the randomized components applying *SigGenEG* that is a Meta-ElGamal signature scheme [21]. *VA* calculates and sends

$$\begin{aligned} SigGenEG(G_k) &= (s_{m_1}, R_1) \\ SigGenEG(H_k \cdot C_i^{(k)} \cdot Y_k \cdot \tilde{r}) &= (s_{m_2}, R_2) \\ SigGenEG(Y_k \cdot \tilde{r}) &= (s_{m_3}, R_3) \end{aligned}$$

back to the sender through the anonymous return channel. After the voter verifies the three signatures, gets authorization of the ballots being processed during the Tallying Stage.

$$\begin{aligned}\tilde{l_1} &\equiv (g^{\beta_k} \pmod P) \pmod Q\\ \tilde{l_2} &\equiv (h^{\beta_k}\cdot\tilde{r} \pmod P) \pmod Q\\ \tilde{l_3} &\equiv (\tilde{r} \pmod P) \pmod Q\end{aligned}$$

and computes

$$ProofGenEG(s_{m_1}, R_1, \tilde{l_1}) = (\overline{s_{m_1}}, \overline{R_1}, \overline{T_1})$$

$$ProofGenEG(s_{m_2}, R_2, \tilde{l_2}) = (\overline{s_{m_2}}, \overline{R_2}, \overline{T_2})$$

$$ProofGenEG(s_{m_3}, R_3, \tilde{l_3}) = (\overline{s_{m_3}}, \overline{R_3}, \overline{T_3}),$$

where *ProofGenEG* for generating a proof of his 'pure' ballots from the randomized ballot signatures sent by *VA*. Voters send $id_k^{\mathcal{R}}||g^{\alpha_k}||(\overline{s_{m_1}}, \overline{R_1}, \overline{T_1})||h^{\alpha_k}\cdot C_i^{(k)}\cdot Y_k||(\overline{s_{m_2}}, \overline{R_2}, \overline{T_2})$ to $\mathcal{BB}$ through a public channel and $Y_k||(\overline{s_{m_3}}, \overline{R_3}, \overline{T_3})$ to *VA* through anonymous channel. The form of the ballot is the ElGamal encryption of $C_i^{(k)}\cdot Y_k \equiv g^{v_i+z_k\cdot\gamma_k} \pmod P$, where $z_k \in \mathbb{Z}_Q$ is sent by *VA* through an anonymous channel, hence z_k is not known by the adversary. If the ballot appearing on $\mathcal{BB}$ is different or missing, then the voter makes a claim and he can cast his vote again.

During the Tallying stage the following computations are made: Verifier Authority runs *ProofVerEG* algorithm for each Y_k and calculates $Y \equiv \prod_{k=1}^{m} Y_k \pmod P$, where only valid randomized components are considered and sends Y to $\mathcal{BB}$. After verifying validity of encrypted ballots with *ProofVerEG*

$$\begin{aligned}\Gamma &\equiv \prod_{k=1}^{m} g^{\alpha_k} \pmod P\\ \Lambda &\equiv \prod_{k=1}^{m} h^{\alpha_k}\cdot C_i^{(k)}\cdot Y_k \pmod P\end{aligned}$$

appear on $\mathcal{BB}$, where only valid ballots are considered. After dividing Λ by Y we get the ElGamal encrypted voting result on $\mathcal{BB}$. Voting Authorities $A_1, A_2, \ldots, A_s$ together calculate the result $C_1^{t_1}\cdot C_2^{t_2}\cdots C_n^{t_n}$ with distributed ElGamal decryption method. Shanks baby step giant step or Pollard rho method might be applied for calculating t_i, $i = 1, \ldots, n$, which gives the election result for candidate i.

Calculation of $t_1, \ldots, t_n$ is considered as a computationally hard problem, it requires $O(m^{(n-1)/2})$ time to get the result.([32]) This scheme can be used for large scale election, if the authorities divide the total value of (Γ, Λ) into parts of reasonable size (e.g. election areas).

Összefoglaló

Ez a disszertáció két, többé-kevésbé független témakörön alapszik, az általánosított számrendszerek, illetve a biztonságos elektronikus választások témakörén. Az első részben kanonikus számrendszereket (CNS) vizsgálunk negyedfokú algebrai számtestekben, majd a háromdimenziós szimmetrikus shift radix rendszereket karakterizáljuk. A disszertáció második felében két biztonságos választási protokollt mutatunk be, az egyik vak aláírási technikán, a másik homomorf kriptorendszeren alapszik.

A kanonikus számrendszerek a racionális egészek algebrai egészekre vonatkozó helyi értékes ábrázolási mód természetes általánosításai (Grünwald [19]). Elsőként Knuth tanulmányozta [30], [31] a kanonikus számrendszerek egy fajtáját, ahol megmutatta, hogy a $b = -1 + \sqrt{-1}$ komplex szám egy a Gauss egészek véges reprezentációját megadó számrendszer bázisa. Az elmúlt évtizedekben széleskörűen általánosították és tanulmányozták ezt az észrevételt.

A CNS elmélete kapcsolódik a véges automaták (K. Scheicher [46], J. M. Thuswaldner [51]), illetve a fraktál csempézés (S. Akiyama és J. M. Thuswaldner [7]) területéhez. S. Akiyama és társai [2] a kanonikus számrendszerek általánosításával új kapcsolatokat nyitott meg más területekkel, ilyen például a Salem számok régóta fennálló problémája.

Egy dinamikus rendszer, a shift radix rendszer (SRS) fogalmát S. Akiyama és társai vezették be a [2] cikkben. Az SRS szoros kapcsolatban áll a kanonikus számrendszerekkel és a β-kifejtésekkel is, lásd a [15, 40, 44] munkákat. Valójában az egységesítése és az általánosítása ezen fogalmaknak. Az SRS-ről, a β-kifejtésekkel és a CNS-kel való kapcsolatáról további ismeretekhez juthatunk a [2], [3], [48] dolgozatokban. Mi a szimmetrikus shift radix rendszereket (SSRS), az SRS egy fontos változatát tanulmányozzuk, melyet a [6] cikkben vezettek be a szerzők.

A kriptográfiai protokollok, például a biztonságos szavazó rendszerek, ugyanolyan szorosan kapcsolódnak a számelmélethez, mint az általánosított számrendszerek. A kriptográfiai primitívek konstrukciójának biztonsága olyan számelméleti problémákon alapszik, melyek kiszámíthatósága nehéz.

Legismertebb problémák a diszkrét logaritmus kiszámítása, illetve az összetett egész számok faktorizálása. Az elektronikus választási sémák az alkalmazott kriptográfiai technikák alapján három fő kategóriába sorolhatók:
Mix-net modell. Chaum [11] vezette be a mix-net fogalmát. A mix-net több összekapcsolt szerverből áll, melyeket mix szervereknek nevezünk. Minden egyes szerver randomizálja, majd permutálja a bejövő üzeneteket, így az input és az output üzenetek nem feleltethetőek meg egymásnak. Több mix-net-en alapuló séma is megjelent az irodalomban (lásd [39], [45], [25] dolgozatokat).
Vak aláíráson alapuló modell. A vak aláírás fogalmával elsőnek Chaum [12] munkájában találkozhatunk. A regisztrációs fázisban a szavazó bizottság hitelesíti a szavazó cédulákat (általában a titkosított szavazatot) anélkül, hogy megtudná a cédula tartalmát. Ez a hitelesítés a vak aláírás technikájával valósítható meg. Ha később az aláírást nyilvánosságra hozzák, nem lehet azt az aláíró folyamattal, azaz a szavazóval, összekapcsolni. További vak aláíráson alapuló szavazó sémákat mutatnak be a [16], [22], [37], [38], [43] dolgozatok.
Homomorf titkosításon alapuló sémák. A homomorf titkosításon alapuló sémák s szervezetettel vezénylik le a Szavazó és Összeszámláló fázist. Ezek a rendszerek titokmegosztással szétosztják a dekódoló kulcsot, vagy a szavazatot magát. Az irodalomban több homomorf titkosításon alapuló séma is megjelent, mint például a [13], [32], [8], [14] és [20] cikkekben tárgyaltakat.

A *visszaigazolás-mentesség* fogalmát Benaloh és Tuinstra vezette be [9]. Ha egy protokoll visszaigazolás-mentes, akkor a szavazót nem lehet lefizetni, illetve megfenyegetni, elérve azt, hogy valamely jelöltre szavazzon. Leegyszerűsítve, ez a fogalom azt jelenti, hogy még akkor sem tudja a szavazó bebizonyítani a támadónak hogy melyik jelöltre szavazott, ha ő maga akarja. Általában ezekkel a tulajdonságokkal rendelkező sémák lehallgathatatlan, illetve szavazó fülke csatornák alkalmazásán alapulnak, vagy egy további, biztonságos hardver eszközt használnak.

Általánosított számrendszerek

A második fejezet témája a **kanonikus számrendszerek** (CNS) karakterizálása. A CNS bázisokat explicite ismerjük néhány másodfokú, harmadfokú és negyedfokú testben (lásd [26],[27],[17],[18],[51],[5],[29],[4],[42] munkákat). Fő eredményként több algebrai számtestben, a negyedfokú körosztási, a legegyszerűbb negyedfokú testekben és a negyedfokú számtestek rendjeinek két családjában, meghatároztuk a CNS bázisokat. Ebben a fejezetben szereplő, Horst Brunotte-val és Pethővel Attilával közös eredményeink a [10] cikkünkben találhatók meg.

Továbbiakban $\mathbb{Q}$ jelöli a racionális számok testét, $\mathbb{Z}$ az egész számok halmazát és $\mathbb{N}$ a nemnegatív egészek halmazát. Jelölje $\mu_\gamma \in \mathbb{Z}[X]$ a γ algebrai egész minimálpolinomját és $\mathcal{C}_\gamma$ a $\mathbb{Z}[\gamma]$ összes CNS bázisának halmazát.

1. Definíció *Jelölje* $P(X) = X^d + p_{d-1}X^{d-1} + \cdots + p_1X + p_0 \in \mathbb{Z}[X]$, $N = \{0, 1, \ldots, |p_0| - 1\}$ *és* $\mathcal{R} := \mathbb{Z}[X]/P(X)\mathbb{Z}[X]$. *A* $\mathbb{Z}[X]$ *-ből* $\mathcal{R}$*-be képező kanonikus epimorfizmus* X *-et vigye át* x*-be. Ha bármely nem-nulla* $A(x) \in \mathcal{R}$ *egyértelműen felírható* $A(x) = a_0 + a_1x + \cdots + a_lx^l$ *alakban, ahol* $a_0, \ldots, a_l \in N, a_l \neq 0$, *akkor* (P, N) *kanonikus számrendszer (CNS).* $P(X)$*-et CNS polinomnak,* N*-et számjegyek halmazának nevezzük.*

Jelölje $\mathcal{C}$ a CNS polinomok halmazát. Belátható, hogy α akkor és csak akkor CNS bázis $\mathbb{Z}[\alpha]$-ban, ha μ_α CNS polinom. Hogy egy adott polinom CNS-e vagy sem, az algoritmus segítségével könnyen eldönthető.

B. Kovács [28] egyik tétele alapján egy rendben akkor és csak akkor létezik CNS, ha létezik hatvány egész bázis. CNS bázisok meghatározására B. Kovács és A. Pethő [29] algoritmusának egy módosított változatát alkalmazzuk. Az algoritmus ismertetéséhez, szükségünk van a következő állításokra és definícióra.

1. Lemma *(B. Kovács – A. Pethő) Bármely nem-nulla* α *algebrai egész esetén a következő konstansok effektíve kiszámíthatóak:*

$$k_\alpha = \min\{k \in \mathbb{Z} \,|\, \mu_\alpha(X + n) \in \mathcal{K} \text{ bármely } n \in \mathbb{Z}, \text{ ahol } n \geq k\},$$

$$c_\alpha = \min\{k \in \mathbb{Z} \,|\, \mu_\alpha(X + k) \in \mathcal{C}\}.$$

2. Definíció *Az* α *algebrai egész* R *alap CNS bázisa, ha teljesül a következő két tulajdonság:*

(1) $\alpha - n$ R *CNS bázisa bármely* $n \in \mathbb{N}$ *esetén.*

(2) $\alpha + 1$ *nem CNS bázis* R*-ben.*

1. Tétel *Legyen* γ *egy algebrai egész. Akkor léteznek* $\mathcal{F}_0(\gamma), \mathcal{F}_1(\gamma) \subset \mathcal{C}_\gamma$ *véges, effektíve kiszámolható, diszjunkt halmazok, melyekre:*

(i) Bármely $\alpha \in \mathcal{C}_\gamma$ *esetén létezik olyan* $n \in \mathbb{N}$, *ahol* $\alpha + n \in \mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma)$.

(ii) $\mathcal{F}_1(\gamma)$ *elemei* $\mathbb{Z}[\gamma]$ *alap CNS bázisai.*

Az algoritmus az 1. tételbeli (i) és (ii) tulajdonságokkal rendelkező $\mathcal{F}_0(\gamma)$ és $\mathcal{F}_1(\gamma)$ halmazokat adja meg.

Az algoritmus a következő:

Input: A γ nem-nulla algebrai egész és $\mathcal{B}$ (véges) halmaz, amely a $\mathbb{Z}[\gamma]$ hatvány egész bázisai ekvivalencia osztályainak reprezentásaiból áll.
Output: Az $\mathcal{F}_0(\gamma)$ és $\mathcal{F}_1(\gamma)$ halmazok.
1. [Inicializálás] Legyen $\{\beta_1, \ldots, \beta_t\} = \mathcal{B} \cup (-\mathcal{B})$, $F_0 = F_1 = T = \emptyset$ és $i = 1$.
2. [Minimál polinom kiszámítása] Legyen $P = \mu_{\beta_i}$.
3. [Van eleme az $F_0 \cup F_1$ halmaznak?] Ha létezik $k \in \mathbb{Z}, \delta \in \{0, 1\}$, hogy $(P, k, \delta) \in T$, akkor tegye a $\beta_i - k$ értéket az F_δ halmazba és menjen a 11-es lépésre.
4. [Az alsó és felső határ meghatározása] Számítsa ki k_{β_i} és c_{β_i} értékeket.
5. [Elem beszúrása az F_1 halmazba] Ha $k_{\beta_i} - c_{\beta_i} \leq 1$, akkor szúrja be a $\beta_i - c_{\beta_i}$ értéket az F_1 halmazba, a $(P, c_{\beta_i}, 1)$-t a T-be és menjen a 11-es lépésre, egyébként menjen a 6-os lépésre az $l = c_{\beta_i} + 1, \ldots, k_{\beta_i} - 1$ értékkel, legyen $p_{k_{\beta_i}} = 1, k = c_{\beta_i}$ és lépjen a 8-as lépésre.
6. [CNS tulajdonság ellenőrzése] Ha $P(X + l) \in \mathcal{C}$, akkor legyen $p_l = 1$, egyébként $p_l = 0$.
7. [CNS bázis feltétel ellenőrzése] Ha $p_k = 0$, akkor lépjen a 9-es pontra.
8. [Elem $F_0 \cup F_1$ halmazba való beszúrása] Ha $p_{k+1} = \cdots = p_{k_{\beta_i}} = 1$, akkor szúrja be $\beta_i - k$ értéket az F_1 halmazba, $(P, k, 1)$-t T-be és lépjen a 11-es pontra, egyébként szúrja be $\beta_i - k$-t az F_0 halmazba és $(P, k, 0)$-t T-be.
9. [A k következő értéke] Legyen $k \leftarrow k + 1$.
10. [Befejeződött a CNS bázis ellenőrzése?] Ha $k \leq k_{\beta_i} - 1$, akkor menjen 7-re.
11. [Következő generátor] Legyen $i \leftarrow i + 1$.
12. [Vége?] Ha $i \leq t$, akkor menjen 2-re.
13. [Megáll] Az $\mathcal{F}_0(\gamma) = F_0$ és $\mathcal{F}_1(\gamma) = F_1$ halmazok listázása és az algoritmus befejeződése.

Térjünk át a 4-edfokú körosztási testekre.

2. Tétel *Legyen $\zeta_5, \zeta_8, \zeta_{12}$ ötödik, nyolcadik és tizenkettedik primitív egységgyök. Ekkor $\mathcal{F}_0(\mathbb{Q}(\zeta_i)) = \emptyset$, ahol $i \in \{5, 8, 12\}$, továbbá*
$\mathcal{F}_1(\mathbb{Q}(\zeta_5)) = \{-2 + \zeta_5, -3 - \zeta_5, -2 + \zeta_5 + \zeta_5^3, -3 - \zeta_5 - \zeta_5^3\}$,
$\mathcal{F}_1(\mathbb{Q}(\zeta_8)) = \{-3 \pm \zeta_8^k \mid k = 1, 3, 5, 7\}$,
$\mathcal{F}_1(\mathbb{Q}(\zeta_{12})) = \{-3 + \zeta_{12}, -3 - \zeta_{12}, -3 + \zeta_{12}^{-1}, -3 - \zeta_{12}^{-1}, -1 - \zeta_{12}^2 + \zeta_{12}^{-1}, -2 + \zeta_{12}^2 - \zeta_{12}^{-1}\}$.

Adott $t \in \mathbb{Z} \setminus \{0, \pm 3\}$ esetén jelölje $P_t(X)$ az $X^4 - tX^3 - 6X^2 + tX + 1$ polinomot. Legyen $\vartheta = \vartheta_t$ a $P_t(X)$ polinom egyik gyöke, ekkor a $K_t = K = \mathbb{Q}(\vartheta_t)$ számtestek végtelen parametrikus családját a *legegyszerűbb negyedfokú számtesteknek* nevezzük. P. Olajos [36] bebizonyította, hogy K_t akkor és

csak akkor rendelkezik hatvány egész bázissal, ha $t = 2$ és $t = 4$, továbbá ezen testek hatvány egész bázisainak az összes generátorát meghatározta. Használva ezt az eredményt kiszámítjuk az összes CNS bázist ezekben a testekben.

3. Tétel *$\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$, $\mathcal{F}_1(\mathbb{Q}(\vartheta_2)) = \mathcal{G}_2$ és $\mathcal{F}_1(\mathbb{Q}(\vartheta_4)) = \mathcal{G}_4$, ahol $\mathcal{G}_2$ egy 19, míg $\mathcal{G}_4$ egy 12 elemű az értekezésben expliciten megadott halmaz.*

K_t-beli $\mathbb{Z}[\alpha]$ polinomrend hatvány egész bázisait G. Lettl és A. Pethő [33] vizsgálta. Ezt alkalmazva bizonyítjuk be a következő tételt.

4. Tétel *Legyen $t \in \mathbb{N} \setminus \{0, 3\}$ és jelölje ϑ az $X^4 - tX^3 - 6X^2 + tX + 1$ polinom egyik gyökét. Ekkor $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$ és $\mathcal{F}_1(\mathbb{Q}(\vartheta)) = \mathcal{G} \cup \mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_4$, ahol*

$$\begin{aligned}
\mathcal{G} &= \begin{cases} \{-3-\vartheta, -t-2+\vartheta, -2-6\vartheta-t\vartheta^2+\vartheta^3, \\ -t-3+6\vartheta+t\vartheta^2-\vartheta^3\}, \ \textit{ha } t \geq 5, \\ \emptyset \ \textit{egyébként}, \end{cases} \\
\mathcal{G}_1 &= \begin{cases} \{-4+\vartheta, -4-\vartheta, -5+6\vartheta+\vartheta^2-\vartheta^3, \\ -3-6\vartheta-\vartheta^2+\vartheta^3, -23+3\vartheta^2-\vartheta^3, -1-3\vartheta^2+\vartheta^3, \\ -14+25\vartheta+2\vartheta^2-4\vartheta^3, -10-25\vartheta-2\vartheta^2+4\vartheta^3\}, \\ \textit{ha } t = 1, \\ \emptyset \ \textit{egyébként}, \end{cases} \\
\mathcal{G}_2 &= \begin{cases} \{-5+\vartheta, -3-\vartheta, -5+6\vartheta+2\vartheta^2-\vartheta^3, \\ -3-6\vartheta-2\vartheta^2+\vartheta^3\}, \ \textit{ha } t = 2, \\ \emptyset \ \textit{egyébként}, \end{cases} \\
\mathcal{G}_4 &= \begin{cases} \{-6+\vartheta, -3-\vartheta, 1+9\vartheta-22\vartheta^2+4\vartheta^3, \\ -78-9\vartheta+22\vartheta^2-4\vartheta^3, -7+6\vartheta+4\vartheta^2-\vartheta^3, \\ -3-6\vartheta-4\vartheta^2+\vartheta^3, -62+74\vartheta+30\vartheta^2-9\vartheta^3, \\ -15-74\vartheta-30\vartheta^2+9\vartheta^3\}, \ \textit{ha } t = 4, \\ \emptyset \ \textit{egyébként}. \end{cases}
\end{aligned}$$

Tekintsük a paraméterezett negyedfokú számtestek rendjeinek egy családját, ahol az összes hatvány egész bázis ismert. Legyen $t \in \mathbb{Z}$, $t \geq 0$, és $P(X) = X^4 - tX^3 - X^2 + tX + 1$. Jelölje α a $P(X)$ polinom egyik gyökét. A következőkben $\mathcal{O} = Z[\alpha]$, $\mathbb{Q}(\alpha)$-beli rendet vizsgáljuk. M. Mignotte, A. Pethő és R. Roth [35] munkája alapján a következő eredményt kapjuk.

5. Tétel *Legyen $t \geq 4$. Ekkor $\mathcal{F}_0(\mathbb{Q}(\alpha)) = \emptyset$ és $\mathcal{F}_1(\mathbb{Q}(\alpha)) = \mathcal{G}_4 \cup \mathcal{G}_t$, ahol*

$$\begin{aligned}
\mathcal{G}_4 &= \left\{209\alpha + 140\alpha^2 - 49\alpha^3 + 350, 209\alpha - 312\alpha^2 + 64\alpha^3 - 71\right\} \\
\mathcal{G}_t &= \big\{\alpha + t + 1, \alpha + t\alpha^2 - \alpha^3 + t + 2, t\alpha + (t-1)\alpha^2 - \alpha^3 + 8, \\
&\quad t\alpha - (t+1)\alpha^2 + \alpha^3 + 2, \alpha - \alpha^3 + 2, \\
&\quad \alpha - t(t^2+1)\alpha^2 + t^2\alpha^3 - t + 1\big\}.
\end{aligned}$$

A harmadik fejezet témája a **szimmetrikus shift radix rendszerek**. Akiyama and Scheicher foglalkozott a kétdimenziós SSRS [6] rendszerekkel, mi a háromdimenziós SSRS esetet vizsgáljuk. Ez a fejezet a Claus Scheicher, Paul Surer és Jörg M. Thuswaldnerrel közös cikk [24] eredményeit taglalja.

3. Definíció ([6]) *Legyen $d \geq 1$ egész, $\mathbf{r} \in \mathbb{R}^d$, és jelölje $\tau_{\mathbf{r}} : \mathbb{Z}^d \to \mathbb{Z}^d$, azt a leképezést, mely során az $\mathbf{a} = (a_1, \ldots, a_d)$ képe $\left(a_2, \ldots, a_d, -\left\lfloor \mathbf{ra} + \frac{1}{2} \right\rfloor\right)$. Ekkor $\tau_{\mathbf{r}}$-et szimmetrikus shift radix rendszernek (SSRS) hívjuk, ha* $\forall \mathbf{a} \in \mathbb{Z}^d \quad \exists n \in \mathbb{N} : \tau_{\mathbf{r}}^n(\mathbf{a}) = \mathbf{0}$.

Legyen

$$\mathcal{D}_d := \left\{ \mathbf{r} \in \mathbb{R}^d \,\middle|\, \forall \mathbf{a} \in \mathbb{Z}^d \, \exists n, l \in \mathbb{N} : \tau_{\mathbf{r}}^k(\mathbf{a}) = \tau_{\mathbf{r}}^{k+l}(\mathbf{a}) \; \forall k \geq n \right\} \text{ és}$$
$$\mathcal{D}_d^0 := \left\{ \mathbf{r} \in \mathbb{R}^d \,|\tau_{\mathbf{r}} \text{ SSRS} \right\}.$$

A [6] cikkben szereplő algoritmus alapján bebizonyítjuk, hogy $\mathcal{D}_3^0$ négy test és egy sokszög egyesítése.

A [6] cikkben megmutatták, hogy

$$\mathcal{E}_d(1) \subset \mathcal{D}_d \subset \overline{\mathcal{E}_d(1)}. \tag{5}$$

Egy adott $\mathbf{r} = (r_1, \ldots, r_d) \in \mathcal{D}_d$ esetén, az $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d \setminus \{0\}$ elem az L periódushoz tartozó $\tau_{\mathbf{r}}$ egy *nem-nulla periódikus pontja*, ha $\mathbf{a} = \tau_{\mathbf{r}}^L(\mathbf{a})$. $\mathcal{D}_d^0$ definíciójából következik, hogy egy ilyen periódikus pont létezésének szükséges és elégséges feltétele, hogy $\mathbf{r} \notin \mathcal{D}_d^0$. Tegyük fel, hogy az $\mathbf{a}$ által definiált periódus átfut a

$$\tau_{\mathbf{r}}^j(\mathbf{a}) = (a_{1+j}, \ldots, a_{d+j}) \quad (0 \leq j \leq L-1)$$

íven, ahol $a_{L+1} = a_1, ..., a_{L+d-1} = a_{d-1}$. Jelöljön

$$(a_1, \ldots, a_d); a_{d+1}, \ldots, a_L$$

egy ilyen periódust, és ezt $\tau_{\mathbf{r}}$ periódusának, vagy egyszerűen $\mathcal{D}_d$ *periódusának* nevezzük.

Legyen $\pi := (a_1, \ldots, a_d); a_{d+1}, \ldots, a_L$ egy nem-nulla periódikus pont. Keressük azon $\mathbf{r} \in \mathcal{D}_d$ pontok $P(\pi)$ halmazát, amelyeknél π a $\tau_{\mathbf{r}}$ egy periódusaként áll elő. A $\tau_{\mathbf{r}}$ definíciója alapján, az $\mathbf{r} \in P(\pi)$ elem kielégíti a következő kétoldali egyenlőtlenség rendszert:

$$-\frac{1}{2} \leq r_1 a_{1+i} + r_2 a_{2+i} + \cdots + r_d a_{d+i} + a_{d+1+i} < \frac{1}{2}, \tag{6}$$

ahol i 0-tól $L-1$-ig megy és $a_{L+1} = a_1, \ldots, a_{L+d} = a_d$. Az ilyen rendszer egy konvex testet határoz meg, mely esetleg elfajuló, sőt üres is lehet. Ezért

$P(\pi)$-t *kivágó testnek* nevezzük. Mivel az összes $\mathbf{r} \in P(\pi)$ pont rendelkezik a megfelelő $\tau_{\mathbf{r}}$ leképezés π periódusával a $P(\pi)$ halmaz és a $\mathcal{D}_d^0$ halmaz metszete üres. Így

$$\mathcal{D}_d^0 = \mathcal{D}_d \setminus \bigcup_{\pi \neq \mathbf{0}} P(\pi),$$

ahol az unió az összes nem-nulla π periódusra vonatkozik. Mivel a periódusok halmaza végtelen, ez a kifejezés nem alkalmas kalkulációkra. A következő tétel megmutatja, hogyan lehet lecsökkenteni az összes lehetséges periódusok halmazát véges halmazra, és megad egy hatékony algoritmust a $H \cap \mathcal{D}_d^0$ kiszámítására, ahol H egy zárt részhalmaza $\operatorname{int} \mathcal{D}_d = \mathcal{E}_d(1)$-nek. Legyen $\mathbf{e}_i$ az i-dik kanonikus egységvektor. Az $\mathbf{r} = (r_1, \ldots, r_d) \in \operatorname{int} \mathcal{D}_d$ esetén, jelölje $\mathcal{V}(\mathbf{r}) \subset \mathbb{Z}^d$ a legkisebb halmazt, mely a következő tulajdonságokkal rendelkezik:

1. $\pm\mathbf{e}_i \in \mathcal{V}(\mathbf{r}), i = 1, \ldots, d,$
2. $(a_1, \ldots, a_d) \in \mathcal{V}(\mathbf{r}) \Rightarrow (a_2, \ldots, a_{d+1}) \in \mathcal{V}(\mathbf{r})$ ahol a_{d+1} kielégíti a

$$-1 < r_1 a_1 + r_2 a_2 + \cdots + r_d a_d + a_{d+1} < 1.$$

$\mathcal{V}(\mathbf{r}) \subset \mathbb{Z}^d$ az $\mathbf{r}$ *tanúhalmazának* nevezzük. Ezen kívül $\mathcal{G}(\mathcal{V}(\mathbf{r})) = V \times E$ jelöljön egy gráfot, melynek csúcsainak halmaza $V = \mathcal{V}(\mathbf{r})$ és éleinek halmaza pedig $E \subset V \times V$ úgy, hogy

$$\forall \mathbf{a} \in V : (\mathbf{a}, \tau_{\mathbf{r}}(\mathbf{a})) \in E.$$

6. Tétel ([6]) *Legyen $\mathbf{r}_1, \ldots, \mathbf{r}_k \in \mathcal{D}_d$ és legyen $H := \square(\mathbf{r}_1, \ldots, \mathbf{r}_k)$ az $\mathbf{r}_1, \ldots, \mathbf{r}_k$ pontok konvex burka. Tegyük fel, hogy $H \subset \operatorname{int} \mathcal{D}_d$ és mérete megfelelően kicsi. Akkor létezik egy olyan algoritmus, mely megad egy véges, irányított, $G(H) = V \times E$ gráfot, ahol a csúcsok halmaza $V \subset \mathbb{Z}^d$ és az élek halmaza $E \subset V \times V$, melyekre teljesül*

1. *$\pm\mathbf{e}_i \in V$, bármely $i = 1, \ldots, d$,*
2. *$\mathcal{G}(\mathcal{V}(\mathbf{x}))$ részgráfja $G(H)$-nek, bármely $\mathbf{x} \in H$,*
3. *$H \cap \mathcal{D}_d^0 = H \setminus \bigcup_\pi P(\pi)$, ahol π végigfut a G gráf nem-nulla egyszerű körei által indukált periódusokon.*

Célunk a $\mathcal{D}_3^0$ karakterizálása. Már tudjuk, hogy

$$\mathcal{E}_3(1) \subset \mathcal{D}_3 \subset \overline{\mathcal{E}_3(1)},$$

továbbá a [47, 49] dolgozatok alapján

$$\mathcal{E}_3(1) = \{(x, y, z) \in \mathbb{R}^3 |\ |x| < 1, |y - xz| < 1 - x^2, |x + z| < |y + 1|\}.$$

adódik. Szükségünk van a $\overline{\mathcal{E}_3(1)}$ halmazra. Könnyen látható, hogy ha a szigorú egyenlőtlenségeket kicseréljük megengedőekre, még nem kapunk zárt halmazt. Meg kell adni még további egyenlőtlenségeket. Legyen

$$\begin{aligned}\mathcal{E}_3' := \big\{(x,y,z) \in \mathbb{R}^3 \big|\ & |x| \le 1 \wedge |y - xz| \le 1 - x^2 \\ & \wedge |x+z| \le |y+1| \wedge |y-1| \le 2 \wedge |z| \le 3\big\}\end{aligned} \tag{7}$$

és tekintsük az $\mathcal{E}_3'$ és az

$$A_c := \big\{(x,y,z) \in \mathbb{R}^3 \mid x - c = 0\big\}$$

sík metszetét egy adott c konstans esetén. A következő lemma megmutatja, hogy $\mathcal{E}_3'$ zárt.

2. Lemma *Bármely $|c| < 1$ esetén az $\mathcal{E}_3'$ és az A_c sík metszete egy $\triangle(A_c^{(1)}, A_c^{(2)}, A_c^{(3)})$ zárt háromszög, ahol $A_c^{(1)} = (c, -1, -c), A_c^{(2)} = (c, 1 - 2c, c - 2), A_c^{(3)} = (c, 2c + 1, c + 2)$.*

7. Tétel $\overline{\mathcal{E}_3(1)} = \mathcal{E}_3'$.

Az $\mathcal{E}_3'$ halmazt definiáló egyenlőtlenségek száma lecsökkenthető, a következőket kapjuk eredményül:

$$\overline{\mathcal{E}_3(1)} = \big\{(x,y,z) \big| |x+z| \le 1 + y \wedge y - xz \le 1 - x^2 \wedge |z| \le 3\big\}.$$

Ahhoz, hogy megadjuk $\mathcal{D}_3^0$ teljes karakterizációját, definiáljuk a következő halmazokat:

$$\begin{aligned}
S_1 := \{(x,y,z) \mid\ & 2x - 2z \ge 1 \wedge 2x + 2y + 2z > -1 \wedge 2x + 2y \le 1 \\
& \wedge 2x \le 1 \wedge 2x - 2y + 2z \le 1\}, \\
S_2 := \{(x,y,z) \mid\ & x - z \le -1 \wedge 2x - 2y + 2z \le 1 \wedge -2x + 2y \le 1 \\
& \wedge 2x > -1\}, \\
S_3 := \{(x,y,z) \mid\ & x - z > -1 \wedge 2x - 2y + 2z \le 1 \wedge -2x + 2y < 1 \\
& \wedge 2x > -1 \wedge 2x - 2z < -1 \wedge 2x + 2y + 2z > -1\}, \\
S_4 := \{(x,y,z) \mid\ & 2x - 2y + 2z \le 1 \wedge -2x + 2y \le 1 \\
& \wedge 2x - 2z = -1, \wedge 2x + 2y + 2z > -1\}, \\
S_5 := \{(x,y,z) \mid\ & -1 < 2x \le 1 \wedge -1 < 2x - 2z \le 1 \\
& \wedge 2x + 2y + 2z > -1 \wedge 2x - 2y + 2z \le 1 \\
& \wedge 2x + 4y - 2z < 3 \wedge 2y \le 1\}
\end{aligned}$$

és jelölje

$$\mathcal{S} := \bigcup_{i \in \{1,\dots,5\}} S_i.$$

az egyesítésüket. Megjegyezzük, hogy S_1, S_2, S_3, S_5 testek, míg S_4 sokszög. A fenti jelölésekkel adódik a következő

8. Tétel $\mathcal{D}_3^0 = \mathcal{S}$.

A bizonyítás váza a következő. Első lépésként a 6. Tétel alapján belátjuk, hogy

$$\mathcal{S} \subseteq \mathcal{D}_3^0. \tag{8}$$

Ahhoz, hogy a másik irányú tartalmazást belássuk, szükségünk van a nemnulla periódusok Π halmazára. Legyen $\mathcal{P} := \bigcup_{\pi\in\Pi} P(\pi)$, továbbá be kell látnunk, hogy

$$\mathcal{S} \cup \mathcal{P} \supseteq \mathcal{D}_3.$$

A (8) reláció alapján $\mathcal{S} \cap \mathcal{P} = \emptyset$. Ebből következik, hogy

$$\mathcal{S} \supseteq \mathcal{D}_3 \setminus \mathcal{P} \supseteq \mathcal{D}_3^0,$$

azaz $\mathcal{D}_3^0 \subseteq \mathcal{S}$. Mivel $\mathcal{D}_3 \subset \overline{\mathcal{E}_3(1)}$, készen vagyunk, ha le tudjuk fedni $\overline{\mathcal{E}_3(1)}$-t a $\mathcal{P} \cup \mathcal{S}$ halmazzal. Számításokkal ez könnyen megmutatható.

Biztonságos elektronikus választások

A negyedik fejezet a választási protokollokban alkalmazott kriptográfiai primitíveket mutatja be. Az ötödik fejezetben, miután felsoroltuk a választási sémákkal szembeni elvárásokat, illetve a résztvevőket, két új, biztonságos szavazó protokollt ismertetünk. Mindkét protokoll rendelkezik a szükséges alapvető elvárásokkal és a gyakorlatban is implementálható. Ennek a fejezetnek az eredményei megtalálhatóak a [22] és [23] cikkekben.

Az elektronikus szavazó sémák elvárásai a következőek: jogosultság, titkosság, egyszer-szavazhatóság, szabályosság, teljesség, individuális és univerzális ellenőrizhetőség, visszaigazolás-mentesség. Ha egy protokoll visszaigazolás-mentes, akkor a szavazó nem vesztegethető, illetve nem fenyegethető meg.

Egy protokoll *ellenálló*, ha visszaigazolás-mentes, és biztosított a véletlenérték támadás, a kényszerített-hiányzás és a szimulációs támadásokkal szemben.

A fejezet első felében egy **vak aláíráson alapuló, ellenálló szavazó sémát** ismertetünk. Több olyan vak aláírási technikát alkalmazó választási protokoll is ismert, mely rendelkezik az alapvető elvárásokkal, mint például az ellenőrizhetőség, jogosultság, egyszer-szavazhatóság, titkosság stb., de nem visszaigazolás-mentes (lásd pl. a [16] és [37] dolgozatokat). Az irodalomban a

legtöbb visszaigazolás-mentes séma lehallgathatatlan csatornát vagy szavazó fülke csatornát használ, ami nem gyakorlatias. A mi sémánk megfelel a jogosultság, titkosság, egyszer-szavazhatóság, szabályosság, teljesség, individuális és univerzális ellenőrizhetőség elvárásoknak, és ellenálló is. A vak aláírási technikán alapuló sémánk két szervezet részvételét tételezi fel, gyakorlatias és nem tartalmaz bonyolult primitíveket, mint például nulla-ismeretű bizonyításokat vagy osztott kriptorendszereket. Ajánlott olyan környezetben implementálni, ahol a résztvevő szervezetek nem fognak össze és a Szavazó Bizottság nem működik együtt a támadókkal.

Jelöljön P, Q két nagy prímet, ahol $Q|(P-1)$ és legyen $g \in \mathbb{Z}_P^*$, melynek rendje Q. A jelöltek listája legyen $C_1, C_2, \ldots, C_n$. Három függvényt alkalmazunk: *vote*, *ifeligible* és *verify*.

1. $vote(V_{ID}, SK_V, x, a, C_i) \rightarrowtail ballot$, ahol V_{ID} a szavazó azonosító száma, SK_V a szavazó titkos kucsa, x, a véletlen paraméterek és C_i a javasolt jelölt. A *ballot* formátuma: $(V_{ID}||r||y, V_{ID}||v)$, ahol

$$\begin{aligned} r &= E_{SK_V}(g) \\ y &\equiv g^{-x} \pmod{P} \\ v &\equiv y^a \cdot C_i \pmod{P} \end{aligned}$$

   és $||$ a konkatenáció jele.

2. $ifeligible(PK_V, r) \rightarrowtail \{0,1\}$, ahol PK_V a szavazó nyilvános kulcsa, r input érték. A függvény 1-et ad vissza, ha $D_{PK_V}(r) = g$ és 0-t, ha a kongruencia nem teljesül.

3. $verify(PK_V, z, s, y) \rightarrowtail \{0,1\}$ kiszámolja, hogy a $PK_V^z \equiv g^s \cdot y \pmod{P}$ kongruencia teljesül-e. Ha teljesül 1-et ad vissza, ha nem, akkor 0-t. Ez a függvény azt ellenőrzi, hogy s-et szabályosan számították-e ki, illetve, hogy ugyanaz a személy küldte-e az s értéket, aki megelőzően *szavazott* az y értékkel és a PK_V publikus kulccsal, a z a Szavazó Bizottság által generált véletlen szám.

A protokoll három jól elhatárolható fázisból áll: *Regisztáció*, *Szavazás* és *Összeszámlálás*. A szavazókon kívül résztvevők még a Hitelesítő Szervezet, mely a regisztrációt és az összeszámlálást vezényli, valamint a Szavazó Bizottság, mely a szavazó fázisért felelős.

A regisztráció során megtörténik a szavazó azonosítása, megkapja elektronikus azonosítóját (SK_V,V_{ID}), valamint a Szavazó Bizottság ElGamal nyilvános kulcsát (PK_A). A Szavazó Bizottság megkapja a szavazó listát, mely tartalmazza a szavazásra jogosultak azonosítóját és nyilvános

kulcsát (V_{ID}, PK_V), valamint megtörténik a szükséges rendszer-paraméterek meghatározása (P,Q,g).

A szavazó fázis során a szavazók elkészítik az elektronikus szavazócédulájukat (*ballot*) a *vote* függvény segítségével. A szavazat tartalmazza a javasolt jelölt azonosítóját, vak aláírási technikával a Szavazó Bizottság hitelesíti azt (v konstrukciója). A Szavazó Bizottság ellenőrzi a szavazó jogosultságát az *ifeligible* függvény segítségével és megnézi szavazott-e már. A Szavazó Bizottság elküld egy titkosított z véletlen számot a szavazónak. A szavazó visszaküldi az s és V_{ID} értékeket, ahol $s \equiv x + z \cdot SK_V \pmod{Q}$, majd a Szavazó Bizottság lefuttatja a *verify* függvényt. A szavazásra jogosultak megkapják a hitelesített $Sig(v, s)$ elektronikus szavazatukat a Szavazó Bizottságtól, ha nem érvényes a szavazat, akkor a szavazó reklamál. A szavazó fázis lezárása után a szavazók elküldik a megfelelő a,s dekódoló kulcsot a Hitelesítő Szervezetnek. A szavazatok, illetve a hirdető táblára küldött információk anonim csatornán továbbítódnak.

Az összeszámlálás során a Szavazó Bizottság a titkosított s,v szavazatokat elküldi a Hitelesítő Szervezetnek. A szavazatokat dekódolják és a végleges eredménnyel együtt nyilvánosságra hozzák a hirdető táblán (s,C_i). A szavazók ellenőrzik, hogy a szavazatuk a táblán van-e. Ha a szavazatuk nem szerepel, vagy hibásan szerepel, akkor reklamálnak. Az egész szavazó eljárás alatt nyilvános és anonim csatornát alkalmazunk, valamint ElGamallal titkosított üzenetet továbbítottunk, így a rendszer gyakorlatias.

A fejezet második felében egy **visszaigazolás-mentes homomorf választási sémát** mutatunk be. A protokollunk homomorf titkosításon alapszik, több szervezet közreműködésével osztott ElGamal kriptorendszert használ (lásd [41]). Ennek a sémának az alapja a [13] dolgozatban szereplő protokoll, ami nem visszaigazolás-mentes. Két visszaigazolás-mentes változatot is találunk az irodalomban, a [32] és a [20] cikkekben levő sémák. Az első egy teljesen megbízható ellenőrző szervezet részvételét tételezi fel, a másik lehallgathatatlan csatornát használ. A mi változatunk nem a szavazó fülke vagy lehallgathatatlan csatornát, hanem a gyakorlatias, anonim válasz csatornát alkalmazza. Nem tételezzük fel egyik szervezetről sem, hogy teljesen megbízható, az egyetlen feltételezés az, hogy a Szavazó Bizottságok között az osztott kulcsgenerálás és dekódolás során legalább egy megbízható. A séma megfelel az alapvető elvárásoknak: jogosultság, titkosság, egyszer-szavazhatóság, szabályosság, teljesség, individuális és univerzális ellenőrizhetőség, visszaigazolás-mentesség és ellenáll a véletlenérték és kényszerített-hiányzás támadásoknak. A protokoll résztvevői az m szavazón kívül, az $\mathcal{R}$ Hitelesítő Szervezet, egy speciális szervezet, az Ellenőrző Szervezet (*VA*) és s Szavazó Bizottság.

Mielőtt rátérnénk a séma részletezésére megadjuk a $ProofGenEG$ generátor és $ProofVerEG$ ellenőrző algoritmust:

ProofGenEG
Input: aláírás: $s_m \in \mathbb{Z}_Q, R \in \mathbb{Z}_Q, \tilde{l} \in \mathbb{Z}_Q$
Output: $\overline{s_m} \in \mathbb{Z}_Q, \overline{R} \in \mathbb{Z}_P, \overline{T} \in \mathbb{Z}_Q$
1. A szavazó választ egy véletlen számot: $\tilde{v} \in \mathbb{Z}_Q$
2. $R' \equiv (R \pmod P) \pmod Q$
3. $\overline{s_m} \equiv \frac{s_m}{\tilde{l}} \pmod Q$
4. $\overline{R} \equiv R^{\frac{\tilde{v}}{\tilde{l}}} \pmod P$
5. $\overline{T} \equiv \frac{R'}{\tilde{v}} \pmod Q$

ProofVerEG
Jelölje EPK_{VA} az Ellenőrző Szervezet ElGamal nyilvános kulcsát.
Input: $m \in \mathbb{Z}_P$, $\overline{s_m} \in \mathbb{Z}_Q, \overline{R} \in \mathbb{Z}_P, \overline{T} \in \mathbb{Z}_Q$
Output: igaz, hamis
1. $m' \equiv (m \pmod P) \pmod Q$
2. Ellenőrzés: $EPK_{VA}^{\overline{s_m}} \cdot \overline{R}^{\overline{T}} \equiv g^{m'} \pmod P$

A regisztrációs fázisban a szavazók személyesen igazolják személyazonosságukat és megkapják elektronikus azonosítójukat. A szükséges rendszerparaméterek, titkos és nyilvános kulcsok legenerálódnak. Legyen P és Q két nagy prím, ahol $Q|(P-1)$. G_Q jelölje $\mathbb{Z}_P^*$ multiplikatív részcsoportját, melynek rendje Q, és legyen $g \in G_Q$ egy tetszőleges elem. A Szavazó Bizottságok együttesen legenerálják a szükséges nyilvános (g, $h \equiv g^K \pmod P$) és titkos ($K \in \mathbb{Z}_Q$) kulcsokat osztott ElGamal kulcsgeneráló módszerrel [41]. $\mathcal{R}$ véletlenül választ $v_i \in \mathbb{Z}_Q^*$, $i = 1, \ldots, n$ elemeket, $C_i \equiv g^{v_i} \pmod P$, ahol C_i jelöli az i-edik jelöltet és egy $M()$ egyirányú hash függvényt. Az összes titkos és nyilvános kulcsot legenerálják: $\mathcal{R}$ RSA kulcsa (titkos: $RSK_{\mathcal{R}}, P_{\mathcal{R}}, Q_{\mathcal{R}}$, nyilvános: $RPK_{\mathcal{R}}, N_{\mathcal{R}}$) és *VA* RSA kulcsa (titkos: RSK_{VA}, P_{VA}, Q_{VA}, nyilvános: RPK_{VA}, N_{VA}), *VA* ElGamal kulcsa (titkos: ESK_{VA}, nyilvános: (EPK_{VA}, P, g)). A szavazó úgy kapja meg azonosítóit, hogy generál egy véletlen $id_k^{\mathcal{R}}$ referencia számot, és $\mathcal{R}$ vakon aláírja, így $\mathcal{R}$ nem tudja az azonosítót hozzárendelni magához a szavazóhoz. Természetesen a kulcsgenerálás során $\mathcal{R}$-nek nincs semmilyen információja a titkos kulcsokról sem.

A szavazó fázis során a szavazók elkészítik az elektronikus szavazatukat. *VA* ellenőrzi a szavazók jogosultságát, és hogy szavaztak-e már úgy, hogy ellenőrzik $\mathcal{R}$ aláírásának érvényességét, megvizsgálva az $id_k^{\mathcal{R}} \pmod{N_{\mathcal{R}}}$ és az $(M(id_k^{\mathcal{R}}))^{RSK_{\mathcal{R}}} \pmod{N_{\mathcal{R}}}$ értékeket. A szavazó kap egy azonosítót,

mely csak a szavazat-ellenőrző fázisban szükséges, abból a célból, hogy ellenőrizzük, hogy a nulla-ismeretű bizonyítást lefuttatta-e. A V_k szavazó vak aláírást kezdeményez, hogy az azonosítóit hitelesítsék: $id_k^{VA} \pmod{N_{VA}}||(M(id_k^{VA}))^{RSK_{VA}} \pmod{N_{VA}}$. Majd V_k elküldi az $id_k^{VA} \pmod{N_{VA}}$ és $(M(id_k^{VA}))^{RSK_{VA}} \pmod{N_{VA}}$ üzeneteket egy anonim-válasz csatornán *VA*-nak. *VA* ellenőzi az aláírást, és ha a szavazóval még nem találkozott korábban, visszaküldi a $z_k \in \mathbb{Z}_Q$ véletlen értéket ugyanazon a csatornán. Mivel az id_k^{VA}-t vakon írták alá és anonim-válasz csatornát használnak, *VA* nem tudja a szavazó személyét. V_k kiválasztja az i-ik jelöltet és a megfelelő $C_i^{(k)}$ értéket a $\mathcal{BB}$-ről. Ahhoz, hogy elkészítse az elektronikus szavazatát választ $\alpha_k, \beta_k, \gamma_k \in \mathbb{Z}_Q$ véletlen számokat és kiszámolja a $G_k \equiv g^{\alpha_k+\beta_k} \pmod{P}$, $H_k \equiv h^{\alpha_k+\beta_k} \pmod{P}$ és $Y_k \equiv g^{z_k \cdot \gamma_k} \pmod{P}$ értékeket. V_k lefuttat egy nem-interaktív nulla-ismeretű bizonyítást, hogy bebizonyítsa az elektronikus szavazat szabályosságát, azaz, hogy a $C_i^{(k)}$ érték tényleg a jelöltek listájából vett. A szavazó választ $r_j, d_j, w_k \in \mathbb{Z}_Q$ véletlen számokat, ahol $1 \leq j \leq n$ és $j \neq i$, majd kiszámolja az $(\mathsf{A}, \mathsf{B}) = (a_1, b_1), (a_2, b_2), \cdots, (a_n, b_n)$ párokat, ahol

$$a_i \equiv g^{w_k} \pmod{P},$$

$$b_i \equiv h^{w_k} \pmod{P},$$

teljesül a kiválasztott i-edik jelöltre és

$$\begin{aligned} a_j &\equiv g^{r_j} \cdot G_k^{d_j} \pmod{P}, \\ b_j &\equiv h^{r_j} \cdot \left(\frac{H_k \cdot C_i^{(k)}}{C_j^{(k)}} \right)^{d_j} \pmod{P} \end{aligned}$$

az összes többi j-edik jelöltre, $j \neq i$. Továbbá, a szavazó kiszámolja a $c_k = M(a_1||..||a_n||b_1||..||b_n||G_k||H_k \cdot C_i^{(k)}||g||h||id_k^{VA}||(M(id_k^{VA}))^{RSK_{VA}})$ kihívást és a $(\mathsf{D}, \mathsf{R}) = (d_1, r_1), (d_2, r_2), \ldots, (d_n, r_n)$ párokat
ahol az i-ik jelöltre

$$\begin{aligned} d_i &\equiv c_k - \sum_{j=1, i \neq j}^{n} d_j \pmod{Q} \\ r_i &\equiv w_k - (\alpha_k + \beta_k) \cdot d_i \pmod{Q} \end{aligned}$$

teljesül. V_k elküldi a következő titkosított randomizált szavazatot és paramétereket *VA*-nak anonim-válasz csatornát használva:

$$(\mathsf{A}, \mathsf{B})||G_k||H_k \cdot C_i^{(k)}||c_k||(\mathsf{D}, \mathsf{R})||id_k^{VA}||(M(id_k^{VA}))^{RSK_{VA}}||\tilde{r} \cdot Y_k,$$

ahol $\tilde{r} \in \mathbb{Z}_P$ véletlen szám. Miután megkapta az összes szükséges adatot, *VA* ellenőrzi, hogy a szavazó az id_k^{VA} azonosítóval lefuttatta-e már a nulla-ismeretű bizonyítást, hogy id_k^{VA} aláírása érvényes-e, és kiszámolja a következő kongruenciákat:

$$\begin{aligned} c_k &\equiv \sum_{j=1}^{n} d_j \pmod{Q}, \\ a_j &\equiv g^{r_j} \cdot G_k^{d_j} \pmod{P},\ j = 1, \ldots, n \\ b_j &\equiv h^{r_j} \cdot \left(\frac{H_k \cdot C_i^{(k)}}{C_j^{(k)}} \right)^{d_j} \pmod{P},\ j = 1, \ldots, n. \end{aligned}$$

Ha az ellenőrző kongruenciák teljesülnek, akkor *VA* aláírja az összes randomizált komponenst *SigGenEG* segítségével, ami egy Meta-ElGamal aláírási séma (lásd a [21] dolgozatot). *VA* kiszámolja és visszaküldi anonim-válasz csatornán a következő mennyiségeket a küldőnek:

$$\begin{aligned} SigGenEG(G_k) &= (s_{m_1}, R_1) \\ SigGenEG(H_k \cdot C_i^{(k)} \cdot Y_k \cdot \tilde{r}) &= (s_{m_2}, R_2) \\ SigGenEG(Y_k \cdot \tilde{r}) &= (s_{m_3}, R_3) \end{aligned}$$

Miután a szavazó ellenőrzi mindhárom aláírást, generálja a hitelesített szavazatokat:

$$\begin{aligned} \tilde{l_1} &\equiv (g^{\beta_k} \pmod{P}) \pmod{Q} \\ \tilde{l_2} &\equiv (h^{\beta_k} \cdot \tilde{r} \pmod{P}) \pmod{Q} \\ \tilde{l_3} &\equiv (\tilde{r} \pmod{P}) \pmod{Q} \end{aligned}$$

és kiszámolja

$$ProofGenEG(s_{m_1}, R_1, \tilde{l_1}) = (\overline{s_{m_1}}, \overline{R_1}, \overline{T_1})$$

$$ProofGenEG(s_{m_2}, R_2, \tilde{l_2}) = (\overline{s_{m_2}}, \overline{R_2}, \overline{T_2})$$

$$ProofGenEG(s_{m_3}, R_3, \tilde{l_3}) = (\overline{s_{m_3}}, \overline{R_3}, \overline{T_3}),$$

ahol *ProofGenEG* generál egy bizonyítékot, mely biztosítja a 'tényleges' szavazatok érvényességét. A szavazó elküldi nyilvános csatornán $\mathcal{BB}$-re az $id_k^{\mathcal{R}} || g^{\alpha_k} || (\overline{s_{m_1}}, \overline{R_1}, \overline{T_1}) || h^{\alpha_k} \cdot C_i^{(k)} \cdot Y_k || (\overline{s_{m_2}}, \overline{R_2}, \overline{T_2})$ üzenetet, és anonim csatornán az $Y_k || (\overline{s_{m_3}}, \overline{R_3}, \overline{T_3})$ értékeket továbbítja *VA*-nak. A szavazat az El-Gamallal kódolt $C_i^{(k)} \cdot Y_k \equiv g^{v_i + z_k \cdot \gamma_k} \pmod{P}$ érték, ahol a $\mathbb{Z}_Q$-beli z_k értéket

VA küldte anonim csatornán, így z_k a támadó számára ismeretlen. Ha a $\mathcal{BB}$-n levő szavazat különbözik, vagy hiányzik, akkor a szavazó reklamál és újra szavazhat.

Az összeszámlálási fázis során a következő számítások történnek: Az Ellenőrző Szervezet lefuttatja a *ProofVerEG* algoritmust minden egyes Y_k-ra és kiszámolja az $Y \equiv \prod_{k=1}^{m} Y_k \pmod{P}$ értéket, ahol csak az érvényes randomizált komponenseket veszi figyelembe, és elküldi Y-t a $\mathcal{BB}$-re. Miután ellenőrizte a titkosított szavazatok érvényességét a *ProofVerEG* algoritmussal, a

$$\begin{aligned} \Gamma &\equiv \prod_{k=1}^{m} g^{\alpha_k} \pmod{P} \\ \Lambda &\equiv \prod_{k=1}^{m} h^{\alpha_k} \cdot C_i^{(k)} \cdot Y_k \pmod{P} \end{aligned}$$

értékek megjelennek $\mathcal{BB}$-én, ahol csak az érvényes szavazatokat veszik figyelembe. Elosztva Λ-t Y-nal, a szavazás eredményének ElGamallal titkosított képe lesz $\mathcal{BB}$-n. Az $A_1, A_2, \ldots, A_s$ Szavazó Bizottságok osztott ElGamal dekódolással együttesen kiszámolják a $C_1^{t_1} \cdot C_2^{t_2} \cdots C_n^{t_n}$ mennyiséget. Shanks baby step giant step vagy Pollard rho algoritmus alkalmazható t_i, $i = 1, \ldots, n$ kiszámítására, mely megadja a szavazatok számát az i jelöltre vonatkozóan.

A $t_1, \ldots, t_n$ értékek kiszámítása nehéz problémának bizonyul, időbonyolultsága: $O(m^{(n-1)/2})$ (lásd a [32] dolgozatot). Ez a séma használható nagy létszámú választások esetén, ha a szervezetek a teljes Γ, Λ értéket felosztják részekre (p.l. választási kerületek).

Bibliography

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, J. M. Thuswaldner, *On a generalization of the radix representation – a survey*, in "High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams", Fields Institute Communications, **41** (2004), 19 – 27.

[2] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, J. M. Thuswaldner, *Generalized radix representations and dynamical systems I*, Acta Math. Hungar., **108** (2005), 207 – 238.

[3] S. Akiyama, H. Brunotte, A. Pethő, J. M. Thuswaldner, *Generalized radix representations and dynamical systems II*, Acta Arithmetica, **121** (2006), 21 – 61.

[4] S. Akiyama, H. Brunotte, A. Pethő, *Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert*, J. Math. Anal. and Appl., **281** (2003), 402 – 415.

[5] S. Akiyama, H. Rao, *New criteria for canonical number systems*, Acta Arith., **111** (2004), 5 – 25.

[6] S. Akiyama, K. Scheicher, *Symmetric shift radix systems and finite expansions*, Mathematica Pannonica, **18** (2007), 101 – 124.

[7] S. Akiyama, J. M. Thuswaldner, *On the topological structure of fractal tilings generated by quadratic number systems*, Comput. Math. Appl., **49** (2005), 1439 – 1485.

[8] O. Baudron, P. Fouque, D. Pointcheval, G. Poupard, J. Stern, *Practical Multi-Candidate Election System*, 20th ACM Symposium on Principles of Distributed Computing ACM, (2001), 274 – 283.

[9] J. Benaloh, D. Tuinstra, *Receipt-free secret-ballot elections*, Proceedings of the 26th ACM Symposium on the Theory of Computing, ACM, (1994), 544 – 553.

[10] H. Brunotte, A. Huszti, A. Pethő, *Bases of canonical number systems in quartic algebraic number fields*, Journal de Théorie des Nombres de Bordeaux, **18** (2006), 537 – 559.

[11] D. Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital pseudonyms*, Communications of the ACM, **24** (1981), 84 – 90.

[12] D. Chaum, *Blind Signatures for Untraceable Payments*, In Advances in Cryptology - CRYPTO '82 Plenum Press, (1983), 199 – 203.

[13] R. Cramer, R. Gennaro, B. Schoenmakers, *A secure and optimally efficient multi-authority election scheme*, Proceedings of EUROCRYPT '97, LNCS Springer-Verlag, **1233** (1997), 103 – 118.

[14] I. Damgard, M. Juric, *A Generalization, a Simplification and Some Applications of Pallier's Probabilistic Public-Key System*, Public Key Cryptography'01, LNCS 1992 Springer-Verlag, (2001), 119 – 136.

[15] Ch. Frougny, B. Solomyak, *Finite beta-expansions*, Ergod. Th. and Dynam. Sys., **12** (1992), 713 – 723.

[16] A. Fujioka, T. Okamoto, K. Ohta, *A practical secret voting scheme for large scale elections*, In Advances in Cryptology - ASIACRYPT '92, LNCS Springer-Verlag, **718** (1992), 244 – 251.

[17] W. J. Gilbert, *Radix representations of quadratic fields*, J. Math. Anal. Appl., **83** (1981), 264 – 274.

[18] E. H. Grossman, *Number bases in quadratic fields*, Studia Sci. Math. Hungar., **20** (1985), 55 – 58.

[19] V. Grünwald, *Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale)*, Giornale di matematiche di Battaglini, **23** (1885), 203 – 221.

[20] M. Hirt, K. Sako, *Efficient receipt-free voting based on homomorphic encryption*, Proceedings of EUROCRYPT 2000, LNCS Springer-Verlag, **1807** (2000), 539 – 556.

[21] P. Horster, H. Petersen, M. Michels, *Meta-ElGamal signature schemes*, Proc. of the 2nd Annual ACM Conference on Computer and Communications Security ACM Press, (1994), 96 – 107.

[22] A. Huszti, *A secure electronic voting scheme*, Periodica Polytechnica Electrical Engineering, **51/3-4** (2007), 1 – 6.

[23] A. Huszti, *A Homomorphic Encryption-Based Secure Electronic Voting Scheme*, submitted for publication.

[24] A. Huszti, K. Scheicher, P. Surer, J. M. Thuswaldner, *Three-dimensional symmetric shift radix systems*, Acta Arithmetica, **129** (2007), 147 – 166.

[25] A. Juels, D. Catalano, M. Jakobsson, *Coercion-Resistant Electronic Elections*, Proceedings of the 2005 ACM workshop on Privacy in the electronic society, (2005), 61 – 70.

[26] I. Kátai, B. Kovács, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged), **42** (1980), 99 – 107.

[27] I. Kátai, B. Kovács, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar., **37** (1981), 159 – 164.

[28] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar., **37** (1981), 405 – 407.

[29] B. Kovács, A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields,* Acta Sci. Math. (Szeged), **55** (1991), 287 – 299.

[30] D. E. Knuth, *An imaginary number system*, Comm. ACM, **3** (1960), 245 – 247.

[31] D. E. Knuth, *The Art of Computer Programming, Vol. 2 Seminumerical Algorithms*, Addison Wesley (1998), London, 3rd edition.

[32] B. Lee, K. Kim, *Receipt-free electronic voting through collaboration of voter and honest verifier*, Proceeding of JW-ISC2000, (2000), 101 – 108.

[33] G. Lettl, A. Pethő, *Complete solution of a family of quartic Thue equations*, Abh. Math. Sem. Univ. Hamburg, **65** (1995), 365 – 383.

[34] E. Magkos, M. Burmester, V. Chrissikopoulos, *Receipt-freeness in large-scale elections without untappable channels*, In B. Schmid et al., editor, First IFIP Conference on E-Commerce, E-Business, E-Government (I3E), (2001), 683 – 694.

[35] M. Mignotte, A. Pethő, R. Roth, *Complete solutions of quartic Thue and index form equations,* Math. Comp., **65** (1996), 341 – 354.

[36] P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experiment. Math., **14** (2005), 129 – 132.

[37] T. Okamoto, *An electronic voting scheme*, Proceedings of IFIP '96, Advanced IT Tools Chapman & Hall, (1996), 21 – 30.

[38] T. Okamoto, *Receipt-Free Electronic Voting Schemes for Large Scale Elections*, Proceedings of Workshop of Security Protocols '97, LNCS Springer-Verlag, **1163** (1996), 125 – 132.

[39] C. Park, K. Itoh, K. Kurosawa, *Efficient anonymous channel and all/nothing election scheme*, In Advances in Cryptology - EUROCRYPT '93, LNCS Springer-Verlag, (1993), 248 – 259.

[40] W. Parry, *On the β-expansions of real numbers*, Acta Math. Acad. Sci. Hungar., **11** (1960), 401 – 416.

[41] T. Pedersen, *Non-interactive and information-theoretic secure verifiable secret sharing*, Proceedings of the 11th CRYPTO Conference, LNCS Springer-Verlag, **576** (1991), 129 – 140.

[42] A. Pethő, *Connections between power integral bases and radix representations in algebraic number fields*, Proc. of the 2003 Nagoya Conf. "Yokoi-Chowla Conjecture and Related Problems", Furukawa Total Pr. Co., (2004), 115 – 125.

[43] I. Ray, I. Ray, N. Narasimhamurthi, *An anonymous electronic voting protocol for voting over the Internet*, Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS '01), (2001), 188 – 190.

[44] A. Rényi, *Representations for real numbers and their ergodic properties*, Acta Math. Acad. Sci. Hungar., **8** (1957), 477 – 493.

[45] K. Sako, J. Kilian, *Receipt-free mix-type voting schemes - a practical solution to the implementation of voting booth*, Proceedings of EUROCRYPT '95, LNCS Springer-Verlag, **921** (1995), 393 – 403.

[46] K. Scheicher, *Kanonische Ziffernsysteme und Automaten,* Grazer Math. Ber., **333** (1997), 1 – 17.

[47] I. Schur, *Über Potenzreihen, die im inneren des Einheitskreises beschränkt sind*, J. reine angew. Math., **148** (1918), 122 – 145.

[48] P. Surer, *New characterisation results for shift radix systems*, Math. Pannon., **18** (2007), 265 – 297.

[49] T. Takagi, Lectures in Algebra, (1965).

[50] R. Tarjan, *Depth-first search and linear graph algorithms*, SIAM J. Comput., **1** (1972), 146 – 160.

[51] J. M. Thuswaldner, *Elementary properties of canonical number systems in quadratic fields*, in: Applications of Fibonacci Numbers, G. E. Bergum et al. (eds.), Kluwer Academic Publishers, Dordrecht, **7** (1998), 405 – 414.

List of papers/ Publikációs lista

1. H. Brunotte, A. Huszti, A. Pethő, *Bases of canonical number systems in quartic algebraic number fields*, Journal de Théorie des Nombres de Bordeaux, **18** (2006), 537 – 559.

    - S. Akiyama, H. Brunotte, A. Pethő, Reducible cubic CNS polynomials, *Periodica Mathematica Hungarica*, **55** (2007), 177 – 183.

2. A. Huszti, K. Scheicher, P. Surer, J. M. Thuswaldner, *Three-dimensional symmetric shift radix systems*, Acta Arithmetica, **129** (2007), 147 – 166.

    - G. Barat, V. Berthé, P. Liardet, J. Thuswaldner, Dynamical directions in numeration, *Annales de l'institut Fourier*, **56** (2006), 1987 – 2092.

3. A. Huszti, *A Secure Electronic Voting Scheme*, Periodica Polytechnica Electrical Engineering, **51/3-4** (2007), 1 – 6.

4. J. Folláth, A. Huszti, A. Pethő, *DESignIn Asymmetric Authentication System*, Proceedings of ICAI'07 7th International Conference on Applied Informatics **1** (2007), 53 – 61.

5. A. Huszti, *A Homomorphic Encryption-Based Secure Electronic Voting Scheme*, submitted for publication.

List of talks/ Előadások

1. A Secure Electronic Exam System, *International Conference on Automata, Languages and Related Topics (ALRT),* Debrecen, Hungary, 2008.

2. Secure Electronic Elections, *Cryptography and Number Theory Seminar,* Niigata University, Niigata, Japan, 2008.

3. Secure Electronic Elections, *Cryptography and Number Theory Seminar,* Nihon University, Tokyo, Japan, 2008.

4. A Secure Electronic Exam System, *Central European Conference on Cryptography,* Graz, Austria, 2008.

5. A Secure Electronic Homomorphic Voting Scheme, *International Conference on Applied Informatics,* Eger, Hungary, 2007.

6. A Secure Electronic Voting Scheme Based on Blind Signatures, *Conference of PhD Students in Computer Science,* Szeged, Hungary, 2006.

7. A Secure Electronic Voting Scheme Based on Blind Signatures, *NyírCrypt Central European Conference on Cryptography,* Nyíregyháza, Hungary, 2006.

8. Canonical Number Systems in Quartic Number Fields, *Number Theory Seminar,* Montanuniversitet, Leoben, Austria, 2005.