INSTITUTE OF MATHEMATICS
of the
Polish Academy of Sciences

ul. Śniadeckich 8, P.O.B. 21, 00-956 Warszawa 10, Poland http://www.impan.pl

IM PAN Preprint 707 (2009)

Andrzej Schinzel
Stanisław Spież
Jerzy Urbanowicz

Admissible Tracks in Shamir's Scheme

Published as manuscript

Received 09 September 2009

Admissible Tracks in Shamir's Scheme

Andrzej Schinzel* Stanisław Spież† Jerzy Urbanowicz‡

Abstract

In the paper we apply techniques of [8] to the classical Shamir secret sharing scheme with threshold k. We call a tuple over a finite field $\mathbb{F}_q$, determining the scheme, a k-admissible track if the secret in the scheme can be placed as an arbitrary coefficient of its generic polynomial. We estimate the number of k-admissible tracks and prove their existence and extendability for sufficiently large q. We give some algorithms for constructing and extending such tracks making use of elementary symmetric polynomials.

Key words. Secret sharing, key mangaement, threshold cryptography, elementary symmetric polynomials, equations in many variables over finite fields.

1 Introduction

1.1 Tracks in Shamir's scheme

In the paper we indicate how the techniques of [8] may be used to Shamir's threshold scheme. Idea of secret sharing is due to Shamir [7] and Blakley [2]. As to other related papers see [1], [4] and [3]. Secret sharing boils down to methods for distributing a secret amongst n shareholders equipped with shares of the secret.

In a threshold scheme an admin does not disclose a secret data D to participants but only distributes n shadow shares $D_0, \ldots, D_{n-1}$ amongst them in such a way that any group of k or more players can collectively efficiently reconstruct the secret but no coalition of less than k players can get any information on D at all.

We follow the standard terminology and notation of [5] and [8]. Throughout the paper n denotes the number of participants and k (≥ 2) denotes the

*Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland; schinzel@impan.gov.pl

†Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland; spiez@impan.gov.pl

‡Institute of Computer Science, Polish Academy of Sciences, and Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland; J.Urbanowicz@ipipan.waw.pl Corresponding author

threshold in the scheme. In the sequel let $\mathbb{F}_q$ be a finite field (q is a prime power). We use the row notation for vectors and (likewise in [8]) adhere to the convention that the numbering of rows and columns in the matrices starts with zero.

Throughout the paper, given $r \in \mathbb{N}$, we write $\mathbf{e}_r = (0, \dots, r-1)$. Moreover, given a subsequence $\rho = (\rho_0, \dots, \rho_{s-1})$ of $\mathbf{e}_r$ with $s \le r$ and an s-th tuple $\mathbf{u} = (u_0, \dots, u_{r-1})$ we denote $\mathbf{u}(\rho) = (u_{\rho_0}, \dots, u_{\rho_{s-1}}) \in \mathbb{F}_q^s$. Furthermore, given $0 \le i \le r-1$, we denote by $\widehat{\mathbf{u}}_i$ the sequence obtained from $\mathbf{u}$ by deleting the term u_i.

Definition 1. *Given $1 \le s \le n$ we call $\mathbf{t} = (t_0, \dots, t_{s-1}) \in \mathbb{F}_q^s$ the track of length s over $\mathbb{F}_q$, if and only if its coordinates t_i are pairwise different elements of $\mathbb{F}_q$. If $s = n$ we simply call $\mathbf{t}$ the track.*

Here a different ordering of elements $\{t_0, \dots, t_{n-1}\}$ is regarded as a distinct track. Two tracks are said to be disjoint, if the sets of their elements are disjoint. Concatenation of two disjoint tracks of lengths n and r respectively gives a track of length $n + r$. Sometimes it is convenient to identify tracks with the same elements. Then the set of the tracks breaks up into disjoint classes of tracks.

Let $\mathbf{x} = (x_0, \dots, x_{s-1})$ be a sequence of indeterminates. Given $s \ge 2$ let $V(\mathbf{x}) = \prod_{0 \le i < j \le s-1}(x_j - x_i) \in \mathbb{F}_q[\mathbf{x}]$ be the classical Vandermonde determinant (which is a homogeneous polynomial of total degree $\binom{s}{2}$). If $s = 1$, by convention, we have $V(\mathbf{x}) = 1$.

Fact. *Let $\mathbf{t} = (t_0, \dots, t_{s-1}) \in \mathbb{F}_q^s$. Then $\mathbf{t}$ is a track, if and only if $V(\mathbf{t}) \ne 0$.*

In the original Shamir's scheme an admin of the system chooses a (pseudo) random sequence of coefficients $a_1, \dots, a_{k-1} \in \mathbb{F}_q$ which (with $a_0 = D$) can be identified with the polynomial $q(t) = a_0 + a_1 t + \dots + a_{k-1} t^{k-1}$. The scheme is determined by the polynomial and a track $\mathbf{t}$ of length $n \ge k$, or equivalently, by the polynomial and the matrix $\mathbf{A}_{poly}(\mathbf{t}) = (t_i^j)_{0 \le i \le n-1,\, 0 \le j \le k-1}$ over $\mathbb{F}_q$ defined for $\mathbf{t}$.

The rows of the matrix $\mathbf{r}_0, \dots, \mathbf{r}_{n-1}$ are of the form $\mathbf{r}_i = (t_i^0, \dots, t_i^{k-1})$, $0 \le i \le n-1$. The matrix $\mathbf{A}_{poly}(\mathbf{t}) = (\mathbf{r}_0, \dots, \mathbf{r}_{n-1})^T$ is uniquely determined by the standard polynomial basis $\mathcal{B}_{poly}$ and the track $\mathbf{t}$.

For a subsequence ρ of length k of $\mathbf{e}_n$ write $\mathbf{A}_{poly}(\mathbf{t}(\rho)) = (t_{\rho(i)}^j)_{0 \le i,j \le k-1}$. Then the secret sharing boils down to some computations related to two matrix equations

$$\mathbf{A}_{poly}(\mathbf{t})\mathbf{a}^T = \mathbf{y}^T, \;\; \mathbf{A}_{poly}(\mathbf{t}(\rho))\mathbf{a}^T = (\mathbf{y}(\rho))^T$$

with $\mathbf{a} = (a_0, \dots, a_{k-1})$ and $\mathbf{y} = (y_0, \dots, y_{n-1})$.

The admin distributes as the shares n points $D_i = (t_i, y_i)$, $0 \leq i \leq n-1$ of the graph of polynomial $q(t)$ with non-zero pairwise different $t_0, \ldots, t_{n-1} \in \mathbb{F}_q$. The shares in Shamir's secret sharing scheme can be also identified with the pairs $D_i = (\mathbf{r}_i, y_i)$, where $y_i = \mathbf{r}_i \cdot \mathbf{a}$, $0 \leq i \leq n-1$. In the original Shamir's scheme we have $q = p$ a prime, $n < p$, and t_i are natural numbers satisfying $0 < t_0 < \ldots < t_{n-1} < p$.

Definition 2. *Let $1 \leq k-1 \leq n$ and fix $0 \leq i \leq k-1$. The track $\mathbf{t} \in \mathbb{F}_q^n$ is said to be a (k,i)-admissible track, if and only if the matrix $\mathbf{A}_{poly}(\mathbf{t})$ is a secret sharing matrix at level i.*

Definition 3. *Let $1 \leq k-1 \leq n$. We call the track $\mathbf{t} \in \mathbb{F}_q^n$ a k-admissible track, if $\mathbf{t}$ is (k,i)-admissible for every $0 \leq i \leq k-1$, or equivalently, if the matrix $\mathbf{A}_{poly}(\mathbf{t})$ is an all-level secret sharing matrix.*

Following Theorem 2 [8], the matrix $\mathbf{A}_{poly}(\mathbf{t})$ is a secret sharing matrix at level i, if and only if all $k \times k$ submatrices of the matrix $\mathbf{A}_{poly}(\mathbf{t})$, and all $(k-1) \times (k-1)$ submatrices of the matrix obtained from $\mathbf{A}_{poly}(\mathbf{t})$ by removing its i-th column are non-singular. In Definitions 2 and 3 we extend the concept of secret sharing matrices to $n = k-1$ too. Then the former condition is empty. If $n \geq k$, this condition is satisfied, if and only if all coordinates t_i of $\mathbf{t}$ are pairwise different. The latter condition is satisfied, if condition (2) below holds.

In the sequel, for simplicity, we also consider the tracks $\mathbf{t} \in \mathbb{F}_q^{k-1}$ (recall that in Shamir's scheme $k \leq n$) satisfying (2), resp. (3), calling them (k,i)-, resp. k-admissible tracks.

For a (k,i)-, resp. k-admissible track all tracks consisting of the same elements are also (k,i)-, resp. k-admissible tracks.

If $\mathbf{t} \in \mathbb{F}_q^n$ is (k,i)-, resp. k-admissible, then the matrix $\mathbf{A}_{poly}(\mathbf{t})$ allows to place the secret D as the i-th, resp. an arbitrary coefficient of a generic polynomial $q(t) = a_0 + a_1 t + \ldots + a_{k-1} t^{k-1}$ in Shamir's scheme.

Let $0 \leq r \leq s$ and let $\mathbf{x} = (x_0, \ldots, x_{s-1})$ be an s-th tuple of indeterminates. In the sequel, we denote by $\tau_r(\mathbf{x})$ the elementary symmetric polynomial of degree r; i.e. the sum of all distinct products of r distinct variables out of $x_0, \ldots, x_{s-1}$. By convention we have $\tau_0(\mathbf{x}) = 1$, and $\tau_r(\mathbf{x}) = 0$ if $r < 0$ or $r > s$. The elementary symmetric polynomials can be also defined inductively by

$$\tau_r(\mathbf{x}) = \tau_r(x_0, \ldots, x_{s-2}) + x_{s-1}\tau_{r-1}(x_0, \ldots, x_{s-2})\,. \tag{1}$$

Let $0 \leq j \leq k-1 \leq n$. In the sequel, we denote by $R_n(k)$ the set of all subsequences ρ of length $k-1$ of the sequence $\mathbf{e}_n$. Let $P_{k,j}, P_k \in \mathbb{F}_q[\mathbf{x}]$ be

symmetric homogeneous polynomials defined by

$$P_{k,j}(\mathbf{x}) = \prod_{\rho \in R_n(k)} \tau_j(\mathbf{x}(\rho))\,, \quad P_k(\mathbf{x}) = \prod_{j=1}^{k-1} \prod_{\rho \in R_n(k)} \tau_j(\mathbf{x}(\rho))\,.$$

In [8] (cf. [3]) it is shown that:

Theorem 1. (See Theorem 2 [8].) *Let* $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) \in \mathbb{F}_q^n$ *be a track and fix* $0 \le i \le k-1$. *Then the secret in Shamir's scheme can be placed as* $D = a_i$ (*i.e.,* $\mathbf{t}$ *is a* (k,i)*-admissible track*), *if and only if*

$$P_{k,k-1-i}(\mathbf{x}) \neq 0\,.$$

Corollary. *A tuple* $\mathbf{t} \in \mathbb{F}_q^n$ *is a* (k,i)*-admissible track, if and only if*

$$V(\mathbf{t}) \neq 0 \text{ and } P_{k,k-1-i}(\mathbf{t}) \neq 0. \tag{2}$$

Theorem 2. (See [8].) *Let* $\mathbf{t} \in \mathbb{F}_q^n$ *be a track. Then the secret in Shamir's scheme can be placed as an arbitrary coefficient of its generic polynomial* (*i.e.,* $\mathbf{t}$ *is a* k*-admissible track*), *if and only if*

$$P_k(\mathbf{x}) \neq 0\,.$$

Corollary. *A tuple* $\mathbf{t} \in \mathbb{F}_q^n$ *is a* k*-admissible track, if and only if*

$$V(\mathbf{t}) \neq 0 \text{ and } P_k(\mathbf{t}) \neq 0\,. \tag{3}$$

For k-admissible tracks $\mathbf{t} \in \mathbb{F}_q^n$ Shamir's scheme is a multi-secret sharing scheme. Then the matrix $\mathbf{A}_{poly}(\mathbf{t})$ allows the admin to change the secret not changing the shares of users and construct a secret sharing scheme in which the shareholders can use the same shares to recover more than one secret.

1.2 Generalizations

Let $\mathbf{c} = (c_0, \ldots, c_{k-1})$ be an increasing sequence of non-negative integers. In a natural way we can extend the concept of the (k,i)- and k-admissible tracks to Lai-Ding's secret sharing scheme, with threshold k and n shareholders, determined by a generic polynomial $q(t) = a_0 t^{c_0} + \ldots + a_{k-1} t^{c_{k-1}}$ and a tuple $\mathbf{t} \in \mathbb{F}_q^n$. In this case we consider the matrix $\mathbf{A}_{\mathbf{c}}(\mathbf{t}) = (t_i^{c_j})_{0 \le i \le n-1,\, 0 \le j \le k-1}$ defined for the tuple $\mathbf{t}$. For a fuller treatment of this case we refer the reader to [3] and [8].

2 Existence and extendability of admissible tracks

2.1 The number of admissible tracks

In this section we shall be concerned with equations in many variables over finite fields. For basic definitions, notation and terminology we refer the reader to [6]. In the sequel we make use of the following theorem:

Theorem 3. (See Lemma 3.3 [6].) *Suppose $s \geq 2$ and let $\mathbf{x} = (x_0, \ldots, x_{s-1})$ be a sequence of indeterminates. Let $F_1(\mathbf{x})$ and $F_2(\mathbf{x})$ be polynomials over $\mathbb{F}_q$ of total degrees d_1 and d_2, respectively, without a common factor of positive degree. Then the number of their common zeros in $\mathbb{F}_q^s$ is at most $q^{s-2}d_1d_2\min\{d_1, d_2\}$.*

Theorems 1, resp. 2 characterize (k, i)-, resp. k-admissible tracks. A question is whether such tracks exist. This question boils down to the question on existence of tracks satisfying (2), resp. (3). In the paper we prove that such tracks exist for sufficiently large q.

By [3] and [8], every track $\mathbf{t} \in \mathbb{F}_q^n$ is $(k, k-1)$-admissible for any $q > n$, and if its coordinates are $\neq 0$ it is also $(k, 0)$-admissible. It is easy to see that not all tracks are $(k, k-2)$-admissible. Indeed, a track $\mathbf{t} \in \mathbb{F}_q^n$ is $(k, k-2)$-admissible, if and only if $t_{\rho_0} + \ldots + t_{\rho_{k-2}} \neq 0$ for every subsequence $\rho = (\rho_0, \ldots, \rho_{k-2})$ of the sequence $\mathbf{e}_n$.

In Theorem 4, resp. 5 below we estimate the number of (k, i)-, resp. k-admissible tracks.

Theorem 4. *Let $n, k \in \mathbb{N}$ $(n \geq k-1 \geq 1)$. Fix $0 < i < k-1$. Then the number of (k, i)-admissible tracks of length n over $\mathbb{F}_q$ is*

$$q^n - \left(\binom{n}{2} + \binom{n}{k-1}\right)q^{n-1} + O(q^{n-2}),$$

where the constant in the O-symbol depends on n, k and i. For $i = 0$ the number is

$$(q-1)\ldots(q-n) = q^n - \binom{n+1}{2}q^{n-1} + O(q^{n-2}).$$

For $i = k-1$ the number is

$$q(q-1)\ldots(q-n+1) = q^n - \binom{n}{2}q^{n-1} + O(q^{n-2}).$$

Proof. Our proof starts with the following lemma:

Lemma 1. *Let* $\mathbf{x} = (x_0, \dots, x_{s-1})$ *be a sequence of indeterminates. For every* $0 < j < s$ *the number of solutions of the equation*

$$\tau_j(\mathbf{x}) = 0 \tag{4}$$

in $\mathbb{F}_q^s$ *is at most* $q^{s-1}+j(j-1)^2q^{s-2}$ *and at least* $q^{s-1}-q^{s-2}-(j-1)(j-2)^2q^{s-3}$.

Proof. By (1) we have

$$\tau_j(\mathbf{x}) = x_0\tau_{j-1}(x_1, \dots, x_{s-1}) + \tau_j(x_1, \dots, x_{s-1})\,.$$

The set of solutions of equation (4) falls naturally into two disjoint classes: solutions for which $\tau_{j-1}(x_1, \dots, x_{s-1}) \neq 0$ and others.

In solutions belonging to the first class, x_0 is uniquely determined by $x_1, \dots, x_{s-1}$ and so the number of solutions of the class is at most q^{s-1}.

For solutions belonging to the second class we have

$$\tau_{j-1}(x_1, \dots, x_{s-1}) = \tau_j(x_1, \dots, x_{s-1}) = 0\,. \tag{5}$$

Since the polynomials τ_{j-1} and τ_j have no common factor, by Theorem 3, the number of solutions of (5) is at most $q^{s-3}j(j-1)^2$. Since in solutions of the second class, x_0 ranges over all elements of $\mathbb{F}_q$, the number of solutions in the second class is at most $q^{s-2}j(j-1)^2$, which completes the proof of the first part of the lemma.

By virtue of (5), the number of solutions of (4) is at least q^{s-1} minus the number of solutions of $\tau_{j-1}(x_1, \dots, x_{s-1}) = 0$. By the already proved part of the lemma the latter number does not exceed $q^{s-2} + (j-1)(j-2)^2q^{s-3}$, which gives the desired lower bound. □

Proof of Theorem 4*:* Throughout the proof

- N_j denotes the number of solutions in $\mathbb{F}_q^n$ of the equation

$$V(\mathbf{x})P_{k,j}(\mathbf{x}) = 0 \quad (j < k-1), \tag{6}$$

- N stands for the number of solutions in $\mathbb{F}_q^n$ of the equation $V(\mathbf{x}) = 0$,
- $N_j(\rho)$ is the number of solutions in $\mathbb{F}_q^n$ of the the equation $\tau_j(\mathbf{x}(\rho)) = 0$,
- $N_j^*(\rho)$ denotes the number of solutions in $\mathbb{F}_q^n$ of the system $V(\mathbf{x}) = 0$, $\tau_j(\mathbf{x}(\rho)) = 0$,
- $N_j(\rho, \sigma)$ is the number of solutions in $\mathbb{F}_q^n$ of the system $\tau_j(\mathbf{x}(\rho)) = 0$, $\tau_j(\mathbf{x}(\sigma)) = 0$.

We have

$$N+\sum_{\rho\in R_n(k)} N_j(\rho) \geq N_j \geq N+\sum_{\rho\in R_n(k)} N_j(\rho)-\sum_{\rho\in R_n(k)} N_j^*(\rho)-\frac{1}{2}\sum_{\substack{\rho,\sigma\in R_n(k)\\ \rho\neq\sigma}} N_j(\rho,\sigma)\,. \tag{7}$$

Now $N = q^n - q(q-1)\dots(q-n+1) = \binom{n}{2}q^{n-1} + O(q^{n-2})$ and by Lemma 1

$$\sum_{\rho\in R_n(k)} N_j(\rho) = \operatorname{card}(R_n(k))q^{n-1} + O(q^{n-2}) = \binom{n}{k-1}q^{n-1} + O(q^{n-2})\,.$$

On the other hand, by Theorem 3, for each ρ and $\sigma \neq \rho$

$$N_j^*(\rho) = O(q^{n-2}), \quad N_j(\rho,\sigma) = O(q^{n-2})\,.$$

Hence (7) gives the theorem for $i = k-1-j > 0$. For $i = 0$, $j = k-1$ the negation of (6) reduces to

$$V(\mathbf{x})\prod_{\nu=0}^{n-1} x_\nu \neq 0\,.$$

Each x_ν can be taken from the same set of $q-1$ elements and all are distinct, hence this number is $(q-1)\dots(q-n)$. □

Remark. The above argument gives also that the number of solutions in $\mathbb{F}_q^n$ of the equation

$$P_{k,j}(\mathbf{x}) = 0 \quad (0 < j < k-1)$$

is

$$\binom{n}{k-1}q^{n-1} + O(q^{n-2})\,.$$

Theorem 5. *Let $n, k \in \mathbb{N}$ $(n \geq k-1 \geq 1)$. Then the number of k-admissible tracks of length n over $\mathbb{F}_q$ is*

$$q^n - \left(\binom{n}{2} + (k-2)\binom{n}{k-1}\right)q^{n-1} + O(q^{n-2})\,.$$

Proof. The polynomials $P_{k,1}(\mathbf{x}), \dots, P_{k,k-2}(\mathbf{x})$ and $V(\mathbf{x})P_{k,k-1}(\mathbf{x})$ are coprime, hence by Theorems 3, 4 and the above remark, the number of solutions of the inequality

$$V(\mathbf{x})\prod_{i=1}^{k-1} P_{k,i}(\mathbf{x}) \neq 0$$

is $q^n - \binom{n}{2}q^{n-1} - (k-2)\binom{n}{k-1}q^{n-1} + O(q^{n-2})$, as required. □

Remark. By Theorem 4, resp. 5, the probability that a chosen at random an n-tuple is a (k,i)-, resp. k-admissible track is

$$1-\frac{\nu}{q}+O(q^{-2}),$$

where $\nu=\binom{n}{2}+\binom{n}{k-1}$, resp. $\binom{n}{2}+(k-2)\binom{n}{k-1}$, and for sufficiently large q, it is close to certainty.

2.2 Extendability of admissible tracks

Let $n,k,r\in\mathbb{N}$ satisfy $1\le k-1\le n<q$ and $n+r<q$. Let $\mathbf{t}'\in\mathbb{F}_q^n$ and $\mathbf{t}''\in\mathbb{F}_q^r$ be disjoint tracks. Fix $0\le i\le k-1$. Denote by $\mathbf{t}$ concatenation of $\mathbf{t}'$ and $\mathbf{t}''$; i.e., $\mathbf{t}=\mathbf{t}'||\mathbf{t}''\in\mathbb{F}_q^{n+r}$. The question is whether for a (k,i)-, resp. k-admissible track $\mathbf{t}'$ there exists a track $\mathbf{t}''$ disjoint with $\mathbf{t}'$ such that $\mathbf{t}$ is a (k,i)-, resp. k-admissible track.

Theorem 6, resp. 8 below gives us an information on extendability of (k,i)-, resp. k-admissible tracks for sufficiently large q. We start with the case when $r=1$. Theorems 7 and 9 deal with the existence of such tracks for relatively small q.

Theorem 6. *Fixed $0<i<k-1$, let $\mathbf{t}'=(t_0,\dots,t_{n-1})\in\mathbb{F}_q^n$ be a (k,i)-admissible track. If $q>n+\binom{n}{k-2}$, then there exists $t_n\in\mathbb{F}_q\setminus\{t_0,\dots,t_{n-1}\}$ such that the track $\mathbf{t}=(t_0,\dots,t_{n-1},t_n)\in\mathbb{F}_q^{n+1}$ is also a (k,i)-admissible track. The number of such t_n is at least*

$$q-n-\binom{n}{k-2}.$$

For $i=0$, resp. $k-1$, such a t_n exists if $q>n+1$, resp. n and the number of such t_n is $q-n-1$, resp. $q-n$.

Proof. Set $\mathbf{t}=(t_0,\dots,t_{n-1},x)$ with an indeterminate x. Write $F(x)=V(\mathbf{t})P_{k,k-1-i}(\mathbf{t})$. We have

$$F(x)=V(\mathbf{t}')P_{k,k-1-i}(\mathbf{t}')\prod_{j=0}^{n-1}(x-t_j)\cdot\prod_{\substack{\rho\in R_{n+1}(k)\\ \rho_{k-2}=n}}\left(a_{\rho,i}x+b_{\rho,i}\right),$$

where $a_{\rho,i},b_{\rho,i}\in\mathbb{F}_q$, $a_{\rho,i}=\tau_{k-2-i}(t_{\rho_0},\dots,t_{\rho_{k-3}})$, $b_{\rho,i}=\tau_{k-1-i}(t_{\rho_0},\dots,t_{\rho_{k-3}})$ and the latter product is taken over all ρ with $\rho_{k-2}=n$.

Note that for any ρ, by (1), $\tau_{k-1-i}(\mathbf{t}(\rho))=a_{\rho,i}x+b_{\rho,i}$ is a non-zero polynomial of x. Indeed, if $a_{\rho,i}=b_{\rho,i}=0$, then we would have

$$t_{\rho_{k-2}}\tau_{k-2-i}(t_{\rho_0},\dots,t_{\rho_{k-3}})+\tau_{k-1-i}(t_{\rho_0},\dots,t_{\rho_{k-3}})=0,$$

and so, by (1), $\tau_{k-1-i}(t_{\rho_0},\dots,t_{\rho_{k-2}})=0$ for every $t_{\rho_{k-2}}\in\mathbb{F}_q$. This is impossible since $\mathbf{t}'$ is a (k,i)-admissible track.

Consequently, by (2), we obtain

$$F(x)=C\prod_{j=0}^{n-1}(x-t_j)\cdot\prod_{\substack{\rho\in R_{n+1}(k)\\ \rho_{k-2}=n}}\left(a_{\rho,i}x+b_{\rho,i}\right)\in\mathbb{F}_q[x]$$

with $C\in\mathbb{F}_q$, $C\neq 0$ constant.

Since the number of zeros of a univariate polynomial F over a field does not exceed $\deg F$, if $q>\deg F$ there exists $t_n\in\mathbb{F}_q$ such that $F(t_n)\neq 0$ and so $V(\mathbf{t})P_{k,k-1-i}(\mathbf{t})\neq 0$. Thus the first part of the theorem follows from (2) and the inequality $\deg F\le n+\binom{n}{k-2}$ if $1<i<k-1$. Hence, it also follows that the number of (k,i)-admissible tracks $\mathbf{t}$ is at least $q-\deg F\le q-n-\binom{n}{k-2}$, which completes the proof if $1<i<k-1$. An easy verification gives the theorem if $i=0$ or $k-1$. □

Corollary. *Let $0<i<k-1$ and let $\mathbf{t}'\in\mathbb{F}_q^n$ be a (k,i)-admissible track. For a fixed $r\in\mathbb{N}$, if $q>n+r-1+\binom{n+r-1}{k-2}$, then there exists a track $\mathbf{t}''\in\mathbb{F}_q^r$ disjoint with $\mathbf{t}'$ such that the track $\mathbf{t}=\mathbf{t}'||\mathbf{t}''$ is also a (k,i)-admissible track. The number of such tracks is at least*

$$\prod_{j=0}^{r-1}\left(q-(n+j)-\binom{n+j}{k-2}\right).$$

For $i=0$, resp. $k-1$, such a $\mathbf{t}''$ exists if $q>n+r$, resp. $n+r-1$ and the number of $\mathbf{t}''$ is $(q-n-1)\dots(q-n-r)$, resp. $(q-n)\dots(q-n-r+1)$.

Proof. The corollary follows from Theorem 6 by induction on r. □

Theorem 7. *Fix $0<i<k-1$. If $q>n-1+\binom{n-1}{k-2}$, then (k,i)-admissible tracks of length n over $\mathbb{F}_q$ exist and the number of such tracks is at least*

$$\prod_{j=0}^{i-1}(q-j)\prod_{j=i}^{k-2}(q-j-1)\prod_{j=k-1}^{n-1}\left(q-j-\binom{j}{k-2}\right).$$

(*Recall that, by Theorem 4, for $i=0$, resp. $k-1$, if $q>n$, resp. $n-1$, (k,i)-admissible tracks of length n over $\mathbb{F}_q$ exist and the number of such tracks is $(q-1)\dots(q-n)$, resp. $q(q-1)\dots(q-n+1)$.*)

Proof. We begin the proof with an auxiliary lemma:

Lemma 2. *For $0 \le i \le k-1$ and $q \ge k$ the number of solutions in $\mathbb{F}_q^{k-1}$ of the inequality*

$$V(x_0, \dots, x_{k-2})\tau_i(x_0, \dots, x_{k-2}) \neq 0 \tag{8}$$

is at least

$$\prod_{j=1}^{k-i-1} (q-j+1) \prod_{j=k-i}^{k-1} (q-j)\,.$$

Proof. We proceed by induction on i. For $i = 0$ the bound is obvious. Assume that the bound is true for $i-1$ and $0 < i \le k-1$. We shall prove it for i. Then we have by (1)

$$\tau_i(x_0, \dots, x_{k-2}) = x_0\tau_{i-1}(x_1, \dots, x_{k-2}) + \tau_i(x_1, \dots, x_{k-2})\,.$$

If $V(x_1, \dots, x_{k-2})\tau_{i-1}(x_1, \dots, x_{k-2}) \neq 0$, (8) will be satisfied, provided x_0 is different from $x_1, \dots, x_{k-2}$ and from $\frac{-\tau_i(x_1,\dots,x_{k-2})}{\tau_{i-1}(x_1,\dots,x_{k-2})}$. By the inductive assumption we obtain at least $\prod_{j=1}^{k-i-1}(q-j+1)\prod_{j=k-i}^{k-1}(q-j)$ solutions. □

Proof of Theorem 7: By Lemma 2, if $q \ge k$, then (k,i)-admissible tracks of length $k-1$ exist and the number of such tracks is at least $\prod_{j=0}^{i-1}(q-j)\prod_{j=i}^{k-2}(q-j-1)$. By the last corollary with $n = k-1$, $r = n-k+1$, if $q > n-1+\binom{n-1}{k-2}$, then each of these tracks can be extended to a (k,i)-admissible track of length n in at least $\prod_{j=k-1}^{n-1}\left(q-j-\binom{j}{k-2}\right)$ ways. This proves the theorem. □

Theorem 8. *Let $\mathbf{t}' = (t_0, \dots, t_{n-1}) \in \mathbb{F}_q^n$ be a k-admissible track. If $q > (n+1)+(k-2)\binom{n}{k-2}$, then there exists $t_n \in \mathbb{F}_q \setminus \{t_0, \dots, t_{n-1}\}$ such that the track $\mathbf{t} = (t_0, \dots, t_{n-1}, t_n) \in \mathbb{F}_q^{n+1}$ is also a k-admissible track. The number of such t_n is at least*

$$q-(n+1)-(k-2)\binom{n}{k-2}\,.$$

Proof. Let $\mathbf{t} = (t_0, \dots, t_{n-1}, x)$ for an indeterminate x. Set $F(x) = V(\mathbf{t})P_k(\mathbf{t})$. We have

$$F(x) = V(\mathbf{t}')P_k(\mathbf{t}')\prod_{j=0}^{n-1}(x-t_j)\cdot\prod_{i=0}^{k-2}\prod_{\substack{\rho\in R_{n+1}(k)\\ \rho_{k-2}=n}}\tau_{k-1-i}(\mathbf{t}(\rho))\,.$$

As in the proof of Theorem 6, in view of $\tau_{k-1}(\mathbf{t}(\rho)) = t_{\rho_0}\dots t_{\rho_{k-2}}$, by (3) we deduce that

$$F(x) = Cx^{\binom{n}{k-2}}\prod_{j=0}^{n-1}(x-t_j)\cdot\prod_{i=1}^{k-2}\prod_{\substack{\rho\in R_{n+1}(k)\\ \rho_{k-2}=n}}\left(a_{\rho,i}x+b_{\rho,i}\right)\in\mathbb{F}_q[x]$$

with $C \in \mathbb{F}_q$, $C \neq 0$ constant and non-zero linear polynomials $\tau_{k-1-i}(\mathbf{t}(\rho)) = a_{\rho,i}x + b_{\rho,i}$.

Note that the equations $F(x) = 0$ and $x^{-\binom{n}{k-2}+1}F(x) = 0$ have the same sets of solutions. Consequently, since the number of zeros of a univariate polynomial over a field does not exceed its degree, the number of $t_n \in \mathbb{F}_q$ such that $F(t_n) \neq 0$ is at least $q - \deg F + \binom{n}{k-2} - 1$, which is, by (3), a lower bound for the number of k-admissible tracks $\mathbf{t} = \mathbf{t}'||(t_n)$. Hence the second part of the theorem follows by the inequality $\deg F \leq n + (k-1)\binom{n}{k-2}$. The first part of the theorem follows from the second part immediately. □

Corollary. *Let $\mathbf{t}' \in \mathbb{F}_q^n$ be a k-admissible track. For a fixed $r \in \mathbb{N}$, if $q > n + r + (k-2)\binom{n+r-1}{k-2}$, then there exists a track $\mathbf{t}'' \in \mathbb{F}_q^r$ disjoint with $\mathbf{t}'$ such that the track $\mathbf{t} = \mathbf{t}'||\mathbf{t}''$ is also a k-admissible track. The number of such tracks is at least*

$$\prod_{j=0}^{r-1} \left(q - (n+j+1) - (k-2)\binom{n+j}{k-2} \right).$$

Proof. The corollary follows from Theorem 8 by simple induction on r. □

Remark. By Theorem 6, resp. 8, the probability that a chosen at random $t_n \in \mathbb{F}_q$ gives a (k,i)-, resp. k-admissible track $\mathbf{t} = \mathbf{t}'||(t_n)$ is at least $1 - \frac{\nu}{q}$, where

$$\nu = \begin{cases} n+1, & \text{if } i = 0; \\ n, & \text{if } i = k-1; \\ (n+1) + \binom{n}{k-2}, & \text{if } i \neq 0, k-1, \end{cases}$$

resp. $\nu = (n+1) + (k-2)\binom{n}{k-2}$, which in typical situation, for large q, is close to certainty.

Theorem 9. *If $q > n + (k-2)\binom{n-1}{k-2}$, then k-admissible tracks exist. The number of such tracks is at least*

$$\prod_{j=0}^{k-2} (q - 2j - 1) \prod_{j=k-1}^{n-1} \left(q - (j+1) - (k-2)\binom{j}{k-2} \right).$$

Proof. We start with the lemma:

Lemma 3. *For all $k \geq 2$ the number of solutions of the inequality*

$$V(x_0, \ldots, x_{k-2}) \prod_{i=1}^{k-1} \tau_i(x_0, \ldots, x_{k-2}) \neq 0 \tag{9}$$

is at least

$$\prod_{j=1}^{k-1}\big(q-2j+1\big)\,.$$

Proof. We proceed by induction on k. For $k=2$ the bound is obvious. Assume that the bound is true for $k-1$ variables. If

$$V(x_1,\dots,x_{k-1})\prod_{i=1}^{k-1}\tau_i\big(x_1,\dots,x_{k-1}\big)\neq 0$$

the inequality (9) will be satisfied provided x_0 is different from $x_1,\dots,x_{k-1}$ and from $\frac{-\tau_i(x_1,\dots,x_k)}{\tau_{i-1}(x_1,\dots,x_k)}$ $(1\le i\le k)$. By the inductive assumption we obtain at least

$$\prod_{j=1}^{k}\big(q-2j+1\big)$$

solutions. □

Proof of Theorem 9*:* By Lemma 3, if $q\ge 2k-2$, then k-admissible tracks of length $k-1$ exist and the number of them is at least $\prod_{j=0}^{k-2}(q-2j-1)$. By the last corollary with $n=k-1$, $r=n-k+1$, if $q>n+(k-2)\binom{n-1}{k-2}$, then each of these tracks can be extended to a k-admissible track of length n in at least $\prod_{j=k-1}^{n-1}\big(q-(j+1)-(k-2)\binom{j}{k-2}\big)$ ways. This proves the theorem. □

Remark. Asymptotically for $q\to\infty$ the lower bounds given in Lemma 2, Theorems 7 and 9 are only slightly weaker than these given in Theorems 4 and 5 and are non-trivial for relatively small q.

3 Algorithms for constructing and extending admissible tracks

In this section we describe algorithms for constructing and extending of (k,i)-admissible and k-admissible tracks.

3.1 Constructing and extending (k,i)-admissible tracks

Let $k\le n<q$. Fix $0\le i\le k-1$. In this subsection, we first describe an algorithm for constructing (k,i)-admissible tracks $\mathbf{t}=(t_0,\dots,t_{k-2})$ of length $k-1$; i.e., such that $\tau_{k-1-i}(t_0,\dots,t_{k-2})\neq 0$. Next, we describe another algorithm which allows to extend a (k,i)-admissible track $\mathbf{t}=(t_0,\dots,t_{m-1})$ of length m with $m\ge k-1$ to a longer (k,i)-admissible track.

The composition of the auxiliary and extending algorithms gives an algorithm for constructing (k, i)-admissible tracks.

Since any track $(t_0, \ldots, t_{n-1})$, $n \geq k-1$ is $(k, k-1)$-admissible we need only consider the cases when $0 \leq i < k-1$. To shorten the notation we set $j = k-1-i$.

3.1.1 Auxiliary Algorithm

INPUT: positive integers k, j with $k \geq 2$, $0 < j \leq k-1$.

OUTPUT: a track $\mathbf{t} = (t_0, \ldots, t_{k-2})$ such that $\tau_j(t_0, \ldots, t_{k-2}) \neq 0$.

1. (*Computing* $t_0, \ldots, t_{k-2}$) Do the following:
   - 1.1. If $j = 0$, for $t_0, \ldots, t_{k-2}$, choose arbitrary $k-1$ pairwise different elements of $\mathbb{F}_q$.
   - 1.2. If $0 < j \leq k-1$ do the following:
     - 1.2.1. For $t_0, \ldots, t_{j-1}$, choose arbitrary non-zero pairwise different elements of $\mathbb{F}_q$.
     - 1.2.2. For $l = j$ to $k-2$ do the following:
       - 1.2.2.1. Set $\mathcal{S}_l \leftarrow \{\frac{-\tau_j(t_0,\ldots,t_{l-1})}{\tau_{j-1}(t_0,\ldots,t_{l-1})}\}$ if $\tau_{j-1}(t_0, \ldots, t_{l-1}) \neq 0$ and $\mathcal{S}_l \leftarrow \emptyset$ otherwise.
       - 1.2.2.2. Select as t_l an arbitrary element of $\mathbb{F}_q \setminus (\{t_0, \ldots, t_{l-1}\} \cup \mathcal{S}_l)$.
2. Return($\mathbf{t}$).

Remark. Note that in step 1.2.2.2 such an element t_l exists if $l+1 < q$. The number of such elements is at least $q-l-1$. The output exists if $k < q$.

3.1.2 Proof of correctness of Algorithm 3.1.1

By definition, the elements $t_0, \ldots, t_{k-2}$ are pairwise different so we need to prove that $\tau_j(t_0, \ldots, t_{k-2}) \neq 0$.

If $j = 0$, then $\tau_j(t_0, \ldots, t_{k-2}) = 1 \neq 0$ for arbitrary $t_0, \ldots, t_{k-2} \in \mathbb{F}_q$. If $0 < j \leq k-1$, then $\tau_j(t_0, \ldots, t_{j-1}) = t_0 \ldots t_{j-1} \neq 0$ since $t_0, \ldots, t_{j-1} \in \mathbb{F}_q \setminus \{0\}$. In particular, if $j = k-1$, then $\tau_j(t_0, \ldots, t_{k-2}) \neq 0$. Now, let $0 < j < k-1$. We show by induction that $\tau_j(t_0, \ldots, t_l) \neq 0$ for each $j \leq l \leq k-2$. Assume that $\tau_j(t_0, \ldots, t_{l-1}) \neq 0$ for some $j \leq l \leq k-2$. Then by (1)

$$\tau_j(t_0, \ldots, t_l) = t_l \tau_{j-1}(t_0, \ldots, t_{l-1}) + \tau_j(t_0, \ldots, t_{l-1}) \neq 0$$

since by step 1.2.2 we have $t_l \neq \frac{-\tau_j(t_0,\ldots,t_{l-1})}{\tau_{j-1}(t_0,\ldots,t_{l-1})}$ if $\tau_{j-1}(t_0, \ldots, t_{l-1}) \neq 0$. □

3.1.3 Extending Algorithm

INPUT: positive integers k, m, r, j with $k \geq 2$, $m \geq k-1$, $0 < j \leq k-1$ and a (k,i)-admissible track $\mathbf{t} = (t_0, \dots, t_{m-1})$ $(i = k-1-j)$.

OUTPUT: $t_m, \dots, t_{m+r-1}$ such that $\mathbf{t}' = \mathbf{t}||(t_m, \dots, t_{m+r-1})$ is a (k,i)-admissible track.

1. (*Computing* $t_m, \dots, t_{m+r-1}$) For $l = m$ to $m+r-1$, do the following:
   1.1. Set $\mathcal{I}_l \leftarrow$ the set of all subsequences $\rho = (\rho_0, \dots, \rho_{k-3})$ of length $k-2$ of the sequence $\mathbf{e}_l$ such that $\tau_{j-1}(t_{\rho_0}, \dots, t_{\rho_{k-3}}) \neq 0$.
   1.2. Set $\mathcal{S}_l \leftarrow \{\frac{-\tau_j(t_{\rho_0},\dots,t_{\rho_{k-3}})}{\tau_{j-1}(t_{\rho_0},\dots,t_{\rho_{k-3}})} :\ \rho \in \mathcal{I}_l\}$.
   1.3. Select as t_l an arbitrary element of $\mathbb{F}_q \setminus (\{t_0, \dots, t_{l-1}\} \cup \mathcal{S}_l)$.
2. Return($\mathbf{t}'$).

Remark. Note that in step 1.3 such an element t_l exists if $l + \binom{l}{k-2} < q$, resp. $l+1$ if $i > 0$, resp. $i = 0$. The number of such elements is at least $q - l - \binom{l}{k-2}$, resp. $q - l - 1$.

3.1.4 Proof of correctness of Algorithm 3.1.3

It suffices to show that the algorithm produces a (k,i)-admissible track in the case when $r = 1$; i.e., that $\mathbf{t}' = (t_0, \dots, t_{m-1}, t_m)$ is a (k,i)-admissible track. Notice that, by construction, the elements $t_0, \dots, t_{m-1}, t_m$ are pairwise different. By assumption, $\tau_j(t_{\rho_0}, \dots, t_{\rho_{k-2}}) \neq 0$ for all subsequences $(\rho_0, \dots, \rho_{k-2})$ of length $k-1$ of the sequence $\mathbf{e}_m$. Since by (1)

$$\tau_j(t_{\rho_0}, \dots, t_{\rho_{k-2}}) = t_{\rho_{k-2}} \tau_{j-1}(t_{\rho_0}, \dots, t_{\rho_{k-3}}) + \tau_j(t_{\rho_0}, \dots, t_{\rho_{k-3}}),$$

it follows that for any subsequence $(\rho_0, \dots, \rho_{k-3})$ of length $k-2$ of the sequence $\mathbf{e}_m$ at least one of the $\tau_{j-1}(t_{\rho_0}, \dots, t_{\rho_{k-3}})$ and $\tau_j(t_{\rho_0}, \dots, t_{\rho_{k-3}})$ is $\neq 0$. Consequently, for all subsequences $(\rho_0, \dots, \rho_{k-3})$ of the sequence $\mathbf{e}_m$ we have

$$\tau_j(t_{\rho_0}, \dots, t_{\rho_{k-3}}, t_m) = t_m \tau_{j-1}(t_{\rho_0}, \dots, t_{\rho_{k-3}}) + \tau_j(t_{\rho_0}, \dots, t_{\rho_{k-3}}) \neq 0$$

since $t_m \neq \frac{-\tau_j(t_{\rho_0},\dots,t_{\rho_{k-3}})}{\tau_{j-1}(t_{\rho_0},\dots,t_{\rho_{k-3}})}$ if $\tau_{j-1}(t_{\rho_0}, \dots, t_{\rho_{k-3}}) \neq 0$. Thus for all subsequences $(\rho_0, \dots, \rho_{k-2})$ of the sequence $\mathbf{e}_{m+1}$ we have $\tau_j(t_{\rho_0}, \dots, t_{\rho_{k-2}}) \neq 0$, and so $(t_0, \dots, t_{m-1}, t_m)$ is a (k,i)-admissible track with $i = k-j-1$. □

Remark. Note that the estimates given in the remarks following the algorithms 3.1.1 and 3.1.3 confirm Theorems 6 and 7.

3.2 Constructing and extending k-admissible tracks

In this subsection, as previously, we first describe an algorithm for constructing a k-admissible track $\mathbf{t} = (t_0, \ldots, t_{k-2})$; i.e., such that $\tau_j(t_0, \ldots, t_{k-2}) \neq 0$ for each $0 \leq j \leq k-1$. Next, we describe another algorithm which allows to extend a k-admissible track $\mathbf{t} = (t_0, \ldots, t_{m-1})$, $m \geq k-1$, to a longer k-admissible track.

As in the previous subsection, the composition of the auxiliary and extending algorithms gives an algorithm for constructing k-admissible tracks.

3.2.1 Auxiliary Algorithm

INPUT: a positive integer k, $k \geq 2$.

OUTPUT: a track $\mathbf{t} = (t_0, \ldots, t_{k-2})$ such that $\tau_j(t_0, \ldots, t_{k-2}) \neq 0$ for each $j = 0, \ldots, k-1$.

1. (*Computing* $t_0, \ldots, t_{k-2}$) Do the following:
   1.1. For t_0, choose an arbitrary non-zero element of $\mathbb{F}_q$.
   1.2. For $l = 1$ to $k-2$ do the following:
      1.2.1. Set $\mathcal{S}_l \leftarrow \{\frac{-\tau_j(t_0,\ldots,t_{l-1})}{\tau_{j-1}(t_0,\ldots,t_{l-1})} : \ j = 1, \ldots, l+1\}$.
      1.2.2. Select as t_l an arbitrary element of $\mathbb{F}_q \setminus (\{t_0, \ldots, t_{l-1}\} \cup \mathcal{S}_l)$.
2. Return($\mathbf{t}$).

Remark. Note that in step 1.2.2 such an element t_l exists if $2l + 1 < q$. The number of such elements t_l is at least $q - 2l - 1$. The output exists if $2(k-1) \leq q$.

3.2.2 Proof of correctness of Algorithm 3.2.1

By definition, the elements $t_0, \ldots, t_{k-2}$ are pairwise different so we need to show that $\tau_j(t_0, \ldots, t_{k-2}) \neq 0$ for each $0 \leq j \leq k-1$. In fact, we show that for each $1 \leq l \leq k-1$ we have $\tau_j(t_0, \ldots, t_{l-1}) \neq 0$ for any $0 \leq j \leq l$. Note that the latter inequality holds for $l = 1$ since $t_0 \neq 0$.

Assuming, for some $1 \leq l \leq k-2$, that $\tau_j(t_0, \ldots, t_{l-1}) \neq 0$ for each for $0 \leq j \leq l$, we shall prove that $\tau_j(t_0, \ldots, t_l) \neq 0$ for each for $0 \leq j \leq l+1$. Since $\tau_0(t_0, \ldots, t_l) = 1 \neq 0$, we need to prove the latter inequality for $1 \leq j \leq l+1$. Note that $\tau_{j-1}(t_0, \ldots, t_{l-1}) \neq 0$ by the inductive hypothesis. By (1), it follows that

$$\tau_j(t_0, \ldots, t_l) = t_l \tau_{j-1}(t_0, \ldots, t_{l-1}) + \tau_j(t_0, \ldots, t_{l-1}) \neq 0$$

since, by step 1.2, we have that $t_l \neq \frac{-\tau_j(t_0,\ldots,t_{l-1})}{\tau_{j-1}(t_0,\ldots,t_{l-1})}$. □

3.2.3 Extending Algorithm

INPUT: positive integers k, m, r with $k \geq 2$, $m \geq k-1$ and a k-admissible track $\mathbf{t} = (t_0, \dots, t_{m-1})$.

OUTPUT: $t_m, \dots, t_{m+r-1}$ such that $\mathbf{t}' = \mathbf{t}||(t_m, \dots, t_{m+r-1})$ is a k-admissible track.

1. (*Computing* $t_m, \dots, t_{m+r-1}$) For $l = m$ to $m+r-1$ do the following:

   1.1. For each $j = 1, 2, \dots, k-1$ set $\mathcal{I}_{l,j} \leftarrow$ the set of all subsequences $\rho = (\rho_0, \dots, \rho_{k-3})$ of length $k-2$ of the sequence $\mathbf{e}_l$ such that $\tau_{j-1}(t_{\rho_0}, \dots, t_{\rho_{k-3}}) \neq 0$.

   1.2. For $j = 1, \dots, k-1$, set $\mathcal{S}_{l,j} \leftarrow \{\frac{-\tau_j(t_{\rho_0}, \dots, t_{\rho_{k-3}})}{\tau_{j-1}(t_{\rho_0}, \dots, t_{\rho_{k-3}})} \colon \ \rho \in \mathcal{I}_{l,j}\}$.

   1.3. Select as t_l an arbitrary element of $\mathbb{F}_q \setminus (\{t_0, \dots, t_{l-1}\} \cup \bigcup_{j=1}^{k-1} \mathcal{S}_{l,j})$.

2. Return($\mathbf{t}'$).

Remark. Since $\mathcal{S}_{l,k-1} = \{0\}$, in step 1.3 such an element t_l exists if $(l+1) + (k-2)\binom{l}{k-2} < q$. The number of such elements t_l is at least $q - (l+1) - (k-2)\binom{l}{k-2}$.

3.2.4 Proof of correctness of Algorithm 3.2.3

The proof is the same as that in 3.1.4 except that now we have to consider all $0 < j \leq k-1$ instead of a fixed j. □

Remark. Note that the estimates in the remarks following the algorithms 3.2.1 and 3.2.3 confirm Theorems 8 and 9.

4 Concluding remarks

We proved existence and extendability of (k, i)-, resp. k-admissible tracks in Shamir's secret sharing scheme and gave some algorithms for their constructing and extending. We estimated the number of such tracks.

The k-admissible tracks allow to construct Shamir's multi-secret sharing schemes with the secret placed as an arbitrary coefficient of its generic polynomial. We can apply the schemes corresponding to k-admissible tracks not only to a single secret but to up to k many secrets with the same shares, and with the same threshold.

In forthcoming papers we shall discuss some related questions for Lai-Ding's secret sharing schemes.

5 Acknowledgement

The authors are grateful to Professor Marian Srebrny for his valuable comments during writing the paper.

References

[1] C.A. Asmuth and J. Bloom, A modular approach to key safeguarding, *IEEE Trans. on Information Theory* **29** (1983), 208—210.

[2] G.R. Blakley, Safeguarding cryptographic keys, *AFIPS Conference Proc.* **48** (1979), 313–317.

[3] C.-P. Lai and C. Ding, Several Generalizations of Shamir's Secret Sharing Scheme, *Internat. J. Found. Comput. Sci.* **15** (2004), 445–458.

[4] M. Mignotte, How to share a secret, In: Beth T. (Ed.), *Cryptography Proc. of the Workshop on Cryptography, Burg Feuerstein,* 1982, Springer-Verlag *Lecture Notes in Computer Science* **149** (1983), 371–375.

[5] A.J. Menezes, P. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[6] W.M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Second Edition, Kendrick Press, Inc., 2004.

[7] A. Shamir, How to share a secret, *Communications of the ACM* **22** (1979), 612–613.

[8] S. Spież, M. Srebrny and J. Urbanowicz, *Secret Sharing Matrices*, submitted for publication.