IV. SCHEMATY PODZIAŁU SEKRETU STRUKTURY WPROWADZEŃ

REMARKS ON MULTIVARIATE EXTENSIONS OF POLYNOMIAL BASED SECRET SHARING SCHEMES

Jakub Derbisz

Institute of Computer Science Polish Academy of Sciences'
fellowship for postdoctoral researchers;
jakub.derbisz@gmail.com

Abstract. We introduce methods that use Gröbner bases for secure secret sharing schemes. The description is based on polynomials in the ring $R = K[X_1, \ldots, X_l]$ where identities of the participants and shares of the secret are or are related to ideals in R. Main theoretical results are related to algorithmical reconstruction of a multivariate polynomial from such shares with respect to given access structure, as a generalisation of classical threshold schemes. We apply constructive Chinese remainder theorem in R of Becker and Weispfenning. Introduced ideas find their detailed exposition in our related works.

Keywords: Gröbner bases, Chinese remainder theorem, Secret Sharing Scheme, access structure, multivariate interpolation.

1. Introduction

We present ideas for conditional generalisation of Shamir's (t, n) threshold secret sharing scheme and Blakley's threshold SSS, and show how to create secure secret sharing schemes on multivariate polynomials, assuming fast calculation of minimal CRT-solution in a variant of CRT-algorithm for multivariate polynomial ring [2]. However, as we will show there are certain possibilities to satisfy this assumption in practice.

In Shamir's scheme one considers randomly chosen polynomial f of one variable and degree $t-1$, and distributes to each of n participants an element c_i of some finite field, publicly assigning it to $i-th$ participant as his identity, and, appropriately the secret value $f(c_i)$. Now, t participants from received elements can reconstruct the polynomial, since t values in t different field elements determine uniquely a polynomial of degree $t-1$.

The study is cofounded by the European Union from resources of the European Social Fund. Project PO KL „Information technologies: Research and their interdisciplinary applications, Agreement UDA-POKL.04.01.01-00-051/10-00.

A question motivating this work is how to construct a secret sharing scheme if instead of choosing a polynomial of one variable one would take multivariate polynomial $g \in K[X_1, \ldots, X_l]$, and keep unchanged the ideas of Shamir's scheme. Hence, now participants publicly receive vectors $\mathbf{c}_i \in K^l$, there are secretly distributed values $g(\mathbf{c}_i)$, and we ask about reconstruction of g. It leads then to a general case where any privileged group of a general access structure would be able to reconstruct a multivariate polynomial from shares of the participants.

First, we propose to define a class of polynomials $\mathcal{P}$ and a set of vectors $\{\mathbf{c}_i \in K^l |\ i = 1, \ldots, n\}$ that would allow, applying Chinese remainder theorem, reconstruction of such g by t or more participants, while less than t participants would know that there are at least $|K|$ polynomials from $\mathcal{P}$ possible to be the polynomial g that was chosen. In our extended works related to this topic we show that there exist and can be found examples for such classes $\mathcal{P}$ and appropriate sets of vectors.

Likewise, later we give an idea for a construction which allows to distribute a multivariate polynomial among the participants forming any monotonic access structure, such that a privileged set would be able to reconstruct it, and unprivileged set wouldn't, meaning that there will be at least $|K|$ possible choices for the polynomial, or, as it is also possible, if a value in some point of the multivariate polynomial is treated as the secret, privileged sets can find this value, and unprivileged sets have no information, i.e., any element from K will be equally probable to be that value.

In latter construction we won't need a class $\mathcal{P}$ with certain properties or appropriately chosen set of vectors, hence the construction will be more explicit. Instead of relying on vectors, we associate with each participant an ideal, giving an algorithm for its construction, and for the secret polynomial, we take any polynomial from $K[X_1, \ldots, X_l]$ of a type

$$f = f_0 + \sum_{1 \leq i_1 < \ldots < i_{k-1} \leq k} c_{i_1 \ldots i_{k-1}} g_{i_1} \cdots g_{i_{k-1}}$$

where $deg(f_0) < deg(g_1 \ldots g_k)$ and constants $c_{i_1 \ldots i_{k-1}}$ are chosen at random with respect to uniform distribution on K (also, the secret can be taken as value in its certain point).

However, as we have mentioned, the constructions are conditional since we assume fast calculations of Gröbner bases needed in reconstructing the secret polynomial by privileged groups when applying CRT-algorithm [2]. The main motivation then is a theoretical and direct generalisation implied by Shamir's scheme. Although, it is possible that in practice these

particular Gröbner bases can efficiently be computed, it is not the subject of this research and we leave this practical question for further consideration. Thus, we haven't been considering whether our constructions allow new applications or, from practical point of view, are in any sense better from constructions already proposed. They, however, show how to transform ideas known in secret sharing schemes into language based on ideals, abstract algebra, which also allowed achieving certain theoretical results, as, for instance, classical Shamir's secret sharing scheme where reconstruction of secret polynomial is based on Chinese remainder theorem, and its generalisations. Our considerations may as well be interesting for those interested in theory of interpolation.
To sum up:
In the first part, our ideas concern a possible framework for general constructions of threshold polynomial based secret sharing schemes which are generalisations of the classical constructions. For instance, we show how to reconstruct a polynomial in Shamir's scheme using CRT, and propose a generalisation. Our primary goal is to introduce an approach for constructing secret sharing schemes based on Gröbner bases and Becker's, Weispfenning's algorithm for finding minimal CRT-solution in $R = K[X_1, \ldots, X_l]$.

In the second part, we propose methods to deal with a general case and the construction of a secret sharing scheme for any general access structure with a use of multivariate polynomial; general means that we have an arbitrary, not necessarily threshold monotonic access structure. Users' identities are ideals of R, secret is a multivariate polynomial, and shares are certain polynomials that come from reducing the secret modulo certain Gröbner bases. In our constructions, we assume efficiency of finding the solution by CRT-algorithm [2].

2. Basic definitions

We will briefly define basic concepts.

Monotonic family Γ on X is a family of subsets of X such that if $A \in \Gamma$ and $A \subseteq B \subseteq X$ then $B \in \Gamma$.
Privileged or qualified sets of participants forming a monotonic family Γ are those sets of participants that are able to reconstruct a secret from received shares of the secret, i.e., there is a fast algorithm allowing to do so.
Anti-monotonic family of sets Λ on X is a collection of subsets of X such that if $A \in \Lambda$ and $B \subseteq A$ then $B \in \Lambda$.
Unprivileged sets in *anti-monotonic family* Λ are those sets that are not able to reconstruct the secret in "reasonable time", due to probabilistic or computational bounds.

Secret sharing scheme Σ, called also simply a sharing scheme, is a method of distributing the secret to the participants.

For a set of participants X an *access structure* is a tripple $(\Sigma, \Gamma, \Lambda)$ where $\Gamma \cup \Lambda = 2^X$, and 2^X is the power set of X.

3. Related results

Our approach is related to the constructions of secret sharing schemes in [20], [5], [1], [16], [9]. It is based on methods from the theory of Gröbner bases, in particular, it is based on new application of the CRT-algorithm [2].

Given a field K, there exist propositions for *public key cryptosystems* that use the multivariate polynomial ring $R = K[X_1, \ldots, X_l]$, see, for instance, [13], [15], and Buchberger's algorithm for Gröbner bases computation [3], [7], [12]. However, as it was pointed out in [15] by Koblitz, and which is often the case while working with Gröbner bases in cryptography, the proofs on which one could rely the security of such cryptosystems are very often not known.

We present provably secure constructions of *secret sharing schemes* based on Gröbner bases methods, however, we assume fast calculations of certain Gröbner bases to be able to efficiently find the CRT-solution in the algorithm from [2]. We can assume instead that appropriate bases were publicly announced in precomputations so the CRT-algorithm used for reconstructing the secret polynomial is fast. In [2], the authors give a generalisation of CRT-algorithm known for principal ideal domain as $K[X]$, to CRT-algorithm in the ring $K[X_1, \ldots, X_l]$.

Propositions for secret sharing schemes based on Chinese remainder theorem can also be found in [1], [16].

4. Computational aspects of the ring $K[X_1, \ldots, X_l]$

We will give the preliminaries, needed facts from the theory of Gröbner bases.

When writing about monomials we would think about monic monomials. Considering computations in the ring of multivariate polynomials $R = K[X_1, \ldots, X_l]$ firstly let us state the division theorem, [7], [3], for a total order on a set of monomials such that when $X^\alpha \leq X^\beta$ then $X^{\alpha+\gamma} \leq X^{\beta+\gamma}$, and it is always $X^\alpha \geq 1$. Here, $X^\delta = X_1^{\delta_1} \ldots X_l^{\delta_l}$, that is δ is a multi-index. In the literature this order is called admissible order, however, we refer to it simply as monomial order, since we consider only this type of order on

monomials. Degree lexicographic order or lexicographic order are examples of monomial orders. Assuming axiom of choice, we can have a well order on a field K such that 0 is the minimal element. Of course, we are usually working with finite fields. Thus, we can naturally extend a monomial order and consider a term order (a term understood as a monomial multiplied by a coefficient). For a given polynomial g leading term in g is a leading monomial in g multiplied by its coefficient.

Theorem 1. *For a given term ordering and a set of polynomials* $\{f_1, \ldots, f_k\}$, *every* $f \in R$ *can be written as*

$$f = a_1 f_1 + \ldots + a_k f_k + r$$

where $a_i, r \in R$ *and either* $r = 0$ *or* r *is a* $K-$*linear combination of monomials, none of which is divisible by* $lt(f_1), \ldots, lt(f_k)$ *where* $lt(f_i)$ *is the leading term of* f_i.

This result is known in the theory of Gröbner bases. Its proof implies an algorithm for dividing a polynomial modulo certain set of polynomials with a given term ordering, which would be referred to as reducing the polynomial modulo given set. Gröbner bases are those sets of polynomials, divided modulo which, for any given polynomial there is exactly one remainder r related to that polynomial.
From now on let us fix a certain term ordering.

Definition 1. Gröbner basis for an ideal I of R is a finite collection G of generators of I such that every nonzero $f \in I$ has leading term that is divisible by the leading term of some polynomial from G. We call a finite set of polynomials a Gröbner basis if it is a Gröbner basis of an ideal generated by this set.
For a Gröbner basis $G = \{g_1, \ldots, g_k\}$ for I there is then an equality of ideals

$$(lt(I)) = (lt(g_1), \ldots, lt(g_k))$$

where $(lt(I))$ is the ideal generated by leading terms of polynomials from I. It is easy to see the uniqueness of remainders modulo fixed Gröbner basis, since a monomial lies in a monomial ideal if and only if it is divided by one of monomial generators of the ideal. Thus, for a Gröbner basis $G = \{g_1, \ldots, g_k\}$, writing from division theorem $f = \sum a_i g_i + r_1$ and $f = \sum a'_i g_i + r_2$, if $r_1 \neq r_2$ we have $r_1 - r_2 \in I$ so $lt(r_1 - r_2) \in (lt(I))$, hence one of the terms in r_1 or in r_2 is divisible by $lt(g_i)$ for some i, so there has to be uniqueness.

Calculation of Gröbner basis depends on the ordering of monomials that one chooses and in general could be computationally expensive. However, both standard and reduced Gröbner bases are often computable in practice [12]. In our setting when the Trusted Authority is choosing in precomputation phase the ideals for which the calculations would be executed, for instance, when there is given a general access structure, as we will have in our proposal for a generalised sharing scheme, abovementioned methods could find their practical use. In our presentation, however, we think of a black box providing for the participants necessary calculations of Gröbner bases so that generalised CRT-algorithm from [2] is fast. We can, however, think that relevant Gröbner bases were calculated during the precomputations (and it will be possible).

This assumption need to be dealt with while thinking about applications, as we have described in the introduction. In this presentation, however, we will be always thinking that we have efficient CRT-algorithm and concentrate on developing "general" theory related to sharing a polynomial.

5. Secure secret sharing schemes using CRT in $K[X_1, \ldots, X_l]$

Firstly, we will present an idea related to threshold multivariate polynomial reconstruction. It is convenient to start with univariate example, which would be a Shamir's (t, n) threshold scheme where reconstruction of a polynomial is based on Chinese remainder theorem.
Let $K = \mathbb{F}_q$ be appropriately large finite field.
We randomly choose a polynomial $f(X) = a_0 + a_1X + \ldots + a_{t-1}X^{t-1}$ (randomly choosing coefficients $a_i \in K$). Participants' identities would be different, nonzero field elements $c_i \in K$, $i = 1, \ldots, n$.
$f(c_i) = r_i$ for $i = 1, \ldots, n$ are secret shares of the participants, i.e., r_i is i-th participant's share.
We can write

$$f(c_i) - r_i = 0. \text{ So } (X - c_i)|(f(X) - r_i), \text{ hence } f \in r_i + (X - c_i).$$

Assume, without loss of generality, that t participants with identities $c_1, \ldots, c_t$ have gathered to reconstruct the polynomial. They would make the calculations using the algorithm from [2]. We state the appropriate theorem related to the CRT-algorithm that will be used.

Theorem 2. *Fix any (admissible) monomial order on R. For ideals $I_1, \ldots, I_m$ of R and polynomials $f_1, \ldots, f_m \in R$, sets intersection $\bigcap_{j=1}^{m}(f_j + I_j)$, if non-empty, is equal to $f' + \bigcap_{j=1}^{m} I_j$ where algorithmically constructible $f' \in R$ is minimal in $\bigcap_{j=1}^{m}(f_j + I_j)$ with respect to quasi-order on polynomials in R induced from term ordering in R.*

Hence, those t participants using quasi-order induced from degree--lexicographic order algorithmically find f' of minimal degree such that:

$$\bigcap_{i=1}^{t}(r_i + (X - c_i)) = f' + \bigcap_{i=1}^{t}(X - c_i) = f' + (\prod_{i=1}^{t}(X - c_i))$$

Since f' is minimal $deg(f') \leq deg(f) \leq t - 1$.
Hence, writing $f = f' + h\prod_{i=1}^{t}(X - c_i)$ gives $h = 0$ and $f = f'$, they have found the chosen polynomial.
Generalisation of threshold construction for $R = K[X_1, \ldots, X_l]$.
First, we will assume the following.
Assumption. Assume that for (t, n) there is a set of points $S \in K^l$ of cardinality n and a class of polynomials $\mathcal{P} \subseteq R$, such that for any t points from S, any t values from K, there is a unique polynomial from $\mathcal{P}$ that on the chosen points takes the chosen values respectively.
Having such $\mathcal{P}$ and S:
Choose randomly $g \in \mathcal{P}$ which would be treated as the *secret*.
$g(c_{i1}, \ldots, c_{il}) = r_i$ is the share of i-th participant where $(c_{i1}, \ldots, c_{il})$ is his identity.
From the division theorem we have $g = a_{i1}(X_1 - c_{i1}) + \ldots + a_{il}(X_l - c_{il}) + r$ and thus r is constant and $r = r_i$.
It means $g \in r_i + (X_1 - c_{i1}, \ldots, X_l - c_{il})$.
If t participants gathers to reconstruct the secret, they can calculate the following using CRT-algorithm:

$$\bigcap_{i=1}^{t}(r_i + (X_1 - c_{i1}, \ldots, X_l - c_{il})) = f' + \bigcap_{i=1}^{t}(X_1 - c_{i1}, \ldots, X_l - c_{il})$$

There is

$$(f' + \bigcap_{i=1}^{t}(X_1 - c_{i1}, \ldots, X_l - c_{il})) \cap \mathcal{P} = \{g\}$$

Thus we have certain form of the solution which with the properties of the class $\mathcal{P}$ may allow to extract it. One could give examples of such classes $\mathcal{P}$

when f' that is meant to be found by t participants is exactly g, as, when $\mathcal{P}$ = class of polynomials of the degree not greater than m, and appropriate S and (n,t) so that the assumption is fulfilled (it is possible). Then:

$$deg(f') \leq deg(g) \leq m \Rightarrow f' \in \mathcal{P} \quad \text{and}$$
$$f'(c_{i1}, \ldots, c_{il}) = r_i \quad \text{for} \quad i = 1, \ldots, t \Rightarrow f' = g$$

On the other hand, $t-1$ participants can't reconstruct g since for any t-th value there is in $\mathcal{P}$ one possibility for g.

Using similar ideas, one can also give an algorithm to securely share a multivariate polynomial in (t,t) threshold scheme, i.e., when all participants have to gather to reconstruct the polynomial, where, before the reconstruction the participants *do not know what is the degree of the polynomial that would be reconstructed*. Only briefly sketching the construction, first we have a method to find "general" identities for participants, so that fulfilled is somewhat weaker assumption, that:
for any t values there is at least one polynomial in $K[X_1, \ldots, X_l]$ which takes those values in the identities respectively.
Shares of the participants are randomly chosen $r_i \in K$ and t participants from $r_i + (X_1 - c_{i1}, \ldots, X_l - c_{il})$ for $i = 1, \ldots, t$, reconstruct the secret polynomial f', which was chosen while constructing the scheme using CRT-algorithm.

Further generalisation, to share a polynomial from $K[X_1, \ldots, X_l]$, so it could be reconstructed only by arbitrarily chosen privileged sets.

For any monotonic family Γ, i.e, family of privileged sets, and anti-monotonic family Λ, i.e., family of unprivileged sets, if $\mathbf{N} = \{N_1, \ldots, N_k\}$ is the family of all maximal unprivileged sets, firstly we distribute non-associated irreducible polynomials $g_1, \ldots, g_k$ such that we give g_i to all participants that do not belong to the set N_i, and we perform this procedure for all $i = 1, \ldots, k$. One can see that participants forming a privileged set have received together all $g_1, \ldots, g_k$ and participants forming an unprivileged set lack of certain g_j, $j \in \{1, \ldots, k\}$
Public identity of m-th participant is an ideal $I_m = (g_{\sigma_1} \ldots g_{\sigma_s}) = (g_{\sigma_1}) \cap \ldots \cap (g_{\sigma_s})$ where polynomials used to construct it come from the set he received.
The secret polynomial would be defined as

$$f = f_0 + \sum_{1 \leq i_1 < \ldots < i_{k-1} \leq k} c_{i_1 \ldots i_{k-1}} g_{i_1} \cdots g_{i_{k-1}}$$

where $deg(f_0) < deg(g_1 \dots g_k)$ (or just $f_0 = 0$) and constants $c_{i_1 \dots i_{k-1}}$ are chosen at random with respect to uniform distribution on K. We may keep as the *secret* only the value $f(a)$ in $a \in K^l$ such that $g_i(a) \neq 0$ for all $i = 1, \dots, k$.
The *share* of m-th participant is a polynomial f_m that comes from reducing f modulo Gröbner basis of I_m which here is its generator. Thus, for $I_m = (h_m)$ there is $f = a_m h_m + f_m$. It gives $f \in f_m + I_m$.
For $I = (g_1 \dots g_k) = \bigcap_{m \in B} I_m$ the participants of a privileged set B take degree-lexicographic monomial order and find f' such that

$$f' + I = \bigcap_{m \in B} (f_m + I_m).$$

Since f is an element of this set $deg(f') \leq deg(f)$.
We can write $f = f' + hg_1 \dots g_k$, $f - f' = hg_1 \dots g_k$ which gives $h = 0$ and $f = f'$, so by CRT-algorithm they have found the polynomial f.

If none of the participants forming an unprivileged set A received, say g_k, for any of its participants, if his ideal $I_m = (h_m)$, we can write $g_1 \dots g_k = b_m h_m$, and $f_c = f + cg_1 \dots g_k$ gives the same reduced polynomial as was the share that he had received. That means participants from A cannot deduce f (distinguish between f and f_c), or similarly find $f(a)$, if it is the secret, when a is taken as described.

Example
Let the set of entities $X = \{P_1, P_2, P_3, P_4\}$ and the family of basis sets (minimal privileged sets)
$\mathbf{B} = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4\}\}$.
The related anti-basis (family of maximal unprivileged sets) is
$\mathbf{N} = \{\{P_1\}, \{P_2, P_4\}, \{P_3, P_4\}\}$.
Let $N_1 = \{P_1\}, N_2 = \{P_2, P_4\}, N_3 = \{P_3, P_4\}$.
We will share a multivariate polynomial from $\mathbb{F}_q[X_1, \dots, X_l]$.
Firstly, we construct public ideals for participants using method based on anti-basis:
We choose g_1, g_2, g_3, non-associated irreducible polynomials (3 since $|\mathbf{N}| = 3$). Accordingly to the method of distribution, we give g_1 to every participant except those in N_1, then g_2 to everyone except the participants in N_2, then g_3 to everyone except those who are in N_3. After all:
P_1 receives the set $\{g_2, g_3\}$ and his related ideal is $I_1 = (g_2 g_3) = (g_2) \cap (g_3)$,
P_2 receives the set $\{g_1, g_3\}$ and his related ideal is $I_2 = (g_1 g_3) = (g_1) \cap (g_3)$,
P_3 receives the set $\{g_1, g_2\}$ and his related ideal is $I_3 = (g_1 g_2) = (g_1) \cap (g_2)$,

P_4 receives the set $\{g_1\}$ and his related ideal is $I_4 = (g_1)$.
Let $I = (g_1 g_2 g_3)$.
We now choose a polynomial that will be the secret, it's of the form

$$f = f_0 + c_1 g_1 g_2 + c_2 g_1 g_3 + c_3 g_2 g_3$$

where c_i, $i = 1, 2, 3$ are chosen randomly from $\mathbb{F}_q$, and f_0 is any polynomial that has degree lower than $deg(g_1 g_2 g_3)$. We choose $a \in \mathbb{F}_q$ such that $g_i(a) \neq 0$, $i = 1, 2, 3$ and make it public.
Shares:
We find f_j which is a reduced form of f modulo Gröbner basis of I_j and give f_j to participant P_j as a share, for $j = 1, 2, 3, 4$.
That means f_j is a remainder in Theorem 1 for f modulo Gröbner basis of I_j. Our situation is simple since I_j is principal and its generator is a Gröbner basis for I_j (it is easy to show, since if $J = (h)$ there is $(lt((h))) = (lt(h))$ as was required, so h forms a Gröbner basis).
Take

$$h_1 = g_2 g_3,\ h_2 = g_1 g_3,\ h_3 = g_1 g_2,\ h_4 = g_1.$$

We have $I_j = (h_j)$, $j = 1, \ldots, 4$.
Writing from the Theorem 1

$$f = a_j h_j + f_j.$$

The polynomial f_j is the share of the participant P_j.

We show that participants from sets of $\mathbf{B}$, from their shares, can reconstruct f.
For instance, for the participants P_1 and P_2.
There is

$$I_1 \cap I_2 = (g_2) \cap (g_3) \cap (g_1) \cap (g_3) = (g_1) \cap (g_2) \cap (g_3) = (g_1 g_2 g_3) = I.$$

In Theorem 2, we fix monomial order: degree-lexicographic, since we want CRT-algorithm to find a polynomial of minimal degree. We have quasi-order on polynomials that is induced from it. Next for the ideals I_1 and I_2 and set of polynomials f_1, f_2, the set $(f_1 + I_1) \cap (f_2 + I_2)$ is non-empty because the intersection contains f, which can be noted when we wrote f from Theorem 1.
CRT-algorithm is used to find f'. There is

$$f' + I_1 \cap I_2 = (f_1 + I_1) \cap (f_2 + I_2).$$

So $f' + I = (f_1 + I_1) \cap (f_2 + I_2)$. Our f' is minimal in $(f_1 + I_1) \cap (f_2 + I_2)$. Since f is also an element of that set, it means that f' is smaller than f with respect to quasi-order induced by degree-lexicographic order on monomials. Hence, $deg(f') \leq deg(f)$. The polynomial f was chosen such that $deg(f) < deg(g_1 g_2 g_3)$.
Thus, we also have, $deg(f - f') < deg(g_1 g_2 g_3)$.
Since $f \in f' + I$ we can write $f = f' + h g_1 g_2 g_3$. Then $f - f' = h g_1 g_2 g_3$. So $h = 0$ and $f' = f$. The participants reconstructed f' which turned out to be f. They can also read $f(a)$.
We note that for other sets in $\mathbf{B}$ it is similar.
We will show that participants of an unprivileged set cannot reconstruct f. For instance, take $N_3 = \{P_2, P_4\}$.
Both P_2 and P_4 haven't received g_2 and their ideals are respectively $I_2 = (g_1 g_3)$ and $I_4 = (g_1)$.
From shares f_2 and f_4 they know nothing about the part $c_2 g_1 g_3$ that is in

$$f = f_0 + c_1 g_1 g_2 + c_2 g_1 g_3 + c_3 g_2 g_3.$$

It is because $f_c = f + c g_1 g_3$ would give them the same shares, if chosen (that is if in f was chosen different coefficient by $g_1 g_3$). That is the case since $g_1 g_3$ is an element of both in I_2 and I_4, and, for example, for the participant P_4:
Since f_4 is reduced form of f modulo I_4, that is $f = a_4 g_1 + f_4$.
Then,

$$f_c = f + c g_1 g_3 = a_4 g_1 + f_4 + c g_1 g_3 = g_1(a_4 + c g_3) + f_4.$$

From uniqueness of remainder in Theorem 1 for Gröbner basis, we get that f_4 is also reduced form of f_c modulo I_4 (since it was before).
Similarly for participant P_2 we get that f_2 is reduced form of f_c.

That means participants P_2 and P_4 cannot determine randomly chosen part $c_2 g_1 g_3$ in f, and from that reason, since $g_1(a) g_3(a) \neq 0$, they cannot deduce the value of $f(a)$ as well.

6. Conclusions

We introduced theoretical ideas that allow, basing on methods with Gröbner bases, to describe secure secret sharing schemes. Since we assume fast calculations of certain Gröbner bases that are necessary for finding

efficiently the CRT-solution in a version of CRT-algorithm for multivariate polynomials [2], the results may be noted as theoretical. However, if one searches for applications of proposed constructions of sharing a multivariate polynomial, conducting further research can be the subject: to investigate polynomials such that needed Gröbner bases could really be calculated quickly or to perform precomputations efficiently. For applications, naturally, it is also interesting to examine and compare efficiency.

References

[1] C. Asmuth, J. Bloom, *A modular approach to key safeguarding*, IEEE Trans. on Information Theory, IT-29(2):208-211, 1983.

[2] T. Becker, V. Weispfenning, *The Chinese remainder problem, multivariate interpolation, and Gröbner bases*, Proc. ISSAC'91, Bonn, ACM Press, 6469, New York 1991.

[3] T. Becker, V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Springer-Verlag, 1993.

[4] M. Ben-Or, S. Goldwasser, A. Wigderson, *Completeness theorems for non-cryptographic fault-tolerant distributed computation*, 1-10, Proc. ACM STOC '88.

[5] G. Blakley, *Safeguarding cryptographic keys*, Proceedings of the National Computer Conference 48: 313–317, 1979

[6] E.F. Brickell, *Some ideal secret sharing schemes*, J. Combin. Math. Combin. Comput. 9, 105-113, 1989.

[7] B. Buchberger, *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, N. K. Bose ed. Recent trends in Multidimensional System theory. Dordrecht: Reidel, 184-232, 1985.

[8] B. Buchberger, F. Winkler, *Gröbner Bases and Applications*, Cambridge University Press 1998.

[9] H. Chen, R. Cramer, *Algebraic geometric secret sharing schemes and secure multi-party computations over small fields*, Advances in Cryptology-CRYPTO 2006, Springer Berlin Heidelberg, 521-536, 2006.

[10] J. Derbisz, *Methods of encrypting monotonic access structures*, Annales UMCS Informatica AI XI, 2, 49-60, 2011.

[11] J.-C. Faugére, *A New Efficient Algorithm for Computing Gröbner Basis (F4)*, Journal of Pure and Applied Algebra 139(1-3), 6188, 1999.

[12] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, in: ISSAC 02: Proceedings from the International Symposium on Symbolic and Algebraic Computation, pp. 7583, 2002.

[13] M. Fellows, N. Koblitz, *Combinatorial cryptosystems galore!*, Contemporary Mathematics, 51-61, 1994.
[14] M. Gasca, T. Sauer, *Polynomial interpolation in several variables*, Adv. Comput. Math., 12 (4), 377–410, 2000.
[15] N. Koblitz, *Algebraiczne aspekty kryptografii*, WNT, Warszawa 2000.
[16] M. Mignotte, *How to share a secret* Cryptography. Springer Berlin Heidelberg, 371-375, 1983.
[17] P.J. Olver, *On multivariate interpolation*, Stud. Appl. Math. 116, 201-240, 2006.
[18] O. Ore, *The general Chinese remainder theorem*, American Mathematical Monthly, 59:365-370, 1952.
[19] T. Sauer, *Polynomial interpolation of minimal degree and Gröbner bases*, Groebner Bases and Applications (Proc. of the Conf. 33 Years of Groebner Bases), eds. B. Buchberger and F. Winkler, London Math. Soc. Lecture Notes, Vol. 251, 483–494 Cambridge University Press, 1998.
[20] A. Shamir, *How to share a secret*, Communications of the ACM 22 (11): 612613, 1979.
[21] T. Tassa, N. Dyn, *Multipartite Secret Sharing by Bivariate Interpolation*, ICALP (2), 288-299, 2006.

UWAGI NA TEMAT WIELOWYMIAROWYCH ROZSZERZEŃ SCHEMATÓW PODZIAŁU SEKRETU OPARTYCH NA WIELOMIANACH

Streszczenie. Wprowadzamy metody wykorzystujące bazy Gröbnera do schematów podziału sekretu. Opis bazuje na wielomianach z pierścienia $R = K[X_1, ..., X_l]$, gdzie tożsamości użytkowników oraz ich udziały są lub są związane z ideałami w R. Główne teoretyczne rezultaty dotyczą algorytmicznej rekonstrukcji wielomianu wielu zmiennych z takich udziałów zgodnie z zadaną (dowolną) strukturą dostępu, co stanowi uogólnienie klasycznych schematów progowych. W pracy wykorzystujemy konstruktywną wersję Chińskiego twierdzenia o resztach w pierścieniu R pochodzącą od Beckera i Weispfenninga. Wprowadzone idee znajdują swój szczegółowy opis w naszych związanych z tym tematem pracach.
Słowa kluczowe: bazy Gröbnera, twierdzenie chińskie o resztach, schemat podziału sekretu, struktura dostępu, wielowymiarowa interpolacja.