Appl. Numer. Math. 208 (2025) 317–339

Contents lists available at ScienceDirect

Applied Numerical Mathematics

journal homepage: www.elsevier.com/locate/apnum

Research Paper

Structured ramp secret sharing schemata over rings of real polynomials

Gerasimos C. Meletiou [a], Nikolaos K. Papadakis [b], Dimitrios S. Triantafyllou [b,*], Michael N. Vrahatis [c]

[a] University of Ioannina, School of Agriculture, GR-47100 Arta, Greece
[b] Department of Mathematics and Engineering Sciences, Hellenic Military Academy, GR-16673 Vari, Greece
[c] Computational Intelligence Laboratory (CILab), Department of Mathematics, University of Patras, GR-26110 Patras, Greece

ARTICLE INFO

MSC:
65F05
65F50
94A60
94A62

Keywords:
Ramp secret sharing schemes
Hierarchical schemata
Greatest common divisor of polynomials
Matrix factorization
Error analysis

ABSTRACT

Two new ramp secret sharing schemata based on polynomials are proposed. For both schemata, the secret is considered to be a polynomial created by the dealer. The participants are separated into $\ell \geqslant 2$, groups, that are specified by the dealer's levels L_i for $i = 1, 2, \ldots, \ell$ and each level L_i, $i \geqslant 2$, is separated into subsets. The shares of the secret are given to participants in the form of polynomials. For the first proposed scheme, the dealer creates ℓ polynomials one for each level. Specific participants from every subset of each level have to cooperate all together in order to construct the polynomial of their level. Next all the authorized participants cooperate for computing the greatest common divisor of the polynomials in order to retrieve the secret. In the second scheme, the authorized participants cooperate per two levels using a bottom-up procedure. In both schemata the greatest common divisor can be evaluated by implementing numerical linear algebra methods, and precisely factorization of matrices of special form such as Sylvester matrices. The triangularization of these matrices can be obtained by exploiting their special structure for the reduction of the required floating point operations. The innovative idea of the paper at hand is the use of real polynomials in secret sharing schemata. This is particularly useful since the greatest common divisor can always be computed with efficient accuracy using effective numerical methods. New theoretical results are proved and provided that support the error analysis of our approach.

1. Introduction

The concepts of *threshold secret sharing scheme* and the *ramp threshold secret sharing scheme* are, in general, described as follows. A (τ, ν) threshold secret sharing scheme is a method of distributing secret information, called *shares* to ν players, in such a way that any τ of the ν players can compute a *secret*, but no subset of ξ, for $\xi < \tau$, players can determine any information about the secret. The integer τ is called *threshold* that we assume to be $1 \leqslant \tau \leqslant \nu$. For details and a discussion on historical issues, we refer the interested reader to Blakley [3], Shamir [24] and Stinson [26].

In general, a (λ, α, ν)-*ramp threshold secret sharing scheme*, where λ, α and ν are positive integers such that $\lambda < \alpha \leqslant \nu$ is a cryptographic structure whereby a dealer distributes a share to each of ν players such that the following two properties are satisfied:

* Corresponding author.
E-mail addresses: gmelet@uoi.gr (G.C. Meletiou), npapadakis@sse.gr (N.K. Papadakis), dtriant@sse.gr (D.S. Triantafyllou), vrahatis@upatras.gr (M.N. Vrahatis).

https://doi.org/10.1016/j.apnum.2024.06.003
Received 1 November 2023; Received in revised form 2 June 2024; Accepted 3 June 2024

Available online 7 June 2024
0168-9274/© 2024 IMACS. Published by Elsevier B.V. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

a) *Reconstruction*: Any subset of κ players with $\kappa \geqslant \alpha$ can compute the secret from the shares that they hold collectively.
b) *Secrecy*: No subset of μ players with $\mu \leqslant \lambda$ can determine any information about the secret.

We use λ and α to denote the *lower* and *upper thresholds* of the scheme, respectively. It is evident that a (λ, α, ν) ramp scheme is a generalization of a threshold scheme in which there are two thresholds. A $(\tau - 1, \tau, \nu)$ ramp scheme is exactly a (τ, ν) threshold secret sharing scheme. The ramp schemata have been proposed by Blakley and Meadows [4] (for additional details, we refer the interested reader to Stinson [27,28]).

Polynomial factorization as well as factorization in general is considered to be a hard task. It is well-known that RSA is based on the difficulty of factoring integers. Concerning polynomial factorization the difficulty depends on the field from which the coefficients of the polynomial emanate. In a relatively recent approach proposed in Meletiou et al. [16], a ramp secret sharing scheme through *Greatest Common Divisor* (GCD) of polynomials has been presented. In that approach the shares are polynomials and the secret is a polynomial derived from the shares through multiplications and GCD computations.

In the paper at hand, two new ramp schemata are presented, where the polynomials are the shares while their GCD determine the secret. Since the GCD-*secret* is always a divisor of every share, the schemata are considered to be ramp ones. The novelty of the proposed schemata is that the corresponding secrets and shares are elements from the polynomial ring $\mathbb{R}[x]$. It is worth mentioning that, the ring of real polynomials of one variable $\mathbb{R}[x]$, is a unique factorization domain in the sense that every real polynomial can always be factorized in a unique way to a product of irreducible components, that is to say to linear polynomials and to quadratic ones with real coefficients and complex roots. Given a real polynomial $f(x)$ we can always factorize it to irreducible components by suitable numerical methods in polynomial time. In addition, for the case of polynomials over other fields a global optimization approach for determining the greatest common divisor is pointed out.

The rest of the paper is organized as follows. In Section 2 the required mathematical material is summarized. In Section 3 two new hierarchical (in the sense given in Remark 1 and Remark 10) ramp secret sharing schemata are presented and analyzed. In addition new theoretical results are proved and provided that support the error analysis of our approach. In Section 4 analytic examples illustrate the two proposed ramp schemata. The paper ends in Section 5 with conclusions and future research directions.

2. Background material

In order to retrieve the secret, the participants have to cooperate revealing their shares and compute the GCD of polynomials. The proposed schemata are ramp ones, since the participants can compute the roots of the polynomials of the corresponding levels described in Section 3 having a partial information about the secret. The choice of the method for computing the GCD of the polynomials depends on the particular polynomial field.

2.1. Real polynomials

Let $\mathbb{R}[x]$ be the ring of polynomials with real coefficients. In the following paragraphs, two algorithms for computing the GCD of polynomials are presented. A distinction can be made regarding the algorithm following the number of polynomials involved.

i) Case of two polynomials
Consider the following two polynomials $a(x), b(x) \in \mathbb{R}[x]$:

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0,$$

and

$$b(x) = b_p x^p + b_{p-1} x^{p-1} + b_{p-2} x^{p-2} + \cdots + b_1 x + b_0,$$

with degrees n and p respectively, where $p \leqslant n$. Then the $(n+p) \times (n+p)$ *Sylvester matrix* (*cf.* [1]), denoted by $S(a,b)$, of these polynomials can be defined as follows:

$$S(a,b) = \begin{bmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & \cdots & a_1 & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_1 & a_0 & 0 \\ 0 & \cdots & 0 & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_1 & a_0 \\ b_p & b_{p-1} & b_{p-2} & \cdots & b_0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & b_p & b_{p-1} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & b_p & b_{p-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & b_p & b_{p-1} & \cdots & b_1 & b_0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & b_p & b_{p-1} & \cdots & b_1 & b_0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & b_p & b_{p-1} & \cdots & b_1 & b_0 \end{bmatrix}. \tag{1}$$

Suppose that $S(a,b) = LU$ and $S(a,b) = QR$ are, respectively, the LU and QR factorization of the Sylvester matrix $S(a,b)$ (see, *e.g.* [1,30]) of the above polynomials $a(x)$ and $b(x)$, then the last non vanishing row of the upper triangular matrix U of LU or of the matrix R of QR provides the coefficients of the *greatest common divisor* $\gcd\{a(x), b(x)\}$ (*cf.* [1,15,30]). Since the Sylvester matrix has a special form, a modification of LU or QR factorization that have been presented by Triantafyllou and Mitrouli in [30] can be implemented in order to decrease the required floating point operations.

ii) Case of several polynomials
Consider the following polynomial $a(x) \in \mathbb{R}[x]$:

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0,$$

of degree n, and the following m polynomials $b_i(x) \in \mathbb{R}[x]$:

$$b_i(x) = b_{i,k}\, x^k + b_{i,k-1}\, x^{k-1} + \cdots + b_{i,1} x + b_{i,0}, \quad i = 1, 2, \ldots, m,$$

of maximal degree p with $p \leqslant n$, then the $(mn + p) \times (n + p)$ *generalized Sylvester matrix* of the polynomials $f(x)$ and $p_i(x)$ for $i = 1, 2, \ldots, m$ is defined as follows (*cf.* [1]):

$$S = \begin{bmatrix} [\widetilde{S}_0] \\ [\widetilde{S}_1] \\ \vdots \\ [\widetilde{S}_m] \end{bmatrix}, \tag{2}$$

where the $p \times (n + p)$ matrix $\widetilde{S}_0$ is given as follows:

$$\widetilde{S}_0 = \begin{bmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & \ldots & 0 \\ 0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & a_n & a_{n-1} & \ldots & a_1 & a_0 \end{bmatrix}, \tag{3}$$

while the $n \times (n + p)$ matrices $\widetilde{S}_i$ for $i = 1, 2, \ldots, m$ are given by:

$$\widetilde{S}_i = \begin{bmatrix} b_{i,p} & b_{i,p-1} & b_{i,p-2} & \ldots & b_{i,0} & 0 & \ldots & 0 \\ 0 & b_{i,p} & b_{i,p-1} & \ldots & b_{i,1} & b_{i,0} & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & b_{i,p} & b_{i,p-1} & \ldots & b_{i,1} & b_{i,0} \end{bmatrix}. \tag{4}$$

Assume that $S = LU$ and $S = QR$ are respectively the LU and QR factorization of the generalized Sylvester matrix S. Then, similarly to the previous case of two polynomials, the last non vanishing row of the upper triangular matrix U of LU or of the matrix R of QR provides the coefficients of the $\gcd\{a(x), b_1(x), \ldots, b_m(x)\}$ (*cf.* [1]).
Since the Sylvester matrix has a special structure, the modification of LU or QR factorization that have been presented by Triantafyllou and Mitrouli in [31] is applied here in order to decrease significantly the required floating point operations for triangularizing the Sylvester matrix.

2.2. Polynomials over other fields

It is worth mentioning that, in general, the cryptographic schemes, including ramp ones, are based on finite fields and discrete structures. At the paper at hand polynomials over the real ring are used. On the other hand it would be interesting to study the cases of elaborating with polynomials over other fields including among others finite fields (see, *e.g.* [26,28]). Specifically, for the proposed schemata the secrets, the shares and in general the cryptographic objects are polynomials from a polynomial ring $\mathbb{F}[x]$, where $\mathbb{F}$ is a suitable field. In that sense the choice of the field is crucial. Also, efficient methods for the GCD computation are of great importance. It is worth mentioning that, concerning the real field, for $a, b \in \mathbb{R}$ the equation $a^2 + b^2 = 0$ implies $a = b = 0$. Therefore, the $\gcd\{f(x), g(x)\}$ can be equivalently obtained by solving, among others, one of the following equations:

a) $f^2(x) + g^2(x) = 0$,
b) $|f(x)| + |g(x)| = 0$,
c) $\max\{|f(x)|, |g(x)|\} = 0$.

For solving the above equations, the corresponding global minimizers can be obtained using computational intelligence and intelligent optimization methods, including particle swarm optimization, differential evolution, memetic algorithms, among others (see, *e.g.* [6,8,20,21,23,29,32]). These methods are capable of handling non-differentiable, discontinuous, noisy and multimodal objective functions and in general they have gained increasing popularity in recent years due to their relative simplicity and their ability to

efficiently and effectively tackle several real-world applications. It is worth noting that the problem of factorization of polynomials over finite fields has been studied extensively. For these issues we refer the interested reader to [2,5,11,17,25].

In a future correspondence we intend to study the applicability of the proposed schemata of the paper at hand over other fields and discrete structure. As well as we intend to analyze the applicability, effectiveness and efficiency of the above mentioned computational intelligence and intelligent optimization methods for tackling the issues and aspects raised above.

3. Ramp secret sharing schemata

In this section we present two new ramp secret sharing schemata with a hierarchy defined later. An entity named *dealer* manages the whole procedure as follows: The dealer creates a polynomial $p(x)$ with several real roots. The *secret* is formed by the polynomial $p(x)$. The dealer constructs $\ell \geqslant 2$ *levels* L_i for $i = 1, 2, \ldots, \ell$. Each *level* L_i, $i \geqslant 2$, consists of *subsets* and the dealer separates the *participants* into these subsets. At each level the number of participants is the same across all subsets. The *shares* of the secret are given by the dealer to every participant in the form of specific polynomials. Note that the dealer must take into consideration that the subsets are mutually exclusive. Thus, a participant cannot own multiple shares of the secret and also is not able to appear on multiple levels.

In general, in ramp schemata there is a trade-off between security and efficiency (*i.e.* storage). Efficiency in terms of the information ratio can be gained by allowing partial information related to the secret which is composed of several sub-secrets to leak out. Of course, in this case, the main disadvantage is the existence of sets of participants with partial information related to the secret.

3.1. Scheme 1: Hierarchical ramp secret sharing

For this scheme the dealer creates a polynomial $p(x)$ with several real roots which determine the secret and $\ell \geqslant 2$ hierarchical levels of participants and shares to the participants of each level polynomials. The authorized groups of participants have to share their parts, construct polynomials and compute their GCD.

Remark 1. The dealer determines the *hierarchy* of the levels by defining:

a) a number of levels,
b) a number of participants associated to each level and
c) a number of participants that have to cooperate at each level.

Notation 1. The levels defined by the dealer have the following form:

$$\text{Level } 1: L_1 = \left\{P_1^{(1)}, P_2^{(1)}, \ldots, P_{r_1}^{(1)}\right\}, \quad |L_1| = r_1 > 1,$$

$$\text{Level } i: \ L_i = \left\{S_1^{(i)}, S_2^{(i)}, \ldots, S_{c_i}^{(i)}\right\}, \quad |L_i| = r_i > r_{i-1}, \ i > 1,$$

where:

a) $S_j^{(i)} = \left\{P_{1j}^{(i)}, P_{2j}^{(i)}, \ldots, P_{k_i j}^{(i)}\right\}$,
b) i is the serial (index) number of the level, $i = 1, 2, \ldots, \ell$,
c) j is the serial number of the subset of the i-th level, $j = 1, 2, \ldots, c_i$,
d) k_i is the number of participants in subset $S_j^{(i)}$,
e) c_i is the number of subsets of the i-th level, with $c_1 = 1$,
f) L_i is a $k_i \times c_i$ table, and
g) $r_i = k_i c_i$ denotes the total number of participants of level L_i for $i = 2, 3, \ldots, \ell$.

Notation 2. Throughout the paper the symbol L indicates levels, P indicates participants while p indicates polynomials.

Scheme 1. The proposed *ramp hierarchical secret sharing scheme* is described below using the following steps:

Step 1: The dealer constructs a polynomial $p(x)$ which determines the secret.
Step 2: The dealer creates the hierarchically structured set

$$L = \left\{L_1, L_2, \ldots, L_\ell\right\},$$

that constitutes a partitioning of the participants into ℓ hierarchically structured levels L_i, $i = 1, 2, \ldots, \ell$. Every L_i has c_i subsets of participants with $c_1 < c_2 < \cdots < c_\ell$ where $\ell \geqslant 2$, (*cf.* Notation 1).
Step 3: The dealer provides different polynomials to all participants of Level 1. In what follows, the dealer shares a polynomial $p_{hk}^{(i)}(x)$ to every participant $P_{hk}^{(i)}$ at Level i for $i = 2, \ldots, \ell$, in such a way that

$$p_i(x) = \sum_{k=1}^{c_i} p_{hk}^{(i)}(x)\ ,\ h \in \{1,2,\dots,k_i\},\ i \in \{2,3,\dots,\ell\},$$

and for any h, k and i

$$\gcd\left\{p_{hk}^{(i)}(x), p(x)\right\} = 1,$$

and for any i

$$\gcd\left\{p_i(x), p(x)\right\} \neq 1,$$

where $p_i(x)$ denotes the corresponding polynomial of Level i and $p_j^{(1)}(x)$ denotes the polynomial of the j-th participant of Level 1.

The dealer distributes the shares such that, if the j-th participant of all the subsets of the Level i cooperates by adding their polynomials they are able to obtain the polynomial $p_i(x)$, for $i = 2,3,\dots,\ell$. For security purposes see regarding the choice of polynomials Remarks 3 and 7.

Step 4: From every Level i for $i = 2,3,\dots,\ell$ one specific participant is selected, *e.g.* the q-th, named $P_{qj}^{(i)}$ from every subset $S_j^{(i)} = \left\{P_{1j}^{(i)}, P_{2j}^{(i)}, \dots, P_{k_ij}^{(i)}\right\}$, $q \in \{1,2,\dots,k_i\}$ such that

$$p_i(x) = \sum_{k=1}^{c_i} p_{qk}^{(i)}(x).$$

Step 5: The participants that are selected by the dealer at each Level i share their polynomials $p_i(x),\ i = 2,3,\dots,\ell$ with the polynomial of a participant from Level 1, say the q-th one, denoted by $p_q^{(1)}$. Next, all of them compute the secret given by the polynomial $p(x)$ as follows:

$$\gcd\left\{p_q^{(1)}(x), p_2(x), p_3(x), \dots, p_\ell(x)\right\} = p(x).$$

Remark 2. In the above steps we use the notation $p_j^{(1)}(x)$ only for the polynomials of the participants of Level 1, while for the rest levels we use the notation $p_i(x)$ that corresponds to the polynomial of Level i, obtained by manipulations between the polynomials of the participants at Level i, for $i = 2,3,\dots,\ell$.

In Table 1 the main steps of Scheme 1 are exhibited. The secret can be obtained by the $\gcd\left\{p_i^{(1)}(x), p_2(x), \dots, p_\ell(x)\right\}$ for any polynomial $p_i^{(1)}(x)$ where $i \in \{1,2,\dots,k_1\}$. The polynomials $p_2(x),\dots,p_\ell(x)$ at each level are obtained if all the participants with the same color at each level add their polynomials.

Remark 3. The authorized participants of the subsets of a level $L_i,\ i = 1,2,\dots,\ell$ can obtain the roots of the polynomial $p_i(x)$ of that level. Some of them constitute the secret but the number of computed roots is much larger than the number of the roots of the secret. The participants do not know which of them constitute the secret. The number of all combinations is so large that they are not able to retrieve the secret in a reasonable computing time.

Remark 4. The root-finding computation complexity of a polynomial of degree n, that has been presented in [19] is of order $O\left(n^{12} + n^9\ (\log|p|)^3\right)$. It is clear that the dealer should choose polynomials of higher degrees as shares for the participants, as they require greater computational effort in the root-finding process. This leads to an overall increased computational effort at each level.

Next, we present some observations that can be considered and used as variants of the proposed schemata. In a future correspondence we intend to analyze rigorously the impact of these variants on the proposed schemata.

Remark 5. It is worth noting that, in order to increase the security of the proposed Scheme 1, the dealer can introduce an *inner tolerance* $\mathrm{tol} > 0$, such that any entry with absolute value less than tol will be zeroed with immediate effect on the numerical computation of the GCD of polynomials. Different tolerances lead to different ranks of the generalized Sylvester matrix leading to different degrees of GCD (see Example 2 in [30], [18]). In the final step the dealer informs the participant of Level 1 about the inner tolerance for the correct GCD to be computed. It is worth mentioning here that the tolerance issue plays a remarkable role since it can increase significantly the security of the scheme.

Remark 6. For non-integer real roots, participants may lack awareness regarding the precision of each computed root. To address this, the dealer can introduce a secondary tolerance linked to the number of significant digits associated with the roots. Furthermore, the dealer has the option to complicate the computational process of root finding at a specific level L_i by introducing a secret having initially multiple roots and finally selecting a secret with altered discrete roots by slightly perturbing the initial ones. This results in heightened difficulty in the root-finding process at a specific level when employing conventional tools such as Newton-Raphson for

Table 1
Exhibition of the main steps of Scheme 1. The secret can be obtained by the gcd $\{p_i^{(1)}(x), p_2(x), \ldots, p_\ell(x)\}$ for any $p_i^{(1)}(x)$, $i \in \{1, 2, \ldots, k_1\}$. The polynomials $p_2(x), \ldots, p_\ell(x)$ at each level are obtained if all the participants with the same color at each level add their polynomials.

L_1			
$P_1^{(1)} \to p_1^{(1)}(x)$	$P_2^{(1)} \to p_2^{(1)}(x)$	…	$P_{k_1}^{(1)} \to p_{k_1}^{(1)}(x)$

L_2				
$S_1^{(2)}$	$S_2^{(2)}$	…	$S_{c_2}^{(2)}$	
$P_{11}^{(2)}$	$P_{21}^{(2)}$	…	$P_{c_2 1}^{(2)}$	$\xrightarrow{(+)} p_2(x)$
$P_{12}^{(2)}$	$P_{22}^{(2)}$	…	$P_{c_2 2}^{(2)}$	$\xrightarrow{(+)} p_2(x)$
⋮	⋮	⋮	⋮	⋮
$P_{1k_2}^{(2)}$	$P_{2k_2}^{(2)}$	…	$P_{c_2 k_2}^{(2)}$	$\xrightarrow{(+)} p_2(x)$

⋮

L_ℓ				
$S_1^{(\ell)}$	$S_2^{(\ell)}$	…	$S_{c_\ell}^{(\ell)}$	
$P_{11}^{(\ell)}$	$P_{21}^{(\ell)}$	…	$P_{c_\ell 1}^{(\ell)}$	$\xrightarrow{(+)} p_\ell(x)$
$P_{12}^{(\ell)}$	$P_{22}^{(\ell)}$	…	$P_{c_\ell 2}^{(\ell)}$	$\xrightarrow{(+)} p_\ell(x)$
⋮	⋮	⋮	⋮	⋮
$P_{1k_\ell}^{(\ell)}$	$P_{2k_\ell}^{(\ell)}$	…	$P_{c_\ell k_\ell}^{(\ell)}$	$\xrightarrow{(+)} p_\ell(x)$

root determination. For instance, let us suppose that the dealer has selected as an initial secret the polynomial $p(x) = x^2$ having a double root at point zero. Perturbing the secret as $\widehat{p}(x) = x^2 + \varepsilon$, then:

a) for $\varepsilon > 0$, the participants will compute two conjugated complex roots,
b) for $\varepsilon < 0$, the participants will compute two real simple discrete roots.

Due to the proximity of the roots, described by Runge's phenomenon [22] and Faber's theorem [10], the authorized participants at a specific level may lack certainty in confirming that they have computed the entire set of roots.

Remark 7. The dealer can multiply the share of each participant by a common polynomial $f(x)$ of high degree with additional roots that are not related to the secret. In this case, if the authorized participants of a certain level compute all the roots of their polynomial the total number of computed roots will be significantly increased, thus resulting to an increased number of root combinations in a potential adversary attack. This is so because the dealer is in a position to give a few common roots to the participants of different levels that are related to the secret but in the same time to give also several common roots that are not related to the secret. At the final step, the dealer informs the participant of Level 1 about the polynomial $f(x)$ that contains the common roots that are not related to the secret. It is worth noting here that if there are many common roots that are not related to the secret, this obviously increases significantly the security of the scheme.

3.1.1. Analyzing Scheme 1

For the computation of the polynomial $p(x)$, one participant from Level 1 is required. Thus, Level 1 is the most significant one in the sense that only one participant of Level 1 is required to cooperate with participants of the lower levels. Indeed, the participants of the i-th Level, $i = 2, 3, \ldots, \ell$ have to cooperate with other participants of the same level in order to compute the corresponding polynomial to that level.

In the i-th Level, there are c_i subsets $S_j^{(i)} = \{P_{1j}^{(i)}, P_{2j}^{(i)}, \ldots, P_{k_i j}^{(i)}\}$ of participants. From every $S_j^{(i)}$, $j = 1, 2, \ldots, c_i$, one participant has to participate. Assume that the participant is the q-th one. Thus, from the first subset of Level i, the $P_{q1}^{(i)}$ participant cooperates with the participant $P_{q2}^{(i)}$ of the second subset of Level i and finally with the q-th participant $P_{qk_i}^{(i)}$ of the last subset of Level i. Then they have to sum their polynomials in order to compute the polynomial of Level i and this should be done for every $i = 2, \ldots, \ell$. Finally, all these participants cooperate with the corresponding one of Level 1 and compute the GCD of their polynomials in order to retrieve the secret $p(x)$.

3.1.2. Error analysis of Scheme 1

Assume that $x \in \mathbb{R}$ and $fl(x) = \hat{x}$ are the corresponding number of x in the floating point arithmetic that is used. Thus, $\hat{x} = x(1+\varepsilon)$, $|\varepsilon| \leqslant u$, where $u = \frac{1}{2}\beta^{1-t}$ is the unit round off, β and t are the base and the number of the significant digits of the used floating point arithmetic. For instance, in IEEE754 of double precision, $\beta = 2$ and $t = 53$, thus $u = \frac{1}{2} \times 2^{1-53}$ (see *e.g.* [14]). This means that $1 + \frac{1}{2} \times 2^{1-53} = 1$, while $1 + 2^{1-53} > 1$ in any machine that uses the floating point arithmetic IEEE754 of double precision.

Suppose that all the coefficients of the polynomials are floating point numbers, thus there is no error in representing a real number as a floating point one. More details related to the errors during numerical computations and matrix factorization through orthogonal transformations can be found in [9,13,33]. Using the algorithm presented by Triantafyllou and Mitrouli in [31] for computing the GCD of several polynomials and the classical bound of the norm of the error concerning the QR factorization of a matrix [9,12,7], we extend the error analysis and propose and prove the new Lemma 1 related to the intermediate stages of iteratively applications of the QR factorization in specific blocks of the modified generalized Sylvester matrix. To this end, for completeness purposes we recall the definition of the *modified generalized Sylvester matrix* (*cf.* [31]). Let $p_i(x)$, $i = 1, 2, \ldots, \ell$ be the ℓ polynomials corresponding to the ℓ levels, with

$$p_i(x) = p_{i,n}x^n + p_{i,n-1}x^{n-1} + \cdots + p_{i,1}x + p_{i,0}, \quad i = 1, 2, \ldots, \ell - 1, \tag{5}$$

and

$$p_\ell(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,$$

where m, n are the largest and the second larger degree of those polynomials, $n \leqslant m$. For simplicity and without loss of generality we assumed that the polynomial of maximum degree m is the ℓ-th one and thus $\widetilde{S}_0$ corresponds to $p_\ell(x)$.

Definition 1. *The $(\ell - 1) \times (n + 1)$ matrix B_0 is formed by the coefficients of the polynomials of the Eq. (5) as follows:*

$$B_0 = \begin{bmatrix} p_{1,n} & p_{1,n-1} & p_{1,n-2} & \cdots & p_{1,0} \\ p_{2,n} & p_{2,n-1} & p_{2,n-2} & \cdots & p_{2,0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{\ell-1,n} & p_{\ell-1,n-1} & p_{\ell-1,n-2} & \cdots & p_{\ell-1,0} \end{bmatrix}. \tag{6}$$

Similarly, by selecting the second rows from every block $\widetilde{S}_i$, $i = 1, 2, \ldots, \ell - 1$ of the generalized Sylvester matrix S of Eq. (2) the block matrix $\big[[\theta][B_0]\big]$ is constructed, where θ is a column vector with zero entries that their number coincides with the number of rows of the matrix B_0. Next, by selecting the third rows from every block $\widetilde{S}_i$, $i = 1, 2, \ldots, \ell - 1$ of the generalized Sylvester matrix S, the block matrix $\big[[\theta]\big[[\theta][B_0]\big]\big]$ is constructed and this procedure is continued until the last row of every block $\widetilde{S}_i$, $i = 1, 2, \ldots, \ell - 1$ has been taken into account. Thus, the *modified Sylvester matrix* obtains the following form:

$$S^* = \begin{bmatrix} [B_0][\theta][\theta][\theta] & \ldots & [\theta][\theta] \\ [\theta][B_0][\theta][\theta] & \ldots & [\theta][\theta] \\ [\theta][\theta][B_0][\theta] & \ldots & [\theta][\theta] \\ & \ddots & \\ [\theta][\theta][\theta][\theta] & \ldots & [B_0][\theta] \\ [\theta][\theta][\theta][\theta] & \ldots & [\theta][B_0] \\ & [\widetilde{S}_0] & \end{bmatrix}. \tag{7}$$

Notice that the above modified generalized Sylvester matrix has m same $(\ell - 1) \times (n + 1)$ blocks, that are right shifted one column each time.

Notation 3. For any two matrices X and Y, we denote the following blockwise matrix by $B_S(X, Y, \theta)$:

$$B_S(X, Y, \theta) = \begin{bmatrix} [X][\theta][\theta][\theta] & \ldots & [\theta][\theta] \\ [\theta][X][\theta][\theta] & \ldots & [\theta][\theta] \\ [\theta][\theta][X][\theta] & \ldots & [\theta][\theta] \\ & \ddots & \\ [\theta][\theta][\theta][\theta] & \ldots & [X][\theta] \\ [\theta][\theta][\theta][\theta] & \ldots & [\theta][X] \\ & [Y] & \end{bmatrix}, \tag{8}$$

where θ denotes the column vector with zero entries that their number coincides with the number of rows of the matrix X, can be used to form *modified Sylvester matrices*. For example the matrix S^* given in Relation (7) can be written as follows:

$$S^* = B_S(B_0, \widetilde{S}_0, \theta). \tag{9}$$

Notation 4. The following block matrix will be frequently used:

$$B_B(X,\Theta)=\begin{bmatrix}[X][\Theta]\\ [\Theta][X]\end{bmatrix}, \tag{10}$$

where Θ is a zero matrix with the same rows of X and different columns.

In order to efficiently compute the QR factorization of S^*, starting from the matrix B_0 of Eq. (6) we define the blocks R_i, B_i as follows:

Definition 2. *Let Q_i, R_i be the result of the QR factorization of the matrix B_i, $i=0,1,\ldots,k-1$ that can be written as $Q_iR_i \leftarrow B_i$. Then the B_{i+1} is defined as follows:*

$$B_{i+1}=B_B\big(R_i,\Theta\big),\quad i=0,1,\ldots,k-2, \tag{11}$$

where R_i is the upper triangular matrix of the QR factorization of B_i. The rows of B_{i+1} are two times the rows of B_i while its columns are increased by 2^i. The matrix B_0 is defined in Eq. (6).

Remark 8. In the rest of the paper by $\varphi(x,y)$ we denote a slowly growing function of x, y as it is described by $\varphi(x)$ in [7]. It is worth noting that, according to [7], in the case where $x\neq y$ the roundoff property is the same as in the case where $x=y$. In addition, the QR factorization of a nonsquare matrix using Housholder transformations is stable (*cf.* [7]). Note that the bound on the numerical error of the QR factorization of any $m\times n$ matrix A can be found in [13, p. 360] or equivalently in [7, p. 145]. Precisely, if A is an $m\times n$ matrix then the QR factorization of A is the exact factorization of a slightly perturbed matrix $A+\Delta A$ such that $A+\Delta A=QR$, where Q is an $m\times m$ orthogonal matrix and R is an upper triangular $m\times n$ matrix. The Frobenius norm of the error ΔA is bounded by $\|\Delta A\|_F\leqslant\tilde{\gamma}_{mn}\|A\|_F$ (*cf.* [13, p. 68 and p. 360]) or equivalently by $\|\Delta A\|_F\leqslant\varphi(m,n)\,u\,\|A\|_F$ (*cf.* [7, p. 145]), where u is the unit round off error.

For clarification purposes, we give briefly present the main steps of the algorithm for computing the GCD of the polynomials of all levels that provides the secret:

a) construct the modified Sylvester matrix S^* of the polynomials,
b) triangularize S^* by applying iterative a blockwise QR factorization to the block matrices B_0 given by Eq. (6) and $B_i=B_B\big(R_{i-1},\Theta\big)$, $i=1,2,\ldots,k-1$ of S^*.

The last non-zero row of the final upper trapezoidal matrix gives the coefficients of the GCD of polynomials [1].

The triagularization of S^* is achieved through properly iterative applications of the QR factorization implemented to the blocks B_i. Note that the QR factorization at iteration i is applied by grouping the blocks from step $i-1$ so that it decreases the number of blocks while increasing the size of the blocks. Using the bounds mentioned in Remark 8, it is possible to derive a series of upper bounds (depending only on B_0) on the error of the QR factorizations of block matrices given by Eq. (11).

Next, a comprehensive and detailed proof of the new proposed Lemma 1 is provided.

Lemma 1. *Let S^* be the modified generalized Sylvester matrix of the polynomials $p_i(x)$, $i=1,2,\ldots,\ell$. The QR decompositions applied to the same blocks B_i, $i=0,1,\ldots,k-1$ given in Definition 2, in the intermediate stages of the triangularization of S^* is the exact QR factorization of small perturbed matrices $B_i+\Delta B_i$, where ΔB_i are small perturbation matrices, such that:*

$$B_i+\Delta B_i=Q_i\,R_i,\quad i=0,1,\ldots,k-1, \tag{12}$$

with

$$\big\|\Delta B_i\big\|_F\leqslant\varphi(m_i,n_i)2^{\sigma_i/2}\,(\ell-1)^{i/2}\,u\,\big\|B_0\big\|_F\quad\text{for}\quad\sigma_i=\sum_{j=0}^{i}j, \tag{13}$$

where $\varphi(m_i,n_i)$ is a slowly growing function of $m_i=2^i(\ell-1)$ and $n_i=n+2^i$ that respectively determine the rows and the columns of B_i at step i, u is the unit round off error and

$$k=\lceil\log_2 m\rceil+1 \tag{14}$$

determines the required number of the iterations of the QR factorization.

Proof. The procedure implements iteratively the QR factorization to the matrices B_i, $i=0,1,\ldots,k-1$. At the first iteration, the QR factorization is implemented on the first block B_0 of S^*. Let R_0 be the computed upper triangular or trapezoidal QR factor of the $(\ell-1)\times(n+1)$ matrix B_0 (*cf.* Eq. (6)) obtained by the Householder transformations. The corresponding QR decomposition is the exact factorization of the block B_0 perturbed by the matrix ΔB_0 such that:

$$B_0 + \Delta B_0 = Q_0 R_0, \quad \text{with} \quad \|\Delta B_0\|_F \leqslant \tilde{\gamma}_{m_0 n_0} \|B_0\|_F,$$

where the matrices B_0, R_0, ΔB_0 are of size $(\ell - 1) \times (n + 1)$, while the orthogonal matrix Q_0 is of size $(\ell - 1) \times (\ell - 1)$, with $\tilde{\gamma}_{mn} = m\tilde{\gamma}_n = cmnu/(1 - cnu)$, $\tilde{\gamma}_n = cnu/(1 - cnu)$ and c is a small integer constant whose value is unimportant [13, p. 68 and p. 360]. Thus, the matrix R_0 is written as follows:

$$R_0 = Q_0^\top (B_0 + \Delta B_0). \tag{15}$$

For simplicity, henceforth we will refer to the upper bound of the Frobenius norm of the error in the QR decomposition as follows (*cf.* [7, p. 145]):

$$\|\Delta B_0\|_F \leqslant \varphi(m_0, n_0)\, u \|B_0\|_F. \tag{16}$$

At the Iteration 2, the QR decomposition is applied to the $2(\ell - 1) \times (n + 2)$ block matrix:

$$B_1 = B_B(R_0, \theta) = \begin{bmatrix} [R_0][\theta] \\ [\theta][R_0] \end{bmatrix}. \tag{17}$$

The number of rows of B_1 is twice the rows of B_0, while the number of its columns is one more than those of B_0. Let R_1 be the computed upper triangular QR factor of B_1, obtained by the Householder transformations. Similarly, the corresponding QR decomposition is the exact factorization of a small perturbed block B_1 such as:

$$B_1 + \Delta B_1 = Q_1 R_1,$$

where $B_1, R_1, \Delta B_1$ are $2(\ell - 1) \times (n + 2)$ matrices, while the orthogonal matrix Q_1 is of size $2(\ell - 1) \times 2(\ell - 1)$, with

$$\|\Delta B_1\|_F \leqslant \varphi(m_1, n_1)\, u \|B_1\|_F,$$

where $m_1 = 2(\ell - 1)$ and $n_1 = n + 2$. Consequently, we obtain:

$$R_1 = Q_1^\top (B_1 + \Delta B_1). \tag{18}$$

The following term $\|\Delta B_1\|_F$ can be bounded as follows:

$$\begin{aligned}
\|\Delta B_1\|_F &\leqslant \varphi(m_1, n_1)\, u \|B_1\|_F = \varphi(m_1, n_1)\, u \left\| \begin{bmatrix} [R_0][\theta] \\ [\theta][R_0] \end{bmatrix} \right\|_F \\
&= \varphi(m_1, n_1)\, u \sqrt{2} \|R_0\|_F = \varphi(m_1, n_1)\, u \sqrt{2} \left\| Q_0^\top (B_0 + \Delta B_0) \right\|_F \\
&= \varphi(m_1, n_1)\, u \sqrt{2} \left\| Q_0^\top \right\|_F \|B_0 + \Delta B_0\|_F \\
&\leqslant \varphi(m_1, n_1)\, u \sqrt{2}\sqrt{\ell - 1} \left\| Q_0^\top \right\|_2 \|B_0 + \Delta B_0\|_F \\
&= \varphi(m_1, n_1)\, u \sqrt{2}\sqrt{\ell - 1} \|B_0 + \Delta B_0\|_F \\
&\leqslant \varphi(m_1, n_1) \sqrt{2}\sqrt{\ell - 1}\, u \left(\|B_0\|_F + \|\Delta B_0\|_F \right) \\
&\leqslant \varphi(m_1, n_1) \sqrt{2}\sqrt{\ell - 1}\, u \left(\|B_0\|_F + \varphi(m_0, n_0)\, u \|B_0\|_F \right) \\
&= \varphi(m_1, n_1) \sqrt{2}\sqrt{\ell - 1}\, u \|B_0\|_F + O\left(u^2\right) \\
&\simeq \varphi(m_1, n_1) \sqrt{2}\sqrt{\ell - 1}\, u \|B_0\|_F.
\end{aligned}$$

In the previous relations we have used that $\|A\|_F \leqslant \sqrt{r}\|A\|_2$, where r is the rank of matrix A, $\|A\|_2 = 1$ for an orthogonal matrix A and we have omitted the negligible term $O\left(u^2\right)$. In conclusion we have:

$$\|\Delta B_1\|_F \leqslant \varphi(m_1, n_1) \sqrt{2}\sqrt{\ell - 1}\, u \|B_0\|_F. \tag{19}$$

Next, the QR decomposition is applied to the $2^2(\ell - 1) \times (n + 2^2)$ matrix B_2:

$$B_2 = B_B(R_1, \Theta) \equiv \begin{bmatrix} [R_1][\theta][\theta] \\ [\theta][\theta][R_1] \end{bmatrix}, \tag{20}$$

where the number of rows of B_2 are twice the rows of B_1, while its columns are two more than those of B_1. Hence, $m_2 = 2^2(\ell - 1)$ and $n_2 = n + 2^2$. Assume that R_2 is the computed upper triangular QR factor of B_2, obtained by the Householder transformations, then the QR decomposition is the exact factorization of a small perturbed block B_2 such as:

$$B_2 + \Delta B_2 = Q_2 R_2,$$

where $B_2, R_2, \Delta B_2$ are $2^2(\ell-1) \times (n+2^2)$ matrices, while the orthogonal matrix Q_2 is of size $2^2(\ell-1) \times 2^2(\ell-1)$, with

$$\|\Delta B_2\|_F \leqslant \varphi(m_2, n_2)\, u\, \|B_2\|_F .$$

At this iteration the matrix R_2 is obtained as follows:

$$R_2 = Q_2^\top (B_2 + \Delta B_2). \tag{21}$$

The following term $\|\Delta B_2\|_F$ can be bounded as:

$$\begin{aligned}
\|\Delta B_2\|_F &\leqslant \varphi(m_2, n_2)\, u\, \|B_2\|_F = \varphi(m_2, n_2)\, u \left\| \begin{bmatrix} [R_1][\theta][\theta] \\ [\theta][\theta][R_1] \end{bmatrix} \right\|_F \\
&= \varphi(m_2, n_2)\, u \sqrt{2}\, \|R_1\|_F \\
&= \varphi(m_2, n_2)\, u \sqrt{2}\, \left\|Q_1^\top (B_1 + \Delta B_1)\right\|_F \\
&= \varphi(m_2, n_2)\, u \sqrt{2}\, \left\|Q_1^\top\right\|_F \|B_1 + \Delta B_1\|_F \\
&\leqslant \varphi(m_2, n_2)\, u \sqrt{2}\, \sqrt{2(\ell-1)}\, \left\|Q_1^\top\right\|_2 \|B_1 + \Delta B_1\|_F .
\end{aligned}$$

Since $\left\|Q_1^\top\right\|_2 = 1$ we equivalently obtain:

$$\begin{aligned}
\|\Delta B_2\|_F &\leqslant \varphi(m_2, n_2)\, u \sqrt{2}\, \sqrt{2(\ell-1)}\, \left(\|B_1\|_F + \|\Delta B_1\|_F\right) \\
&= \varphi(m_2, n_2) \sqrt{2}\, \sqrt{2(\ell-1)}\, u \left(\sqrt{2}\, \|R_0\|_F + \|\Delta B_1\|_F\right) \\
&\leqslant \varphi(m_2, n_2) \sqrt{2}\, \sqrt{2(\ell-1)}\, u \left(\sqrt{2}\, \|R_0\|_F + \varphi(m_1, n_1)\, u\, \|B_1\|_F\right) \\
&= \varphi(m_2, n_2)\, \sqrt{2}^2\, \sqrt{2(\ell-1)}\, u\, \|R_0\|_F + O\left(u^2\right) \\
&\simeq \varphi(m_2, n_2)\, \sqrt{2}^2\, \sqrt{2(\ell-1)}\, u\, \|R_0\|_F \\
&= \varphi(m_2, n_2)\, \sqrt{2}^2\, \sqrt{2(\ell-1)}\, u\, \left\|Q_0^\top (B_0 + \Delta B_0)\right\|_F .
\end{aligned}$$

From the above we can easily obtain the following:

$$\begin{aligned}
\|\Delta B_2\|_F &\leqslant \varphi(m_2, n_2)\, \sqrt{2}^2\, \sqrt{2(\ell-1)}\, \sqrt{\ell-1}\, u\, \|B_0\|_F + O\left(u^2\right) \\
&\simeq \varphi(m_2, n_2)\, \sqrt{2}^2\, \sqrt{2^1(\ell-1)^2}\, u\, \|B_0\|_F .
\end{aligned}$$

Finally we conclude that:

$$\|\Delta B_2\|_F \leqslant \varphi(m_2, n_2)\, \sqrt{2^{0+1+2}(\ell-1)^2}\, u\, \|B_0\|_F . \tag{22}$$

Assume that at the $(i-1)$-th iteration the matrix R_{i-1} is the computed upper triangular QR factor of B_{i-1}, obtained by the Householder transformations. Then the QR decomposition is the exact factorization of a small perturbed block B_{i-1} such as:

$$B_{i-1} + \Delta B_{i-1} = Q_{i-1} R_{i-1},$$

where $B_{i-1}, R_{i-1}, \Delta B_{i-1}$ are $2^{i-1}(\ell-1) \times (n+2^{i-1})$ matrices, while the orthogonal matrix Q_{i-1} is of size $2^{i-1}(\ell-1) \times 2^{i-1}(\ell-1)$, with

$$\|\Delta B_{i-1}\|_F \leqslant \varphi(m_{i-1}, n_{i-1})\, \sqrt{2}^{i-1}\, \sqrt{2^{\sigma_{i-2}}\, (\ell-1)^{i-1}}\, u\, \|B_0\|_F , \tag{23}$$

where $\sigma_{i-2} = \sum_{j=0}^{i-2} j$.

Next by using the notation given in Definition 2 the matrix B_i can be written as follows:

$$B_i = B_B\left(R_{i-1}, \Theta\right) = \begin{bmatrix} [R_{i-1}][\Theta] \\ [\Theta][R_{i-1}] \end{bmatrix}.$$

Thus, at the i-th iteration we obtain:

$$
\begin{aligned}
\|\Delta B_i\|_F &\leqslant \varphi(m_i,n_i)\,u\,\|B_i\|_F = \varphi(m_i,n_i)\,u\left\|\begin{bmatrix}[R_{i-1}][\Theta]\\ [\Theta][R_{i-1}]\end{bmatrix}\right\|_F\\
&= \varphi(m_i,n_i)\,u\,\sqrt{2}\,\|R_{i-1}\|_F\\
&= \varphi(m_i,n_i)\,u\,\sqrt{2}\,\left\|Q_{i-1}^{\top}(B_{i-1}+\Delta B_{i-1})\right\|_F\\
&= \varphi(m_i,n_i)\,u\,\sqrt{2}\,\left\|Q_{i-1}^{\top}\right\|_F\|B_{i-1}+\Delta B_{i-1}\|_F\\
&\leqslant \varphi(m_i,n_i)\,u\,\sqrt{2}\,\sqrt{2^{i-1}(\ell-1)}\left\|Q_{i-1}^{\top}\right\|_2\|B_{i-1}+\Delta B_{i-1}\|_F\\
&= \varphi(m_i,n_i)\,u\,\sqrt{2}\,\sqrt{2^{i-1}(\ell-1)}\|B_{i-1}+\Delta B_{i-1}\|_F\\
&\leqslant \varphi(m_i,n_i)\,u\,\sqrt{2}\sqrt{2^{i-1}(\ell-1)}\,\left(\|B_{i-1}\|_F+\|\Delta B_{i-1}\|_F\right).
\end{aligned}
$$

Equivalently we have:

$$
\begin{aligned}
\|\Delta B_i\|_F &\leqslant \varphi(m_i,n_i)\,\sqrt{2}\,\sqrt{2^{i-1}(\ell-1)}\,u\,\left(\sqrt{2}\|R_{i-2}\|_F+\|\Delta B_{i-1}\|_F\right)\\
&= \varphi(m_i,n_i)\,\sqrt{2}^2\,\sqrt{2^{i-1}(\ell-1)}\,u\|R_{i-2}\|_F+O\left(u^2\right)\\
&\simeq \varphi(m_i,n_i)\,\sqrt{2}^2\,\sqrt{2^{i-1}(\ell-1)}\,u\|R_{i-2}\|_F\\
&= \varphi(m_i,n_i)\,\sqrt{2}^2\,\sqrt{2^{i-1}}\,\sqrt{\ell-1}\,u\left\|Q_{i-2}^{\top}(B_{i-2}+\Delta B_{i-2})\right\|_F\\
&= \varphi(m_i,n_i)\,\sqrt{2}^2\,\sqrt{2^{i-1}}\,\sqrt{\ell-1}\,u\left\|Q_{i-2}^{\top}\right\|_F\|B_{i-2}+\Delta B_{i-2}\|_F\\
&\leqslant \varphi(m_i,n_i)\,\sqrt{2}^2\,\sqrt{2^{i-1}}\,u\sqrt{2^{i-2}(\ell-1)^2}\left(\|B_{i-2}\|_F+\|\Delta B_{i-2}\|_F\right)\\
&= \varphi(m_i,n_i)\,\sqrt{2}^2\,\sqrt{2^{(i-1)+(i-2)}}\,\sqrt{\ell-1}^2\,u\left(\|B_{i-2}\|_F+\|\Delta B_{i-2}\|_F\right).
\end{aligned}
$$

Using iteratively the previous approach and the notation $\sigma_{i-1}=\sum_{j=0}^{i-1} j$ we obtain:

$$
\begin{aligned}
\|\Delta B_i\|_F &\leqslant \varphi(m_i,n_i)\,\sqrt{2}^{i-1}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i-1}\,u\left(\|B_1\|_F+\|\Delta B_1\|_F\right)\\
&= \varphi(m_i,n_i)\,\sqrt{2}^{i-1}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i-1}\,u\left(\sqrt{2}\|R_0\|_F+\|\Delta B_1\|_F\right)\\
&= \varphi(m_i,n_i)\,\sqrt{2}^{i-1}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i-1}\,u\,\sqrt{2}\|R_0\|_F+O\left(u^2\right).
\end{aligned}
$$

Next by removing the negligible term $O\left(u^2\right)$ we have:

$$
\begin{aligned}
\|\Delta B_i\|_F &\lesssim \varphi(m_i,n_i)\,\sqrt{2}^{i-1}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i-1}\,u\,\sqrt{2}\|R_0\|_F\\
&= \varphi(m_i,n_i)\,\sqrt{2}^{i-1}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i-1}\,u\,\sqrt{2}\left\|Q_0^{\top}(B_0+\Delta B_0)\right\|_F\\
&= \varphi(m_i,n_i)\,\sqrt{2}^{i-1}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i-1}\,u\,\sqrt{2}\,\left\|Q_0^{\top}\right\|_F\|B_0+\Delta B_0\|_F\\
&\leqslant \varphi(m_i,n_i)\,\sqrt{2}^{i-1}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i-1}\,u\,\sqrt{2}\,\sqrt{\ell-1}\,\|B_0+\Delta B_0\|_F\\
&\leqslant \varphi(m_i,n_i)\,\sqrt{2}^{i}\,\sqrt{2^{\sigma_{i-1}}}\,\sqrt{\ell-1}^{i}\,u\left(\|B_0\|_F+\|\Delta B_0\|_F\right)\\
&= \varphi(m_i,n_i)\,\sqrt{2^{\sigma_i}}\,\sqrt{\ell-1}^{i}\,u\|B_0\|_F+O\left(u^2\right)\\
&\simeq \varphi(m_i,n_i)\,2^{\sigma_i/2}(\ell-1)^{i/2}\,u\|B_0\|_F,
\end{aligned}
$$

where the relation $\left\|Q_0^{\top}\right\|_F\leqslant\sqrt{\ell-1}\left\|Q_0^{\top}\right\|_2=\sqrt{\ell-1}$ is used. Thus, we conclude that:

$$
\|\Delta B_i\|_F\leqslant\varphi(m_i,n_i)2^{\sigma_i/2}(\ell-1)^{i/2}u\|B_0\|_F. \tag{24}
$$

Hence, by induction the above relation holds for any $i = 0, 1, \ldots, k-1$, where k determines the maximum number of iterations of the implementation of the QR factorization process.

The number k can be specified using the following procedure. For the i-th step the number of rows of the block B_i is doubled at each step and the number of its columns is increased by 2^{i-1}. Thus, the number of rows of B_i is $2^i(\ell-1)$ while the number of its columns is $n+2^i$. At any step during the procedure, if the number of the same blocks B_i is odd, the last one is moved under $\widetilde{S}_0$ in order to have even number of same blocks for implementing the next iteration. At the first step, there are m same blocks B_0. Since the rows are doubled, then at the second step there are $m/2$ same blocks B_1. In the case where m is odd the last same block is moved under $\widetilde{S}_0$. At the third step there are $m/2^2$ same blocks B_2 and so on. Assume that j is the number of implementations of QR factorization such that the number of the remaining same blocks is two. Note that, in case where the remaining same blocks are three, the last one is moved under $\widetilde{S}_0$. Thus, at the j-th step the remaining same blocks are always two. Hence, it holds that $m/2^j = 2$ which results to $j = \lceil \log_2 m \rceil - 1$ applications of the QR factorization to the blocks B_i. In addition, one more QR factorization is applied to the first block B_0 and one more is applied to the block $\widetilde{S}_0$ as well as to any other blocks that are moved below $\widetilde{S}_0$.

Hence, the maximum number of the required implementations of the QR factorization is given by (*cf.* [31]):

$$k = \lceil \log_2 m \rceil + 1.$$

Thus, the lemma is proved. □

Remark 9. The number of the same blocks in the modified generalized Sylvester matrix can be handled by the dealer as follows. Particularly, the dealer is in a position to design the scheme such that the number of the same blocks to be even at every step. Thus, it is not required for any block to be moved under $\widetilde{S}_0$. This can be done if the maximum degree m of polynomials and consequently the number of the same blocks is a power of two. In that way less computations are required and therefore a smaller number of errors regarding the floating point manipulations take place.

We now prove the stability of the iterative block QR decomposition of S^*. To this end we use the following notations.

Notation 5. The following block matrix will be frequently used in what follows:

$$B_Q(Q, I, \Theta, \widehat{\Theta}, \widetilde{\Theta}) = \begin{bmatrix} [Q] & [\Theta] & [\Theta] & [\Theta] & \ldots & [\Theta] & [\widetilde{\Theta}] \\ [\Theta] & [Q] & [\Theta] & [\Theta] & \ldots & [\Theta] & [\widetilde{\Theta}] \\ [\Theta] & [\Theta] & [Q] & [\Theta] & \ldots & [\Theta] & [\widetilde{\Theta}] \\ & & & \ddots & & & \\ [\Theta] & [\Theta] & [\Theta] & [\Theta] & \ldots & [Q] & [\widetilde{\Theta}] \\ [\widehat{\Theta}] & [\widehat{\Theta}] & [\widehat{\Theta}] & [\widehat{\Theta}] & \ldots & [\widehat{\Theta}] & [I] \end{bmatrix}, \tag{25}$$

where Q is a $\nu \times \nu$ orthogonal matrix derived here by the QR factorization square, Θ is a $\nu \times \nu$ zero matrix, I is a $\mu \times \mu$ identity matrix, $\widehat{\Theta}$ is a $\mu \times \nu$ zero matrix while $\widetilde{\Theta}$ is a $\nu \times \mu$ zero matrix.

Definition 3. *We define the following* perturbation block matrix ΔE_i*:*

$$\Delta E_i = \begin{bmatrix} [\Delta B_i][\widetilde{\Theta}_i][\theta] & \ldots & [\theta][\Theta_i] \\ [\widetilde{\Theta}_i][\Delta B_i][\theta] & \ldots & [\theta][\Theta_i] \\ & \ddots & \\ [\theta][\theta] \ \ldots \ [\theta] & \ldots & [\theta][\Delta B_i] \\ & [\Theta] & \end{bmatrix}, \quad i = 0, 1, \ldots, k-1, \tag{26}$$

where ΔB_i is the $2^i(\ell-1) \times (n+2^i)$ that it has been used in Lemma 1, Θ_i is a zero matrix of size $2^i(\ell-1) \times (n+2^i)$, $\widetilde{\Theta}_i$ is a zero matrix of size $2^i(\ell-1) \times 2^i$, while θ is a zero column vector with $2^i(\ell-1)$ entries and Θ is a $n \times (m+n)$ zero matrix.

Observations 1. *The following explicitly clarified observations have to be taken into consideration for providing a comprehensive and detailed proof of the new proposed Theorem 1 that follows.*

a) Let $\widetilde{S}_0$ and B_0 be the matrices given by Eqs. (3) and (6) respectively and S^* be the modified generalized Sylvester matrix of the polynomials $p_i(x)$, $i = 1, 2, \ldots, \ell$ given by Eq. (7).
b) Let $Q_i B_{i+1} = B_i + \Delta B_i$, $i = 0, 1, \ldots, k-1$ be the exact QR factorization of a slightly perturbed block B_i, given by Eq. (11), where Q_i is an orthogonal matrix and ΔB_i a small perturbation matrix.
c) Set $S_0 = S^*$ and let $Q_i = \widehat{B_Q(Q_i}, I, \Theta, \widehat{\Theta}, \widetilde{\Theta})$ be the orthogonal matrix given by Eq. (25) that fulfills the block-QR factorization $\widehat{Q}_i S_{i+1} = S_i + \Delta E_i$, $i = 0, 1, \ldots, k-2$, where ΔE_i is a small perturbation matrix given by Eq. (26). For $i = k-1$ an additional block QR factorization is performed for triangularizing the matrix S_{k-1} giving an orthogonal matrix $\widehat{Q}_{k-1}$ and an upper triangular

matrix S_k such that $\widehat{Q}_{k-1}S_k = S_{k-1} + \Delta E_{k-1}$. The last non zero row of S_k gives the coefficients of the GCD of the polynomials [1].

d) Let the $(\ell m+n)\times(\ell m+n)$ orthogonal matrix $\widetilde{Q}_0$ be the product $\widehat{Q}_{k-1}^{\top}\widehat{Q}_{k-2}^{\top}\cdots\widehat{Q}_1^{\top}\widehat{Q}_0^{\top}$, where ℓ is the number of levels of Scheme 1 and m, n are the largest degree and the second larger degree of the considered polynomials.

Theorem 1. *According to Observations 1 consider the following iterative application of the QR factorization to the blocks B_i of the matrix S_i:*

$$S_{i+1} = \widehat{Q}_i^{\top}(S_i + \Delta E_i), \quad i = 0, 1, \ldots, k-1, \tag{27}$$

with

$$\|\Delta E_i\|_F \leqslant \varphi(m_i, n_i)\, 2^{(\sigma_{i-1}+1)/2}\,(\ell-1)^{i/2}\, u\, \|S^*\|_F, \quad i = 0, 1, \ldots, k-1, \tag{28}$$

where $\sigma_i = \sum_{j=0}^{i} j$, for $\sigma_{-1} = 0$, $\varphi(m_i, n_i)$ are slowly growing functions of m_i, n_i and u is the unit round off error.

The final exact QR factorization of S^* is given by the following trapezoidal $(\ell m+n)\times(m+n)$ matrix resulting from the iterative block QR factorizations:

$$S_k = \widetilde{Q}_0\, S^* + \mathcal{E}, \quad \textit{with} \quad k = \lceil \log_2 m \rceil + 1, \tag{29}$$

where k is the required number of iterations. In addition, the Frobenius norm of the above error matrix $\mathcal{E}$ is bounded as follows:

$$\|\mathcal{E}\|_F \leqslant \sqrt{\ell m+n} \sum_{i=0}^{k-1} \left\{\varphi(m_i, n_i)\, 2^{(\sigma_{i-1}+1)/2}\,(\ell-1)^{i/2}\right\} u\, \|S^*\|_F. \tag{30}$$

Proof. Consider the following $(\ell m+n)\times(m+n)$ modified generalized Sylvester matrix S^* of the polynomials of all the levels (*cf.* Notation 3):

$$S^* = B_S(B_0, S_0, \theta).$$

The matrix S^* has m same $(\ell-1)\times(n+1)$ blocks B_0. Using Lemma 1, by applying the QR factorization to B_0, we compute the exact QR factorization of a slightly perturbed matrix B_0 such that:

$$B_0 + \Delta B_0 = Q_0 R_0, \tag{31}$$

with

$$\left\|\Delta B_0\right\|_F \leqslant \varphi(m_0, n_0)\, u \left\|B_0\right\|_F, \tag{32}$$

where $\varphi(m_0, n_0)$ is a slowly growing function of m_0, n_0 (*cf.* [7]), $m_0 = \ell - 1$ is the number of rows and $n_0 = n+1$ is the number of columns of B_0.

Consider the $(\ell m+n)\times(\ell m+n)$ block matrix $\widehat{Q}_0$ (*cf.* Notation 5):

$$\widehat{Q}_0 = B_Q(Q_0, I, \Theta, \widehat{\Theta}, \widetilde{\Theta}),$$

where Q_0 is an orthogonal $(\ell-1)\times(\ell-1)$ matrix derived by the QR factorization of the matrix B_0, I is an $n\times n$ identity matrix, Θ is an $(\ell-1)\times(\ell-1)$ zero matrix, $\widehat{\Theta}$ is an $n\times(\ell-1)$ zero matrix and $\widetilde{\Theta}$ is an $(\ell-1)\times n$ zero matrix. The first iteration of the QR factorization to the blocks of S^* can be achieved as follows:

$$S_1 \simeq \widehat{Q}_0^{\top}\, S^* = B_S(R_0, S_0, \theta).$$

The above matrix S_1 is the exact result of the application of the QR factorization to slightly perturbed blocks B_0 of S^* such that:

$$S^* + \Delta E_0 = \widehat{Q}_0\, S_1,$$

where the $(\ell m+n)\times(m+n)$ matrix ΔE_0 is given by:

$$\Delta E_0 = B_S(\Delta B_0, \Theta, \theta).$$

For the Frobenius norms of ΔE_0 and S^* hold that:

$$\|\Delta E_0\|_F = \Big(\sum_i \sum_j \{\Delta E_0\}_{ij}^2\Big)^{1/2} = \sqrt{m}\,\|\Delta B_0\|_F, \tag{33}$$

and

$$\|S^*\|_F^2 = m \sum_i \sum_j \{B_0\}_{ij}^2 + \sum_i \sum_j \{S_0\}_{ij}^2 = m\,\|B_0\|_F^2 + \|S_0\|_F^2.$$

Consequently we obtain:

$$\|B_0\|_F^2 = m^{-1}\|S^*\|_F^2 - m^{-1}\|S_0\|_F^2 \leqslant m^{-1}\|S^*\|_F^2 + m^{-1}\|S^*\|_F^2 = 2m^{-1}\|S^*\|_F^2,$$

which implies that

$$\|B_0\|_F \leqslant \frac{\sqrt{2}}{\sqrt{m}}\|S^*\|_F. \tag{34}$$

By virtue of Lemma 1 and using Eqs. (32) and (34) the Eq. (33) becomes:

$$\|\Delta E_0\|_F \leqslant \quad \varphi(m_0, n_0)\sqrt{2}u\|S^*\|_F.$$

For the matrix S_1 it holds the following:

$$S_1 = Q_0^\top\left(S^* + \Delta E_0\right) = B_S(R_0, S_0, \theta).$$

Consider the $2(\ell - 1)\times(n+2)$ upper left block B_1 of S_1:

$$B_1 = \begin{bmatrix} [R_0][\theta] \\ [\theta][R_0] \end{bmatrix}.$$

By applying the QR factorization to the above matrix B_1 the computed orthogonal and upper triangular matrices Q_1 and R_1 are respectively the exact factors of the QR factorization of a slightly perturbed matrix B_1 such that $B_1 + \Delta B_1 = Q_1 R_1$. Using Lemma 1 we obtain that:

$$\|\Delta B_1\|_F \leqslant \varphi(m_1, n_1)\sqrt{2}\sqrt{\ell - 1}\,u\|B_0\|_F,$$

where $n_1 = n_0 + 1 = n + 2$ is the number of columns of B_1 and n_0 is the number of columns of B_0.

Similarly, the application of the QR factorization to the blocks of S_1 is achieved as follows:

$$S_2 \simeq \widehat{Q}_1^\top S_1 = B_S(R_1, S_0, \theta).$$

The above matrix S_2 is the exact result of the application of the QR factorization to slightly perturbed blocks B_1 of S_1 such that $S_1 + \Delta E_1 = \widehat{Q}_1 S_2$, with

$$\|\Delta E_1\|_F = \sqrt{\frac{m}{2}}\|\Delta B_1\|_F \leqslant \sqrt{\frac{m}{2}}\varphi(m_1, n_1)\sqrt{2}\sqrt{\ell - 1}\,u\|B_0\|_F.$$

Consequently, using Eq. (34) we get:

$$\|\Delta E_1\|_F \leqslant \varphi(m_1, n_1)\sqrt{m(\ell - 1)}\sqrt{2}u\frac{1}{\sqrt{m}}\|S^*\|_F,$$

or equivalently

$$\|\Delta E_1\|_F \leqslant \varphi(m_1, n_1)\sqrt{2}\sqrt{\ell - 1}\,u\|S^*\|_F,$$

where

$$\widehat{Q}_1 = B_Q(Q_1, I, \Theta, \widehat{\Theta}, \widetilde{\Theta}).$$

The matrix $\widehat{Q}_1$ has $m/2$ same blocks Q_1 since B_1 has the double rows of B_0 and

$$\Delta E_1 = B_S(\Delta B_1, \Theta, \theta).$$

For the matrix S_2 it holds that:

$$S_2 = \widehat{Q}_1^\top\left(S_1 + \Delta E_1\right) = \widehat{Q}_1^\top\left(\widehat{Q}_0^\top\left(S^* + \Delta E_0\right) + \Delta E_1\right) = B_S(R_1, S_0, \theta).$$

At the third iteration of our approach we apply the QR factorization to the following $2^2(\ell - 1)\times(n + 2^2)$ matrix B_2:

$$B_2 = \begin{bmatrix} [R_1][\theta][\theta] \\ [\theta][\theta][R_1] \end{bmatrix}.$$

Note that B_2 is the upper left block of the matrix S_2.

Assume that Q_2 and R_2 are respectively the computed orthogonal and upper triangular matrices of the QR factorization of B_2. This concerns the exact QR factorization of a slight perturbation ΔB_2 of matrix B_2 such that:

$$B_2 + \Delta B_2 = Q_2 R_2.$$

Consider the matrix

$$\widehat{Q}_2 = B_Q(Q_2, I, \Theta, \widehat{\Theta}, \widetilde{\Theta}).$$

Similarly to the previous steps we have $S_2 + \Delta E_2 = \widehat{Q}_2\, S_3$. By virtue of Lemma 1 using Eq. (22) we obtain:

$$\|\Delta E_2\|_F = \sqrt{\frac{m}{4}}\,\|\Delta B_2\|_F \leqslant \sqrt{\frac{m}{4}}\,\varphi(m_2, n_2)\,\sqrt{2}^{\,3}\,\sqrt{\ell-1}^{\,2}\,u\,\|B_0\|_F,$$

where $m/4$ is the number of the same blocks B_2. Using Eq. (34) we have:

$$\|\Delta E_2\|_F \leqslant \varphi(m_2, n_2)\,\sqrt{2}^{\,2}\,\sqrt{\ell-1}^{\,2}\,u\,\|S^*\|_F.$$

The matrix S_3 is written as follows:

$$S_3 = \widehat{Q}_2^{\top}\big(\widehat{Q}_1^{\top}\big(\widehat{Q}_0^{\top}\big(S^* + \Delta E_0\big) + \Delta E_1\big) + \Delta E_2\big).$$

Suppose that at the $(i-1)$-th iteration it holds that:

$$S_{i-1} + \Delta E_{i-1} = \widehat{Q}_{i-1} S_i, \tag{35}$$

with

$$\|\Delta E_{i-1}\|_F \leqslant \varphi(m_{i-1}, n_{i-1})\,2^{(\sigma_{i-2}+1)/2}\,(\ell-1)^{(i-1)/2}\,u\,\|S^*\|_F. \tag{36}$$

At the i-th step it holds that:

$$S_i + \Delta E_i = \widehat{Q}_i S_{i+1}, \tag{37}$$

with

$$\|\Delta E_i\|_F = \sqrt{\frac{m}{2^i}}\,\|\Delta B_i\|_F. \tag{38}$$

By virtue of Lemma 1, using Eq. (24) and Eq. (34) we obtain an upper bound for the $\|\Delta E_i\|_F$ as follows:

$$\begin{aligned}
\|\Delta E_i\|_F &\leqslant \sqrt{\frac{m}{2^i}}\,\varphi(m_i, n_i)\,2^{\sigma_i/2}\,(\ell-1)^{i/2}\,u\,\|B_0\|_F \\
&\leqslant \sqrt{\frac{m}{2^i}}\,\varphi(m_i, n_i)\,2^{\sigma_i/2}\,(\ell-1)^{i/2}\,u\,\frac{\sqrt{2}}{\sqrt{m}}\,\|S^*\|_F \\
&= \varphi(m_i, n_i)\,2^{(\sigma_{i-1}+1)/2}\,(\ell-1)^{i/2}\,u\,\|S^*\|_F.
\end{aligned}$$

Thus, for the i-th iteration we conclude that:

$$\|\Delta E_i\|_F \leqslant \varphi(m_i, n_i)\,2^{(\sigma_{i-1}+1)/2}\,(\ell-1)^{i/2} u\,\|S^*\|_F, \text{ for } \quad i = 0, 1, \ldots, k-1,$$

where $k = \lceil \log_2 m \rceil + 1$.

Next, by using Relation (27) the matrix S_k can be given as follows:

$$\begin{aligned}
S_k = {} & \widehat{Q}_{k-1}^{\top}\widehat{Q}_{k-2}^{\top}\cdots\widehat{Q}_1^{\top}\widehat{Q}_0^{\top}\,S^* + \widehat{Q}_{k-1}^{\top}\widehat{Q}_{k-2}^{\top}\cdots\widehat{Q}_0^{\top}\,\Delta E_0 + \\
& + \widehat{Q}_{k-1}^{\top}\widehat{Q}_{k-2}^{\top}\cdots\widehat{Q}_1^{\top}\,\Delta E_1 + \cdots + \widehat{Q}_{k-1}^{\top}\widehat{Q}_{k-2}^{\top}\,\Delta E_{k-2} + \widehat{Q}_{k-1}^{\top}\Delta E_{k-1}.
\end{aligned}$$

Since the product of orthogonal matrices is an orthogonal matrix, by using the notation:

$$\widetilde{Q}_j = \widehat{Q}_{k-1}^{\top}\widehat{Q}_{k-2}^{\top}\cdots\widehat{Q}_j^{\top}, \quad \text{for} \quad j = 0, 1, \ldots, k-1,$$

the matrix S_k can be written as follows:

$$S_k = \widetilde{Q}_0\,S^* + \widetilde{Q}_0\,\Delta E_0 + \widetilde{Q}_1\,E_1 + \cdots + \widetilde{Q}_{k-2}\,\Delta E_{k-2} + \widetilde{Q}_{k-1}\Delta E_{k-1}.$$

The above relation can be written as follows:

$$S_k = \widetilde{Q}_0\,S^* + \mathcal{E},$$

where

$$\mathcal{E} = \widetilde{Q}_0\,\Delta E_0 + \widetilde{Q}_1\,\Delta E_1 + \cdots + \widetilde{Q}_{k-2}\,\Delta E_{k-2} + \widetilde{Q}_{k-1}\Delta E_{k-1},$$

Table 2
Order of the bound of the error in Eq. (13) in terms of the number of levels ℓ and m that indicates the maximum degree of the considered polynomials.

ℓ	m	$q_1 = 2^{\sigma_k/2}\,(\ell-1)^{k/2}$	$q_2 = 2^{\sigma_k/2}\,(\ell-1)^{k/2}\,u$
10	10	$4.398769864405275 \times 10^{4}$	$4.883615583490014 \times 10^{-12}$
10	100	$1.719926784000000 \times 10^{9}$	$1.909502316266298 \times 10^{-7}$
10	500	$1.120824015769286 \times 10^{13}$	$1.244364628860000 \times 10^{-3}$
20	10	$2.848452422491905 \times 10^{5}$	$3.162417463999817 \times 10^{-11}$
20	100	$3.416286822400000 \times 10^{10}$	$3.792840288951993 \times 10^{-6}$
20	500	$4.699946188118873 \times 10^{14}$	$5.217988472548800 \times 10^{-2}$
30	10	$8.198227433000379 \times 10^{5}$	$9.101860857230614 \times 10^{-11}$
30	100	$1.854094704640000 \times 10^{11}$	$2.058458630926907 \times 10^{-5}$
30	500	$3.893273110505203 \times 10^{15}$	$4.322401448436880 \times 10^{-1}$

Table 3
Upper bounds of the error given by Relation (28) in terms of the number of levels ℓ and m, n that indicate the maximum and the second maximum degrees of the considered polynomials respectively. The upper bounds exhibited for $n = m$ can be used for obtaining upper bounds for the cases where $n < m$. The constant ς is given by $\varsigma = \max_i \left\{\varphi(m_i, n_i)\right\}$.

ℓ	(m,n)	$\sqrt{\ell m + n}\,\sum_{i=0}^{k-1} \left\{\varphi(m_i,n_i)\,2^{(\sigma_{i-1}+1)/2}\,(\ell-1)^{i/2}\right\} u$
10	(10, 10)	$\varsigma \times 1.220381792939832 \times 10^{-12}$
10	(100, 100)	$\varsigma \times 1.722399261064825 \times 10^{-8}$
10	(500, 500)	$\varsigma \times 6.137129109342957 \times 10^{-5}$
20	(10, 10)	$\varsigma \times 7.177318144680123 \times 10^{-12}$
20	(100, 100)	$\varsigma \times 3.208395515893840 \times 10^{-7}$
20	(500, 500)	$\varsigma \times 2.430872035454000 \times 10^{-2}$
30	(10, 10)	$\varsigma \times 1.995122339686522 \times 10^{-11}$
30	(100, 100)	$\varsigma \times 1.702624960813450 \times 10^{-6}$
30	(500, 500)	$\varsigma \times 1.974772651999400 \times 10^{-2}$

determines the total error of the decomposition. Next, we compute an upper bound of the Frobenius norm of the error $\mathcal{E}$ of the considered decompositions.

$$
\begin{aligned}
\left\|\mathcal{E}\right\|_F &= \left\|\widetilde{Q}_0\,\Delta E_0 + \widetilde{Q}_1\,\Delta E_1 + \cdots + \widetilde{Q}_{k-2}\,\Delta E_{k-2} + \widetilde{Q}_{k-1}\Delta E_{k-1}\right\|_F \\
&\leqslant \left\|\widetilde{Q}_0\right\|_F \left\|\Delta E_0\right\|_F + \left\|\widetilde{Q}_1\right\|_F \left\|\Delta E_1\right\|_F + \cdots + \\
&\quad + \left\|\widetilde{Q}_{k-2}^{\top}\right\|_F \left\|\Delta E_{k-2}\right\|_F + \left\|\widetilde{Q}_{k-1}^{\top}\right\|_F \left\|\Delta E_{k-1}\right\|_F \\
&\leqslant \max_i \left\{\left\|\widetilde{Q}_i\right\|_F\right\} \sum_{j=0}^{k-1} \left\|\Delta E_j\right\|_F \\
&\leqslant \sqrt{\ell\, m + n}\, \max_i \left\{\left\|\widetilde{Q}_i\right\|_2\right\} \sum_{j=0}^{k-1} \left\|\Delta E_j\right\|_F .
\end{aligned}
$$

Hence, by virtue of Relation (28) we conclude that

$$
\left\|\mathcal{E}\right\|_F \leqslant \sqrt{\ell\, m + n} \sum_{j=0}^{k-1} \varphi(m_i, n_i)\, 2^{(\sigma_{i-1}+1)/2}\,(\ell-1)^{i/2}\, u\, \left\|S^*\right\|_F .
$$

Thus, the theorem is proved. □

In Table 2 the quantities $q_1 = 2^{\sigma_k/2}(l-1)^{k/2}$ and $q_2 = q_1\,u$ of the bound of Lemma 1 are exhibited, where $k = \lceil \log_2 m \rceil + 1$ is the number of applications of the QR factorization, ℓ is the number of the levels which equals to the number of polynomials, m is the maximum degree of polynomials, u is the unit round off error and $\sigma_i = \sum_{j=0}^{i} j$. The quantity q_2 approximates the order of the final error, in terms of the number of polynomials and the maximum degree of them.

In Table 3 the bound $\sqrt{\ell m + n}\,\sum_{i=0}^{k-1} \left\{\varphi(m_i,n_i)\,2^{(\sigma_{i-1}+1)/2}\,(\ell-1)^{i/2}\right\} u$ of the Frobenius norm of the error matrix $\mathcal{E}$ in Relation (30) of Theorem 1 is exhibited, where k, ℓ, m, u and σ_i are the same notations given in Table 2, with $\sigma_{-1} = 0$ and n is the second larger degree of polynomials. The constant ς refers to the $\max_i \left\{\varphi(m_i, n_i)\right\}$, where $\varphi(m_i, n_i)$ is a slowly growing function of m_i, n_i. The considered bound in Table 3 is important since it approximates the total error for the whole process of the iteratively applications of the QR factorization.

3.1.3. Computational complexity of Scheme 1

Assume that $p_q^{(1)}(x),\ p_i(x)\ \in \mathbb{R}[x],\ i=2,3,\ldots,\ell$ are ℓ the polynomials of the levels $L_i,\ i=1,2,\ldots,\ell$. Then the computational complexity of the algorithm for computing the GCD of polynomials by applying the modified version of LU factorization with partial pivoting to the modified Sylvester matrix in flops is (*cf.* [31]):

$$N_{\mathrm{LU}}^{(1)} = \frac{1}{2}(m+n)^3\left(2\log_2 m - \frac{1}{3}\right) + (m+n)^2\big(n + 2(\ell-1)\log_2 m\big), \tag{39}$$

where $m,\ n$ are the maximum and the second maximum degree of the polynomials respectively, ℓ is the number of levels and 1 flop is the required time for computing one addition and one multiplication. In case where the implementation of the iterative applications of the block QR decomposition instead of the modified LU factorization, the final complexity of the method is given by the total required number of flops $N_{\mathrm{QR}}^{(1)}$ (*cf.* [31]):

$$N_{\mathrm{QR}}^{(1)} = (m+n)^3\left(2\log_2 m - \frac{1}{3}\right) + (m+n)^2\big(n + 2(\ell-1)\log_2 m\big). \tag{40}$$

3.1.4. Benefits of Scheme 1

A benefit of this scheme is that in the case where the selected participant of the starting Level 1 is not able to cooperate for any reason, then the participant is substituted by any other participant of Level 1. The same remains true if anyone of the participants of the Level i can not cooperate, but in that case the whole tuple has to be substituted by another one (any tuple of a level sums to the polynomial corresponding to that level). Let us suppose that the q-th participant of the j-th subset of Level i can not cooperate with the other ones. Then all the c_i q-th participants of the subsets of Level i are substituted with *e.g.* r-th ones of the subsets of the same level, $q,\ r\in\{1,2,\ldots,k_i\},\ q\neq r$.

Another benefit is that the sum of the shares of every q-th participant of the subset $S_j^{(i)},\ j=1,2,\ldots,c_i$ of any level i has to result to $p_i(x),\ i=2,3,\ldots,\ell$. Thus, if the participants of any selected authorized subset $\widehat{S}=\big(P_{q1}^{(i)},P_{q2}^{(i)},\ldots,P_{qc_i}^{(i)}\big)$ add their shares and the sum is not the polynomial $p_i(x)$ that all other tuples of the same level have computed, then we conclude that one or more participants of the tuple have given false information. The calculation process for the entire tuple will be deemed inaccurate by the dealer. The dealer is required to replace the entire subset $\widehat{S}$ of Level i with another authorized set of the same level until certain subsets yield the same polynomial $p_i(x)$. This issue introduces a self-correcting mechanism in Scheme 1.

Since the c_i is the number of subsets of the level L_i and $c_1<c_2<\cdots<c_\ell,\ \ell\geqslant 2,\ i\in\{1,2,\ldots,\ell\}$, the higher index c_i, the less significance of the level is, because more participants of the level are necessary in order to compute the polynomial $p_i(x)$ of their level. Thus, the scheme exhibits a hierarchical structure.

3.2. Scheme 2: bottom-up hierarchical ramp secret sharing

This scheme is a variation of the scheme that is described in §3.1. The Notation 1 is also used for Scheme 2. Similarly to Scheme 1 the dealer creates a polynomial $p(x)$ with several roots which constitutes the secret as it is described in §3.1. The first four steps of §3.1 remain the same.

The main difference lies into Step 5 for both schemata regarding the cooperation of the participants. Specifically, while in Scheme 1 the authorized participants compute the secret as the GCD of the polynomials of all levels all together, in Scheme 2, the authorized participants of the levels cooperate pairwise bottom up, starting by computing the GCD of their polynomials per two levels from the last level to the first one. Also, in Scheme 2 there is an additional step. In this step, named Step 6, the authorized participant of Level 1 has been informed about the computed GCDs of the polynomials of the other levels and by multiplying them computes the secret.

Remark 10. The hierarchy of the levels is defined by the importance of the information that can derive each level. Thus, by using a bottom-up hierarchy every level computes a polynomial containing a part of the secret. The retrieved information of Level i is more significant than the one of Level j if $i<j$ for $i,j\in\{1,2,\ldots,\ell\},\ i\neq j$.

Scheme 2. The proposed *bottom-up ramp hierarchical secret sharing scheme* is described below using the following steps:

Step 1: The dealer constructs a polynomial $p(x)$ which is the secret.

Step 2: Using Notation 1 the dealer creates the hierarchically structured set

$$L=\big\{L_1,L_2,\ldots,L_\ell\big\},$$

of ℓ levels of participants, $L_i,\ i=1,2,\ldots,\ell$ as they are denoted in Notation 1. The set L is a partitioning of ℓ hierarchically structured levels, where for the number of subsets c_i of the levels it holds that $c_1<c_2<\cdots<c_\ell$, where $\ell\geqslant 2$.

Step 3: The dealer provides different polynomials to all participants of Level 1. In what follows, the dealer distributes the shares $p_{h,k}^{(i)}(x)$ (*i.e.* the polynomials) to each participant $P_{hk}^{(i)}(x)$ at Level i for $i=2,3,\ldots,\ell$, in such a way that

$$p_i(x)=\sum_{k=1}^{c_i} p_{hk}^{(i)}(x),\quad h\in\{1,2,\ldots,\ k_i\},\quad i\in\{2,3,\ldots,\ell\},$$

where i denotes the Level and it holds that $\gcd\{p_{hk}^{(i)}(x), p(x)\} = 1$ for any h, k and i, $p_i(x)$ denotes the corresponding polynomial for Level i, $i = 2, 3, \dots, \ell$ (created by the dealer), $p_j^{(1)}(x)$ denotes the polynomial of the j-th participant of Level 1 and $\gcd\{p_i(x), p(x)\} \neq 1$ for any i, as well as $\gcd\{p_j^{(1)}(x), p(x)\} \neq 1$, $j \in \{1, 2, \dots, k_1\}$.

Step 4: The dealer selects one specific participant, *e.g.* the j-th, named $P_{jl}^{(i)}$ from every subset $S_l^{(i)} = \{P_{1l}^{(i)}, P_{2l}^{(i)}, \dots, P_{k_i l}^{(i)}\}$ from every level i, $i = 1, 2, \dots, \ell$, $j \in \{1, 2, \dots, k_i\}$ such that

$$p_i(x) = \sum_{k=1}^{c_i} p_{jk}^{(i)}(x).$$

Step 5: The authorized participants of levels i and $(i+1)$, compute the GCD of their polynomials $p_i(x)$ and $p_{i+1}(x)$, $i = \ell - 1, \ell - 2, \dots, 3, 2$ with a bottom-up process and provide the total gathering pieces of information to the authorized participants of the next level. That is to say:

$$g_i(x) = \gcd\{p_{i+1}(x), p_i(x)\}, \quad i = \ell - 1, \ell - 2, \dots, 3, 2.$$

Assume that the dealer selects the j-th participant of Level 1. Then $P_j^{(1)}$ cooperates with the authorized participants of Level 2 and computes the GCD of their polynomials. Thus,

$$g_1(x) = \gcd\{p_2(x), p_j^{(1)}(x)\}.$$

Step 6: The secret $p(x)$ is computed by the selected by the dealer j-th participant of Level 1, $j \in \{1, 2, \dots, k_1\}$, by multiplying the computed GCDs $g_i(x)$, $i = \ell - 1, \dots, 2, 1$. Thus,

$$p(x) = \prod_{i=1}^{\ell-1} g_i(x). \tag{41}$$

In Table 4 the main steps of Scheme 2 are exhibited. The secret can be obtained by Eq. (41). The polynomials $p_2(x), \dots, p_\ell(x)$ at each level are obtained if all the participants with the same color at each level add their polynomials.

3.2.1. Analyzing Scheme 2

Similarly to the Scheme 1, for the computation of the polynomial $p(x)$, one participant from Level 1 is required. On the other hand, as it is already mentioned before, the participants selected from Level i will cooperate with those of $(i-1)$-th Level for, $i = \ell, \ell - 1, \dots, 2$, in a bottom-up cooperation of two levels every time. The selected participants (of the same color, *cf.* Table 4) of the ℓ-th Level provide their computed polynomial $p_\ell(x)$ to the authorized participants (of the same color, possibly with a different color than the previous one) of the next Level $L_{\ell-1}$. The participants of Level $L_{\ell-1}$ compute the GCD $g_{\ell-1}(x)$ of their polynomial $p_{\ell-1}(x)$ with $p_\ell(x)$ such that to retrieve the less significant information about the secret that has be given by the dealer. As the process continues with this bottom-up procedure, the higher in hierarchy levels will retrieve the more significant information about the secret. Finally, a participant of Level 1 will compute the secret $p(x)$.

The benefits of this scheme are similar with those described in §3.1.4.

3.2.2. Computational complexity of Scheme 2

Assume that $f(x)$, $q(x) \in \mathbb{R}[x]$ are two polynomials of degree n and p respectively, where $p \leqslant n$. The computational complexity of the algorithm for computing the GCD of the two polynomials is $(2(pn + (n-p)n^2))$ flops. The computation has been performed by applying the modified version of QR factorization to the modified Sylvester matrix, described in [30]. Since in the proposed Scheme 2, $(\ell - 1)$ GCDs of two polynomials have to be computed, the final complexity of the method is given by the total required number flops $N_{\text{flops}}^{(2)}$:

$$N_{\text{flops}}^{(2)} = (\ell - 1)\big(2(pn + (n-p)n^2)\big). \tag{42}$$

3.2.3. Error analysis of Scheme 2

The QR factorization applied to the Sylvester matrix S, used for the computation of the GCD of two polynomials of degrees m and n is the exact QR factorization of a slightly perturbed matrix $S + E$ such that $S + E = QR$. In the case where the inner products are accumulated in double precision, the Frobenius norm of E is bounded as follows (*cf.* [7, p. 145], [33, p. 236]):

$$\|E\|_F \leqslant 12.5\,(m+n)\,u\,\|S\|_F,$$

where u denotes the unit round off error. Note that the above bound of the error concerns the cooperation of two levels.

Table 4
Exhibition of the main steps of Scheme 2. The secret is obtained by a participant of Level 1 by multiplying the GCDs $g_i(x)$, $i = 1, 2, \ldots, \ell - 1$.

$$p(x) = g_{\ell-1}(x)\, g_{\ell-2}(x) \cdots g_2(x)\, g_1(x)$$

$\uparrow$

L_1

$P_1^{(1)} \to p_1^{(1)}(x)$	$P_2^{(1)} \to p_2^{(1)}(x)$	$\ldots$	$P_{k_1}^{(1)} \to p_{k_1}^{(1)}(x)$

$\uparrow\ p_2(x),\ \{g_{\ell-1}(x), g_{\ell-2}(x), \ldots, g_2(x)\}$

L_2

$S_1^{(2)}$	$S_2^{(2)}$	$\ldots$	$S_{c_2}^{(2)}$	
$P_{11}^{(2)}$	$P_{21}^{(2)}$	$\ldots$	$P_{c_2 1}^{(2)}$	$\xrightarrow{(+)} p_2(x) \to g_2(x) = \gcd\{p_2(x), p_3(x)\}$
$P_{12}^{(2)}$	$P_{22}^{(2)}$	$\ldots$	$P_{c_2 2}^{(2)}$	$\xrightarrow{(+)} p_2(x) \to g_2(x) = \gcd\{p_2(x), p_3(x)\}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$P_{1k_2}^{(2)}$	$P_{2k_2}^{(2)}$	$\ldots$	$P_{c_2 k_2}^{(2)}$	$\xrightarrow{(+)} p_2(x) \to g_2(x) = \gcd\{p_2(x), p_3(x)\}$

$\uparrow\ p_3(x),\ \{g_{\ell-1}(x), g_{\ell-2}(x), \ldots, g_3(x)\}$

$\vdots$

$\uparrow\ p_{\ell-2}(x),\ \{g_{\ell-1}(x), g_{\ell-2}(x)\}$

$L_{\ell-2}$

$S_1^{(\ell-2)}$	$S_2^{(\ell-2)}$	$\ldots$	$S_{c_{\ell-2}}^{(\ell-2)}$	
$P_{11}^{(\ell-2)}$	$P_{21}^{(\ell-2)}$	$\ldots$	$P_{c_{\ell-2}1}^{(\ell-2)}$	$\xrightarrow{(+)} p_{\ell-2}(x) \to g_{\ell-2}(x) = \gcd\{p_{\ell-2}(x), p_{\ell-1}(x)\}$
$P_{12}^{(\ell-2)}$	$P_{22}^{(\ell-2)}$	$\ldots$	$P_{c_{\ell-2}2}^{(\ell-2)}$	$\xrightarrow{(+)} p_{\ell-2}(x) \to g_{\ell-2}(x) = \gcd\{p_{\ell-2}(x), p_{\ell-1}(x)\}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$P_{1k_{\ell-2}}^{(\ell-2)}$	$P_{2k_{\ell-2}}^{(\ell-2)}$	$\ldots$	$P_{c_{\ell-2}k_{\ell-2}}^{(\ell-2)}$	$\xrightarrow{(+)} p_{\ell-2}(x) \to g_{\ell-2}(x) = \gcd\{p_{\ell-2}(x), p_{\ell-1}(x)\}$

$\uparrow\ p_{\ell-1}(x),\ \{g_{\ell-1}(x)\}$

$L_{\ell-1}$

$S_1^{(\ell-1)}$	$S_2^{(\ell-1)}$	$\ldots$	$S_{c_1-1}^{(\ell-1)}$	
$P_{11}^{(\ell-1)}$	$P_{21}^{(\ell-1)}$	$\ldots$	$P_{c_{\ell-1}1}^{(\ell-1)}$	$\xrightarrow{(+)} p_{\ell=1}(x) \to g_{\ell-1}(x) = \gcd\{p_{\ell-1}(x), p_\ell(x)\}$
$P_{12}^{(\ell-1)}$	$P_{22}^{(\ell-1)}$	$\ldots$	$P_{c_{\ell-1}2}^{(\ell-1)}$	$\xrightarrow{(+)} p_{\ell-1}(x) \to g_{\ell-1}(x) = \gcd\{p_{\ell-1}(x), p_\ell(x)\}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$P_{1k_{\ell-1}}^{(\ell-1)}$	$P_{2k_{\ell-1}}^{(\ell-1)}$	$\ldots$	$P_{c_{\ell-1}k_{\ell-1}}^{(\ell-1)}$	$\xrightarrow{(+)} p_{\ell-1}(x) \to g_{\ell-1}(x) = \gcd\{p_{\ell-1}(x), p_\ell(x)\}$

$\uparrow\ p_\ell(x)$

L_ℓ

$S_1^{(\ell)}$	$S_2^{(\ell)}$	$S_3^{(\ell)}$	$\ldots$	$S_{c_\ell}^{(\ell)}$	
$P_{11}^{(\ell)}$	$P_{21}^{(\ell)}$	$P_{31}^{(\ell)}$	$\ldots$	$P_{c_\ell 1}^{(\ell)}$	$\xrightarrow{(+)} p_\ell(x)$
$P_{12}^{(\ell)}$	$P_{22}^{(\ell)}$	$P_{32}^{(\ell)}$	$\ldots$	$P_{c_\ell 2}^{(\ell)}$	$\xrightarrow{(+)} p_\ell(x)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$P_{1k_\ell}^{(\ell)}$	$P_{2k_\ell}^{(\ell)}$	$P_{3k_\ell}^{(\ell)}$	$\ldots$	$P_{c_\ell k_\ell}^{(\ell)}$	$\xrightarrow{(+)} p_\ell(x)$

4. Illustrative examples

4.1. Ramp hierarchical secret sharing Scheme 1

The following example illustrates the Scheme 1. Let us suppose that the secret is the polynomial $p(x) = x^3 - 6x^2 + 11x + 6 = (x-1)(x-2)(x-3)$ and the dealer creates three levels and subsets in them as presented in Table 5.

Level 3 consists of 4 subsets of participants. The participants of this level with the same row-index can add their shares and compute the polynomial of Level 3. Thus, either participants $P_{11}^{(3)}$, $P_{12}^{(3)}$, $P_{13}^{(3)}$, $P_{14}^{(3)}$ will add their polynomials,

$$\begin{aligned} p_3(x) &= p_{11}^{(3)}(x) + p_{12}^{(3)}(x) + p_{13}^{(3)}(x) + p_{14}^{(3)}(x) \\ &= x^6 - 21x^5 + 175x^4 - 735x^3 + 1624x^2 - 1764x + 720 \\ &= (x-1)(x-2)(x-3)(x-4)(x-5)(x-6), \end{aligned}$$

or participants $P_{21}^{(3)}$, $P_{22}^{(3)}$, $P_{23}^{(3)}$, $P_{24}^{(3)}$ will add their polynomials,

$$p_3(x) = p_{21}^{(3)}(x) + p_{22}^{(3)}(x) + p_{23}^{(3)}(x) + p_{24}^{(3)}(x).$$

Similarly, three participants with the same row-index (color) from Level 2 add their shares and compute the polynomial of the Level. If $P_{11}^{(2)}$, $P_{12}^{(2)}$, $P_{13}^{(2)}$ add their polynomials, they compute the polynomial of Level 2. Thus,

Table 5
Example of the levels, subsets and participants that are implemented in Scheme 1.

Level	Subset	Participant	Polynomial
1		$P_1^{(1)}$	$p_1^{(1)}(x) = x^6 - 28x^5 + 302x^4 - 1580x^3 + +4149x^2 - 5112x + 2268$
		$P_2^{(1)}$	$p_2^{(1)}(x) = x^6 - 27x^5 + 280x^4 - 1410x^3 + +3589x^2 - 4323x + 1890$
2	$S_1^{(2)}$	$P_{11}^{(2)}$	$p_{11}^{(2)}(x) = 3x^5 - 35x^4 + 65x^3 + 174x + 100$
		$P_{21}^{(2)}$	$p_{21}^{(2)}(x) = 10x^5 - 90x^4 - 100x^2 + 274x - 20$
	$S_2^{(2)}$	$P_{12}^{(2)}$	$p_{12}^{(1)}(x) = -2x^5 + 30x^4 - 260x^2 + 100x + 300$
		$P_{22}^{(2)}$	$p_{22}^{(2)}(x) = -8x^5 - 25x^4 + 65x^3 - 10x^2 - 60$
	$S_3^{(2)}$	$P_{13}^{(2)}$	$p_{13}^{(2)}(x) = -12x^4 + 40x^3 - 35x^2 - 100x - 568$
		$P_{23}^{(2)}$	$p_{23}^{(2)}(x) = -x^5 + 98x^4 + 40x^3 - 185x^2 + +100x - 88$
3	$S_1^{(3)}$	$P_{11}^{(3)}$	$p_{11}^{(3)}(x) = x^6 + 1624x^2 + 400$
		$P_{21}^{(3)}$	$p_{21}^{(2)}(x) = 15x^6 - 71x^5 - 835x^3 - 700x + 20$
	$S_2^{(3)}$	$P_{12}^{(3)}$	$p_{12}^{(3)}(x) = -21x^5 - 735x^3 + 120$
		$P_{22}^{(3)}$	$p_{22}^{(3)}(x) = -10x^6 - 100x^4 + 45x^3 + 1000x^2 - -464x + 100$
	$S_3^{(3)}$	$P_{13}^{(3)}$	$p_{13}^{(3)}(x) = 175x^4 - 15x^3 - 50$
		$P_{23}^{(3)}$	$p_{23}^{(3)}(x) = -4x^6 + 10x^5 + 150x^4 + 55x^3 + +600x^2 + 50$
	$S_4^{(3)}$	$P_{14}^{(3)}$	$p_{14}^{(3)}(x) = 15x^3 - 1764x + 250$
		$P_{24}^{(3)}$	$p_{24}^{(3)}(x) = 40x^5 + 125x^4 + 24x^2 - 600x + 550$

$$\begin{aligned} p_2(x) &= p_{11}^{(2)}(x) + p_{12}^{(2)}(x) + p_{13}^{(2)}(x) \\ &= x^5 - 17x^4 + 105x^3 - 295x^2 + 374x - 168 \\ &= (x-1)(x-2)(x-3)(x-4)(x-7). \end{aligned}$$

The same polynomial can be derived by the participants of every subset of Level 2 with the same row-index (color), thus

$$p_2(x) = p_{21}^{(2)}(x) + p_{22}^{(2)}(x) + p_{23}^{(2)}(x).$$

Finally, any participant of Level 1, can cooperate with the participants of the lower levels for computing the GCD of their polynomials in order to retrieve the secret

$$p(x) = \gcd\left\{p_1^{(1)}(x),\, p_2(x),\, p_3(x)\right\} = (x-1)(x-2)(x-3),$$

or equivalently

$$p(x) = \gcd\left\{\{p_2^{(1)}(x),\, p_2(x),\, p_3(x)\right\}.$$

It is worth noting here that, every level can factor its polynomial which includes the $p(x)$ (ramp scheme), but can not clarify which factors have to be multiplied with in order to compute the secret. If any two levels compute the GCD of their polynomials, they will be led to a polynomial of higher degree than $p(x)$ which will include the secret but again they can not clarify the correct factors.

As it is exhibited in Table 5 the first participant of Level 1 has received the polynomial

$$\begin{aligned} p_1^{(1)}(x) &= x^6 - 28x^5 + 302x^4 - 1580x^3 + 4149x^2 - 5112x + 2268 \\ &= (x-1)(x-2)(x-3)(x-6)(x-7)(x-9), \end{aligned}$$

and the second participant of Level 1 the polynomial

$$\begin{aligned} p_2^{(1)}(x) &= x^6 - 27x^5 + 280x^4 - 1410x^3 + 3589x^2 - 4323x + 1890 \\ &= (x-1)(x-2)(x-3)(x-5)(x-7)(x-9). \end{aligned}$$

The authorized participants of Level 2 compute the polynomial

$$\begin{aligned} p_2(x) &= x^5 - 17x^4 + 105x^3 - 295x^2 + 374x - 168 \\ &= (x-1)(x-2)(x-3)(x-4)(x-7), \end{aligned}$$

and the authorized participants of Level 3 compute the polynomial

Table 6
Example of the levels, subsets and participants that are implemented in Scheme 2.

Level	Subset	Participant	Polynomial
1		$P_1^{(1)}$	$p_1^{(1)}(x) = x^3 - 17x^2 + 86x - 112 = (x-8)(x-7)(x-2)$
		$P_2^{(1)}$	$p_2^{(1)}(x) = x^3 - 18x^2 + 95x - 126 = (x-9)(x-7)(x-2)$
2	$S_1^{(2)}$	$P_{11}^{(2)}$	$p_{11}^{(2)}(x) = 35x^3 + 10x^2 + 14x + 10$
		$P_{21}^{(2)}$	$p_{21}^{(2)}(x) = 10x^3 - 10x^2 - 27x - 20$
	$S_2^{(2)}$	$P_{12}^{(2)}$	$p_{12}^{(2)}(x) = -30x^3 - 2x^2 + 10x - 30$
		$P_{22}^{(2)}$	$p_{22}^{(2)}(x) = -8x^3 - 2x^2 + 30x - 4$
	$S_3^{(2)}$	$P_{13}^{(2)}$	$p_{13}^{(2)}(x) = -4x^3 - 17x^2 - 20x - 2$
		$P_{23}^{(2)}$	$p_{23}^{(2)}(x) = x^3 + 32x^2 + 20x^3 - 13x + 12$
3	$S_1^{(3)}$	$P_{11}^{(3)}$	$p_{11}^{(3)}(x) = 5x^4 + 50x^2 - 10x + 10$
		$P_{21}^{(3)}$	$p_{21}^{(3)}(x) = -4x^4 - 33x^3 - 70x + 5$
	$S_2^{(3)}$	$P_{12}^{(3)}$	$p_{12}^{3)}(x) = -2x^4 - 3x^3 - 40x + 20$
		$P_{22}^{(3)}$	$p_{22}^{(3)}(x) = -10x^+12x^3 + 10x^2 - 40x + 10$
	$S_3^{(3)}$	$P_{13}^{(3)}$	$p_{13}^{(3)}(x) = -x^4 - 10x^2 - 40x + 18$
		$P_{23}^{(3)}$	$p_{23}^{(3)}(x) = -5x^4 + 8x^3 + 60x^2 + 50$
	$S_4^{(3)}$	$P_{14}^{(3)}$	$p_{14}^{(3)}(x) = x^4 - 2x^3 + 19x^2 - 17x + 12$
		$P_{24}^{(3)}$	$p_{24}^{(3)}(x) = 20x^4 - 11x^2 + 3x - 5$

$$\begin{aligned} &p_{11}^{(3)}(x) + p_{12}^{(3)}(x) + p_{13}^{(3)}(x) + p_{14}^{(3)}(x) = \\ &\quad = p_3(x) = x^6 - 21x^5 + 175x^4 - 735x^3 + 1624x^2 - 1764x + 720 \\ &\quad = (x-6)(x-5)(x-4)(x-3)(x-2)(x-1). \end{aligned}$$

Hence, we obtain:

$$\begin{aligned} &\gcd\left\{p_1^{(1)}(x), p_2^{(1)}(x)\right\} = (x-1)(x-2)(x-3)(x-7)(x-9), \\ &\gcd\left\{p_1^{(1)}(x), p_2(x)\right\} = (x-1)(x-2)(x-3)(x-7), \\ &\gcd\left\{p_1^{(1)}(x), p_3(x)\right\} = (x-1)(x-2)(x-3)(x-6) \quad \text{and} \\ &\gcd\left\{p_2(x), p_3(x)\right\} = (x-1)(x-2)(x-3)(x-4). \end{aligned}$$

Similarly,

$$\begin{aligned} &\gcd\left\{p_2^{(1)}(x), p_2(x)\right\} = (x-1)(x-2)(x-3)(x-7) \quad \text{and} \\ &\gcd\left\{p_2^{(1)}(x), p_3(x)\right\} = (x-1)(x-2)(x-3)(x-5). \end{aligned}$$

Thus, any combination of unauthorized participants or any combination of Levels less than ℓ cannot compute the secret. They are in a position to obtain a partial information about the secret since they can factor their polynomials or their GCDs but they do not know which of the computed roots is part of the secret and with which sequence if it is required. In addition, as it is mentioned in Remarks 3-7, the dealer can increase significant the computational complexity of the root finding procedure.

4.2. Bottom-up ramp hierarchical secret sharing Scheme 2

The following example illustrates the Scheme 2. Let us suppose that the secret is the polynomial $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$ and the dealer creates three levels and subsets in them as they are presented in Table 6.

As in the previous scheme, participants having the same row-index from every subset in Level i add their polynomials and compute the polynomial of their level i, $i = 2, 3$. Thus, in Level 2, either the participants of the tuple $\left(P_{11}^{(2)},\ P_{12}^{(2)},\ P_{13}^{(2)}\right)$ add their polynomials and compute the polynomial $p_2(x)$ as follows

$$\begin{aligned} p_2(x) &= p_{11}^{(2)}(x) + p_{12}^{(2)}(x) + p_{13}^{(2)}(x) \\ &= x^3 - 9x^2 + 20x - 12 = (x-6)(x-2)(x-1), \end{aligned}$$

or the participants of the tuple $\left(P_{21}^{(2)},\ P_{22}^{(2)},\ P_{23}^{(2)}\right)$ add their polynomials in order to compute the same polynomial

$$p_2(x) = p_{21}^{(2)}(x) + p_{22}^{(2)}(x) + p_{23}^{(2)}(x).$$

Similarly, at Level 3, either the participants of the tuple $\left(P_{11}^{(3)},\ P_{12}^{(3)},\ P_{13}^{(3)},\ P_{14}^{(3)}\right)$ add their polynomials in order to compute the polynomial $p_3(x)$:

$$\begin{aligned} p_3(x) &= p_{11}^{(3)}(x) + p_{12}^{(3)}(x) + p_{13}^{(3)}(x) + p_{14}^{(3)}(x) \\ &= x^4 - 13x^3 + 59x^2 - 107x + 60 = (x-5)(x-4)(x-3)(x-1), \end{aligned}$$

or the participants of the tuple $\left(P_{21}^{(3)},\ P_{22}^{(3)},\ P_{23}^{(3)},\ P_{24}^{(3)}\right)$ add their polynomials in order to compute the same polynomial $p_3(x) = p_{21}^{(3)}(x) + p_{22}^{(3)}(x) + p_{23}^{(3)}(x) + p_{24}^{(3)}(x)$.

The difference here is that this scheme is a bottom-up one. The two lower levels, namely Levels 3 and 2, are cooperating in order to compute the GCD of their polynomials. Thus,

$$g_2(x) = \gcd\left\{p_3(x),\, p_2(x)\right\} = x - 1.$$

Next, the authorized participants in Level 2 inform the authorized participant in Level 1 about the computed factor $(x-1)$. The authorized participants of Levels 2 and 1 are now cooperating for computing their GCD. From Level 1 any of $P_1^{(1)}$ or $P_2^{(1)}$ is able to participate. Thus,

$$g_1(x) = \gcd\left\{p_1^{(1)}(x),\, p_2(x)\right\} = x - 2,$$

or

$$g_1(x) = \gcd\left\{p_2^{(1)}(x),\, p_2(x)\right\} = x - 2.$$

The single participant in Level 1 that cooperated with Level 2, multiplies the polynomials $g_1(x)$ and $g_2(x)$ resulting to the secret $p(x) = g_1(x) \cdot g_2(x)$.

5. Conclusions and future research directions

Two ramp secret sharing schemata have been derived. Both schemata follow a hierarchical structure. Scheme 2 operates by following a bottom-up procedure across a predefined number of levels which constitute the hierarchy of the participants. In both proposed approaches the hierarchy is defined by two factors. Specifically, (a) the number of participants defining each level, and (b) the number of the specific participants required to collaborate in order to compute the polynomial of their respective level.

Both proposed schemata are characterized by the following issues and aspects. A lower position in levels indicates lower significance for the participants involved. An entity referred to as the dealer manages the entire process. The dealer initiates by creating a polynomial with several real roots. The polynomial constitutes the secret shares. The dealer organizes the levels, where each level comprises a number of subsets. The dealer, also, distributes shares of the secret to each participant in the form of specific polynomials. The proposed schemata, utilize fast, efficient and effective numerical linear algebra algorithms for computing the greatest common divisor of polynomials. Specifically orthogonal transformations such as Householder transformations are applied. In terms of theoretical results, our error analysis demonstrates the stability of the proposed procedure. The algorithms employed triangularize Sylvester matrices, which possess a distinctive structure, with the aim of minimizing the required floating-point operations.

In a future correspondence we intend to rigorously study and analyze the variants of the proposed schemata that we have mentioned at the paper at hand. It is worth mentioning that, an innovation of the proposed approaches is, among others, that they rely on solely over the ring of real polynomials. The dealer effortlessly is able to modify the proposed schemata by creating variants to enhance security, achieving increased difficulty for attackers, including, among others the following: (a) the adjustment of the associated root identification within a specific tolerance range, (b) the parametrical manipulation of specific polynomial features regarding the number, the multiplicity and the density of the related roots in a specific interval, (c) the enhancement of the complexity in the root-finding process for tackling possible attacks by expanding the set of the number of zeros of the polynomials. This can be achieved by expanding additional shares that have no relation with the secret (fake shares). In addition, in the proposed schemata, the dealer has the capability to identify non-conforming participants, or those who provided incorrect information about their shares. The subset containing faulty information can be properly and promptly identified and replaced by another.

Finally, we would like to point out that, in general, the new proposed Theorem 1 can be applied to other cases for the determination of the upper bounds of the error for computing the GCD of polynomials in terms of the degree and the number of polynomials.

CRediT authorship contribution statement

The authors contributed equally to this work.

Acknowledgement

It is a pleasure to thank the referees for their careful comments.

References

[1] S. Barnett, Greatest common divisor from generalized Sylvester resultant matrices, Linear Multilinear Algebra 8 (1980) 271–279.
[2] E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Comput. 24 (1970) 713–735.
[3] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, in: American Federation of Information Processing Societies – Conference Proceedings, vol. 48, AFIPS Press, Montvale, New Jersey, 1979, pp. 313–317.
[4] G.R. Blakley, Catherine Meadows, Security of ramp schemes, advances in cryptology, CRYPTO'84, Lect. Notes Comput. Sci. 196 (1985) 242–268.
[5] D.G. Cantor, H. Zassenhaus, A new algorithm for factoring polynomials over finite fields, Math. Comput. 36 (154) (1981) 587–592.
[6] M. Clerc, J. Kennedy, The particle swarm–explosion, stability, and convergence in a multidimensional complex space, IEEE Trans. Evol. Comput. 6 (2002) 58–73.
[7] B.N. Datta, Numerical Linear Algebra and Applications, Brooks/Cole, USA, 1995.
[8] R. Dawkins, The Selfish Gene, Oxford University Press, New York, 1976.
[9] J.W. Demmel, Applied Numerical Linear Algebra, SIAM Society for Industrial and Applied Mathematics, Philadelphia, 1997.
[10] G. Faber, Über die interpolatorische Darstellung stetiger Funktionen, Jber. Deutsch. Math. Verein 23 (1914) 192–210.
[11] J. von zur Gathen, D. Panario, Factoring polynomials over finite fields: a survey, J. Symb. Comput. 31 (2001) 3–17.
[12] G.H. Golub, C.F. Van Loan, Matrix Computations, 4th edition, Johns Hopkins University Press, Baltimore, 2013.
[13] N.S. Higham, Accuracy and Stability of Numerical Algorithms, SIAM Society for Industrial and Applied Mathematics, Philadelphia, 1996.
[14] IEEE Computer Society, IEEE Standard for Floating-Point Arithmeti, IEEE STD 754-2019, IEEE, 2019, pp. 1–84.
[15] N. Karcanias, M. Mitrouli, S. Fatouros, A resultant based computation of the GCD of two polynomials, in: Proc. of 11th IEEE Mediteranean Conf. on Control and Automation, Rodos Palace Hotel, MED'03, Rhodes, Greece, June 18–20, 2003.
[16] G.C. Meletiou, D.S. Triantafyllou, M.N. Vrahatis, First study for ramp secret sharing schemes through greatest common divisor of polynomials, in: Computational Mathematics and Variational Analysis, in: Springer Optimization and Its Applications, vol. 159, 2020, pp. 247–259, Chapter 14.
[17] H. Niederreiter, New deterministic factorization algorithms for polynomials over finite fields, Contemp. Math. 168 (1994) 251–268.
[18] I. Pace, S. Barnett, Comparison of algorithms for calculation of g.c.d. of polynomials, Int. J. Syst. Sci. 4 (1973) 211–226.
[19] V. Pan, Univariate polynomials: nearly optimal algorithms for numerical factorization and root-finding, J. Symb. Comput. 33 (2002) 701–733.
[20] K.E. Parsopoulos, M.N. Vrahatis, Recent approaches to global optimization problems through particle swarm optimization, Nat. Comput. 1 (2–3) (2002) 235–306.
[21] K.E. Parsopoulos, M.N. Vrahatis, Particle Swarm Optimization and Intelligence: Advances and Applications, Information Science Reference (IGI Global), Hershey, PA, USA, 2010.
[22] C. Runge, Über empirische Funktionen und die Interpolation zwischen äquidistanten Ordinaten, Z. Math. Phys. 246 (1901) 224–243.
[23] H.-P. Schwefel, Evolution and Optimum Seeking, Wiley, New York, 1995.
[24] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.
[25] V. Shoup, A new polynomial factorization algorithm and its implementation, J. Symb. Comput. 20 (4) (1995) 363–397.
[26] D.R. Stinson, An explication os secret sharing schemes, Des. Codes Cryptogr. 2 (1992) 357–390.
[27] D.R. Stinson, R. Wei, An application of ramp schemes to broadcast encryption, Inf. Process. Lett. 69 (1999) 131–135.
[28] D.R. Stinson, Ideal ramp schemes and related combinatorial objects, Discrete Math. 341 (2018) 299–307.
[29] R. Storn, K. Price, Differential evolution-a simple and efficient heuristic for global optimization over continuous spaces, J. Glob. Optim. 11 (1997) 341–359.
[30] D. Triantafyllou, M. Mitrouli, Two resultant based methods computing the greatest common divisor of two polynomials, Lect. Notes Comput. Sci. 3401 (2005) 519–526.
[31] D. Triantafyllou, M. Mitrouli, On rank and nullspace computation of the generalized Sylvester matrix, Numer. Algorithms 54 (2010) 297–324.
[32] I.C. Trelea, The particle swarm optimization algorithm: convergence analysis and parameter selection, Inf. Process. Lett. 85 (2003) 317–325.
[33] J.H. Wilkinson, The Algebraic Eigenvalue Problem, Clarendon Press, Oxford, 1965.