Error detection in the decentralized voting protocol

Alexander Bogdanov[1][0000−0002−7724−6119],
Alexei Uteshev[1][0000−0002−8344−3266], and Valery Khvatov[2]

[1]Faculty of Applied Mathematics, St. Petersburg State University
7–9 Universitetskaya nab., St. Petersburg, 199034, Russia
http://www.apmath.spbu.ru/en/
& Plekhanov Russian University of Economics
Stremyanny lane 36, Moscow, 117997, Russia
https://www.rea.ru/en/
{bogdanov@csa.ru, a.uteshev@spbu.ru}
[2]BGX Technologies AG
Hofstrasse 1a, CH-6300 Zug, Switzerland
{valery.khvatov@gmail.com}
http://www.bgx.ai/

Abstract. The decentralized voting protocol based on the Lagrange interpolant construction is analyzed for the potential error detection in the set of shares. We suggest an algorithm for the error locator polynomial construction based on procedure of computation the determinants of the Hankel type generated by the sequence of special symmetric functions of the set of shares.

Keywords: Voting protocol · homomorphic secret sharing · error correction · polynomial interpolation

1 Introduction

The decision making problem in a consortium of voters in the lack of the confidence between the members, is of vital importance for variety of applications ranging from elections to blockchain. The growing economic paradigm of the platform economy, represented by Uber, Airbnb, Spotify and other technology startups requires a transition to decentralized information exchange systems. From the point of view of computing and storing information, the central problem is the lack of a single trusted environment between the participants in the information exchange. Last years there has been an intensive development of relevant computational architectures that range from creating systems with zero tolerance levels of trust in each other to regulated pseudo-trusted environments (Private Blockchain). Consortium-based approaches have an intermediate position, allowing to reach a compromise between the necessary level of environmental security and an acceptable performance of information exchange.

Even if the qualified majority of the consortium behaves honestly, some of the unreliable voters and/or vote-counters (administrators) might influence the voting protocol in order to falsify (compromise) the result. The different approaches for the fault tolerant protocol construction has been developed during past decades; they could be principally distinguished by the attitude to the confidentiality of the voting result by each consortium member. Some of them, concerned with the Byzantine Generals Problem, are focused onto consortiums where all the decisions are assumed to be open at any stage of the vote [1]. This assumption enables the protocol construction based on free distribution of the voting related information between the members. On the contrary, the consortiums where each voter does not know of the others, corresponds only with administrator(s), and wants his vote to be secret, should also be treated as meeting the demands of life.

The voting systems are in demand with the interaction of participants who have real-life relationships with each other, participating in information exchange, but making decisions from different economic backgrounds and interests. The arising task of reaching a consensus within the consortium is the basic for building vertical and horizontal integration of the interacting parties. In the case of vertical integration, interaction occurs along the value chain, when information about the object of economic activity is transmitted along the system, and in the horizontal, the creation of partner ecosystems that complement each other and create new, shared values. Such tasks arise in the real economy in many sectors: building a food chain distribution, energy exchange, trade in digital goods, loyalty systems, etc. When solving problems of exchange, it is necessary to take into account the speed of transactions, their confidentiality, resistance to errors and malicious distortions.

These aspects can be effectively incorporated in protocols which combine secret sharing and decentralized voting. In this regard, the Homomorphic Secret Sharing recently became a topic of intensive investigations [3]. In the present paper we treat such a protocol based on the Lagrange interpolant construction [2] (its brief description is given in Section 3).

The problem of our concern is that of potential error detection in some steps of the protocol. In Section 4 we treat it first as the one of the (systematic) error occurrence in the data set provided by a polynomial function. It turns out that under some assumptions on relationship between the number of potential errors and the redundancy in the correct values in the data set, the erroneous values can be detected. The algorithm is based on finding zero sets of specially constructed polynomials of the Hankel type.

2 Algebraic preliminaries: polynomial interpolation

The classical univariate polynomial interpolation problem over an infinite field, say $\mathbb{Q}$, is formulated as follows. Given the set of values for the variables x and y

$$\{(x_j, y_j)\}_{j=1}^{K} \subset \mathbb{Q}^2, \tag{1}$$

with distinct (nodes) $\{x_j\}_{j=1}^{K}$, find a polynomial $f(x)$ such that $\{f(x_j) = y_j\}_{j=1}^{K}$. If $\deg f \leq K-1$ then the problem has a unique solution which can be represented in several forms. Set

$$W(x) := \prod_{j=1}^{K}(x-x_j)\ , W_j(x) := \frac{W(x)}{x-x_j} \quad \text{for} \ \ j \in \{1,\dots,K\}\,.$$

Then the polynomial interpolant in Lagrange form is computed as

$$f(x) \equiv \sum_{j=1}^{K} y_j \frac{W_j(x)}{W_j(x_j)} \equiv \sum_{j=1}^{K} y_j \frac{W_j(x)}{W'(x_j)}\,. \tag{2}$$

Note that formula (2) does not provide one with the explicit representation for the coefficients of the interpolant

$$f(x) \equiv a_0 x^{K-1} + a_1 x^{K-2} + \dots + a_{K-1}\,. \tag{3}$$

For this aim, a further expansion of $\{W_j(x)\}_{j=1}^{K}$ in the powers of x is needed. This can be organized with the aid of special symmetric functions of the data set (1).

Theorem 1 (Euler, Lagrange). *For the polynomial $F(x) \in \mathbb{R}[x]$ with the leading coefficient equal to A_0, the following equalities are valid*

$$\sum_{j=1}^{K} \frac{F(x_j)}{W'(x_j)} = \begin{cases} 0 & if \ \ \deg F < K-1, \\ A_0 & if \ \ \deg F = K-1. \end{cases} \tag{4}$$

We now generate two sequences from the data set (1)

$$\sigma_\ell = \sum_{j=1}^{K} \frac{x_j^{K+\ell-1}}{W'(x_j)} \quad \text{for} \ \ \ell \in \{1,\dots,K\} \tag{5}$$

and

$$\tau_\ell = \sum_{j=1}^{K} y_j \frac{x_j^{\ell}}{W'(x_j)} \quad \text{for} \ \ \ell \in \{0,1,\dots\}\,. \tag{6}$$

Theorem 2. *The following formulas connect the values (5) and (6) with the coefficients of the interpolant:*

$$\tau_0 = a_0,\ \tau_\ell = a_0\sigma_\ell + a_1\sigma_{\ell-1} + \dots + a_{\ell-1}\sigma_1 + a_\ell \ \ \textit{for}\ \ell \in \{1,\dots,K-1\}\ .$$

Proof. It follows from (4)

$$\tau_\ell = \sum_{j=1}^{K} \frac{x_j^{\ell} y_j}{W'(x_j)} = \sum_{j=1}^{N} \frac{(a_0 x_j^{K-1} + a_1 x_j^{K-2} + \dots + a_\ell x_j^{K-\ell-1} + \dots + a_{K-1}) x_j^{\ell}}{W'(x_j)}$$
$$= a_0\sigma_\ell + a_1\sigma_{\ell-1} + \dots + a_{\ell-1}\sigma_1 + a_\ell\ .$$

□

Theorem 2 provides one with the procedure for computation the coefficients of the interpolant (3) recursively starting with that of the highest order of the variable. One can organize an alternative counterpart of this procedure starting the computations with the free term of the interpolant. For instance, one has

$$a_{K-1} = f(0) = (-1)^{K-1} \tau_{-1} \prod_{j=1}^{K} x_j \quad \text{where} \quad \tau_{-1} := \sum_{j=1}^{K} y_j \frac{1}{x_j W'(x_j)} \tag{7}$$

provided that $\{x_j \neq 0\}_{j=1}^{N}$.

The values (6) will be of use in Section 4 for the problem of the potential error detection in the data set (1). We will be also in need there of an auxiliary result evidently following from Theorem 1:

Corollary 1. *For the polynomial interpolant generated by the set (1) to be of the degree $k < K - 1$, it is necessary and sufficient that*

$$\tau_0 = 0, \dots, \tau_{K-k-2} = 0, \tau_{K-k-1} \neq 0\,. \tag{8}$$

3 Decentralized voting protocol

Assume that a consortium consists of $N > 2$ voters and $k > 2$ administrators. Every vote consists of two possible outcomes, either yes or no. In the ideal case, these results are delivered to administrator(s) and counted accordingly. However, in the real life, a particular administrator might corrupt the voting result. The aim is to make a voting scheme involving $k > 2$ administrators in which every particular one receives only a piece (a share) of information from every voter, while the result of the vote can be restored only from the whole collection of the administrators' receipts.

To organize the sharing, let the ℓth administrator generate a nonzero integer x_ℓ and makes it public for the consortium. The obtained k numbers $x_1, \dots, x_k$ should be distinct (otherwise, some of numbers should be replaced to avoid collisions).

At the same time, let the jth voter generate a polynomial of a degree $\leq k-1$ with arbitrary integer coefficients, except for the free term which is taken to be equal to $+1$ if he votes yes, and -1 otherwise. This polynomial is kept secret. Thus, the voters hold the system of polynomials

$$f_1(x), \dots, f_N(x) \tag{9}$$

such that $\{f_1(0), \dots, f_N(0)\} \subset \{-1, 1\}$ and the polynomial

$$F(x) := \sum_{j=1}^{N} f_j(x)$$

possesses a degree $\deg F \leq k - 1$ and the free term equal to the voting result of the consortium (number of votes yes minus number of votes no).

The next aim is to extract this result, i.e. to compute the polynomial $F(x)$ provided that its summands (9) are still kept secret.

Each voter computes the value of his polynomial at $x_1, \dots, x_k$ and communicates the obtained values to the corresponding administrators, i.e. the number $f_j(x_\ell)$ is sent off from the jth voter to the ℓth administrator.

Each administrator sums up the received values and makes the result public for the consortium members. Evidently one has

$$\{Y_\ell := \sum_{j=1}^{N} f_j(x_\ell) = F(x_\ell)\}_{\ell=1}^{k}\,, \tag{10}$$

and, therefore, the k values of the polynomial $F(x)$ become available to everybody interested in them. Since $\deg F(x) \le k-1$, the polynomial $F(x)$ is uniquely defined by these values, and the value $F(0)$, computed via (7), yields then the result of the vote.

What prevents the intention to falsify a share by the ℓth administrator? He is not able to definitely match the obtained share $f_j(x_\ell)$ with the voting result $f_j(0)$ and thereby looses motivation to forge the share.

We finally formulate two assumptions that ensure the trustworthy of the voting result.

Assumption 1. The shares $\{Y_\ell\}_{\ell=1}^{k}$ are assumed to be uncorrupted. Even if each administrator does not forge his share, it could be got wrong due to communication failures of the shares $\{f_j(x_\ell)\}$.

Assumption 2. The voters (and their shares $\{f_j(x_\ell)\}$) are assumed to be honest. Otherwise, if the jth one would generate a polynomial $\widetilde{f}_j(x)$ such that $\widetilde{f}_j(0) = +3$ and communicates then the values $\{\widetilde{f}_j(x_\ell)\}_{\ell=1}^{k}$ to the corresponding administrators, the voting result gets $+2$ extra votes yes.

We next intend to discuss whether it is possible to modify the voting scheme for the case where any of these assumptions is violated. For this aim, we rethink the polynomial interpolation problem.

4 Error detection in the data set

If the data set (1) is generated by a polynomial of a degree $k < K-1$ then it is redundant for computation of this polynomial. Any subset of the data set containing $k+1$ entries is sufficient for the polynomial restoration. One can establish its true degree on checking the conditions (8).

Suppose now that some of the values $y_1, \dots, y_N$ originally generated by a polynomial of a degree $k < K-1$ are corrupted, but we do know neither their amount nor their position. One may then expect that generically the degree of the interpolant formally constructed by (2) would be greater than k, and, therefore, some of the equalities (8) would be violated. This provides one with a sufficient condition for the existence of an error in the data set.

In order to locate the erroneous values, compute the values (6) and compose the following determinant

$$\mathcal{H}_L(x;\{\tau\}) := \begin{vmatrix} \tau_0 & \tau_1 & \tau_2 & \dots & \tau_L \\ \tau_1 & \tau_2 & \tau_3 & \dots & \tau_{L+1} \\ \vdots & \vdots & \vdots & & \vdots \\ \tau_{L-1} & \tau_L & \tau_{L+1} & \dots & \tau_{2L-1} \\ 1 & x & x^2 & \dots & x^L \end{vmatrix}_{(L+1)\times(L+1)} \tag{11}$$

for $L \in \mathbb{N}$. Expanding (11) by its last row, $\mathcal{H}_L(x;\{\tau\})$ can be represented as a polynomial in x which is sometimes referred to as the Lth **Hankel polynomial** generated by (6).

Example 1. The data set

x	-3	-2	-1	0	1	2	3	4	5
y	19	-2	-7	-8	3	14	37	35	107

is generated by a second order polynomial with the exception of some erroneous values. Construct the polynomials (11) and find outs whether their zeros belongs to the set $\{-3, -2, , \dots, 5\}$ or not.

Solution. Compute the values (6):

$$\tau_0 = \frac{1}{70},\ \tau_1 = \frac{53}{1680},\ \tau_2 = \frac{193}{1680},\ \tau_3 = \frac{47}{112},\ \tau_4 = \frac{407}{240},\ \tau_5 = \frac{11233}{1680}, \dots$$

The sequence of polynomials (11) starts as follows

$$\mathcal{H}_1(x;\{\tau\}) \equiv \frac{1}{70}x - \frac{53}{1680},\ \mathcal{H}_2(x;\{\tau\}) \equiv \frac{1823}{2822400}x^2 - \frac{6691}{2822400}x + \frac{29}{705600},$$

and these polynomials do not possess zeros in the desired set. The next polynomial does:

$$\mathcal{H}_3(x;\{\tau\}) \equiv \frac{33}{313600}(x+2)(x-1)(x-4)\,.$$

It turns out that the numbers $\{-2, 1, 4\}$ are the values of arguments where the given data set do not coincide with the set $\{(x_j, f(x_j))\}_{j=-3}^{5}$ where $f(x) := 4\,x^2 + 3\,x - 8$. Therefore, the polynomial $\mathcal{H}_3(x;\{\tau\})$ is the **error locator** one for the redundant but somewhere erroneous data set generated by $f(x)$. □

We reveal this trick in the proof of the following result where it is assumed that the number of erroneous values in the data set (1) equals E.

Theorem 3. *Let $E \in \{1, 2, \dots, \lfloor K/2 \rfloor - 1\}$ and $e_1, \dots, e_E$ be distinct numbers from $\{1, 2, \dots, K\}$. Let polynomial $f(x)$ be of a degree $k < K - 2E$. Let the data set satisfy the conditions*

(a) *$y_j = f(x_j)$ for $j \in \{1, \dots, K\} \setminus \{e_1, \dots, e_E\}$,*

(b) $\widehat{y}_{e_s} := f(x_{e_s}) \neq y_{e_s}$ *for* $s \in \{1, \dots, E\}$.

Then

$$\mathcal{H}_E(x; \{\tau\}) \equiv \frac{\displaystyle\prod_{s=1}^{E} (y_{e_s} - \widehat{y}_{e_s}) \prod_{1 \le s < t \le E} (x_{e_t} - x_{e_s})^2}{\displaystyle\prod_{s=1}^{E} W'(x_{e_s})} \prod_{s=1}^{E} (x - x_{e_s}) \, . \tag{12}$$

Proof. Assume, without loss of generality, that $\{e_s = s\}_{s=1}^{E}$. Denote

$$\theta_\ell := \sum_{s=1}^{E} \frac{\varepsilon_s x_s^\ell}{W'(x_s)} \qquad \text{where } \varepsilon_j := y_j - \widehat{y}_j \text{ for } \ j \in \{1, \dots, E\}, \ell \in \{0, 1, 2, \dots\} \, .$$

One has:

$$\tau_\ell = \sum_{s=1}^{E} \frac{\varepsilon_s x_s^\ell}{W'(x_s)} + \sum_{j=1}^{N} \frac{f(x_j) x_j^\ell}{W'(x_j)} \overset{(4)}{=} \theta_\ell \qquad \text{for } \ \ell \in \{0, \dots, N - n - 2\} \, .$$

Rewrite the expression for $\mathcal{H}_E(x; \{\tau\})$:

$$\mathcal{H}_E(x; \{\tau\}) \equiv \mathcal{H}_E(x; \{\theta\}) \equiv \left| \begin{array}{lllll} \theta_0 & \theta_1 & \dots & \theta_{E-1} & \theta_E \\ \theta_1 & \theta_2 & \dots & \theta_E & \theta_{E+1} \\ \vdots & \vdots & & \vdots & \vdots \\ \theta_{E-1} & \theta_E & \dots & \theta_{2E-2} & \theta_{2E-1} \\ 1 & x & \dots & x^{E-1} & x^E \end{array} \right| \, .$$

The set of zeros of this polynomial coincides with $\{x_1, \dots, x_E\}$. This follows from the equalities

$$\sum_{s=1}^{E} \frac{\varepsilon_s x_s^{\ell-1}}{W'(x_s)} \mathcal{H}_E(x_s; \{\theta\}) = \left| \begin{array}{lllll} \theta_0 & \theta_1 & \dots & \theta_{E-1} & \theta_E \\ \theta_1 & \theta_2 & \dots & \theta_E & \theta_{E+1} \\ \vdots & \vdots & & \vdots & \vdots \\ \theta_{E-1} & \theta_E & \dots & \theta_{2E-2} & \theta_{2E-1} \\ \theta_{\ell-1} & \theta_\ell & \dots & \theta_{\ell+E-2} & \theta_{\ell+E-1} \end{array} \right| = 0 \ \text{ for } \ \ell \in \{1, \dots, E\} \, .$$

These relationships compose the system of E homogeneous linear equations connecting the values $\{\mathcal{H}_E(x_s; \{\theta\})\}_{s=1}^{E}$. The determinant of this system

$$\det \left[\frac{\varepsilon_s x_s^{\ell-1}}{W'(x_s)} \right]_{\ell, s=1}^{E} = \frac{\displaystyle\prod_{s=1}^{E} \varepsilon_s}{\displaystyle\prod_{s=1}^{E} W'(x_s)} \det \left[x_s^{\ell-1} \right]_{\ell, s=1}^{E} = \frac{\displaystyle\prod_{s=1}^{E} \varepsilon_s \prod_{1 \le \ell < t \le E} (x_t - x_\ell)}{\displaystyle\prod_{s=1}^{E} W'(x_s)} \tag{13}$$

does not vanish due to the assumption **(b)** of the theorem. Therefore all the values $\{\mathcal{H}_E(x_s;\{\theta\})\}_{s=1}^E$ should be equal zero and

$$\mathcal{H}_E(x;\{\tau\}) \equiv C \prod_{s=1}^{E} (x-x_s)$$

for some constant $C \in \mathbb{R}$. It turns out that the expression for the leading coefficient of $\mathcal{H}_E(x;\{\theta\})$ looks similar to (13):

$$\left| \begin{array}{llll} \theta_0 & \theta_1 & \dots & \theta_{E-1} \\ \theta_1 & \theta_2 & \dots & \theta_E \\ \vdots & \vdots & & \vdots \\ \theta_{E-1} & \theta_E & \dots & \theta_{2E-2} \end{array} \right|$$

$$= \left| \begin{array}{cccc} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_E \\ \vdots & \vdots & & \vdots \\ x_1^{E-1} & x_2^{E-1} & \dots & x_E^{E-1} \end{array} \right| \cdot \left| \begin{array}{cccc} \dfrac{\varepsilon_1}{W'(x_1)} & 0 & \dots & 0 \\ & \dfrac{\varepsilon_2}{W'(x_2)} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \dfrac{\varepsilon_E}{W'(x_E)} \end{array} \right| \cdot \left| \begin{array}{cccc} 1 & x_1 & \dots & x_1^{E-1} \\ 1 & x_2 & \dots & x_2^{E-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_E & \dots & x_E^{E-1} \end{array} \right|$$

$$= \frac{\displaystyle\prod_{s=1}^{E} \varepsilon_s \prod_{1 \le \ell < t \le E} (x_t - x_\ell)^2}{\displaystyle\prod_{s=1}^{E} W'(x_s)} .$$

This concludes the proof of (12). □

Now we can come back to the problems stated in Section 3.

5 Administrators' faulty shares

We first treat the case where Assumption 1 from Section 3 is violated, i.e. some of the values (10) might be corrupted. Assume that the number of expected errors would not exceed some a priory agreed estimation E small enough compared with the total number of shares. To detect these errors in the framework of the results of Section 4, one should organize redundancy in the interpolation problem. This can be performed in two possible ways: either diminishing the degrees of the polynomials $\{f_j(x)\}$ generated by the voters or by increasing the number of administrators. The underlying mathematics for these alternatives is the same, and we restrict ourself with the treatment of the case where the number of administrators is now equal to K and $K > k-1 \ge \deg f_j(x) - 1$.

(A) Compute $\tau_0, \dots, \tau_{K-k-3}$ via (6). If all these numbers vanish, the errors are not detected.

(B) If any of these numbers is nonzero, an error is detected. Compute the sequence of polynomials $\mathcal{H}_1(x;\{\tau\}), \mathcal{H}_2(x;\{\tau\}), \dots$ via (11). For each non-identically zero polynomial $\mathcal{H}_L(x;\{\tau\})$ verify if its zero set is a subset of $\{x_1,\dots,x_K\}$.

(C) Let $\mathcal{H}_E(x;\{\tau\})$ with $E < \lfloor (K-k+1)/2 \rfloor$ be the first such a polynomial with $x_{e_1},\dots,x_{e_E}$ being its zeros. Remove the corresponding erroneous values $\{(x_{e_s}, Y_{e_s})\}_{s=1}^E$ from the set $\{(x_\ell, Y_\ell)\}_{\ell=1}^K$, and compute the value (7) for the remained subset. Take it as the voting result.

(D) If none of the polynomials $\mathcal{H}_1(x;\{\tau\}),\dots,\mathcal{H}_{\lfloor (K-k+1)/2 \rfloor -1}(x;\{\tau\})$ possesses the property from the point **(C)**, the number of erroneous values exceeds the allowable restriction and their location is not possible.

6 Voters' dishonest shares

How is it possible to verify the correctness of voters' decisions, namely that the numbers $f_1(0),\dots,f_N(0)$ belong to the set of acceptable values $\{+1,-1\}$? Collecting together all the shares $\{f_j(x_\ell)\}_{\ell=1}^k$ of the number $f_j(0)$ distributed between the administrators, the counting center would be able to restore this number. However, this procedure violates the confidentiality of voting.

The confidentiality would be maintained if the counting center is able to evaluate somehow $f_j^2(0)$ in the lack of the knowledge of $f_j(0)$. At the same time, the knowledge of $f_j^2(0)$ is enough for confirmation of the correctness of the jth voter ballot. Note that the number $f_j^2(0)$ can be made available via interpolation, i.e. via the data set composed of the pairs $(x_j, f_j^2(x_\ell))$ submitted by the administrators. The only problem is that the number of such pairs should increase twice compared with the degrees of the polynomials $f_j(x)$. This results in an additional demand to the redundancy, namely that the number K of administrators and degree $k-1$ of the exploited polynomials should be connected by the inequality $K \ge 2k-1$. Under this assumption, any number $f_j^2(0)$ is evaluated via (7).

7 Computational remarks

1. To avoid the round off errors, all the algorithms are built in $\mathbb{Z}_p$ for sufficiently large prime p. The only specifics of computation in $\mathbb{Z}_p$ is that the division operation by the involved integers should be interpreted as computation of inversion of these integers modulo p.

2. Each Hankel polynomial $\mathcal{H}_L(x;\{\tau\})$ over $\mathbb{Z}_p$ can always be represented with the sequence of coefficients with alternation in signs, i.e.

$$\mathcal{H}_L(x;\{\tau\}) \equiv_p c(x^L - b_1 x^{L-1} + b_2 x^{L-2} - \dots + (-1)^L b_L)$$

where $\{c, b_1, b_2, \dots, b_L\} \subset \{1,2,\dots,p-1\}$. If the values $\{x_j\}_{j=1}^K$ are positive integers, then the problem of resolving an algebraic equation over $\mathbb{Z}_p$ can be reduced to that of finding positive integer zeros for a polynomial with integer coefficients. The latter is resolved via checking the divisors of b_L.

3. There exists a procedure of computation of the sequence of Hankel polynomials $\{\mathcal{H}_L(x;\{\tau\})\}_{L\in\mathbb{N}}$ which is recursive in the order of these polynomials. Namely, three Hankel polynomials of the consecutive orders are linked by the identity in the form

$$\alpha\mathcal{H}_L(x;\{\tau\})-(x+\beta)\mathcal{H}_{L-1}(x;\{\tau\})+1/\alpha\mathcal{H}_{L-2}(x;\{\tau\})\equiv 0$$

Here α and β are some constants evaluated via the coefficients of $\mathcal{H}_{L-1}(x;\{\tau\})$ and $\mathcal{H}_{L-2}(x;\{\tau\})$. The related details can be found in [4].

8 Conclusion

The problem of error detection in the set of shares of decentralized voting protocol is resolved with the aid of an alternative solution of the classical polynomial interpolation problem.

In particular, the algorithm can be used to create close economic relationships among enterprise participants, taking advantage of its unique capabilities to form hierarchal (real-life) communications among nodes and guaranteeing security and flexibility in sharing data.

References

1. Lamport, L., Shostak, R. , Pease, M. The Byzantine Generals Problem, ACM T. Progr. Lang. Sys. **4** (3), 382–401 (1982)
2. Shamir, A. How to share a secret, Commun. ACM, **22** (11), 612-613 (1979)
3. Boyle, E. Gilboa, N., Ishai, Y. Breaking the circuit size barrier for secure computation under DDH, CRYPTO. 509–539 (2016)
4. Uteshev A.Yu., Baravy I. *Solution of interpolation problems via the Hankel polynomial construction.* arXiv: cs.SC/1603.08752 (2016).