UDC 621.394.147 Вестник СПбГУ. Прикладная математика. Информатика... 2019. Т. 15. Вып. 2
MSC 94A62

Faulty share detection in Shamir's secret sharing*

A. Yu. Uteshev[1], *A. V. Marov*[2]

[1] St. Petersburg State University, 7–9, Universitetskaya nab., St. Petersburg, 199034, Russian Federation
[2] RAIDIX, 33 (A), nab. reki Smolenki, St. Petersburg, 199178, Russian Federation

For citation: Uteshev A. Yu., Marov A. V. Faulty share detection in Shamir's secret sharing. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2019, vol. 15, iss. 2, pp. 274–282. https://doi.org/10.21638/11702/spbu10.2019.210

For Shamir's secret key sharing algorithm, we develop the procedure for detection of faulty shares. This procedure consists of the error locator polynomial construction for the data set $\{(x_j, y_j)\}_{j=1}^N$ with y values generated from x ones by a polynomial interpolant of a degree $n < N-1$ with possible occurrence of some errors. The error locator polynomial is sought out in the form of an appropriate Hankel polynomial

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

where $\tau_\ell := \sum_{j=1}^N y_j \frac{x_j^\ell}{W'(x_j)}$; $W(x) := \prod_{j=1}^N (x - x_j)$.

Keywords: Shamir's secret sharing, polynomial interpolation, Hankel polynomials, error correction.

1. Introduction. Let the secret integer number (key) S should be split into N pieces, i. e. integers $S_1, \dots, S_N$ (shares) should be created to be distributed between the N distinct members of some consortium (shareholders). The sharing should be organized in such a way that, for a given number $k < N$ (threshold), the key S can be restored from any subset of k shares $S_{i_1}, \dots, S_{i_k}$, but cannot be restored from a fewer number of shares. The secret S, as well as computation of its shares and their distribution between the consortium members, are entrusted to an honest dealer.

Several constructive schemes were suggested for the secret share management like, for instance, those based on multidimensional hyperplane intersection or Chinese Remainder Theorem. In the present paper we deal with Shamir's algorithm [1] based on solution of the polynomial interpolation problem. The classical univariate polynomial interpolation problem (over an infinite field, say $\mathbb{R}$) is formulated as follows. Given the data set of values for the variables x and y

$$\begin{array}{c|c|c|c|c} x & x_1 & x_2 & \dots & x_N \\ \hline y & y_1 & y_2 & \dots & y_N \end{array}, \quad \{x_j, y_j\}_{j=1}^N \subset \mathbb{R}, \tag{1}$$

* This work is supported by the Russian Foundation for Basic Research (project N 17-29-04288).

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

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

Then interpolation polynomial in Lagrange form is computed as

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

In Shamir's algorithm, to share the secret key S, the dealer first chooses an arbitrary prime number $p > S$, $p \gg n$ and constructs arbitrary polynomial over $\mathbb{Z}_p$:

$$f(x) := S + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}, \quad \{a_1, \dots, a_{k-1}\} \subset \{0, 1, \dots, p-1\}. \tag{3}$$

Next he enumerates the members of the consortium by consecutive integers $1, 2, \dots, n$ and supplies the j-th of them with the value $y_j := f(j) \pmod p$, with this value treated as the j-th share of the secret value S. To restore the secret S, the shareholders needs to collect at least k pares (j, y_j). Lagrange formula (2) computes the polynomial (3) modulo p; its free term coincides with S. The only specifics of computation in $\mathbb{Z}_p$ is that the division operation by the integers involved in (2) should be interpreted as computation of inversion of these integers modulo p.

The algorithm fails if one of the shares is corrupted (accidentally or intentionally) either in transmission or at storage. Assuming that the number of uncorrupted shares exceeds that of corrupted ones, is it possible to restore the secret S? We will demonstrate that the answer is positive if some redundancy in the number of true shares over false ones can be guaranteed.

2. Error detection in interpolation table. In the present section we detail the algorithm of error location dealing with the interpolation problem over $\mathbb{R}$, while in the next one it is modified for $\mathbb{Z}_p$.

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*:

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

If the data set (1) is generated by a polynomial of a degree $n < N-1$ then the set is redundant for computation of this polynomial. Any subset of the data set containing $n+1$ entries is sufficient for the polynomial restoration.

Define the sequences of symmetric functions from the data set (1):

$$\tau_\ell := \sum_{j=1}^{N} y_j \frac{x_j^\ell}{W'(x_j)} \quad \text{for} \quad \ell \in \{0, 1, \dots\}. \tag{5}$$

The following result is a trivial consequence of theorem 1.

Theorem 2. *If the data set* (1) *is generated by a polynomial of a degree $n < N-1$, then*

$$\tau_0 = 0, \dots, \tau_{N-n-2} = 0, \tau_{N-n-1} \neq 0. \tag{6}$$

Suppose now that some of the values $y_1, \dots, y_N$ generated by a polynomial of a degree $n < N-1$ 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 n, and, therefore, some of equalities (6) 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, generate by (5) the two sequences of *Hankel determinants*:

$$H_L(\{\tau\}) := \det\left[\tau_{i+j-2}\right]_{i,j=1}^{L} = \begin{vmatrix} \tau_0 & \tau_1 & \tau_2 & \dots & \tau_{L-1} \\ \tau_1 & \tau_2 & \tau_3 & \dots & \tau_L \\ \vdots & \vdots & \vdots & & \vdots \\ \tau_{L-1} & \tau_L & \tau_{L+1} & \dots & \tau_{2L-2} \end{vmatrix}_{L\times L}$$

and

$$\mathcal{H}_L(x;\{\tau\}) := \det\left[\tau_{i+j-2}x - \tau_{i+j-1}\right]_{i,j=1}^{L}$$

for $L \in \mathbb{N}$. The last determinant can be represented in an alternative form as

$$\mathcal{H}_L(x;\{\tau\}) \equiv \begin{vmatrix} \tau_0 & \tau_1 & \tau_2 & \dots & \tau_L \\ \tau_1 & \tau_2 & \tau_3 & \dots & \tau_{L+1} \\ \vdots & \vdots & \vdots & & \vdots \\ \tau_{L-1} & \tau_L & \tau_{L+1} & \dots & \tau_{2L-1} \\ 1 & x & x^2 & \dots & x^L \end{vmatrix}_{(L+1)\times(L+1)} \tag{7}$$

and is sometimes referred to as the L-th *Hankel polynomial* generated by (5).

Example 1. The data set

x	-2	$\mathbf{-1}$	0	1	2	3	4
y	30	$\mathbf{12}$	8	9	18	35	60

is generated by the polynomial $f(x) = 4\,x^2 - 3\,x + 8$ with the exception of a single erroneous value at the node $x_2 = -1$. The sequence of polynomials (7) is as follows:

$$\mathcal{H}_1(x;\{\tau\}) \equiv \frac{1}{40}(x+1), \quad \mathcal{H}_2(x;\{\tau\}) \equiv 0, \quad \mathcal{H}_3(x;\{\tau\}) \equiv -\frac{2}{5}(x+1), \dots$$

and one may watch the expression for the error position as a zero of both polynomials $\mathcal{H}_1(x;\{\tau\})$ and $\mathcal{H}_3(x;\{\tau\})$. □

Theorem 3. *Let $e \in \{1, 2, \dots, N\}$. Let the polynomial $f(x) = a_0 x^n + \dots + a_n$ be of a degree $n < N-2$. Let the data set* (1) *satisfy the conditions*

(a) $y_j = f(x_j)$ *for* $j \in \{1, \dots, N\} \setminus \{e\}$,

(b) $\widehat{y}_e := f(x_e) \neq y_e$,

then

$$\mathcal{H}_1(x;\{\tau\}) \equiv \frac{(y_e - \widehat{y}_e)}{W'(x_e)}(x - x_e)\,. \tag{8}$$

P r o o f. We assume $x_e = x_1$ and set $\varepsilon := y_1 - \widehat{y}_1$. With the aid of (4), one obtains

$$\tau_\ell = \frac{x_1^\ell y_1}{W'(x_1)} + \frac{x_2^\ell y_2}{W'(x_2)} + \dots + \frac{x_N^\ell y_N}{W'(x_N)} =$$

$$= \left(\frac{x_1^\ell \widehat{y}_1}{W'(x_1)} + \frac{\varepsilon x_1^\ell}{W'(x_1)} \right) + \frac{x_2^\ell y_2}{W'(x_2)} + \cdots + \frac{x_N^\ell y_N}{W'(x_N)} =$$

$$= \sum_{j=1}^{N} \frac{f(x_j) x_j^\ell}{W'(x_j)} + \frac{\varepsilon x_1^\ell}{W'(x_1)} = \frac{\varepsilon x_1^\ell}{W'(x_1)} \quad \text{for} \quad \ell \in \{0, 1\}\,.$$

Thus,

$$\mathcal{H}_1(x; \{\tau\}) \equiv \begin{vmatrix} \tau_0 & \tau_1 \\ 1 & x \end{vmatrix} \equiv \begin{vmatrix} \varepsilon / W'(x_1) & \varepsilon x_1 / W'(x_1) \\ 1 & x \end{vmatrix} = \frac{\varepsilon}{W'(x_1)} (x - x_1)\,,$$

and (8) is proved. □

We now turn to the case of the occurrence of several errors in the data set. We denote the number of erroneous values by E.

Example 2. The data set

x	-2	$\mathbf{-1}$	0	1	$\mathbf{2}$	3	4
y	30	$\mathbf{-7}$	8	9	$\mathbf{11}$	35	60

is generated by the polynomial $f(x) := 4\,x^2 - 3\,x + 8$ with the exception of two erroneous values at $x_2 = -1$ and $x_5 = 2$. The sequence of polynomials (7) is as follows:

$$\mathcal{H}_1(x; \{\tau\}) \equiv \frac{1}{80}(3\,x + 38), \quad \mathcal{H}_2(x; \{\tau\}) \equiv -\frac{77}{320}(x + 1)(x - 2), \ldots$$

and this time the erroneous nodes are detected as the zeros of the polynomial $\mathcal{H}_2(x; \{\tau\})$. □

Theorem 4. *Let $E \in \{2, 3, \ldots, \lfloor N/2 \rfloor - 1\}$ and $e_1, \ldots, e_E$ be distinct numbers from $\{1, 2, \ldots, N\}$. Let polynomial $f(x)$ be of a degree $n < N - 2E$. Let the set* (1) *satisfy the conditions*

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

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

then

$$\mathcal{H}_E(x; \{\tau\}) \equiv \frac{\displaystyle\prod_{s=1}^{E} (y_{e_s} - \widehat{y}_{e_s}) \prod_{1 \leqslant s < t \leqslant E} (x_{e_t} - x_{e_s})^2}{\displaystyle\prod_{s=1}^{E} W'(x_{e_s})} \prod_{s=1}^{E} (x - x_{e_s})\,. \tag{9}$$

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

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

Represent the expression for τ_ℓ in the form

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

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

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

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

$$\sum_{s=1}^{E} \frac{\varepsilon_s x_s^{\ell-1}}{W'(x_s)} \mathcal{H}_E(x_s;\{\theta\}) = \begin{vmatrix} \theta_0 & \theta_1 & \dots & \theta_{E-1} & \theta_E \\ \theta_1 & \theta_2 & \dots & \theta_E & \theta_{E+1} \\ \vdots & \vdots & & \vdots & \vdots \\ \theta_{E-1} & \theta_E & \dots & \theta_{2E-2} & \theta_{2E-1} \\ \sum\limits_{s=1}^{E} \frac{\varepsilon_s x_s^{\ell-1}}{W'(x_s)} & \sum\limits_{s=1}^{E} \frac{\varepsilon_s x_s^{\ell}}{W'(x_s)} & \dots & \sum\limits_{s=1}^{E} \frac{\varepsilon_s x_s^{\ell+E-2}}{W'(x_s)} & \sum\limits_{s=1}^{E} \frac{\varepsilon_s x_s^{\ell+E-1}}{W'(x_s)} \end{vmatrix} =$$

$$= \begin{vmatrix} \theta_0 & \theta_1 & \dots & \theta_{E-1} & \theta_E \\ \theta_1 & \theta_2 & \dots & \theta_E & \theta_{E+1} \\ \vdots & \vdots & & \vdots & \vdots \\ \theta_{E-1} & \theta_E & \dots & \theta_{2E-2} & \theta_{2E-1} \\ \theta_{\ell-1} & \theta_\ell & \dots & \theta_{\ell+E-2} & \theta_{\ell+E-1} \end{vmatrix} = 0 \quad \text{for} \quad \ell \in \{1,\dots,E\}.$$

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

$$\det\left[\frac{\varepsilon_s x_s^{\ell-1}}{W'(x_s)}\right]_{\ell,s=1}^{E} = \frac{\prod\limits_{s=1}^{E}\varepsilon_s}{\prod\limits_{s=1}^{E} W'(x_s)} \det\left[x_s^{\ell-1}\right]_{\ell,s=1}^{E} = \frac{\prod\limits_{s=1}^{E}\varepsilon_s \prod\limits_{1\leqslant \ell<t\leqslant E}(x_t-x_\ell)}{\prod\limits_{s=1}^{E} W'(x_s)} \tag{10}$$

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 (10):

$$\begin{vmatrix} \theta_0 & \theta_1 & \dots & \theta_{E-1} \\ \theta_1 & \theta_2 & \dots & \theta_E \\ \vdots & \vdots & & \vdots \\ \theta_{E-1} & \theta_E & \dots & \theta_{2E-2} \end{vmatrix} = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_E \\ \vdots & \vdots & & \vdots \\ x_1^{E-1} & x_2^{E-1} & \dots & x_E^{E-1} \end{vmatrix} \times$$

$$\times \begin{vmatrix} \varepsilon_1/W'(x_1) & 0 & \dots & 0 \\ & \varepsilon_2/W'(x_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \varepsilon_E/W'(x_E) \end{vmatrix} \cdot \begin{vmatrix} 1 & x_1 & \dots & x_1^{E-1} \\ 1 & x_2 & \dots & x_2^{E-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_E & \dots & x_E^{E-1} \end{vmatrix} =$$

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

This concludes the proof of (9). □

The upper bound for the number of potential errors in the data set (1) from theorem 4 should be considered as a tight one. This claim is demonstrated by the following example.

Example 3. The occurrence of three errors in the data set

x	-2	$\mathbf{-1}$	0	1	$\mathbf{2}$	$\mathbf{3}$	4
y	30	$\mathbf{-7}$	8	9	$\mathbf{11}$	$\mathbf{-1}$	60

generated by the polynomial $f(x) := 4\,x^2 - 3\,x + 8$ does not permit one to uniquely restore this polynomial. Indeed, the faulty table can be interpreted as the one obtained from

x	-2	-1	0	1	2	3	4
y	-31	-7	8	14	11	-1	-22

originated by the polynomial $f_1(x) := -9/2\,x^2 + 21/2\,x + 8$ and further corrupted in the values $f_1(-2)$, $f_1(1)$ and $f_1(4)$. □

R e m a r k 1. The developed approach for the error detection has a definite relationship to Coding Theory and specifically to the *Berlekamp—Welch algorithm* for error correction in Reed—Solomon codes [2]. In the framework of this algorithm, the polynomial (9) is referred to as the *error locator polynomial*, and is found via the solution of the *rational interpolation problem* for the data set (1). In the papers [3, 4] the Jacobi's approach for resolving the rational interpolation problem is developed consisting in independent computation of numerator and denominator of the interpolant. Computation of the error locator polynomial (9) via its representation in the Hankel polynomial form (7) is a part of that algorithm.

We conclude the present section with two extra results that aim to optimize the computational aspects of the suggested algorithm. Their proofs and further related references can be found in [3, 4].

Theorem 5. *Let the conditions of theorem 4 be fulfilled. If* $n := \deg f < N - 2E - 1$, *then*

$$\mathcal{H}_{N-n-E-1}(x; \{\tau\}) \equiv C\mathcal{H}_E(x; \{\tau\})$$

for some constant $C \neq 0$. *If* $n < N - 2E - 2$, *then*

$$\mathcal{H}_{E+1}(x; \{\tau\}) \equiv 0, \dots, \mathcal{H}_{N-n-E-2}(x; \{\tau\}) \equiv 0\,.$$

The polynomial $\mathcal{H}_L(x; \{\tau\})$ should be interpreted as a *suspicious* to be the error locator one if the polynomial $\mathcal{H}_{L+1}(x; \{\tau\})$ is identically zero or coincides with $\mathcal{H}_L(x; \{\tau\})$ up to a numerical factor. Example 1 demonstrates this effect.

For a small number of expected errors, computation of the sequence of Hankel polynomials required for their detection, does not cause difficulties. As for the larger orders, one might expect that the algebraic time complexity for the computation of a parameter dependent determinant (7) is as great as that for the characteristic polynomial of the integer matrix, i. e. $\mathcal{O}(\mathfrak{n}^3)$ (with $\mathfrak{n}$ standing for the length of input). Fortunately, the Hankel structure of the determinant (7) allows one to diminish this estimation. Represent the L-th Hankel polynomial generated by any sequence $\{c\} = \{c_0, c_1, \dots, \}$ in canonical form

$$\mathcal{H}_L(x;\{c\}) \equiv h_{L0}x^L + h_{L1}x^{L-1} + \cdots + h_{LL} \quad \text{with} \quad h_{L0} = H_L(\{c\})\,.$$

Theorem 6. *Any three consecutive Hankel polynomials*

$$\mathcal{H}_{L-2}(x;\{c\}),\ \mathcal{H}_{L-1}(x;\{c\}),\ \mathcal{H}_L(x;\{c\})$$

are connected by the identity

$$H_L^2\mathcal{H}_{L-2}(x;\{c\}) + (H_Lh_{L-1,1} - H_{L-1}h_{L1} - H_LH_{L-1}x)\,\mathcal{H}_{L-1}(x;\{c\}) + \\ + H_{L-1}^2\mathcal{H}_L(x;\{c\}) \equiv 0\,. \tag{11}$$

In the case $H_{L-1} \neq 0$, the identity (11) reduces the computation of $\mathcal{H}_L(x;\{c\})$ to that of $\mathcal{H}_{L-1}(x;\{c\})$ and $\mathcal{H}_{L-2}(x;\{c\})$. Similar statement is also valid for the constants involved in (11), i. e. they can be expressed via the coefficients of those polynomials:

$$\begin{cases} h_{L0} = H_L &= c_{L-1}h_{L-1,L-1} + c_Lh_{L-1,L-2} + \cdots + c_{2L-2}h_{L-1,0}\,, \\ h_{L1} &= -(c_Lh_{L-1,L-1} + c_{L+1}h_{L-1,L-2} + \cdots + c_{2L-1}h_{L-1,0})\,. \end{cases}$$

Thus, the complexity of the recursive procedure for computing the sequence of Hankel polynomials can be estimated as $\mathcal{O}(\mathfrak{n}^2)$.

3. Error detection in the sequence of shares.

Example 4. Let the secret key $S = 1234$ has been distributed between $N = 7$ shareholders with $k = 3$ threshold. The dealer set $p = 2017$ and generated the shares

$$\{y_j = f(j) \pmod p\}_{j=1}^7 \quad \text{with} \quad f(x) := 1234 + 271\,x + 82\,x^2\,.$$

However, later on, the attempts to restore the secret via the selection of several distinct triples of the consortium shareholders fail. On collecting together all the shares the result is as follows:

j	1	2	3	4	5	6	7
y	1587	350	768	1613	605	778	1098

Under assumption that the number of faulty shares does not exceed 2, detect them and restore the secret S.

Solution. Due to the claim of theorem 4, to correct up to 2 potential errors in the table, it is sufficient to compute 4 numbers τ_j. We first perform the computations with rational numbers and at the final stage convert them to integers. Since the values

$$\tau_0 = -\frac{3937}{180},\quad \tau_1 = -\frac{1801}{18},\quad \tau_2 = -\frac{38333}{90},\quad \tau_3 = -\frac{79132}{45}$$

are non zero, theorem 2 indicates the presence of error in the given data set. To locate them, we compute Hankel polynomials (7). The polynomial

$$\mathcal{H}_1(x;\{\tau\}) = \frac{1}{180}(-3937\,x + 18010) \equiv_p 1199(-3937\,x + 18010) \equiv_p 1334\,x - 12$$

does not have zeros in $\{1, \dots, 7\}$. Next polynomial

$$\mathcal{H}_2(x;\{\tau\}) \equiv_p 156\,x^2 + 769\,x + 1872 \equiv_p 156(x^2 + 2009\,x + 12) \equiv_p 156(x-2)(x-6)$$

possesses two zeros in this set. Therefore, the shares corresponding to $j = 2$ and $j = 6$ should be considered as erroneous. Taking any three of the five remained values for j, one can restore the polynomial $f(x)$. □

R e m a r k 2. As a matter of fact, to restore S from the subset of true shares, we are in need of solely the free term of the corresponding interpolation polynomial. It is worth mentioning that it directly relates to the values (5). For instance, in the case of reliability of the whole data set (1), from (2) it evidently follows the equality

$$f(0) = (-1)^{N-1}\tau_{-1}\prod_{j=1}^{N} x_j$$

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

If the error locator polynomial is of a degree E then its canonical form modulo p can always be chosen with the sequence of coefficients with alternation in signs, i. e.

$$\mathcal{H}_E(x;\{\tau\}) \equiv_p c(x^E - b_1x^{E-1} + b_2x^{E-2} - \cdots + (-1)^E b_E)\,,$$

where $\{c, b_1, b_2, \ldots, b_E\} \subset \{1, 2, \ldots, p-1\}$. This permits one to reduce the problem of resolving an algebraic equation over $\mathbb{Z}_p$ to that of finding positive integer zeros for a polynomial with integer coefficients. The latter is resolved via checking the divisors of b_E.

4. Conclusion. We have suggested an approach for the detection of faulty shares in Shamir's secret sharing scheme. The developed algorithm might be useful in the decentralized voting protocol management.

The authors thank the referees for valuable suggestions that helped to improve the quality of the paper.

References

1. Shamir A. How to share a secret. *Communications of the ACM*, 1979, vol. 22 (11), pp. 612–613. doi:10.1145/359168.359176

2. Welch L. R., Berlekamp E. R. *Error correction for algebraic block codes.* US Patent N 4 633 47, Dec. 30, 1986. Available at: https://patentscope.wipo.int/search/en/detail.jsf?docId=US37599078 (accessed: 10.01.2019).

3. Uteshev A. Yu., Baravy I. *Solution of interpolation problems via the Hankel polynomial construction.* arXiv: cs.SC/1603.08752. 2016. Available at: https://arxiv.org/abs/1603.08752 (accessed: 10.01.2019).

4. Uteshev A. Yu., Baravy I. Solution of the rational interpolation problem via the Hankel polynomial construction. *Vestnik of Saint Peterburgs University. Series 10. Applied Mathematics. Computer Science. Control Processes*, 2016, iss. 4, pp. 31–43.

Received: January 30, 2019.
Accepted: March 15, 2019.

A u t h o r's i n f o r m a t i o n:

Alexei Yu. Uteshev — Dr. Sci. in Physics and Mathematics, Professor; a.uteshev@spbu.ru

Aleksei V. Marov — Marov.A@raidix.com

Обнаружение ошибок в схеме Шамира разделения секрета*

А. Ю. Утешев [1], *А. В. Маров* [2]

[1] Санкт-Петербургский государственный университет, Российская Федерация,
199034, Санкт-Петербург, Университетская наб., 7–9
[2] RAIDIX, Российская Федерация,
199178, Санкт-Петербург, наб. реки Смоленки, 33 (А)

Для цитирования: *Uteshev A. Yu., Marov A. V.* Faulty share detection in Shamir's secret sharing // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2019. Т. 15. Вып. 2. С. 274–282.
https://doi.org/10.21638/11702/spbu10.2019.210 (In English)

Для схемы Шамира разделения секрета предлагается процедура обнаружения ошибочных долей секрета. Разработан алгоритм построения полинома локаторов ошибок для набора данных $\{(x_j, y_j)\}_{j=1}^{N}$, в котором значения y_j, изначально генерируемые из x_j посредством полиномиального интерполянта степени $n < N-1$, подвергаются частичным искажениям. Полином локаторов ошибок строится в виде подходящего ганкелевого полинома

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

при $\tau_\ell := \sum_{j=1}^{N} y_j \dfrac{x_j^\ell}{W'(x_j)}$, $W(x) := \prod_{j=1}^{N}(x - x_j)$.

Ключевые слова: схема Шамира разделения секрета, полиномиальная интерполяция, ганкелевы полиномы, исправление ошибок.

Контактная информация:

Утешев Алексей Юрьевич — д-р физ.-мат. наук, проф.; a.uteshev@spbu.ru

Маров Алексей Валерьевич — Marov.A@raidix.com

* Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 17-29-04288).