# Application of hierarchic authentication to isogenies of elliptic curves for providing safety of data routing in the systems of analysis of digital production traffic[a]

*Elena* Alexandrova[1], *Maria* Poltavtseva[1*], and *Anastasia* Yarmak[1]

[1]Peter the Great St. Petersburg Polytechnic University, Institute of Computer Sciences and Technologies, 195251 Polytechnicheskaya st. 29, Russian Federation

**Abstract.** The article discusses the peculiarities of the process of information routing in the course of acquisition and processing big data of digital production, including systems of traffic analysis. Such a specific features variability of physical nodes-processors with the retention of functional stringency of order of information processing is distinguished. Inordertoprovidesafetyofthedescribedprocessofinformationprocessingand possibility of restoration of a chain of processing every fragment of data, the authors offer a protocol of hierarchic authentication developed thereby on isogenies of elliptic curves. The work includes algorithms of shaping parameters, generation of keys, generation and checking signature. The evaluation of signature stability again basic types of attacks has been performed. A solution offered by the authors can be used both in traditional and, in future, in quantum systems. A simulation of corresponding signature dimensions has been performed in the work.

## 1 Introduction

A current development of industrial manufacture, "the 4th industrial revolution" [1] and computerization of production processes have brought about a necessity of occurrence of unique information systems encompassing activity of enterprises and organizations from management of physical objects to business processes [2]. They are based on a set of new solutions, both in the field of element base (quick controllers, data processing centers, in future – quantum computation equipment), and in the field of software (virtualization, cloud technologies, analytical systems, big data processing systems).

According to current analytical and industrial investigations the big data technologies are one of the main technologies making a basis of digital production. They appear as one

[a] With financial support from the Ministry of Education and Science of the Russian Federation in the framework of the Federal targeted program "Investigations and developments in the priority field of development of Russian science and technology complex for 2014-2020", Agreement No. 14.578.21.0231, agreement unique identifier RFMEFI57817X0231)

[*]Corresponding author: poltavtseva@ibks.spbstu.ru

of fundamentals of digital economics both in private [3], and in state [4] sources. From the point of view of informational safety the big data systems of digital production take on two roles:

1) as an instrument of protection strategy implementation;
2) as an object of ensuring safety.

In the first case the big data technology is used for providing security of digital economics system as a whole. The assessment of security of big heterogeneous system of digital production requires analysis of a great number of poorly structured parameters correlated with different management levels (physical level, SCADA level, corporate network level, etc.). The analysis of traffic of highway network with the aim of revealing intrusions can be used as an example of such application. This, generally speaking, private task of security analysis already requires processing of terabytes and petabytes of information.

In the second case it is referred to security of the transferred data proper, ensuring confidentiality of processing thereof. The digital production contemplates enormous volumes of transferred data from the parameters and indicators of sensors to confidential documentation. Not only the places of origin, processing and final use of such sort of information are mutually spaced from one another logically and geographically, but some individual steps too, such as processing and storage of information encompass a plurality of heterogeneous computation nodes [5].

At that it is important that the data of systems of ensuring security shall be protected in the same way, if not more than the other data. The influence of ill-minded person on the system of providing informational security and detecting intrusions throw into question a possibility of its application as a whole. Therefore, a relevant task consists in the development of means of enhancing security of systems of big data processing taking into account the prospects of technologies development.

## 2. Specific features of data routing in the course of acquisition and processing thereof in digital production systems

The traditional components of architectures of analytical systems mixing takes place in the up-to-date big data systems, including systems of processing network traffic. The classical analysis includes sequentially: data sources; components of extraction and conversion; components of storage; sampling, restructuring and delivery; presentations of data and information receivers in the form of analysts or business proposals. The modern architectures make it possible to distinguish three architectural layers:

1. Data sources.
2. Heterogeneous environment of data transfer and processing.
3. Data consumers.

The components of processing, such as conversion, storage, restructuring, etc. appear to be distributed between these layers (Fig. 1), at that, a distribution can differ depending on architecture of a particular system.

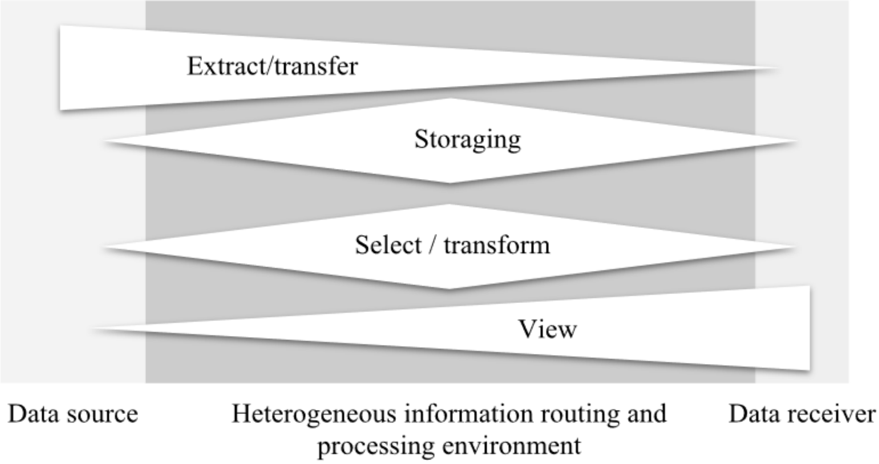

**Fig. 1.** Distribution of data processing components.

Such a distribution contemplates information processing at different stages with the use of distributed nodes and systems, when the movement of a particular information fragment with respect to computation system can differ depending on a great number of parameters, such as:

- data source;
- data type;
- temporary data characteristics;
- work load of different fragments of information transmission network;
- work load of computation nodes

and others. Since the source and type of data are not the only determining factors for forming a route, it is impossible to forecast in advance, where particularly, at what particular nodes they are going to be processed. A variability of routes of processing information is shown in Fig. 2.

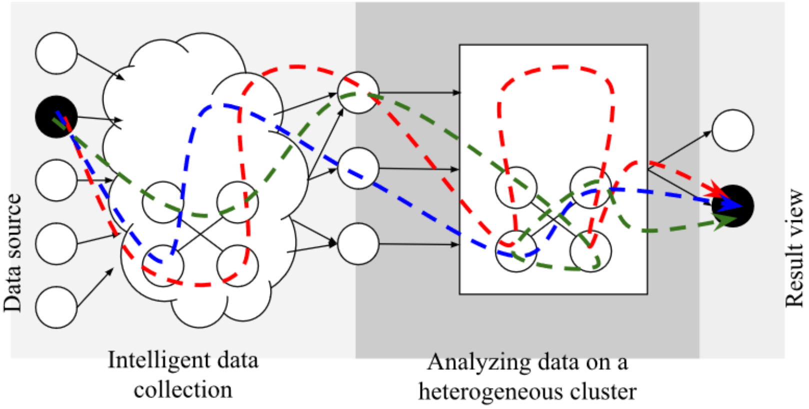
Data source
Intelligent data collection
Analyzing data on a heterogeneous cluster
Result view

**Fig. 2.**Variability of routes of processing information of one source.

The highway routers can come forward as a source of data in the systems of traffic analysis, while a client part of SIEM system of security analysis will come forward as a receiver [6]. The source and receiver of data in Fig. 2 are highlighted in black color, different paths of information routing between them in the course of processing are shown. In this case the system of traffic analysis features the following peculiarities:

1. Data processing takes place according to a predetermined diagram, set of functionally type-safe nodes on the basis of data-driven approach.
2. Number of functional types of processor nodes is countable and small.
3. Particular physical processor node can differ for every data fragment.

In other words, the typical set of processor nodes does not depend on the system characteristics, but on the initial data only (e.g., whether the information was fragmented or not), and features low variability. Thus, in order to provide for security of such sort of system from influence in the chain of processing data of external nodes, it is necessary to have a possibility to establish the entire chain of processors (both ideological and physical). In order to do so, the authors suggest using a mechanism of hierarchical digital signature. The following can be referred to as the requirements to a signature:

1. Possibility of tracing an entire chain of data processing.
2. Applicability of the offered algorithm of hierarchical signature with the advanced solutions of element base (in particular, with quantum calculations).

In order to attain these requirements, the authors suggest using a hierarchical authentication on isogenies of elliptic curves.

# 3. Hierarchical authentication on isogenies of elliptic curves

## 3.1. Authentication in classical and quantum systems

As of today there exist several classes of cryptographic systems presumably resistant to attacks on quantum computer:

1. Patterns of signature based on hash functions (pattern of signature of Merkle [7], Lemport [8], et al.).
2. Encryption schemes based on coding theory (cryptosystems of Mac-Elis [9], Niederwriter [10], et al.).
3. Cryptosystems based on noncommutative groups [11], e.g., braid groups, polycyclic groups, etc.
4. Cryptosystems based on grids (e.g., NTRU [12]).

The significant drawbacks obstructing the use of such systems in practice is a big size of the signature and cryptotext as well as low rate of data conversion as compared with the well-known classical cryptographic systems. The rapidly advancing technologies in the field of quantum calculations on the one hand, make it possible to increase the calculations rate, while on the other hand, they can endanger the available cryptosystems with an open key, which security is based, as a rule, on factorization task and calculation task of discrete logarithm in the cyclic group of elementary order. After invention of quantum computer these tasks can be solved during multinomial time by means of P. Shore algorithm. Therefore, it is necessary to use the other mathematical structures and build new protocols, which could remain relevant in case of inventing quantum computer of sufficiently big digit capacity.

The use of isogenies as the main mathematical structure gives a chance to design different diagrams: key derivation protocols, evidences with zero footprints, encryption with an open key, electronic digital signature (impossible-to-deny signal, blind signature) have been proposed as of today. However, as of the present moment there are no known examples of using isogenies for building diagrams of hierarchical authentication.

The application of rank-order digital signature makes it possible to solve a problem of creating signature on behalf of several entities and monitor the order of procedure of forming a message signature, providing by the same hierarchical authentication taking into account the structure of the group itself.

It is necessary to take into account a number of requirements, when developing a diagram of rank-order signature, in particular, the length of signature shall be invariable with respect to dimensionality of the group of signatories, while a check of the signature shall be simplified as much as possible demanding no verification of a chain of all signatures of the group participants.

## 3.2. Hierarchical Authentication on Isogeny of Elliptic Curves

Let us assume that $E(\mathbb{F}_{p^2})$ is a supersingular elliptic curve, where, $p = l_A^{e_A} l_B^{e_B} f \pm 1$,$< P_A, Q_A > \ = E\left[l_A^{e_A}\right]$, $< P_B, Q_B > \ = E[l_B^{e_B}]$. A unique isogeny $\varphi$: $E \rightarrow E'$ with nucleus $R$exists for curve $E$and finite subgroup $R \subset E$. Let us designate $E^{'} = \varphi(E) = E/< R >$. The following computationally complex assumptions are used when building protocols on isogenies of supersingular curves [13].

*Decisional Supersingular Isogeny (DSSI) problem*: Let us assume that $E_A(\mathbb{F}_{p^2})$ is the other supersingular curve. Make definite, whether curves $E_A$ and $E$ are connected by isogeny of degree $l_A^A$.

*Computational Supersingular Isogeny (CSSI) problem:*Let us assume that $\varphi_A: E \rightarrow E_A$ is isogeny with nucleus$< R_A >$, where $R_A \in_R E, \# < R_A > = l_A^{e_A}$. Use data $E_A$, $\varphi_A(P_B)$, $\varphi_A(Q_B)$ to find generatrix $< R_A >$of isogeny nucleus$\varphi_A$.

*Supersingular Computational Diffie–Hellman (SSCDH) problem:* Let us assume that $\varphi_A: E \rightarrow E_A$ is isogeny with nucleus$< m_A P_A + n_A Q_A >$,$\varphi_B: E \rightarrow E_B$ is isogeny with nucleus$< m_B P_B + n_B Q_B >$, where $m_A, n_A$ $(m_B, n_B)$ are random normal numbers of $\mathbb{Z}/\ l_A^{e_A}\mathbb{Z}$ (accordingly $\mathbb{Z}/\ l_B^{e_B}\mathbb{Z}$), not divisible by $l_A^{e_A}$(accordingly $l_B^{e_B}$). Use these curves $E_A$, $E_B$ as well as points $\varphi_A(P_B)$, $\varphi_A(Q_B)$,$\varphi_B(P_A)$, $\varphi_B(Q_A)$ to find *j*-invariant of a curve $E/\ < m_A P_A + n_A Q_A, m_B P_B + n_B Q_B >$.

*Supersingular Decision Diffie–Hellman (SSDDH) problem:* Having data taken with a probability of 1/2 from one of two finite sequences:

$(E_A,\ \ E_B, \varphi_A(P_B),\ \ \varphi_A(Q_B)$,$\varphi_B(P_A)$,$\varphi_B(Q_A), E_{AB})$, where $E_{AB} \cong E_0/< m_A P_A + n_A Q_A, m_B P_B + n_B Q_B >$;

$(E_A,\ \ E_B, \varphi_A(P_B),\ \ \varphi_A(Q_B)$,$\varphi_B(P_A)$,$\varphi_B(Q_A), E_C)$, where $E_C \cong E_0/< m^{'}{}_A P_A + n'{}_A Q_A, m'{}_B P_B + n'{}_B Q_B >$;

define, what finite sequence they have been taken from.

Suggested authentication network includes four procedures:

1. *Algorithm of parameters generation*, which results in initialization of generally-known network parameters
2. *Algorithm of keys generation*, which effects generation of open key–closed key pair for a user by means of protocol parameters
3. *Algorithm of shaping signature*, receiving a closed key of the user, message *m*, as well as a list of open keys of the users, who have signed the message earlier, and a current signature value $\sigma_i$. to the input. As a result of work the algorithm returns a new value $\sigma_{i+1}$ or an error, if the input data appeared to be incorrect;
4. *Algorithm of checking signature*, receiving a list of open keys of the users, message $m$ and a current signature value $\sigma$. to the input. As a result of successful verification

the algorithm returns value 1, and otherwise – it returns 0.

Let us assume that $E(\mathbb{F}_{p^2})$ is a supersingular elliptic curve set over characteristic field $p = l_A^{eA} l_B^{eB} l_S^{es} f \pm 1$with a number of points equal $(l_A^{eA} l_B^{eB} l_S^{es} f)^2$.

Let us also register points being the generatrices of torsion subgroups: $< P_A, Q_A > \; = E[l_A^{eA}]$, $< P_B, Q_B > \; = E[l_B^{eB}]$,$< P_S, Q_S > \; = E[l_S^{es}]$. According to a suggested protocol points $P_A, Q_A$ and $P_B, Q_B$are used for generation of nuclear of users' isogenies, while points $P_S, Q_S$ are used for shaping a secret isogeny $\varphi_s$.

Generation of network parameters takes place according to the following algorithm:

1. Select security parameter $\lambda$ and generate field characteristic with a specified number of points $(l_A^{eA} l_B^{eB} l_S^{es} f)^2$.
2. Generate elliptic curve $E\left(\mathbb{F}_{p^2}\right)$.
3. Find points $\{P_S, Q_S\}$ forming the torsion subgroups$E[l_S^{es}]$.
4. Generate a random point $P_M \in E[l_S^{es}]$.
5. Determine hash function $H: \{0,1\}^* \rightarrow \mathbb{Z}$.

Subsequently, the open network parameters equal: $p, E, \{P_S, Q_S\}, P_M, H$.

In order to shape an open key of a group with number $n$ of participants, where every one represents a node – data processor as well as personal keys of the group users, it is necessary to perform the following actions.

1. Generate a secret isogeny $\varphi_S: E \rightarrow E_s$ by means of a nucleus $< m_S P_S + n_S Q_S >$, where $m_S n_S \in \mathbb{Z}/l_S^{es}\mathbb{Z}$ are random numbers not divisible by $l_S$, $< P_S, Q_S > \; = E[l_S^{es}]$.
2. Plot a chain of isogenies $\varphi_1 \rightarrow \varphi_2 \rightarrow \ldots \rightarrow \varphi_n$, where $\varphi_i: E_{i-1} \rightarrow E_i$, $E_0 = E, i = 1, \ldots, n$, by means of random selection of generatrices $P_i, Q_i \in E_i\left[l_i^{e_i}\right], i = \{A, B\}$, and nucleus coefficients $m_i$,$n_i \in \mathbb{Z}/l_i^{e_i}\mathbb{Z}$, not divisible by$l_i$.
3. Calculate: $\psi(P_M) = \varphi_n \diamond \varphi_{n-1} \diamond \ldots \diamond \varphi_2 \diamond \varphi_1(P_M)$, where $\varphi_i: E_{i-1} \rightarrow E_i, E_0 = E,$" $\diamond$ " is an operation of composition of isogenies. Set an open key of a group $gpk = (E_s, \psi(P_M), deg\psi)$.
4. For every node processor or user $u_i, i = 1, .., n$, set open key–closed key pair $(pk_i, sk_i)$ in the following way: $pk_i = (E_i, P_i, Q_i), sk_i = (m_i, n_i, m_S, n_S)$.

In order to sign message $M$ the first user $u_1$ of the chain will carry out the following actions (Fig. 3):

1. Calculates hash value from a message: $h = H(M)$.
2. Generates a random point $Q \neq P_M$, $Q \in E[l_S^{es}]$ and assumes$Q_M = hQ$.
3. Generates isogeny $\varphi_1: E \rightarrow E_1$ on the basis of a personal closed key by means of nucleus $< m_1 P_1 + n_1 Q_1 >$and calculates the values$\varphi_1(Q_M), \varphi_1(P_s), \varphi_1(Q_s)$.
4. Generates isogeny $\varphi_{1s}: E_1 \rightarrow E_{1s}$ on the basis of a closed key of the group by means of nucleus$< m_s \varphi_1(P_s) + n_s \varphi_1(Q_s) >$.
5. Assumes: $Q_{M,1} \leftarrow \varphi_1(Q_M), P_{s,1} \leftarrow \varphi_1(P_s), Q_{s,1} \leftarrow \varphi_1(Q_s)$.
6. Shapes a signature $\sigma_1 = (E_{1s}, Q, Q_{M,1}, P_{s,1}, Q_{s,1})$ and hands it over to the next user.

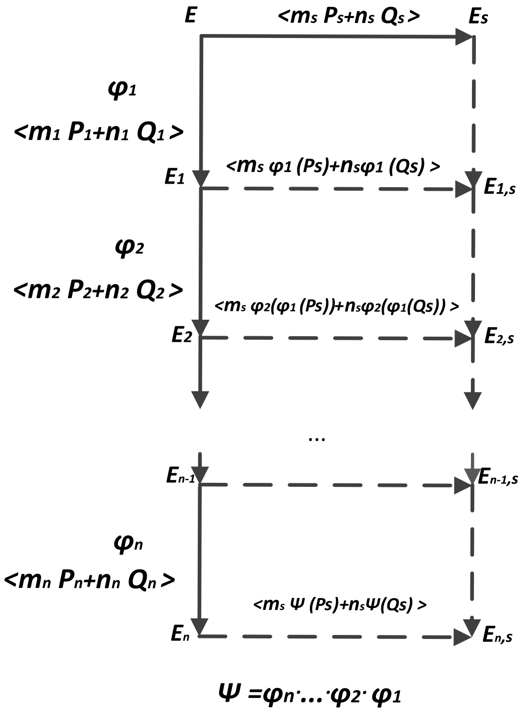

**Fig. 3.** Rank-Order Collective Signature Generation Network.

A user (node – processor) $u_i$ performs the following actions on the basis of a signature $\sigma_{i-1} = (E_{i-1,s}, Q, Q_{M,i-1}, P_{s,i-1}, Q_{s,i-1})$ received from the previous user:

1. Generates user's isogeny $\varphi_i: E_{i-1} \to E_i$ by means of nucleus $< m_iP_i + n_iQ_i >$and calculates values$\varphi_i(Q_{M,i-1}), \varphi_i(P_{s,i-1}), \varphi_i(Q_{s,i-1})$.
2. Using an open key of the previous user $E_{i-1}$ and value $E_{i-1,s}$ obtained from signature $\sigma_{i-1}$, it checks knowledge of secret isogeny $\varphi_s$ by the user $u_{i-1}$, as in the evidence circuit [13]. In order to do so, it calculates isogeny $\varphi_{i-1,s}: E_{i-1} \to E'_{i-1,s}$ by means of nucleus $< m_sP_{s,i-1} + n_sQ_{s,i-1} >$ and checks equation $E'_{i-1,s}$and $E_{i-1,s}$.
3. Finds curve $E_{i,s}$ in the way of plotting isogeny $\varphi_{is}: E_i \to E_{is}$ by means of nucleus$< m_s\varphi_i(P_{s,i-1}) + n_s\varphi_i(Q_{s,i-1}) >$.
4. Assumes: $Q_{M,i} \leftarrow \varphi_i(Q_{M,i-1}), P_{s,i} \leftarrow \varphi_i(P_{s,i-1}), Q_{s,i} \leftarrow \varphi_i(Q_{s,i-1})$.
5. Shapes signature $\sigma_i = (E_{is}, Q, Q_{M,i}, P_{s,i}, Q_{s,i})$ and submits it to the next user.

Based on the calculated signature $\sigma_n = (E_{ns}, Q, Q_{M,n}, P_{s,n}, Q_{s,n})$ the last user of the chain of processing data$u_n$ shapes a collective signature of a message:

$\sigma = (Q, Q_{M,n})$.

The following actions are to be performed when checking a signature:

Having message $M$, signature $\sigma = (Q, Q_{M,n})$ and open key of the group $\psi(P_M)$ an inspector calculates the following values of Weil coupling:

$$e_{l_s^{es}}(\psi(P_M), Q_{M,n}) \overset{?}{=} e_{l_s^{es}}(P_M, hQ)^{deg\psi} ,$$

where, $\psi$ is an isogeny corresponding to composition of the user's isogenies, i.e. $\psi = \varphi_n \diamond \varphi_{n-1} \diamond \dots \diamond \varphi_2\varphi_1$, $deg\psi = deg\varphi_n \cdot \dots \cdot deg\varphi_1$.

If the equality has been fulfilled, the result will be: signature is correct, otherwise the result will be: signature is incorrect.

This check is correct, since with respect to bilinear mappings the following interrelations are met:

$$e_{l_S^{es}}\left(\psi(P_M), Q_{M,n}\right) = e_{l_S^{es}}\left(\psi(P_M), \psi(Q_M)\right)= e_{l_S^{es}}\left(\psi(P_M), \psi(hQ)\right) = e_{l_S^{es}}(P_M, hQ)^{deg\psi} .$$

## 3.3. Analysis of suggested solution security

The isomorphism of groups of classes of isogenies and groups of classes of ideals exists for supersingular and non-supersingular curves. A ring of endomorphisms of elliptic curve is cumulative for supersingular curves, while a group of classes of ideals is Abelian. This property has been used in attack [14] for solving an analog of the CSSI task for non-supersingular curves over subexponential time on quantum computer. In case of supersingular curves a ring of endomorphisms is noncommutative, while the group properties are not met for the classes of ideals, therefore, an attack from work [14] can not be applied, and the task of finding isogenies of supersingular curves features an exponential stability in this case.

*Opening the user's personal closed key.* Let us assume that there are open parameters of the system $p$, $E, \{P_S, Q_S\}, P_M, H$as well as open keys $gpk = (E_s, \psi(P_M), deg\psi)$ and $pk_i = (E_i, P_i, Q_i)$. Then cracking the user's personal closed key is confined to a task of finding a generatrix of isogeny nucleus $\varphi_i$with respect to available images $\varphi_i\left(Q_{M,i-1}\right), \varphi_i\left(P_{s,i-1}\right), \varphi_i\left(Q_{s,i-1}\right)$,, which is complex for calculation.

Since the points $(P_S, Q_S)$ are generatrices of the subgroup $E_{i-1}\left[l_S^{es}\right]$, the values $\varphi_i(P_S), \varphi_i(Q_S)$ help an intruder calculate the action $\varphi_i$ for the entire subgroup $E_{i-1}\left[l_S^{es}\right]$, since any element $E_{i-1}\left[l_S^{es}\right]$ is a linear combination of generatrices $P_S, Q_S$. However, there is no algorithm making it possible to use this information for determiningisogeny $\varphi_i$. If the intruder has a possibility of calculating action $\varphi_i$ in the points of subgroup $E_{i-1}\left[l_i^{e_i}\right]$, where the generatrices $< P_i, Q_i >= E_{i-1}\left[l_i^{e_i}\right]$are used during generation of nucleus $\varphi_i$, then it is possible to open isogeny $\varphi_i$by means of quantum computer. Besides, in such case it is possible to launch an attack using a classic computer too by calculating generatrix of dual isogeny nucleus. Thus, it is not realistic to transfer action $\varphi_i$ to $E_{i-1}\left[l_S^{es}\right]$ to values at $E_{i-1}\left[l_i^{e_i}\right]$ and, by the same, come to know a secret isogeny of the user $\varphi_i$.

*Incorporation of intruder's signature into a chain.* Let us assume that the illegal intruder possesses signature $\sigma_{i-1} = (E_{i-1,s}, Q, Q_{M,i-1}, P_{s,i-1}, Q_{s,i-1})$, which has been received from a previous user $u_{i-1}$, and wants to build in its own signature before sending it to the next user $u_i$. In order to do so, it needs to have its own elliptic curve $E_{adv}$ in the list of open keys of the group users. Then it is obliged to provide the next user with an evidence of awareness of secret isogeny $\varphi_s$in the way of plotting isogeny $\varphi_{adv,s}: E_{adv} \to E_{adv,s}$ including value $E_{adv,s}$into a signature. However, the attacker should know for this purpose the closed key values $m_s, n_s$, which are known to the legitimate group users only. If the legitimate system user possessing an open key and a closed key corresponding to it, is the intruder, it succeeds to prove to the next user that it is a legitimate group member. But the final isogeny $\psi'$will look as follows in case of embedding signature into a chain:

$$\psi' = \varphi_n \diamond \varphi_{n-1} \diamond \varphi_{adv} \diamond \ldots \diamond \varphi_2\varphi_1,$$

while its degree will increase $deg\varphi_{adv}$ times. In this case in the course of checking signature the equation

$$e_{l_M}(\psi[P_M], \psi'[hQ]) = e_{l_M}(P_M, hQ)^{deg\psi}$$

will not be fulfilled, since the open group key $\psi(P_M)$ comprises an image of a legitimate chain, and the value $deg\psi \neq deg\psi'$.

*Changing order of message signing.* In case of a confederacy involving a group of users, who want to violate a hierarchy of signature formation, value $deg\psi'$ will be equal $deg\psi$, however, the resulting isogeny $\psi'$will differ by an order of succeeding of the user's isogenies, therefore, the check interrelation will not be used too. Any additional signature incorporated by an intruder will bring about the increase of degree of the resulting isogeny, which legitimate value is provided in the open key of a group. Therefore, a complete signature falsification is possible only under condition of incorrect generated system parameters.

*Message false representation.*Let us assume that there is a signature $\sigma = (Q, Q_{M,n})$ of message$M$and the intruder has an intention to find a document $M'$corresponding to this signature $\sigma$. For this purpose it will calculate its hash $h' = H(M')$ trying to find such a value $h'Q$in order to fulfill the check interrelation. Since $Q$ is a part of signature, it can not be substituted, therefore, the message false representation is confined to solving task of finding hash function collision.

The authors have performed simulation of the offered pattern with the use of computerized algebra system Sage for a group consisting of five users. As a result, an evaluation signature length has been obtained that will vary depending on the security level for classical (Table 1) and quantum computer (Table 2).

**Table 1.** Size of signature taking into account security requirements for classic computer.

| Parameter$\lambda$ | Character length, bit | Signature size, bit |
|---|---|---|
| 80 | 480 | 1,920 |
| 112 | 672 | 2,690 |
| 128 | 768 | 3,074 |
| 192 | 1,152 | 4,610 |

**Table 2.** Size of signature taking into account security requirements for quantum computer.

| Parameter$\lambda$ | Character length, bit | Signature size, bit |
|---|---|---|
| 80 | 720 | 2,882 |
| 112 | 1,008 | 4,034 |
| 128 | 1,152 | 4,610 |
| 192 | 1,728 | 6,914 |

Standard GOST R 34.10-2012 [15] is based on the discrete logarithm problem in group of points of elliptic curve and specifies the algorithm of forming message signature. The length of signature depends on the order of subgroup of points of elliptic $q$and equals. The value $q$also depends on security level and can assume values: $2^{254} < q < 2^{256}$for$\lambda = 128$ or$2^{508} < q < 2^{512}$for$\lambda = 192$. Thus, the size of a signature formed according to GOST R 34.10-2012 equals 512 bit or 1,024 bits.

An offered pattern of the signature is inferior to standard GOST R 34.10-2012 with respect to criterion of signature size, however, it helps provide group authentication and form a collective signature from several participants. At that, the size of collective digital signature is equivalent to signature size, formed by one user. The offered pattern also additionally helps check the order of signature formation, which makes it possible to trace a chain of data processing.

## 4. Conclusion

As a result of performed work the authors offer a diagram of hierarchical authentication on the basis of isogenies of elliptic curves for ensuring security of data routing in the systems of analysis of digital production, in particular, in the systems of traffic analysis. Thepeculiaritiesofinformationrouting in the course of processing big data in such systems demanding application of participants' hierarchical authentication have been revealed.

In order to solve the assigned tasks, a decision has been taken to use a collective signature with introduction of an additional property of checking order of forming it. The authors have developed a corresponding pattern of authentication and a set of algorithms providing its functioning. A pattern offered in the work comprises a description of algorithms making it possible to effect generation of parameters according to an assigned security level, forming keys of the users and a group, forming a signature and its check.

The security analysis has been carried out, in which context consideration has been given to the scenarios of attacks aimed at violating the order of signature, message false representation, opening user's keys and incorporating intruder's signature into a chain. It has been established that the offered pattern is stable with respect to these attacks taking into account assumptions complex for calculation.

As a result of simulation of a developed pattern in the computerized algebra system Sage, the digital values signature size for characteristics of different length have been received, both for quantum and for traditional systems. A comparison made with the existing impossible-to-deny signal on isogenies of elliptic curves shows that the proposed pattern helps create a signature of lesser length. In case of adhering with the requirements to selecting field characteristic the developed pattern although gives up the standard of digital signature GOST R 34.10-2012 with respect to signature size, but it helps provide verification of the order of forming a signature; in this case the signature length does not depend on the group dimensionality, and the used task of finding isogenies grants a possibility of providing stability with respect to quantum computer.

## References

1. K. Shwab, *The fourth industrial revolution* (Crown Business, New York, 2016)
2. Yu. S. Vasiliev, D. P. Zegzhda, M. A. Poltavtseva, Computer systems, **4** (2017)
3. Industry 4.0 How to navigate digitization of the manufacturing sector. McKinsey Digital [online], Available at: http://www.cloud-finder.ch/fileadmin/Dateien/PDF/Themenkategorien/industrie40/McKinsey_Report_Industry_4.0_s.pdf (2015)
4. Program "Digital economics of the Russian Federation" has been approved by the Resolution of the Government of the Russian Federation No. 1632-p dated July 28, 2017 [online], Available at: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (2017)
5. D. Pudov, Open systems. DBMS, **4** (2017)
6. D. S Lavrova, Automatic Control and Computer Sciences,**50(8)** (2016)
7. R. C. Merkle et al., *Secrecy, authentication, and public key systems* (UMI Research Press, Ann Arbor, 1979)
8. L. Lamport, SRI International, **238** (1979)
9. R. J. McEliece, Coding Thv, **4244** (1978)
10. H. Niederreiter, Problems of control and information theory,**15 (2)** (1986)

11. I. Anshel, M. Anshel, D Goldfeld, Mathematical Research Letters,**6** (1999)
12. J. Hoffstein, J. Pipher, J. H. Silverman, International Algorithmic Number Theory Symposium (1998)
13. L. De Feo, D. Jao, J. Plut, Cryptology ePrint Archive, report, **2011/506** (2011)
14. A. Childs, D. Jao, V. Soukharev, Math. Cryptol.,**8 (1)** (2010)
15. GOST R. R 34.10-2012– Federal Technical Regulation and Metrology Agency.Information technologies.Cryptographic protection of information.Processes of forming and checking electronic digital signature. Instead of GOST – P. 34.10-2001 (2001)