Remote Object Confidential Control Technology based on Elliptic Cryptography

Vadym Poltorak[1], Bohdan Zhurakovskyi[1], Volodymyr Saiko[2], Tamara Loktikova[3], and Olena Nesterova[4,5]

[1] *Igor Sikorsky Kyiv Polytechnic Institute, 37 Beresteiskyi pros., Kyiv, 03056, Ukraine*
[2] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv, 01033, Ukraine*
[3] *Zhytomyr Polytechnic State University, 103 Chudnivska str., Zhytomyr, 10005, Ukraine*
[4] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[5] *Dragomanov Ukrainian State University, 9 Pyrohova str., Kyiv, 01601, Ukraine*

Abstract
Data such as commands for controlling a remote mobile object and data on the state of its systems and subsystems are critical for successful, reliable, and unhindered control of it by the operator entity under the conditions of using an unsecured shared access channel. The mechanism of confidential transmission of critical data through an unprotected channel is developed based on a group of points on an elliptic curve. Encrypting and decryption procedures have been justified and developed to ensure confidentiality when transferring control commands to a remote moving object.

Keywords
Confidential control, elliptic curve cryptography, remote object.

1. Remote Object Control

By the term remote moving object, we will understand a certain artificially created technical system that can move freely in space. This moving object can perform motion in a straight line, or non-linearly (for example, some kind of rotation) in predetermined directions, along or around predetermined spatial axes.

Remote-moving objects play a very important role in the lives of people and society nowadays. We see more and more examples of the benefits that distant moving objects bring to people over time. Remote moving objects can perform many useful functions: from the delivery of pizza up to order to the search for mines and the compilation of mining maps of large areas. And from unmanned taxis to samples of unmanned weapons.

Most such moving objects are remotely controlled using control commands and data transmission channels [1].

At the same time, one of the important problems remains the possibility of capture of the control channel of a remote object by an unfriendly control subject in the absence of information protection tools of the channel and its control commands.

The data transmission channels for control commands and the state of the remote object must maintain the confidentiality, integrity, and authenticity of the data to avoid loss of control data, loss of reliability, and accuracy of the remote object control [1–3].

Cryptography offers several algorithms that can support the requirements for the control channel named above and they have stood the test of time. First of all, we are talking about crypto algorithms based on the finite Galois field *GF(q)* [1–2].

However, it is known that such crypto-algorithms require the use of an alphabet with

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL v.poltorak@kpi.ua (V. Poltorak); zhurakovskybiyu@tk.kpi.ua (B. Zhurakovskyi); vgsaiko@gmail.com (V. Saiko); dfikt_ltn@ztu.edu.ua (T. Loktikova); o.nesterova@kubg.edu.ua (O. Nesterova)
ORCID: 0000-0001-9231-9411 (V. Poltorak); 0000-0003-3990-5205 (B. Zhurakovskyi); 0000-0002-3059-6787 (V. Saiko); 0000-0002-3525-0179 (T. Loktikova); 0000-0002-0402-0370 (O. Nesterova)

very, very large amounts of symbols and key sizes to ensure high requirements for the crypto-resistance of the protected information channel [2].

Protecting the status data and control commands of a remote object, which are relatively small in size and volume, using algorithms with large alphabets and key sizes can lead to unnecessary consumption of control system resources, such as time and energy required for data processing and response on control commands, memory consumption, etc.

In this sense, the achievements of Elliptic Curve Cryptography (ECC), which is a relatively young field in cryptography and which is still being developed, are of great interest [4–8]. ECC demonstrates an order of magnitude smaller key sizes and significantly lower consumption of energy, computing resources, and device memory compared to known algorithms based on *GF(q)*.

However, certain features should be taken into account. Currently, only one additive group is formed within the ECC because only one group operation is defined on the set of its elements, and points. This happens in contrast to *GF(q)*, where two direct operations on the elements of the set are defined and, accordingly, two groups are formed: additive and multiplicative [3].

The presence of one group within the ECC and its sufficiency for organizing an analog of the Diffie-Hellman algorithm and an analog of the scheme for setting and verifying an electronic digital signature on the ECC made it possible to implement these algorithms and schemes on the ECC base and actively use them.

On the other hand, the existence of only one group in the ECC probably to some extent limits the functionality of applying the ECC to enciphering and deciphering data to ensure their confidentiality and integrity. Probably for this reason, the number of publications is small on the research of such a topic, encryption/decryption of data to ensure their confidentiality and integrity in the management of a remote mobile object.

Therefore, in this work, attention is paid to the exploration of ways of enciphering and deciphering data about the state of a remote moving object and its control commands to ensure their confidentiality and integrity.

1.1. The Remote Object Control Goal

We consider remote control of a moving object as a certain mechanism for releasing the human operator from performing actions and functions that pose a threat to his health and life. Such actions and functions are transferred to a remote moving object, which acts as a remote human operator tool.

The publications describe many examples of successful countermeasures by an unfriendly entity against the activity of moving objects by remote intervention in their control subsystem, which did not have information protection [9].

That is why the goal of remote object control should include such important characteristics as reliability and unobstructivity of information and management processes.

To achieve this goal, it is proposed to investigate the involvement of cryptography on elliptic curves to ensure the confidentiality, integrity, and authenticity of commands for controlling a remote moving object and information data about the state of its systems and subsystems.

In the first approach, we will focus on the possibility of ensuring the confidentiality of such messages in the remote object control channel [10].

1.2. The Remote Object Control System Composition

The management system of any object always assumes the presence of a control loop, which includes

- Remote controlled object itself.
- Control entity that forms and sets control commands and receives data about the state of the controlled object's systems and performs control of a remote object.
- Channel for transmitting control commands to a remote object (direct channel).
- Channel for information data transferring about the state of the control object, its systems, and subsystems from the object's embedded sensors (return channel) [11].

The model of the remote object control system is presented in Fig. 1, where the corresponding components are marked as follows:

1. The remote object.
2. A control entity.
3. Direct channel.
4. Return channel.

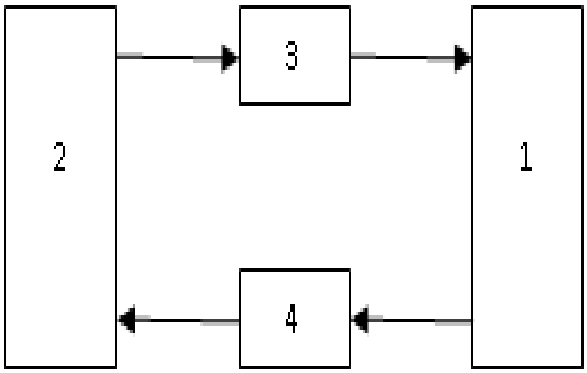

Figure 1: Remote object control system

1.3. Principles of Remote Object Control System Functioning

The main feature of the object control system is the presence of feedback 4 from object 1 to subject 2 of management. See please Fig. 1 above.

Remote object 1 performs specific functions and actions according to control commands from control subject 2 [12]. Control subject 2 forms and transmits control commands to remote object 1 through direct channel 3. This is a command transmission channel (direct channel). The state of the control object 1, its systems and subsystems, and data from its sensors must be delivered to the control subject 2 through the return channel 4 of data transmission [13].

We have two data channels to worry about:

- Direct—a channel of control commands.
- Reverse—data channel about the state of the managed object.

Each such channel is a combination of the signal propagation medium and the equipment forming the channel.

We understand a signal as a useful purposeful perturbation of the physical state of the environment in which the signal propagates [14].

It is known that in addition to the useful process of generating and transmitting signals, physical processes occur in the environment that affect useful signals and distort them in a certain way. This can lead to data errors during their reception and requires the presence of error detection and correction tools in the channel equipment. We will assume that such tools are present in the channel [15].

Sources of signal disturbances and, accordingly, data can be both natural and artificial, intentionally created to hinder the process of reliable and accurate control of a remote object.

However, these are not all the reasons for possible violations of data circulation in the chain of the object's remote control system. Artificial means, such as high-energy interference, can have a strong effect. In a radio channel, for example, they can suppress the signals of the control system under certain conditions [16].

This will lead to a violation of such a property of the management system as the availability of data and the managed object.

Combating high-energy interference to preserve the availability of data and the controlled object during control is an important task that requires a separate study (for example, broadband, noise-like signals against spectrally concentrated interference, etc.) [17].

Another example of artificial reasons for the loss of data availability in channels and, as a result, the loss of controllability of a remote object is an unfriendly entity, let's call it that [18]. An unfriendly entity can succeed in seizing control of a remote object when it has access to signals in the propagation environment unless the command and state data of the remote object is protected by cryptographic tools [19].

Violation of these control commands or information about the state of the object will lead to a violation of the availability, accuracy, and reliability of the object's control processes.

In this work, attention is focused on the protection of control commands or data about the status of a remote object with cryptographic tools, and an attempt is made to involve ECC in the solution of such a problem [20].

2. Technology of Confidential Object Control based on ECC

In order not to lose the main ideas and achievements of world cryptography based on Elliptic curves in the further presentation, let's immediately review the architectural model of Elliptic cryptography from a distance.

Let's mention in passing that the term model means a non-exhaustive description of the object of research or its properties, which the researcher considers sufficient at the moment to get an idea about the object itself [21].

With this in mind, the model can be dynamic and change as often as we deem necessary.

Given the presence of several components of Elliptic Cryptography, let's review their place, role, and interaction in this architectural model. Please pay attention to Fig. 2.

This model presents four functional layers, each of which has its tasks and originates from the corresponding mathematical foundation [22].

The first layer is located at the highest architectural level of this model. It provides, in fact, cryptographic functionality, or user services.

This is a layer of cryptographic algorithms and protocols, that should deliver the desired security services to the user: confidentiality, integrity, authentication of objects of information activity (messages), non-repudiation (preventing the subject from renouncing the responsibilities assumed or actions performed in the system), etc.

For example, in this layer, there should be such a service as an analog of the Diffie-Hellman crypto-algorithm based on ECC, which is designed to agree on a single secret key of a communication session between two stations at the edges of an unprotected common communication environment.

This service can serve as one of the components of both the forward channel and the reverse channel (please refer to elements 3 and 4 in Fig. 1).

It can become the basis for the creation and implementation of the key management subsystem and their safe distribution for the remote object control system [23].

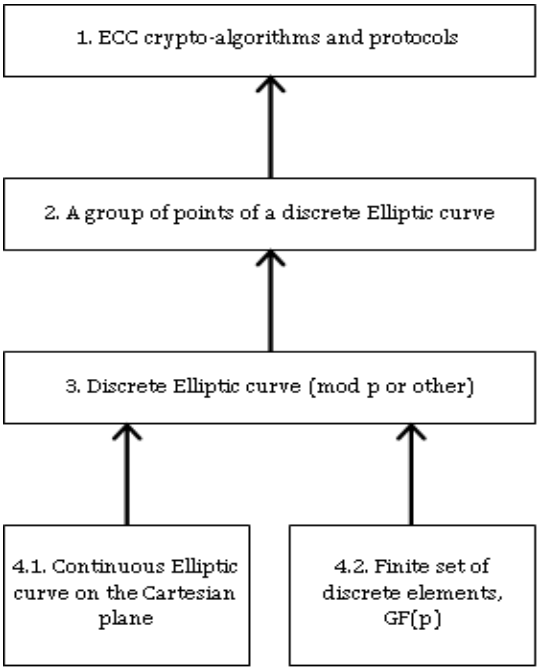

Figure 2: The ECC architectural model

Let's look at the second layer of the model in Fig. 2. This is a layer of discrete information objects, symbols of the alphabet, physical carriers of information, or its discrete quanta.

This is a discrete working alphabet of the information system, a finite set of its symbols (limited from above in number), together with one closed operation defined on them, conventionally called "addition."

The closedness of the operation here is understood in the sense of a certain way of setting the element δ of the set to one or two elements α and β of the same set.

In ECC, the elements of a discrete finite alphabet (finite set) are certain points of the Elliptic curve given by its equation on the Cartesian plane. Accordingly, this equation ties together the coordinates of such points.

They say: "The point $M(x, y)$ belongs to the curve given by its equation".

Such a finite set of elements is called a group; we denote it by the symbol G. A single closed operation is defined on the elements of the set G, they are points on a discrete elliptic curve.

In the set of elements of G, the points of the curve, a single element with the properties of the so-called "zero" for the group is defined. This is a point distant from infinity, and it is often called "infinity" or "∞".

In the set of elements G, the points of the curve, there is defined an inverse element β to

each element α of the set, such that as given by the expression (1)

$$\alpha + \beta = \infty. \quad (1)$$

Recall that the point ∞ plays the role of a kind of zero in ECC terms.

In the operations on the elements of the set *G*, the axioms about commutativity and associativity of the operands (or elements) are fulfilled, which are the points of the discrete elliptic curve.

Let's look at the third layer of the ECC architectural model in Fig. 2. The source of elements of the group *G* is a discrete elliptic curve with a limited, calculated number of its points, the coordinates of which are purely integers.

We can think of them as symbols of the working alphabet to combine with them control commands and data about the state of the remote-controlled object.

This means that a discrete elliptic curve is the locus of points (only with integer coordinates) that satisfy the discrete equation of an elliptic curve.

How is this achieved? Let's pay attention to the fourth layer of the ECC architectural model in Fig. 2. We can see two sources and two pillars of Elliptical Cryptography, ECC.

The fourth layer of the ECC architectural model in Fig. 2 is represented by parts 4.1 and 4.2. Part 4.1 is the first source and first pillar of the ECC, namely the continuous elliptic curve on the Cartesian plane. A discrete elliptic curve is formed from it by discretizing its continuous equation in the form given by the expression (2)

$$f\ (y) \equiv \varphi(x)\ mod\ p, \quad (2)$$

where *p* is prime.

Under certain requirements, this can be done with another modulo, for example, of the irreducible polynomial *P(x)*.

This action leads to the "filtering" of all those points of the elliptic curve that have only integer coordinates on the two axes (*x* and *y*) of the Cartesian plane.

This happens within the number line from 0 to *(p-1)* on each of the two axes (if such an action is performed by *mod p*).

All the remaining points of the continuous elliptic curve, which have non-integer coordinates, are rejected as a result of taking by *mod p*.

The number of points of a discrete elliptic curve with integer coordinates is limited and can be counted, which allows us to form a set *G* limited by the number of elements on the 2nd layer of the model in Fig. 2.

The set *G* of points of a discrete elliptic curve formed in this way, together with the addition operation defined on points of this set, forms an arithmetic additive group *G+*.

Part 4.2 of the model in Fig. 2 is the second source and second pillar of the ECC. This is a finite set of discrete elements together with arithmetic operations assigned to them. It may be, for example, a finite Galois field *GF (p)*, where p is prime. Elements of the set *GF (p)* are integers in this case and allow us to describe the coordinates of points of the group *G+* with integer values directly.

The arithmetic system *GF(p)* has a complete set of closed operations on the integers *a* = 0...*(p-1)*. Direct operations, addition, and multiplication are defined here as basic.

The operation of raising *b* to power *j*, where *b* belongs to *GF(p)*, is considered as the *j*-fold multiplication of *b* by itself by the definition of multiplication over *GF(p)*.

Inverse operations, subtraction, and division are not difficult to organize due to the presence of inverse elements for addition (for all *a*) and multiplication (except for *a* = 0).

All these arithmetic operations can naturally be performed on the integer coordinates of the points of the discrete elliptic curve, as they say, in the group G+ of the points of the elliptic curve.

2.1. Important Features of Performing a Group Operation on Points of an Elliptic Curve

Arithmetic operations on the integer coordinates of the points of the elliptic curve in the *G+* group are performed on each of the two numerical lines separately, on the X-axis and the Y-axis, of course, in the range of existence of these integer coordinates from 0 to *(p-1)*, and obviously by *mod p* [3].

Above, in the overview of the ECC architectural model in Fig. 2, we gradually opened the scenes on the main components of the ECC, moving down the layers of the model. And we reached two sources and two basic

pillars, on which the ECC has been based since the very beginning of its existence.

Now we will proceed in the reverse order, from the bottom to the top, and analyze in more detail the properties and features of the main components of the ECC in each layer of the architecture model according to Fig. 2.

Let's start with a point 4.1. This is the first source and the first pillar on which the ECC rests, a continuous elliptic curve on the Cartesian plane.

Analytical geometry on the Cartesian plane in the continuous version describes a curved line as the locus of points that satisfy the continuous equation of a curve in the form given by the expression (3)

$$f\ (y) = \varphi(x). \qquad (3)$$

The number of such points that satisfy equation (3) reaches infinity in the continuous case.

There is an important remark for understanding the procedure for operating on the points of an elliptic curve. Its implementation is completely based on the concept of analytic geometry and the problem known as the solution of a right triangle.

Among the tasks solved by analytical geometry on a continuous plane, there is, for example, the following: given the equation of a curve on the plane in the form of the equation (3) and point *M (x, y)* on the curve. Please refer to Fig. 3. An important component of calculations in problems of analytical geometry is the direction of one or another straight line on a plane.

It is determined by the angle β of the inclination of the straight line to the horizontal X-axis.

The calculation of analytical geometry problems involves not the angle β itself, but the angular coefficient k of the slope of the line to the horizontal axis X. The coefficient k is otherwise known as the tangent of the angle β of the slope of the line to the horizontal axis X.

By its essence, the tangent k of the angle β is defined as the ratio of the increment ΔY of the vertical coordinate to the increment ΔX of the horizontal coordinate on a straight line when the point M slides along it, which is represented by expression (4)

$$k = \frac{\Delta Y}{\Delta X}. \qquad (4)$$

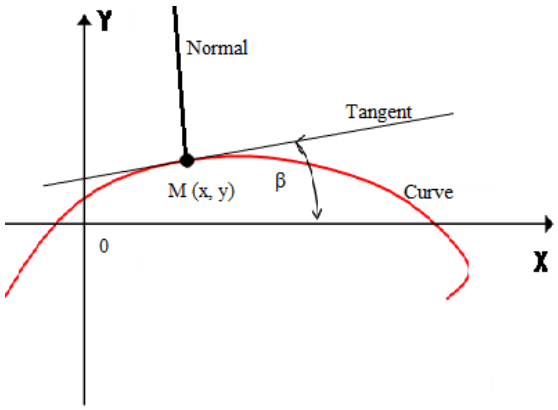

Figure 3: Illustration of the angle of inclination β

Let us choose for further consideration, for example, the variant of a continuous elliptic curve given by the equation (4)

$$y^2 = x^3 + ax + b, \qquad (4)$$

where a and b are coefficients that determine the shape of the curve and determine its suitability for cryptographic use.

It is a third-order elliptic curve represented in Weierstrass form. Since 1985, it has been almost the only type of elliptic curve for cryptographic applications [3]. In recent years, other types of curves have also been used.

An operation on the points of an elliptic curve is given on a continuous curve. However, the important features of performing a group operation on points are preserved even when moving to the discrete case due to taking their coordinates as *mod p*.

An elliptic curve generates the results of a group operation in a group $G+$ of its points in interaction with a straight line, which can occupy one of several characteristic positions with a certain inclination by the angle β on the same Cartesian plane.

The presence and number of common points in a straight and elliptic curve play a role in determining and performing a group operation. Common points in a straight line and an elliptic curve can only be intersection points and/or tangent points.

The most characteristic locations and slopes of the line for group operation are the angle β in the range ($-90<\beta<+90$) degrees and the other, $\beta = 90$.

In the first case ($-90<\beta<+90$), in terms of the number of common points of a straight line and a curve, the most characteristic of a group operation are:

- three points of intersection, which specifies the general case of an operation on two points with different *x* coordinates.
- one point of intersection and one tangent, which specifies the case of an operation on two points with the same *x* and *y* coordinates, provided that $y \neq 0$.

In the second case ($\beta = 90$), in terms of the number of common points of a straight line and a curve, the most characteristic of a group operation are:

- two points of intersection with a vertical line, which specifies the case of an operation on two points with different *y* coordinates and the same *x*, the line in this case is parallel to the *Y* axis, which results in a point at infinity ∞.
- one tangent point specifying the case of an operation over two points with the same *x* and *y* coordinates, and under the condition that y = 0, this results in a point at infinity ∞ too.

2.2. A Discrete Elliptic Curve Group of Points

Important preparation properties of a group operation on points are saved when moving to the discrete case of an elliptic curve due to taking their coordinates as *mod p*.

We need the group operational features and properties of the set of points of the discrete elliptic curve to explain the procedure for ensuring the confidentiality of critical data in the future. We will remind you that as critical data, we chose remote object management commands and data on the state of its systems.

The formation of the set of discrete points of the group *G*+, as the alphabet of the information system, is formed by the execution of taking modulo by the expression similar to (2).

Let's apply this action to expression (4)

$$(y^2 \equiv x^3 + ax + b)\ mod\ p. \qquad (4)$$

We will obtain a set of a certain number of N points *Ti* (*xi, yi*) of the discrete elliptic curve E, together with a point at infinity, I = 1 ... N.

This set is the alphabet A of the information system which includes all of such points.

Let the generating point *P* (*xp, yp*) of the group *G*+ have additive order n. This means that adding *P* to itself *n* times generates the only singular point ∞ in the group as shown in equation (5)

$$P + P + \cdots + P = nP = \infty. \qquad (5)$$

This is how the first cycle of *P* addition, which has a length of the order of *n*, is formed and completed.

The multiple additions of *P* (*xp, yp*) *i* times to itself (*I* = 1 ... n) runs through the values of all points *Ti* (*xi, yi*) from the set of this group once, including the point ∞ as it is shown in the equation (6)

$$P + P + \cdots + P = iP = Ti\ (xi, yi). \qquad (6)$$

Further addition of *P* will cause multiple cycles of order *n* up to infinity. We plan to work mainly in the first cycle, adding some higher ones as needed.

Any point *Ti* (*xi, yi*) of the group *G*+ can be represented by a generating point *P* and a scalar factor *i* (not a point).

Then the system alphabet *A* can be given as in expression (7)

$$A = \{T_1, T_2, \dots, T_i, \dots, T_N\}. \qquad (7)$$

Or, taking into account the property of the generating point *P*, the set *A* can be represented through it as it is shown in the equation (8)

$$A = \{P, 2P, 3P, \dots, iP, \dots, nP, \}. \qquad (8)$$

Critical data subject to protection, or remote object control commands are presented in the form of numbers *m* (numerical images) and will be associated with the *x* coordinate of the corresponding point *T* from the alphabet *A* (7), *x* = *m*, then we get the information point $T_m(m, y)$.

The point $T_m(m, y)$ has in this group the inverse point $T_{mr}(m, y_r)$ with the same coordinate *x* = *m* and a different coordinate y_r. They are located on a vertical line that intersects the curve at these two points at an angle of ($\beta = 90$) and there is a valid expression (9)

$$T_m(m, y) + T_{mr}(m, y_r) = \infty. \qquad (9)$$

We will need to use expression (9) in the following sections.

2.3. Data Encryption Procedure

Encryption and decryption of critical data *m* requires a key *k* as a random variable. It is required both at the sending station of Fig. 1, block 2 and at the receiving station, block 1.

In this approach to encryption and decryption, only the "symmetric" principle is possible, with one unique key *k*. As discussed

above, the matching of the single key k at the two ends of the channel is performed using the Diffie-Hellman algorithm.

With the participation of the key k, we will calculate the masking point $T_k(x_k, y_k)$ on the sender's side to mask the information point $T_m(m, y)$

$$T_k(x_k, y_k) = k\,P\,(x_p, y_p). \quad (10)$$

We encrypt an information point $T_m(m, y)$ by adding a masking point $T_k(x_k, y_k)$ from (10) to it

$$T_c = T_k(x_k, y_k) + T_m(m, y). \quad (11)$$

Expression (11) gives the point of the cryptogram with its coordinates $T_c(x_c, y_c)$.

This point as the cryptogram must be transmitted over an insecure sharing environment to the recipient. This can be done by passing two of its coordinates (x_c, y_c).

An unfriendly entity or attacker does not have a masking point $T_k(x_k, y_k)$ and cannot find it in a reasonable amount of time. Therefore, he does not have the opportunity to quickly intervene in the processes of controlling a remote object.

2.4. Data Decryption Procedure

The receiver knows the generating point P and the key k. With the participation of the key k, it calculates the unmasking point (T_{kr}), which is the inverse point to the masking point T_k at the sender side by the group operation rule, similar to (9) and (5)

$$T_k + (T_{kr}) = n\,P = \infty. \quad (12)$$

The receiver needs to "subtract" the masking point T_k (10) from the cryptogram point T_c (11) to restore the information point $T_m(m, y)$ on the receiving side, according to the group operation rule.

The "subtraction" operation is not defined in the group, but there are inverse points by the group operation as (12). Let's take into account (10), then

$$\begin{aligned}(T_{kr}) &= n\,P - T_k = n\,P - k\,P \\ &= (n-k)\,P.\end{aligned} \quad (13)$$

So the receiver does not need to restore the masking point itself. It can calculate the unmasking point (T_{kr}) by the expression (13).

Then the information point $T_m(m, y)$ will be found by adding it as

$$T_m(m, y) = T_c + (T_{kr}). \quad (14)$$

Let's take into account that information point

$$T_m(m, y) = t_m\,\mathrm{P}. \quad (15)$$

Opening (14) taking into account (10), (11), (12), and (15) shows that identity (16) is obtained

$$\begin{aligned}T_m(m, y) = (k + t_m)\mathrm{P} + (\mathrm{n} - \mathrm{k})\mathrm{P} &= \\ = \mathrm{kP} + t_m P + nP - kP &\\ == t_m P + nP &\\ = t_m P + \infty == t_m P &\\ = T_m(m, y).&\end{aligned} \quad (16)$$

It is obvious that the information point $T_m(m, y)$ was confidentially transferred over the direct channel, carrying critical data or some command m for remote object control.

3. Discussion

In the presented concept of confidential management of a remote mobile object, it was possible to apply the principle of symmetric crypto-transformation using a single secret key for the sender and the recipient. The problem of key distribution and management is a separate important area of information security in shared access environments. Within the framework of this work, this problem was not analyzed in depth. The authors relied on the availability of an analog of the Diffie-Hellman algorithm over a group of elliptic curve points to provide an approach to confidentiality from the position of a single mathematical foundation.

Masking of information elements of an alphabet (sufficiently large) with other elements of the same alphabet, randomly generated with the participation of a random key based on a group of points of an elliptic curve, allows to ensure the confidentiality of critical data of a remote object management system. The crypto-resistance of this approach is based on the complexity of solving the problem of the discrete logarithm in the group of points of the elliptic curve.

The issue of testing the integrity and authenticity of critical data, control commands, and data on the status of a remote object, in the presented concept of its control system, requires further research.

The issue of substantiation and coordination of many parameters, such as the size of the working alphabet of the system; the desired and sufficient power of the set of the group of points; dimensions and format of keys; size and format of critical data to be protected; division into blocks and formatting

of critical data in the case of their large volume into streams; and also, the effect of involving the principles of block stream encryption in feedback modes, etc., all this also require further research.

References

[1] B. Sklar, Digital Communications: Fundamentals and Applications, 2nd Edition, Prentice Hall (2001).

[2] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Wiley (1996).

[3] H. Tilborg, Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial (Springer International Series in Engineering and Computer Science) 2000th Edition, Springer (1999).

[4] A. Bessalov, et al., Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves, in: Workshop on Classic, Quantum, and Post-Quantum Cryptography, vol. 3504 (2023) 12–25.

[5] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 1–11.

[6] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

[7] A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45.

[8] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

[9] M. Al-Bassam, et al., Fraud and Data Availability Proofs: Detecting Invalid Blocks in Light Clients, Financial Cryptography and Data Security (2021) 279–298. doi: 10.1007/978-3-662-64331-0_15.

[10] O. Shevchenko, et al., Methods of the Objects Identification and Recognition Research in the Networks with the IoT Concept Support, in: Cybersecurity Providing in Information and Telecommunication Systems vol. 2923 (2021) 277–282.

[11] B. Zhurakovskyi, et al., Calculation of Quality Indicators of the Future Multiservice Network, Future Intent-Based Networking (2022) 197–209. doi: 10.1007/978-3-030-92435-5_11.

[12] B. Ibrahimov, A. Alieva, Research and Analysis of Quality of Service Indicators for Multimedia Traffic Using Fuzzy Logic, 14th Int. Conf. Theory Appl. Fuzzy Syst. Soft Comput. (2020) 773–780. doi: 10.1007/978-3-030-64058-3_97.

[13] M. Moshenchenko, Optimization Algorithms of Smart City Wireless Sensor Network Control, in: Cyber-security Providing in Information and Telecommunication Systems II vol. 3188 (2021) 32–42.

[14] M. Ahmad, S. Singh, S. Khurana, Cryptographic One-Way Hash Function Generation Using Twelve-Terms 4D Nonlinear System, Int. J. Inf. Technol. 13 (2018) 2295–2303. doi: 10.1007/s41870-018-0199-8.

[15] S. Zhu, G. Wang, C. Zhu, A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes, Entropy, 21(8) (2019) 790.

[16] R. Parvaz, M. Zarebnia, A Combination Chaotic System and Application in Color Image Encryption, Opt. Laser Technol. 101 (2018) 30–41.

[17] Y. Bingle, D. Schaeffer, Should the Private Sector Conduct “Hack Back” Operations Against Cyberattackers? An ethical dilemma: Cyber self-defense or cyber vigilante?, IEEE International Symposium on Technology and Society (2021) 28–31.

[18] E. Hagras, et al., Authenticated Public Key Elliptic Curve Based on Deep Convolutional Neural Network for Cybersecurity Image Encryption Application, Sensors, 23(14) (2023), 6589. doi:10.3390/s23146589.

[19] Cybersecurity: Selected Cyberattacks, 2012–2021, Washington: Congressional Research Service (2021). URL: https://crsreports.congress.gov/product/pdf/R/R46974
[20] B. Zhurakovskyi, et al., Smart House Management System, Emerging Networking in the Digital Transformation Age (2023) 268–283. doi: 10.1007/978-3-031-24963-1_15.
[21] H. Muhi-Aldeen, et al., Technology of Secure Data Exchange in the IoT System, in: Information Security and Information Technologies III vol. 3200 (2021) 115–121.
[22] B. Zhurakovskyi, et al., Secured Remote Update Protocol in IoT Data Exchange System, in: Cybersecurity Providing in Information and Telecommunication Systems vol. 3421 (2023) 67–76.
[23] D. Pliatsios, et al., A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics, IEEE Commun. Surv. Tutorials 22(3) (2020) 1942–1976. doi:10.1109/comst.2020.2987688.