UDC 62-50:519.7(045)

V. V. Kirichenko

INFORMATION SECURITY OF COMMUNICATION CHANNEL WITH UAV

Aircraft Control Systems Department, National Aviation University, Kyiv, Ukraine
E-mail: vkir28@ukr.net

***Abstract*—*This paper analyses the issues of closing the communication channel with an unmanned aerial vehicle by using cryptographic means. Requirements applicable to such means are formulated. The method of information encryption envisaging use of direct and reverse dynamical systems is considered. There has been carried out a series of experiments on information conversion with the encryption-decryption system that showed some algorithm features based on the above mentioned systems.*

Index Terms—Aircraft motion control; unmanned aerial vehicle; UAV communication channels; cryptographic protection; block packet cipher; Lorenz system; ring of integers.

I. INTRODUCTION

Today, unmanned aerial vehicles (UAV) are widely used not only in the military, but also in the civil sector. They are increasingly used to solve such macroeconomic tasks as aerial photography, meteorological measurements, monitoring of pipeline and electric power supply line condition, etc. The recent global boom in using unmanned aircraft can be explained by the benefits offered by such vehicles that is to say low price, cost efficiency, ease of use, and security for maintenance staff.

At the same time, a range of problems associated with the intense development of this direction, both organizational, regulatory and technical ones emerge full blown. Moreover, the issues of information security, in particular the closure of communication channels used to contact UAV, become critical.

Today, there are a number of technical issues hindering the UAV development. The overarching task is to ensure information transmission between an aerial vehicle also called, for brevity's sake, the 'Board' and a ground control station (GCS) that we further designate using the term the 'Ground' to the volume required, at the given rate and without noise. This task can be solved by increasing the capacity and noise resistance of the information transmission channels.

Topical issues of classified information in communication channels with ground control UAV investigated in many recent papers, for example [1], [2]. However, analysis of recent research and publications shows that these issues are not completely addressed in the literature.

The most important information kinds exchanged by the Board and the Ground include the command-line, telemetric and video information.

Command-line information constitutes digital fixed-length blocks (packages) arriving through the radio channel from the Ground to the Board to adjust the layout of the vehicle controls for completion of maneuver commands transmitted by the GCS operator.

Telemetric information transmitted from the Board to the Ground in the form of digital packages as well includes data on the layout of the UAV controls.

Video information constitutes broadband signals picked up from the on-board digital video cameras (or thermal cameras).

ON-board video cameras are needed to give the panorama in sight of UAV to detect various objects afield and determine their coordinates, to explore areas of forest and peat-bog fires, major man-induced disasters, to perform environmental monitoring, etc. Particular tactical tasks carried out using the aircraft-borne video cameras are confidential and protected from unauthorized disclosure. The use of stream ciphers offers a simple solution for cryptographic information security in broadband video transmission system.

The problem of vulnerability of the channels used to transmit information between UAV and the ground control station more often being a tablet computer or a laptop, can be solved by using one of the following methods [3]:

– the use of autonomous UAV;
– the use of satellite repeaters;
– closure of communication lines by using cryptographic means.

In most applications, the last of the above mentioned methods turns to be the most appropriate and cost-effective one.

In evaluating the requirements applicable to channel protection system using cryptographic means, the following aspects can be distinguished: speed-of-response, encryption reliability, weight and overall dimensions of the on-board system part. These factors are in conflict with each other, especially with increasing channel carrying capacity and low weight of UAV.

Several factors determine the choice of the encryption algorithm, such as organizational (including certification issues) and technical ones, of which an important moment is feasibility on the available component basis.

The aim of this paper is to develop of software and modeling cypher algorithm that ensures high-speed streamed cryptographic conversion of signals transmitted from the UAV board.

II. Mathematical Description

In recent years, a new direction in cryptology is being developed, which is associated with the use of dynamical systems with chaotic behavior [4], [5]. One of the basic approaches in this direction is based on the use of inverse control systems for developing cryptographic algorithms [6].

Dynamical systems with chaotic behavior are being widely used now and are used in various fields, in particular for ensuring cryptographic protection of information [5]. Such systems can serve as the basis for pseudorandom sequence generators that are further used to encrypt plaintext data. On the other hand, every dynamical system of the input-output structure can be directly used for conversion of information. On the basis of such systems an encoder is developed. The log-in is a digitized message, while the log-out is an encrypted signal directed to the telecommunications network. A necessary condition for unique decrypting is availability of the feedback system.

In this paper, the system was realized the whole diagram of which is shown in Fig. 1.

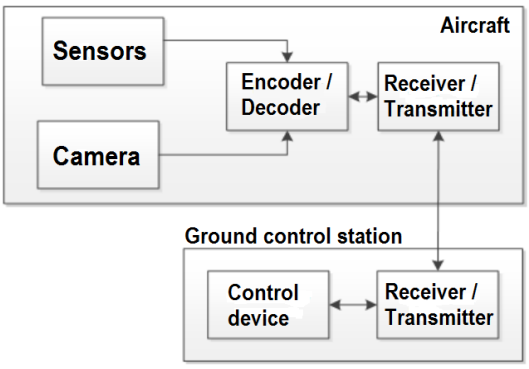

Fig. 1. Conceptual diagram of the system

The cheapest of the UAV does not provide cryptographic protection of the communication channel. That is, the same commands coming from the ground to the board and from board to the ground correspond to the same signals. This allows an attacker to take control of the UAV.

UAV modules communicate with each other using standard protocols for data exchange. One of the most popular and easiest ways to transfer the data is realized in the UAV via Universal Asynchronous Receiver-Transmitter (UART). Usual, UART, consists of two data channels TXD (transmit) and RXD (receive), supply (+ 5V) and ground (GND), the rest of the wire support. This means that when you connect devices via UART, you need to connect TX1 → RX2, RX1 ← TX2.

To connect the encoder uses two UART. First UART connected to the apparatus, other – to the transceiver. The encoder can be implemented on a microcontroller (MKB for the board and MKG for the ground). All command - telemetry information before sending the air passes through the encoder.

Since in most cases the user does not have the ability to change the program UAV control, it may be offered the option of curtain protection. The bottom line is that the encoder is included in the break after the board/ground equipment and to the transceiver. Thus between transceivers (radio) are always transmitted cryptographically protected data.

Any information processed by different discrete calculators can eventually be represented by a sequence of bits (0 or 1). This representation, in fact, is used in its conversion using a variety of dynamical chaotic systems. However, in computing systems to represent different types of data they use larger units that is to say 88 bytes (bit), and machine words from 16 to 64, usually depending on the machine digit capacity. Most commonly byte representation of information is used. Thus, the code tables in computing systems for representing textual information indicate correspondence between 256 bytes and characters of different scripts.

In many cases, the use of the byte information representation also simplifies algorithms of its processing by computing systems. Therefore, we will further consider the byte to be a unit of digital information, and the information processed in computer environment, will be represented as a sequence of different bytes.

The method of data encryption will be the method of direct information conversion by a dynamical chaotic system using forward and backward systems.

The encryption algorithm used in this work is based on the use of discrete analogue of the Lorenz dynamical chaotic system [7].

The final Lorenz machine is described by the system of equations:

$$\begin{cases} x_1(t+1) = x_1(t) + hA_1(x_2(t) - x_1(t)); \\ x_2(t+1) = x_2(t) + h(A_2 x_1(t) - x_2(t) \\ \qquad\qquad - x_1(t)x_3(t) + Au(t)); \\ x_3(t+1) = x_3(t) + h(x_1(t)x_2(t) - A_3 x_3(t)); \end{cases}$$

$$y(t) = x_2(t) + h(A_2 x_1(t) - x_2(t) - x_1(t)x_3(t) + Au(t)).$$

Whereas, an additive component – the current input symbol of initial information $u(t)$, $y(t)$ is the relative symbol of ciphered information. A set of input and output symbols, components $x_i(t)$, i =1, 2, 3 are understood as the elements of the Galois field $GF(q)$ or the ring $Z(q)$, and operations of addition or multiplication are relative operations in this field or ring. This allows the use of inexpensive signal processing controller is not great AC.

For digital information conversion, the fields and rings of characteristic 2 are usually used, that is to say $q = 2n$, $n \in N$. Given the nature of information representation in the computer memory, the program uses the fields $GF(2^{8k})$ or the rings $Z(2^{8k})$, k = 1, 2, 3, 4. This is due to the fact that the information file is stored in the computer memory as a sequence of bytes. There are several types of the Galois field representation. The program uses two of them: integer representation, and vector representation. Implicitly, polynomial representation is also applied in developing calculation algorithms in the fields.

Decryption is done by the reverse Lorenz machine, which exists for every $A \in GF(q)$ or $A \in Z(q), A \neq 0$.

The key of the decryption system are system coefficients and initial state for the machine. Now we represent the system of Lorenz equations as follows:

$$\begin{cases} \dot{S}_1 = a_{11}S_1 + a_{12}S_2; \\ \dot{S}_2 = a_{21}S_1 + a_{22}S_2 + a_{23}S_1S_3 + a_{24}u; \\ \dot{S}_3 = a_{31}S_3 + a_{32}S_1S_2; \end{cases}$$
$$y = \dot{S}_2.$$

Coefficients (a_{11}, a_{12}, a_{21}, a_{22}, a_{23}, a_{24}, a_{31}, a_{32}) of the Lorenz machine, as well as initial states S_1, S_2 S_3 are the key for the encryption system. If needed, the key parameter may be also the value k that indicated the size of the processed block of information (information bit) in k byte.

The major steps of the ciphering algorithm are:

– initialization (setting) of the machine – coefficients, initial state according to the encryption key state and the size of the quantum are set;

– processing of the next quantum of information in accordance with the system that is in the current state, along with release of the encrypted quantum and transition to a new state. This step is repeated until the end of the file being processed.

Re-calculation of the values of the machine states S_i is performed in the field $GF(2^p)$ or in the ring $Z(2^p)$.

The addition algorithm is simple, since only the fields and rings of characteristic 2 are used. The addition algorithm applies integer representation of the field or ring elements. The division algorithm is carried out using the following formula: $\frac{a}{b} = ab^{-1}$. The reverse element b^{-1} is calculated using the following formula: $b^{-1} = 2^p - b + 1$, where b is represented as a whole-number value. When carrying out this operation, vector representation is converted into the whole-number representation, and then visa versa. Despite the fact that the operation of taking an inverse element is performed in the program once when calculating the coefficients of the inverse machine, such method of calculating the inverse element is acceptable.

An encryption system using the Lorenz machine is symmetrical. This means that when decrypting the file the same key is used as for encryption. Lorenz reverse machine is defined by the system:

$$\begin{cases} S_1^{`} = a_{11}S_1 + a_{12}S_2; \\ S_2^{`} = a_{21}^{back}S_1 + a_{22}^{bsck}S_2 + a_{23}^{back}S_1S_3 + a_{24}^{back}y; \\ S_3^{`} = a_{31}S_3 + a_{32}S_1S_2; \end{cases}$$
$$u = S_2^{`},$$

where $a_{21}^{back} = \frac{-a_{21}}{a_{24}}$, $a_{22}^{back} = \frac{-a_{22}}{a_{24}}$, $a_{23}^{back} = \frac{-a_{23}}{a_{24}}$,

$a_{24}^{back} = \frac{1}{a_{24}}$.

Re-calculation of coefficients of the reverse machine occurs during system setup for file decryption. As a result of encoder output will be a sequence, which should have the properties of a pseudo-random one.

To study the pseudo-random sequence of numbers, there are two groups of tests.

Graphic tests. Statistical properties of sequences are displayed as curves, the form of which is used to make conclusions about the properties of the sequence under test.

Evaluation tests. Statistical properties of sequences are defined by numerical characteristics. Based on evaluation criteria, conclusions about the proximity degree for characteristics of the sequence under test and a true random sequence are made. To estimate the pseudo random sequence of numbers generated using the Lorenz system, a package of statistical NIST tests was applied [8].

To visualize the input, as well as the output binary sequence it is divided into 560 equal parts, and then recorded as rows of some matrix. The image of such

matrix is shaped according to the following rule: a black square represents an element that is equal to "0", while a white square is an element equal to "1". The following graphs (Fig. 2) represent:

– the sequence consisting of units;

– the sequence that has some kind of periodic nature;

– a random sequence.

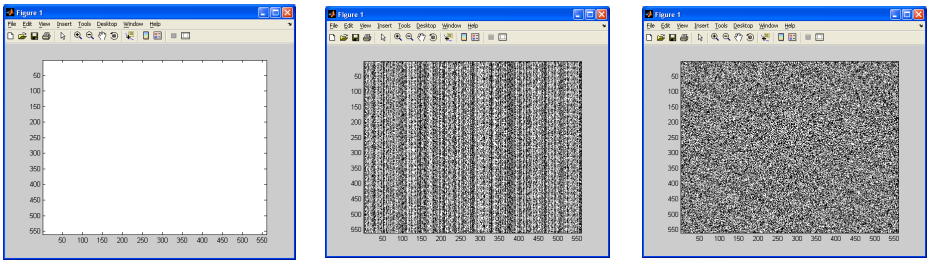

Fig. 2. Visualization of binary sequence

For encryption, the Lorenz system was used in finite rings (2^p) and fields GF (2^p) $8 \leq p \leq 128$.

Test 1. Analysis of algorithms using graphical visualization. For this test 10 various incoming sequences of 320 000 length were used. Each sequence was ciphered by each algorithm 20 times with different, randomly chosen parameters. As a result of the tests performed, the following conclusions were made:

1) On ciphering in the ring Z (2^8) using the Lorenz system, no uniform image was observed in any case (Fig. 3).

2) Where there are distinct areas in the source file, their contours remain in the output file.

Sample 1. Encryption using the Lorenz system in the ring Z (2^8).

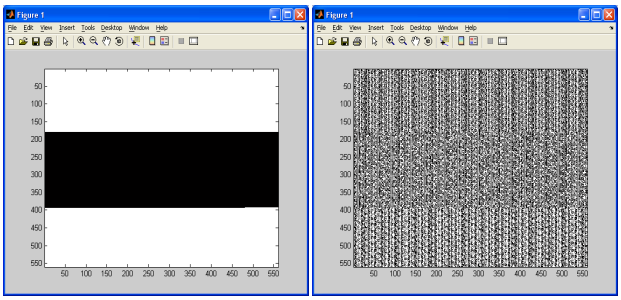

Fig. 3. Lorenz encryption systems in the ring Z (2^8)

– When the ring output increases, the 'blurring' improves.

– When non-linearity is added in the first equation of the Lorentz system, the picture 'improves' slightly.

– In the fields GF (2^8), GF (2^{16}), the modified Lorenz system has a uniform blurred image.

Test 2. Using the package of NIST statistical tests to assess the quality of pseudo-random sequence generators. In this test, a sequence of units of length 1,000,000 is encrypted 125 times. Each parameter moves in increments of $2^p/5$, and all possible combinations are considered. Thus, we obtained 125 sequences. A battery of NIST tests in applied to them.

The NIST tests show that encryption by the Lorenz system in the ring Z (2^8) produces an unsatisfactory result. With the increasing ring output the result improves while the test time reduces. When adding a predicate to the system a slight improvement of the result is observed. Performing all operations in the fields GF (2^p) significantly improves the results.

For comparison, we implemented the algorithm A5 [9], is used to produce a pseudo-random sequence of three linear shift register with feedback, and the algorithm RC4 [9], specifically designed for stream ciphers. A5 algorithm is used to encrypt the session between the telephone subscriber's handset and the base station in the European digital mobile communication system GSM (Group Special Mobile).

As a result of experiments, it was found that ciphers using inverse control system for the conversion and transmission of information in the field GF (2^{16}) or ring Z_{32} is not as effective as known algorithms and have high speed performance. Thus, a new algorithm has a high degree of protection and can be used for secure transmission of messages via telecommunication line or by other means.

III. CONCLUSIONS

The present study has analyzed the issues of closing the communication channel with unmanned aerial vehicles by cryptographic means. The requirements applicable to such means have been defined.

The developed software package realizes one of the possible algorithms of cryptographically secured transmission of broadband video signals from the UAV board to the Ground.

Any controlled dynamic system with the input-output structure can be used directly for conversion of information. The idea of using inverse control systems with complex behavior of trajectories is at the heart of the objective to synthesize a new efficient algorithms of information protection, primarily from the unauthorized access.

The researches carried out and their evaluation allow us suggest that we obtained new results that extend the theoretical basis of the modern cryptology and seem to be efficient for developing efficient cryptographic algorithms. At the same time, there is a number of open issues related to the impact of dynamic parameters on the stability of cryptographic algorithms to attacks, resistance to information distortion, and appearance of invariant varieties.

REFERENCES

[1] V. Slyusar. (2010). Data transmission from the board of the UAV: NATO standards. *ELECTRONICS: NTB*, no. 3. pp. 80–86. http:// www.slyusar.kiev.ua /UAV-1.pdf

[2] V. M. Ilyushka and T.M. Narytnik, "The data transmission system based on high-altitude unmanned aerial vehicle (SPD "Phaeton")". *Communication*, 2004, no. 7. pp. 38–39.

[3] S. V. Galushko, "Unmanned aerial vehicles radically change the face of the future of aviation". *Science and Life*, 2001, no. 9, pp. 18–20.

[4] V. V. Kirichenko, "The effectiveness of the use of inverse control systems for the conversion and transmission of information." *Abstracts of the 11th International Scientific and Technical Conference* "*Modeling, identification, synthesis control systems*". Moscow. 2008, pp. 46–47.

[5] V. V. Kirichenko, "Using inverse control systems for encoding and transmission." *Abstracts of Scientific and Technical Conference* "*The problems of global communication, navigation, surveillance and air traffic management CNS/ATM*". 2014, Kyiv. 139 p.

[6] A. M. Kovalev, V. A. Kozlovsky and V. F. Scsherbak, Generalized Inverse dynamical systems in problems of encryption, *Applied Discrete Mathematics*, 2009, no. 1, pp. 20–21.

[7] M. J. Sobhy and A. Shehata, Secure computer communication using haotic algorithms. *Int. J. of Bifurcation and Chaos*. vol. 10, no. 12, 2000, pp. 2831–2839.

[8] *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, San Vo. National Institute of Standards and Technology Special Publication 800-22 revision 1a, April 2010. 131 p. http://csrc.nist.gov/groups/ST/toolkit/rng /documents/SP800-22rev1a.pdf

[9] B. Ya. Ryabko and A. N. Fionov, *Cryptographic methods of information protection*. Moscow: Hotline-Telecom. 2005, 232 p.

Received July 19, 2015

Kirichenko Victor. Ph. D. Associate Professor.
Aircraft control systems Department, National Aviation University, Kyiv, Ukraine.
Education: Donetsk National University, Donetsk, Ukraine (1999).
Research interests: control systems and data processing.
Publications: 43.
E-mail: vkir28@ukr.net

В. В. Кириченко. Інформаційна безпека каналу зв'язку з безпілотним літальним апаратом
В роботі проаналізовані питання закриття каналу зв'язку з безпілотним літальним апаратом криптографічними засобами. Сформульовано вимоги, пропоновані до таких засобів. Запропоновано спосіб шифрування інформації, що використовує пряму і зворотну динамічні системи. З програмою шифрування - дешифрування виконано ряд експериментів з перетворення інформації, які показали деякі особливості алгоритмів, заснованих на вищевказаних системах.
Ключові слова: керування рухом літака; безпілотний літальний апарат; канали зв'язку БПЛА; криптографічний захист; пакет блоку шифрування; система Лоренца; кільце цілих чисел.

Кириченко Віктор Вікторович. Кандидат фізико-математичних наук. Доцент.
Кафедра систем управління літальних апаратів, Національний авіаційний університет, Київ, Україна.
Освіта: Донецький Національний університет, Донецьк, Україна (1999).
Напрямок наукової діяльності: системи управління та обробка інформації.
Кількість публікацій: 43.
E-mail: vkir28@ukr.net

В. В. Кириченко. **Информационная безопасность канала связи с беспилотным летательным аппаратом**
В работе проанализированы вопросы закрытия канала связи с беспилотным летательным аппаратом криптографическими средствами. Сформулированы требования, предъявляемые к таким средствам. Предложен способ шифрования информации, использующий прямую и обратную динамические системы. С программой шифрования - дешифрования выполнен ряд экспериментов по преобразованию информации, которые показали некоторые особенности алгоритмов, основанных на вышеуказанных системах.
Ключевые слова: управление движением самолета; беспилотный летательный аппарат; каналы связи БПЛА; криптографическая защита; пакет блока шифрования; система Лоренца; кольцо целых чисел.

Кириченко Виктор Викторович. Кандидат физико-математических наук, доцент.
Кафедра систем управления летательных аппаратов, Национальный авиационный университет, Киев, Украина.
Образование: Донецкий Национальный университет, Донецк, Украина (1999).
Направление научной деятельности: системы управления и обработка информации.
Количество публикаций: 43.
E-mail: vkir28@ukr.net