Hardware Data Encryption Complex Based on Programmable Microcontrollers

Nataliia Tmienova[1] and Bogdan Sus[2]

[1] Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[2] Institute of High Technologies of Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
tmyenovox@gmail.com, bnsuse@gmail.com

Abstract. The growing danger of computer crime puts forward a new set of urgent tasks. At the same time, the development of hardware encryption systems can be effective in the solving some of them. To study the hardware possibilities of reducing the probability of unauthorized access to information, an available complex for demonstrating data encryption based on programmable microcontrollers is proposed. The article provides a diagram of the corresponding demonstration complex with a description of its work.

The algorithms and methods of information protection between devices using combined communication channels and embedded systems are offered. The software-hardware complex, which uses a combination of engineering and software solutions, provides the possibility to conduct spectral analysis of data streams and research noise and signals that may occur in optical communication lines and radio channels.

In addition, this complex can be used for laboratory work on cryptography and data protection in communication lines.

Keywords: Cryptography, Hardware Encryption Systems, Programmable Microcontrollers, STM32, Security, Privacy, Forensics Analysis, Embedded Systems.

1 Introduction

Currently, a growing trend of data security disturbance is being observed. Information leaks often occur as a result of poor security management or as a result of using outdated or improperly implemented security procedures and technologies. Data encryption using appropriate key management schemes can significantly reduce data leakage.

However, when we use the key methodology, the following main problems arise: the generation and safe transfer of keys to interaction participants; setting of a secure information transmission channel between the interaction participants before the transfer of keys; authentication. There are two key methodologies: symmetric (with a secret key) and asymmetric (with a public key). Each methodology uses its own procedures, its own key distribution methods, key types, as well as key encryption and decryption algorithms [1].

Although cryptography with well-known standards, modern algorithms and libraries is quite effective, the development of hardware encryption systems still remains an urgent task [2, 3]. Information security software tools are potentially vulnerable, since the entire process of encoding (encrypting/decrypting) data is performed in the internal computer memory, which can be accessed by any application running on the computer.

This means that it is possible to conduct multi-level attacks on any software, including the one aimed at ensuring the security of the information. Thus, it is practically impossible to build a high-level protection by software tools only [4]. To restrict access to means performing cryptographic transformations, it is necessary to transfer them from a computer to a closed hardware subsystem.

As a result, the attacker will not be able to access directly the encoding processes (encryption/decryption). Firstly, the hardware implementation of the encryption algorithm guarantees the invariance of the algorithm itself, whereas the software algorithm can be intentionally modified. In addition, the hardware encoder eliminates any interference in the encoding process.

Another advantage is the use of a hardware random number generator, which guarantees absolute randomness of the generation of encryption keys and improves the quality of the implementation of various cryptographic algorithms. In addition, the hardware encoder allows you to load directly encryption keys into the encryption processor, bypassing the computer's RAM, while in the software encoder the keys are in memory even during the operation of the encoder. It is important that it is possible to create various systems for distinguishing and restriction of access to computer on the base of the hardware encoder. Also, the use of hardware systems makes it difficult to conceal evidence of interference in the communication channel [4].

In this paper, to investigate the hardware capabilities of reducing the probability of unauthorized access to information, an accessible data encryption complex based on programmable microcontrollers is proposed. This embedded system allows the combined use of optical and wireless communication channels.

Optic-fiber communication lines allow the information transfer over long distances with minimal distortion, which allows improving the protection technology of information transmission in optical communication lines from the harmful effects of intruders due to unauthorized connection.

The use of polarization modulation of light in the hardware complex arouses the additional interest. With the help of optical information of processing devices, the decomposition of optical signals is performed by a given system of functions. The work of such devices is based on the application of electronically controlled anisotropic environment that change the polarization of the light beam. This effect allows to process signals.

This complex can also be used to successfully students' study of technologies, algorithms and physical methods of encryption and secure transmission of signals in communication channels, hardware capabilities of reducing the probability of unauthorized access to information upon data leakage during laboratory work.

2 Complex Description

To evaluate the effectiveness of data encryption algorithms in optic-fiber systems, a number of practical solutions that include software codes and hardware implementation based on embedded systems have been developed.

Optical fiber, preferably, does not have protection from third-party connections and listening. At present, a large amount of critical information is transmitted through the optical channel, and there is the risk that it may get to the intruders who has the necessary resources and equipment. Connection to optic fiber is a process in which the security of an optical channel is disturbed by the flow or leakage of light information. Therefore, a combination of standard optical channels with the radio channels, which are switched by a special algorithm, is offered. This complicates the information leakage when connecting of intermediate device.

Nowadays, there is a need for new effective ways of encryption keys forming. Additionally, the access key can be transmitted by the means of RFID cards. The possibility of using a hardware random number sensor, which produces a statically random and unpredictable signal converted then into a digital form, guarantees the possibility of encryption keys generating and improves the quality of the various cryptographic algorithms implementation.

The suggested encryption does not eliminate the possibility of data intercepting through the optical channel, but makes stolen information inappropriate for intruders. There are high requirements to RFID systems, since these systems are very tiny with power from the electromagnetic field.

The complex is based on the high-performance microcontroller of STM32 series [5, 6].

To connect the transmitters, receivers and the computer, the device interface is used.

The information encryption complex has the following basic functions:

- transmission and reception of signals by separate optical channels;
- transmission and reception of signals over a common optical channel with the use of spectral multiplexing;
- transmission of signals or encryption key via radio channel with the use of digital noise filtering algorithms;
- the possibility of synchronous switching of communication channels.

The diagram of the demonstration complex is shown in Figure 1.

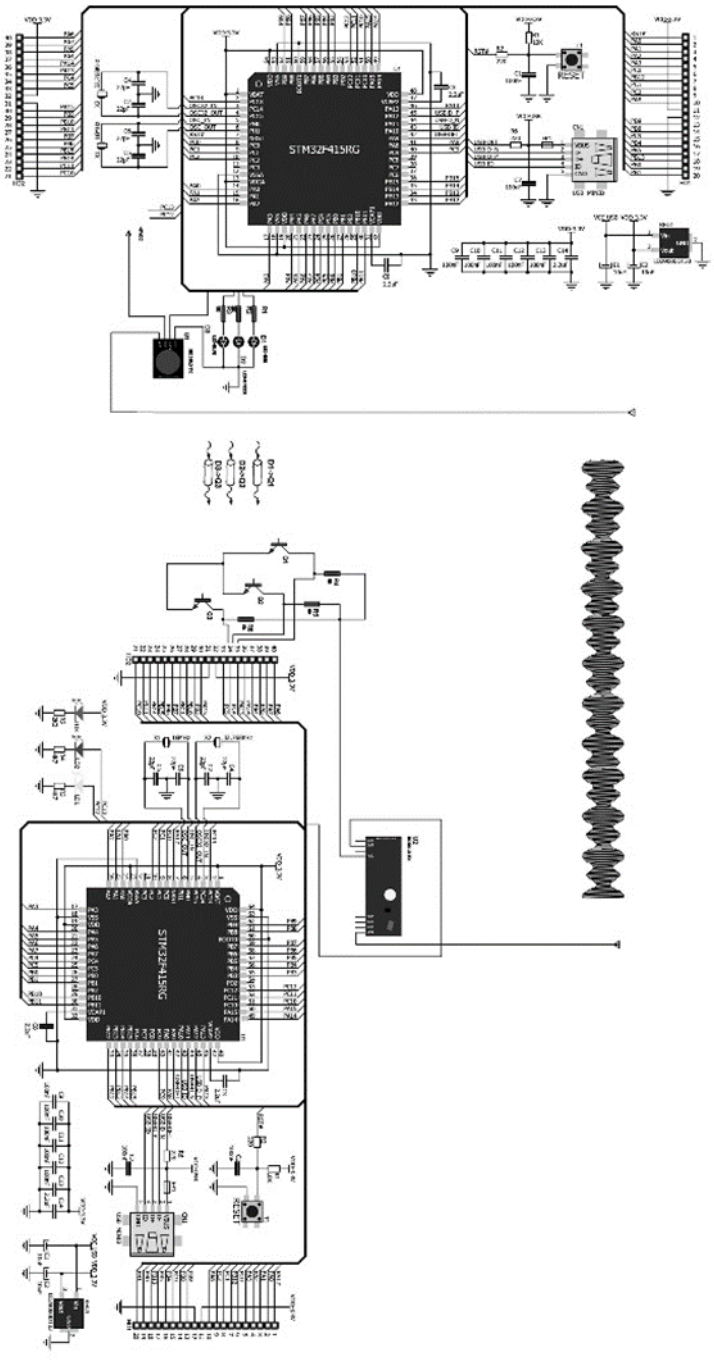

Fig.1. Diagram of the demonstration complex.

A modified VirtualWire open source library for STM32CubeMX [7] is used for radio modules functioning. For encoding signals, STM32 library for AES Encryption and x-cube-cryptolib libraries are implemented, which support such encryption algorithms as AES-128, AES-192, AES-256, ECB (Electronic Codebook Mode), CBC (Cipher-Block Chaining), CTR (Counter Mode) CFB (Cipher Feedback), OFB (Output Feedback), CCM (CBC-MAC), GCM (Galois Counter Mode), CMAC, KEYWRAP, XTS); hash functions supported by HMAC (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) [8, 9].

The devices transmit a message, which can be additionally encrypted by the software and hardware means. When software encryption is used, all types of information are splitted into short fixed-length packages containing special headers (so-called cells). At the next step, the spectral multiplexing in the digital channel is implemented. In this case, the cells may have different priorities.

The message is entered into the terminal program window of the STM32 module that is used as the transmitter. For the evidence in the case of demonstration mode of transmitting information through an optical channel, red, green, and blue LEDs can be used. Each color of the LED symbolizes a separate data transmission channel.

For transmission of data, the radio channel on available modules MX-F01 and MX-RM-5V was used. The module can be implemented to RC-control of models, security and automation projects, and wireless sensors systems construction up to 150 m [10]. The connection between the radio modules and the microcontroller is organized through the peripheral interface of the USART (Universal Synchronous/Asynchronous Receiver-Transmitter) in UART5 mode operation. The transmitting module is connected to a PC12 pin configured to data transmission via the USART interface, and the PD2 output configured as receiver.

Additional ARM CryptoCell hardware features can be activated in the case of use nRF52832 transmission modules. The nRF52832 integrated circuit is a powerful, highly flexible ultra-low power multiprotocol system on chip suited for Bluetooth low energy and 2.4GHz ultra low-power wireless applications. The nRF52832-MDK 2.4GHz open source modules can be also used with nRF5 SDK, nRF5 multi-frameworks. It enables access to 24 I/Os, interfaces via headers, and has a programmable RGB LED for optical communication. Module has a 2.4GHz chip antenna onboard, which is quite convenient to develop Internet of things wireless secured applications. It enables STM32 CPU host offloading and acceleration of operation and the increase of cryptographic endurance and date conversion speed [11].

The number of LEDs and radio modules can be scaled according to the number of data channels. Additionally, it is possible to use RFID labels to change configuration settings and encryption keys. During transmission of encrypted message, synchronous switching of channels is implemented (switching of transmitters and receivers according to a certain encryption algorithm) (Fig. 2). The reception efficiency varies depending on the transmission speed and the delay between the packets. In this demonstration device, a combination of optical channels with spectral multiplexing of signals, combining multiple channels into one stream, use of delays, transmission of redundant information, noise overlays and a hopping code algorithm can be also used.

In the radio channel, the function of the transformation in the frequency band is also possible. With the change of carrier frequency for different signals, each of them can be transferred to another frequency band using a cyclic inversion.

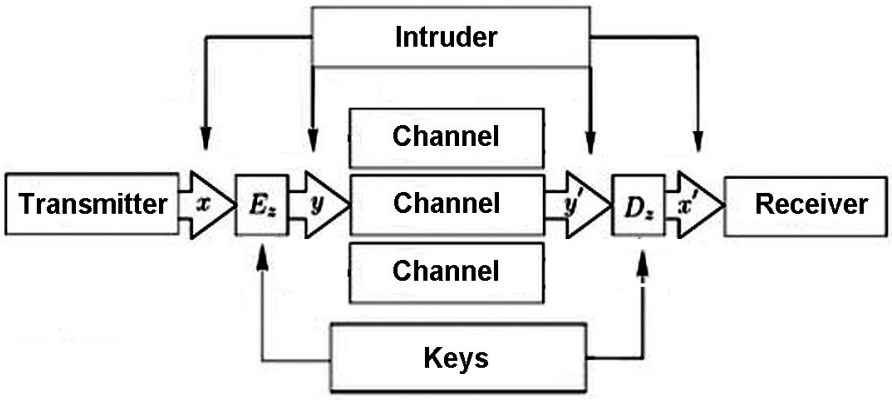

Fig.2. Switching of receiver and transmitter (x - data packets, y - encrypted data, Ez - encryption algorithms).

As the use of radio transmitters and receivers with digital frequency synthesis, the implementation of the hopping frequency tuning is possible. As an optical fiber, an OD AV Optical Fiber Cable of type Toslink can be used. The decrypted message is displayed in the serial port terminal program window that receives data from the STM32 controller, which operates in receiver mode. This encoding is especially effective for the transmission of short data packets.

Digital processor systems are always operate in a precisely defined state, which changes only when a certain command is received from a program. Randomness is emulated during generation so-called pseudo-random numbers by the means of a special mathematical function. Since the set of such numbers looks completely random, an attacker using the same procedure can easily generate exactly the same numbers. Such procedures are not well suited for strong encryption.

Therefore, our installation operates with additional analog random sequence generator, which is assembled from the available elements. The sources of entropy are the phase shift detector of the AC power supply, the noise detector of the radio transmitter, and the quantum noise of the photo charge-coupled detector of the camera. Johnson noise is chosen as the main source of random numbers, which is generated by all passive resistive elements of the electrical circuits of the installation. Since it is a thermal noise due to the thermal motion of atoms, its value increases with temperature and resistance, and makes up the most significant component of entropy in this random sequence generator.

Additional encryption of information in the optical channel is possible by changing the polarization. The use of polarized light in the device allows to realize the optical representation of alternating functions or matrices and to carry out both direct and reverse transformations in one cycle, simultaneously obtaining in the initial plane of the corresponding combination of light fields by polarization and intensity. The operation of polarization cells on liquid crystals and analyzers is varied according to encryption algorithm. After each iteration of the algorithm, the nuisance parameters are re-estimated using their revised means, conditional on the updated set of change points. The low speed of information transmission in this mode is limited with the use of low-cost electromechanical systems for polarizer and analyzer devices. The polarization modulation provides the optical realization of direct and reverse transformations in the communication line, as well as the separation of channels in the digital transmission of data. The software solution can be easily adapted for 32- and 64-bit microcontrollers with architecture ARM7 and ARM9.

3 Using of the Demonstration Complex in the «Internet of Things»

The complex is designed to selection of the optimal multi-channel technology for data encryption in microcontroller systems with limited memory. Currently, computer systems, including intelligent systems, automated and telecommunication systems for managing things consist of a wide range of embedded devices. Especially it concerns the so-called «Internet of Things», which is a wireless network that is self-configurable between objects of different classes.

The wide implementation of embedded systems requires an integrated combination of software and hardware solutions for the protection of information both in the computing systems and in communication channels. Such devices can often store some amount of indirect information about the behavior of their owners. Information can be obtained from the analysis of various received signals, even in analog form, from the objects of monitoring and from signals of control to these objects.

For example, indirect information can be obtained from the analysis of intercepted signals from monitoring objects and semiconductor sensors, usually in analog form. The outgoing control of these objects in the form of discrete and continuous signals, as well as the conversion of analog signals into digital and vice versa during the digital transmission of data through standard interfaces can be also intercepted.

In «Smart Home» systems, for instance, most of devices are electronically controlled. Any controlling device or computing device can be potentially used for criminal activity, so it is highly desirable to split this information into parts and apply the encryption. (For example, the stream of video data from CCTV cameras or video registrators, it is desirable to split into separate encrypted channels and transmit through the combined lines of communication in order to reduce the probability of interception or falsification of data).

But the most important task on the «Internet of Things» is to ensure the security of the main and additional data communication channels. Implementation of optical and wireless interfaces for connecting the main embedded devices to «Smart Home» systems and the use of combined communication channels will significantly increase the security of data transmission. The intruder must have physical access to all memory chips and use reverse engineering technology to obtain low-level information from the flash memory chips to get some data only about the encryption algorithm. Due to the implementation of the multichannel data transmission circuit, the CPU load is also reduced.

The complex provides an opportunity to carry out modeling in the engineering design of prototypes of a secure system for the «Internet of Things» and to investigate the technical characteristics of the expected equipment. It is possible to conduct a comparative testing of the security of data of various devices, depending on the used channel, the algorithm and the key of encryption and communications. Since the encryption key can be transmitted over a channel that is randomly selected and can be split into parts by the special algorithm, this significantly complicates the access of potential intruder and analysis of the encrypted information. Another advantage of the suggested system is the possibility of scaling the number of communication channels without significant increase of the costs and the ability to support various encryption protocols without major reconfiguration of the system.

4 Using of the Demonstration Complex for Conducting of Laboratory Activities

This complex has been used to successfully students' study of technologies, algorithms and physical methods of encryption and secure transmission of signals in communication channels. Most of the activities were performed in the laboratories, where students have the opportunity to setup experiments with spectrum analysis, optical communications and wireless transmissions. Hardware capabilities and appropriate signal-processing algorithms of reducing the probability of unauthorized access to information upon data leakage during laboratory activities in «Electronics and microprocessor technology», «Programming the Internet of Things» and «Security of Networks and Computer systems» have been studied in practice.

For modeling of periodic encrypted data the noise is considered as a set of displacements from the underlying periodic sequence in the data. The resulting high frequency data sequence is digitized as a wave, using the Fourier transform, decomposed into harmonic components. Encrypted data packets can be easily represented as digitized wave functions. In such case, encryption is a process that is identical to radio transmission when high-frequency radiation is modulated by a low-frequency signal.

For the spectrum analysis of the radio signals additional low-cost radio frequency experimentation board USRP B210 was used. Software Defined Radio provides a common API, which is used by several software frameworks [12]. It allows receiving and transmitting any radio signal in the range from 70 MHz to 6 GHz.

It should be noted that the application of the described demonstration complex showed the effectiveness and feasibility of its use during the laboratory work on the discipline «Security of Networks and Computer systems». We discovered that the use of hardware systems at laboratory activity contributes to improving of material mastering on a related topics by about 20 percent in the control group of students. It is important that students were actively studying during activities with the demonstration complex.

Active learning involves an active role of students in the process of new knowledge or skills obtaining [13]. An integral part of such training is the integration of software with hardware systems and devices. Students who are actively learning likely recall information in various situations related to solving of specific interdisciplinary tasks in practice during development of their applications. In this training, students learn to not only how to create prototypes of secure communication and implement interdisciplinary projects but also receive a set of non-specialized, professional skills that are responsible for high performance and successful participation in the learning process.

5 Conclusions

The growing danger of computer crime poses a set of new topical issues. At the same time, the development of hardware encryption complexes can be effective on the way to overcome some of them.

The discussed demonstration complex allows us to assess the efficiency of encrypting data streams in channels, compare packets received from the transmitter with the number of sent data packets, analyze the spectrum of the encrypted signal and the radio channel noise by the means of computer graphics techniques.

In addition, the complex provides an opportunity to carry out modeling in the engineering design of prototypes of secure systems for the «Internet of Things» and to investigate the technical characteristics of the expected equipment. It is possible to conduct a comparative testing of the security of data in various devices, depending on the used channel, the algorithm and the key of encryption and communications.

We also note that the demonstration complex can be used for conducting of laboratory classes for the development of protocols and algorithms for the transmission of information and digital signal processing filters analysis, periodic subsequences, duration of inactivity and user-driven events detection, and calculation of statistical parameters of encrypted channel data as close as possible to random distribution.

The complex makes it possible to conduct physical experiments to monitor signals in an optical fiber and a radio communication channels for the choice of an optimal algorithm for encryption stability and simulation for coherent and incoherent optical processors.

The proposed approaches can be used to modify data transmission equipment and evaluate the reliability of encryption. It can be also used for the reverse engineering demonstrations and laboratory activities.

This complex can be successfully implemented in the following areas: banking, military and medical industries, telephony. The main advantages include the reliability of transmission, the simplicity of implementation, the flexibility of the functionality and the possibilities of application and modernization.

References

1. Introduction to Cryptography - authorized translation of an article by J. Chandler "Cryptography 101" (in Russian) [Electronic Resource]. Mode of access: http://citforum.ck.ua/security/cryptography/crypto_1.shtml
2. Security of information systems (in Russian) [Electronic Resource]. Mode of access: http://intuit.valrkl.ru/course-1312/index.html.
3. Security with STM32 & Secure Elements [Electronic Resource]. Mode of access: http://www.emcu.it/SILICA-STDay2016/X/Presentazioni/2_STM32&SecureElements.pdf
4. Stallings W. Cryptography and network security: principles and practice. – New York: Prentice Hall, – 2006. – 680 p.
5. Cortex-M Series from ARM.com [Electronic Resource]. Mode of access: http://www.arm.com/products/processors/cortex-m.
6. Cortex-M4 Technical Reference Manual. [Electronic Resource]. Mode of access: http://infocenter.arm.com/help/topic/com.arm.doc.ddi0439b/DDI0439B_cortex_m4_r0p0_trm.pdf
7. VirtualWire library for Arduino and other boards [Electronic Resource]. Mode of access: https://www.airspayce.com/mikem/arduino/VirtualWire/
8. STM32 cryptographic library (UM0586)) [Electronic Resource]. Mode of access: https://www.st.com/en/embedded-software/STM32-cryp-lib.html
9. STM32 crypto library (UM1924) [Electronic Resource]. Mode of access: https://www.st.com/content/ccc/resource/technical/document/user_manual/group0/f9/6e/f2/a2/b4/ec/49/c0/DM00215061/files/DM00215061.pdf/jcr:content/translations/en.DM00215061.pdf
10. Complete Guide for RF 433MHz Transmitter/Receiver [Electronic Resource]. Mode of access: https://randomnerdtutorials.com/rf-433mhz-transmitter-receiver-module-with-arduino/
11. nRF52832 module [Electronic Resource]. Mode of access: https://www.nordicsemi.com/Products/Low-power-short-range-wireless/nRF52832
12. USRP B210 [Electronic Resource]. Mode of access: https://www.ettus.com/content/files/b200-b210_spec_sheet.pdf
13. Koppelman, H. Active learning in asynchronous distance education/ IADIS International Conference on Cognition and Exploratory Learning in Digital Age (CELDA 2009).