AMERICAN Journal of Science on Integration and Human Development
Volume 01, Issue 10, 2023 ISSN (E): 2993-2750

Analysis of Cryptographic Hardware

Makhkamova Dildora Begaliyevna
Tashkent University of Information Technologies, Tashkent, Uzbekistan

Abstract:

In this article, the characteristics of encryption cryptographic hardware and their analysis, as well as effective methods of hardware implementation of encryption algorithms are considered. Effective methods of hardware implementation of encryption algorithms are described in detail in the presented work. The advantages of a hardware encoder are shown, including that it allows encryption keys to be loaded directly into the encryption processor, bypassing the computer's RAM, while a software encoder stores the keys in memory while the encoder is running. Basic schemes and file encryption process are also presented in the article.

Keywords: Encryption, hardware implementation, CDPD, encoder, BIOS, the cryptographic processor, decryption.

Nowadays, there are technologies that allow to bring the guaranteed means of information protection as close as possible to a wide range of users and create personal encryption systems, which until recently were impossible due to a number of problems such as creation, storage and distribution of basic data, etc. Cryptographic algorithms are used for important tasks such as data encryption, authentication, and digital signature.

The hardware module includes means of generating the private key of the owner and is provided with protection mechanisms against obtaining information about the private key of the disposer.

Three types of encoders are most commonly used today as cryptographic encryption tools:

- software tools
- hardware
- hardware and software tools

Their main difference is not only in the method of encryption and the level of reliability of data protection, but also in the price, which is often a decisive factor for users.

In practice, the cheapest solution is software, followed by hardware and finally hardware. But although the price of hardware encoders is much higher than that of software, it is almost always justified by the high quality of information protection, which cannot be compared with the price difference.

First, a hardware implementation of an encryption algorithm guarantees that the algorithm itself is immutable, but a software algorithm can be deliberately changed. In addition, the hardware encoder eliminates any interference in the encryption process. Another advantage is the hardware that guarantees absolute randomness in the creation of encryption keys and improves the quality of the implementation of various cryptographic algorithms, for example, the electronic digital signature according to GOST R 34.10-94/2001 algorithms using a random number generator.

In addition, a hardware encoder allows the encryption keys to be loaded directly into the encryption processor, bypassing the computer's RAM, while a software encoder stores the keys in memory while the encoder is running. What is also important is that based on hardware encryption, you can create various systems to limit and restrict access to the computer. And finally, hardware encryption loads the computer's central processor.

The classic version of a hardware encoder for a personal computer is an expansion card installed in a slot on the computer's motherboard. Similar cryptographic data protection devices CDPD (CDPD - cryptographic data protection devices) are produced today by several Russian companies, including Ankad. As a rule, a hardware encoder includes a control unit, an encryption processor, a hardware random number generator, a controller, memory chips, operation mode switching keys, and interfaces for connecting main devices.

The control unit, as its name suggests, is used to control the operation of the entire encoder. It is usually based on a microcontroller. The encryption processor is a special chip or programmable logic device that performs data encryption. In general, CDPD has several encryption processors. can be, for example, mutual control (by quickly comparing received encrypted or plain data) and parallelization of the encryption process. To generate encryption keys, the device generates a statistically random and unpredictable signal, which is then converted into a digital form has a random number generator. Commands and data exchange between the encoder and the computer is provided by the controller. The interaction of the encoder with the computer's motherboard is carried out through the CDPD controller. To store the microcontroller program, a non-volatile memory installed in one or more microcircuits is required. The same internal ROM (ROM-read only memory) is used for recording the operation log and other purposes.

Interfaces for connecting key carriers provide more reliable protection. In principle, the keys can be stored on a regular floppy disk, but in this case they must be read through the system bus of the computer, which means that, theoretically, there is a possibility of intercepting them. Therefore, hardware encoders usually provide an interface to directly connect the main storage devices. In this case, it is preferable to work with connectors and Touch Memory electronic tablets to connect smart card readers.

In general, hardware encryption has two main modes of operation: boot and perform operations. The first starts when the computer starts up, when the computer interrogates all internal and external devices connected to it in the BIOS. Meanwhile, the encoder takes control and executes a sequence of commands hard-wired into its memory, prompting the user to first enter the master encryption key, that is, the corresponding key carrier to be used later. After the download is complete, the encoder waits for commands and data from the computer to perform encryption operations.

Basic schemes and file encryption process

Hardware encryptors must support encryption keys of several levels. Usually, a three-level hierarchy of keys is implemented: more levels, as a rule, no longer provide a significant improvement in the quality of protection, and a smaller number may not be sufficient for a number of basic schemes. possible A three-level hierarchy allows for the use of session or packet keys (level 1), long-term user or network keys (level 2), and master keys (level 3).

Each level of keys corresponds to a key cell in the cryptographic processor's memory. This means that data encryption is performed only on the first-level keys (session or set), and the rest are designed to encrypt the keys themselves when building different key schemes.

The three-level scheme is best illustrated by a simplified example of the file encryption process. During the initial boot phase, the master key is entered in keybox 3. But for three-level encryption, you need to get two more. The session key is generated by the encoder asking the RNG to get a random number loaded into the key cell 1 corresponding to the session key. It encrypts the contents of the file and creates a new file that stores the encrypted data. Next, the user is prompted for a long-term key, which is loaded into key cell 2 by decoding using the master key in the cell. By the way, a serious encryptor must have a key-to-key decryption mode inside the encryption processor; in this case the key never leaves the encoder. Finally, file decryption first encrypts the session key using the user's long-term key, and then recovers the data using it. In principle, a single key can be used for encryption, but a multi-key scheme has significant advantages.

First, the load on the long-term key is reduced - it is used only to encrypt short session keys. This makes it difficult for a potential attacker to cryptanalyze the encrypted data to obtain the long-term key.

Second, when you change the long-term key, you can encrypt the file very quickly: just re-encrypt the session key from the old long-term key to the new one.

Third, the key carrier is unloaded - only the master key is stored in it, and all long-term keys (and you can have as many as you want - for different purposes) can be stored encrypted with the master key.

To improve the functionality / price ratio, hardware encoders are equipped with various additional protection functions. The most useful and frequently used of them is the electronic lock function, which protects the personal computer from unauthorized access and allows you to control the integrity of the operating system files and used applications.

The memory of each encoder operating in electronic interlock mode shall contain the following information created by the security administrator or equivalent official:

- the list of users allowed to access the computer protected by this coder and the information necessary for their authentication;
- a list of managed files with a calculated hash value for each of them (except for operating system files, any other files can be included in this list, for example, the Normal.dot template used by default by the Microsoft Word word processor);
- a log containing a list of successful and unsuccessful computer access attempts;
- in the second case, indicating the reason for refusal of entry.

In today's development, where the volume of information exchange has increased dramatically, crypto-resistant tools that ensure the protection of information are being developed and put into practice. They are hardware-technical and hardware-software tools, and they differ in the speed of operation and tolerance of algorithms and other cryptographic features.

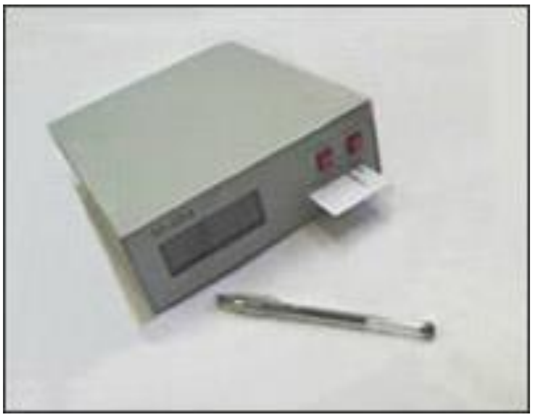

Figure 1. M-484 encoder

According to the technical characteristics of the M-484 encoder:

- operating speed: 40 kbit/s, 115.2 kbit/s in subscriber mode;

- operating mode multi-duplex;
- power consumption 220 V, battery 12-14V;

This device is certified and based on GOST 28147-89 encryption algorithm:

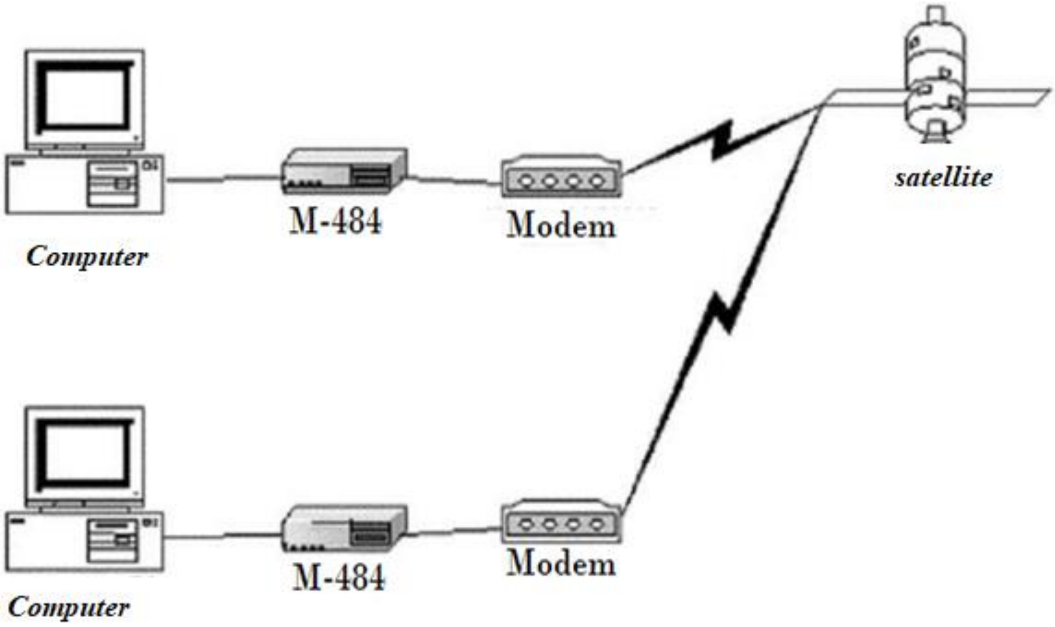

Figure 2. Schematic diagram of using M-484 in a network.

Figure 3. CN-9120 encoder.

The technical characteristics of the CN-9120 encoder are as follows:

- encryption algorithm AES 128-256 bits;
- maximum speed: 100gbit/s;
- operating mode: full duplex;
- encryption mode: CTR
- AES 128 or 256-bit keys;

Figure 4. CIS Crypto 4000 cipher

High-speed encoder "Polindrome" 40xx series encoder has the following features:

- implements information encryption at the 2nd level of the OSI model at a speed of up to 1 Gbit/s;
- encrypts information according to GOST R 34.12-2015 ("Kuznechik") algorithm in Gamma mode;

- Creates open and closed keys according to GOST P 34.10-2012 algorithm;
- Centralized automatic control system of keys;
- Body protected from physical effects;
- Availability of roles in product installation;
- the ability to configure the product through the SNMPv1/2/3 protocol or the console;
- Centralized automatic management of keys;
- Protection of packages from duplication;
- SFP or SFP+ internal and external network connections;
- Support for jumbo frames;
- External power source.

High-speed encryption "Polindrome" uses programmable logic circuits (FPGA) for data encryption, which allows data to be encrypted with minimal delays of up to 10 micro/s. Table 2.10 below is a comparison table of the advantages and disadvantages of this device. given.

Conclusion.

Cryptographic hardware and the basis of their operation were researched and existing hardware was analyzed. As can be seen from the comparison table of hardware encoders, they mainly implement US and Russian standards. Modern ciphers use GOST R 34.12-2015 ("Kuznechik") standards. High-speed encryption Polindrome" 40xx series cipher implements information encryption in gamma mode according to the GOST R 34.12-2015 algorithm; creates public and private keys according to the GOST P 34.10-2012 algorithm.

References.

1. S. Ganiev, M. Karimov and K. Tashev "Information security".2006.
2. Z.T. Khudoykulov, Sh.Z. Islamov, U.R. Mardiyev "Cryptography 1", Tashkent 2021.
3. V. Platonov "Software-hardware means of ensuring information security of high-speed networks". M.: Academy. 2006
4. https://securityboulevard.com
5. https://www.greengeeks.com
6. https://ieeexplore.org