Lightweight ciphers - CryptoWiki

Lightweight cryptography - section of cryptography, which aims at the development of algorithms for use in devices that are not able to provide most of the existing codes and have sufficient resources (memory, power, size) for the operation.

The use of lightweight cryptography

Most modern algorithms designed for use as part of a computer software systems without hardware optimization software. This fact makes it impossible to use most of existing cryptographic algorithms in devices with limited processing power, small volume and low power consumption. Methods of cryptographic protection of data in systems with low cost became the basis of lightweight cryptography.

Lightweight cryptography becomes relevant in the situation with "Internet of Things", which is a wireless self-configuring network between objects of different classes, that can include appliances, vehicles, smart sensors and RFID-tags (RFID).

Often developers of lightweight algorithms are forced to choose between the two, sometimes mutually particular requirements for algorithms: safety, cost and productivity. In practice, it is easy to optimize any two of the three design goals: safety and cost, safety and productivity or the cost and performance, but it is very difficult to optimize all three design goals simultaneously. In this regard, there are many implementations of lightweight cryptography algorithms: both software and hardware. They have different and sometimes conflicting characteristics.

The key aspects of lightweight cryptography

Innovative approaches to solve the problem of creating effective methods and understand means of lightweight cryptography are:

- use the classic cryptographic algorithms, if it possible;
- modification of the classical algorithms with adaptation to the hardware features and limitations of systems at a low cost;
- development of new specialized solutions in the methodological, algorithmic and software and hardware terms.

Each of these approaches has its drawbacks. Until now, most of the decisions in the field of knowledge refers to the third approach, and show good results. At the same time, however, it should be remembered that the cryptographic algorithm adaptation to the characteristics of the hardware basis with limited resources may have unwanted consequences. They can be expressed in the emergence of additional weaknesses in the algorithm or weakening their overall durability.

The main criteria for lightweight cipher

Firstly, it is an eternal search for a balance between reliability, performance and price.

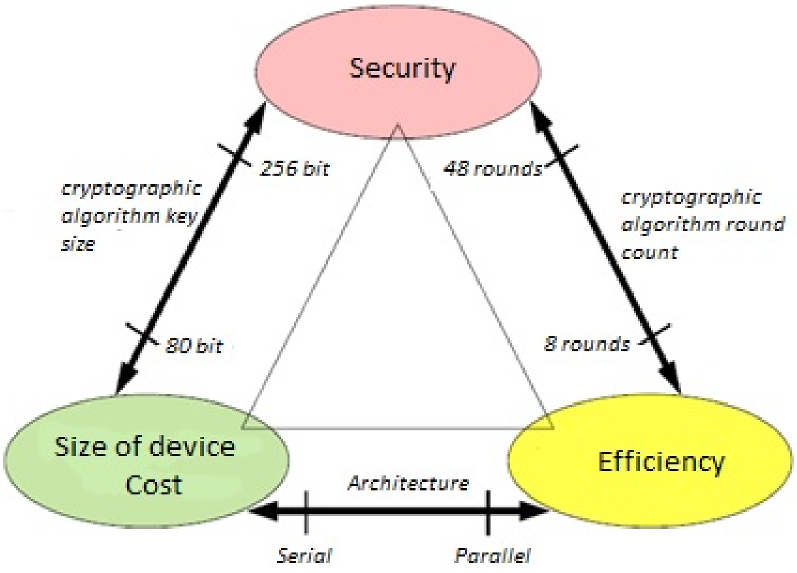

Figure 1. Interaction of reliability, performance and price scheme [14]

The key size of block cipher determines the ratio of the reliability / cost, the number of rounds of encryption - reliability / performance and features of the hardware design - price / performance. As a rule, any two of the three design goals can be easily achieved, while meeting all three requirements - an extremely difficult task. For example, it is possible to provide an acceptable balance between reliability and performance, however, to implement such algorithm will require a large area on the circuit, which leads to increased cost. On the other hand, it is possible to create a reliable and cheap system, but with limited capacity.

Secondly, chip area is limited.

Thirdly, it is important to power circuits, and accordingly,to define the type of the circuit (active or passive), depending on which will impose additional requirements to the circuit.

Are the lightweight encryption algorithms different from the universal? There are main approaches for cryptographers to get undemanding resources with relatively strong encryption algorithm:

- reducing the size of the main parameters of the algorithm: the block encrypted data encryption key and the internal state of the algorithm;
- attempts to compensate for involuntary loss of resistance due to the design of algorithms, based on well-studied, commonly used operations carried out by elementary linear / non-linear conversion. Such operations can be presented as part of a designer from which cryptographers "collect" algorithm has the right qualities;
- the use of "cheap" in terms of resource consumption, but the conversion efficiency, such as the control bits permutation (which selects a particular option permutations depending on the value of the control bit, this bit can be, for example, certain bit of the key), shift registers, and so forth;
- use of transformations for which the embodiments are possible depending on the particular resource encoder (e.g., reduced memory requirements, but at the expense of encryption speed, or vice versa).

It should be noted that the lightweight encryption algorithms are created either for low or medium level of security, or for systems, which will take into account the specifics of the algorithms and the solution that will be found to allow the implementation of an algorithm to make as safe as possible for its level of resistance.

One of the basic concepts that are used to consider the lightweight cryptography algorithms is GE - gate equivalent (the equivalent logic gate). This value is the measurement unit, which allows you to define the complexity of the production technology, regardless of the complexity of digital electronic circuits.

For the current CMOS technology it is equivalent to the gate NAND with two entrances. Table 1 presents a summary of the complexity of the implementation of various logic gates.

Table 1 — GE-area requirements of standard logic elements [14]

Element	Technological process, нм	Area, нм^2	GE
NOT	0,18	6,451	0,67
NOT-AND	0,18	9,677	1
NOT-OR	0,18	9,677	1
AND	0,18	12,902	1,33
OR	0,18	12,902	2,33
Multiplexor	0,18	22,579	2,67
Modulo 2	0,18	25,805	4,67
Modulo 3	0,18	45,158	5,33

Thus, while developing an algorithm for applying the lightness, observation the limit on number of equivalent gates, with which can be made hardware implementation of the algorithm. Initially it was thought that the maximum limit will be considered 2000-3000 GE, but at the moment, with the development of lightweight cryptography, this threshold was lowered to 1000 GE.

There are algorithms that are considered to be a reference. In cryptography, it is AES. It's standard is an algorithm in 1997, whose capacity reaches 70 Gbit / s (2004). However, this solution is not suitable for the lightweight cryptography, because the hardware implementation will require a 250,000 GE. At the same time there is a more compact implementation of AES, dated 2006, her figure is 3100-3400 GE. Unfortunately, today's requirements for lightweight cryptography, this indicator is also in excess of the permissible limits.

The main criteria for search lightweight algorithms is satisfying requirements for the hardware implementation of the algorithm. At the moment the threshold of 1000 GE was able to overcome only a small number of algorithms, some of which will be discussed in a future article in Lightweight block ciphers and Lightweight stream cipher

Determination of benefits and disadvantages of lightweight ciphers

Since the lightweight algorithms were developed for specific requirements, then it is directly followed the advantages and disadvantages of this family of algorithms. And the main advantage is the extremely low demand for resource and for power consumption, making the lightweight algorithms extremely fast in operation and "unpretentious" to the environment in which they will be carried out for work. In addition, it makes lightweight algorithms extremely inexpensive in implementation for for further usage.

However, since the lightweight algorithms are designed to handle small amounts of information, they do not have high bandwidth. The very existence of constraints in 1000 GE says that light ciphers primarily designed not to soft but to hardware implementation. As well as to realize, for example, more s-boxes in the block cipher algorithm, or use the key of great length, it requires more GE, then the developers of lightweight algorithms gets quite challenging.

In addition, these restrictions make it very difficult to optimize the existing algorithms to the requirements of lightweight cryptography, because many of them lost a lot of resistance, being limited in computing resources. This greatly delays the process of developing a lightweight algorithms, although there is a standard for encryption lite series ISO/IEC 29192. Moreover, it's increasing a number of successful attacks on the favorites among existing algorithms lightweight cryptography. All this makes the use of lightweight algorithms in practice highly specialized and quite challenging.

Right below are the articles that describe the implementation of the lightweight algorithms based on block and stream ciphers.

Lightweight block ciphers

This article describes the "lightweight" algorithms based on block encryption, namely:

- Present;
- GOST 28147-89;
- Clefia;
- Katan.

Lightweight stream ciphers

Talking about flow algorithms, it can be said that they are good for encrypting large amounts of data. All of these algorithms require initialization period, where the development of the internal state is done in the idle(there is no encryption). If encryption is required huge amounts of data, then the initializing time is negligible. However, for example, a traffic size of the RFID tag is so small that the initialization will exceed the time of encryption even more than several times. And, most likely, future development of lightweight algorithms will be given to the block algorithm.

In this article discussed such lightweight algorithms based on stream ciphers, as:

- Grain v1;
- Trivium;
- Bean;
- Hummingbird.

Practical application of lightweight cipher, singularity of their implementation

As shown above, the scope of lightweight cryptography algorithms has limited advantages and disadvantages of this family of algorithms. Practice has shown that one of the areas in which the lightweight algorithms gained immense popularity is the access system. This can be explained by two factors:

- firstly, the simplicity of implementation of the technology applied to the ACS (it's enough to use identifiers read-only with a small: three or four bytes - length of the code);
- secondly, convenience in comparison with any other types of identifiers: contact, with a magnetic stripe, Wiegand.

And since, according to IdTechEx, in 2015 will be produced 2 billion active RFID-tags and passive about a trillion, sharply raises the question of the protection of RFID-tags, where can be used lightweight cryptography. We should also mention the prospect of using lightweight algorithms for wireless communication between appliances, vehicles, fire and security detectors.

Definition of RFID-systems

RFID-Systems is one of the fastest growing areas in the field of computerization of small devices. RFID (Eng. Radio Frequency IDentification, RFID) - a method for the automatic identification of objects by means of radio signals which are read from or written to the data stored in the so-called RFID-tags. Any RFID-system consists of a reader and RFID-tags (sometimes also uses the term RFID-tag). Most RFID-tag consists of two parts: the integrated circuit for storing and processing information and an antenna for receiving and transmitting the signal. By type of power supply RFID-tags are divided into the following categories:

- passive;
- active;
- semipassive.

Passive RFID-tags have no internal power energy. The electric current, induced in the antenna as electromagnetic signal from the reader, provides sufficient power for operation of the silicon chip, placed in the label, and transmitting a response signal. Active RFID-tags have their own power source and does not depend on the energy of the reader, so they are read in the far distance, are large in size and can be equipped with additional electronics. However, such tags are most expensive, and have limited battery time.

Semipassive RFID-tags, also called semiactivity, are very similar to passive tags, but equipped with a battery that provides chip energy. Currently, RFID-technologies are used in a variety of fields from agriculture to transport.

According to CEO of the State Corporation "Rosnano" Russia may move to chips for credit cards with interactive radio RFID, by which in the coming years the world will have a revolution in retailing. Proving this we can bring the fact that "Rosnano" and IT-company "Systematics" create a venture to develop RFID tags. Investment in the project will amount to 690 million rubles and the company's revenue in 2015 should reach 800 million rubles.

In conclusion it can be said that these technologies will soon become widely spread. But do not forget about security issues. Particularly acute this problem stands in the application of RFID-technology in the military or financial spheres. Because of the rigid price controls, protection system should not only be reliable and productive, but also cheap in implementation.

Problems in ensuring security of RFID-tags

The main problem in securing RFID-tag is maintaining the confidentiality of the information stored in the tag. This is due to the fact that RFID technology allows to read information from a distance of several meters. Because of this, human rights defenders are often opposed to the mass distribution of RFID-tags, proving possibility in invasion of privacy. The following scenario is possible in unauthorized use of RFID-tags: the attacker, using the reader, is able to consider the victim's identifiers and use this information against it (to gain unauthorized access to a database and get information about moving or making a purchase). In other words, the technology of RFID-tags, in addition to the many benefits, has a number of drawbacks, not allowing the wide spread introduction of them.

Encryption in passive RFID-tags is a special case, even among devices with very limited computing resources. Passive RFID-tags do not have their own power supply, so they are activated by means of the induced signal reader. Thus, encryption chips must be less resource-intensive; RFID-tag must encrypt data and send response back to the reader before induced attenuation of the signal. Due to the severe restrictions on internal computing resources of RFID-tags, it becomes impossible to use existing cryptographic algorithms, which creates urgency of developing a lightweight algorithms corresponding to these restrictions.

Industry links

Small demands on processing power and low power consumption at a relatively high resistance - this combination makes it possible to ensure the confidentiality of information, not only when dealing with personal data stored on the RFID-tag, but also for wireless communication between devices, which contain the compromise information which is undesirable . General computerization leads to the fact that most of the things that surround us have access to wireless networks up to household appliances.

Thus, due to the economic costs, the rare manufacturer is worried about the security of the transmitted information. The use of lightweight algorithms, if threat not to close completely, at least reduce the likelihood of its implementation.

One way to protect vehicles - installation of car alarms, based on the authentication technology through unprotected channel, while interactive codes, especially in cheaper models, are transmitted in open way. The use of lightweight algorithms will improve the reliability of protection at the lowest cost of resources and energy consumption.

Wireless fire and security alarms are widely spread nowadays. They are easily installed and used, has flexible settings, including dynamic routing capabilities. However, to obtain an attacker access to the control system detectors, it is possible to create false alarms or disable the protection that raises the question of the protection of information transmitted in such systems. One of the solutions to this problem may be using lightweight algorithms.