Architectural Principles of Cryptographic Core

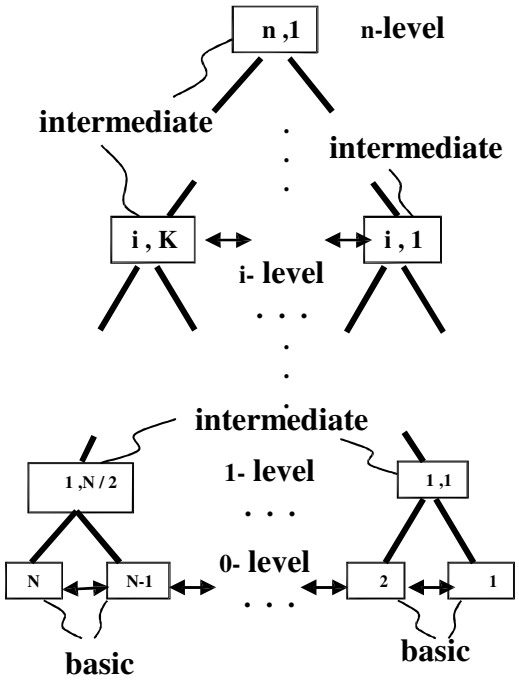

Fig. 1

At the base of our architecture of the cryptographic core is the principle of organizing simultaneous functioning of simple basic devices in a hierarchical (tree-like) structure. The advantages of this structure are evident. As a rule, many elements from which these schemes are constructed consist of only two main types (Fig.1). The first type is utilized in construction of the hierarchical structure of the base (basic element), and the second type is used to construct the intermediate levels (intermediate element). All links are local in their nature. The number of connections in a single element is always constant, i.e. does not depend on the actual location of the element in the structure of the scheme. Such schemes are not much more complicated in their complexity than the schemes with linear or two-dimensional structural links. For structures such as shown in Fig. 1, the total number of elements is only twice as many as in the linear structure that this structure is based upon (only the basic elements). The number of basic elements is equal to the number of intermediate elements plus one.

Generally, the complexity of the intermediate element is several times less than the complexity of the basic element, therefore the overall complexity of the hierarchical structure is close to that of the linear structure, which this structure is based upon.

The above described architecture allows representation of the linear structure, which lies at its base in the shape of a rectangular operational matrix (Fig. 2).

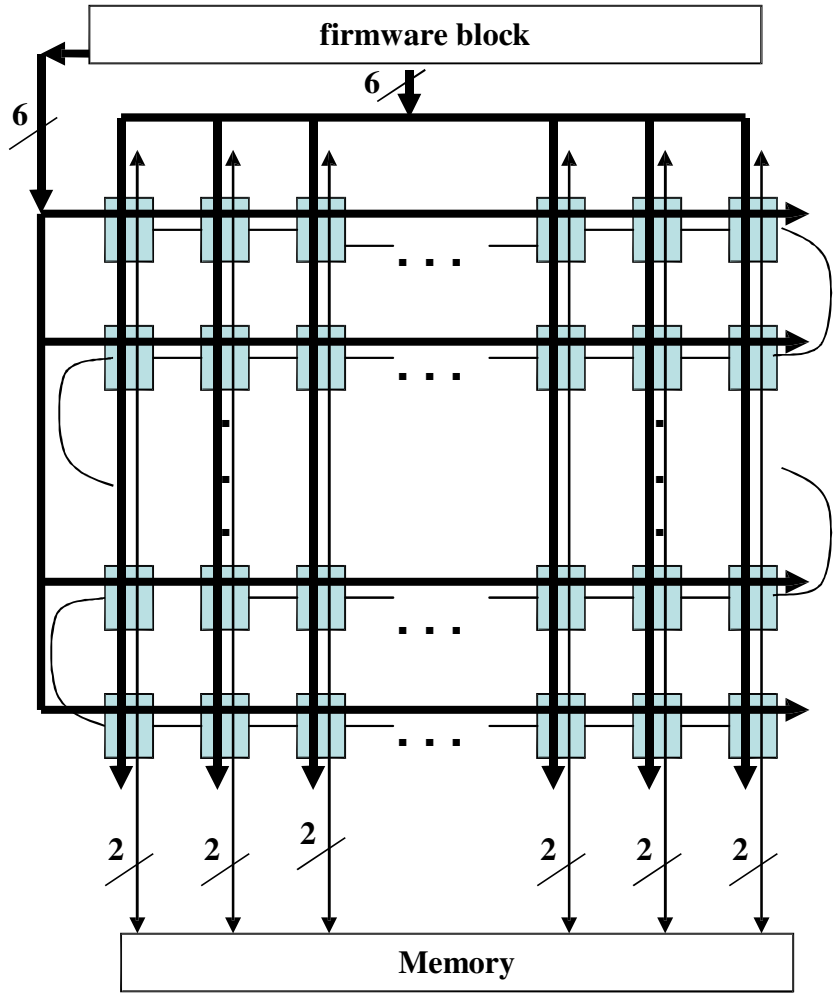

Fig.2

Our innovation is the development of a basic element of the operating matrix corresponding to the following properties:

1. Low complexity (when implemented in silicon, not more than 50 gates).
2. Functionality, supporting all the basic operations of cryptographic core within the matrix without writing/reading in/from memory.
3. Allowing the matrix to operate at very high frequency comparable to the number of matrix elements.

The first condition ensures that an electrical circuit implementing the basic element will contain only a few dozen transistors while occupying a tiny chip area, consuming minimum power and operating with minimal time delay. The basic elements are arranged on the surface of the crystal in a regular manner, in the form of a rectangular matrix, through which only a few controlled lines transfer data. All of the above simplifies the synchronizing of the design process by a hundredfold. An important advantage of this approach is its simplicity and speed of designing photo masks for the serial production of the final microchips. It would be enough to design a mask for the basic element. Even with the full physical simulation, this work can be done very quickly, in a matter of weeks. Then the resulting topology is simply multiplied to the number of basic elements utilized in the microchip. The bulk of the work was performed at the stage of determining the structure of the basic element.

In the selection process many basic functions that were used to calculate all the necessary operations were chosen first.

Next, the firmware was created for each function, which was then debugged at the appropriate emulator.

The functionality test of a cryptographic core was carried out on the prototyping of its FPGA.

Testing has shown its complete performance efficiency. Moreover, the cryptographic core of the FPGA was used to test the real possibility of its use for streaming encryption duplex telephone communication with a throughput of 128 Kb/sec. As a streaming encryption the scheme was used by BBS (Blum-Blum-Shub) module length 1K. The cryptographic durability of this scheme is equivalent to or better than the durability of RSA encryption with key lengths of 1K.

There has been prototyping and simulation of the topology of the cryptographic core on a library of standard gates to determine the basic characteristics (the maximum clock frequency, power and area). The results are shown in the Tab.1 below.

Technology	**Conditions**	**Process**	**Voltage**	**Temperature**	**Frequency**	**Power (@ Max Frequency)**	**Area**
130nm	BC-BC	Best	1.1v	0 Deg. C	2.85 Ghz	.2079 mW / Mhz	.182 mm2
130nm	WC-TYP	Typical	1.0v	120 Deg. C	2.00 Ghz	.1609 mW / Mhz	.182 mm2
130nm	WC- WC	Worst	0.9v	120 Deg. C	1.54 Ghz	.1079 mW / Mhz	.182 mm2
180nm	BC-BC	Best	2.0v	0 Deg. C	2.00 Ghz	1.270 mW / Mhz	.394 mm2
180nm	WC-TYP	Typical	1.6v	120 Deg. C	1.05 Ghz	.5299 mW / Mhz	.394 mm2
180nm	WC- WC	Worst	1.6v	120 Deg. C	.80 Ghz	.5460 mW / Mhz	.394 mm2

Tab.1

As was pointed out above, if you do the special design of the topology of the basic operating element of the matrix cryptographic core based on its links and loads, it will improve all the parameters: in frequency by at least 25%; in capacity by 100%; in size by 100%.

The development of this special topology would not take much time and does not take huge computing resources for physical simulation. This topology could be easily scaled to 90nm and 65nm technologies.

The sheer simplicity of the topological structure of operating matrixes provides a very high accuracy of the parameters of the scaled topology.