implemented in VHDL in 2012 by S. E. Soldatov, a student of the Information Security and Cryptography Department of Tomsk State University. For preliminary verification, all individual units in L_1-processor and its architecture on the whole were simulated by means of the program product ModelSim PE Student Edition 10.1d. Besides, the programmable logical integrated circuit of L_1-processor was synthesized with the help of the computer-aided design system ISE WebPACK 9.2i by Xilinx. The maximal operating frequency of the circuit equals 50 MHz which is equivalent to the circuit delay of 20 ns. The size of the circuit is the third of the size of Nexys2 FPGA debugging board by Digilent Inc.

This result shows that the implementation in hardware of the processor for LYaPAS-T is the quite real affair promising trustworthy means for effective performance of cryptographic and other combinatorial algorithms.

BIBLIOGRAPHY

1. *Agibalov G. P., Lipsky V. B., and Pankratova I. A.* Cryptographic extension of Russian programming language // Applied Discrete Mathematics. Application. 2013. No. 6. P. 93–98.

УДК 004.43, 004.056

AES IN LYAPAS

O. V. Broslavskiy

Programs in vLYaPAS representing the encryption and key expansion algorithms for symmetric block cipher AES are presented.
Keywords: *AES, LYaPAS.*

The objective of the paper is to present the description of the AES encryption and key expansion algorithms [1, 2] in the revised Russian programming language vLYaPAS [3]. The presented programs show the compactness, transparency and effectiveness of cryptographic algorithm representations in the language which was originally aimed at the representation of logical synthesis algorithms. It is assumed that the number of the cipher rounds is 10, and the lengths of the cipher block and key equal 128 bits. A ciphertext block is considered as a 2-measured array of 4×4 bytes. It is called a *state* and is represented by a logical complex of cardinality 4 whose elements are the rows of the state.

Further, the texts of the head programs and their subprograms are given. The external parameters in them are the following: L1 — the state (with the initial value equaled a plaintext block); L2 — the array of eleven 128-bit round keys (the complex of cardinality 44); L3 — ciphertext block; L4 — substitution table (S-box) for the operation of byte substitution; L5 — private key.

Encryption of a block

```
Encrypt(L1,L2,L4/L3)
   *AddRoundKey(L1,L2,0/L3) 0i
§1 Δi⊕10↪2
   *SubBytes(L3,L4/L3)
   *ShiftRows(L3/L3)
   *MixColumns(L3/L3)
   *AddRoundKey(L3,L2,i/L3) → 1
§2 *SubBytes(L3,L4/L3)
   *ShiftRows(L3/L3)
   *AddRoundKey(L3,L2,10/L3) **
```

Addition modulo 2 of a text block and a round key

```
AddRoundKey(L1,L2,n/L3)    *** n − the number of a round
   Q1 ⇒ Q3 n<2 ⇒ n
   L1.0 ⊕ L2n ⇒ L3.0
   Δn L1.1 ⊕ L2n ⇒ L3.1
   Δn L1.2 ⊕ L2n ⇒ L3.2
   Δn L1.3 ⊕ L2n ⇒ L3.3 **
```

Byte substitution with the help of S-box

```
SubBytes(L1,L4/L1)
*** every byte in L1 with the value i is substituted for the youngest byte
*** of ith element in L4
   ¯i FFh⇒m
§1 Δi ⊕ Q1↪2
   L1i&m⇒a L1i>8&m⇒b L1i>16&m⇒c L1i>24⇒d
   L4d<8∨L4c<8∨L4b<8∨L4a ⇒ L1i  →1
§2 **
```

Cyclic shift of state rows

```
ShiftRows(L1/L1)
   ¯i
§1 Δi ⊕ Q1↪2
   i&3<3⇒n 32-n⇒t L1i>t⇒q L1i<n∨q⇒L1i →1
§2 **
```

Mixing bytes in state columns

```
MixColumns(L1/L1)
   @+L2(4) 4⇒Q2 ¯j
§11 Δj⊕4↪2 j<3⇒q ¯k
§111 Δk⊕4↪112 L1k>q&FFh ⇒L2k →111
§112 *MixColumn(L2/L2) ¯k
§113 Δk⊕4↪11 FFh<q¬&L1k ⇒L1k L2k<q∨L1k ⇒L1k →113
§2 **
```

Product of a vector-column and a matrix over the field GF(2^8)

```
MixColumn(L1/L1)
   @+L3(4) @+L4(4) Q1⇒Q3⇒Q4 ¯i
§1 Δi⊕Q3↪2 *xtime(L1i/a) a⇒L3i →1
§2 L3.0 ⊕ L3.1 ⊕ L1.1 ⊕ L1.2 ⊕ L1.3 ⇒ L4.0
   L1.0 ⊕ L3.1 ⊕ L3.2 ⊕ L1.2 ⊕ L1.3 ⇒ L4.1
   L1.0 ⊕ L1.1 ⊕ L3.2 ⊕ L3.3 ⊕ L1.3 ⇒ L4.2
   L3.0 ⊕ L1.0 ⊕ L1.1 ⊕ L1.2 ⊕ L3.3 ⇒ L4.3 ¯i
§3 Δi⊕4↪4 L4i⇒L1i →3
§4 **
```

Multiplication of a field GF(2^8) element by x (mod $x^8 + x^4 + x^3 + x + 1$)

```
xtime(x/x)
   x<1⇒x&100h↪0 x⊕11Bh⇒x
§0 **
```

Key expansion

```
KeyExpansion(L5,L4/L2)
   @+L3(12) *DefineVi(L3/L3) *** L3 − constants v_i in the expansion procedure
   44⇒Q2 ¯i Or
§1 Δi⊕4↪2 L5i⇒L2i →1
§2 Δr⊕11↪3 r<2⇒j
§21 j-1⇒s-3⇒k j>2⇒m L2s>24⇒q L2s<8 ∨ q⇒q
   *SubWord(q,L4/q) *** byte substitution in q according to S-box
   L2k⊕q⊕L3m⇒L2j Δj ¯n
§22 Δn⊕3↪2 j-1⇒s-3⇒k L2k⊕L2s⇒L2j Δj →22
§3 **
```

Computer experiments show that the encryption speed for russian text (L. N. Tolstoy. War and Piece) on a computer with the processor i5-2540M, 250 GHz, 4 GB memory is near to 2.4 MB/c.

BIBLIOGRAPHY

1. *Mollin R. A.* An Introduction to Cryptography. Boca Raton, London, New York: Chapman & Hall/CRC, 2007.
2. *Tokareva N. N.* Symmetric Cryptography. Short Course: text-book. Novosibirsk: NSU, 2012. (in Russian).
3. *Agibalov G. P., Lipsky V. B., and Pankratova I. A.* Cryptographic extension of Russian programming language // Applied Discrete Mathematics. Application. 2013. No. 6. P. 93–98.