ISSN No:-2456-2165

Creation of Database of Irreducible Polynomial Over A Finite Field GF(2) Based on FPGA

Bekmuratova AB., Bakytzhan A.B.
Faculty of physics and technologies, Al-farabi named Kazakh National University
Almaty, Kazakhstan

Abstract:- Cryptographic systems based on non-positional polynomial systems make it possible to create an effective highly reliable cryptographic system that ensures confidentiality, authenticity and integrity of stored and transmitted information. The basis of non-positional polynomial number systems are irreducible polynomials over the field GF(2). The article discusses a method for creating a database of irreducible polynomials in a finite field GF(2) based on software logic integrated circuits. The main idea of the algorithm for creating a base of irreducible polynomials in a finite field GF(2) is to study the nonlinearity of all polynomials in a finite field GF(2) using the Ben-Or algorithm. The algorithm is implemented in the Verilog HDL language. However, multiplication on finite fields is often a time-consuming task requiring hardware and software. To solve the problem, an FPGA is used, which allows to implement parallel multipliers that perform a full multiplication operation in several cycles. Functional and temporal modeling of the behavioral model algorithm was performed using examples and the correctness of the algorithm was confirmed. The scheme of the device at the register transfer level (RTL) for FPGA is obtained.

Keywords:- *Irreducible Polynomials, Cryptography, Programmable Logic Integrated Circuits, Ben-or Algorithm.*

I. INTRODUCTION

Unverifiable polynomials have found their application in various fields of mathematics, information technology, as well as unverifiable polynomials are widely used in cryptography and are currently relevant. The properties of irreducible polynomials make it possible to maximize the efficiency of the computer implementation of arithmetic in the final fields[1].

Currently, fundamental and applied research is being carried out on the development and study of reliable and effective non-traditional cryptographic methods, algorithms and software tools for protecting information[3].

The use of non-positional polynomial systems in the construction of symmetric cryptosystems significantly increases the cryptographic security of the encryption algorithm[2].

Well-known algorithms and encryption methods, schemes for the formation of EDS and standards are built on positional computing systems. Computational and cryptography methods the developed algorithms of non-positional polynomial systems make it possible to significantly increase the cryptanalysis of encryption algorithms and digital signature schemes (formation and verification) [4], as well as reduce the length of hash values and electronic signature. The effectiveness of this approach is based on the possibilities of parallelization of computational procedures on each basis of non-positional polynomial systems of calculus[5]. The use of these computing systems makes it possible to combine the software and hardware implementation of encryption, the formation of an electronic digital signature and error detection/correction functions.

In a non-positional polynomial base of a computing system, the value of the encryption algorithm is as follows. The initial open message is represented as a sequence of blocks of a given length N (Bitta)[6]. Each block is interpolated as an order of residues $a_1(x), a_2(x), \dots, a_n(x)$. Some polynomials F(x) GF(2) over a field of degree N from the division into different non-quoted polynomials $p_1(x), p_2(x), \dots, p_n(x)$ over a field of GF(2) [2]:

$$F(x) = a_1(x), a_2(x), \dots, a_n(x))$$

In gloomy F(x) $\equiv a_i(x)\big(mod\ p_i(x)\big), i = \overline{1,n}$,, n-the number of selected working bases. Non-dispositive polynomials $p_1(x), p_2(x), \dots, p_n(x)$are called the working bases of non-dispositive polynomial computing systems. according to the Chinese theorem on residues, the view is the only one if the working bases of non-positional polynomial systems for calculating $p_i(x)$ are different[7].

Above the field GF(2) with the degree m_j in a row of all non-quotient polynomials, the working base is selected from the conditions for performing the following equation[8]:

$$k_1 m_1 + k_2 m_2 + \cdots + k_s m_s = N.$$

In sadness $\leq m_j \leq N, k_1 + k_2 + \cdots + k_s = n.$

A pseudo-random bit sequence of length n is used as a secret key. From dividing some other polynomial over the field of degree GF(2) N into the same working bases $p_1(x), p_2(x), \dots, p_n(x)$ it is also interpreted as a residual sequence $\beta_1(x), \beta_2(x), \dots, \beta_n(x)$:

$$G(x) = \big(\beta_1(x), \beta_2(x), \dots, \beta_n(x)\big), G(x) \equiv \beta_i(x)\left(mod_{pi}(x)\right), i = \overline{1,n.}$$

ISSN No:-2456-2165

Then the H (x) ciphertext is obtained from the polynomials F(x) and G(X) as a result of performing some function, which is also interpreted as the regularity of the residues $\gamma_1(x), \gamma_2(x), \dots, \gamma_n(x)$ after $p_1(x), p_2(x), \dots, p_n(x)$

From the work-based division of non-positional polynomial systems of computation H (x) :

$$H(x) = \big(\gamma_1(x), \gamma_2(x), \dots, \gamma_n(x)\big),$$

$$H(x) \equiv \gamma_i(x)\big(mod\ p_i(x)\big), i = \overline{1,n}.$$

In the developed cryptosystem, the operation of multiplying residual polynomials by a module on the basis of work is used as such a function:

$$\gamma_i(x) = \alpha_i(x)\beta_i(x) mod\ p_i(x), i = \overline{1,n}.$$

Cipher H(x) in free encryption, the inverse polynomial calculation $\beta_i^{-1}(x)$ is performed for each polynomial $\beta_i(x)$ from the following comparison execution conditions:

$$\beta_i(x)\beta_i^{-1}(x) \equiv 1\big(mod\ p_i(x)\big), i = \overline{1,n}.$$

As a result, a polynomial is obtained

$$G^{-1}(x) = \big(\beta_1^{-1}(x), \beta_2^{-1}(x), \dots, \beta_n^{-1}(x)\big).$$

G (x) is invertible to a polynomial. Then the elements of the corresponding sequence (2) and (3) are restored as a result of performing the following operation:

$$\alpha_i(x) = \beta_i^{-1}(x)\gamma_i(x) mod p_i(x). i = \overline{1,n}.$$

In the considered model of an encryption system based on non-positional polynomial systems,a given length of N bits is a system based on the polynomial operation $\rho_1(x), \rho_2(x), \dots, p_n(x)$ and the Secret Key $G(x) = \big(\beta_1(x), \beta_2(x), \dots, \beta_n(x)\big)$, chosen as the full key[9-10].

In this paper, the algorithm for sampling and constructing the base of irreducible polynomials from polynomials in the finite field GF(2) is implemented on the basis of PLIS[10-11]. the main idea of the algorithm for constructing a base of irreducible polynomials in the finite field GF(2) of N degrees is to study the irreducible property of all polynomials in the finite field Gf(2) using the Ben-or algorithm[9].

II. METHODOLOGY

➢ *The Ben-or Algorithm*

This Algorithm is Based on the Following Concept:

- for i ≥ 1, the polynomial $x^{q^i} - x \in F_q[x]$ is the product of all normalized non-quoted polynomials in the field $F_q[x]$ [3].
- Algorithm: the Ben-or algorithm for checking a polynomial for nonexistence.
- Input: f(x) ∈ $F_q[x]$ is a normalized polynomial of N degrees.
- Output: "True " is a polynomial whose polynomial f(x) cannot be quoted
- "False" is a polynomial in which the polynomial f(x) is given
- cycle: for the value i = 1 − ден n/2:

  $q = \gcd(f(x), (x^{q^i} - x) \mathrm{mod} f(x))$
  if q ≠ 1is "false"
  end of cycle

The Ben-or algorithm calculates the values $q = \gcd(f(x), (x^{q^i} - x) \mathrm{mod} f(x))$ for values from i=1 to n⁄2, and is considered to be a polynomial if the value q has a "false" value at least 1 time. In order for a polynomial to be irreducible, it is necessary that the output value is true in all values from i = 1 to n/2 [4].

Creation of Database of Irreducible Polynomial Over A Finite Field Gf(2) Based on FPGA.

Given that the number of polynomials of degree n in the field GF(2) is 2^n and that polynomials without a regular term are polynomials to be given since they are divided by x, it is determined that the total number of polynomials to be given is 2^{n-1}.

Algorithm: GF(2) Creating a base of irreducible polynomials in a finite field

Input: n-GF(2) polynomial degree in the finite field n ≥ 1.

a-is an algorithm of research on an irreducible property.
Output: base of irreducible polynomials

if n = 1
b=1; s=1;
if n > 1
b=2^n + 1; s=2;

end cycle: from j=b to 2^(n+1)-1 in steps s: if a(j)="True", write the polynomial j to the base end of cycle

Polynomials with a step s from b to $2^{n+1} - 1$ are compiled into the base of non-quoted polynomials if they are not checked by the Ben-or algorithm.

➢ *Figure 1 Shows the RTL Scheme of the Ben-or Algorithm.*

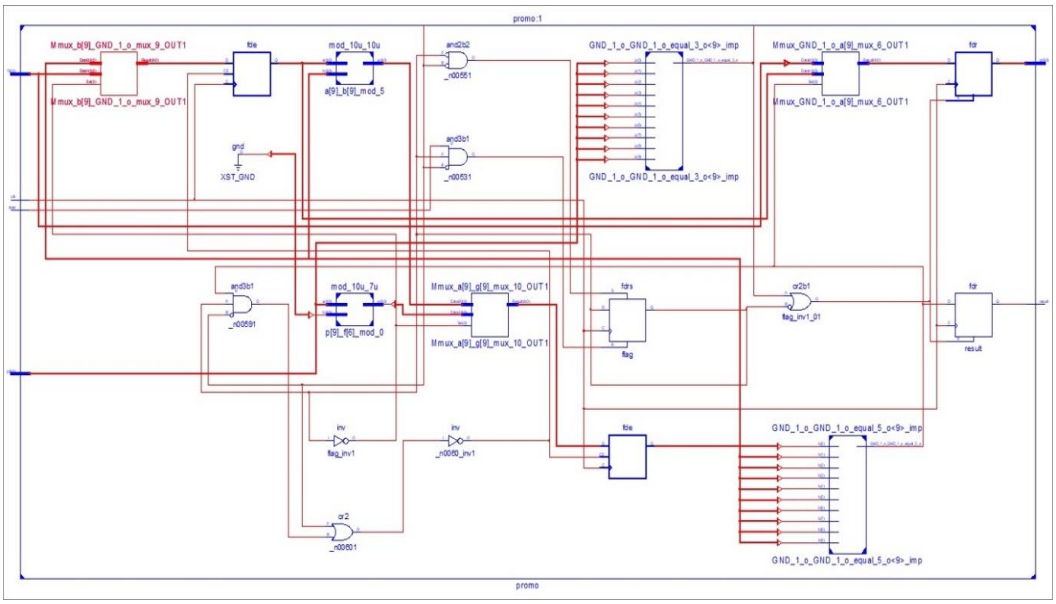

Fig 1 RTL Scheme of the Ben-or Algorithm Created in FPGA

III. RESULTS AND DISCUSSION

Polynomial f=10111 was received as input. Since the polynomial has 5 digits, *i*=1 to 3 according to the algorithm. The polynomial was tested by the Ben-Or algorithm and *q*=1 for all values from *i*=1 to 3, that is, the polynomial is an irreducible polynomial. Figure 2 shows the input and output values of the algorithm.

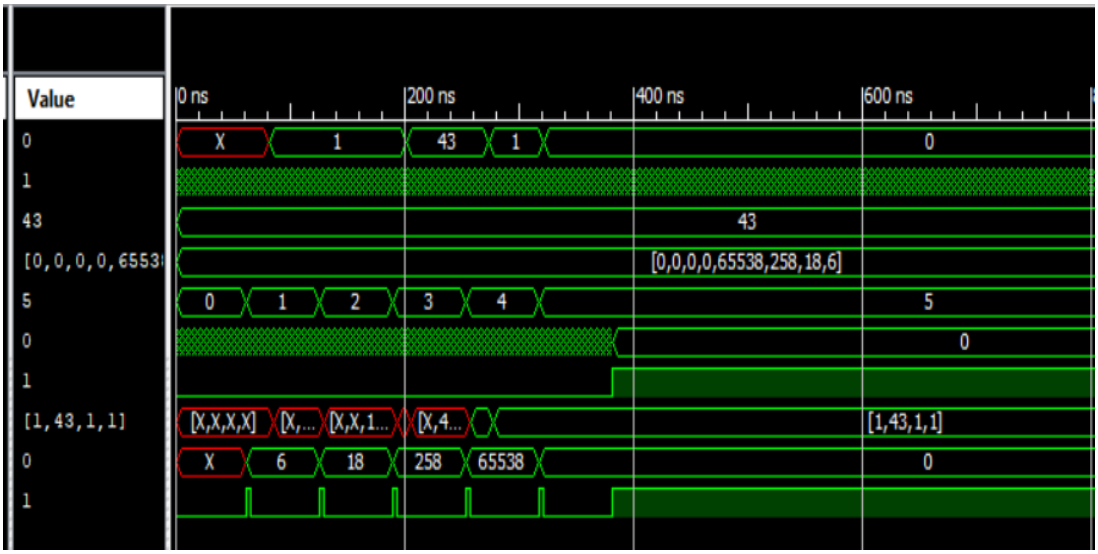

Fig 2 Input and Output Values of Ben-or Algorithm Created in FPGA

Table 1 Device Utilization Summary

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	26	126800	0%
Number of Slice LUTs	352	63400	0%
Number of fully used LUT-FF pairs	23	355	6%
Number of bonded IOBs	30	210	14%
Number of BUFG/BUFGCTRLs	1	32	3%

➢ *Timing Summary:*

- Speed Grade: -1
- Minimum period: 17.159ns (Maximum Frequency: 58.278MHz)

IV. CONCLUSION

Irreducible polynomials are important in cryptography based on non-positional polynomial systems. In the non-positional polynomial system (NPSS), irreducible polynomials in the finite field GF(2) are used as bases.

In this work, a database of non-quoted polynomials was developed, which are used as keys in symmetric cryptographic information security algorithms. to create a base of irreducible polynomials in the finite field GF(2) of N degrees, all polynomials in the finite field GF(2) were studied for the irreducible property using the Ben-or algorithm.

The Ben-or algorithm is a probabilistic algorithm for testing polynomials for an irreducible property over infinite fields. The Ben-or algorithm quickly detects irreducible factors of a smaller degree, thus performing much less calculations than other algorithms[5].

The given algorithm was implemented in Nexys 4 Artix-7 FPGA Board.

REFERENCES

[1] Amerbaev V. M., Biyashev R. G., Nysanbaeva S. E. Application of non-positional number systems in cryptographic protection//Izv. National acad. Sciences Rep. Kazakhstan. Ser. Phys.-Math. 2005. No. 3. S. 84-89.

[2] Nysanbaeva S. E., Varennikov A. V. Formation of a database of irreducible irreducible polynomials over a finite field GF(2) // Informatics and applied mathematics: Mat. IV Intl. scientific conf. (September 25-29, 2018). Part 2.–Almaty, 2019. – 647 p.

[3] Daniel Panario and Bruce Richmond. Analysis of ben-or's polynomial irreducibility test. In proceedings of the eighth international conference on Random structures and algorithms, pages 439–456, New York, NY, USA, 1998. John Wiley & Sons, Inc

[4] Daniel Panario, Boris Pittel, Bruce Richmond, and Alfredo Viola. Analysis of rabin's irreducibility test for polynomials over finite fields. Random Structures and Algorithms, 19:525–551, October 2001.

[5] Hayman, Steven, "Testing Irreducibility of Trinomials over GF(2)" (2012). Honors Projects. Paper 14.

[6] D.Schinianakis., T.Stouraitis, RNS-based RSA and ECC cryptography basic operations, algorithms, and hardware, Embedded Systems Design with Special Arithmetic and Number Systems, Springer(2017)

[7] N.Szabo, R.Tanaka, Residue arithmetic and its applications to computer technology. New-York (1967).

[8] M.A.Bayoumi, G.A.Jullien, W.C. Miller, AVLSI Implementation of RNS-Based Architectures, International Symposium on Circuits and Systems(1985)

[9] Voloshin D.N. Zinchenko Yu.E., Dyachenko O.N. Conveyor devices on FPGA. . [Electronic resource]. Access mode http://uran.donntu.org/~masters/2012/fknt/voloshin/diss/index.htm

[10] Kougi P.M. Architecture of conveyor computers. / Per. from English. M.: Radio and communication, 1985

[11] Ivanov M.A., Chugunkov I.V., Theory, application and quality assessment of generators of pseudo-random sequences. -M.: K-Obzor, 2003-136s.