Reconfigurable Multiplicator Over 2^{16}, 2^{15} and 2^{14} for DVB-S2X Standard

T. A. Zubov
Siberian Federal University
Krasnoyarsk, Russian Federation

V. V. Sukhotin
Siberian Federal University
Krasnoyarsk, Russian Federation
vsuhotin@sfu-kras.ru

A. V. Khnykin
Siberian Federal University
Krasnoyarsk, Russian Federation
akhnykin@sfu-kras.ru

A. N. Kamyshnikov
Siberian Federal University
Krasnoyarsk, Russian Federation

V. V. Evstratko
Siberian Federal University
Krasnoyarsk, Russian Federation

***Abstract*—This paper shows that massive streams of data and high data rates requires high-performance digital data-processing systems, development of data transmission optimization methods, optimization of digital filtering and coding/decoding processes. Also forming of reconfigurable parallel multiplicator over Galois field (GF(2^{16}), GF(2^{15}) and GF(2^{14})) for DVB-S2X standard is described, that allow to reduce number of gates for BCH decoding process. Optimization of formed reconfigurable multiplicator is provided. Corresponding outputs are given.**

Keywords—Galois field, Q-network, IP-network, multiplicator, multiplexer, gate, convolution.

I. INTRODUCTION

It's not a secret, that satellite technologies, like navigation and data transmission, are widely used in human's daily routine. Perspectives and priorities of satellite data systems progress [1] are based on transition to satellites, built on HTS technology (high-throughput satellite). This decision allow to use small-scale subscriber terminals, that enables data rates higher than 1 Gbit/s, and will allow to build ultrawideband communication systems with high level of anti-jam signal protection. Massive streams of data and high data rates will require high-performance digital data-processing systems, data transmission optimization [2], optimization of coding/decoding processes [3] and digital filtering [4]. Let's overlook optimization of video signal decoding process, which is used in DVB-S2X standard.

II. FORMING OF RECONFIGURABLE PARALLEL MULTIPLICATOR FOR DVB-S2X

As a matter of practice, multiplication over single Galois field is applied not in every instance, for example, when looking into BCH decoding [5; 6] described in DVB-S2X standard [7], it is seen, that this standard uses multiplication over three different Galois fields: GF(2^{16}) (normal FECFRAME, n=64800), GF(2^{15}) (average FECFRAME, n=32400) and GF(2^{14}) (short FECFRAME, n=16200), that operation requires three different multiplicators over three Galois fields. Realization of every multiplicator using low complexity bit parallel structure (LCBP) [8], shown on Fig. 1, is far resource-intensive challenge. Only for *IP*-network, that realize convolution [8] of two m-bit words A and B [8] and form $2m$-1 bit word on output, of GF(2^m) will require m^2 number of AND gates and $(m-1)^2$ number of XOR gates, and for Q-network, that realize reduction of $2m-1$ bit word to m-bit C [8] in GF(2^m), number of XOR gates is defined by number of ones in Q matrix. Number of gates for all three Galois fields is provided by Table 1.

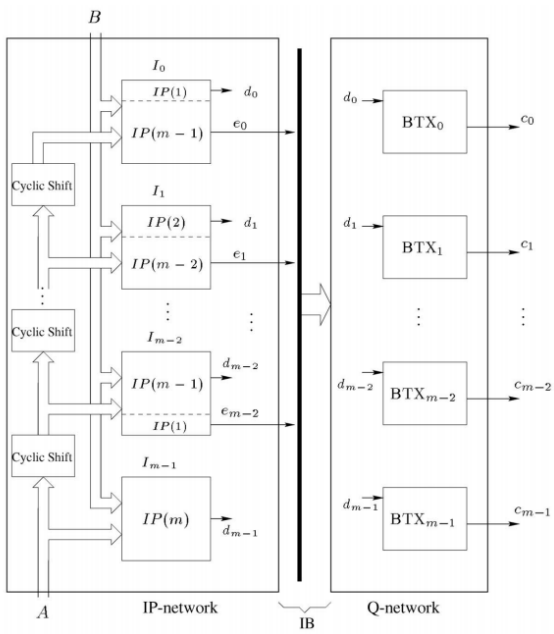

Fig. 1. LCBP multiplicator structure over GF(2^m) field

TABLE I. AMOUNT OF GATES IN MULTIPLICATORS OVER GALOIS FIELDS FOR DVB-S2, DVB-S2X STANDARDS

Field	Generating polynomial $P(x)$	*IP*-network		*Q*-network
		AND	XOR	XOR
GF(2^{16})	$1+x^2+x^3+x^5+x^{16}$	256	225	71
GF(2^{15})	$1+x^2+x^3+x^5+x^{15}$	225	196	67
GF(2^{14})	$1+x+x^3+x^5+x^{14}$	196	169	62

This work was supported by the Ministry of Education and Science of the Russian Federation in the framework of the Federal target program "Research and development on priority directions of development of the scientific-technological complex of Russia for 2014-2020" (agreement no. 05.605.21.0185, unique ID project RFMEFI60519X0185).

As seen in Table I, greater part of gates is concentrated in *IP*-network. To build reconfigurable multiplicator it is necessary to form common structure for all three fields.

In accordance to Table I, greater part of gates is concentrated in *IP*-network, where operation of vectors *A* and *B* convolution is performed. Knowing the fact that convolution is a linear operation, we can reduce amount of gates for convolution operation of three different fields (GF(2^{16}), GF(2^{15}) and GF(2^{14})) by using of common structure of *IP*-network for higher Galois field GF(2^{16}). For this task it is necessary to complement input words *A* and *B* by zero bits A_{15} and B_{15}, and for field GF(2^{15}) to complement A_{15}, A_{14}, B_{15} and B_{14} bits. Therefore, calculation of *S* vector, appearing to be convolution result, in common structure for fields GF(2^{16}), GF(2^{15}) and GF(2^{14}) will be the following:

$$\begin{aligned} s_{GF_{16}} &= \left[d_0,\ldots,d_{15},e_0,\ldots,e_{14}\right]^T, \\ s_{GF_{15}} &= \left[d_0,\ldots,d_{14},e_0,\ldots,e_{13},0,0\right]^T, \\ s_{GF_{14}} &= \left[d_0,\ldots,d_{13},e_0,\ldots,e_{12},0,0,0,0\right]^T. \end{aligned} \tag{1}$$

In (1) adaptation of S_{GF15} and S_{GF14} vectors to S_{GF16} length is based on example, given in [9].

Excess matrix for GF(2^{16}) will be represented in the following way:

$$Q_{GF(2^{16})} = \begin{array}{c} \begin{array}{cccccccccccccccc} d_0 & d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8 & d_9 & d_{10} & d_{11} & d_{12} & d_{13} & d_{14} & d_{15} \end{array} \\ \begin{bmatrix} 1 & & 1 & 1 & & 1 & & & & & & & & & & \\ & 1 & & 1 & 1 & & 1 & & & & & & & & & \\ & & 1 & & 1 & 1 & & 1 & & & & & & & & \\ & & & 1 & & 1 & 1 & & 1 & & & & & & & \\ & & & & 1 & & 1 & 1 & & 1 & & & & & & \\ & & & & & 1 & & 1 & 1 & & 1 & & & & & \\ & & & & & & 1 & & 1 & 1 & & 1 & & & & \\ & & & & & & & 1 & & 1 & 1 & & 1 & & & \\ & & & & & & & & 1 & & 1 & 1 & & 1 & & \\ & & & & & & & & & 1 & & 1 & 1 & & 1 & \\ & & & & & & & & & & 1 & & 1 & 1 & & 1 \\ 1 & & 1 & 1 & & 1 & & & & & & 1 & & 1 & 1 & \\ & 1 & & 1 & 1 & & 1 & & & & & & 1 & & 1 & 1 \\ 1 & & & 1 & 1 & & & 1 & & & & & & 1 & & 1 \\ 1 & 1 & 1 & 1 & 1 & & & & 1 & & & & & & 1 & \end{bmatrix} \end{array} \begin{array}{c} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \\ e_9 \\ e_{10} \\ e_{11} \\ e_{12} \\ e_{13} \\ e_{14} \end{array} \tag{2}$$

Ones in $Q_{GF(2m)}$ represent XOR operations for vertical elements *e* and horizontal elements *d* of vectors, that allows to proceed from augmented vector to *m*-digit vector and perform multiplication over GF(2^m) field. For illustrative purposes zeroes are omitted.

Excess matrix for GF(2^{15}) will be represented in the following way:

$$Q_{GF(2^{15})} = \begin{array}{c} \begin{array}{ccccccccccccccc} d_0 & d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8 & d_9 & d_{10} & d_{11} & d_{12} & d_{13} & d_{14} \end{array} \\ \begin{bmatrix} 1 & & 1 & 1 & & 1 & & & & & & & & & \\ & 1 & & 1 & 1 & & 1 & & & & & & & & \\ & & 1 & & 1 & 1 & & 1 & & & & & & & \\ & & & 1 & & 1 & 1 & & 1 & & & & & & \\ & & & & 1 & & 1 & 1 & & 1 & & & & & \\ & & & & & 1 & & 1 & 1 & & 1 & & & & \\ & & & & & & 1 & & 1 & 1 & & 1 & & & \\ & & & & & & & 1 & & 1 & 1 & & 1 & & \\ & & & & & & & & 1 & & 1 & 1 & & 1 & \\ & & & & & & & & & 1 & & 1 & 1 & & 1 \\ 1 & & 1 & 1 & & 1 & & & & & & 1 & & 1 & 1 \\ & 1 & & 1 & 1 & & 1 & & & & & & 1 & & 1 & 1 \\ 1 & & & 1 & 1 & & & 1 & & & & & & 1 & & 1 \\ 1 & 1 & 1 & 1 & 1 & & & & 1 & & & & & & 1 & \end{bmatrix} \end{array} \begin{array}{c} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \\ e_9 \\ e_{10} \\ e_{11} \\ e_{12} \\ e_{13} \end{array} \tag{3}$$

Excess matrix for GF(2^{14}) will be represented in the following way:

$$Q_{GF(2^{14})} = \begin{array}{c} \begin{array}{ccccccccccccccc} d_0 & d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8 & d_9 & d_{10} & d_{11} & d_{12} & d_{13} \end{array} \\ \begin{bmatrix} 1 & 1 & & 1 & & 1 & & & & & & & & & \\ & 1 & 1 & & 1 & & 1 & & & & & & & & \\ & & 1 & 1 & & 1 & & 1 & & & & & & & \\ & & & 1 & 1 & & 1 & & 1 & & & & & & \\ & & & & 1 & 1 & & 1 & & 1 & & & & & \\ & & & & & 1 & 1 & & 1 & & 1 & & & & \\ & & & & & & 1 & 1 & & 1 & & 1 & & & \\ & & & & & & & 1 & 1 & & 1 & & 1 & & \\ & & & & & & & & 1 & 1 & & 1 & & 1 & \\ 1 & 1 & & 1 & & 1 & & & & & 1 & 1 & & 1 & \\ & 1 & 1 & & 1 & & 1 & & & & & & 1 & 1 & \\ 1 & 1 & 1 & & & & & 1 & & & & & 1 & 1 & \\ & 1 & 1 & 1 & & & & & 1 & & & & & 1 & 1 \end{bmatrix} \end{array} \begin{array}{c} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \\ e_9 \\ e_{10} \\ e_{11} \\ e_{12} \end{array} \tag{4}$$

Diagram of reconfigurable multiplicator, which minimizes the number of gates in *IP*-network, is shown in Fig. 2.

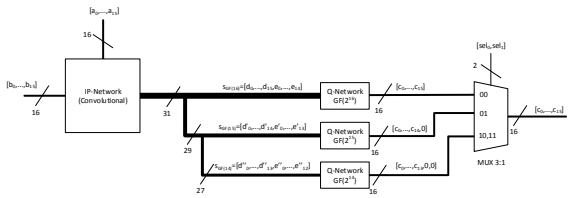

Fig. 2. Reconfigurable multiplicator over Galois fields GF(2^{16}), GF(2^{15}) and GF(2^{14})

Given diagram consists of one convolution block for two 16-bit *A* and *B* vectors, 3 blocks of *Q*-network for Galois fields GF(2^{16}), GF(2^{15}) and GF(2^{14}) excesses calculation, and 16 3-input multiplexers, controlled by SEL signal. As it shown on Fig. 3, each multiplexer consists of 4 AND gates, 2 OR gates and 2 NOT gates.

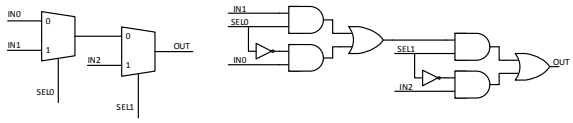

Fig. 3. 3-input multiplexer MUX 3:1

Table II provides number of gates for optimized reconfigurable multiplicator.

TABLE II. AMOUNT OF GATES IN RECONFIGURABLE MULTIPLICATORS OVER GALOIS FIELDS FOR DVB-S2, DVB-S2X STANDARDS

Field	**Generating polynomial *P*(*x*)**	***IP*-network**		***Q*-network**	**MUX 3:1, 16 pcs**		
		AND	**XOR**	**XOR**	**AND**	**OR**	**NOT**
GF (2^{16})	$1+x^2+x^3+x^5+x^{16}$	256	225	71	64	32	32
GF (2^{15})	$1+x^2+x^3+x^5+x^{15}$			67			
GF (2^{14})	$1+x+x^3+x^5+x^{14}$			62			

Total	**AND**	**XOR**	**OR**	**NOT**
	320	425	32	32
Number of CMOS transistors	2112	2864	288	96
Total	5576 transistors			

Comparing results of Tables I and II minimization of number of used gates is becoming obvious (from 1467 to 809), thus Galois multiplicator of reconfigurable design utilizes 658 gates or 4806 transistors less than standalone Galois multiplicators.

III. FURTHER OPTIMIZATION OF RECONFIGURABLE MULTIPLICATOR FOR DVB-S2X STANDARD

Matrices (2) and (3) are similar, it is linked with the fact their generator polynomial differs only in high-order terms (x^{16} and x^{15}). It is possible to evaluate from (2) and (3) the following:

$$Q_{GF(2^{16})_{i,j}} = \begin{cases} Q_{GF(2^{15})_{i,j}}, 0 \le i \le 8, 0 \le j \le 8 \\ 0, i = 9, 0 \le j \le 8 \\ Q_{GF(2^{15})_{i-1,j}}, 10 \le i \le 14, 0 \le j \le 8 \\ Q_{GF(2^{15})_{ij}}, 0 \le i \le 13, 9 \le j \le 14 \end{cases} \quad (5)$$

The exception is the last column of matrix (2) $Q_{GF(2^{15})_{i,15}}, 0 \le i \le 14$, where higher term c_{15} over GF(2^{16}) field is being evaluated, which is can be zeroed or ignored for GF(2^{15}) field, and also the row $Q_{GF(2^{16})_{14,j}}$, $9 \le j \le 14$, where the non-zero element is the $Q_{GF(2^{16})_{14,14}}$, which can be zeroed by zero-value e_{14}.

Full matrix (2), evaluated from (3), will look the following way:

$$Q_{GF(2^{16})} = \begin{bmatrix} \begin{bmatrix} Q_{GF(2^{15})_{0...8,0...8}} \\ 0 \\ Q_{GF(2^{15})_{9...13,0...8}} \end{bmatrix} & \begin{bmatrix} Q_{GF(2^{15})_{0...13,9...14}} \\ Q_{GF(2^{16})_{14,9...14}} \end{bmatrix} & Q_{GF(2^{16})_{0...14,15}} \end{bmatrix} \quad (6)$$

The last column can be zeroed or ignored, same is true for $Q_{GF(2^{16})_{14,14}}$ provided by the fact e_{14} row is zeroes, knowing that the matrix (6) will be represented in the following way:

$$Q'_{GF(2^{16})} = \begin{bmatrix} \begin{bmatrix} Q_{GF(2^{15})_{0...8,0...8}} \\ 0 \\ Q_{GF(2^{15})_{9...13,0...8}} \end{bmatrix} & \begin{bmatrix} Q_{GF(2^{15})_{0...13,9...14}} \\ 0 \end{bmatrix} \end{bmatrix} \quad (7)$$

Thus, for these two submatrices it is necessary to figure out two vectors s' and s'' taking into consideration that e_0 for GF(2^{15}) is d_{15}.

$$\begin{aligned} s_{GF_{16}} &= [d_0, ..., d_{15}, e_0, ..., e_{14}]^T, \\ s'_{GF_{15}} &= [d_0, ..., d_{14}, 0, d_{15}, e_0, ..., e_7, 0, e_8, ..., e_{12}]^T, \\ s''_{GF_{15}} &= [d_0, ..., d_{14}, 0, d_{15}, e_0, ..., e_{12}, 0]^T. \end{aligned} \quad (8)$$

For these two vectors d_{15} of 29 or 30 terms of $s_{GF(2^{16})}$ vector will be zeroed, also 25 and 30 terms for s′ and s″ accordingly:

$$s'_{GF(2^{15})_i} = \begin{cases} s_{GF(2^{16})_i}, 0 \le i \le 14 \\ s_{GF(2^{16})_{29}} = 0, i = 15 \\ s_{GF(2^{16})_{i-1}}, 16 \le i \le 24 \\ s_{GF(2^{16})_{30}}, i = 25 \\ s_{GF(2^{16})_{i-2}} = 0, 26 \le i \le 30 \end{cases} \quad s''_{GF(2^{15})_i} = \begin{cases} s_{GF(2^{16})_i}, 0 \le i \le 14 \\ s_{GF(2^{16})_{30}} = 0, i = 15 \\ s_{GF(2^{16})_{i-1}}, 16 \le i \le 29 \\ s_{GF(2^{16})_{i-1}} = 0, i = 30 \end{cases} \quad (9)$$

In view of the fact that vectors starting to shift by one term starting from d_{15} for GF(2^{15}) field, 3 *S* vectors will differ starting from 15 term. Adjusting $Q_{GF(2^{16})}$ for $Q_{GF(2^{15})}$ will require two 16-bit 2-input multiplexers, consisting of 62, 32 and 32 AND, OR and NOT gates each. However output multiplexor will change from 3-input to 2-input, as it shown on Fig. 4.

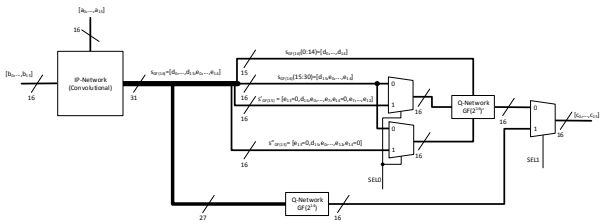

Fig. 4. Optimized reconfigurable structure

Table III provides number of gates in transformed reconfigurable multiplicator over Galois fields. As it seen in Table III total amount of gates is 806, which is 3 gates or 216 transistors less, then in diagram, shown on Fig. 2.

Correlation between (2) and (4) expressions is not very obvious as it was between (2) and (3) expressions, therefore diagram can be complicated after derivation of one *Q*-matrix from another. Such approach gives insignificant profit even for similar (2) and (4) matrices, and for derivation (2) and (4) amount of gates can increase compared in relation to diagrams on Fig.4 and Fig.2, making the further optimization pointless.

TABLE III. AMOUNT OF GATES IN OPTIMIZED RECONFIGURABLE MULTIPLICATORS OVER GALOIS FIELDS FOR DVB-S2, DVB-S2X STANDARDS

Field	**Generating polynomial *P*(*x*)**	***IP*-network**		***Q*-network**	**MUX 3:1, 16 pcs**		
		AND	***XOR***	***XOR***	***AND***	***OR***	***NOT***
GF (2^{16})	$1+x^2+x^3+x^5+x^{16}$	256	225	71	96	48	48
GF (2^{15})	$1+x^2+x^3+x^5+x^{15}$						
GF (2^{14})	$1+x+x^3+x^5+x^{14}$			62			
Total	**AND**	**XOR**		**OR**	**NOT**		
	352	358		48	48		
Number of CMOS transistors	2112	2864		288	96		
Total	5360 transistors						

IV. CONCLUSION

This work described forming the reconfigurable structure of multiplicator over Galois field (GF(2^{16}), GF(2^{15}) and GF(2^{14})), which is apllied in DVB-S2X standard. Such structure allow to reduce number of gates in *IP*-network by limiting by higher field and by exploiting of convolution operation linearity for values (m^2) AND and $(m-1)^2$ XOR gates instead of $(m)^2+(m-1)^2+(m-2)^2$ AND and $(m-1)^2+(m-2)^2+(m-3)^2$ XOR gates. Also by means of permutations of *d* and *e* vectors elements and of allocation comparison for non-zero elements of *Q* excess matrix it is becoming possible to reduce the amount of XOR gates in *Q*-network. However reconfigurable structure requires multiplexers able to modify multiplicator field by several existing fields. Regardless introducing multiplexers reconfigurable structure benefits in reducing the amount gates by 658 gates (4806 transistors), and optimized reconfigurable structure provides further benefit in reducing the amount by 3 gates (216 transistors).

REFERENCES

[1] Testoyedov N.A., Kuzovnikov A.V. Perspectives and development priorities of the information satellite systems // The Research of the Science City, 2017, vol. 1, no. 1, pp. 7-10.

[2] Polyak M.G., Mishurov A.V. Methods of optimization of information transmission in satellite communication systems // The Research of the Science City, 2016, no. 3-4, pp. 50-52.

[3] Poperechnyj P. S. Rekonfiguriruemyj blok pomehoustojchivogo kodirovanija dlja sistem na kristalle // Problemy razrabotki perspektivnyh mikro- i nanojelektronnyh sistem (MES), 2016, no. 1, pp. 266-273.

[4] Kaplun D., Gulenko M. Cifrovye fil'try v poljah Galua // Komponenty i tehnologii, 2008, no. 3, pp. 168-172.

[5] Sagalovich Ju. L.Vvedenie v algebraicheskie kody. Moscow, MFTI, 2007, 262 p.

[6] Morelos-Saragosa R. Iskusstvo pomehoustojchivogo kodirovanija. Metody, algoritmy, primenenie. Moscow, Tehnosfera, 2005, 320 p.

[7] ETSI. Digital video broadcasting (DVB). Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broad-band satellite applications; Part 2: DVB-S2 Extensions (DVB-S2X): EN 302 307 V1. 3.1, 2014.

[8] Reyhani-Masoleh A., Anwar Hasan M. Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over GF(2m) // IEEE Transactions on Computers, 2004, vol. 53, no. 8, pp. 945–959.

[9] Zubov T.A., Sukhotin V.V., Khnykin A.V., Mishurov A.V., Gorchakovsky A.A. Reconfigurable parralel multiple in the Galois fields in combination logic, J. Sib. Fed. Univ. Eng. technol., 2019, 12(7), 802-809. DOI: 10.17516/1999-494X-0180