

ИНФОРМАТИКА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 681.32

Разработка элементов криптопроцессора с использованием отечественной САПР "Ковчег"

О. А. Зобнина

Пермский национальный исследовательский политехнический университет
Россия, 614990, г. Пермь, ул. Комсомольский пр., 29
zobnina.olka@gmail.com; +7-922-37-78-699

А. Н. Каменских

Пермский национальный исследовательский политехнический университет
Россия, 614990, г. Пермь, ул. Комсомольский пр., 29
antoshkinoinfo@yandex.ru; +7-902-64-12-545

Г. К. Королёв

Пермский государственный национальный исследовательский университет
Россия, 614990, г. Пермь, ул. Букирева, 15
ЗАО "ИВС-СЕТИ", Россия, 614015, Пермь, ул. Н. Островского, 65
korolevgk@mail.ru; +7-950-44-31-343

С. Ф. Тюрин

Пермский национальный исследовательский политехнический университет
Россия, 614990, г. Пермь, ул. Комсомольский пр., 29
tyurinsergfe@yandex.ru; +7-952-32-02-510
Пермский государственный национальный исследовательский университет
Россия, 614990, г. Пермь, ул. Букирева, 15

Исследуется криптопроцессор – абонентский шифратор "КРИПТОН" с целью оценки возможности реализации на отечественной элементной базе в рамках задач импортозамещения. Анализируется ГОСТ 28147-89, описывающий используемые в "КРИПТОНЕ" алгоритмы зашифрования и расшифрования. Выясняется, что одними из основных операций над двумя 32-битными операндами являются поразрядное сложение по модулю 2, сложение по модулю 2 в степени 32, сдвиг, в том числе циклический, подстановка. Для реализации алгоритма необходимы 11 32-разрядных регистров, сумматоры, кодопреобразователь подстановки и управляющий автомат. Показывается, что используемые элементы, в том числе программируемые логические интегральные схемы (ПЛИС) иностранных производителей, могут быть заменены отечественными аналогами. Предлагается вместо ПЛИС использовать базовые матричные кристаллы (БМК). Разрабатываются некоторые устройства криптопроцессора с использованием отечественной САПР "Ковчег". Моделирование подтверждает работоспособность предложенных устройств.

Ключевые слова: *криптопроцессор; базовый матричный кристалл; САПР.*

DOI: 10.17072/1993-0550-2019-2-60-66

Введение

Обеспечение информационной безопасности в нашей стране в последние годы стало одной из самых важных государственных за-

дач. Устройство криптографической защиты данных (УКЗД) серии "КРИПТОН" предназначено для криптографической защиты данных в компьютерах типа IBM-PC [1].

Общий вид платы криптопроцессора, подключаемого к РС, показан на рис. 1.

© Зобнина О. А., Каменских А. Н., Королёв Г. А., Тюрин С. Ф., 2019

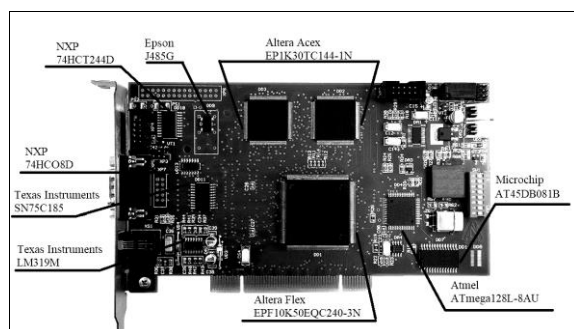


Рис. 1. Общий вид платы криптопроцессора

В качестве основных элементов плата содержит так называемые программируемые логические интегральные схемы (ПЛИС, FPGA – Field-Programmable Gate Array) и флэш-память для хранения конфигурации, загружаемой при включении питания (рис. 2).

Фирма	Название	Тип	№ производителя	Количество логических элементов	Количество входов/выходов I/O	Рабочее напряжение питания	Рабочий ток источника питания	Общий объем памяти
Intel	FPGA	FLEX 10K	EPF10K50EQC2-40-3N	2880	189	2.5 V	10 mA	20480 bit
Intel	FPGA	ACEX 1K	EP1K30TC144-1N	1728	102	2.5 V	5 mA	24876 bit
Atmel	Flash	Память	AT45DB081B	-	28	2.5 V	4 mA	8 Mбит

Рис. 2. Основные элементы криптопроцессора

В качестве вспомогательных элементов используется, например, микроконтроллер, обеспечивающий загрузку конфигурации и обмен данными с компьютером (рис. 3).

Фирма	Название	№ производителя	Количество входов/выходов	Рабочее напряжение питания	Рабочий ток источника питания
Microchip Technology	MCU: 8-разрядный микроконтроллер	ATMEGA128L-AU	53 I/O	2.7 V	3 mA
NXP Semiconductors	Линейные драйверы буфера	74HCT244D	20 I/O	4.5 V	6 mA
NXP Semiconductors	Quad 2-input AND gate	74HC08D	14 I/O	2 V	20 mA
Texas Instruments	Драйвер в приемник	SN75C185N	20 I/O	4.5 V	3,2 mA
Texas Instruments	Аналоговые компараторы	LM319M	14 I/O	5 V	4,3 mA

Рис. 3. Вспомогательные элементы криптопроцессора

В связи с требованиями импортозамещения электронной компонентной базы возникает необходимость анализа возможности реализации функций криптопроцессора (УКЗД серии "КРИПТОН") на отечественной элементной базе. Анализ возможностей базовых матричных кристаллов отечественного производителя показывает, что ПЛИС могут быть заменены базовыми матричными кристаллами (БМК) серии 5503 [2, 3].

Состав серии БМК 5503 представлен на рис. 4.

Тип БМК	Количество логических элементов	Количество внешних контактов	Напряжение питания, В	Рабочая частота, МГц
H5503XM1	576	28	5	30
H5503XM1Y	576	28	5	30
H5503XM2	1296	42	5	30
H5503XM5	3072	64	5	30
5503БЦ7У	5478	64	5	25

Рис. 4. Состав серии БМК 5503

В этом случае память конфигураций не потребуется. В качестве микроконтроллера для обмена информацией с РС выберем отечественный микроконтроллер 1986BE9х на ядре Cortex-M3 производства ЗАО "ПКК Миландр" [4].

1. Анализ алгоритмов зашифрования и расшифрования

Рассмотрим алгоритмы зашифрования и расшифрования информации, установленные ГОСТ 28147-89 [5]. Так, например, исследуем криптосхему зашифрования в режиме простой замены, которая изображена на рис. 5.

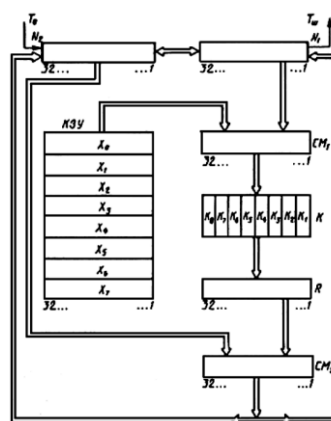


Рис. 5. Криптосхема зашифрования в режиме простой замены

Процедура предполагает ввод 64-разрядных исходных данных двумя словами N1, N2 по 32 бита каждый. В кодирующее запоминающее устройство (КЗУ) вводятся восемь 32-разрядных слов – это ключ. Алгоритм состоит из 32 циклов. В первом цикле N1 суммируется по модулю 2 в степени 32 со словом ключа X0 в сумматоре CM1 (N1 сохраняет исходное значение). Результат поступает в блок подстановки K, где преобразуется, а затем в регистре R сдвигается циклически на 11 разрядов вправо (в сторону старших разрядов). Полученный результат суммируется по модулю 2 поразрядно с N2 в сумматоре CM2.

Результат записывается в N1, при этом предварительно слово N1 переписывается в N2. Это конец первого цикла.

Далее работа осуществляется аналогично с другими словами ключа. В некоторых последующих циклах порядок считывания ключей меняется. По окончании 32-го цикла слово из сумматора CM2 переписывается в N2, а значение N1 сохраняется. Информация N1 и N2 представляет собой зашифрованные данные. Расшифрование информации выполняется по тому же алгоритму с изменениями порядка считывания ключей.

2. Реализация основных блоков криптопроцессора в САПР "Ковчег"

Для получения блоков суммирования по модулю используем имеющиеся в библиотеке элементов элементы сложения по модулю два (XOR). Построим схему XOR на три входа в системе САПР БИС "Ковчег" (рис. 10).

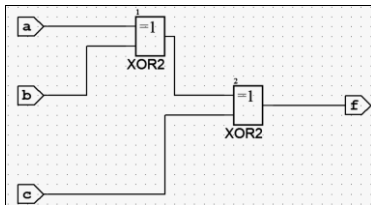


Рис. 10. Схема для функции $a \oplus b \oplus c$

Далее находим в панели управления команду "Тесты", это необходимо для того, чтобы в дальнейшем получить временную диаграмму (рис. 11).

```
1  DEFAULT_TEST;
2
3  DEFAULT_TEST:
4  a = 0,0,0,0,1,1,1,1;
5  b = 0,0,1,1,0,0,1,1;
6  c = 0,1,0,1,0,1,0,1;
7  f = h;
```

Рис. 11. Тест для функции $a \oplus b \oplus c$

Следующим шагом являются "Контрольные точки". Эти "точки" программа формирует сама. Контрольные точки захватывают входы и выходы. Они формируют то, что будет отображаться на временной диаграмме (рис. 12).

```
1  пример описания:
2
3  "Группа1, Группа2, Группа3, Группа4:"
4  "Группа1 : A, BUS[5:4], BUS[*]Q, BUS[3]D;"
5  "Группа2 : D1.D1(I0, *), D2<1:3>(I[1:0]H, 0, I[*], I[1]);"
6  "Группа3 : Метка1 [OUT1, OUT2, *, BUS[*], BUS3, BUS[4], D1.D1<*>(I[0:1], I[1], I[*])]"
7  "Группа4 : Метка2 [D2(*)]B, Метка3 [D2(1)]B;"
8
9  ALL;
10 ALL: *;
```

Рис. 12. Контрольные точки схемы $a \oplus b \oplus c$

Временная диаграмма формируется сама (рис. 13).

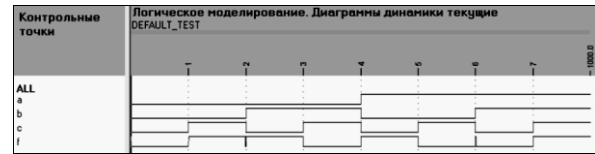
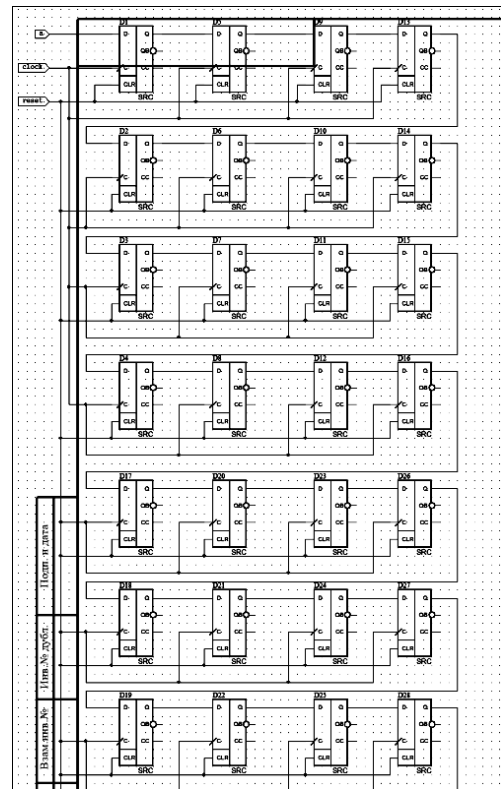


Рис. 13. Временная диаграмма работы схемы $a \oplus b \oplus c$

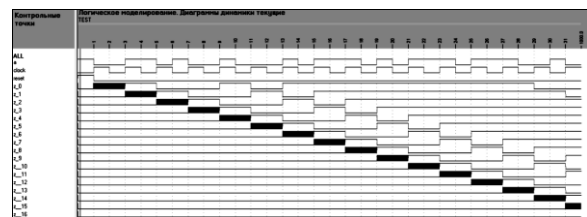
Таким образом, функция $a \oplus b \oplus c$ реализуется правильно.

Аналогично реализуются схемы сумматоров по модулю 2 в степени 32, сдвигающие регистры и др.

Так, схема 32-разрядного сдвигающего регистра и ее тестирование представлены на рис. 14.



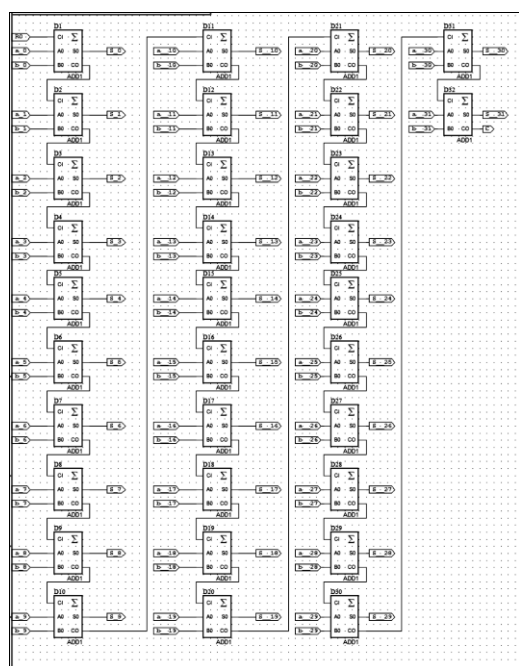
а)



б)

Рис. 14. Проверка работы сдвигающего регистра: а) фрагмент схемы; б) тест регистра на некоторой последовательности

Схема сумматора по модулю 2 в степени 32 изображена на рис. 15.



а)

Контрольные точки	Логическое моделирование. Диаграммы динамики функции
ALL	
PS	
S_0	
S_1	
S_2	
S_3	
S_4	
S_5	
S_6	
S_7	
S_8	
S_9	
S_10	
S_11	
S_12	
S_13	
S_14	
S_15	
S_16	
S_17	
S_18	
S_19	
S_20	
S_21	

б)

Рис. 15. Сумматор по модулю 2 в степени 32:
а) схема; б) тест схемы на единичных операндах

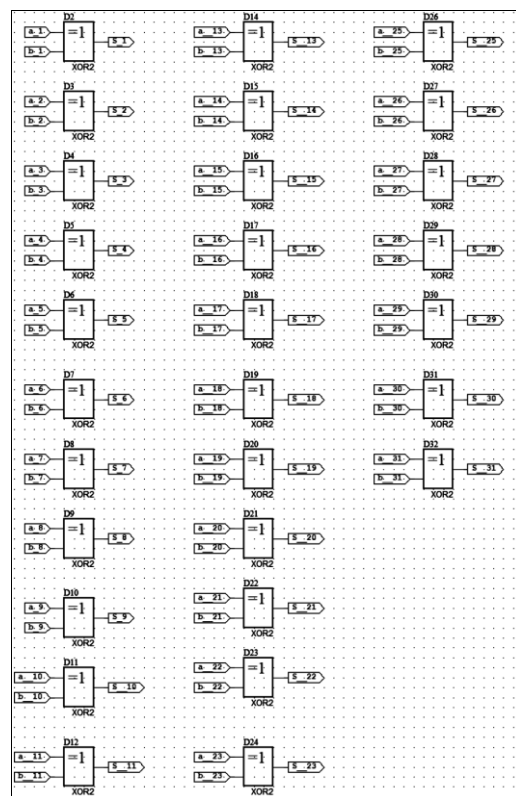
Таким образом, можно убедиться и на других тестах, что схема работает правильно. Сумматор по модулю 2 на 32 разряда представлен на рис. 16.

3. Реализация операций с полиномами

Для дополнительного получения сигнатур информационных посылок в криптопроцессоре целесообразно использовать операции с двоичными полиномами. Реализация операций с полиномами базируется на автоматах умножения и деления полиномов на основе D-триггеров с обратными связями, использующими элементы сложения по модулю 2 (XOR). Образующий полином (неприводи-

мый многочлен) определяет точки подключения элементов сложения по модулю 2.

Пример схемы умножения на полином $G = x^3 + x + 1$ в САПР "Ковчег" изображен на рис. 17.



а)

Контрольные точки	Логическое моделирование. Диаграммы динамики функции
ALL	
PS	
S_0	
S_1	
S_2	
S_3	
S_4	
S_5	
S_6	
S_7	
S_8	
S_9	
S_10	
S_11	
S_12	
S_13	
S_14	
S_15	
S_16	
S_17	
S_18	
S_19	
S_20	
S_21	

б)

Рис. 16. Сумматор по модулю 2
а) схема; б) тест схемы на случайно заданных операндах

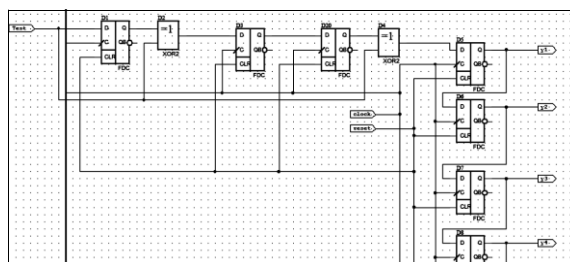


Рис. 17. Схема умножения на образующий полином $G = x^3 + x + 1$

Подготовим для полинома тест для собранной нами схемы. Правильность работы схемы подтверждается временной диаграммой, изображенной на рис. 18.



Рис. 18. Тест для схемы умножения на полином $G = x^3 + x + 1$

Аналогично строится схема деления на образующий полином.

Правильность работы схемы деления подтверждается временной диаграммой, изображенной на рис. 19.

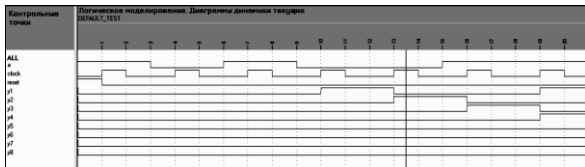
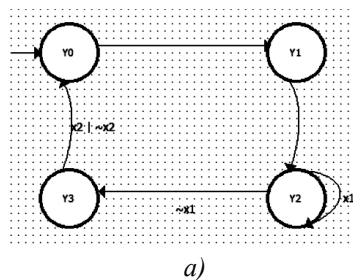


Рис. 19. Тесты для делителя на $G = x^3 + x + 1$

4. Реализация управляющего автомата

Для алгоритма зашифрования и расшифрования необходим управляющий автомат. Для его реализации предлагается использовать средство State Machine САПР Quartus фирмы Интел [7–11] и конвертировать полученный файл в САПР "Ковчег" по полученным логическим функциям.

Пример графа автомата с двумя входными переменными x_2x_1 приведен на рис. 20.



State Properties

General	Incoming Transitions	Outgoing Transitions	Actions	Format
Output Port	Output Value	Additional Conditions		
1. 21	0			
2. 22	0			
3. 23	0			
4. 24	0	x_2		
5. 24	1	x_2		
6. 25	0	x_2		
7. 25	1	x_2		

б)

```
module test (clk, vcc, reset, clock, x1, x2, y1, y2, y3, y4, y5, y6, y7, y8, y9, y10, y11, y12, y13, y14, y15, y16, y17, y18, y19, y20, y21, y22, y23, y24, y25, y26, y27, y28, y29, y30, y31, y32, y33, y34, y35, y36, y37, y38, y39, y40, y41, y42, y43, y44, y45, y46, y47, y48, y49, y50, y51, y52, y53, y54, y55, y56, y57, y58, y59, y60, y61, y62, y63, y64, y65, y66, y67, y68, y69, y70, y71, y72, y73, y74, y75, y76, y77, y78, y79, y80, y81, y82, y83, y84, y85, y86, y87, y88, y89, y90, y91, y92, y93, y94, y95, y96, y97, y98, y99, y100, y101, y102, y103, y104, y105, y106, y107, y108, y109, y110, y111, y112, y113, y114, y115, y116, y117, y118, y119, y120, y121, y122, y123, y124, y125, y126, y127, y128, y129, y130, y131, y132, y133, y134, y135, y136, y137, y138, y139, y140, y141, y142, y143, y144, y145, y146, y147, y148, y149, y150, y151, y152, y153, y154, y155, y156, y157, y158, y159, y160, y161, y162, y163, y164, y165, y166, y167, y168, y169, y170, y171, y172, y173, y174, y175, y176, y177, y178, y179, y180, y181, y182, y183, y184, y185, y186, y187, y188, y189, y190, y191, y192, y193, y194, y195, y196, y197, y198, y199, y200, y201, y202, y203, y204, y205, y206, y207, y208, y209, y210, y211, y212, y213, y214, y215, y216, y217, y218, y219, y220, y221, y222, y223, y224, y225, y226, y227, y228, y229, y230, y231, y232, y233, y234, y235, y236, y237, y238, y239, y240, y241, y242, y243, y244, y245, y246, y247, y248, y249, y250, y251, y252, y253, y254, y255, y256, y257, y258, y259, y260, y261, y262, y263, y264, y265, y266, y267, y268, y269, y270, y271, y272, y273, y274, y275, y276, y277, y278, y279, y280, y281, y282, y283, y284, y285, y286, y287, y288, y289, y290, y291, y292, y293, y294, y295, y296, y297, y298, y299, y300, y301, y302, y303, y304, y305, y306, y307, y308, y309, y310, y311, y312, y313, y314, y315, y316, y317, y318, y319, y320, y321, y322, y323, y324, y325, y326, y327, y328, y329, y330, y331, y332, y333, y334, y335, y336, y337, y338, y339, y340, y341, y342, y343, y344, y345, y346, y347, y348, y349, y350, y351, y352, y353, y354, y355, y356, y357, y358, y359, y360, y361, y362, y363, y364, y365, y366, y367, y368, y369, y370, y371, y372, y373, y374, y375, y376, y377, y378, y379, y380, y381, y382, y383, y384, y385, y386, y387, y388, y389, y390, y391, y392, y393, y394, y395, y396, y397, y398, y399, y400, y401, y402, y403, y404, y405, y406, y407, y408, y409, y410, y411, y412, y413, y414, y415, y416, y417, y418, y419, y420, y421, y422, y423, y424, y425, y426, y427, y428, y429, y430, y431, y432, y433, y434, y435, y436, y437, y438, y439, y440, y441, y442, y443, y444, y445, y446, y447, y448, y449, y450, y451, y452, y453, y454, y455, y456, y457, y458, y459, y460, y461, y462, y463, y464, y465, y466, y467, y468, y469, y470, y471, y472, y473, y474, y475, y476, y477, y478, y479, y480, y481, y482, y483, y484, y485, y486, y487, y488, y489, y490, y491, y492, y493, y494, y495, y496, y497, y498, y499, y500, y501, y502, y503, y504, y505, y506, y507, y508, y509, y510, y511, y512, y513, y514, y515, y516, y517, y518, y519, y520, y521, y522, y523, y524, y525, y526, y527, y528, y529, y530, y531, y532, y533, y534, y535, y536, y537, y538, y539, y540, y541, y542, y543, y544, y545, y546, y547, y548, y549, y550, y551, y552, y553, y554, y555, y556, y557, y558, y559, y560, y561, y562, y563, y564, y565, y566, y567, y568, y569, y570, y571, y572, y573, y574, y575, y576, y577, y578, y579, y580, y581, y582, y583, y584, y585, y586, y587, y588, y589, y590, y591, y592, y593, y594, y595, y596, y597, y598, y599, y600, y601, y602, y603, y604, y605, y606, y607, y608, y609, y610, y611, y612, y613, y614, y615, y616, y617, y618, y619, y620, y621, y622, y623, y624, y625, y626, y627, y628, y629, y630, y631, y632, y633, y634, y635, y636, y637, y638, y639, y640, y641, y642, y643, y644, y645, y646, y647, y648, y649, y650, y651, y652, y653, y654, y655, y656, y657, y658, y659, y660, y661, y662, y663, y664, y665, y666, y667, y668, y669, y670, y671, y672, y673, y674, y675, y676, y677, y678, y679, y680, y681, y682, y683, y684, y685, y686, y687, y688, y689, y690, y691, y692, y693, y694, y695, y696, y697, y698, y699, y700, y701, y702, y703, y704, y705, y706, y707, y708, y709, y710, y711, y712, y713, y714, y715, y716, y717, y718, y719, y720, y721, y722, y723, y724, y725, y726, y727, y728, y729, y730, y731, y732, y733, y734, y735, y736, y737, y738, y739, y740, y741, y742, y743, y744, y745, y746, y747, y748, y749, y750, y751, y752, y753, y754, y755, y756, y757, y758, y759, y760, y761, y762, y763, y764, y765, y766, y767, y768, y769, y770, y771, y772, y773, y774, y775, y776, y777, y778, y779, y780, y781, y782, y783, y784, y785, y786, y787, y788, y789, y790, y791, y792, y793, y794, y795, y796, y797, y798, y799, y800, y801, y802, y803, y804, y805, y806, y807, y808, y809, y810, y811, y812, y813, y814, y815, y816, y817, y818, y819, y820, y821, y822, y823, y824, y825, y826, y827, y828, y829, y830, y831, y832, y833, y834, y835, y836, y837, y838, y839, y840, y841, y842, y843, y844, y845, y846, y847, y848, y849, y850, y851, y852, y853, y854, y855, y856, y857, y858, y859, y860, y861, y862, y863, y864, y865, y866, y867, y868, y869, y870, y871, y872, y873, y874, y875, y876, y877, y878, y879, y880, y881, y882, y883, y884, y885, y886, y887, y888, y889, y890, y891, y892, y893, y894, y895, y896, y897, y898, y899, y900, y901, y902, y903, y904, y905, y906, y907, y908, y909, y910, y911, y912, y913, y914, y915, y916, y917, y918, y919, y920, y921, y922, y923, y924, y925, y926, y927, y928, y929, y930, y931, y932, y933, y934, y935, y936, y937, y938, y939, y940, y941, y942, y943, y944, y945, y946, y947, y948, y949, y950, y951, y952, y953, y954, y955, y956, y957, y958, y959, y960, y961, y962, y963, y964, y965, y966, y967, y968, y969, y970, y971, y972, y973, y974, y975, y976, y977, y978, y979, y980, y981, y982, y983, y984, y985, y986, y987, y988, y989, y990, y991, y992, y993, y994, y995, y996, y997, y998, y999, y1000, y1001, y1002, y1003, y1004, y1005, y1006, y1007, y1008, y1009, y1010, y1011, y1012, y1013, y1014, y1015, y1016, y1017, y1018, y1019, y1020, y1021, y1022, y1023, y1024, y1025, y1026, y1027, y1028, y1029, y1030, y1031, y1032, y1033, y1034, y1035, y1036, y1037, y1038, y1039, y1040, y1041, y1042, y1043, y1044, y1045, y1046, y1047, y1048, y1049, y1050, y1051, y1052, y1053, y1054, y1055, y1056, y1057, y1058, y1059, y1060, y1061, y1062, y1063, y1064, y1065, y1066, y1067, y1068, y1069, y1070, y1071, y1072, y1073, y1074, y1075, y1076, y1077, y1078, y1079, y1080, y1081, y1082, y1083, y1084, y1085, y1086, y1087, y1088, y1089, y1090, y1091, y1092, y1093, y1094, y1095, y1096, y1097, y1098, y1099, y1100, y1101, y1102, y1103, y1104, y1105, y1106, y1107, y1108, y1109, y1110, y1111, y1112, y1113, y1114, y1115, y1116, y1117, y1118, y1119, y1120, y1121, y1122, y1123, y1124, y1125, y1126, y1127, y1128, y1129, y1130, y1131, y1132, y1133, y1134, y1135, y1136, y1137, y1138, y1139, y1140, y1141, y1142, y1143, y1144, y1145, y1146, y1147, y1148, y1149, y1150, y1151, y1152, y1153, y1154, y1155, y1156, y1157, y1158, y1159, y1160, y1161, y1162, y1163, y1164, y1165, y1166, y1167, y1168, y1169, y1170, y1171, y1172, y1173, y1174, y1175, y1176, y1177, y1178, y1179, y1180, y1181, y1182, y1183, y1184, y1185, y1186, y1187, y1188, y1189, y1190, y1191, y1192, y1193, y1194, y1195, y1196, y1197, y1198, y1199, y1200, y1201, y1202, y1203, y1204, y1205, y1206, y1207, y1208, y1209, y1210, y1211, y1212, y1213, y1214, y1215, y1216, y1217, y1218, y1219, y1220, y1221, y1222, y1223, y1224, y1225, y1226, y1227, y1228, y1229, y1230, y1231, y1232, y1233, y1234, y1235, y1236, y1237, y1238, y1239, y1240, y1241, y1242, y1243, y1244, y1245, y1246, y1247, y1248, y1249, y1250, y1251, y1252, y1253, y1254, y1255, y1256, y1257, y1258, y1259, y1260, y1261, y1262, y1263, y1264, y1265, y1266, y1267, y1268, y1269, y1270, y1271, y1272, y1273, y1274, y1275, y1276, y1277, y1278, y1279, y1280, y1281, y1282, y1283, y1284, y1285, y1286, y1287, y1288, y1289, y1290, y1291, y1292, y1293, y1294, y1295, y1296, y1297, y1298, y1299, y1300, y1301, y1302, y1303, y1304, y1305, y1306, y1307, y1308, y1309, y1310, y1311, y1312, y1313, y1314, y1315, y1316, y1317, y1318, y1319, y1320, y1321, y1322, y1323, y1324, y1325, y1326, y1327, y1328, y1329, y1330, y1331, y1332, y1333, y1334, y1335, y1336, y1337, y1338, y1339, y1340, y1341, y1342, y1343, y1344, y1345, y1346, y1347, y1348, y1349, y1350, y1351, y1352, y1353, y1354, y1355, y1356, y1357, y1358, y1359, y1360, y1361, y1362, y1363, y1364, y1365, y1366, y1367, y1368, y1369, y1370, y1371, y1372, y1373, y1374, y1375, y1376, y1377, y1378, y1379, y1380, y1381, y1382, y1383, y1384, y1385, y1386, y1387, y1388, y1389, y1390, y1391, y1392, y1393, y1394, y1395, y1396, y1397, y1398, y1399, y1400, y1401, y1402, y1403, y1404, y1405, y1406, y1407, y1408, y1409, y1410, y1411, y1412, y1413, y1414, y1415, y1416, y1417, y1418, y1419, y1420, y1421, y1422, y1423, y1424, y1425, y1426, y1427, y1428, y1429, y1430, y1431, y1432, y1433, y1434, y1435, y1436, y1437, y1438, y1439, y1440, y1441, y1442, y1443, y1444, y1445, y1446, y1447, y1448, y1449, y1450, y1451, y1452, y1453, y1454, y1455, y1456, y1457, y1458, y1459, y1460, y1461, y1462, y1463, y1464, y1465, y1466, y1467, y1468, y1469, y1470, y1471, y1472, y1473, y1474, y1475, y1476, y1477, y1478, y1479, y1480, y1481, y1482, y1483, y1484, y1485, y1486, y1487, y1488, y1489, y1490, y1491, y1492, y1493, y1494, y1495, y1496, y1497, y1498, y1499, y1500, y1501, y1502, y1503, y1504, y1505, y1506, y1507, y1508, y1509, y1510, y1511, y1512, y1513, y1514, y1515, y1516, y1517, y1518, y1519, y1520, y1521, y1522, y1523, y1524, y1525, y1526, y1527, y1528, y1529, y1530, y1531, y1532, y1533, y1534, y1535, y1536, y1537, y1538, y1539, y1540, y1541, y1542, y1543, y1544, y1545, y1546, y1547, y1548, y1549, y1550, y1551, y1552, y1553, y1554, y1555, y1556, y1557, y1558, y1559, y1560, y1561, y1562, y1563, y1564, y1565, y1566, y1567, y1568, y1569, y1570, y1571, y1572, y1573, y1574, y1575, y1576, y1577, y1578, y1579, y1580, y1581, y1582, y1583, y1584, y1585, y1586, y1587, y1588, y1589, y1590, y1591, y1592, y1593, y1594, y1595, y1596, y1597, y1598, y1599, y1600, y1601, y1602, y1603, y1604, y1605, y1606, y1607, y1608, y1609, y1610, y1611, y1612, y1613, y1614, y1615, y1616, y1617, y1618, y1619, y1620, y1621, y1622, y1623, y1624, y1625, y1626, y1627, y1628, y1629, y1630, y1631, y1632, y1633, y1634, y1635, y1636, y1637, y1638, y1639, y1640, y1641, y1642, y1643, y1644, y1645, y1646, y1647, y1648, y1649, y1650, y1651, y1652, y1653, y1654, y1655, y1656, y1657, y1658, y1659, y1660, y1661, y1662, y1663, y1664, y1665, y1666, y1667, y1668, y1669, y1670, y1671, y1672, y1673, y1674, y1675, y1676, y1677, y1678, y1679, y1680, y1681, y1682, y1683, y1684, y1685, y1686, y1687, y1688, y1689, y1690, y1691, y1692, y1693, y1694, y1695, y1696, y1697, y1698, y1699, y1700, y1701, y1702, y1703, y1704, y1705, y1706, y1707, y1708, y1709, y1710, y1711, y1712, y1713, y1714, y1715, y1716, y1717, y1718, y1719, y1720, y1721, y1722, y1723, y1724, y1725, y1726, y1727, y1728, y1729, y1730, y1731, y1732, y1733, y1734, y1735, y1736, y1737, y1738, y1739, y1740, y1741, y1742, y1743, y1744, y1745, y1746, y1747, y1748, y1749, y1750, y1751, y1752, y1753, y1754, y1755, y1756, y1757, y1758, y1759, y1760, y1761, y1762, y1763, y1764, y1765, y1766, y1767, y1768, y1769, y1770, y1771, y1772, y1773, y1774, y1775, y1776, y1777, y1778, y1779, y1780, y1781, y1782, y1783, y1784, y1785, y1786, y1787, y1788, y1789, y1790, y1791, y1792, y1793, y1794, y1795, y1796, y1797, y1798, y1799, y1800, y1801, y1802, y1803, y1804, y1805, y1806, y1807, y1808, y1809, y1810, y1811, y1812, y1813, y1814, y1815, y1816, y1817, y1818, y1819, y1820, y1821, y1822, y1823, y1824, y1825, y1826, y1827, y1828, y1829, y1830, y1831, y1832, y1833, y1834, y1835, y1836, y1837, y1838, y1839, y1840, y1841, y1842, y1843, y1844, y1845, y1846, y1847, y1848, y1849, y1850, y1851, y1852, y1853, y1854, y1855, y1856, y1857, y1858, y1859, y1860, y1861, y1862, y1863, y1864, y1865, y1866, y1867, y1868, y1869, y1870, y1871, y1872, y1873, y1874, y1875, y1876, y1877, y1878, y1879, y1880, y1881, y1882, y1883, y1884, y1885, y1886, y1887, y1888, y1889, y1890, y1891, y1892, y1893, y1894, y1895, y1896, y1897, y1898, y1899, y1900, y1901, y1902, y1903, y1904, y1905, y1906, y1907, y1908, y1909, y1910, y1911, y1912, y1913, y1914, y1915, y1916, y1917, y1918, y1919, y1920, y1921, y1922, y1923, y1924, y1925, y1926, y1927, y1928, y1929, y1930, y1931, y1932, y1933, y1934, y1935, y1936, y1937, y1938, y1939, y1940, y1941, y1942, y1943, y1944, y1945, y1946, y1947, y1948, y1949, y1950, y1951, y1952, y1953, y1954, y1955, y1956, y1957, y1958, y1959, y1960, y1961, y1962, y1963, y1964, y1965, y1966, y1967, y1968, y1969, y1970, y1971, y1972, y1973, y1974, y1975, y1976, y1977, y1978, y1979, y1980, y1981, y1982, y1983, y1984, y1985, y1986, y1987, y1988, y1989, y1990, y1991, y1992, y1993, y1994, y1995, y1996, y1997, y1998, y1999, y2000, y2001, y2002, y2003, y2004, y2005, y2006, y2007, y2008, y2009, y2010, y2011, y2012, y2013, y2014, y2015, y2016, y2017, y2018, y2019, y2020, y2021,
```

Выводы

Импортозамещение электронной компонентной базы и программного обеспечения являются важнейшими вопросами обеспечения информационной безопасности страны, без решения которых невозможен технологический прорыв, обеспечивающий суверенитет и независимость государства в XXI в. Использование базовых матричных кристаллов, разрабатываемых в ТЦ "МИЭТ", изучение в вузах соответствующей САПР "Ковчег" в существенной мере позволяет продвинуться в этом направлении, особенно в области реализации криптоалгоритмов. Предложенная для учебных целей реализация криптопроцессора позволяет в перспективе отказаться от зарубежных ПЛИС. В дальнейшем целесообразно рассмотреть вопрос использования отечественных ПЛИС, выпускаемых в Воронежском ОА КТЦ-Электроника.

Список литературы

1. Абонентские шифраторы "КРИПТОН". URL: <http://asic.ru> (дата обращения: 06.05.19).
2. Сайт микросхем заказных и полузаказных больших интегральных схем ASIC. URL: <http://asic.ru> (дата обращения: 06.05.19).
3. Денисов А.Н., Фомин Ю.П., Коняхин В.В., Федоров Р.А. Библиотека функциональных ячеек для проектирования полузаказных микросхем серий 5503 и 5507 / под общ. ред. А.Н. Саурова. М.: Техносфера, 2012. 304 с.
4. Мария Ермак. Российские микроконтроллеры с ядром Cortex. URL: [M3https://www.milandr.ru/upload/semi/sovremennye_rossiyskie_32_kh_razryadnye_mk_s_yadrom_arm_cortex_m3.pdf](https://www.milandr.ru/upload/semi/sovremennye_rossiyskie_32_kh_razryadnye_mk_s_yadrom_arm_cortex_m3.pdf) (дата обращения: 07.05.2019).
5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования — Техэксперт. URL: <http://docs.cntd.ru/document/1200007350> (дата обращения: 05.05.2019).
6. Гаврилов С.В., Денисов А.Н., Коняхин В.В., Макарецва М.М. САПР "Ковчег 3.0" для проектирования микросхем на БМК серий 5503, 5507, 5521 и 5529. М., 2013. 295 с.
7. Quartus II Help v11.1 > enum_encoding VHDL Synthesis Attribute. URL: http://quartushelp.altera.com/11.1/mergedProjects/hdl/vhdl/vhdl_file_dir_enum_encoding.htm (дата обращения: 07.05.19 г.)
8. Тюрин С.Ф., Громов О.А., Греков А.В. Реализация цифровых автоматов в системе Quartus фирмы Altera: лабораторный практикум. Пермь: Изд-во ПНИПУ, 2011. 133 с.
9. Математическая логика и теория алгоритмов. Моделирование логики: учеб. пособие / С.Ф. Тюрин, Д.Р. Валеев, А.В. Мазунина, В.А. Суворова, А.А. Чесноков / под ред. С.Ф. Тюрин. Перм. гос. нац. исслед. ун-т, 2015. 176 с.
10. Тюрин С.Ф., Каменских А.Н., Зобнина О.А. Использование в учебном процессе отечественной системы автоматизированного проектирования (САПР) "Ковчег" // Вестник Пермского университета. Математика. Механика. Информатика. 2018. № 2 (41). С. 75–79.
11. Зобнина О.А., Каменских А.Н., Тюрин С.Ф. Синтез конечного автомата с использованием отечественной САПР "Ковчег". В сб.: Автоматизированные системы управления и информационные технологии: матер. всерос. науч.-техн. конф.: в 2-х т. 2018. С. 28–32.

Design of a cryptoprocessor elements with the domestic CAD "Ark"

О. А. Zobnina

Perm National Research Polytechnic University; 29, Komsomolsky Av., Perm, 614990, Russia
zobnina.olka@gmail.com; +7-922-37-78-699

А. Н. Kamenskih

Perm National Research Polytechnic University; 29, Komsomolsky Av., Perm, 614990, Russia
antoshkinoinfo@yandex.ru; +7-902-64-12-545

Г. К. Korolev

Perm State University; 15, Bukireva st., Perm, 614990, Russia
ZAO IVS-NET; 65, N. Ostrovsky st., Perm, 614015, Russia
korolevgk@mail.ru; +7-950-44-31-343

S. F. Tyurin

Perm National Research Polytechnic University; 29, Komsomolsky Av., Perm, 614990, Russia

Perm State University; 15, Bukireva st., Perm, 614990, Russia

tyurinsergfeo@yandex.ru; +7 952-320-02-510

Article investigates a crypto processor – the "CRYPTON" subscriber coder/decoder in order to assess the feasibility of implementation with the domestic elements in the framework of import substitution tasks. Authors study GOST 28147-89, which describes the encryption and decryption algorithms used in "CRIPTON". It turns out that one of the basic operations on 2 32-bit operands is bitwise XOR, addition modulo 2 in degree 32, a shift, including cyclic, permutation. To implement the algorithm we need eleven 32-bit registers, adders, a substitution code converter and a finite state machine. It is shown that the elements used, including of foreign manufacturers FPGAs can be replaced by domestic analogs. It is proposed to use Uncommitted Logic Array (ULA) instead of FPGAs. Some devices of the crypto processor are being developed using the domestic CAD system Ark. Simulation confirms the performance of the proposed devices.

Keywords: *cryptoprocessor; uncommitted logic array; CAD.*