The high-speed device for the accelerated coercion of number on the module

S Tynymbaev, R Berdibayev, Zh Zhaibergenova*

Kazakh National Research Technical University, Satpayev Str. 22, Kazakhstan, Almaty

**Corresponding author's e-mail: zhanshuak@gmail.com*

Abstract

This article presents the method of an acceleration of coercion execution operator on the module where for each two step discharges of the given number are processed that leads to residual formation process acceleration. The article considers development of the high-speed hardware solution of coercion operator on the module.

Keywords: high-speed device, module, cipher, coercion

1 Introduction

Perhaps to realize encoding programmatically it is hardware and software. The hardware encoding has a row of essential advantages:

- hardware of encoding has high speed;
- application of a specialized processor with cipher for execution of cryptography conversions unloads the central processor of the computer; also installation on one computer of several hardware scramblers is possible that it even more increases information processing rate;
- the hardware implementation of a crypto algorithm guarantees its integrity;
- encoding and storage of keys is carried out in the board of the scrambler, but not in a random access memory of the computer.
- on the basis of the hardware scramblers it is possible to create systems of information security from illegal access and demarcation of access to the computer, etc. [1, 2].

The vast majority of the modern cryptosystems are used asymmetric encoding [3]. Feature of asymmetric encryption algorithms is that for an encryption and decoding of information different keys are used.

In asymmetric crypto algorithms such operations as multiplication of numbers, squaring and coercion of numbers on the module are executed.

The most bulky of them is coercion operator on the module since it represents receiving a remainder of division of number on module, and division operation – the most difficult of arithmetical operations. And this operation repeats repeatedly since instead of repeated multiplication and divisions of very large number (a^x) on the module, for an acceleration of exponentiation on the module, multistep sequential multiplication of exponentiation on the module is used, multistep sequential multiplication with coercion on the module on each step every time of the new work is used.

The wide experience in development of high-speed integer multipliers and squarer's for different class of computing systems is so far accumulated. For an acceleration of basic operations of multiplication and squaring it is possible to use matrix multipliers, a circuit of adders of Wallace, Dad's counter, systolic and Vedic multipliers [5, 6].

As for an acceleration of basic coercion operator on the module, such task in traditional computing systems didn't stand. Therefore the high-speed hardware solution of coercion operator on the module is a key problem in case of the hardware implementation of the crypto algorithms using exponentiation of numbers in a level on the module.

2 Operation execution process

One of the operation approaches of an acceleration of execution coercion operators of numbers on the module is considered, on the basis of the dividing device where for a step of division two discharges of the given number are processed, accelerating residual formation process.

The functional diagram of such device of coercion of number A on the module where in high orders of the register RGA [2n-1/n] in each step of division the partial residuals of R_i are created is provided on Figure 1.

Conditions of formation of the partial residuals (R_i) is defined (Table 1).

TABLE 1condition of formation of residuals

Conditions for the analysis	R_i
2^2* R_{i-1}< C	4 R_{i-1}
C<=2^2* R_{i-1}<2C	4 R_{i-1}-C
2C<=2^2* R_{i-1}<3C	4 R_{i-1}-2C
3C<=2^2* R_{i-1}	4 R_{i-1}-3C

Check of all conditions it is executed at the same time, the adder for formation of the module of the multiple to three for this purpose will be required ($3\bar{C}$). Apparently from the Figure 1 it is executed on the SMO adder on which inputs values $\bar{C}$ (carry) and C with the left shift on one discharge towards the high order of the module, i.e. 2C move. Computation of 4_{Ri-1}-C, 4_{Ri-1}-2C and 4_{Ri-1}-3C will require the appropriate SM_1, SM_2, SM_3 adders. In these adders subtraction operation is replaced with addition operation by submission with inputs of low orders of adders the one code, and on the first inputs of adders the next residual shifted on two discharges to the left, i.e. 4_{Ri-1} moves, and on the second inputs of SM_1, SM_2, SM_3 adders modules $3\bar{C}$, $2\bar{C}$ and $\bar{C}$ respectively move.

In case of additions of number 4_{Ri-1} with modules $3\bar{C}+1$, $2\bar{C}+1$ and $\bar{C}+1$ on outputs of these adders transfers of $\bar{C}3$, $\bar{C}2$, $\bar{C}1$ are created of polarity bits and value of the signs S_3(sign), S_2, S_1. If the received residual on an adder i-go output the positive, $\bar{C_i} = \mathbf{1}$ at the same time S_i=0, and if the received residual on an adder i-go output the negative, $\bar{C_i} = 0$ and S_i=1.

On outputs of the considered adders the smallest positive residual (SPR) will allow us to define the analysis of combinations of transfers and signs. If on outputs of all adders received residuals with the negative signs, then the previous residual shifted on two discharges towards the senior 4Ri-1 is transferred to high orders of the register RGA[2n-1/n], through the diagrams AND6 and OR1.

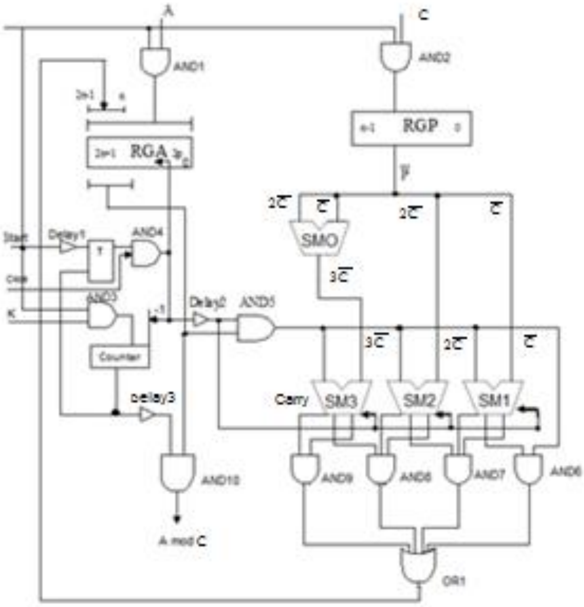


FIGURE 1 An example. The functional diagram of coercion of number on the module

Conditions of formation of the next smallest positive residual (R_i) are given (Table 2). Depending on value of transfers from polarity bits and values of signs of residuals.

TABLE 2 Conditions of formation of the next smallest positive residual (R_i)

C3	S3	C2	S2	C1	S1	SM3	SM2	SM1	2 R_{i-1}
1	0	1	0	1	0	R_i	-	-	-
0	1	1	0	1	0	-	R_i	-	-
0	1	0	1	1	0	-	-	R_i	+
0	1	0	1	0	1	-	-	-	R_i=4*R_{i-1}

From the Table 2, and also from the diagram provided on Figure 1 it is visible that in case of $\bar{C}_3 = \bar{C}_2 = \bar{C}_1 = 1$, and S_3 = S_2 = S_1=0 as the smallest positive residual of R_i determined by C_2 residual with an output of SM_3 which is transferred to a diagram AND9 output by C_3 signal. At the same time the signal of S_3 = S_2 = S_1 locks transmissions from outputs SM_2, SM_3 and value 4_{Ri-1} with the diagrams AND8, AND7 and AND6.

In case of $\bar{C}_3 = 0$, $\bar{C}_2 = \bar{C}_1 = 1$ next partial residual is created on counter total exits of adder SM_2 and outputs of adder SM_3 are locked with a signal C_3=0, and the signal of S_2 = 0 and S_1=0 locks counter total exits of SM_2 and passing of a code 4_{Ri-1} on inputs of OR circuit 1.

In case of $\bar{C}_3 = \bar{C}_2 = 0$ and $\bar{C}_1 = 1$ the next residual of R_i is created by $\bar{C}_2 = 0$ and $\bar{C}_1 = 0$ on counter total exit of SM_1 at the same time signals of $\bar{C}_3 = 0$, $\bar{C}_2 = 0$ lock outputs of adders SM_3 and SM_1, and the signal of S_1=0 locks passing 4_{Ri-1} on register RGA inputs.

In case of $\bar{C}_3 = \bar{C}_2 = \bar{C}_1 = 0$ value of a signal S_1=1 as the next residual is defined by C_2 by the diagram AND6 with value $4_{Ri-1.}$

Set of AND6/AND9 and OR1 form the Figure 1 the generator of the smallest positive residual (SFD), and the SFD together with SM3, SM2, SM1 adders form the generator of the partial residuals.

3 Diagrams of coercion on the module

On a signal "Start" the given number A is accepted through the diagram AND1 in the register RGA, the module is accepted in the register C number of shifts K = $\log_2 n/2$ (where n-number of discharges modules C). Through the figures AND3 registers in the counter of clock pulses (CCP). The delayed signal "Start-up" on the line of time delay Delay1 writes time of numbers of A,C,K on the appropriate diagrams arrives on a trigger T input. The trigger will be set by this signal in 1 status which arrives on the first input of the diagram AND4. After that the first clock signal on permission will appear on an output of the diagram AND4 abd shifts on two discharges of the register RGA, and subtracts unit from the counter. The delayed first TI on the line of a time delay of Delay2 arrives on the first input of the diagram AND5, and on the second inputs of this diagram the high orders RGA arrives. Here it should be noted that summary delay period on Delay1, the trigger of the diagram AND4 and Delay2 shall be more than time formation the multiple 3C on counter total exit of adder SMO.

From outputs the SMO adder the code 3C moves on the second input of the SM3 adder, and on the second inputs of the adder the code C with single position shift moves to the left; on the second inputs the SM1 adder moves a code $\bar{C}$.

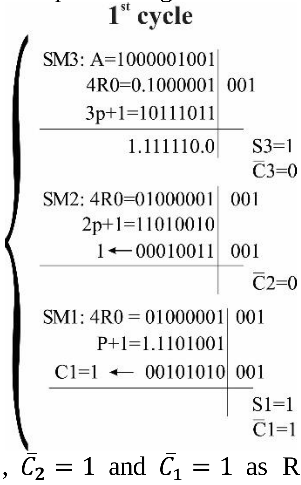
From a diagram AND5 output high orders of the register RGA moves also on the first inputs of SM3, SM2 and SM1 adders, and also on the second input of the diagram AND6.

In SM3, SM2, SM1 adders operations 4_{Ri-1}+3C+1, $_{4Ri-1}$+2C+1, 4_{Ri-1}+C+1 are executed. Respectively, and on an output of the diagram SFD the smallest positive residual which moves on register A inputs is created. After that on an input of AND4 the second clock signal which shifts register RGA contents on two discharges to the left arrives and after a time delay of the second clock signal shifted on two discharges from R1 moves through the diagrams AND5 on inputs of all adders, and in these adders values $3\bar{C}+1$, $2\bar{C}+1$ and $\bar{C}+1$ with 4R$_1$ are added and on an output of the SFD the following residual of R$_2$ which is accepted in the register RGA is created. Detention by the second clock signal is subtracted from the indication of the counter of clock pulses counter unit.

Formation of the next private residual continues until the indication of the counter is nullified. At the same time in the counter of clock signals the signal "The end of operation" is created and the trigger will be set by this signal in a bullet status that locks submission of the next clock pulse in the diagram of the device. The same signal the diagram AND10 gives result from the register RGA on an output.

Below an example of computation of residual in the considered device is reviewed.

At the same time
A=521$_{10}$=1000001001
$\bar{C}$=23$_{10}$=0010111
$\bar{C}$+1=1001001
2$\bar{C}$=00101110
2$\bar{c}$+1=11010010
3$\bar{c}$=01000101
3$\bar{c}$+1=10111011
where A is the example of the given number

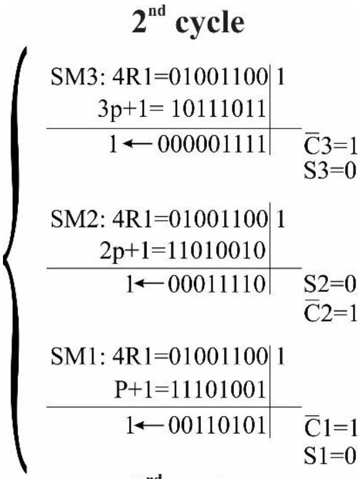


```
1st cycle

SM3: A=1000001001|
      4R0=0.1000001| 001
      3p+1=10111011|
------------------------
          1.111110.0|   S3=1
                        C̄3=0
SM2: 4R0=01000001| 001
      2p+1=11010010|
    1 ←— 00010011| 001
------------------------
                 |      C̄2=0

SM1: 4R0 = 01000001| 001
       P+1=1.1101001|
  C1=1 ←  00101010| 001
------------------------
                  |     S1=1
                        C̄1=1
```

As $\bar{C}_3 = 0$, $\bar{C}_2 = 1$ and $\bar{C}_1 = 1$ as R$_1$ selected like R$_1$=10011

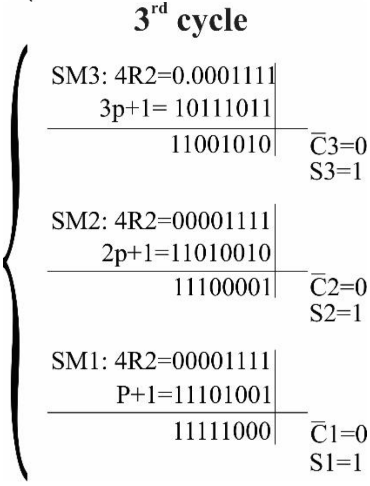


```
2nd cycle

SM3: 4R1=01001100| 1
     3p+1= 10111011|
------------------------
    1 ←— 000001111|    C̄3=1
                       S3=0

SM2: 4R1=01001100| 1
     2p+1=11010010|
------------------------
     1←—00011110|      S2=0
                       C̄2=1

SM1: 4R1=01001100| 1
      P+1=11101001|
------------------------
     1←—00110101|      C̄1=1
                       S1=0
```



```
3rd cycle

SM3: 4R2=0.0001111|
     3p+1= 10111011|
------------------------
          11001010|    C̄3=0
                       S3=1

SM2: 4R2=00001111|
     2p+1=11010010|
------------------------
          11100001|    C̄2=0
                       S2=1

SM1: 4R2=00001111|
      P+1=11101001|
------------------------
          11111000|    C̄1=0
                       S1=1
```

R$_3$=1111=15$_{10}$
Check: 521 mod 23 = 15 mod 23

7 Conclusions

On the basis of the dividing device where for a step of division two discharges of the given number are processed, accelerating residual formation process approaches of an acceleration of execution coercion operators on the module P is considered with example.

References

[1] Shan'gin V F 2012 *Zashita informatsii v komp'uternyh sistemah i setyah* Press 160p

[2] Ryabko B YA, Fionov A I 2004 *Osnovy sovremennoi kriptografii dlya specialistov v informatsionnyh tehnologiyah* M:Nauchnyi mir

[3] Rostovtsev A G, Mahovenko E B 2005 *Teoriticheskaya kriptografiya* SPb:Professional 280p

[4] Orlov S A, Tsil'ker B YA 2014 *Organizatsiya EVM i system* SPb:Piter

[5] Sethi K, Panda R 2012 An improved squaring circuits for binary numbers *International Journal of Advanced Computer Science and Application* **3**(2) 116 p