Lernplattform Moodle
Technische Universität München

Frage 1

Antwort gespeichert

Erreichbare Punkte: 1,00

What are the variables $X_i^{(1)}$ and $Y_i^{(9)}$ with i ∈ {1,...,4}?

Wählen Sie eine oder mehrere Antworten:

- [ ] $X_i^{(1)}$ is the encrypted output
- [x] $Y_i^{(9)}$ is the encrypted output
- [x] $X_i^{(1)}$ is the clear text input
- [ ] $Y_i^{(9)}$ is the clear text input

Frage 2

Antwort gespeichert

Erreichbare Punkte: 1,00

Which output feeds the input $X_i^{(r+1)}$, r ∈ {1, ... ,7} ?

Wählen Sie eine Antwort:

- ( ) The output of the transformation step $Y_i^{(9)}$
- ( ) The output of the next round $Y_i^{(r+2)}$
- ( ) The output of the same round $Y_i^{(r+1)}$
- (•) The output of the previous round $Y_i^{(r)}$

Frage 3

Antwort gespeichert

Erreichbare Punkte: 1,00

How are a and b calculated from the input vectors $X_i^{(r)}$ and $Z_i^{(r)}$ of the modulo-multiplier?

Wählen Sie eine Antwort:

- ( ) $a = X_i^{(r)} \forall X_i^{(r)}$ and $b = Z_i^{(r)} \forall Z_i^{(r)}$
- ( ) $a = 0 \,\&\, X_i^{(r)} \forall X_i^{(r)}$ and $b = 0 \,\&\, Z_i^{(r)} \forall Z_i^{(r)}$
- ( ) $a = 1 \,\&\, X_i^{(r)} \forall X_i^{(r)}$ and $b = 1 \,\&\, Z_i^{(r)} \forall Z_i^{(r)}$
- (•) $a = \begin{cases} 0 \,\&\, X_i^{(r)} \; for \; X_i^{(r)} \in \{1,2,\cdots,2^n-1\} \\ 1 \,\&\, X_i^{(r)} \; for \; X_i^{(r)} = 0 \end{cases}$ and $b = \begin{cases} 0 \,\&\, Z_i^{(r)} \; for \; Z_i^{(r)} \in \{1,2,\cdots,2^n-1\} \\ 1 \,\&\, Z_i^{(r)} \; for \; Z_i^{(r)} = 0 \end{cases}$

Frage 4

Antwort gespeichert

Erreichbare Punkte: 1,00

a and b to be two integer out of $\{1, \cdots, 2^n\}$. How many bits are necessary for the unsigned representation of a and b? How many for the product ab (worst-case)? Please consider in your answer that you really check the **minimum** number of necessary bits!

Wählen Sie eine Antwort:

- a: n bits, b: n bits, ab: $2 * n$ bits
- a: $n + 1$ bits, b: $n + 1$ bits, ab: $2 * n$ bits
- a: $n + 1$ bits, b: $n + 1$ bits, ab: $2 * n + 1$ bits
- a: $n + 1$ bits, b: $n + 1$ bits, ab: $2 * (n + 1)$ bits

Frage 5

Antwort gespeichert

Erreichbare Punkte: 1,00

What would be the value of n for the modulo-multiplier in the IDEA algorithm?

Antwort:

16

Frage 6

Antwort gespeichert

Erreichbare Punkte: 1,00

Which bits are masked by the modulo 2^n operation, which do remain? How many bits are necessary for the result of (ab mod 2^n)? (Hint: The LSB has number 0!)

Wählen Sie eine Antwort:

- The left bits (MSBs) are masked and the right bits (LSBs) remain. n bits are necessary for the result.
- The right bits (LSBs) are masked and the left bits (MSBs) remain. n bits are necessary for the result.
- The left bits (MSBs) are masked and the right bits (LSBs) remain. $n + 1$ bits are necessary for the result.
- The right bits (LSBs) are masked and the left bits (MSBs) remain. $n + 1$ bits are necessary for the result.
- The left bits (MSBs) are masked and the right bits (LSBs) remain. $n - 1$ bits are necessary for the result.
- The right bits (LSBs) are masked and the left bits (MSBs) remain. $n - 1$ bits are necessary for the result.

Frage 7

Antwort gespeichert

Erreichbare Punkte: 1,00

Which simple bit operation is the equivalent of $(ab \text{ div } 2^n)$? Which bits of the product ab remain? Where are they after the division? How many bits are needed for the result? Take also the case of a or b equal to 2^n into consideration!

Wählen Sie eine Antwort:

- It is equivalent to a right-shift operation of n bits. The left bits (MSBs) of the product ab remain. $n+1$ bits are necessary for the result.
- It is equivalent to a right-shift operation of n bits. The left bits (MSBs) of the product ab remain. n bits are necessary for the result.
- It is equivalent to a right-shift operation of n bits. The left bits (MSBs) of the product ab remain. $n-1$ bits are necessary for the result.
- It is equivalent to a right-shift operation of $n-1$ bits. The left bits (MSBs) of the product ab remain. $n+1$ bits are necessary for the result.
- It is equivalent to a right-shift operation of $n-1$ bits. The left bits (MSBs) of the product ab remain. n bits are necessary for the result.
- It is equivalent to a right-shift operation of $n-1$ bits. The left bits (MSBs) of the product ab remain. $n-1$ bits are necessary for the result.
- It is equivalent to a right-shift operation of $n+1$ bits. The left bits (MSBs) of the product ab remain. $n+1$ bits are necessary for the result.
- It is equivalent to a right-shift operation of $n+1$ bits. The left bits (MSBs) of the product ab remain. n bits are necessary for the result.
- It is equivalent to a right-shift operation of $n+1$ bits. The left bits (MSBs) of the product ab remain. $n-1$ bits are necessary for the result.

Frage 8

Antwort gespeichert

Erreichbare Punkte: 1,00

What is the result of $(ab \bmod (2^n+1))$, if $(ab \bmod 2^n) = (ab \text{ div } 2^n)$? Is this case possible if a and b were integers in the range of $\{1, \cdots, 2^n\}$ and 2^n+1 was a prime number?

The result of $(ab \bmod (2^n+1))$ is 0 and it is not possible.

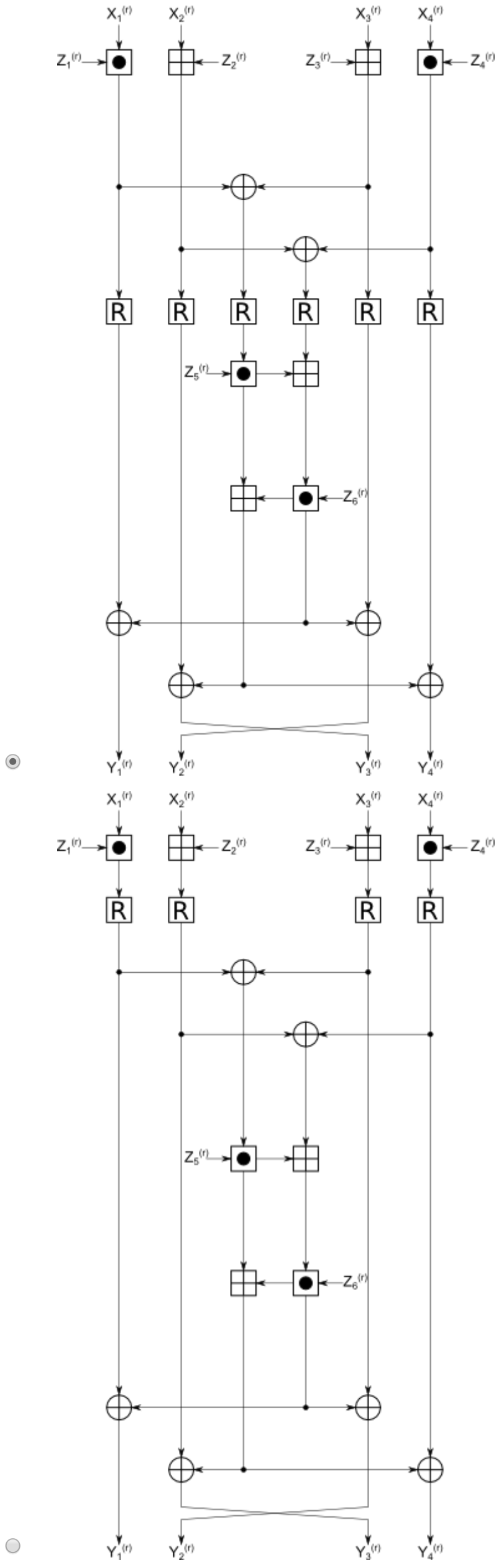
Frage 9

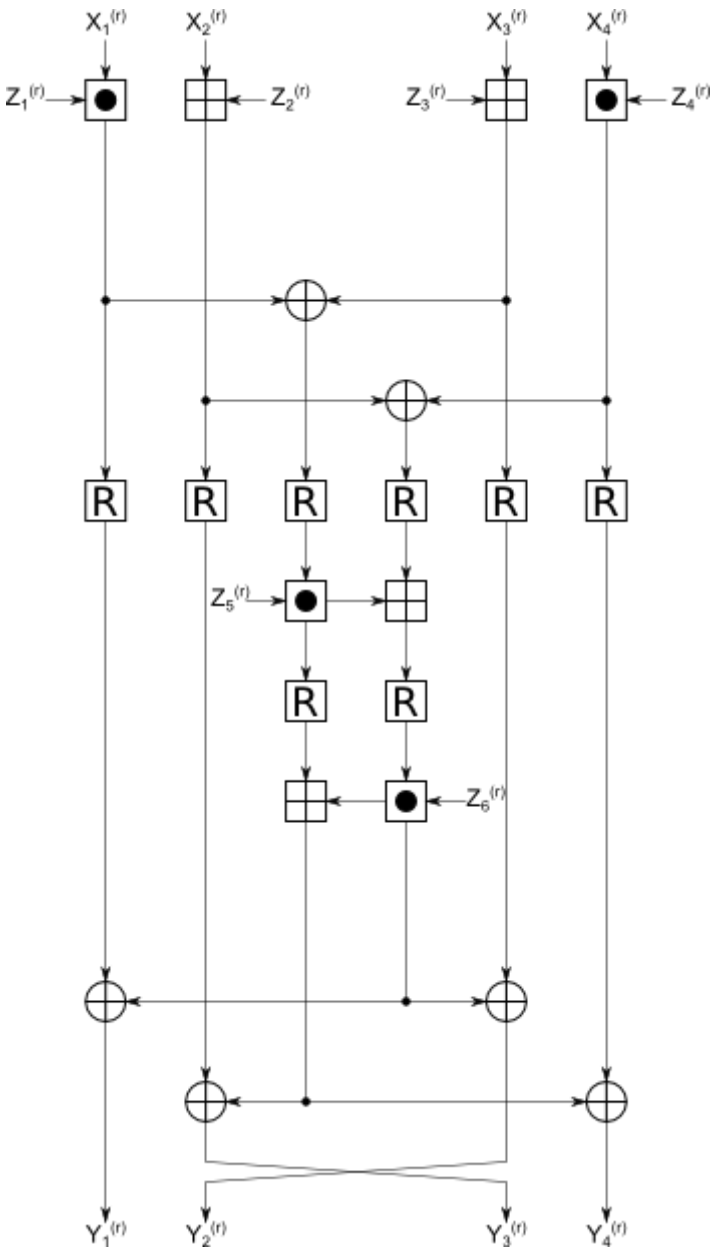
Antwort gespeichert

Erreichbare Punkte: 1,00

How would you split up the round in 2 steps if you had 2 modulo-multipliers, 2 adders and unlimited XOR modules? If more options are correct, choose the one with the shortest critical path.

Wählen Sie eine Antwort:




$X_1^{(r)}$
$X_2^{(r)}$
$X_3^{(r)}$
$X_4^{(r)}$
$Z_1^{(r)}$
$Z_2^{(r)}$
$Z_3^{(r)}$
$Z_4^{(r)}$
R
$Z_5^{(r)}$
$Z_6^{(r)}$
$Y_1^{(r)}$
$Y_2^{(r)}$
$Y_3^{(r)}$
$Y_4^{(r)}$

Frage 10

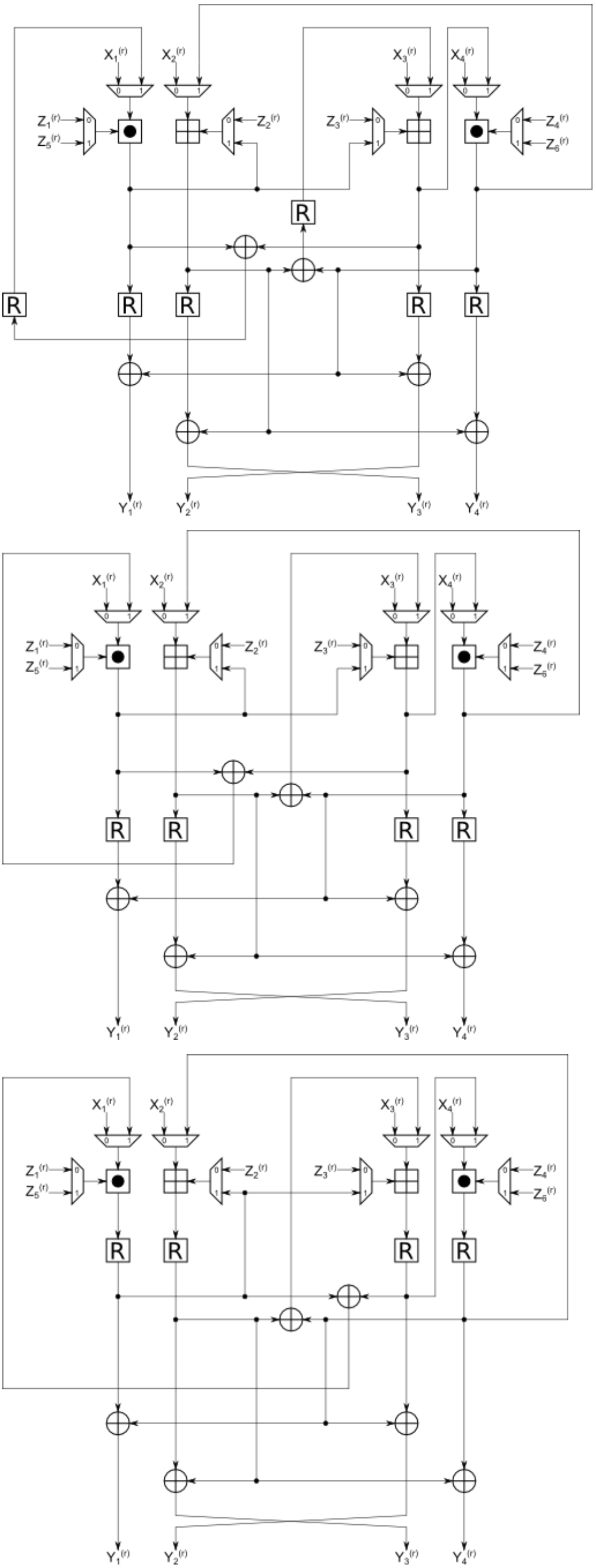
Antwort gespeichert

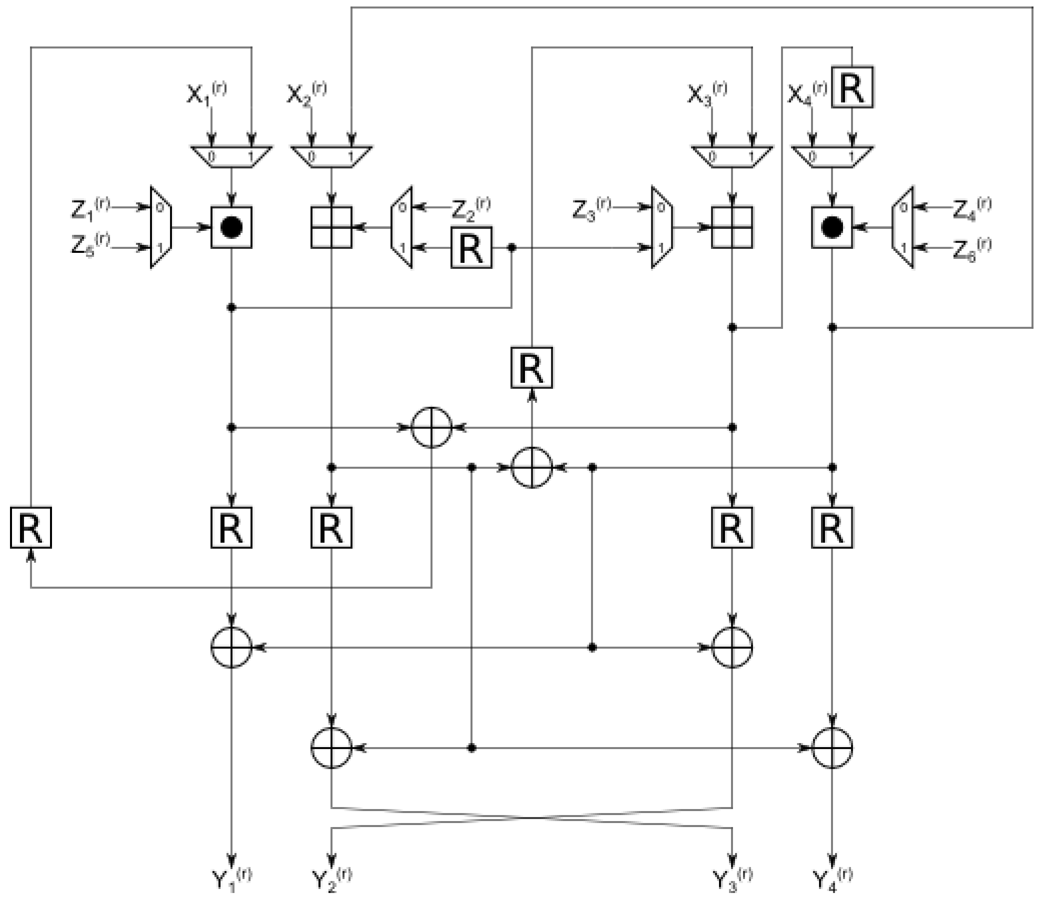
Erreichbare Punkte: 1,00

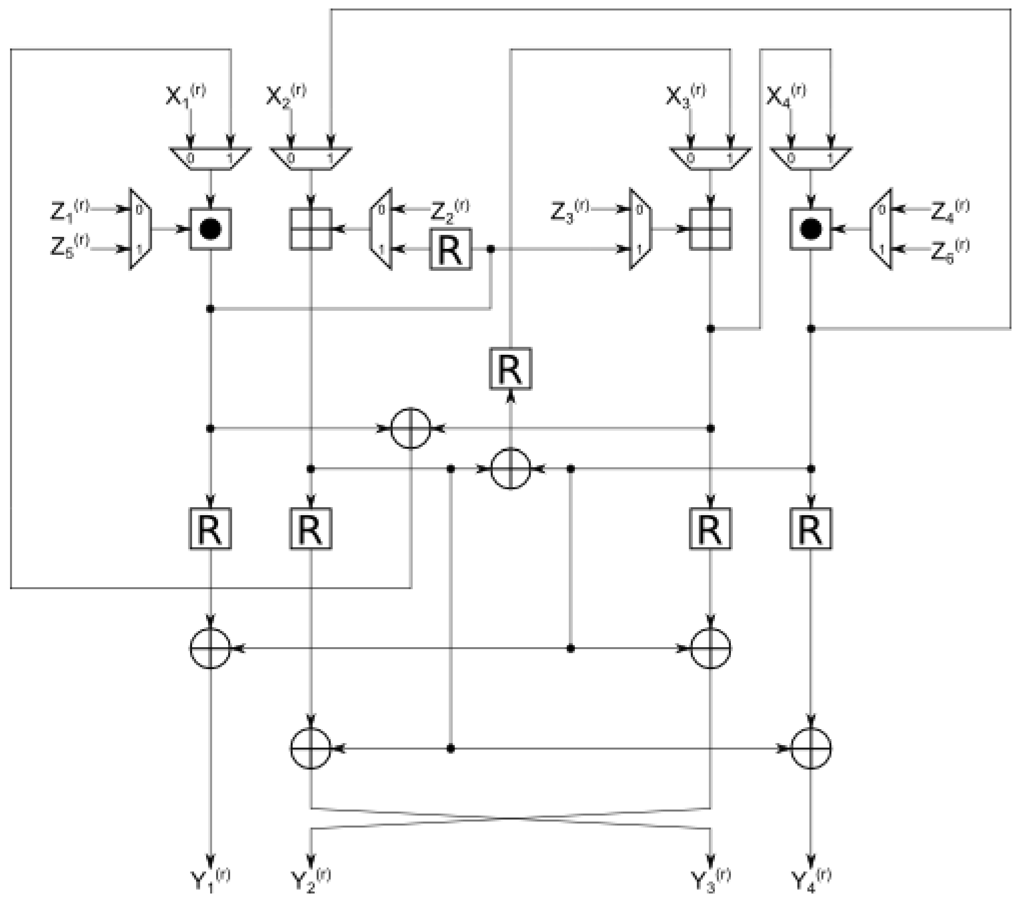
Design a datapath with 2 adder and 2 modulo-multiplier. The design should have two steps. Make your choice based on the splitting in task 3.1 (previous question).

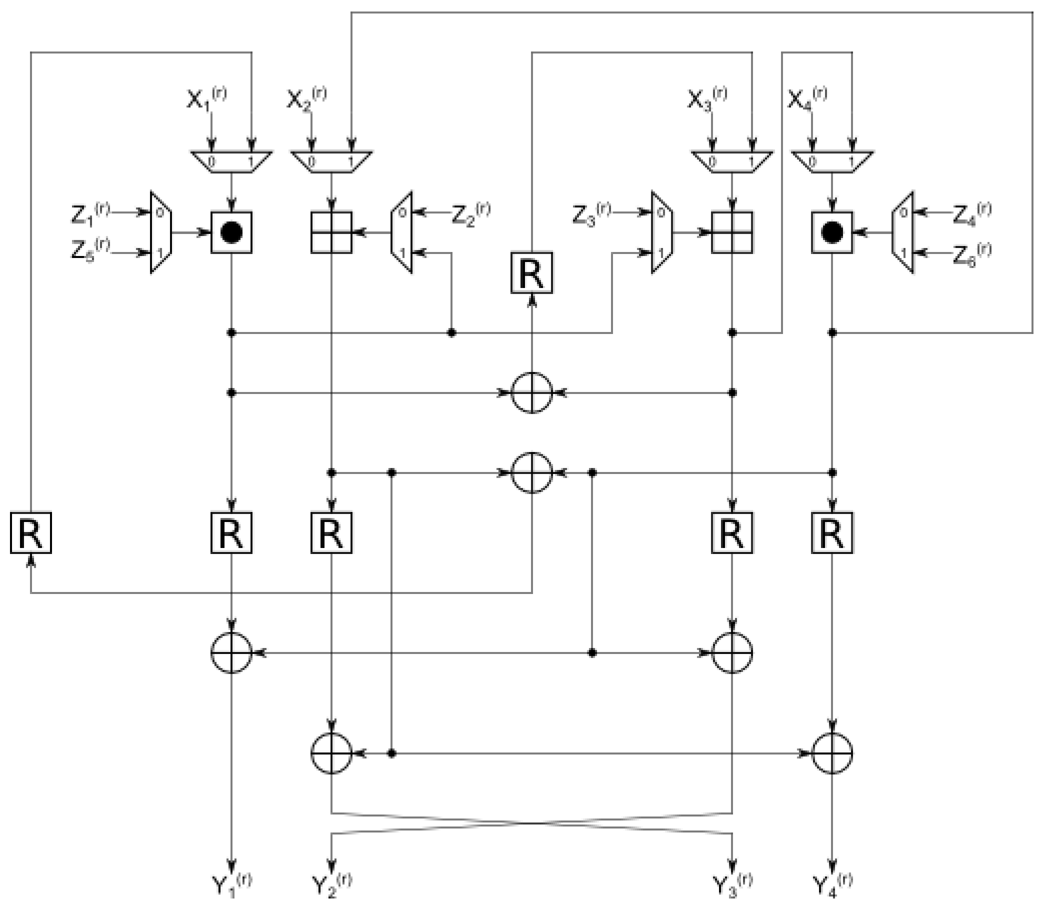
Hint: The correct result must be available after 2 steps at the output.

Wählen Sie eine Antwort:




X1(r)
X2(r)
X3(r)
X4(r)
Z1(r)
Z5(r)
Z2(r)
Z3(r)
Z4(r)
Z6(r)
R
Y1(r)
Y2(r)
Y3(r)
Y4(r)


X1(r)
X2(r)
X3(r)
X4(r)
Z1(r)
Z5(r)
Z2(r)
Z3(r)
Z4(r)
Z6(r)
R
Y1(r)
Y2(r)
Y3(r)
Y4(r)


X1(r)
X2(r)
X3(r)
X4(r)
Z1(r)
Z5(r)
Z2(r)
Z3(r)
Z4(r)
Z6(r)
R
Y1(r)
Y2(r)
Y3(r)
Y4(r)

Frage 11

Antwort gespeichert

Erreichbare Punkte: 1,00

Every SLICE provides two function generators (F and G). These are used to perform one XOR operation each. How many SLICEs are therefore required to realize a 16 bit XOR operation?

Antwort:

8

Frage 12

Antwort gespeichert

Erreichbare Punkte: 1,00

The delays given in table 3 can be used to estimate the propagation delays in the single components of the CLB. How many ns does a 16 bit XOR operation take? Is the time dependent on the input width?

It takes 3 ns and it is independent on the input width.

Frage 13

Antwort gespeichert

Erreichbare Punkte: 1,00

Use your knowledge to find the maximum delay in ns of a 16 bit adder. Consider the fact that at time t=0, all input signals are valid.

Hint: What path causes the longest delay?

Antwort:

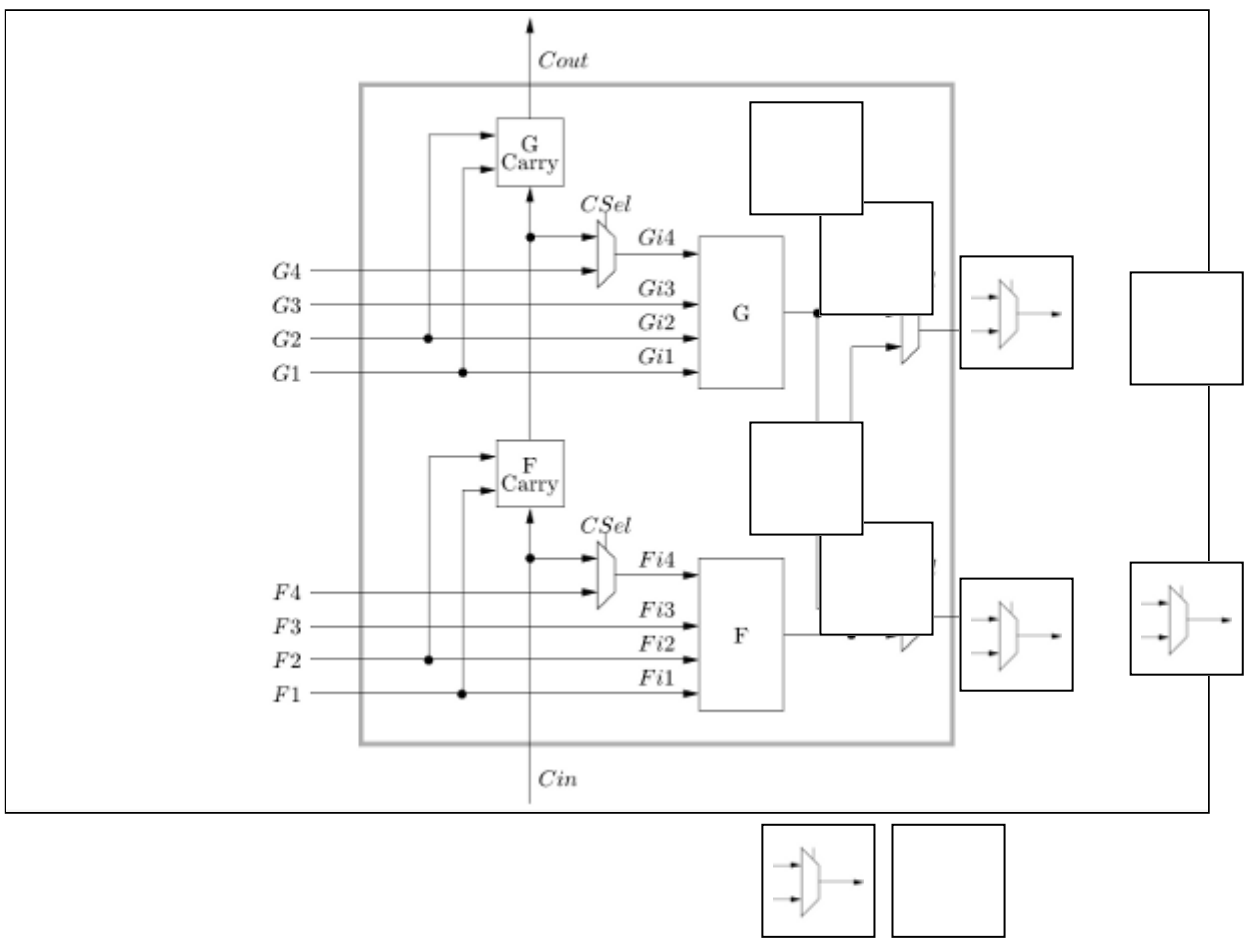
18

Frage 14

Antwort gespeichert

Erreichbare Punkte: 0,50

As shown in Fig. 46, a 4 to 1 multiplexer can be also realized with three 2 to 1 multiplexers arranged in two stages. Drag and drop three multiplexers on the SLICE on that places where one multiplexer is implemented or used. Please assume that just **output X** is used as output. Drag and drop blank images onto all other components which are not used for the 4 to 1 multiplexer.



Frage 15

Antwort gespeichert

Erreichbare Punkte: 0,50

Estimate the propagation delay in ns of a 16 bit wide 4 to 1 multiplexer based on your previous considerations.

Antwort:

3

Frage 16

Antwort gespeichert

Erreichbare Punkte: 2,00

Estimate the computing time for the complete encryption process in case the algorithm is implemented directly as described in section 4.6. Use the module delays from sections 6.1.1 to 6.1.5 (Remember: the delay of the adder is just 10ns). For simplification reasons take the longest path of one round as base, multiply it with the amount of rounds and add the longest path of the output transformation. How many encryptions per second are possible with this implementation?

The longest path through one round (In the case of several possibilities choose one!) starts from input X [1], ends at output Y [4] and it takes [92] ns for the signal to be stable at all outputs of the round. The whole encryption takes [758] ns and therefore [1319261] whole encryptions per second are possible.

Would it be possible - if necessary using additional registers - to start a new calculation while the current encryption is not yet finished?

[Yes, with using additional registers after each round.]

If it is possible, what would be the minimal clock cycle and the resulting encryptions per second? If it is not possible leave the spaces empty.

The minimal clock cycle is [96] ns and therefore [10416666] whole encryptions per second are possible.

Frage 17

Antwort gespeichert

Erreichbare Punkte: 1,00

Find the shortest clock cycle for which the Resource Constrained Scheduling 1 works correctly (Remember the delay of a 2:1 MUX is 0ns). Considering section 5.2.4, how many clock cycles are needed to finish one complete encryption?

The shortest clock cycle are [96] ns. And the whole encryption needs [9] clock cycles. That results in [1157407] whole encryptions per second.

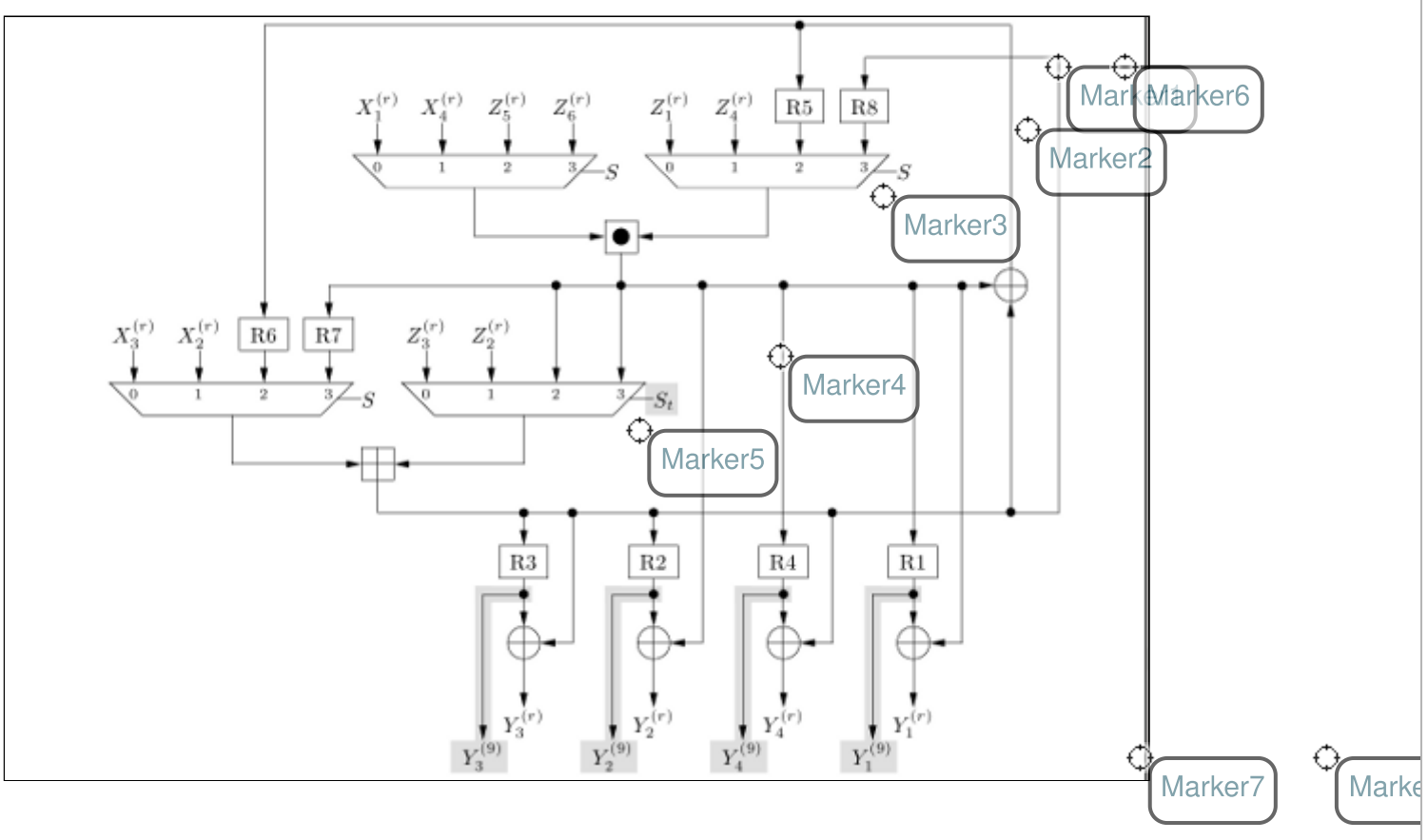
Frage 18

Antwort gespeichert

Erreichbare Punkte: 0,50

Find the shortest clock cycle for which the clocked round module works correctly. Consider that depending on the control signal there are four different paths through each multiplexer. Furthermore, a register is only the end of a combinational path if it also accepts the result of the current calculation. Show how the longest possible path (means the longest combinational active path between two consecutive registers) is created. Mark all the components of the longest path including the register at the start and the end in the correct order. (Marker1 should be put on the first register and the next component gets Marker2 and so on. The last marker should be again on a register) Please make sure the **circle of the marker** are directly put on the components.

Hint: You do not need to set all of the markers!



Frage 19

Antwort gespeichert

Erreichbare Punkte: 0,50

How many ns does one clock cycle take?

Antwort:

42

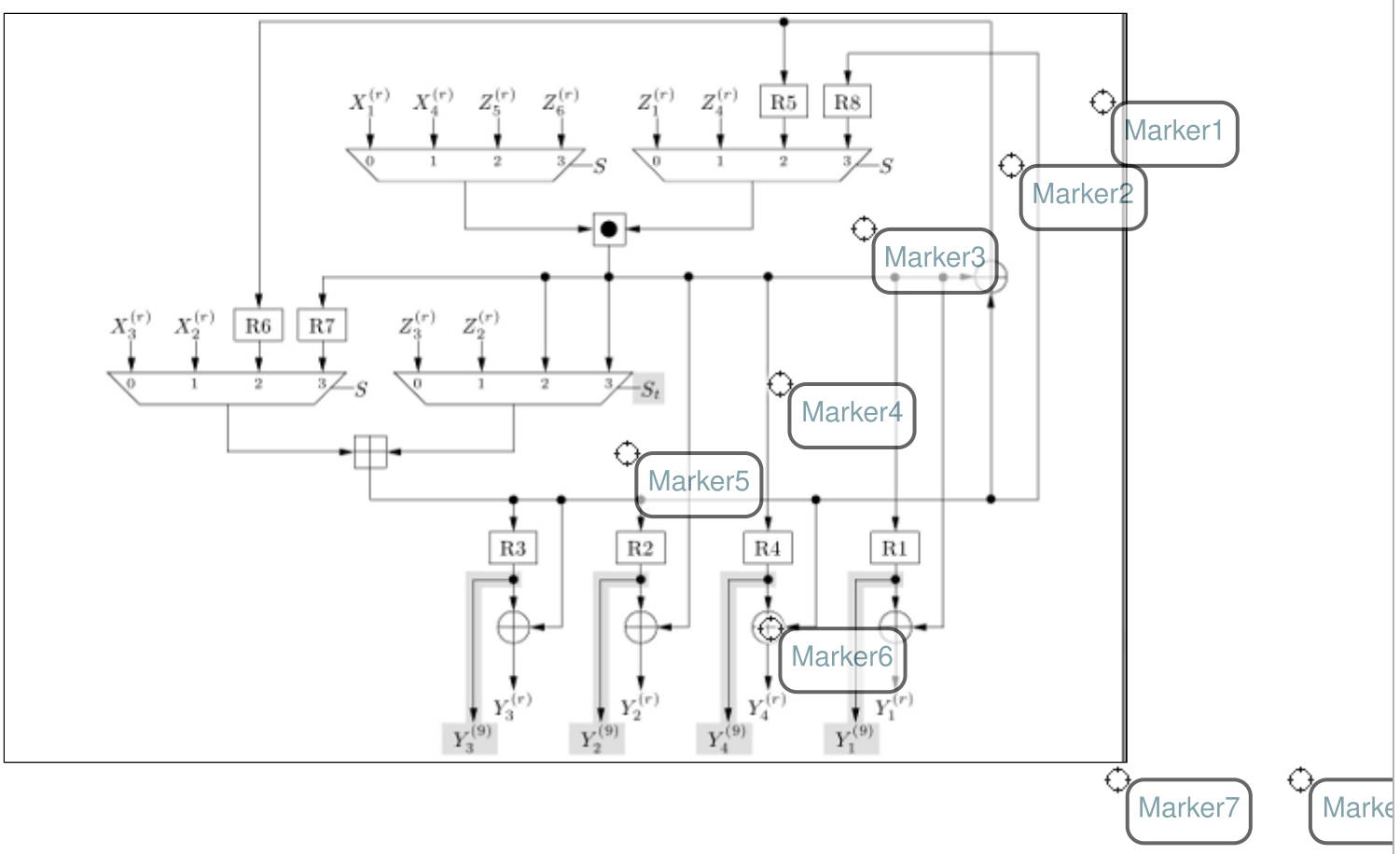
Frage 20

Antwort gespeichert

Erreichbare Punkte: 0,34

Find the shortest clock cycle inside the extended round module for which RCS 2 (extended round module, register R1 to R4, input multiplexer Si, round counter and key generator) still works correctly. Please note there is a different delay of a 4:1 and a 2:1 MUX! Trace the critical part inside the clocked round! Please make sure the **circle of the marker** are directly put on the components.

Hint: You do not need to set all of the markers!



Frage 21

Antwort gespeichert

Erreichbare Punkte: 0,33

Is the minimal clock cycle (whole IDEA algorithm) longer than the shortest cycle of the clocked round module? If yes, what causes the longer cycles?

Wählen Sie eine Antwort:

- No
- Yes, because of an additional delay of an XOR gate.
- Yes, because of an additional delay of an register.
- Yes, because of an additional delay of an MUX.

Frage 22

Antwort gespeichert

Erreichbare Punkte: 0,33

What is the shortest clock cycle in ns?

Antwort:

45

Frage 23

Antwort gespeichert

Erreichbare Punkte: 1,00

Find the number of clock cycles for an complete RCS2 encryption. Assume that the external start signal was active for the rising edge of the clock signal with the number 0, starting an encryption (see figure in the manual). At which rising clock edge are the signals *init* and *result* set? At which rising clock edge does *ready* indicate the completion of the encryption? Please note the section 5.3.2, 5.3.5 and 5.3.6.

The *init* signal is set at number 0 , 8 , 16 , 24 , 32 , 40 , 48 , 56 , 64 of the rising edge of the clock.

The *result* signal is set at number 7 , 15 , 23 , 31 , 39 , 47 , 55 , 63 , 69 of the rising edge of the clock.

The *ready* signal is set at number 70 of the rising edge of the clock.

Frage 24

Antwort gespeichert

Erreichbare Punkte: 1,00

How long does a complete encryption in RCS2 take? Please note that the whole encryption is considered as finished when the *ready* signal is recognized at a rising clock edge. Please calculate the number based on the shortest clock cycle from the previous questions. How many encryptions per second are possible?

One complete encryption takes 3195 ns and therefore 312989 whole encryptions per second are possible.

Frage 25

Antwort gespeichert

Erreichbare Punkte: 1,00

How many clock cyles are needed for a complete encryption in RCS2+? Please note that the whole encryption is considered as finished when the *ready* signal is recognized at a rising clock edge. How many encryptions per second are possible? Please calculate the number based on the shortest clock cycle from the previous questions.

The complete RCS2+ encryption needs 45 clock cycles and therefore 493827 whole encryptions per second are possible.

Frage 26

Antwort gespeichert

Erreichbare Punkte: 4,00

Complete the following two tables. Please calculate the required area in terms of used SLICEs and do **not use** the synthesis result. For calculating the required area calculate the number of required 16 bit components first and enter them in the first table. For simplification reasons the control module and the key generator module are disregarded. For the second table assume that one SLICE can just be used for the same gate type (i.e. if a XOR gate is implemented in the LUT, the MUX or register on that SLICE can not be used). Please note that in the direct implementation not all the Modulo Multiplier are mapped on a hardware multiplier.

For calculating the required input and output pins, please use the ports of the implemented IDEA Algorithm and not the physical ports of the board.

Number of Required 16 Bit Components

Implementation	1	2	3	4	5
XOR	48	48	6	5	5
Adder	34	34	6	1	1
Modulo Multiplier with Hardware Multiplier	20	20	6	1	1
Modulo Multiplier without Hardware Multiplier	14	14	0	0	0
16 Bit Register	0	32	4	12	12
MUX 2:1	0	0	4	4	4
MUX 4:1	0	0	0	4	4

Comparison of the Different Implementations

Implementation	1	2	3	4	5
Required area in SLICEs	894	1150	144	240	240
Required Input/Output PINs	192 / 64	193 / 64	194 / 65	194 / 65	194 / 65

◄ File templates for Code Submission

Direkt zu:

VHDL Introduction ►