Projeto de um IP Soft Core para Detecção de Ataques DDoS

Aluno: Pedro Lucas Falcão Lima
Orientador: Ricardo Jardel Nunes da Silveira

Motivação

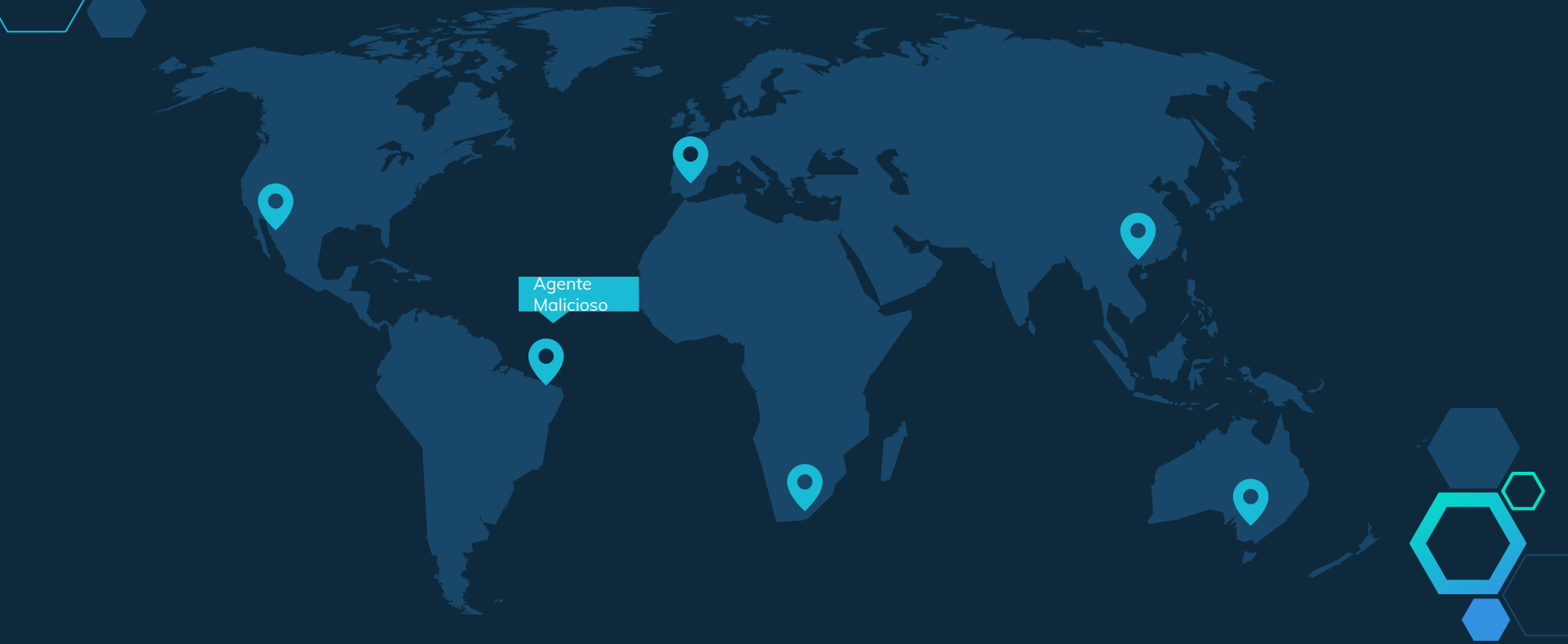
- Internet
- Ataques
- Ataques DoS
- Ataques DDoS
- Detecção
- Análise de dados
- Solução em hardware
- FPGA's

Módulo

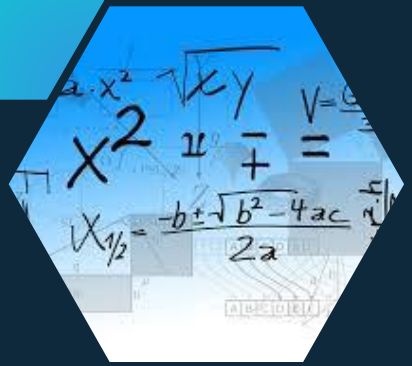
Objetivos

- Realizar detecção em tempo real.
- Módulo em hardware com maior desempenho em relação a softwares e trabalhos similares.
- Desenvolvimento utilizando métodos otimizados, agregando agilidade e confiabilidade.

Ataques DDoS

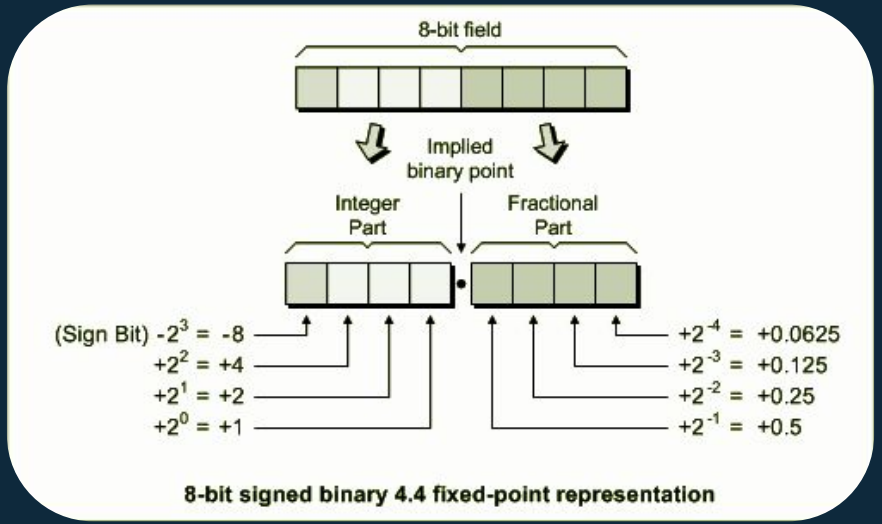


Porque utilizar um sistema embarcado?

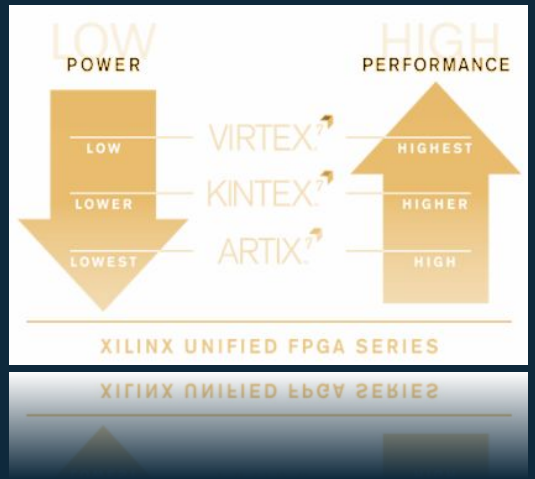


Técnicas Utilizadas nas operações aritméticas

-Operações comuns
- Média Aritmética
- Utilização de IP cores
- Aritmética de ponto fixo



FPGAs



FPGAs oferecem adaptabilidade dinâmica, que é importante para aplicações que requerem

mudanças frequentes em suas configurações, como a detecção de ataques DDoS que evoluem

com freqüência.

Em poucas palavras, é necessário a construção de um módulo em hardware que realize os métodos estatísticos, especificamente a correlação.

Cálculos de correlação

$(X[3], Y[3]) = Vectors\ to\ be\ measured$

$TH = Threshold$

1. $M_X = \frac{X_1 + X_2 + X_3}{3}, \quad M_Y = \frac{Y_1 + Y_2 + Y_3}{3}$
2. $(M_X)^2 = M_X \times M_X, \quad (M_Y)^2 = M_Y \times M_Y$
3. $M_{X^2} = \frac{X_1^2 + X_2^2 + X_3^2}{3}, \quad M_{Y^2} = \frac{Y_1^2 + Y_2^2 + Y_3^2}{3}$
4. $SD_X = \sqrt{|M_{X^2} - (M_X)^2|}, SD_Y = \sqrt{|M_{Y^2} - (M_Y)^2|}$
5. $N_1 = |X_1 - Y_1|, \quad N_2 = |X_2 - Y_2|, \quad N_3 = |X_3 - Y_3|$
6. $D_1 = ||M_X - SD_X| - X_1| + ||M_Y - SD_Y| - Y_1|,$
   $D_2 = ||M_X - SD_X| - X_2| + ||M_Y - SD_Y| - Y_2|,$
   $D_3 = ||M_X - SD_X| - X_3| + ||M_Y - SD_Y| - Y_3|$
7. $NaHiD_{VERC}(X,Y) = |1 - \frac{\frac{N_1}{D_1} + \frac{N_2}{D_2} + \frac{N_3}{D_3}}{3}|$
8. $A \Leftrightarrow TH > NaHiD_{VERC}(X,Y)$

$ax_1 = X_1 + X_2, \quad ay_1 = Y_1 + Y_2, \quad M_X = \frac{ax_1 + X_3}{4}$

$M_Y = \frac{ay_1 + Y_3}{4}, \quad mx_1 = X_1^2, \quad mx_2 = X_2^2$

$mx_3 = X_3^2, \quad my_1 = Y_1^2, \quad my_2 = Y_2^2, \quad my_3 = Y_3^2$

$(M_X)^2 = M_X \times M_X, \quad (M_Y)^2 = M_Y \times M_Y$

$amx_1 = mx_1 + mx_2, \quad amy_1 = my_1 + my_2$

$M_{X^2} = \frac{amx_1 + mx_3}{4}, \quad M_{Y^2} = \frac{amy_1 + my_3}{4}$

$V_X = |M_{X^2} - (M_X)^2|, \quad V_Y = |M_{Y^2} - (M_Y)^2|$

$SD_X = \sqrt{V_X}, \quad SD_Y = \sqrt{V_Y}$

$MSD_X = |M_X - SD_X|, \quad MSD_Y = |M_Y - SD_Y|$

$DX_1 = |MSD_X - X_1|, \quad DY_1 = |MSD_Y - Y_1|$

$DX_2 = |MSD_X - X_2|, \quad DY_2 = |MSD_Y - Y_2|$

$DX_3 = |MSD_X - X_3|, \quad DY_3 = |MSD_Y - Y_3|$

$D_1 = DX_1 + DY_1, D_2 = DX_2 + DY_2, D_3 = DX_3 + DY_3$

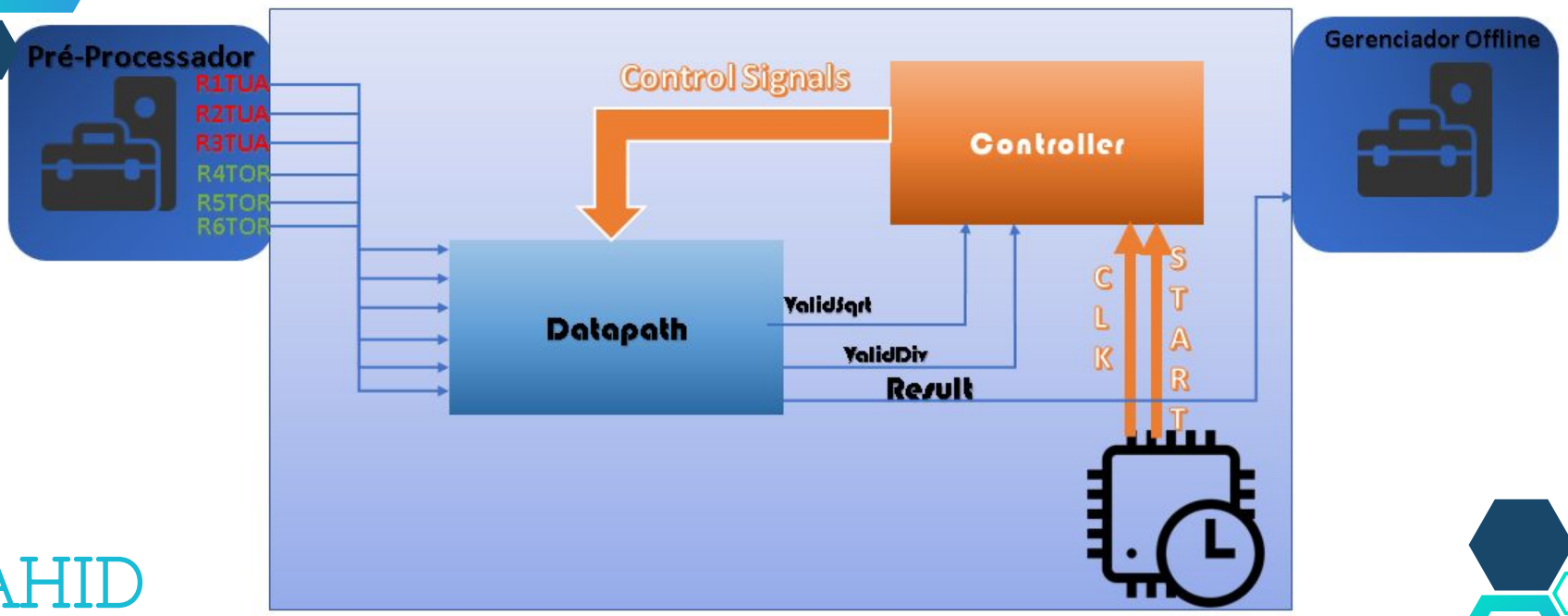
$N_1 = |X_1 - Y_1|, \quad N_2 = |X_2 - Y_2|, \quad N_3 = |X_3 - Y_3|$

$Q_1 = \frac{N_1}{D_1}, \quad Q_2 = \frac{N_2}{D_2}, \quad Q_3 = \frac{N_3}{D_3}$

$aQ_1 = Q_1 + Q_2, \quad aQ_2 = \frac{aQ_1 + Q_3}{4}$

$NaHiD_{VERC} = |1 - aQ_2|, \quad aT = NaHiD_{VERC} - TH$

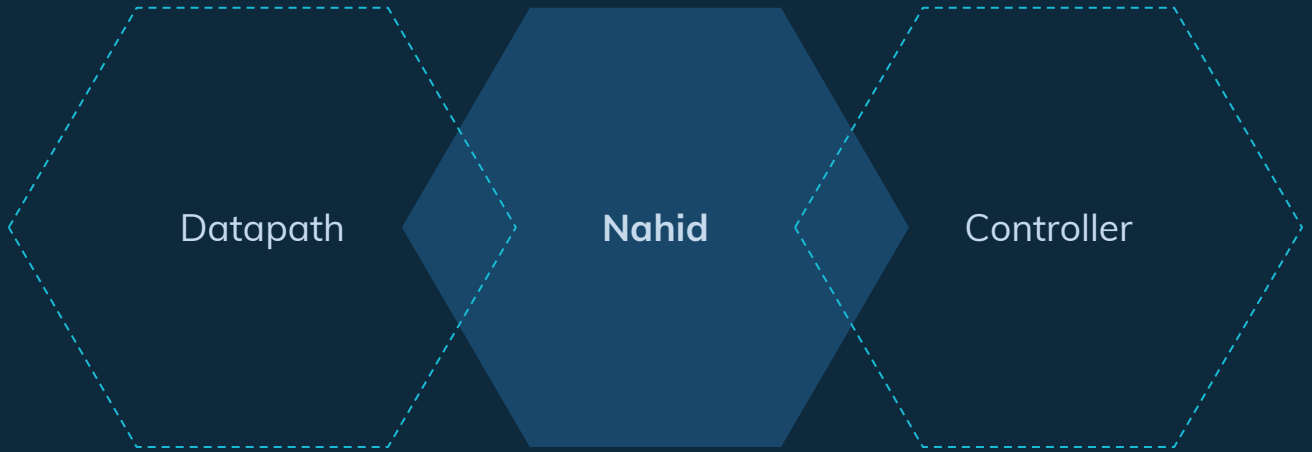
Nahid



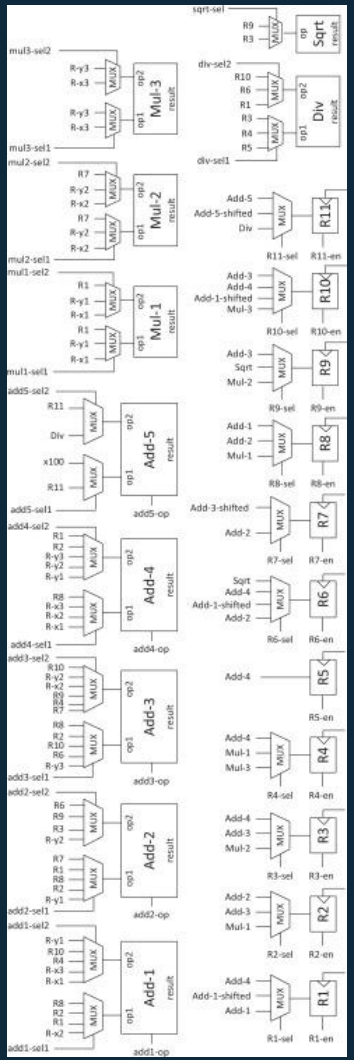
NAHID

"Módulo de mais alto nível"

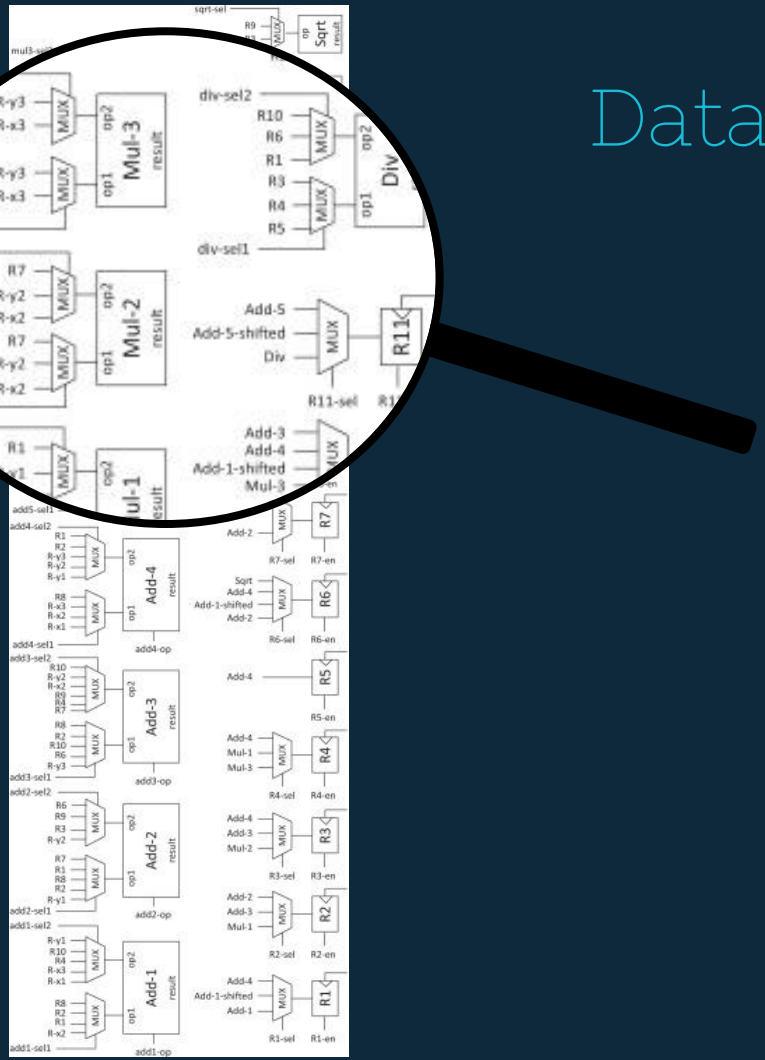
Relação entre componentes e módulo



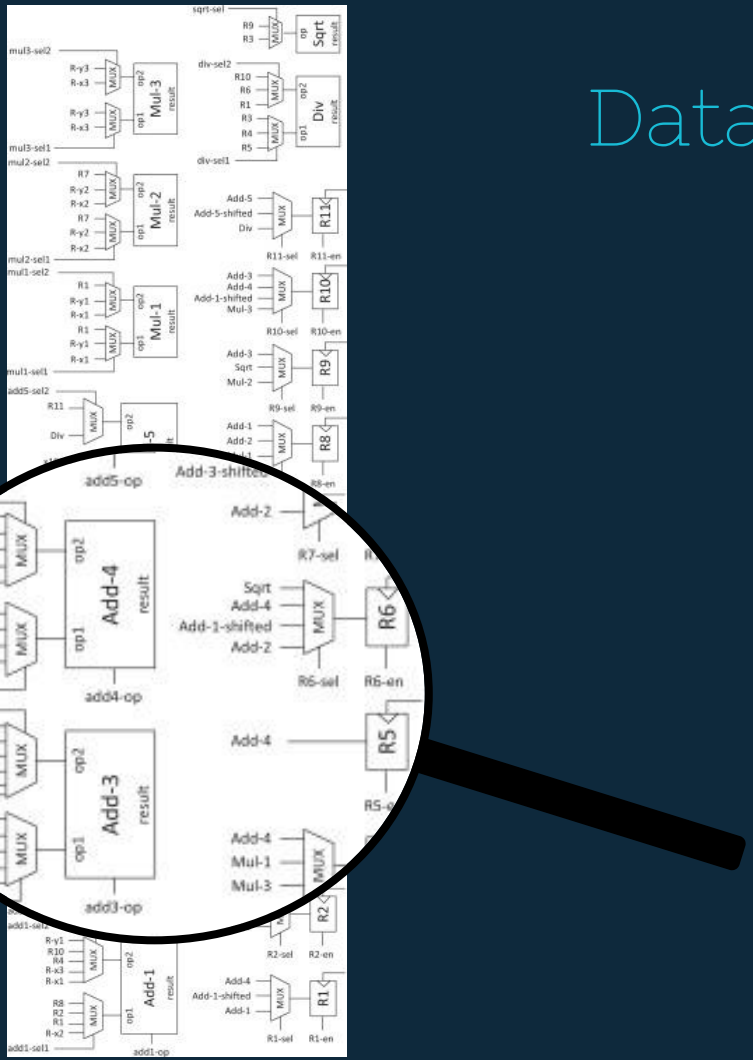
Datapath


sqrt-sel
R9
R3
MUX
op
Sqrt
result
mul3-sel2
R-y3
R-x3
MUX
op2
Mul-3
result
op1
mul3-sel1
div-sel2
R10
R6
R1
R3
R4
R5
op2
Div
result
op1
div-sel1
mul2-sel2
R7
R-y2
R-x2
Mul-2
mul2-sel1
Add-5
Add-5-shifted
Div
R11
R11-sel
R11-en
mul1-sel2
R1
R-y1
R-x1
Mul-1
mul1-sel1
Add-3
Add-4
Add-1-shifted
Mul-3
R10
R10-sel
R10-en
add5-sel2
R11
Div
x100
Add-5
add5-op
add5-sel1
Add-3
Sqrt
Mul-2
R9
R9-sel
R9-en
add4-sel2
R-y3
R-y2
R-y1
R8
R-x3
R-x2
R-x1
Add-4
add4-op
add4-sel1
Add-1
Add-2
Mul-1
R8
R8-sel
R8-en
add3-sel2
R10
R-y2
R-x2
R5
R4
R2
R-y3
Add-3
add3-op
add3-sel1
Add-3-shifted
Add-2
R7
R7-sel
R7-en
add2-sel2
R6
R9
R3
R-y2
R2
R1
R8
Add-2
add2-op
add2-sel1
Sqrt
Add-4
Add-1-shifted
Add-2
R6
R6-sel
R6-en
add1-sel2
R-y1
R10
R4
R-x3
R-x1
Add-1
add1-op
add1-sel1
Add-4
Mul-1
Mul-3
R4-sel
R4-en
Add-4
R5-en
Add-4
Add-3
Mul-2
R3-sel
R3-en
Add-2
Add-3
Mul-1
R2-sel
R2-en
Add-4
Add-1-shifted
Add-1
R1-sel
R1-en

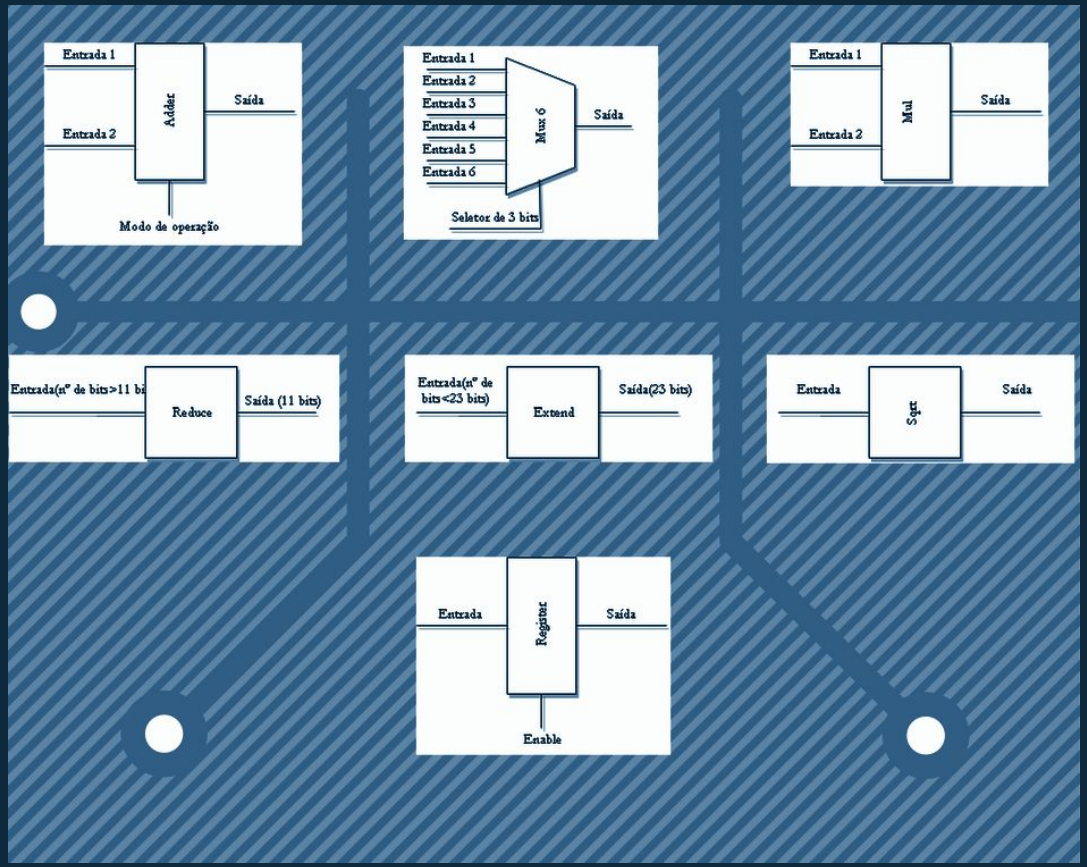
Datapath


sqrt-sel
Sqrt
div-sel2
R10
R6
R1
R3
R4
R5
Div
div-sel1
mul3-sel1
mul2-sel2
R-y3
R-x3
Mul-3
R7
R-y2
R-x2
Mul-2
Add-5
Add-5-shifted
Div
R11
R11-sel
Add-3
Add-4
Add-1-shifted
Mul-3
Mul-1
add5-sel1
add4-sel2
Add-4
add4-op
add4-sel1
add3-sel2
Add-3
add3-op
add3-sel1
add2-sel2
Add-2
add2-op
add2-sel1
add1-sel2
Add-1
add1-op
add1-sel1
Add-2
R7-sel
R7-en
Sqrt
Add-4
Add-1-shifted
Add-2
R6-sel
R6-en
R5-en
Mul-1
Mul-3
R4-sel
R4-en
Add-3
Mul-2
R3-sel
R3-en
R2-sel
R2-en
Add-1
Add-1-shifted
R1-sel
R1-en
MUX
op1
op2
result

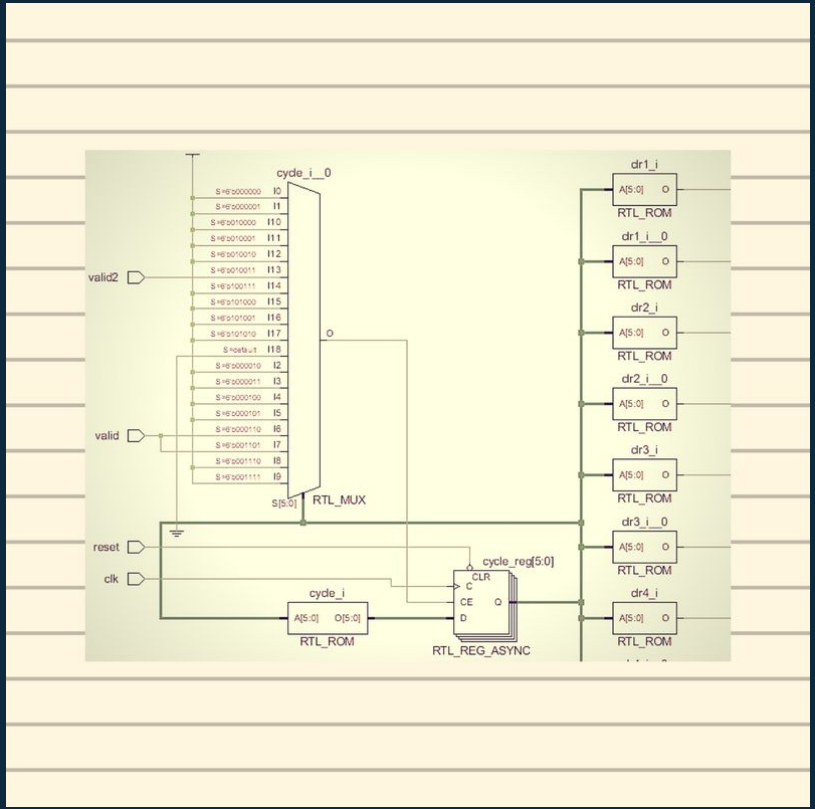
Datapath


Add-4
Add-3
add4-op
add3-op
add4-sel1
add3-sel2
R6
R5
R6-sel
R6-en
R5-en
Sqrt
Add-4
Add-1-shifted
Add-2
Mul-1
Mul-3

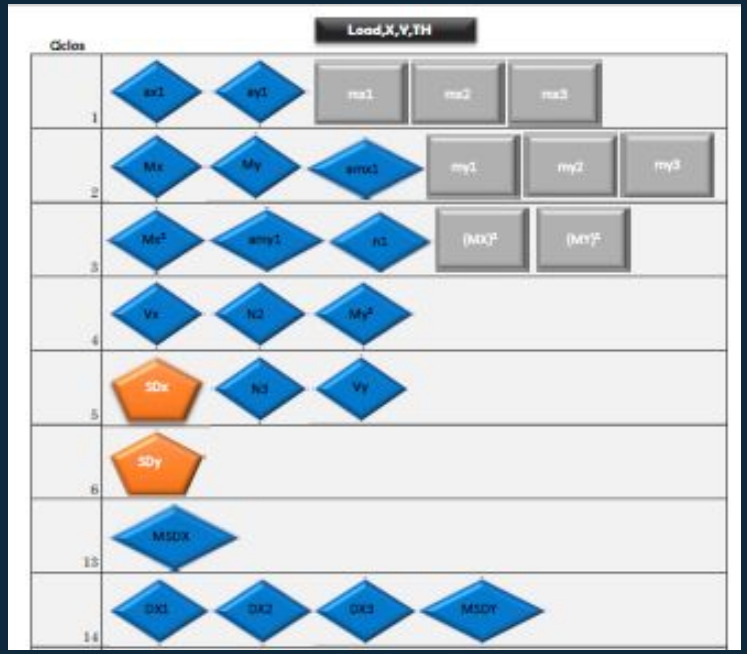
Datapath

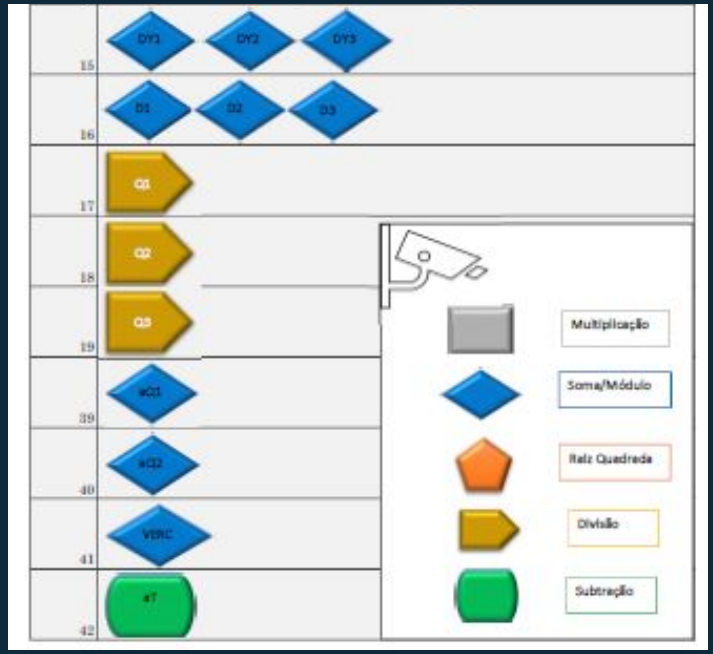

Entrada 1
Entrada 2
Adder
Saída
Modo de operação
Entrada 1
Entrada 2
Entrada 3
Entrada 4
Entrada 5
Entrada 6
Mux 6
Saída
Seletor de 3 bits
Entrada 1
Entrada 2
Mul
Saída
Entrada(nº de bits>11 bi
Reduce
Saída (11 bits)
Entrada(nº de bits<23 bits)
Extend
Saída(23 bits)
Entrada
Sqrt
Saída
Entrada
Register
Saída
Enable

Controller


cycle_i__0
valid2
valid
reset
clk
O
S[5:0]
RTL_MUX
cycle_i
A[5:0]
O[5:0]
RTL_ROM
cycle_reg[5:0]
CLR
C
CE
D
Q
RTL_REG_ASYNC
dr1_i
dr1_i__0
dr2_i
dr2_i__0
dr3_i
dr3_i__0
dr4_i
A[5:0]
O
RTL_ROM

Controller


Lead,X,Y,TH
Ciclos
1
2
3
4
5
6
13
14
ax1
ay1
mx1
mx2
mx3
Mx
My
amx1
my1
my2
my3
Mx²
amy1
n1
(MX)²
(MY)²
Vx
N2
My²
SDx
N3
Vy
SDy
MSDX
DX1
DX2
DX3
MSDY


15
16
17
18
19
39
40
41
42
DY1
DY2
DY3
D1
D2
D3
Q1
Q2
Q3
aQ1
aQ2
VERC
47
Multiplicação
Soma/Módulo
Raiz Quadrada
Divisão
Subtração

Relatório de Utilização

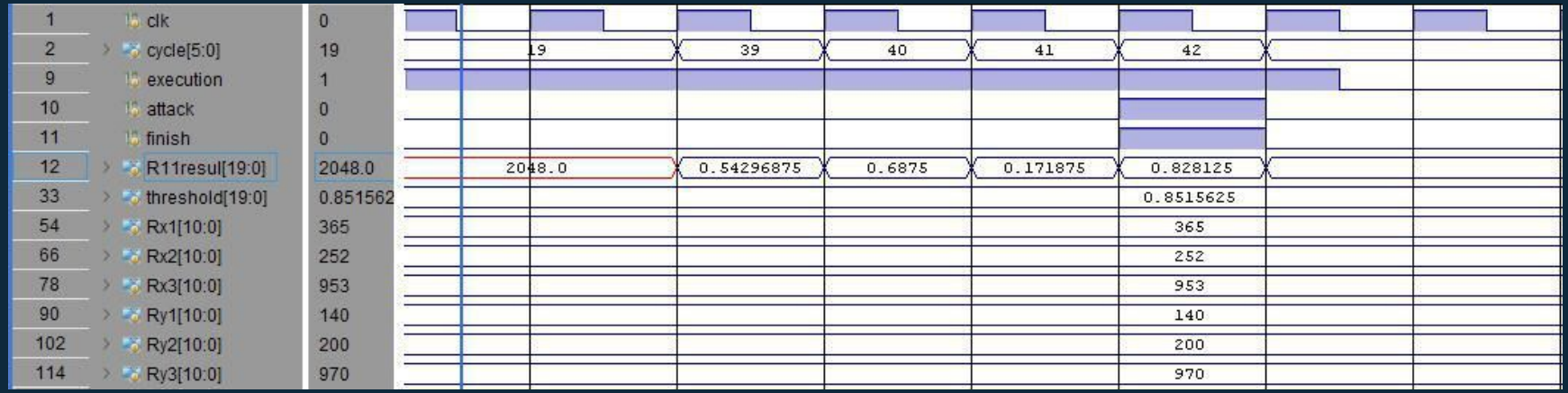
Tipo	Usado	Disponível	Utilização(%)
CLB LUTs*	1905/1302	28800/216960	0.6/¨0.6
LUT as Logic	1891/1301	28800/216960	0.6/¨0.6
LUT as Memory	14/1	7860/99840	0.01/<0.01
Lut as Shifter Register		14/1	
CLB Registers	1131/1180	28800/433920	0.3/0.27
Register as Flip Flop	1255/1122	2386/433920	52/0.26
Frequency(MHZ)		118/120	

Análise de detecção

Detecção	Matlab	Módulo	Erro(%)
1-(P1=365,P2=252,P3=953,D1=140,D2=200,D3=970)	0,82493	0,95585	1
2-(P1=128,P2=515,P3=852,D1=130,D2=470,D3=970)	0,96874	0,96625	1.02
3-(P1=150,P2=300,P3=853,D1=123,D2=340,D3=876)	14/1	0,95468	0.9

Detector	Artigo de Comparação	Trabalho Proposto	Software(Matlab)
Tempo de Detecção	354 ns	350 ns	296 µs

Simulação


1 clk 0
2 cycle[5:0] 19
9 execution 1
10 attack 0
11 finish 0
12 R11resul[19:0] 2048.0
33 threshold[19:0] 0.851562
54 Rx1[10:0] 365
66 Rx2[10:0] 252
78 Rx3[10:0] 953
90 Ry1[10:0] 140
102 Ry2[10:0] 200
114 Ry3[10:0] 970
19
39
40
41
42
2048.0
0.54296875
0.6875
0.171875
0.828125
0.8515625
365
252
953
140
200
970

Ganhos em tempo de execução e de utilização de recursos.

Precisão considerável nos resultados de correlação

Utilização de uma FPGA mais recente e de baixo custo

Resultados melhores ou similares

Utilização de componentes, da IDE Vivado da Xilinx

Agilidade no desenvolvimento e confiabilidade

Trabalhos Futuros

A implementação de um sistema completo de verificação funcional do módulo implementado, bem como a realização de testes do mesmo em uma FPGA inserida em um ambiente de rede real, submetido um ataque DDoS intencional.

Bibliografia

- HOQUE, N. et al. Real-time DDoS Attack Detection Using FPGA. Computer Communications, v. 110, n. Supplement C, p. 48 – 58, 2017. ISSN 0140-3664. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0140366416306442>.
- YU, S. et al. Discriminating ddos attacks from flash crowds using flow correlation coefficient. IEEE Transactions on Parallel and Distributed Systems, IEEE, v. 23, n. 6, p. 1073–1080, 2012.
- HEATH, S. Embedded systems design. [S.l.]: Newnes, 2002.
- ALECRIM, E. Ataques DoS (Denial of Service) e DDoS (Distributed DoS). [S.l.]: Disponível na Internet em< http://www. infowester. com/col120904. php> em, 2008.

Obrigado

Alguma pergunta?

Você pode me achar em:

- pedrolfalc@gmail.com
- 999084309