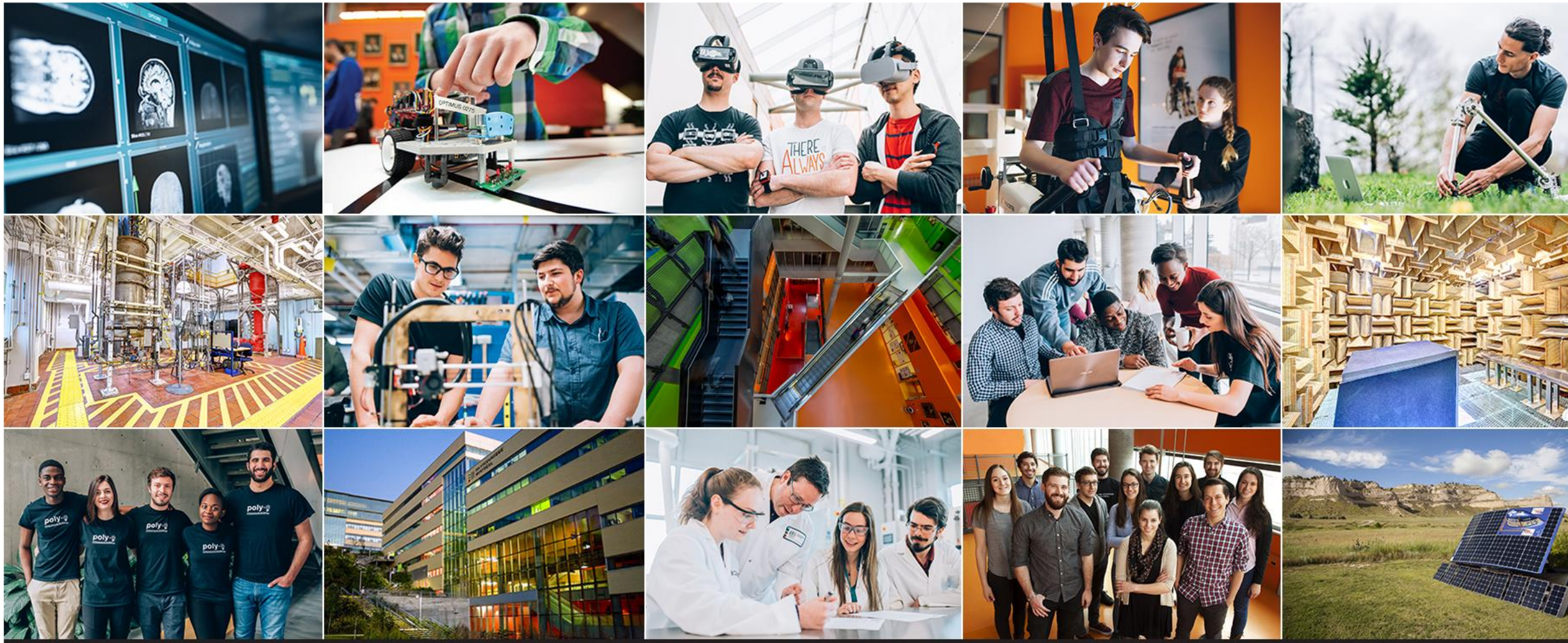


POLYTECHNIQUE MONTRÉAL

TECHNOLOGICAL UNIVERSITY

IP Core Identification in FPGA Configuration Files using Machine Learning Techniques

Mahmood et al.

Presented by John Doe

March 26, 2024

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

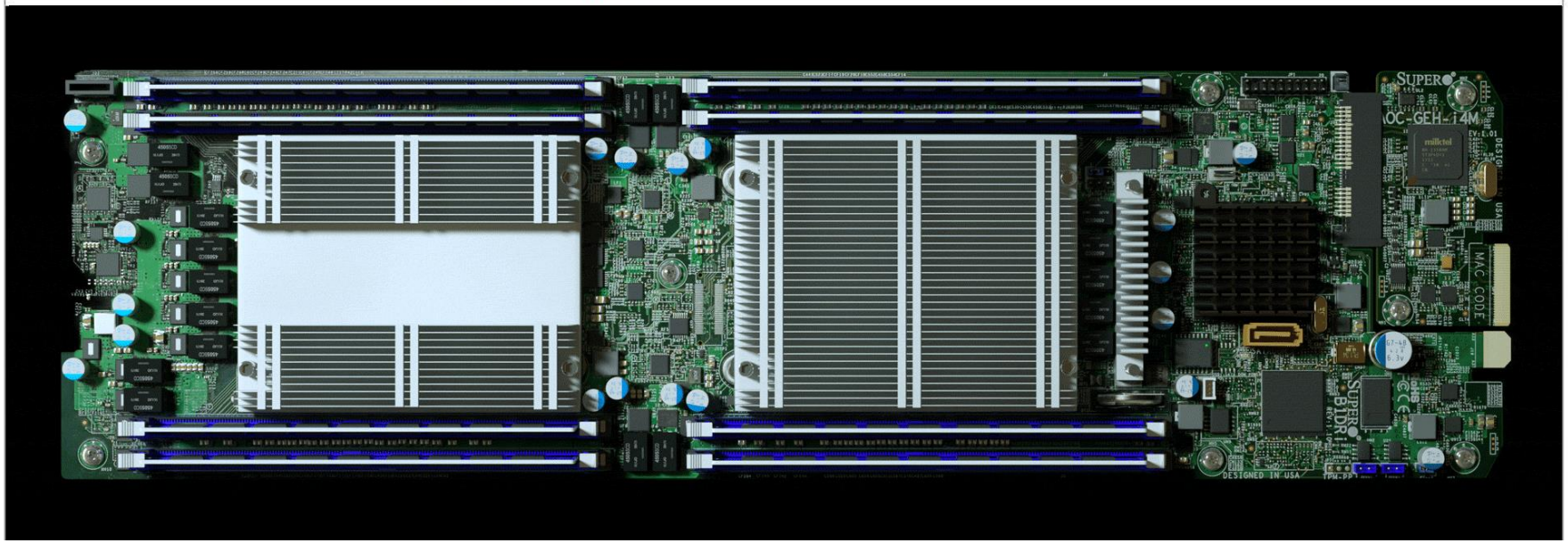
Bloomberg

Live TV | Markets | Economics | Industries | Tech | Politics | Businessweek | Opinion | More | US Edition

Businessweek | Feature

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.



https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

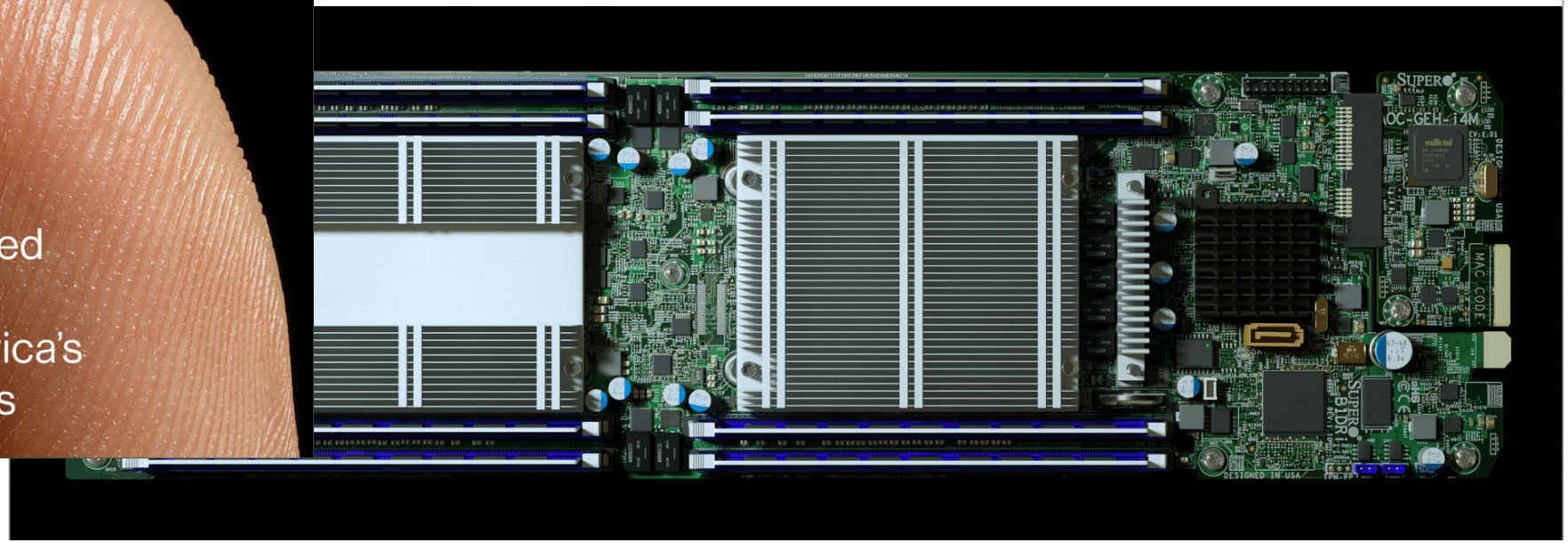
Bloomberg

Live TV | Markets | Economics | Industries | Tech | Politics | Businessweek | Opinion | More | US Edition

Businessweek | Feature

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

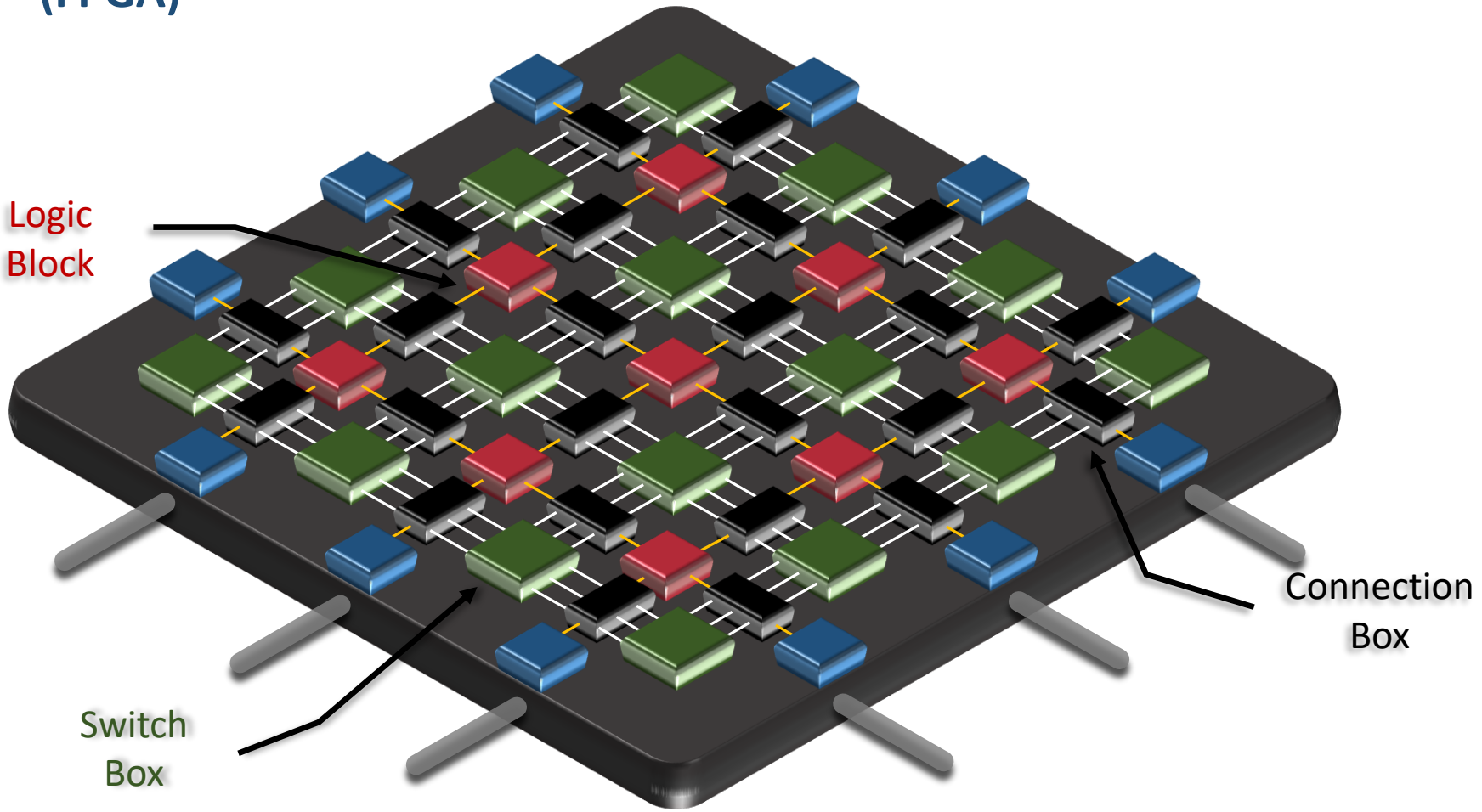


https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

What are FPGAs and Why Should I be Interested?

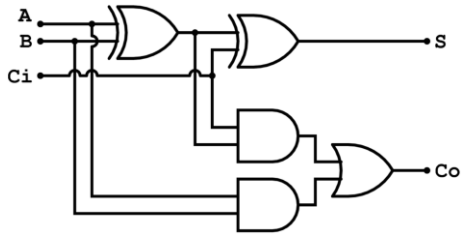
Field-Programmable Gate Array (FPGA)

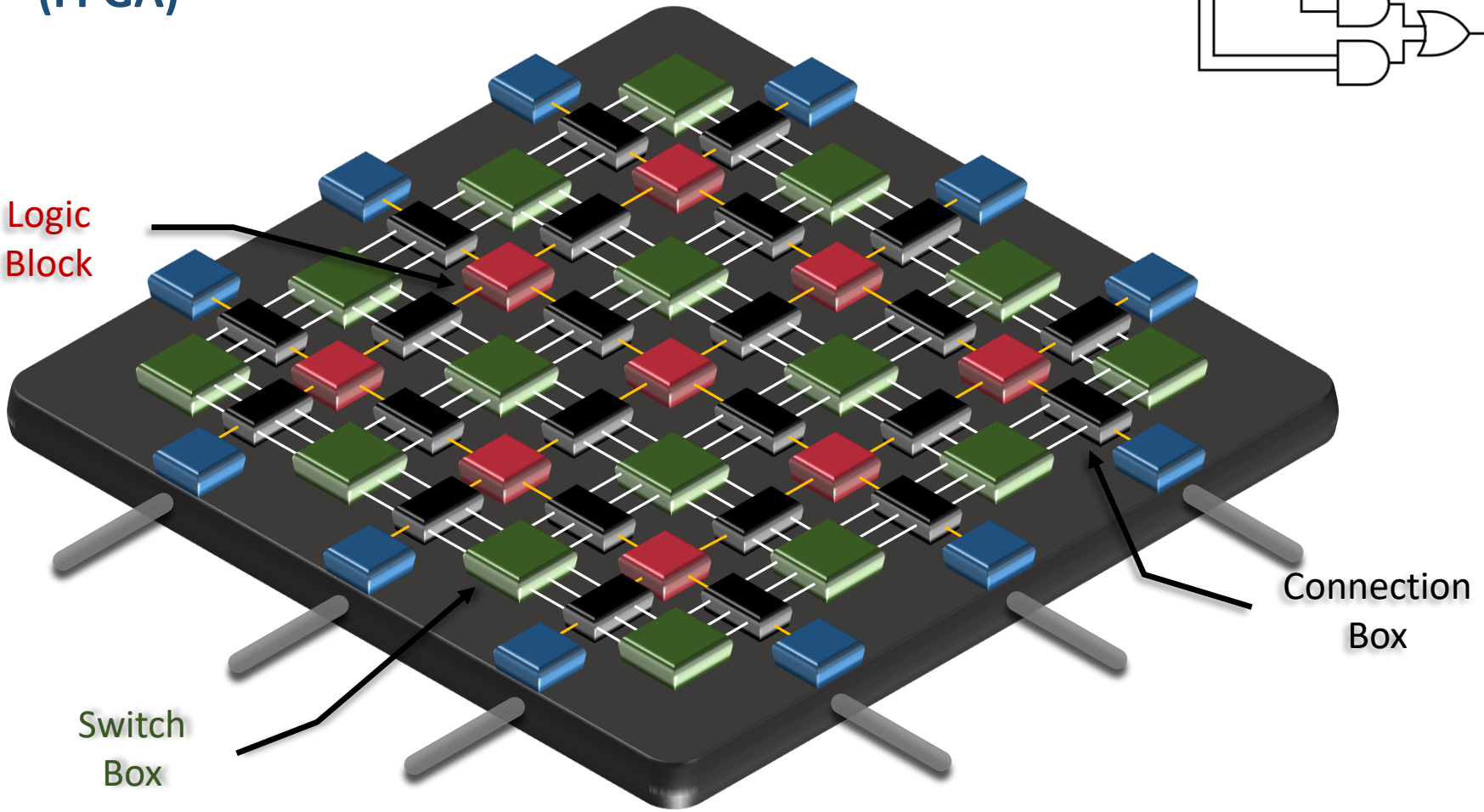


POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

What are FPGAs and Why Should I be Interested?

Field-Programmable Gate Array (FPGA)

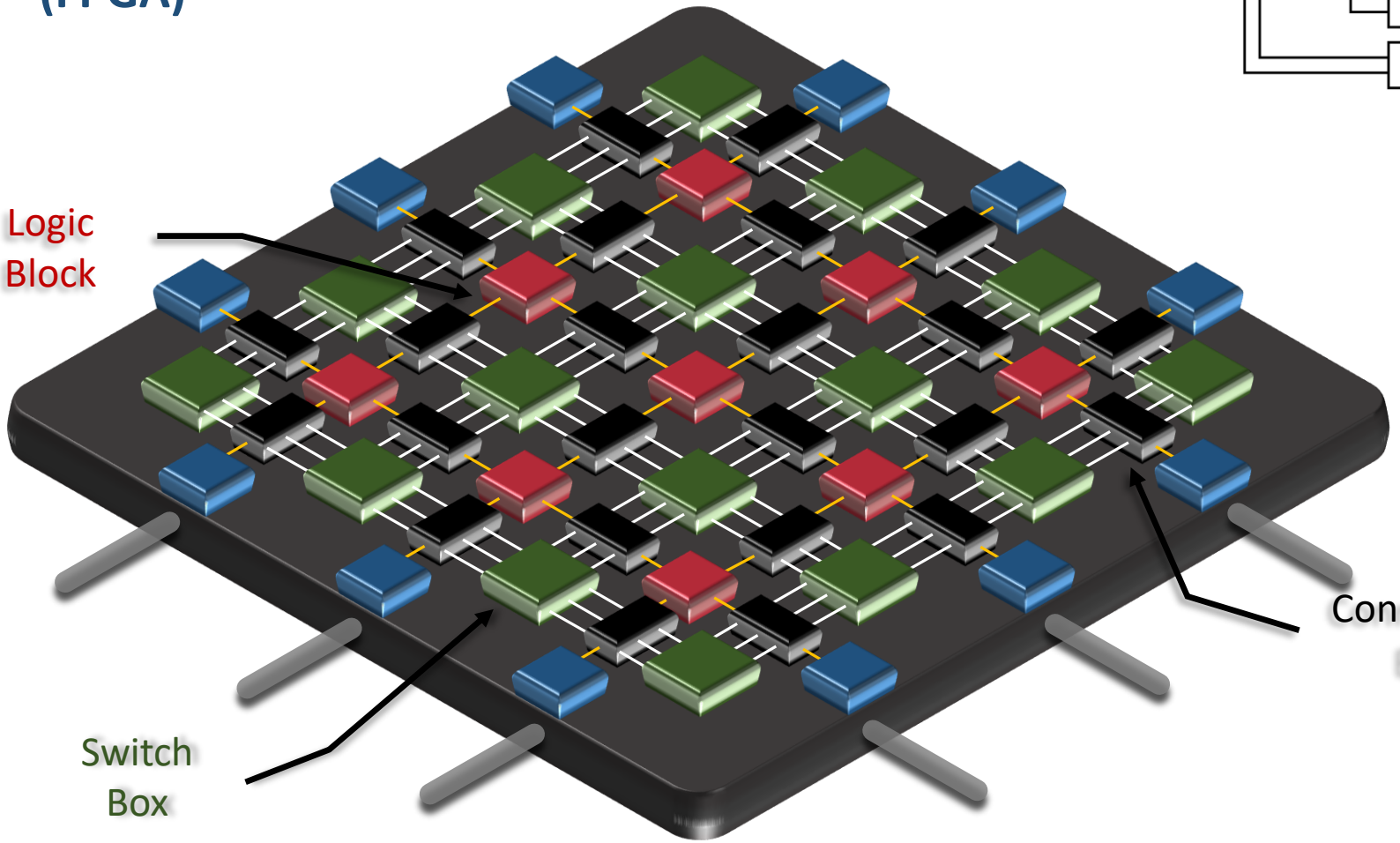


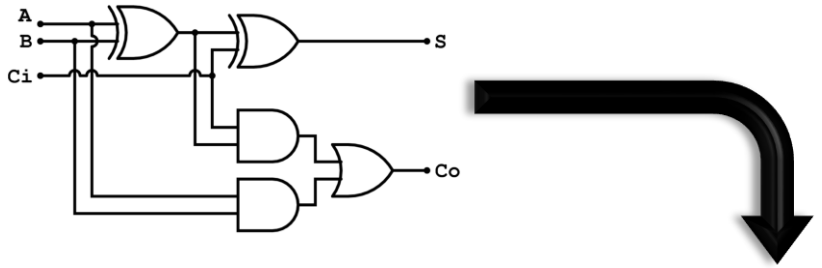


POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

What are FPGAs and Why Should I be Interested?

Field-Programmable Gate Array (FPGA)



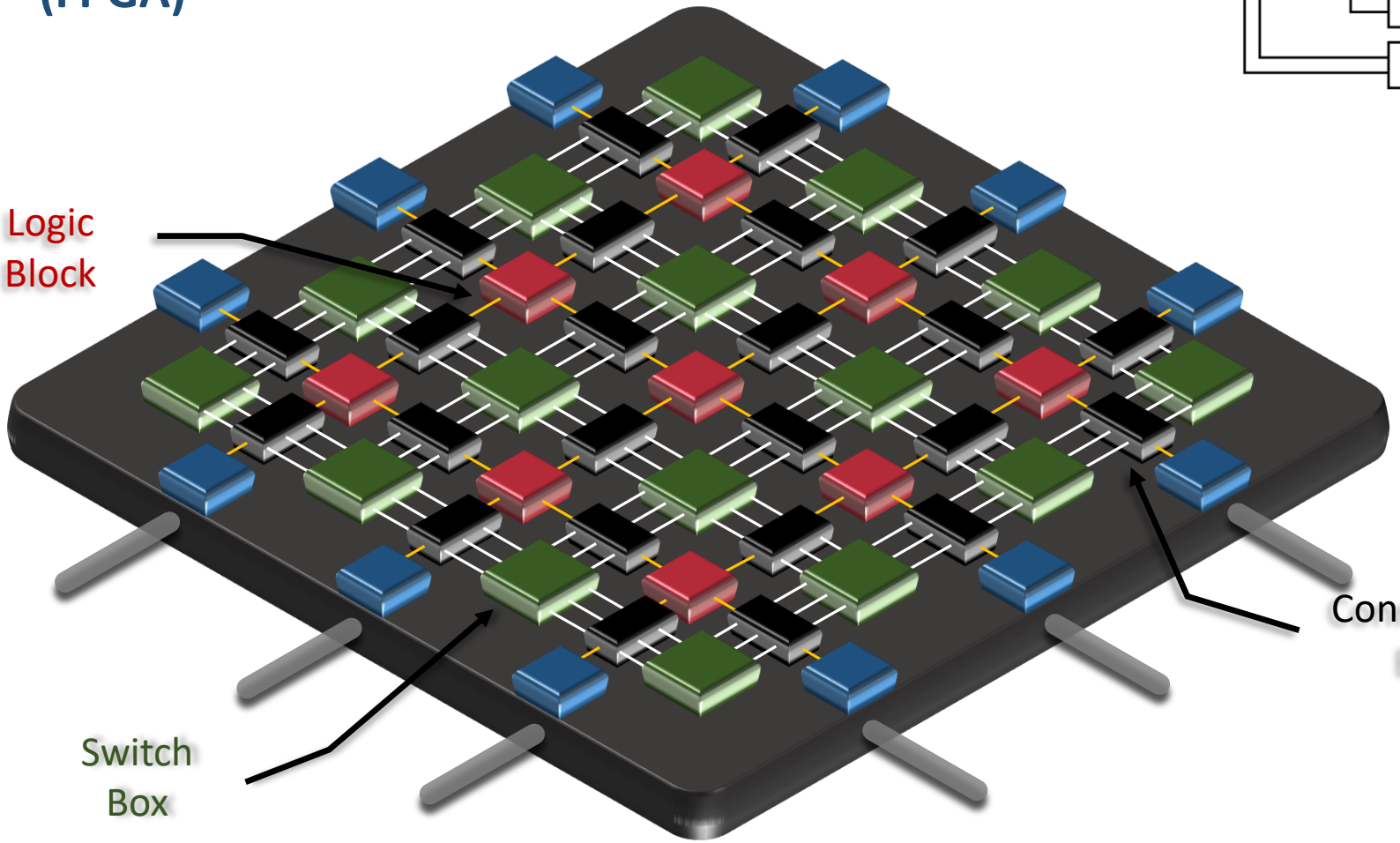


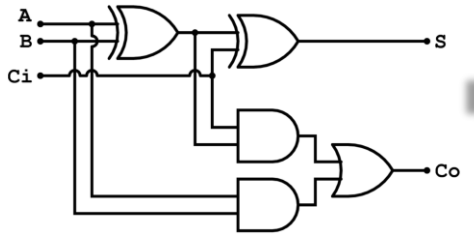

```
`timescale 1ns / 1ps module
full_adder( A, B, Cin, S, Cout);

 input wire A, B, Cin;
 output reg S, Cout;

 always @(A or B or Cin)
  begin
   S = A ^ B ^ Cin;
   Cout = A&B | (A^B) & Cin;
  end
endmodule
```

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

What are FPGAs and Why Should I be Interested?

Field-Programmable Gate Array (FPGA)

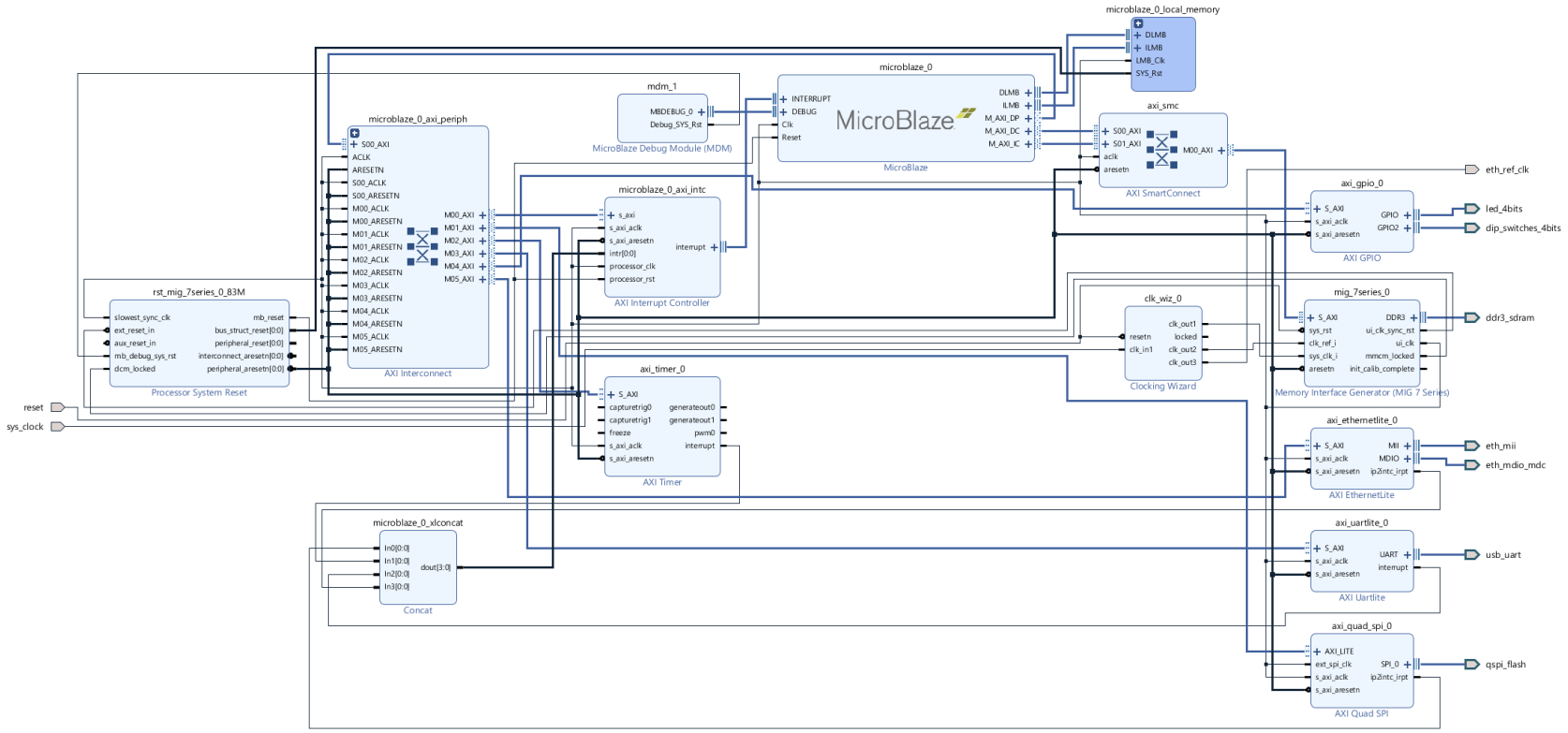





```
`timescale 1ns / 1ps module
full_adder( A, B, Cin, S, Cout);

 input wire A, B, Cin;
 output reg S, Cout;

 always @(A or B or Cin)
  begin
   S = A ^ B ^ Cin;
   Cout = A&B | (A^B) & Cin;
  end
endmodule
```

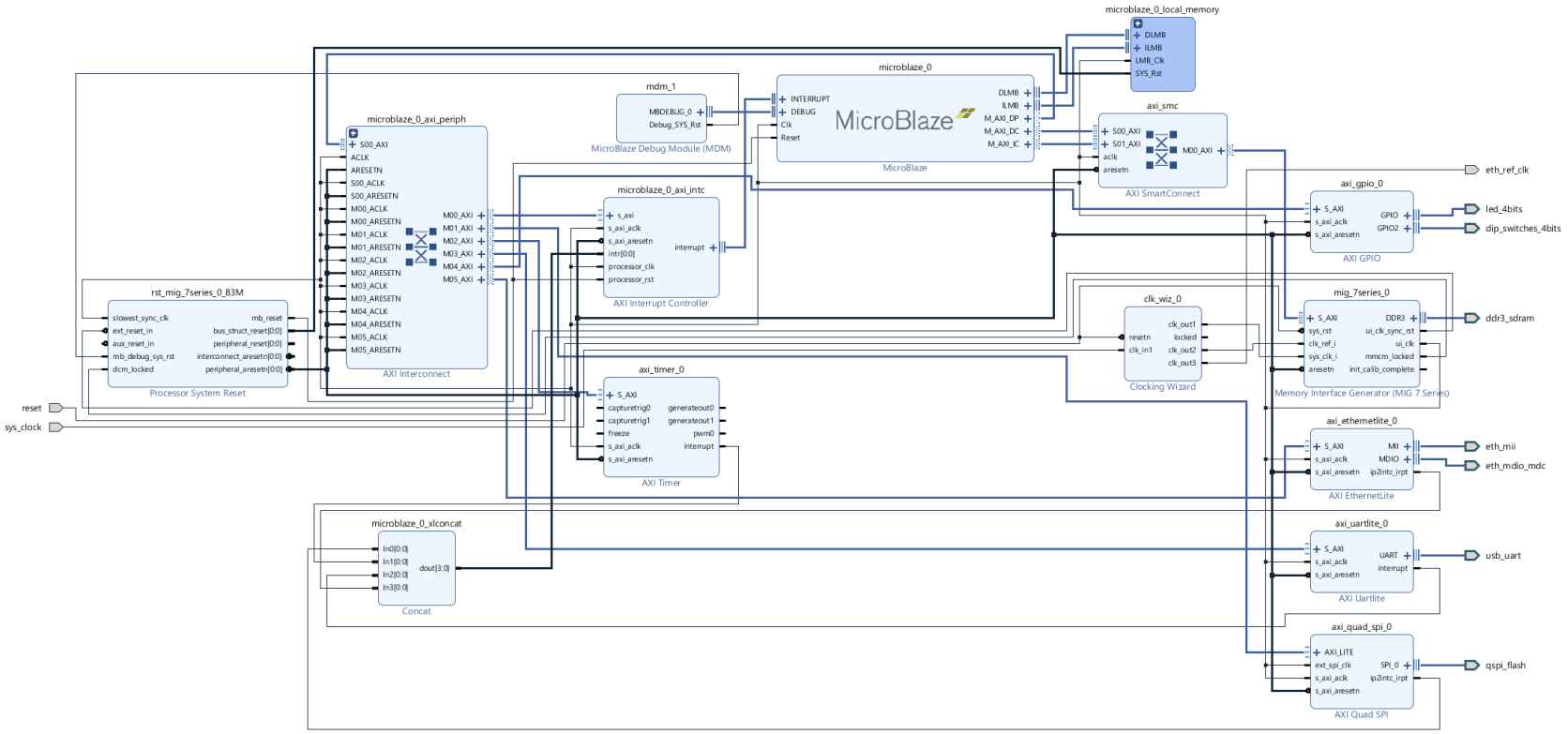
POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

What are FPGAs and Why Should I be Interested?

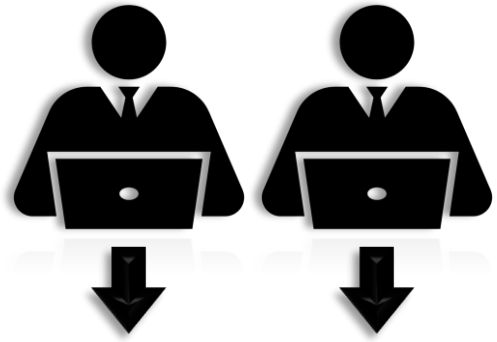


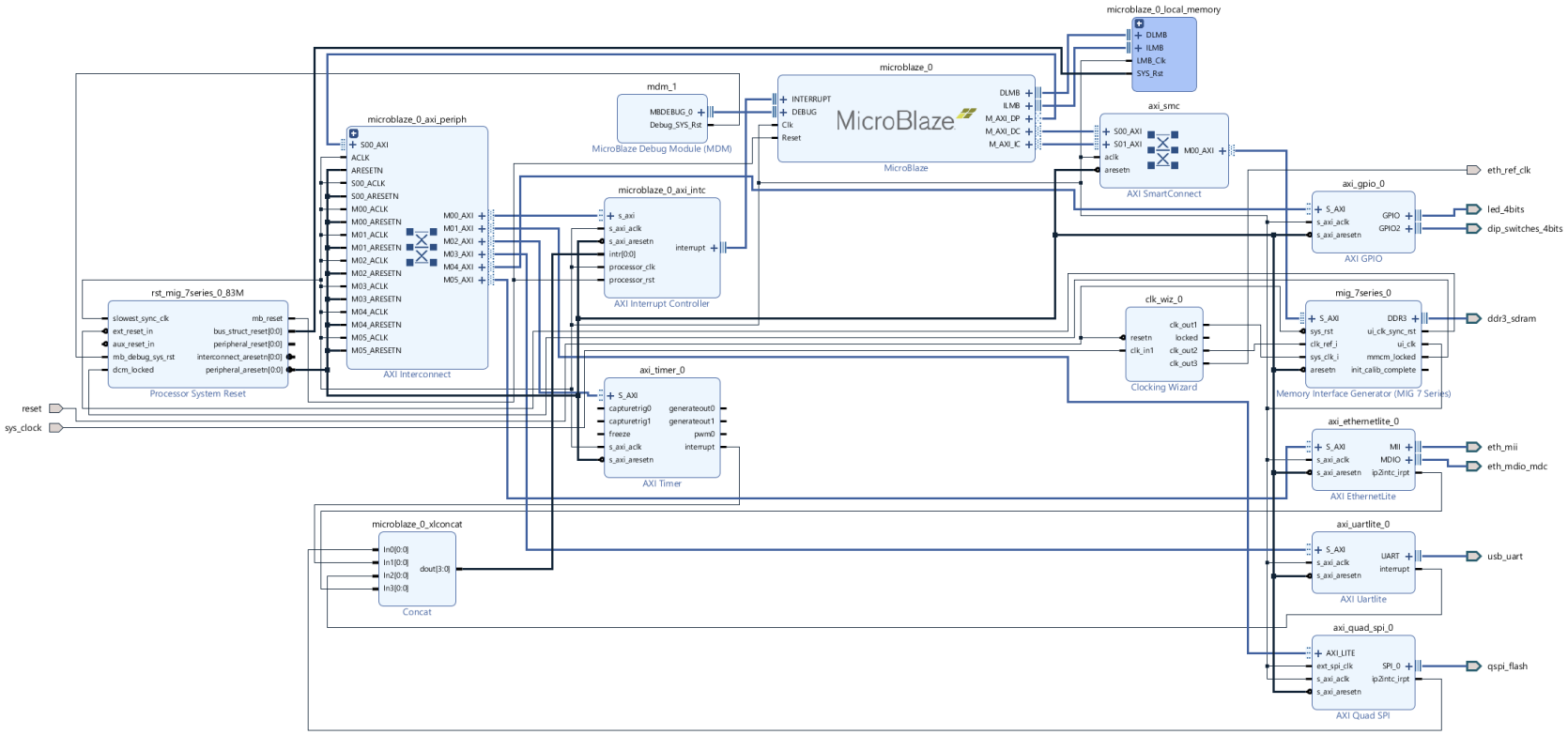
POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

What are FPGAs and Why Should I be Interested?



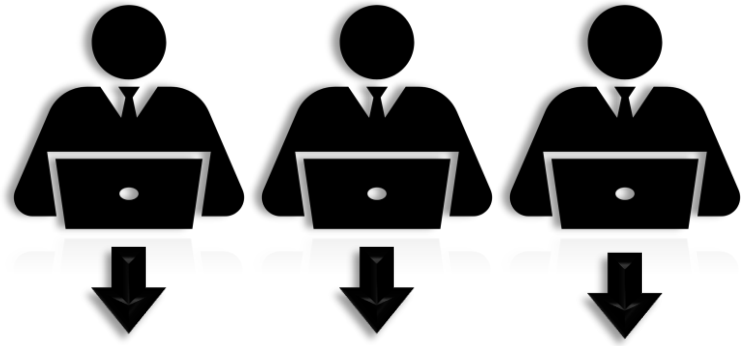
What are FPGAs and Why Should I be Interested?

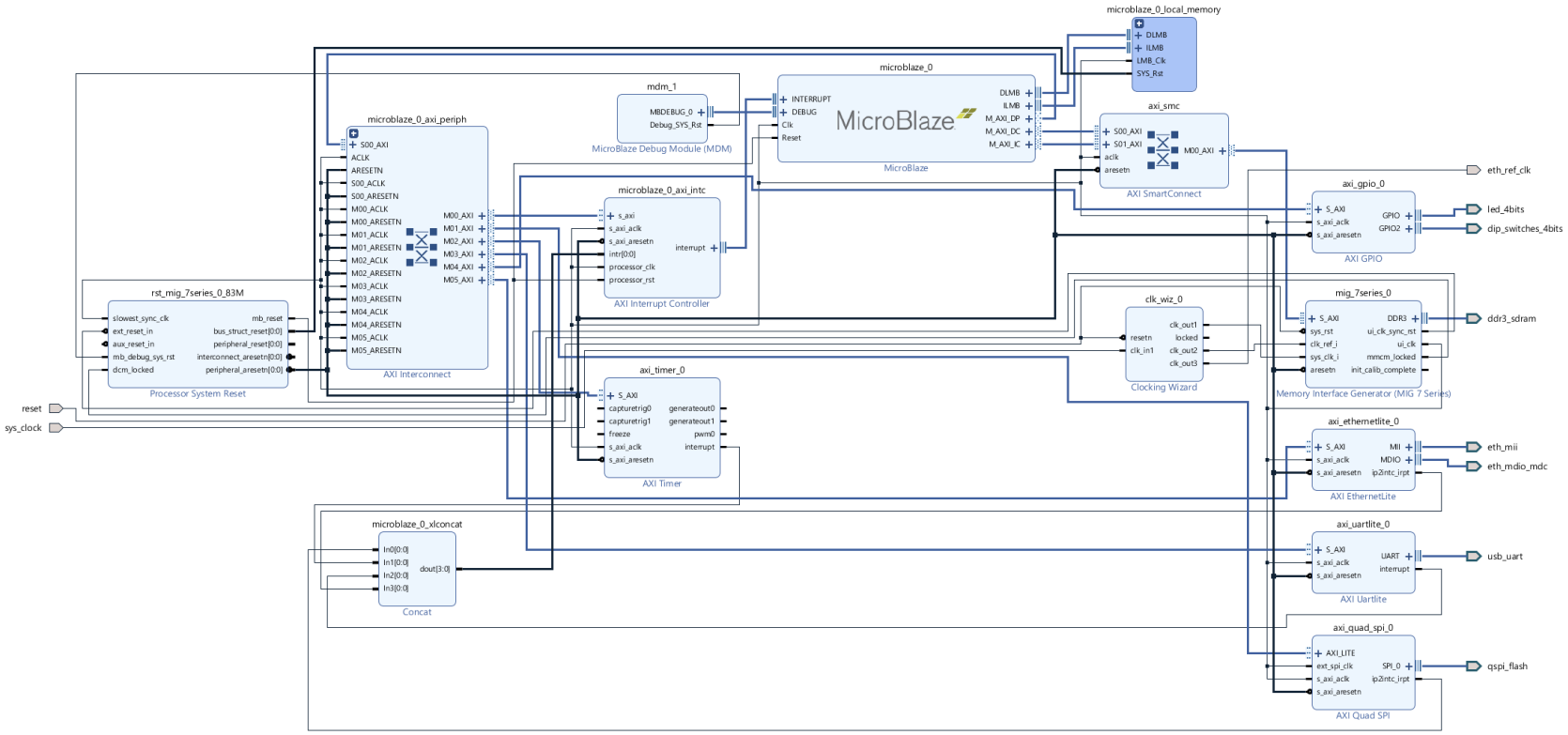




POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

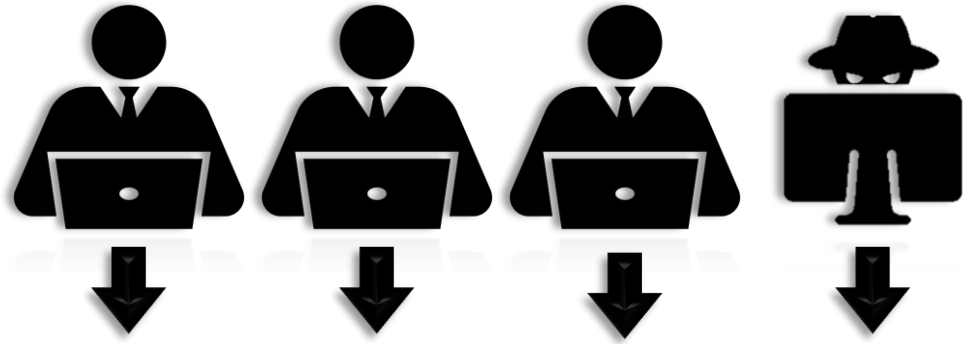
What are FPGAs and Why Should I be Interested?

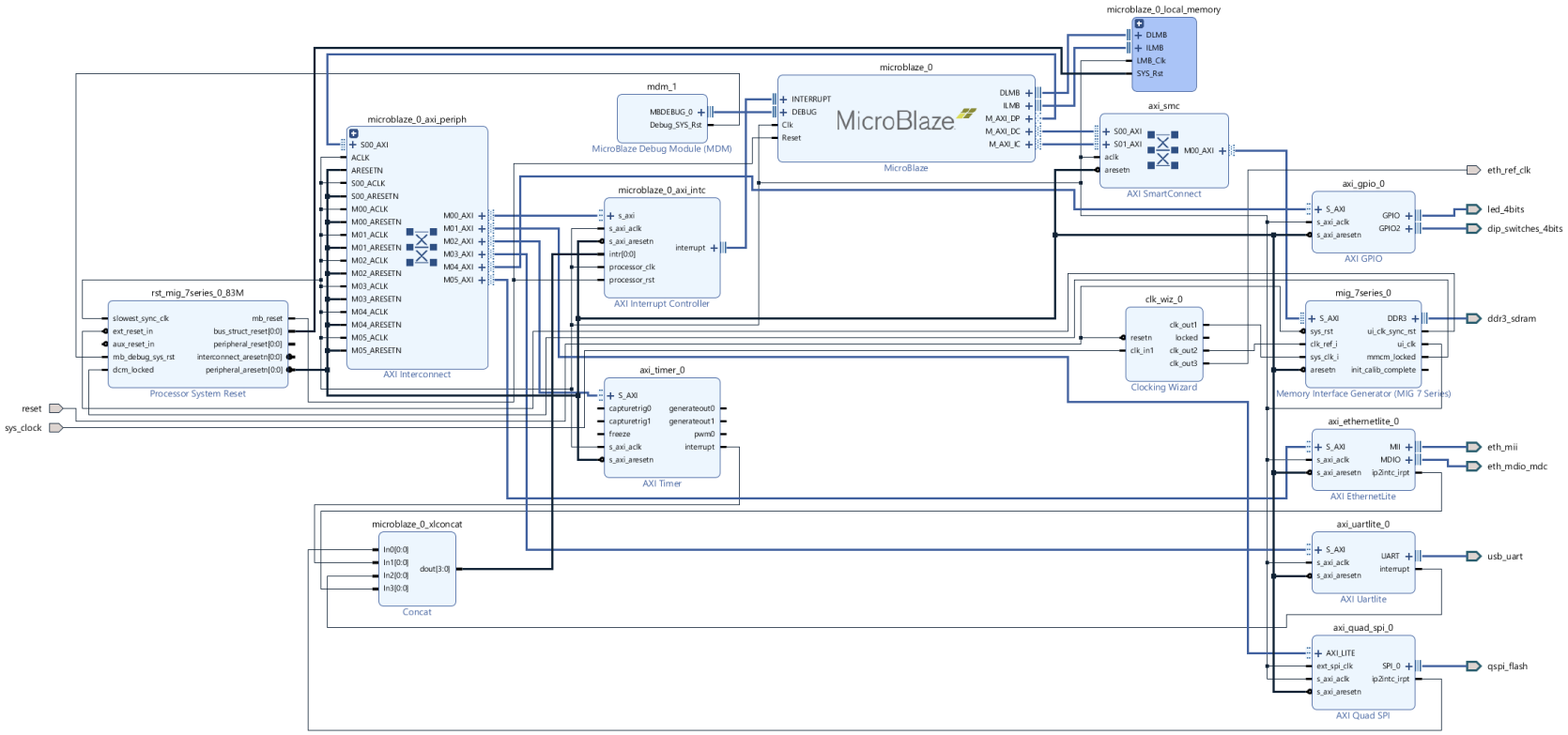




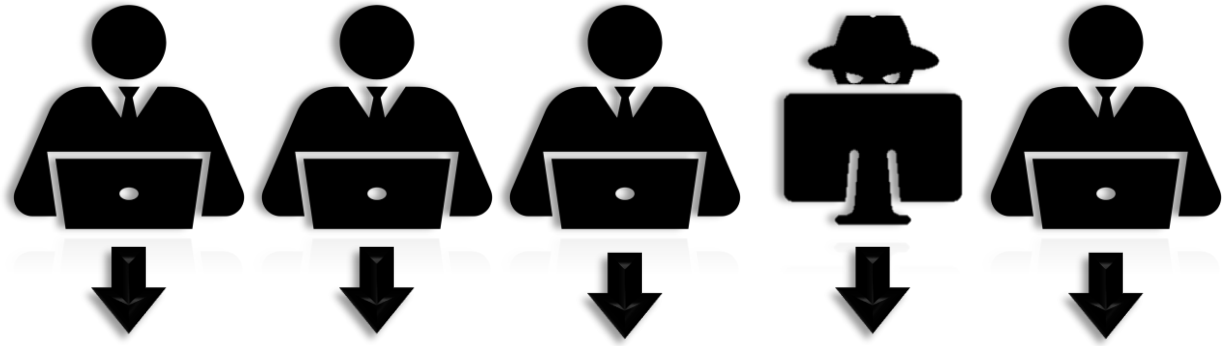
POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

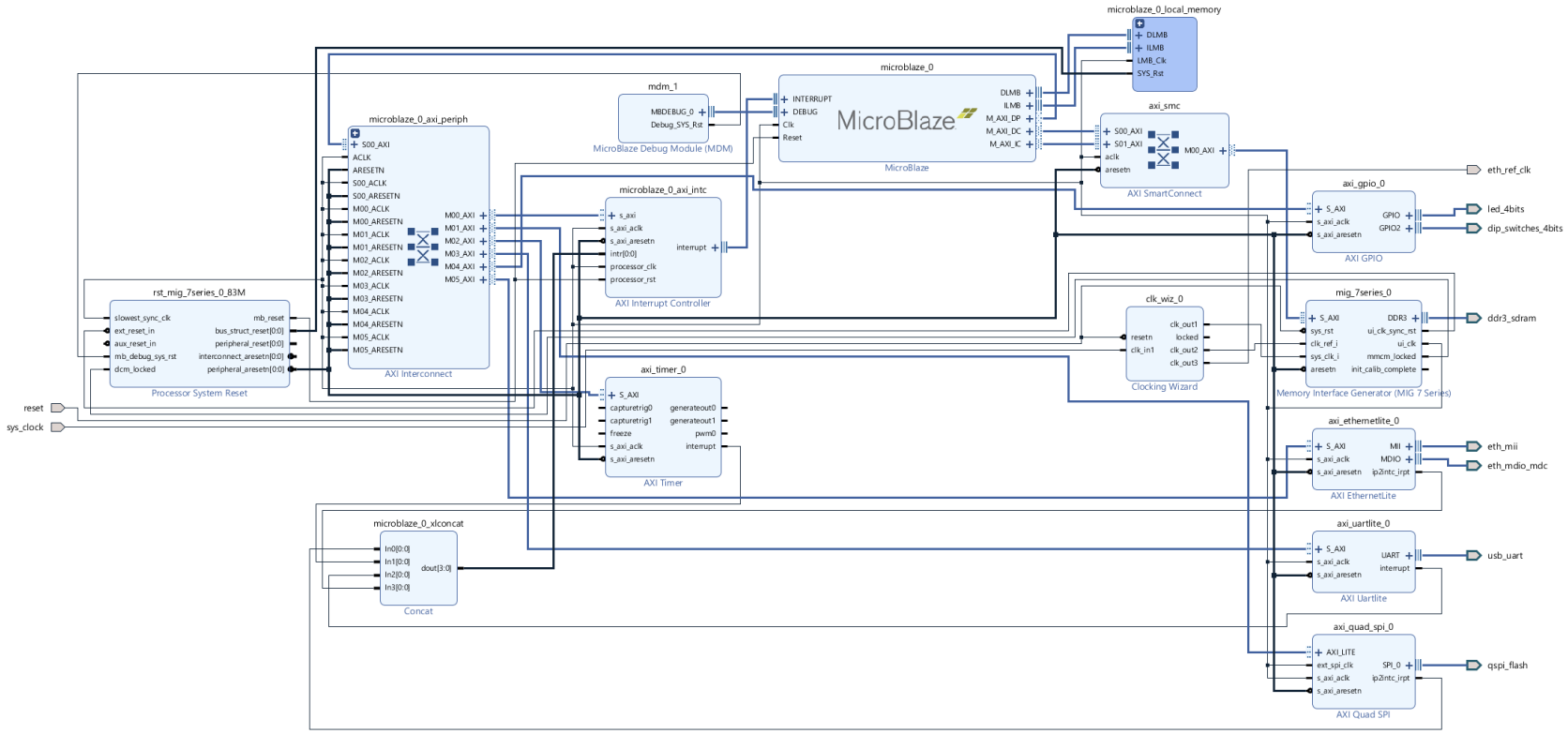
What are FPGAs and Why Should I be Interested?





What are FPGAs and Why Should I be Interested?



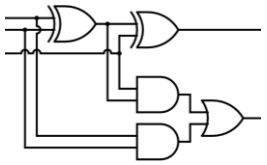


POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Methodology

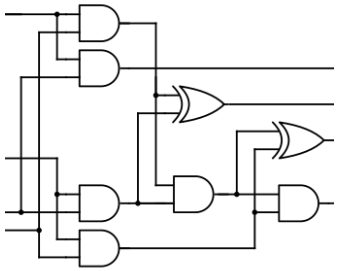
Positive Class

Adder

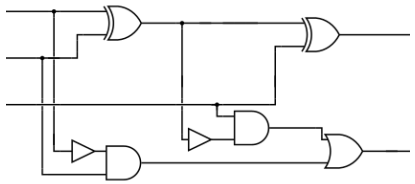


Negative Class

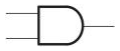
Multiplier



Subtractor



AND



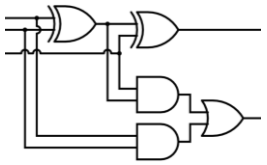
One-vs-All Classification:

Individual Neural network models are trained to identify one hardware module (eg. Adder) against all other modules.

Methodology

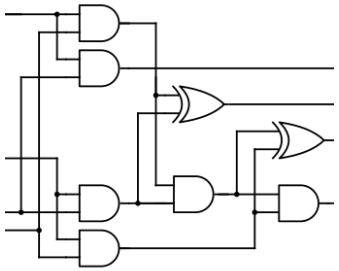
Positive Class

Adder

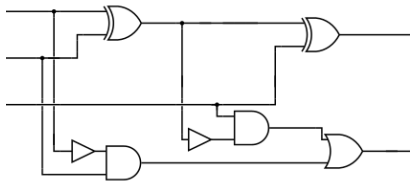


Negative Class

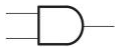
Multiplier

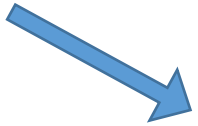


Subtractor



AND





One-vs-All Classification:

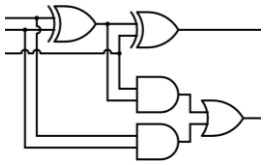
Individual Neural network models are trained to identify one hardware module (eg. Adder) against all other modules.

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Methodology

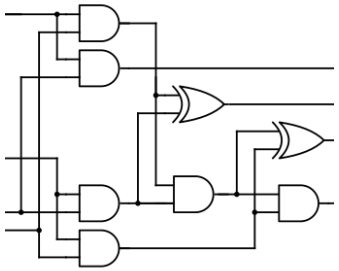
Positive Class

Adder

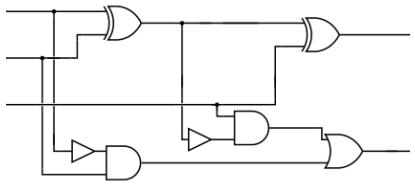


Negative Class

Multiplier



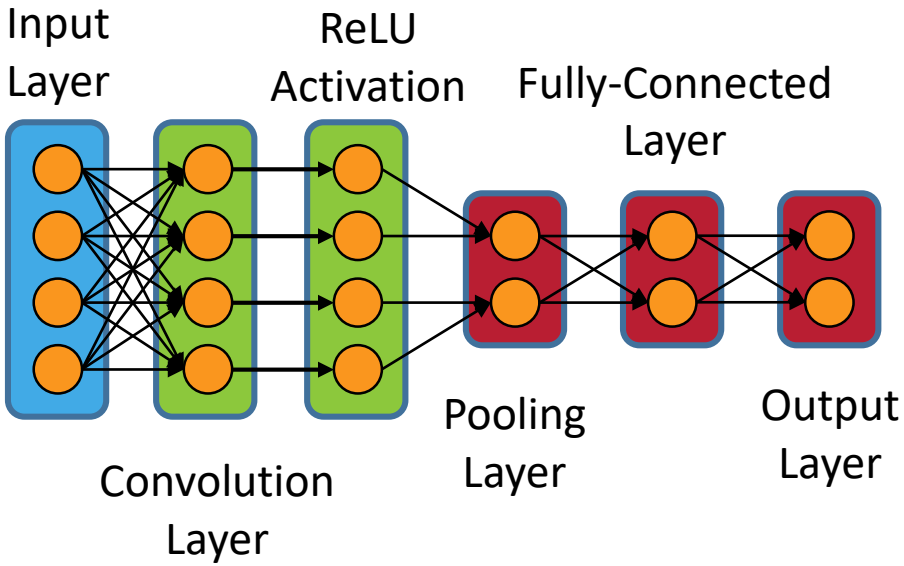
Subtractor



AND

One-vs-All Classification:

Individual Neural network models are trained to identify one hardware module (eg. Adder) against all other modules.

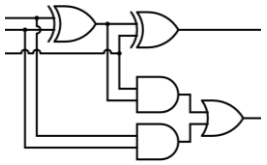


POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Methodology

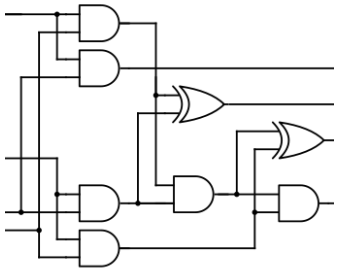
Positive Class

Adder

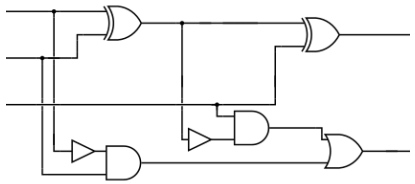


Negative Class

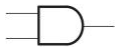
Multiplier



Subtractor

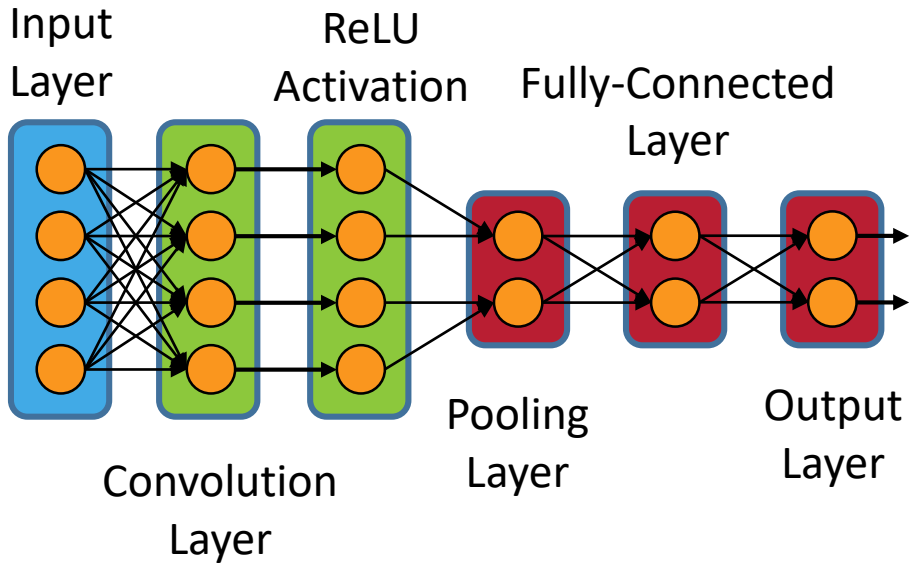


AND



One-vs-All Classification:

Individual Neural network models are trained to identify one hardware module (eg. Adder) against all other modules.



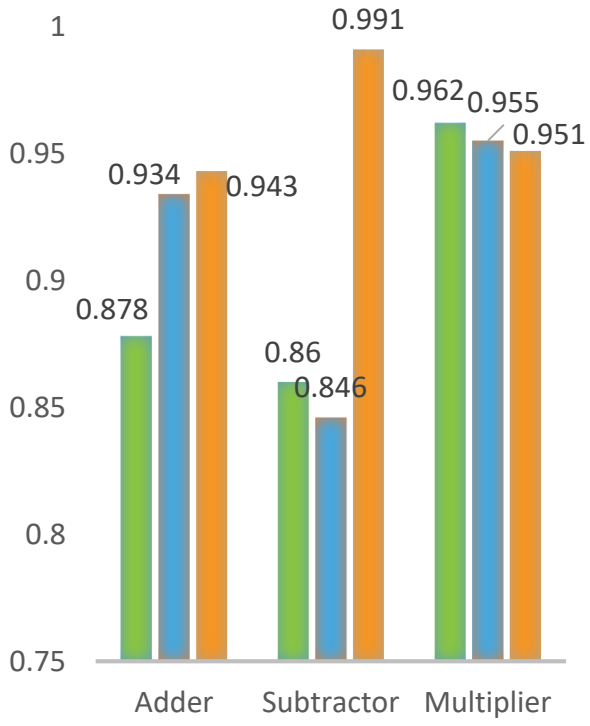
Adder

Not Adder

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Evaluation and Results

Significant success in identifying IP Cores using Convolutional Neural Networks



- **Evaluated on Adder, Subtractor, and Multiplier Module Classification**

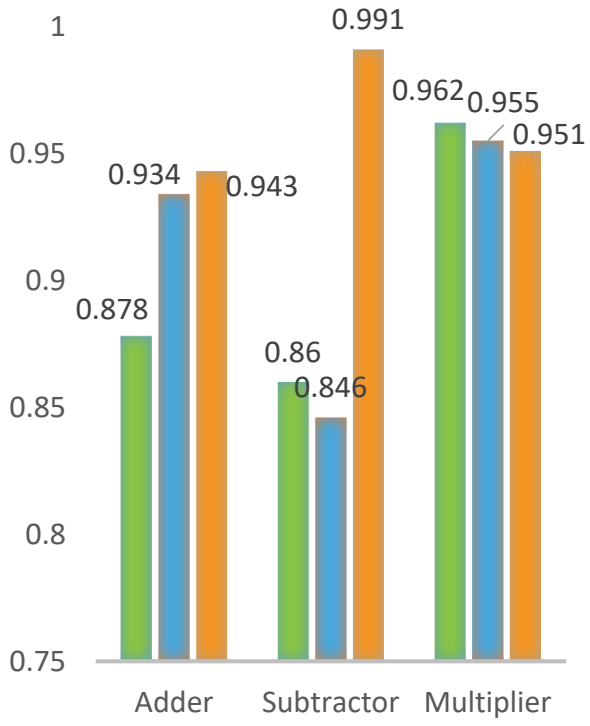
87.8 % - 96.2 %

Accuracy

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Evaluation and Results

Significant success in identifying IP Cores using Convolutional Neural Networks



- **Evaluated on Adder, Subtractor, and Multiplier Module Classification**

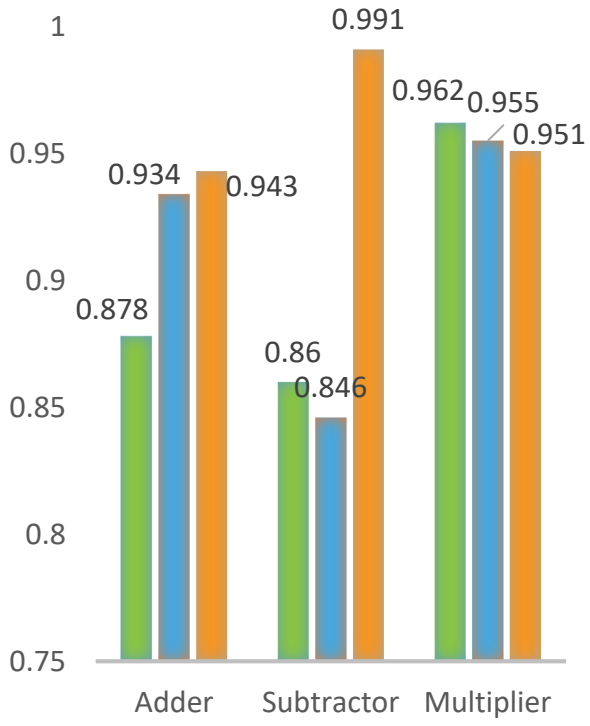
87.8 % - 96.2 %
Accuracy

84.6 % - 95.5 %
Precision

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Evaluation and Results

Significant success in identifying IP Cores using Convolutional Neural Networks



- **Evaluated on Adder, Subtractor, and Multiplier Module Classification**

87.8 % - 96.2 %
Accuracy

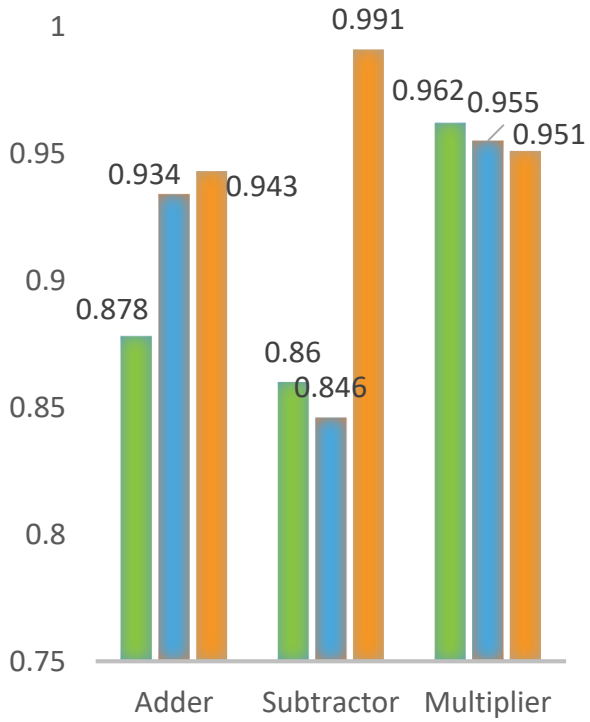
84.6 % - 95.5 %
Precision

94.3 % - 99.1 %
Recall

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Evaluation and Results

Significant success in identifying IP Cores using Convolutional Neural Networks



- **Evaluated on Adder, Subtractor, and Multiplier Module Classification**

87.8 % - 96.2 %
Accuracy

84.6 % - 95.5 %
Precision

94.3 % - 99.1 %
Recall

Shows promise for applications in Trojan detection

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Conclusion

Paper Presentation: IP Core Identification in FPGA Configuration Files using Machine Learning Techniques

There is a Need for Post-Development Integrity Verification in FPGA Designs

Main Findings

- **CNNs can successfully identify know logic blocks** in generated binaries with an accuracy rate of over 87.8 %, high precision and high recall

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Conclusion

Paper Presentation: IP Core Identification in FPGA Configuration Files using Machine Learning Techniques

There is a Need for Post-Development Integrity Verification in FPGA Designs

Main Findings

- **CNNs can successfully identify know logic blocks** in generated binaries with an accuracy rate of over 87.8 %, high precision and high recall

Implications

- Enable developers to **scan their designs** for known **malicious logic**

POLYTECHNIQUE MONTRÉAL
TECHNOLOGICAL UNIVERSITY

Conclusion

Paper Presentation: IP Core Identification in FPGA Configuration Files using Machine Learning Techniques

There is a Need for Post-Development Integrity Verification in FPGA Designs

Main Findings

- **CNNs can successfully identify know logic blocks** in generated binaries with an accuracy rate of over 87.8 %, high precision and high recall

Implications

- Enable developers to **scan their designs** for known **malicious logic**

Future Works

- **Test** the approach with **complex logic blocks**

THANK YOU!

john.doe@polymtl.ca

POLYTECHNIQUE MONTRÉAL

TECHNOLOGICAL UNIVERSITY

Follow us!