# FPGA's

## OVERVIEW, USES AND SECURITY

By Shaun Price

# Contents

- What are FPGA's?
- How are FPGA's used?
- Security and FPGA's

# What are FPGA's

- FPGA or Field Programable Gate Arrays are:
- Integrated circuits (IC's).
- Hardware configured after production.
- Reconfigurable multiple times unlike ASIC's (typical IC).

# What are FPGA's (cont.)

- Very low power compared to a CPU
- Very high speed because the process instructions in parallel
- High cost compared to an ASIC
- A mature technology developed in the early 1980's

# How are they configured

- HDL (Hardware Description Language)
- VHDL, Verilog, Lucid,…
- Logic Diagram
- OpenCL
- Matlab
- Verilog Examples can be found at www.asic-world.com
- Open Source IP Cores (code for FPGA's) can be found at: OpenCores

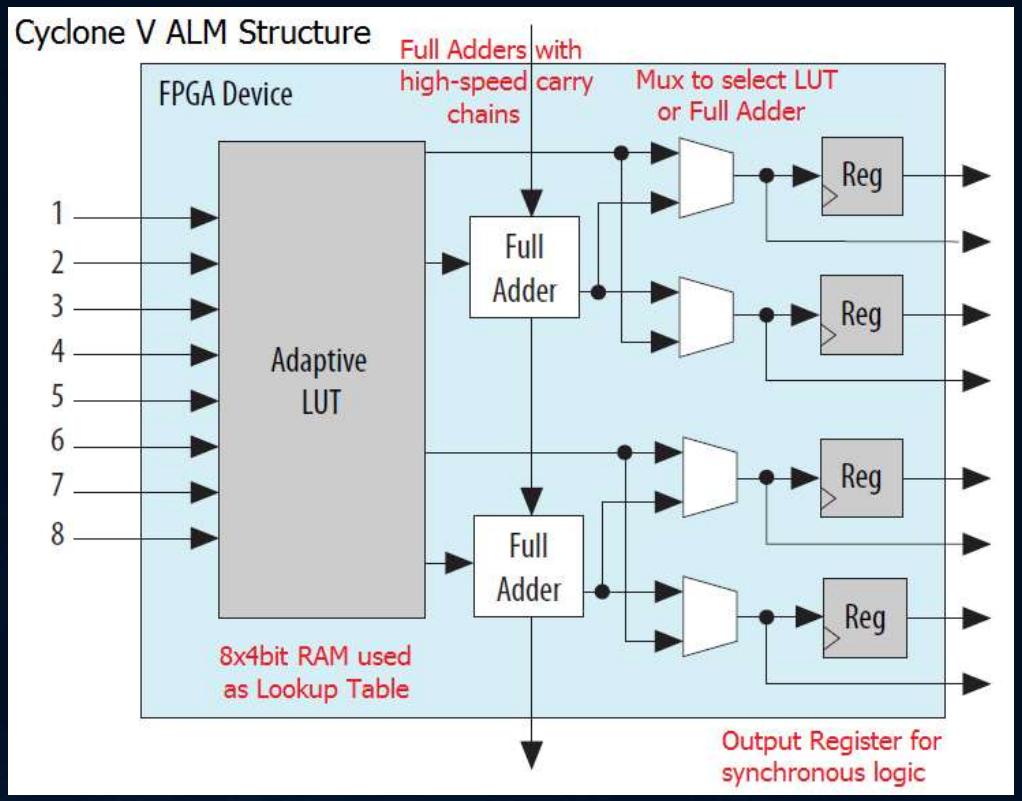
# What are FPGA's Used To Do

- Networking (Routers, Switches, Load Balancers)
- Signal progressing systems.
- Image processing (Video, Computer Vision, Digital Displays).
- Machine learning (Neural Nets)
- Compression (Swarm64DB, Hadoop/Spark)
- Data Analytics (High frequency trading)
- Cryptography (including blockchain and HSM's)

# Manufacturers of FPGA's

- Xilinx
- Altera (Intel)
- Lattice Semiconductor

# FPGA Internals



# FPGA's at Amazon AWS

- EC2 F1 Instances (https://aws.amazon.com/ec2/instance-types/f1/)
  - Xilinx Ultrascale PLUS, 64 GiB DDR4 ECC protected memory, Dedicated PCIe x16 connection, 2.5 million logic elements, 6,800 Digital Signal Processing (DSP) engines
- Useful for:
  - Running Neural Nets
  - Database compression
  - Video Streaming
  - Blockchain
  - Data analytics

# FPGA's at Microsoft Azure

- Most Microsoft Azure CLOUD SmartNET FPGA network cards
- SmartNET cards are upgradable and offload Software Defined Network Components from the CPU to the FPGA.
  - Fastest Latency and Highest Bandwidth of any cloud provider.
- FPGA based machine learning (Project Brainwave)
  - Under the hood. Not user configurable!
  - Running Neural Nets (not training – done with GPU's)
  - ResNet50 Feature Classifier (others to come)
  - Based on Intel's Stratix 10 FPGA's
  - Optimised/swappable machine learning cores


Microsoft Azure SmartNET Card

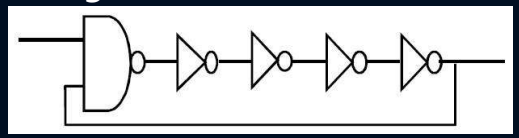
# FPGA's in InfoSec

- Encryption/Decryption
  - Hardware Security Modules (HSM's)
  - Streaming data encryption/decryption
  - Blockchain
- Custom circuits
  - Custom Security Devices
  - Network Monitoring
  - Data Stream Tapping/Manipulation

# FPGA's Security

- Attacks
  - Side Channel Attacks
    - Local power attacks
    - Remote Power attacks on shared FPGA's
    - Long Wire Attacks on shared FPGA's
  - IP Theft
- Security
  - Shared FPGA's - Limit Long Wires
  - Shared FPGA's - Don't share sensitive functions on the same FPGA with others
  - IP Theft - Use FPGA's supporting encrypted config and tamperproof key's

Ring Oscillator



*The oscillator works because there are small delays between each component from the capacitance, resistance and inductance all circuits have. Changes in the voltage due to power consumption of the FPGA cause the delays to increase and decrease which in turn changes the frequency of the oscillator. This means you can monitor the bit states (0 or 1) of circuits within the FPGA.*