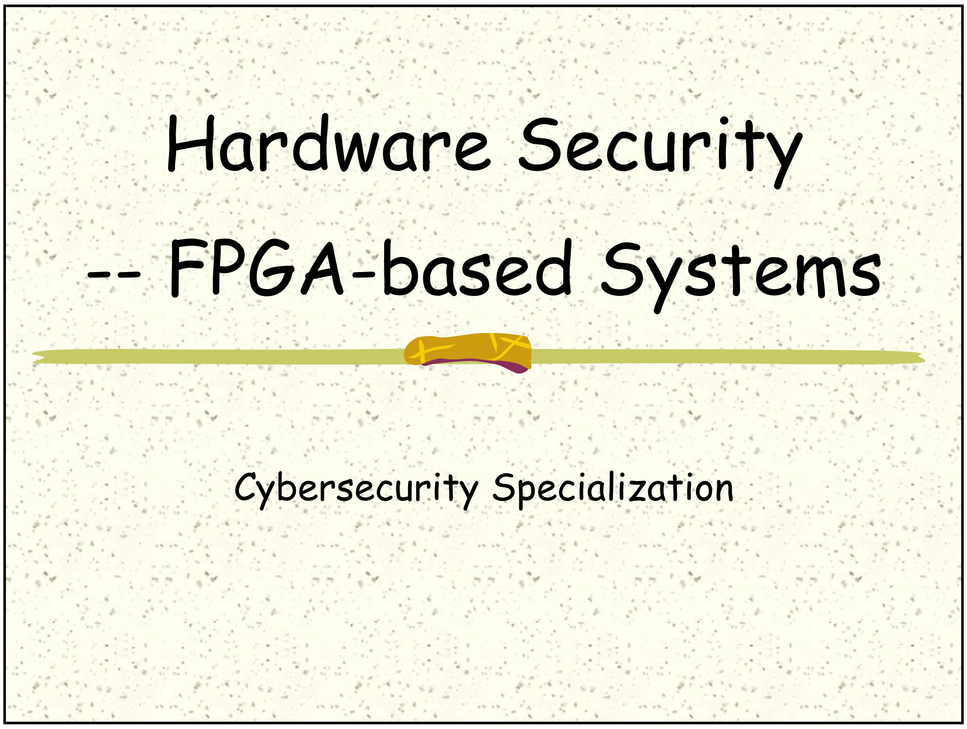
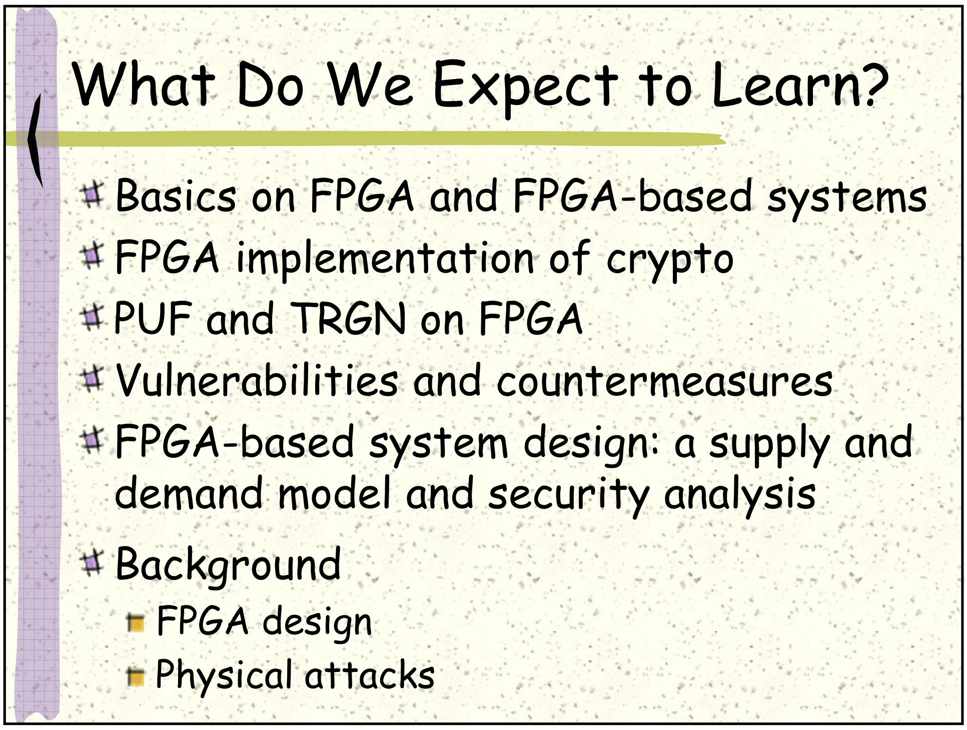


Hardware Security
-- FPGA-based Systems

Cybersecurity Specialization



What Do We Expect to Learn?

- Basics on FPGA and FPGA-based systems
- FPGA implementation of crypto
- PUF and TRGN on FPGA
- Vulnerabilities and countermeasures
- FPGA-based system design: a supply and demand model and security analysis
- Background
  - FPGA design
  - Physical attacks

What is FPGA?

- Field Programmable Gate Array
  - Structure of FPGA
  - Capacity (2014 data)
    - billions of transistors
    - 10 nm technology
- What are on FPGA?
  - Programmable logic cells
  - Build-in function units
  - Memory blocks
  - Other IPs

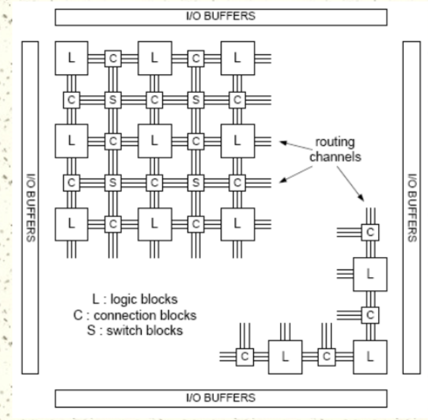
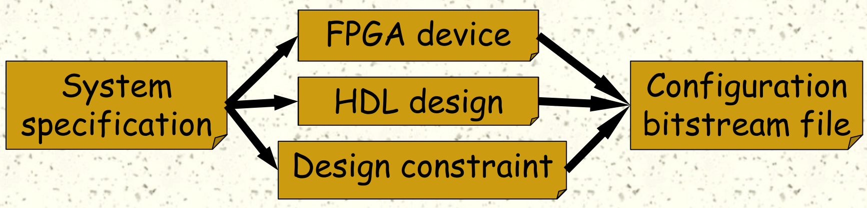


Image source: wikipedia

Design of FPGA-based Systems

- FPGA-based systems design



System specification

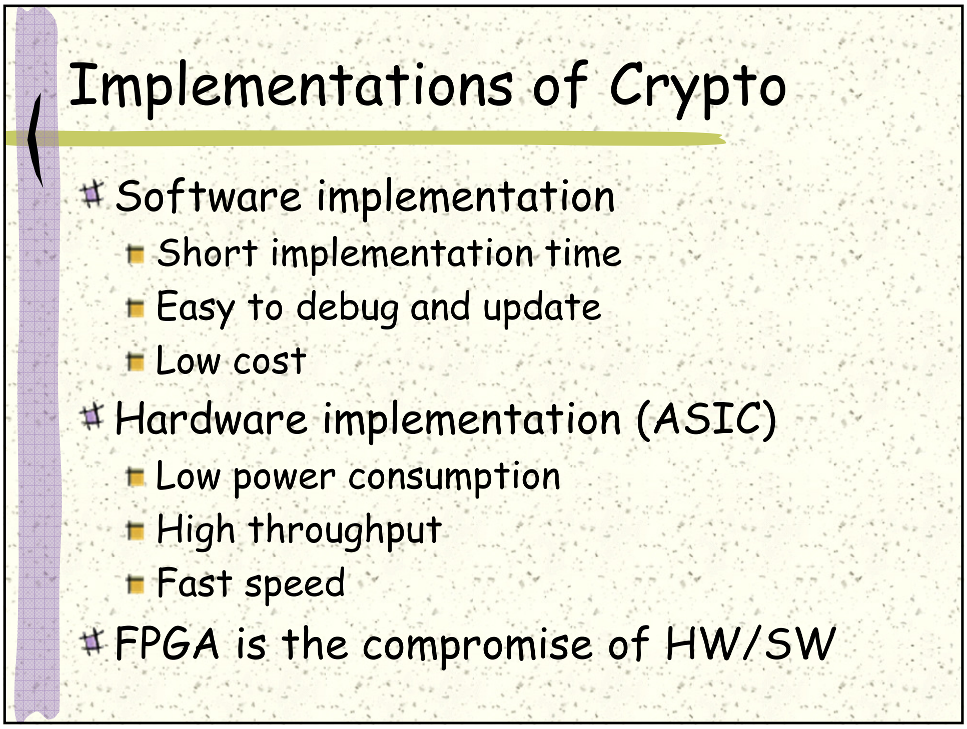
FPGA device

HDL design

Design constraint

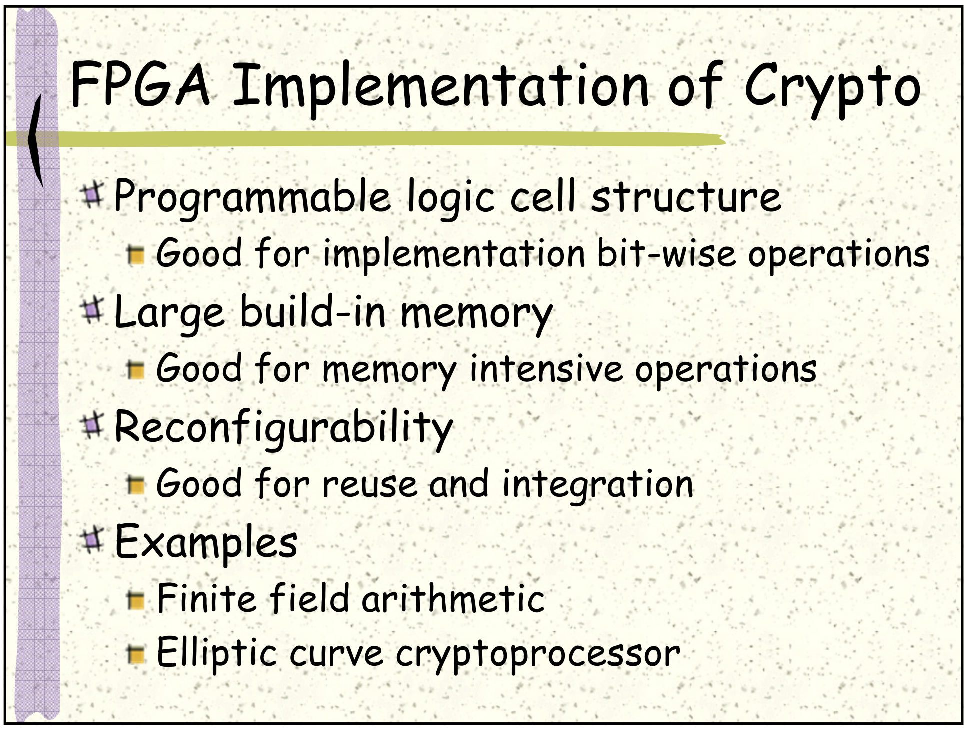
Configuration bitstream file

- Advantages (vs. ASIC)
  - Short time-to-market
  - Low cost
  - Reconfigurability
- Advantages (vs. SW)
  - High performance
  - Low power
  - Low cost



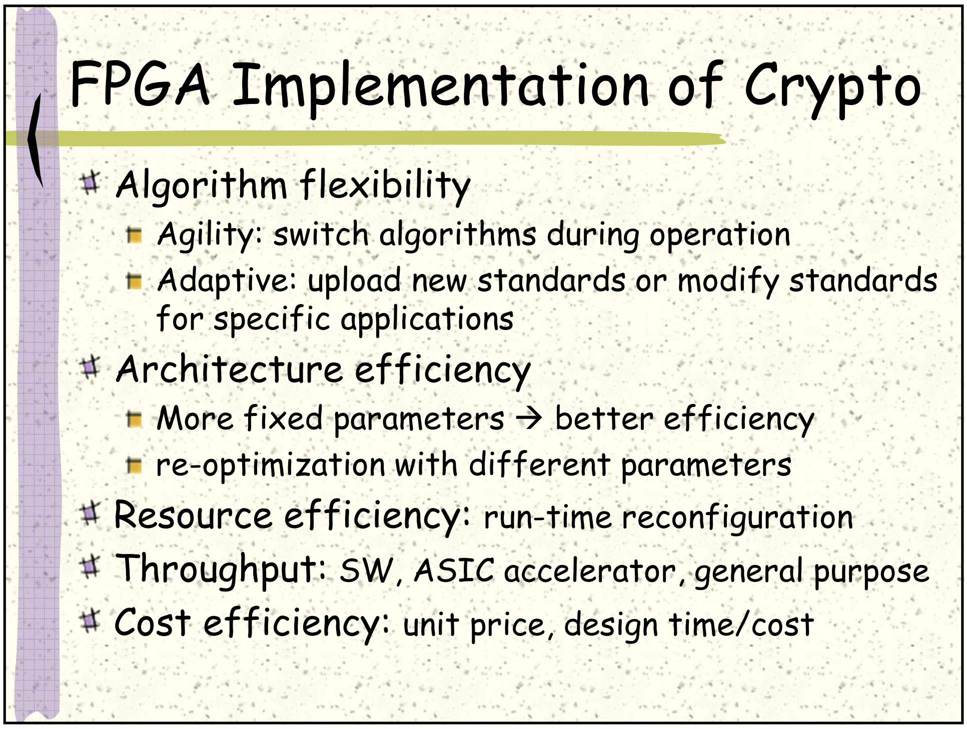
Implementations of Crypto

- Software implementation
  - Short implementation time
  - Easy to debug and update
  - Low cost
- Hardware implementation (ASIC)
  - Low power consumption
  - High throughput
  - Fast speed
- FPGA is the compromise of HW/SW



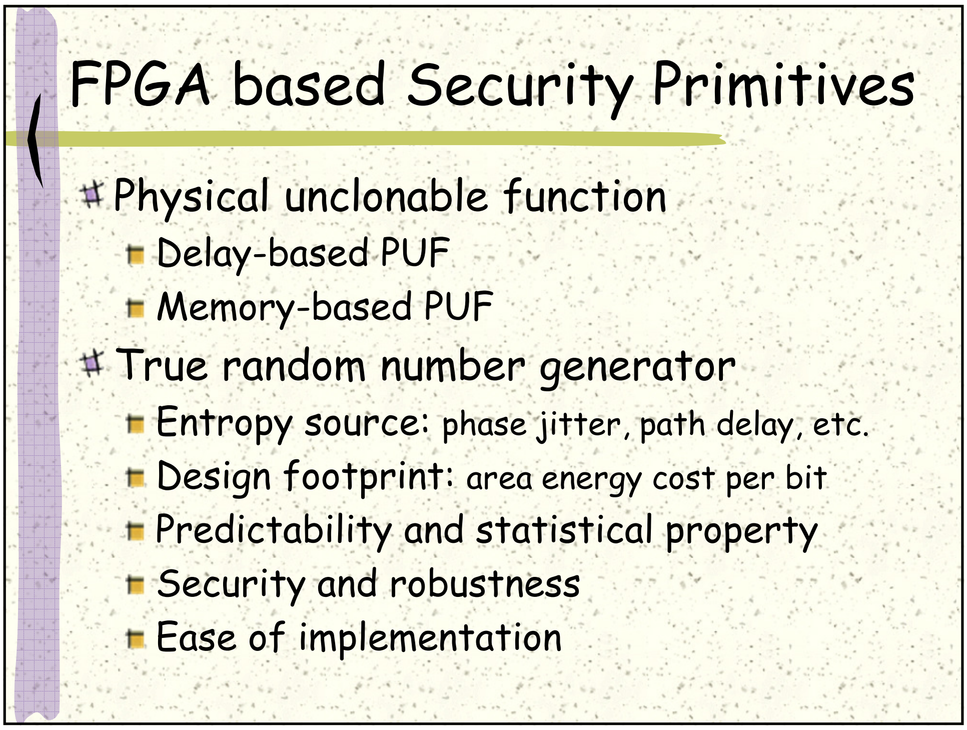
FPGA Implementation of Crypto

- Programmable logic cell structure
  - Good for implementation bit-wise operations
- Large build-in memory
  - Good for memory intensive operations
- Reconfigurability
  - Good for reuse and integration
- Examples
  - Finite field arithmetic
  - Elliptic curve cryptoprocessor



FPGA Implementation of Crypto

- Algorithm flexibility
  - Agility: switch algorithms during operation
  - Adaptive: upload new standards or modify standards for specific applications
- Architecture efficiency
  - More fixed parameters → better efficiency
  - re-optimization with different parameters
- Resource efficiency: run-time reconfiguration
- Throughput: SW, ASIC accelerator, general purpose
- Cost efficiency: unit price, design time/cost



FPGA based Security Primitives

- Physical unclonable function
  - Delay-based PUF
  - Memory-based PUF
- True random number generator
  - Entropy source: phase jitter, path delay, etc.
  - Design footprint: area energy cost per bit
  - Predictability and statistical property
  - Security and robustness
  - Ease of implementation