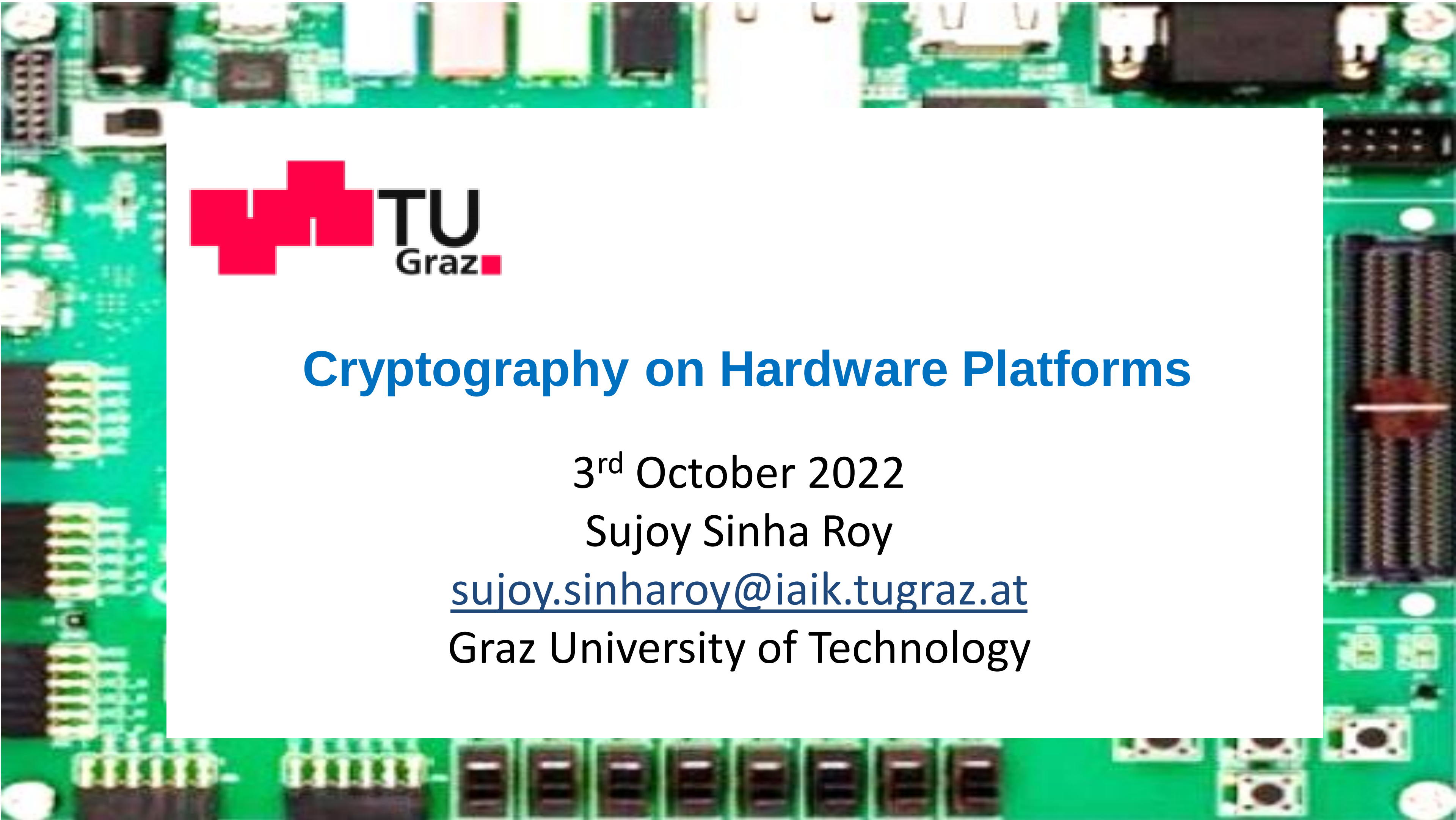


Cryptography on Hardware Platforms

3rd October 2022

Sujoy Sinha Roy

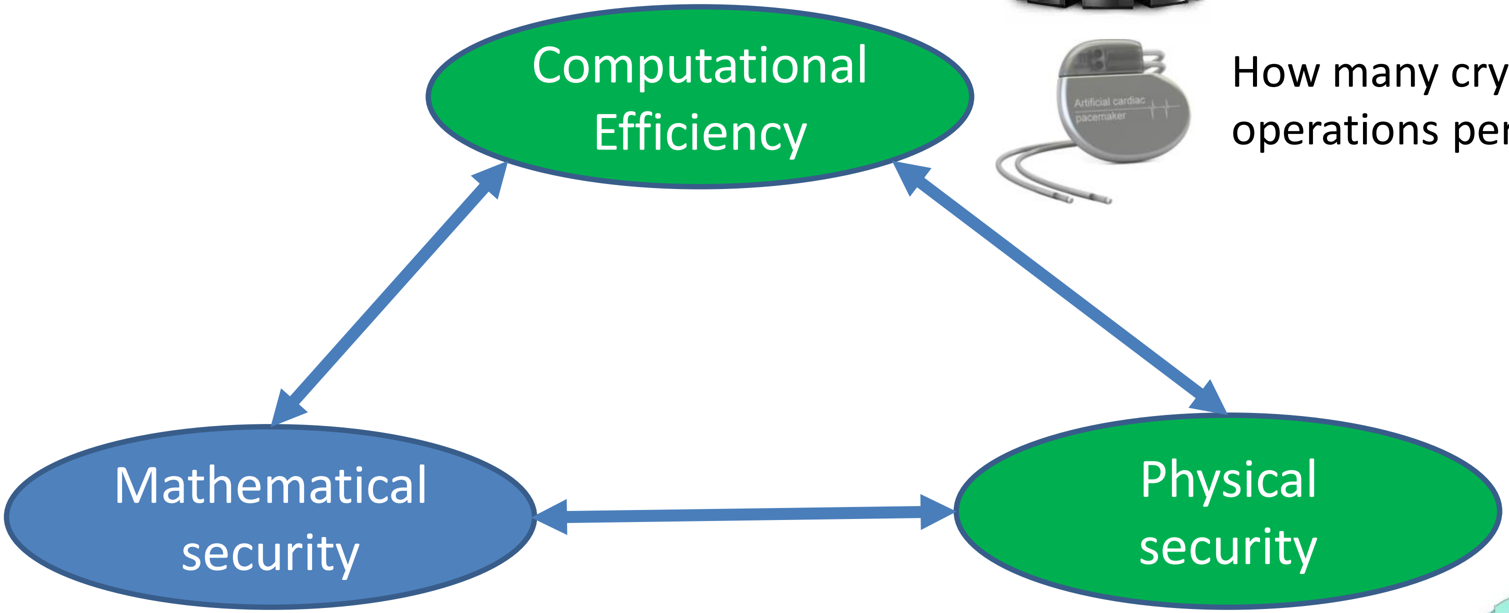
sujoy.sinharoy@iaik.tugraz.at

Graz University of Technology

Challenges in implementing cryptography

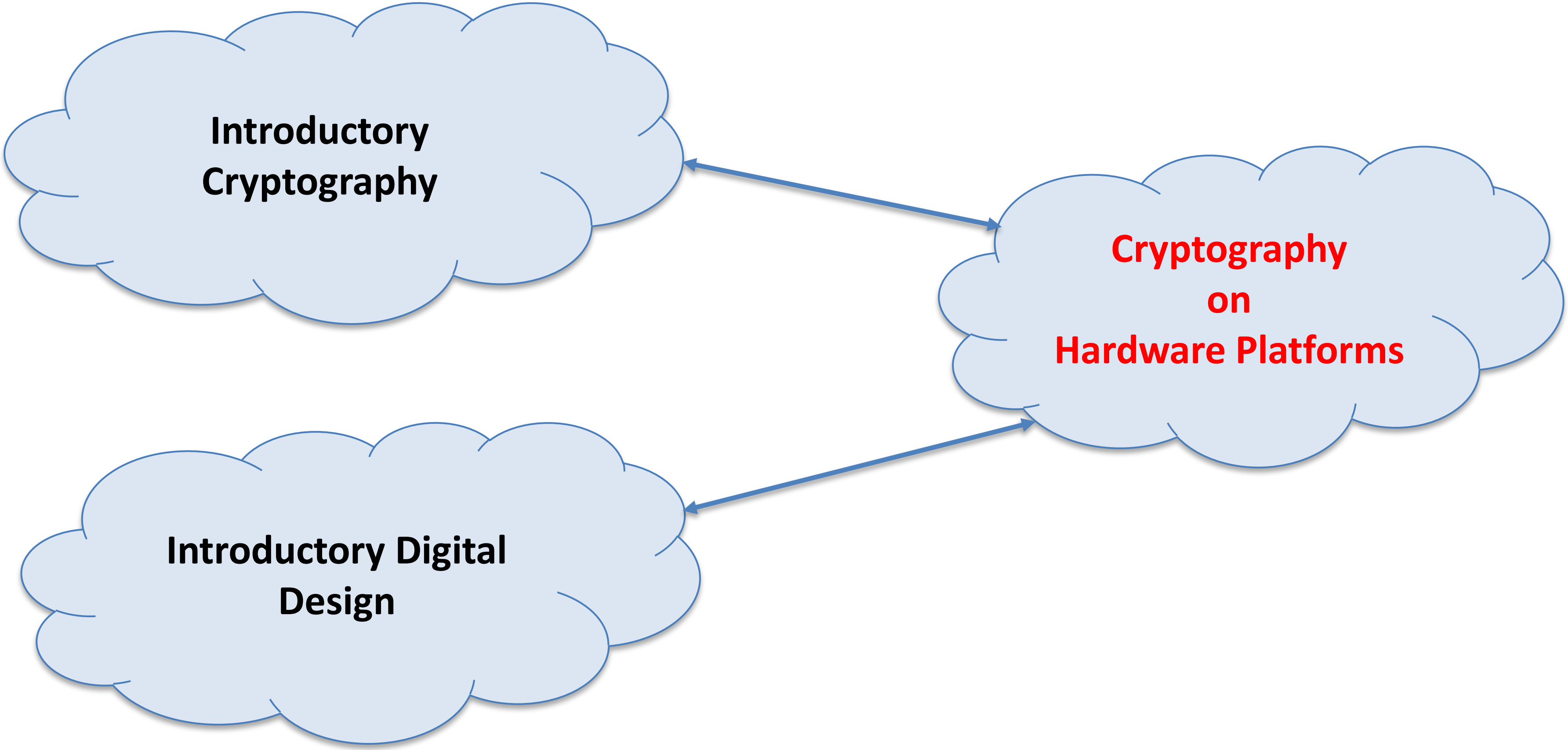
How many crypto operations per second?

How many crypto operations per Joules?



Cryptography engineers work on the green vertices.

Where does this new course fit?



Introductory Cryptography

Cryptography on Hardware Platforms

Introductory Digital Design

New course Cryptography on Hardware Platforms

Learning goals

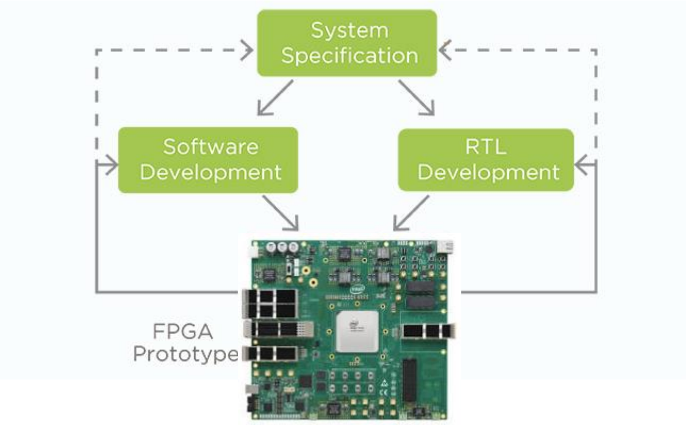
1. FPGA design flow.

2. Problem-oriented hardware development for cryptography.

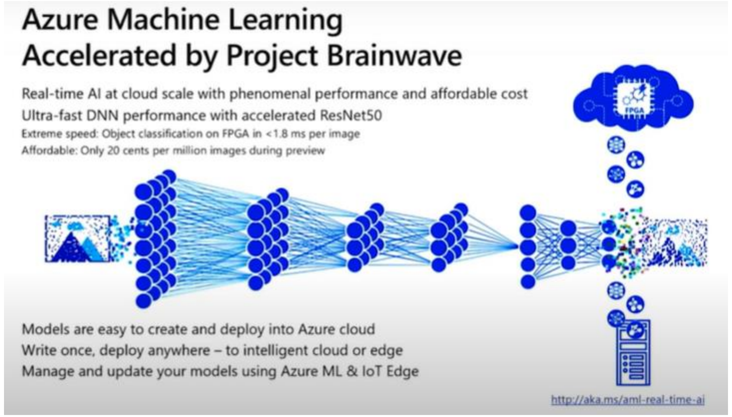
3. Optimized implementation techniques.

4. Secure implementation techniques.

Popular applications of FPGAs



Prototyping of designs



Azure Machine Learning
Accelerated by Project Brainwave

Real-time AI at cloud scale with phenomenal performance and affordable cost
Ultra-fast DNN performance with accelerated ResNet50
Extreme speed: Object classification on FPGA in <1.8 ms per image
Affordable: Only 20 cents per million images during preview

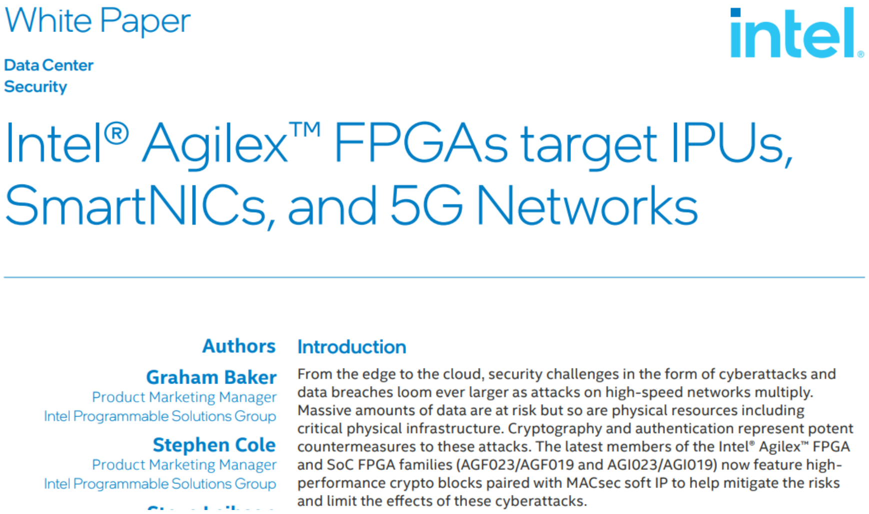
Models are easy to create and deploy into Azure cloud
Write once, deploy anywhere – to intelligent cloud or edge
Manage and update your models using Azure ML & IoT Edge

http://aka.ms/aml-real-time-ai

Acceleration of ML applications

https://www.youtube.com/watch?v=t3Vo37V9oU8&t=2325s

Popular applications of FPGAs



White Paper

Data Center
Security

intel.

Intel® Agilex™ FPGAs target IPUs, SmartNICs, and 5G Networks

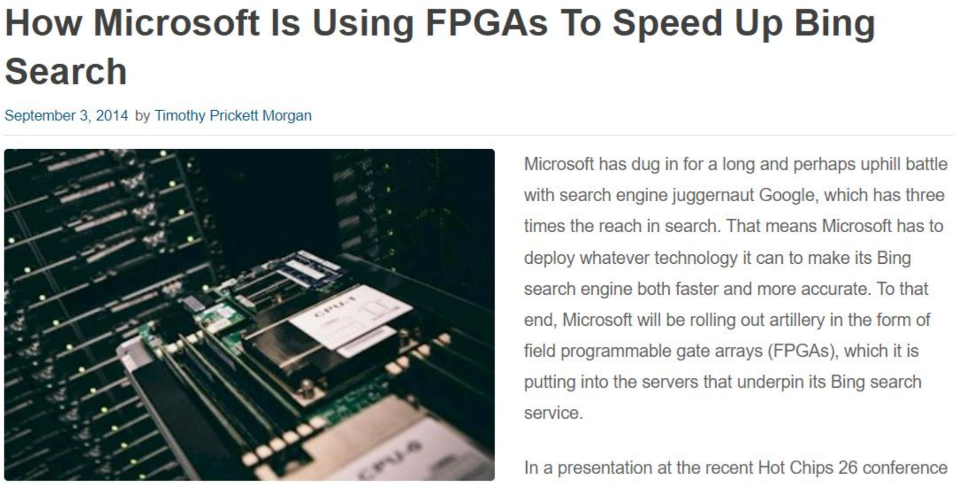
Authors

Graham Baker
Product Marketing Manager
Intel Programmable Solutions Group

Stephen Cole
Product Marketing Manager
Intel Programmable Solutions Group

Introduction

From the edge to the cloud, security challenges in the form of cyberattacks and data breaches loom ever larger as attacks on high-speed networks multiply. Massive amounts of data are at risk but so are physical resources including critical physical infrastructure. Cryptography and authentication represent potent countermeasures to these attacks. The latest members of the Intel® Agilex™ FPGA and SoC FPGA families (AGF023/AGF019 and AGI023/AGI019) now feature high-performance crypto blocks paired with MACsec soft IP to help mitigate the risks and limit the effects of these cyberattacks.

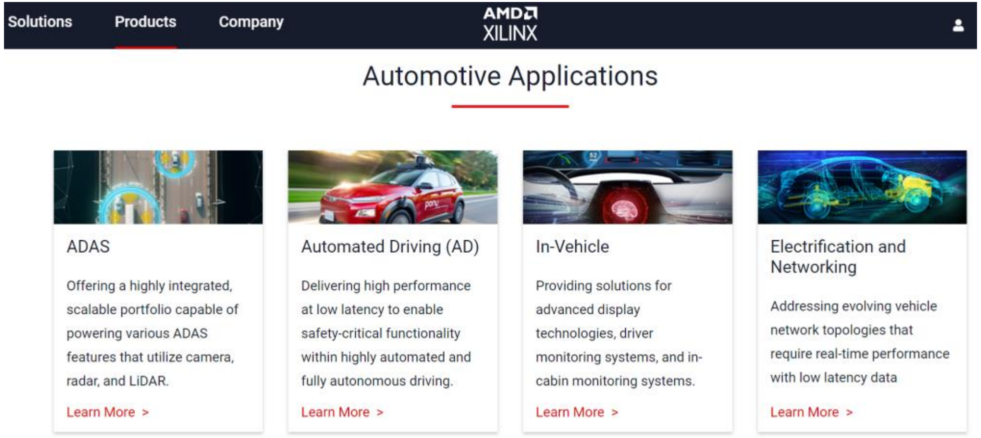


How Microsoft Is Using FPGAs To Speed Up Bing Search

September 3, 2014 by Timothy Prickett Morgan

Microsoft has dug in for a long and perhaps uphill battle with search engine juggernaut Google, which has three times the reach in search. That means Microsoft has to deploy whatever technology it can to make its Bing search engine both faster and more accurate. To that end, Microsoft will be rolling out artillery in the form of field programmable gate arrays (FPGAs), which it is putting into the servers that underpin its Bing search service.

In a presentation at the recent Hot Chips 26 conference



Automotive Applications

ADAS

Offering a highly integrated, scalable portfolio capable of powering various ADAS features that utilize camera, radar, and LiDAR.

Learn More >

Automated Driving (AD)

Delivering high performance at low latency to enable safety-critical functionality within highly automated and fully autonomous driving.

Learn More >

In-Vehicle

Providing solutions for advanced display technologies, driver monitoring systems, and in-cabin monitoring systems.

Learn More >

Electrification and Networking

Addressing evolving vehicle network topologies that require real-time performance with low latency data

Learn More >

How is ‘Cryptography on Hardware Platforms’ relevant?

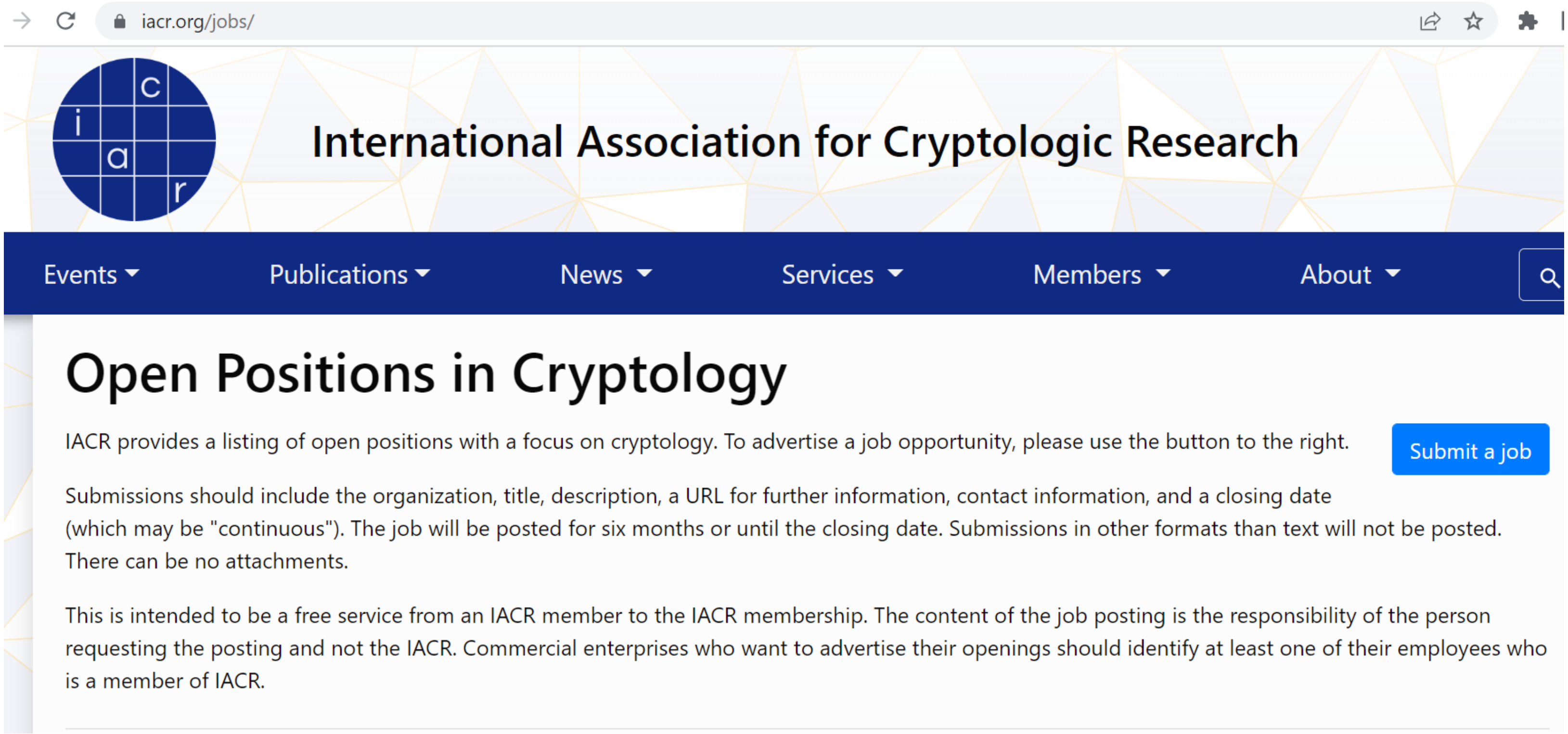
- Active area of research

  New cryptographic needs, New protocols, New platforms, …

- Industry needs people who can make crypto ‘work’

  Only a handful of universities offer courses on cryptographic implementation techniques …

… some job advertisements from the internet



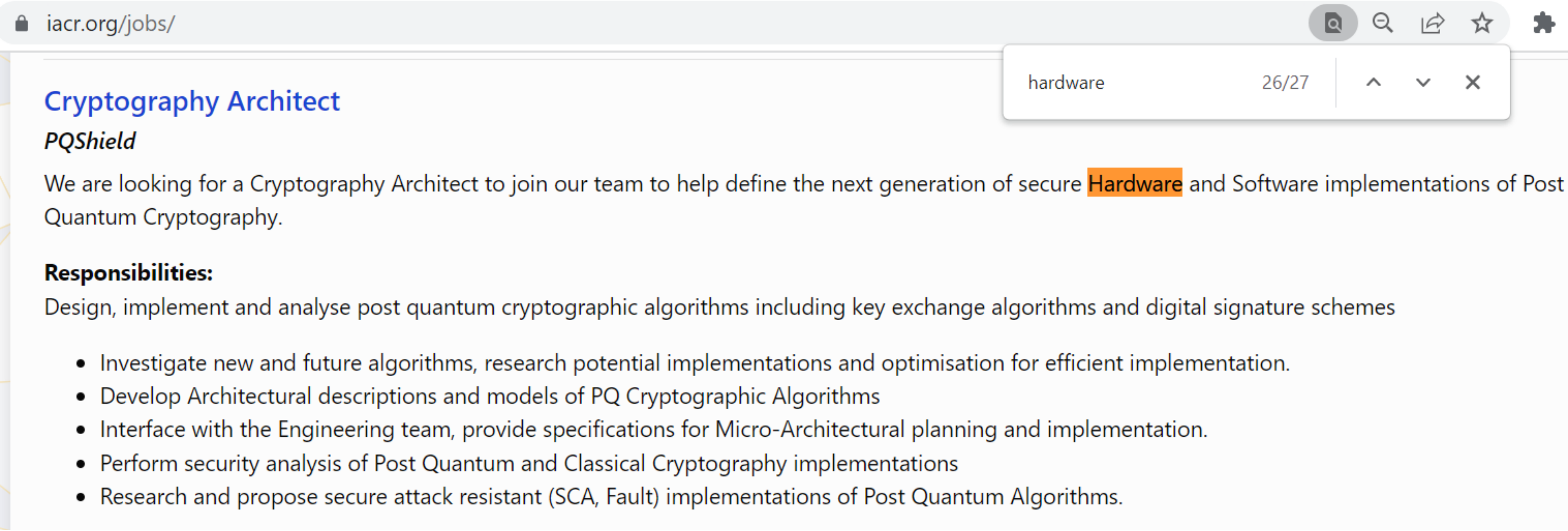
Open Positions in Cryptology

IACR provides a listing of open positions with a focus on cryptology. To advertise a job opportunity, please use the button to the right.

Submissions should include the organization, title, description, a URL for further information, contact information, and a closing date (which may be "continuous"). The job will be posted for six months or until the closing date. Submissions in other formats than text will not be posted. There can be no attachments.

This is intended to be a free service from an IACR member to the IACR membership. The content of the job posting is the responsibility of the person requesting the posting and not the IACR. Commercial enterprises who want to advertise their openings should identify at least one of their employees who is a member of IACR.

… some job advertisements from the internet



Cryptography Architect

PQShield

We are looking for a Cryptography Architect to join our team to help define the next generation of secure Hardware and Software implementations of Post Quantum Cryptography.

Responsibilities:
Design, implement and analyse post quantum cryptographic algorithms including key exchange algorithms and digital signature schemes

- Investigate new and future algorithms, research potential implementations and optimisation for efficient implementation.
- Develop Architectural descriptions and models of PQ Cryptographic Algorithms
- Interface with the Engineering team, provide specifications for Micro-Architectural planning and implementation.
- Perform security analysis of Post Quantum and Classical Cryptography implementations
- Research and propose secure attack resistant (SCA, Fault) implementations of Post Quantum Algorithms.

Tentative topics to be covered

1. FPGA design flow
2. Public-key Primitives
3. Symmetric-key Primitives
4. True Random Number Generation
5. Physically Unclonable Functions
6. Homomorphic Encryption (optional)

The Teachers

Sujoy Sinha Roy

Ahmet Can Mert

Email: sujoy.sinharoy@tugraz.at
Office: 2nd Floor IAIK

Email: ahmet.mert@iaik.tugraz.at
Office: 2nd Floor IAIK

When?

On Mondays starting from 3rd October. (www.iaik.tugraz.at/chw)

- Monday 10 – 11am

- Tuesday 9:15 – 11am

The lectures and practical will be in the IAIK Seminar room.

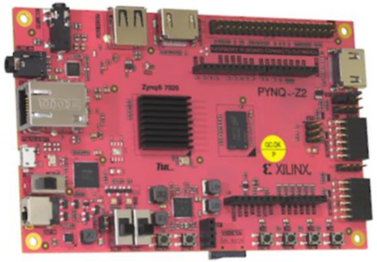
Office hours

- There are no fixed office hours for this course.
- Best option: attend practical sessions and discuss with us directly.
- Besides, you may book appointments by email.

Structure of ‘Cryptography on Hardware Platforms’

- 5 ECTS.

- Evaluation: 100% from 2 practical assignments → No written exam.



Implement crypto on FPGA-Arm platform

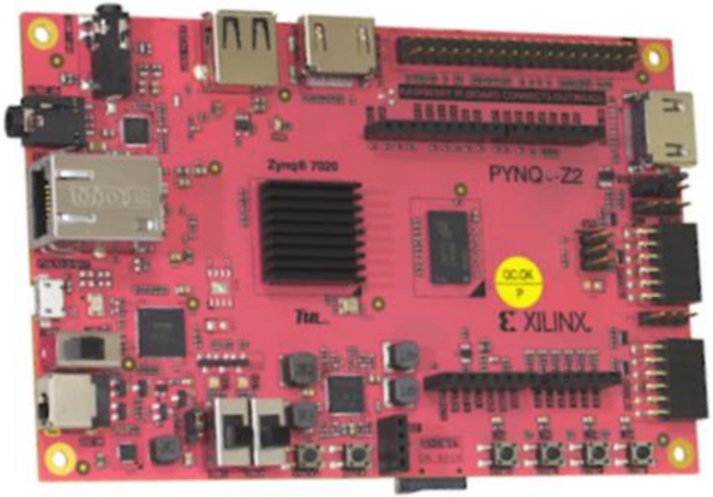
- Work in teams of 2 people.

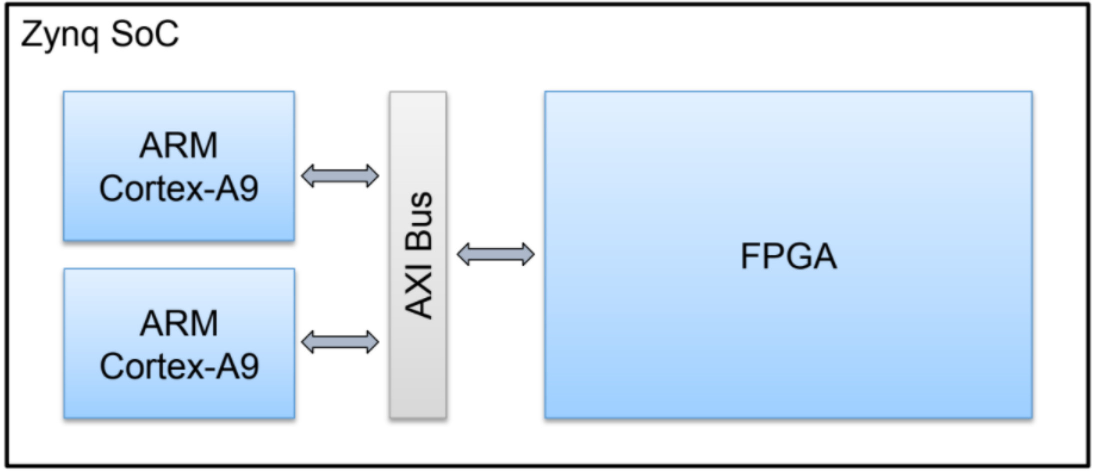
- Oral defence after submitting assignments.

Our hardware platform for prototyping

This course: We will run crypto in real hardware!

Xilinx PYNQ-Z2





Processing System (PS): ARM Cores where you put your SW program

Programmable Logic (PL): FPGA for your Verilog Crypto cores

Zynq SoC uses AXI bus for communications