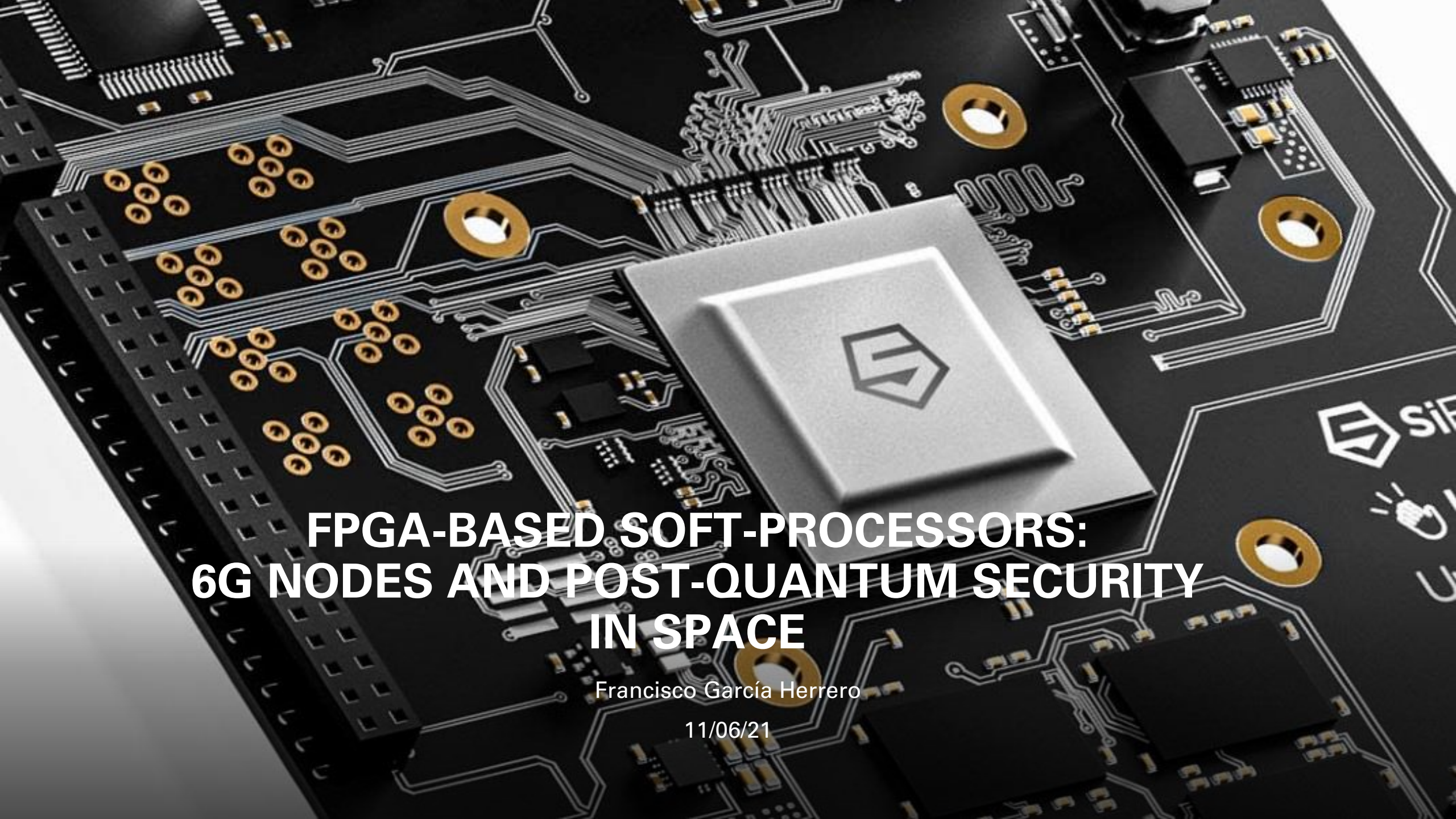


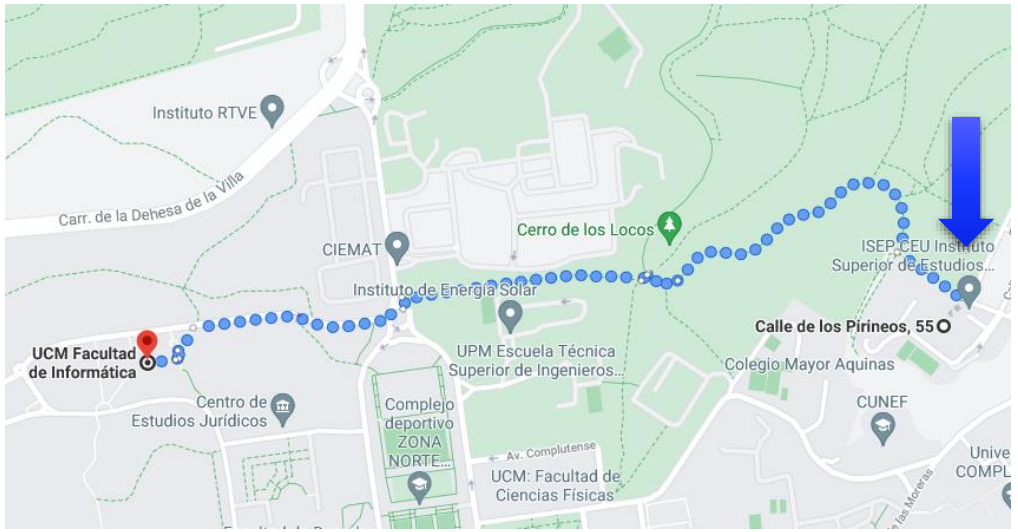
FPGA-BASED SOFT-PROCESSORS: 6G NODES AND POST-QUANTUM SECURITY IN SPACE

Francisco García Herrero

11/06/21

ARIES

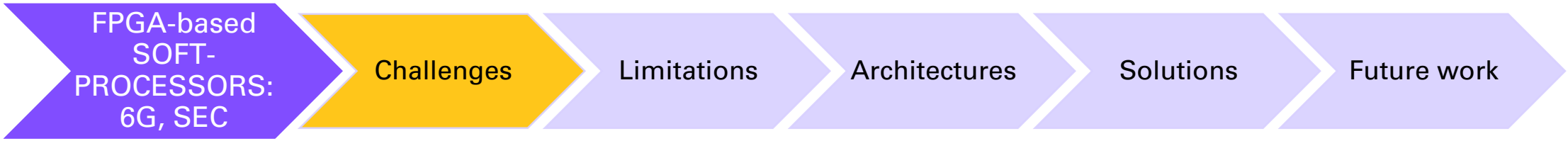
UNIVERSIDAD NEBRIJA | ARIES



http://www.nebrija.es/aries/

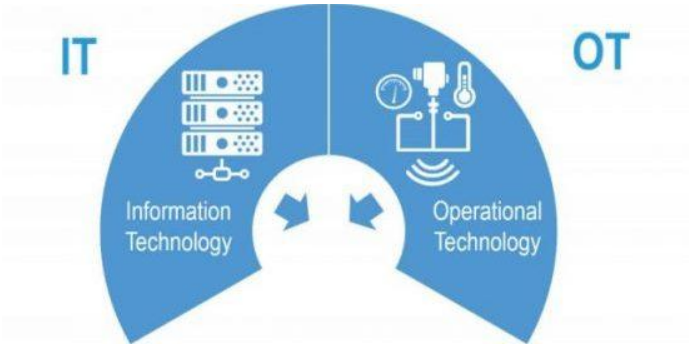
Index

Index


FPGA-based SOFT-PROCESSORS: 6G, SEC
Challenges
Limitations
Architectures
Solutions
Future work

Challenges

- Convergence of Operational and Information Technologies
  - **OT :** safety critical and real-time (RT), which means requiring, guaranteed extra-functional properties as **real-time behavior**, reliability, availability, industry-specific safety standards, and **security**
  - **IT :** such as Cloud Computing and Service Oriented Architecture. Cannot offer the properties required from the OT level

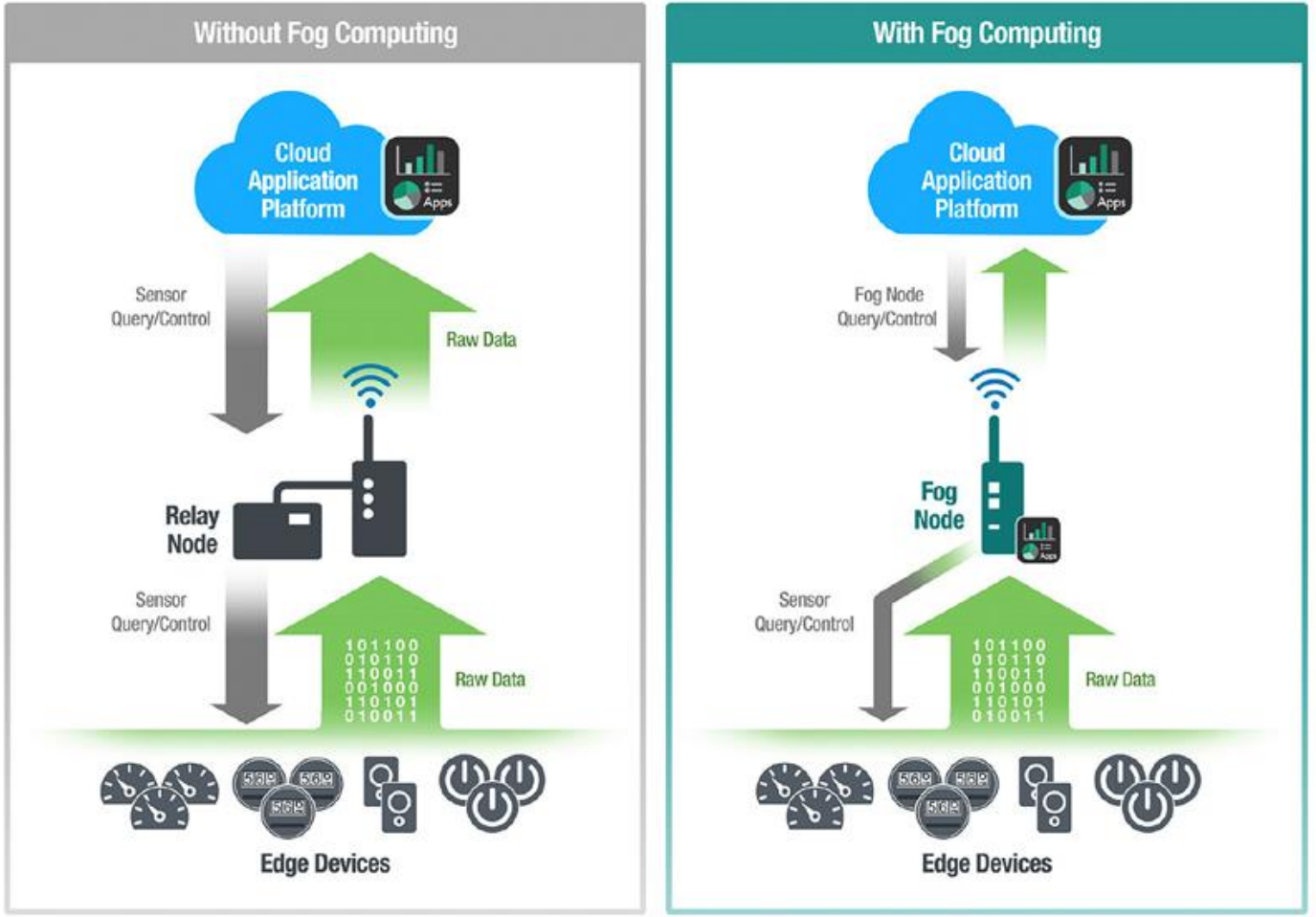


Challenges

- The devices send all the information to a centralized authority, which processes the data
  - Latency
  - Heavy workload at the cloud side (limitations and availability)
  - Privacy (sec)
- A platform, which enables the computation, communication and storage closer to the network is required
- Middleware will further facilitate the ’things’ to realize their potentials
  - Industrial automation, robotics or autonomous vehicles, where real-time decision making by using machine learning approaches is crucial

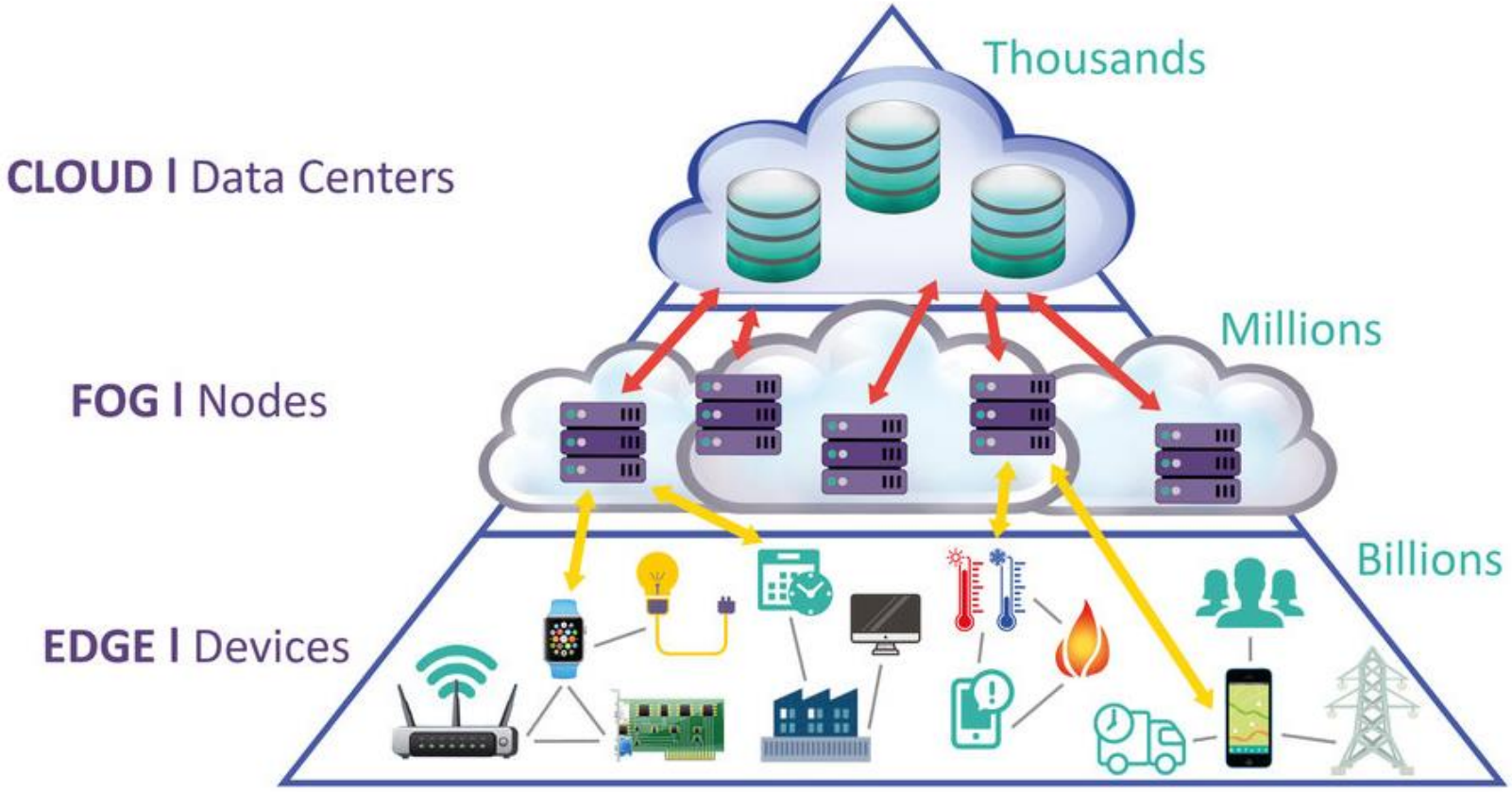
Qian, Jia & Sengupta, Sayantan & Hansen, Lars. (2019). Active Learning Solution on Distributed Edge Computing.

Challenges



https://www.moxa.com

Challenges



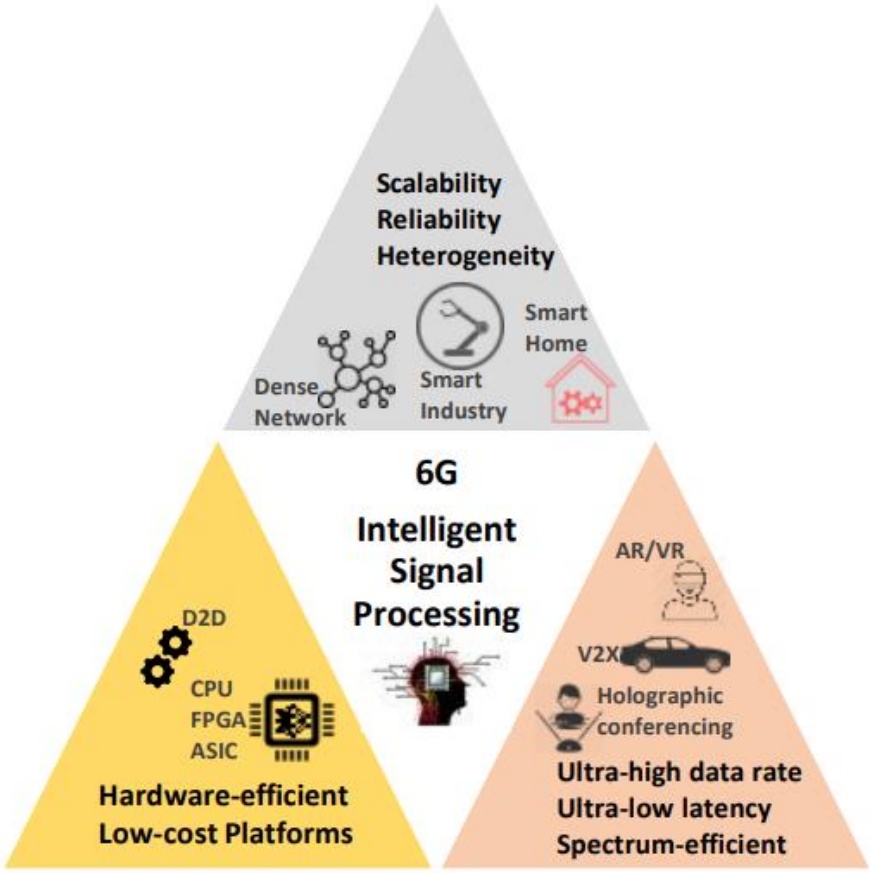
Qian, Jia & Sengupta, Sayantan & Hansen, Lars. (2019). Active Learning Solution on Distributed Edge Computing.

Challenges

- The emerging communication requirements for 6G are:
  - Ultra-low (undetectable ~ 0.1ms) latency with very high reliability (10^{-9} frame error rate)
  - Intelligent adaptive radio with Machine Learning (ML) on the edge
  - Very high energy efficiency (~ 1pJ/bit) to reduce the overall network energy consumption
  - Cost-efficient computational platforms such as FPGA, ASIC.

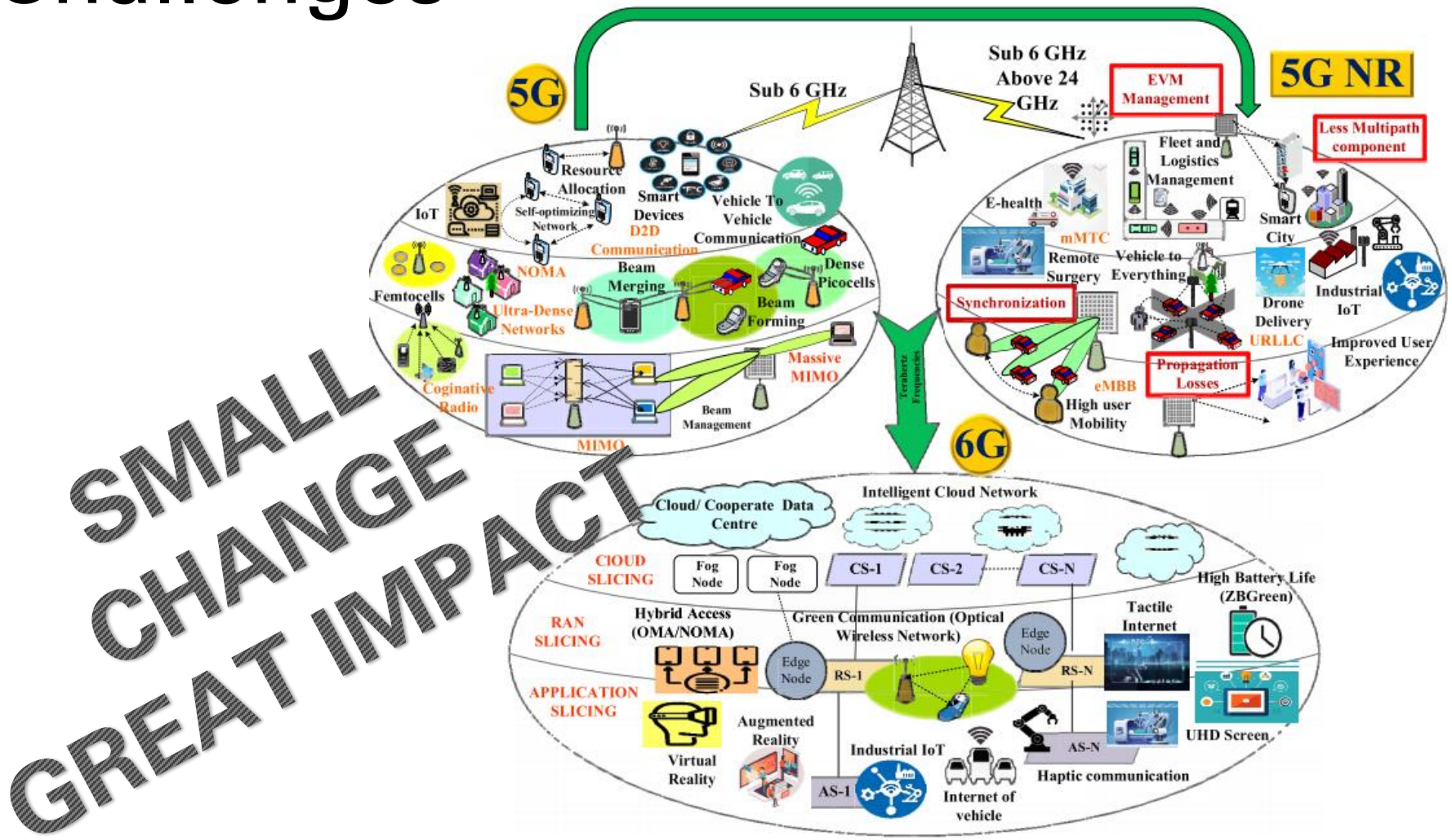
E. Calvanese Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Kténas, N. Cassiau, and C. Dehos, “6G: The Next Frontier,” arXiv e-prints, p. arXiv:1901.03239, Jan. 2019.

Challenges



Jagannath, Anu & Jagannath, Jithin & Melodia, Tommaso. (2020). Redefining Wireless Communication for 6G: Signal Processing Meets Deep Learning.

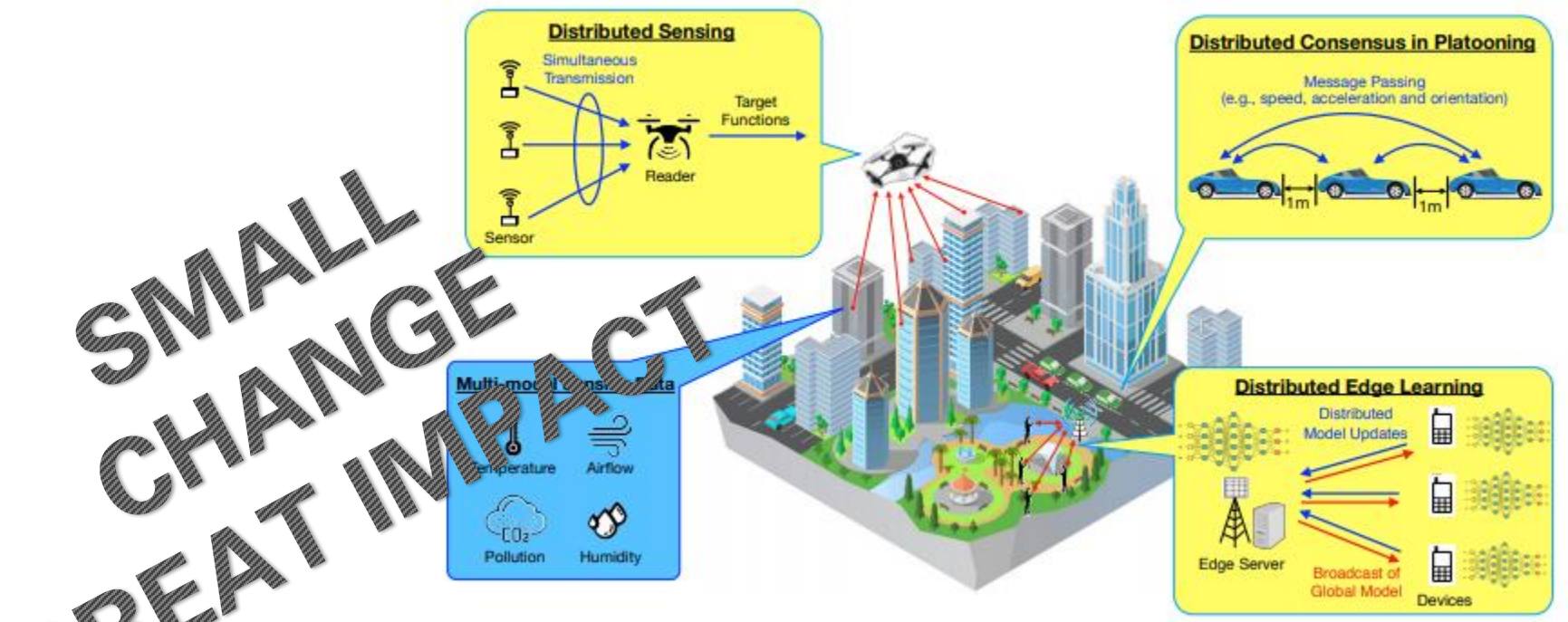
Challenges



SMALL CHANGE GREAT IMPACT

A. Dogra, R. K. Jha and S. Jain, "A Survey on Beyond 5G Network With the Advent of 6G: Architecture and Emerging Technologies," in IEEE Access, vol. 9, pp. 67512-67547, 2021

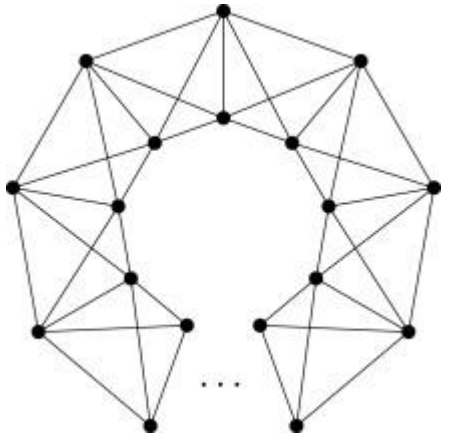
Challenges



Zhu, Guangxu & Xu, Jie & Huang, Kaibin. (2020). Over-the-Air Computing for 6G -- Turning Air into a Computer.

Challenges

INCREASE ACCURACY AND SECURITY



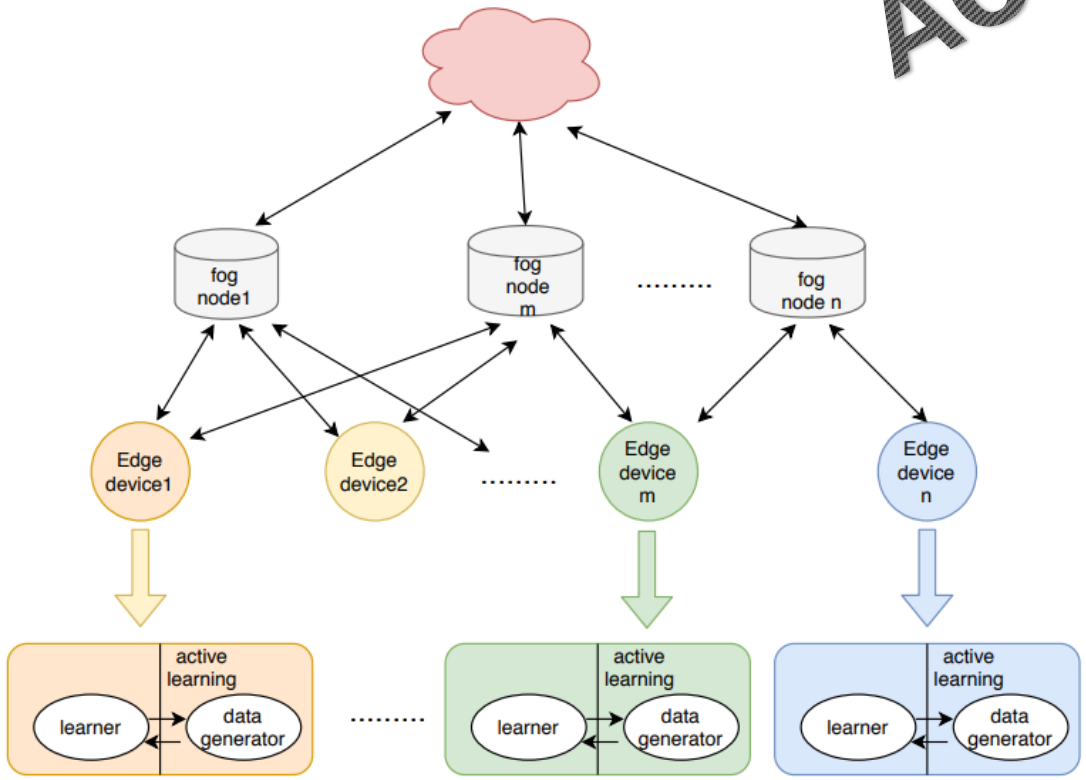
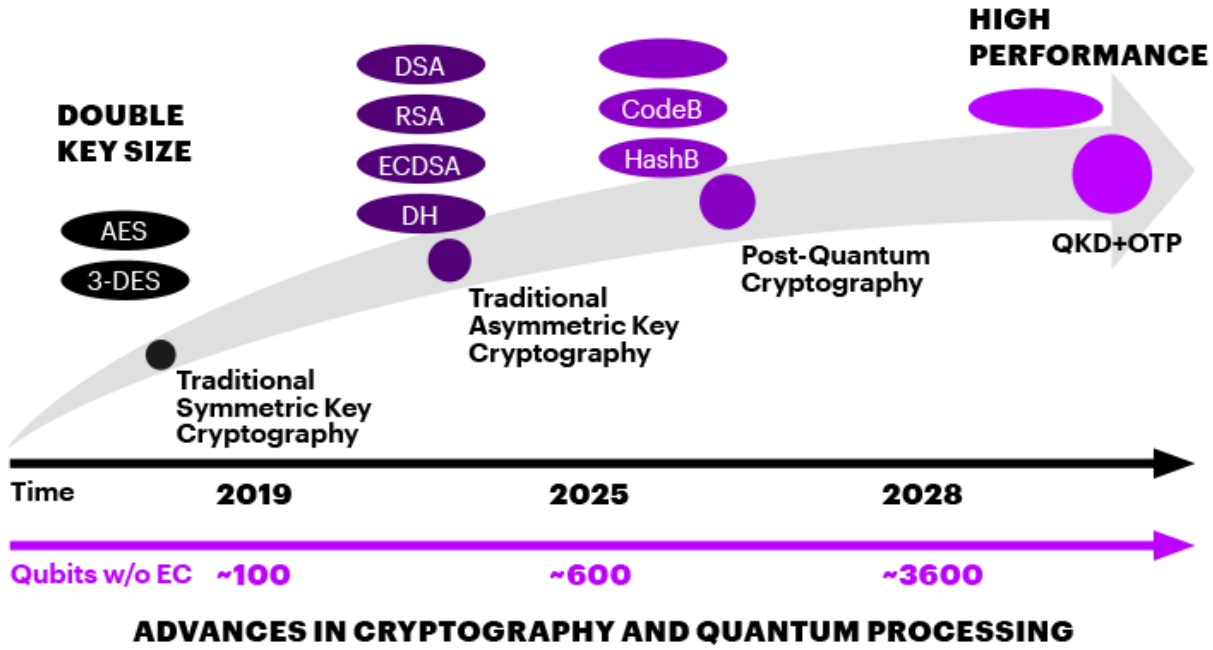


FIGURE 4. Timeline for future standardization events (copyright Accenture)



Challenges

China sends 'world's first 6G' test satellite into orbit

China has successfully launched what has been described as "the world's first 6G satellite" into space to test the technology.

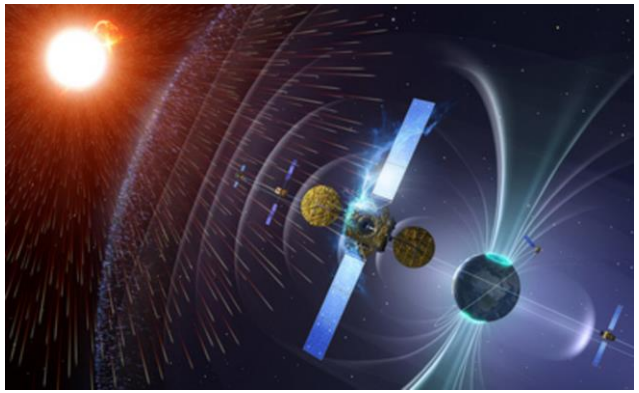
It went into orbit along with 12 other satellites from the Taiyuan Satellite Launch Center in the Shanxi Province.

The telecoms industry is still several years away from agreeing on 6G's specifications, so it is not yet certain the tech being trialled will make it into the final standard.

It involves use of high-frequency terahertz waves to achieve data-transmission speeds many times faster than 5G is likely to be capable of.

The satellite also carries technology which will be used for crop disaster monitoring and forest fire prevention.

7 November 2020 | BBC News | China



FAULTY

6G in the Sky: On-Demand Intelligence at the Edge of 3D Networks

Emilio Calvanese Strinati[1] | Sergio Barbarossa[2] | Taesang Choi[3] | Antonio Pietrabissa[5] | Alessandro Giuseppi[5] | Emanuele De Santis[5] | Josep Vidal[4] | Zdenek Becvar[6] | Thomas Haustein[7] | Nicolas Cassiau[1] | Francesca Costanzo[2] | Junhyeong Kim[3] | Ilgyu Kim[3]

[1]CEA-Leti, MINATEC Campus, Grenoble, France
[2] Sapienza University of Rome, DIET, via Eudossiana 18, 00184 Rome, Italy
[3]Telecommunications & Media Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea
[4]Dept Signal Theory and Communications, Universitat Politecnica de Catalunya, Jordi Girona 31, 08034 Barcelona, Spain
[5]University of Rome "La Sapienza" and Space Research Group of CRAT, Via Ariosto 25, 00185, Roma, Italy
[6]Faculty of Electrical Engineering, Czech Tecnical University in Prague, Technicka 2, 16627 Prague, Czech Republic
[7]Wireless Communications and Networks, Fraunhofer HHI, Einsteinufer 37, 10587 Berlin, Germany

Correspondence
*Corresponding author: Emilio Calvanese Strinati, Email: emilio.calvanese-strinati@cea.fr

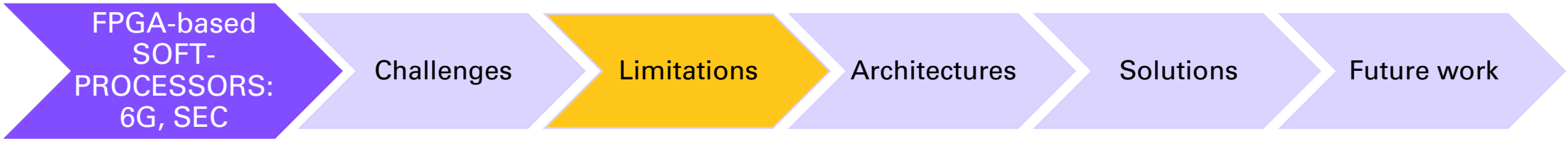
Funding Information
This research was supported by the European Union in the Horizon 2020 EU-Korea project 5G-ALLSTAR, GA no. 815323, by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT No. 2018-0-00175), and by Grant No. P102-18-27023S funded by Czech Science Foundation.

Abstract

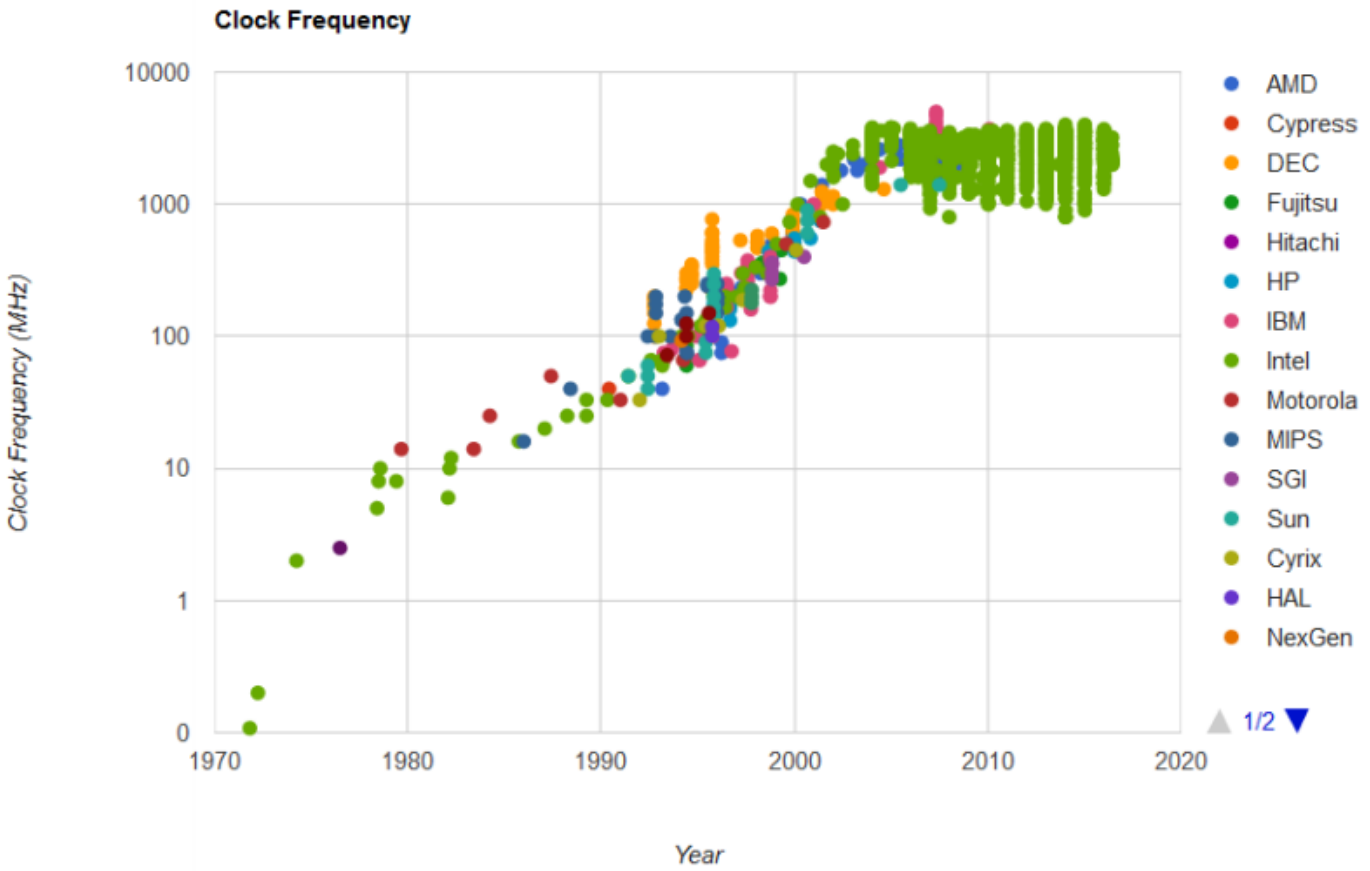
6G will exploit satellite, aerial and terrestrial platforms jointly to improve radio access capability and to unlock the support of on-demand edge cloud services in the three dimensional space (3D) by incorporating Mobile Edge Computing (MEC) functionalities on aerial platforms and low orbit satellites. This will extend the MEC support to devices and network elements in the sky and will forge a space borne MEC enabling intelligent personalized and distributed on demand services. 3D end users will experience the impression of being surrounded by a distributed computer fulfilling their requests in apparently zero latency. In this paper, we consider an architecture providing communication, computation, and caching (C3) services on demand, anytime and everywhere in 3D space, building on the integration of conventional ground (terrestrial) base stations and flying (non-terrestrial) nodes. Given the complexity of the overall network, the C3 resources and the management of the aerial devices need to be jointly orchestrated via AI-based algorithms, exploiting virtualized networks functions dynamically deployed in a distributed manner across terrestrial and non-terrestrial nodes.

KEYWORDS:
6G, 5G, B5G, Non-Terrestrial Communications, UAV, Satellite, HAPS, MEC, 3D services, 3D connectivity.

Index


FPGA-based SOFT-PROCESSORS: 6G, SEC
Challenges
Limitations
Architectures
Solutions
Future work

Limitations

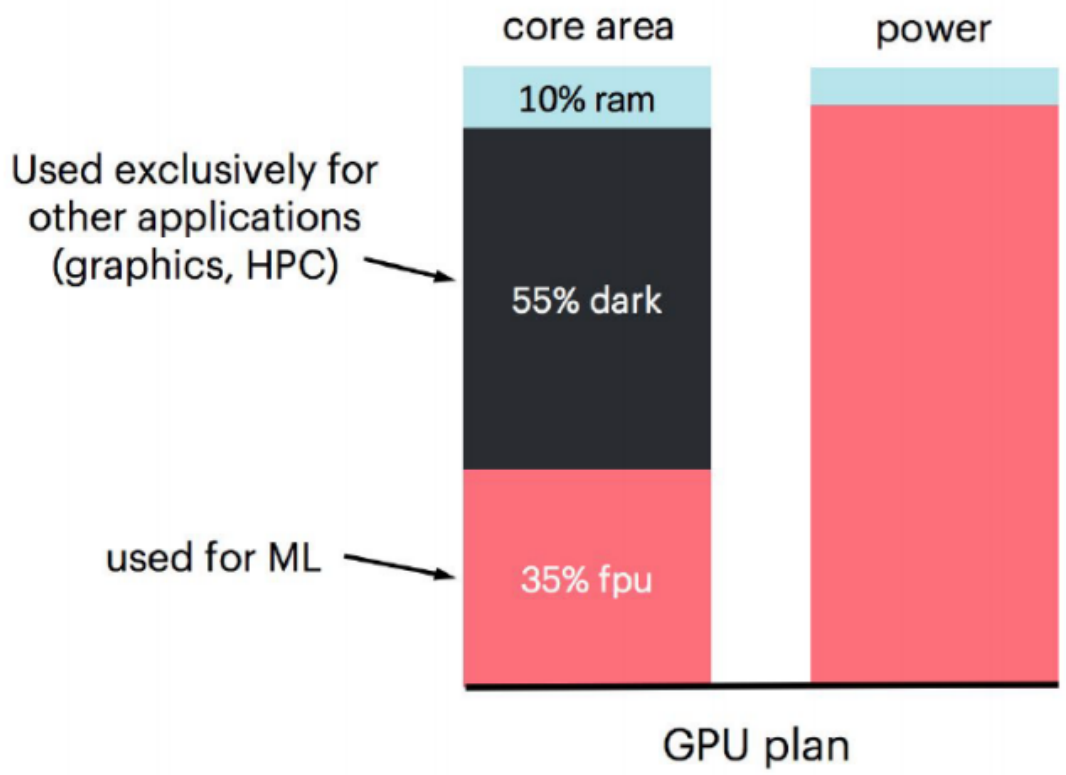


Stanford VLSI group, http://cpudb.stanford.edu/visualize/clock_frequency

Limitations

Why not GPUs for AI and ML?

GPUs were built for graphics workloads and *evolved* for high performance computing and AI workloads



https://cdn2.hubspot.net/hubfs/729091/NIPS2017/NIPS%2017%20-%20IPU.pdf?t=1513603679766

Limitations

- At Facebook data centers, the vast majority of online inference runs on the abundant 1xCPU (single-socket) or 2xCPU(dual-socket) production machines
- As more ML workloads are increasing, these expenses are staggering and Facebook has now started its open source compiler effort called GLOW(Graph LOWering) for enabling cheaper machine learning accelerators

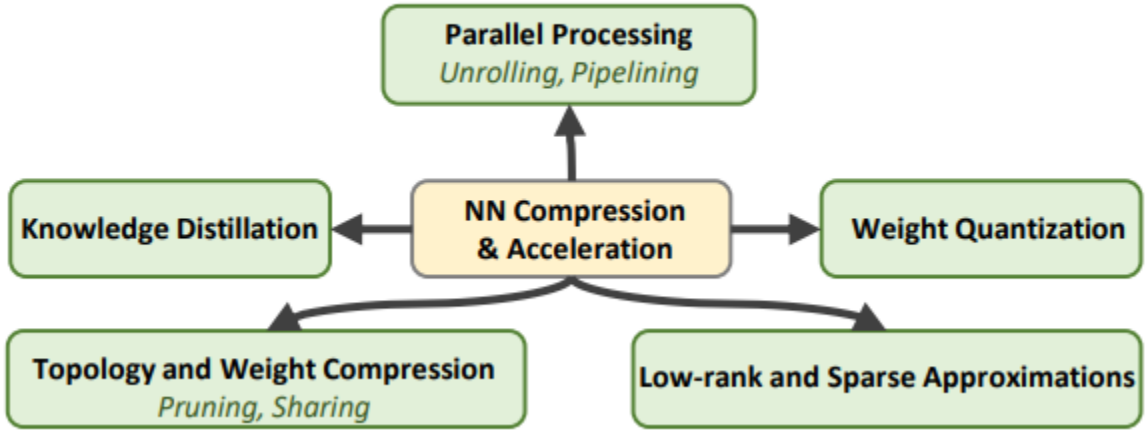
FACEBOOK AI

https://research.fb.com/wp-content/uploads/2017/12/hpca-2018-facebook.pdf

Limitations

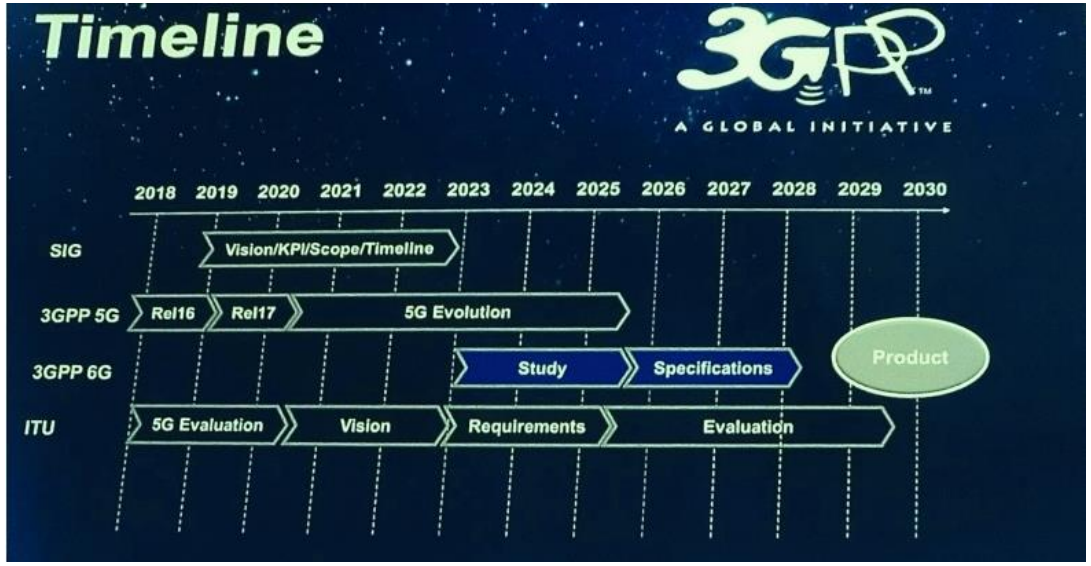
- The memory footprint of deep NN grows with the number of neurons and layers.
- This will become critical for memory-constrained platforms such as CPUs, FPGAs, ASICs, etc with only a few megabytes of memory.
  - Example, the ResNet-50 architecture with 50 convolutional layers requires 95 MB of memory for storage and over 3.8 billion floating-point multiplications when processing an image.
  - Such computationally intensive and memory extensive architectures cannot be directly implemented on embedded computational platforms.

Limitations



J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, and T. Melodia, "Neural networks for signal intelligence," in Machine Learning for Future Wireless Communications. John Wiley & Sons, Ltd, 2020, ch. 13, pp. 243–264.

Limitations



https://www.3gpp.org/

TIME

Finland selects IQM to build its first quantum computer; to deliver a 50-qubit machine by 2024.

https://www.meetiqm.com/

<<By the time, we make an ASIC, there will be new neural networks that won't be supported on that ASIC.>>

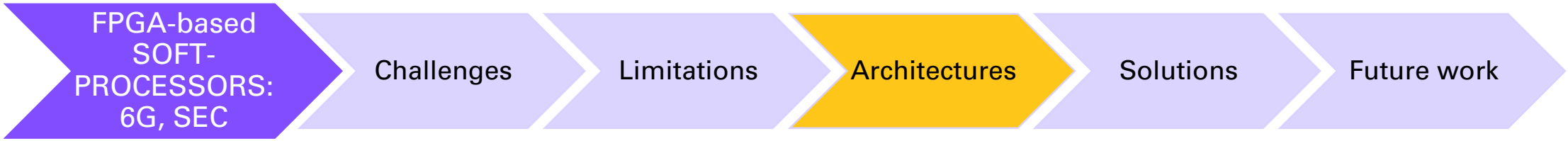
Western Digital®

Rigetti right now

Aspen-9		Median Time Duration (μs)		Median Fidelity (per op.)	
Deployed	07.02.21	T1 Lifetime	27	Single-qubit gates	99.8%
Qubits	31	T2 Lifetime	19	Two-qubit gates (CZ)	95.8%
				Two-qubit gates (XY)	95.4%

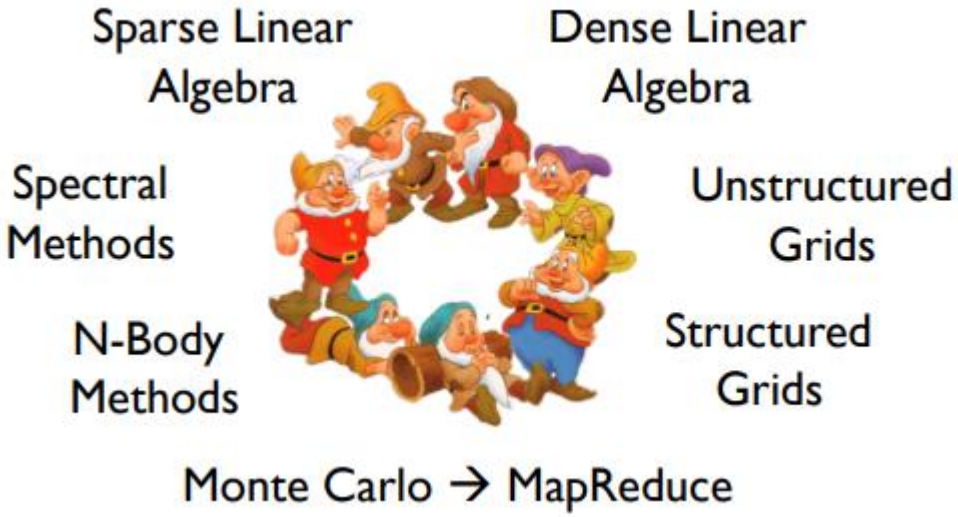
https://www.rigetti.com/

Index


FPGA-based SOFT-PROCESSORS: 6G, SEC
Challenges
Limitations
Architectures
Solutions
Future work

Approach

- A dwarf is an algorithmic method that captures a pattern of computation and communication
  - Methods important for science and engineering
- They decouple research, allowing analysis of programming support without waiting years for full application development



Computer Architecture is Back - The Berkeley View on the Parallel Computing Landscape, David Patterson, Krste Asanovíc, Kurt Keutzer, 2007

https://parlab.eecs.berkeley.edu/research/193

Approach

Crypto+AI

Vector ISA Goodness

- Reduced instruction bandwidth
- Reduced memory bandwidth
- Lower energy
- Exposes DLP
- Masked execution
- Gather/Scatter
- From small to large VPU

RISC-V Vector Extension

- Small
- Natural memory ordering
- Masks folded into vregs
- Scalar, Vector & Matrix
- Typed registers (extension)(*)
- Reconfigurable
- Mixed-type instructions
- Common Vector/SIMD programming model
- Fixed-point support
- Easily Extensible
- Best vector ISA ever ☺

Domains

- Machine Learning
- Graphics
- DSP
- Crypto
- Structural analysis
- Climate modeling
- Weather prediction
- Drug design
- And more…

Architectures

FEATURES COMPARISON OF SOFT-CORES

Category	Microblaze	LEON3	OpenRISC1200	OpenFire	AeMB	MB Lite
Maximum Frequency (MHz)	250	400/183 (ASIC/FPGA)	300/185 (ASIC/FPGA)	198	136	229
Interface	FSL, OPB, PLB, LMB	AMBA 2.0	Wishbone	OPB, FSL	Wishbone	Wishbone
Pipeline (Stages)	7-stages	7-stages	5-stages	3-stages	3-stages	5-stages
Architecture	Microblaze	Sparc V8	ORBIS	MicroBlaze	MicroBlaze	MicroBlaze
Language	VHDL	VHDL	Verilog	Verilog	Verilog	VHDL
Implementation	FPGA	FPGA/ASIC	FPGA/ASIC	FPGA	FPGA	FPGA
Address/ Data Bus	32-bits	32-bits	32/64-bits	32-bits	32-bits	32-bits

M. Makni, M. Baklouti, S. Niar, M. W. Jmal and M. Abid, "A comparison and performance evaluation of FPGA soft-cores for embedded multi-core systems," 2016 11th International Design & Test Symposium (IDT), 2016, pp. 154-159, doi: 10.1109/IDT.2016.7843032.

Less vulnerable to obsolescence

Some Candidates...

A2I
A2O
AEMB
Amber
ao486
ARC
BERI
Chiselwatt
Cortex-M1
CPU86
Dossmatik
ERIC5
f32c
H2 CPU
Instant SoC
JOP
LatticeMico32
LatticeMico8
LEON2(-FT)
LEON3/4
Libre-SOC
LXP32
MCL51
MCL65
MCL86
MicroBlaze
Microwatt
MRISC32-A1
Navré
NEO430
NEORV32
Nios, Nios II
OpenFire
OpenPiton
OpenRISC
OpenSPARC T1
Other architectures
PacoBlaze
pAVR
PicoBlaze
PowerPC 405S
PowerPC 440S
PowerPC 470S
RISC5
s80x86
SecretBlaze
SpartanMC
SYNPIC12
Tacus/PIPE5
TSK3000A
TSK51/52
VexRiscv
xr16
YASEP
Zet
ZipCPU
ZPU

Architectures

Gartner's Report on RISC-V momentum in IoT and business environments

→ READ THE REPORT

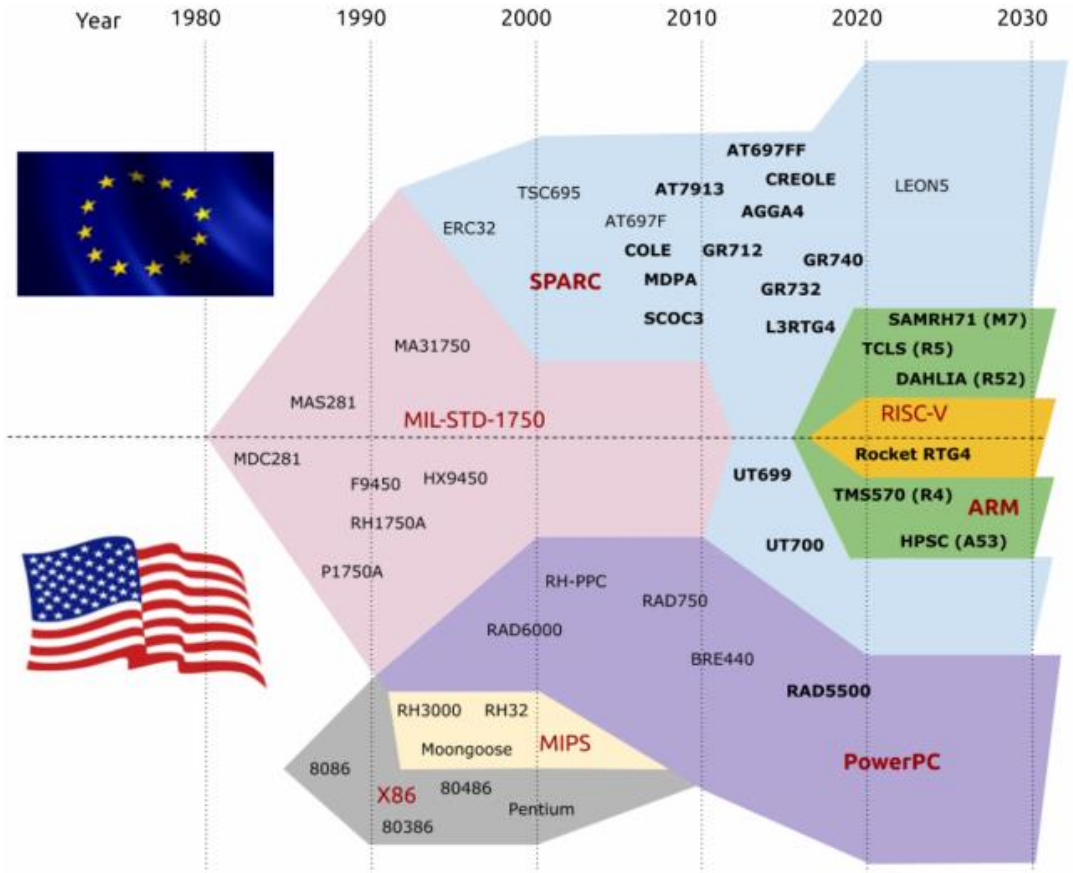
INDUSTRY SUPPORT

Gartner

Attributions for Gartner Research Documents:
Gartner, Market Trends: Custom ICs Based on RISC-V Will Enable Cost-Effective IoT Product Differentiation, Amy Teng, 5 June 2020

https://www.gartner.com

Architectures



Di Mascio, S., Menicucci, A., Furano, G., Monteleone, C., and Ottavi, M., “The Case for RISC-V in Space,” Applications in Electronics Pervading Industry, Environment and Society, Apple Pies, 2018, edited by S. Saponara, and A. De Gloria, Vol. 550, Lecture Notes in Electrical Engineering, Springer, Cham, 2019, pp. 319–325

Architectures

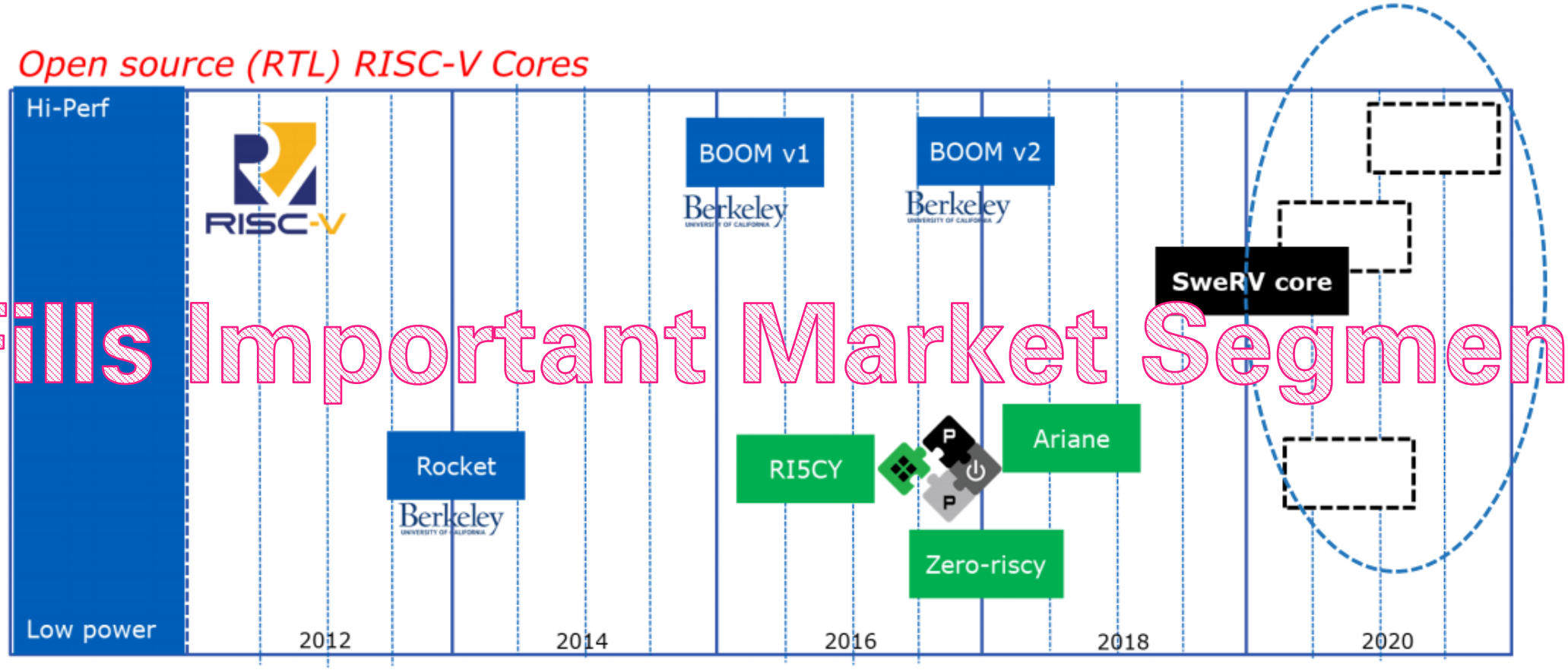
GREAT COMMUNITY

COMPUTING, OPEN SOURCE, RISC-V, TECHNOLOGY AND STRATEGY

Driving to Data-Centric Architectures and 1B RISC-V Cores

https://www.westerndigital.com/company/innovations/risc-v

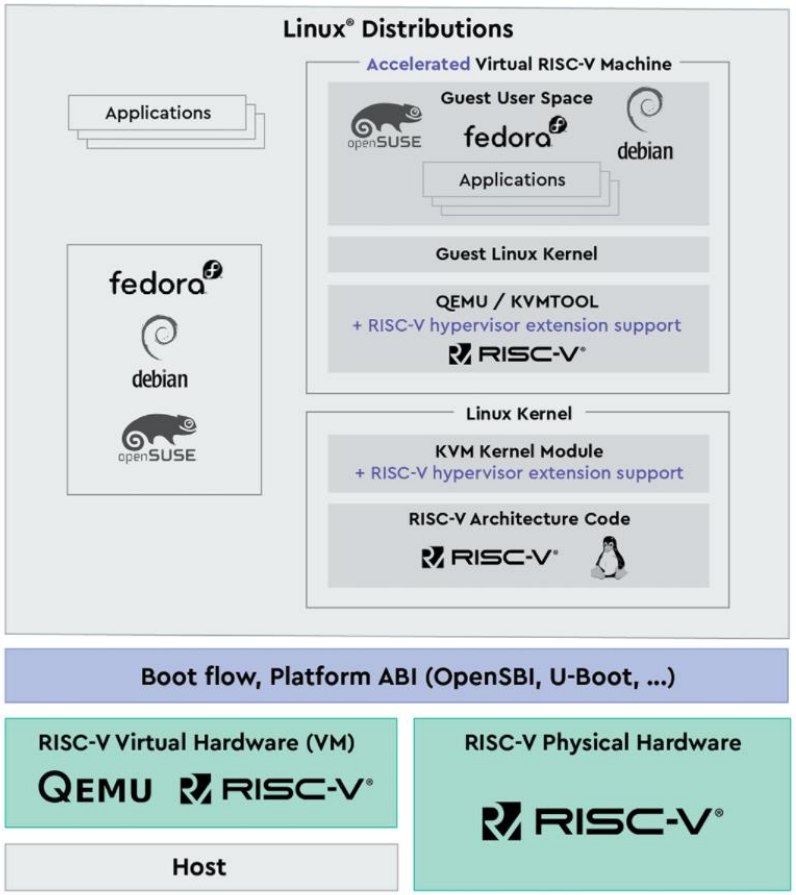
Architectures

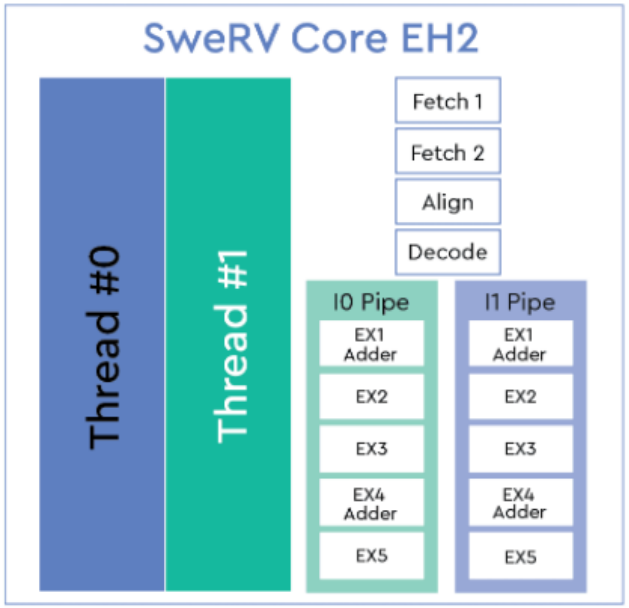


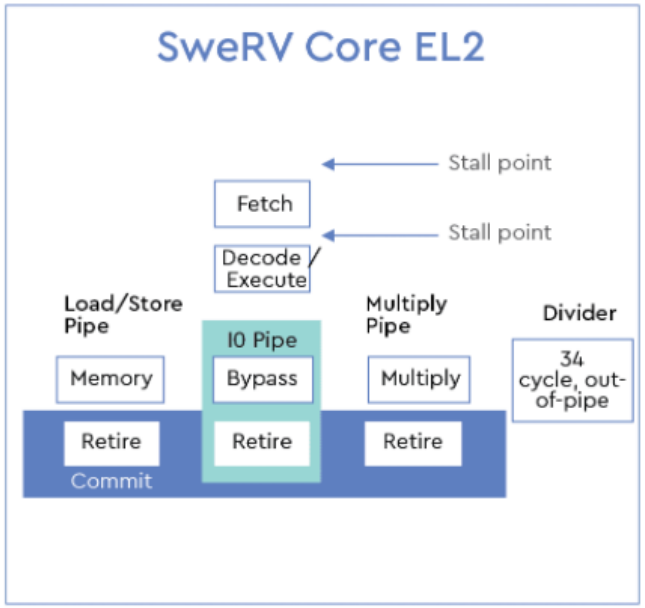
Fills Important Market Segments

https://chipsalliance.org/

Architectures

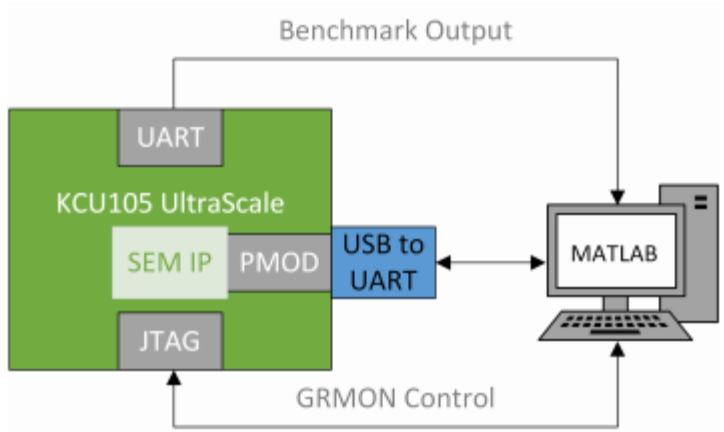






https://www.westerndigital.com/company/innovations/risc-v

Architectures



electronics

MDPI

Article

Analysis of the Critical Bits of a RISC-V Processor Implemented in an SRAM-Based FPGA for Space Applications

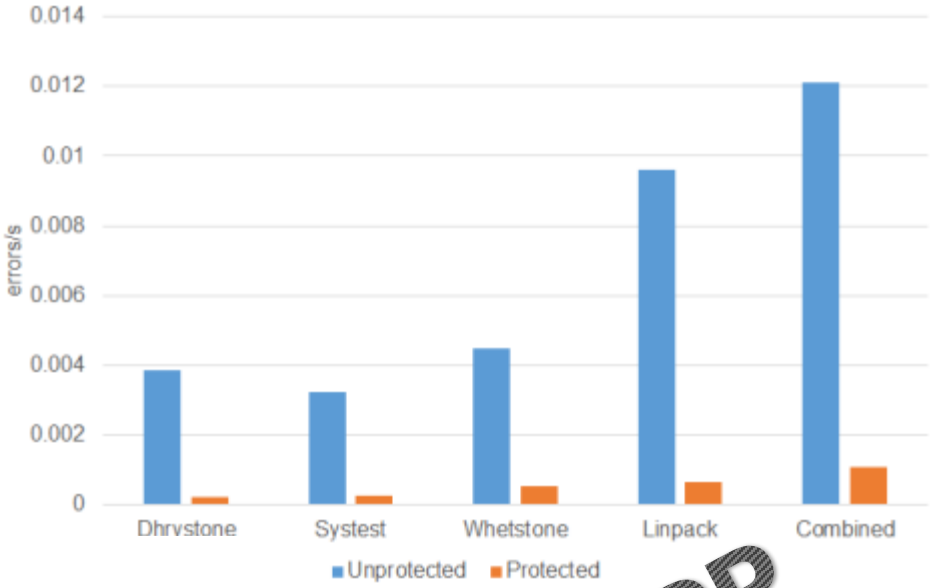
Luis Alberto Aranda [1,*], Nils-Johan Wessman [2], Lucana Santos [3], Alfonso Sánchez-Macián [1], Jan Andersson [2] and Roland Weigand [3] and Juan Antonio Maestro [1]

1 ARIES Research Center, Universidad Antonio de Nebrija, Pirineos 55, 28040 Madrid, Spain; asanchep@nebrija.es (A.S.-M.); jmaestro@nebrija.es (J.A.M.)
2 Cobham Gaisler, Kungsgatan 12, SE-411 91 Göteborg, Sweden; nisse@gaisler.com (N.-J.W.); jan@gaisler.com (J.A.)
3 European Space Agency, Keplerlaan 1, P.O. Box 299, 2220AG Noordwjik ZH, The Netherlands; lucana.santos@esa.int (L.S.); roland.weigand@esa.int (R.W.)
* Correspondence: laranda@nebrija.es

UNIVERSIDAD NEBRIJA

esa

COBHAM
Cobham Gaisler AB



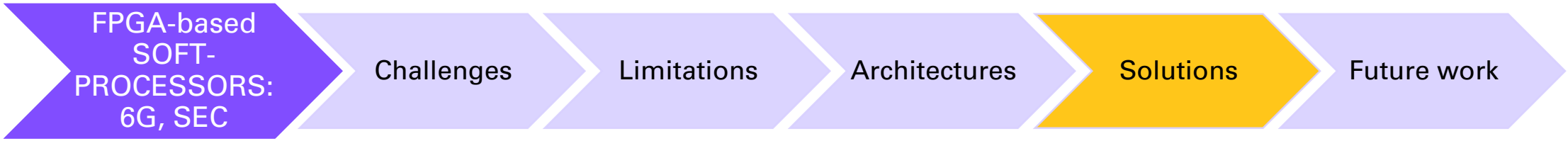
Availability

NOEL-V is part of the GRLIB IP Library from release 2020.2 There are also pre-built FPGA development board bitstreams available. Additional features for the NOEL-V processor will become available as part of milestone releases. The table below shows the planned milestones. Please note that the future milestone features and dates are tentative.

Milestone	Description	Date
v5	The v5 release adds fault-tolerance features and performance improvements: - Release of fault-tolerance support - FT adaptations to specific target technologies. - C extension - H extension	2021-Jul

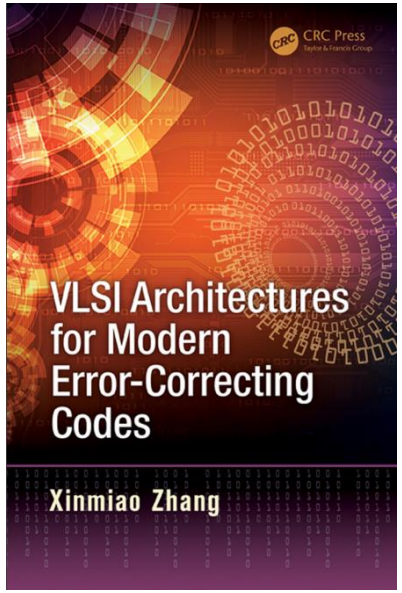
SPACE APP

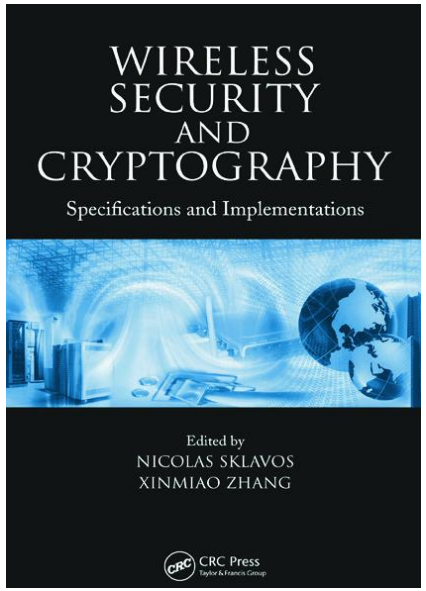
Index

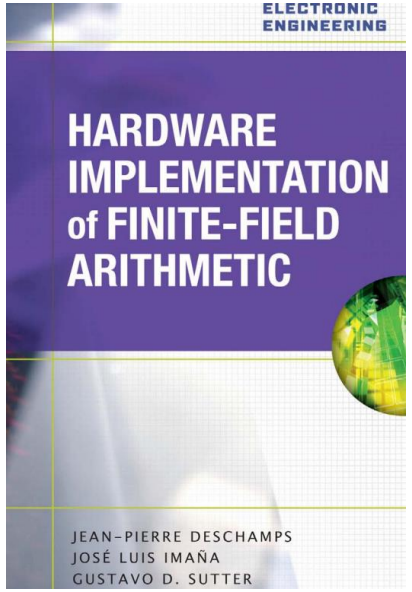

FPGA-based SOFT-PROCESSORS: 6G, SEC
Challenges
Limitations
Architectures
Solutions
Future work

Solutions

- Common operations and functions in Crypto and ECC





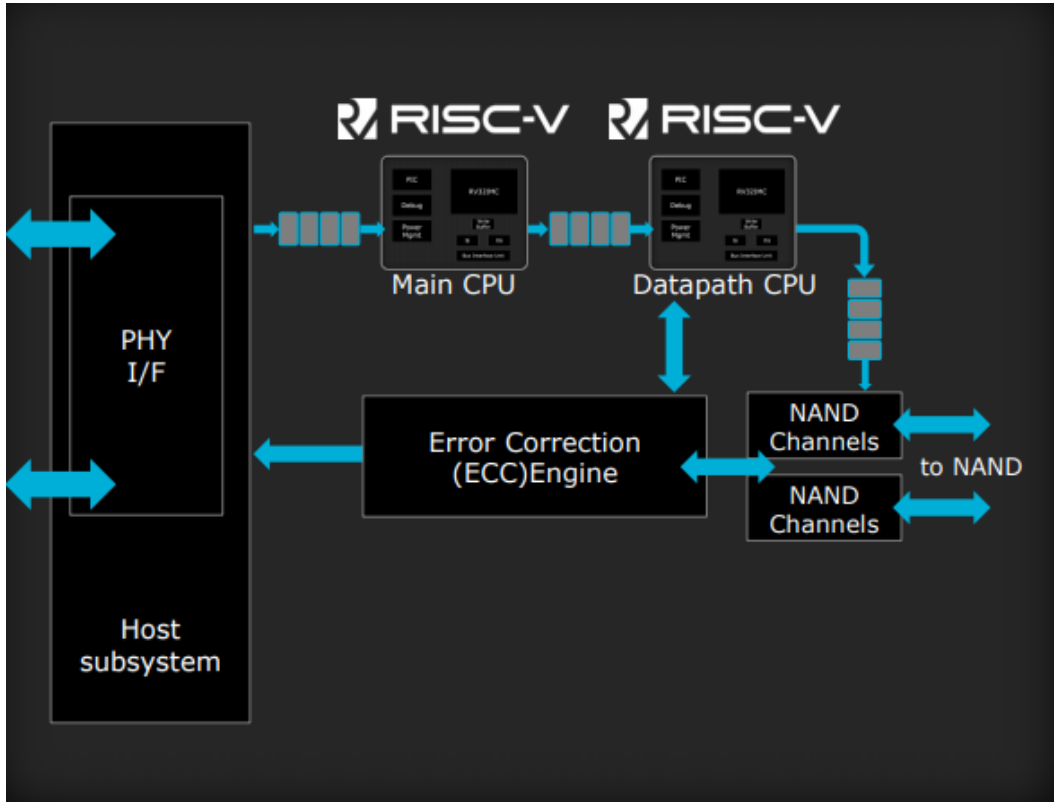


Solutions

- Common operations and functions in Crypto and ECC

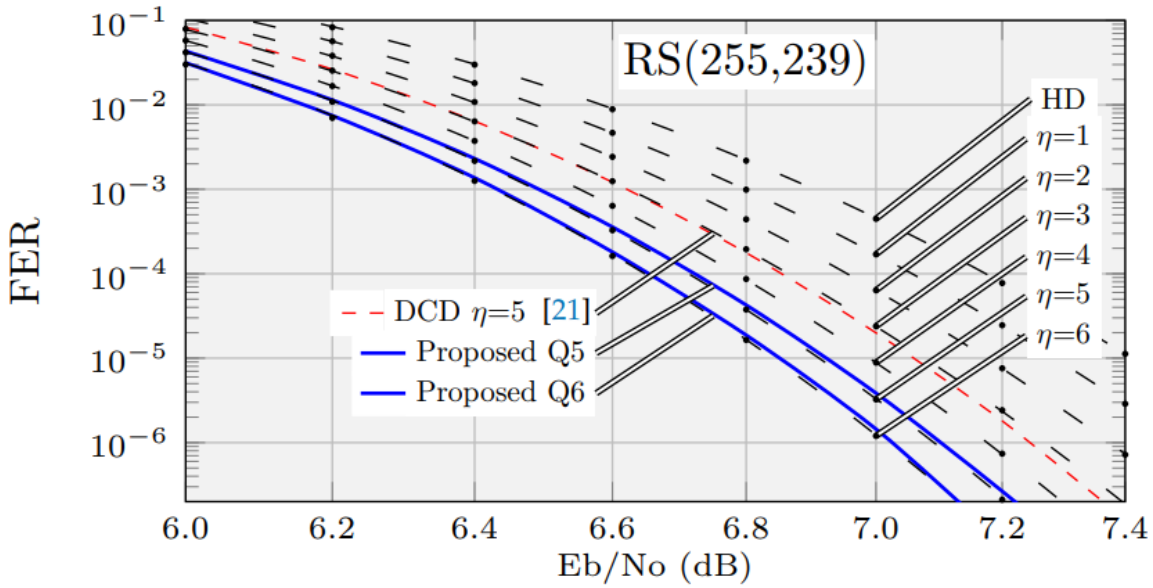
Multi-purpose SoC for consumer SSD applications

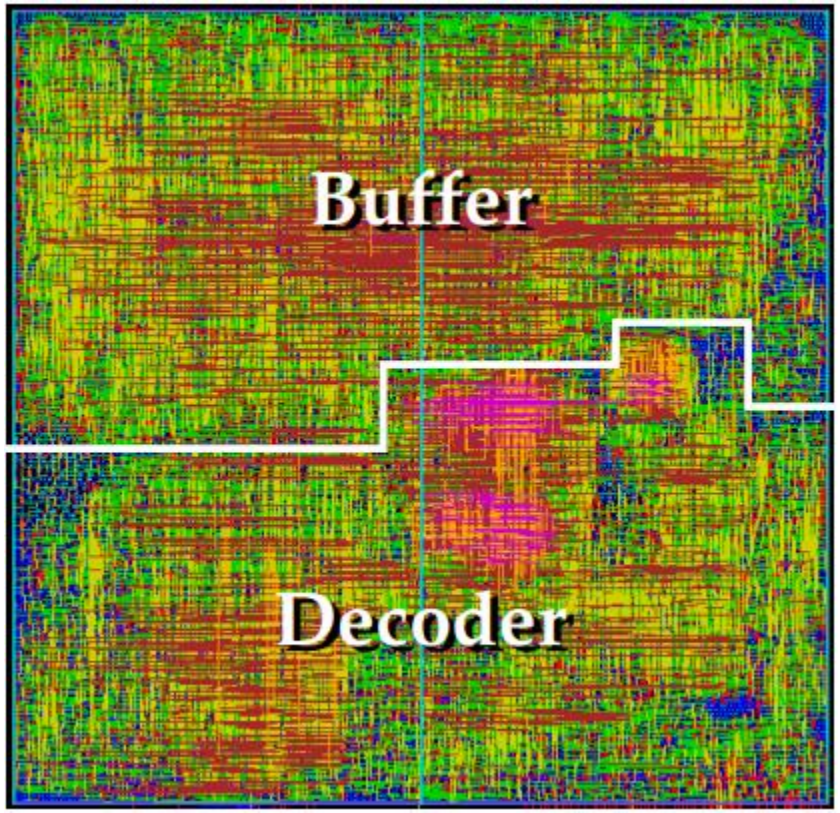
Freedom of power and performance optimization for end application



Solutions

- ECC classical solution





Torres, V.; Valls, J.; Canet, M.J.; García-Herrero, F. Soft-Decision Low-Complexity Chase Decoders for the RS(255,239) Code. *Electronics* 2019, *8*, 10.

Solutions

- Crypto: not only classical but post-quantum
  - Support for different algebraic models (not for different applications)

Encryption / KEMs	Arithmetic
Crystals-Kyber	GF(q), NTT, ring
Classic McEliece	GF(2^m)
NTRU	GF(q), NTT, ring
SABER	GF(q), NTT, ring
BIKE	GF(2^m)
FrodoKEM	GF(q)
HQC	GF(2^m)
NTRU Prime	GF(q), NTT, ring
SIKE	GF(q)

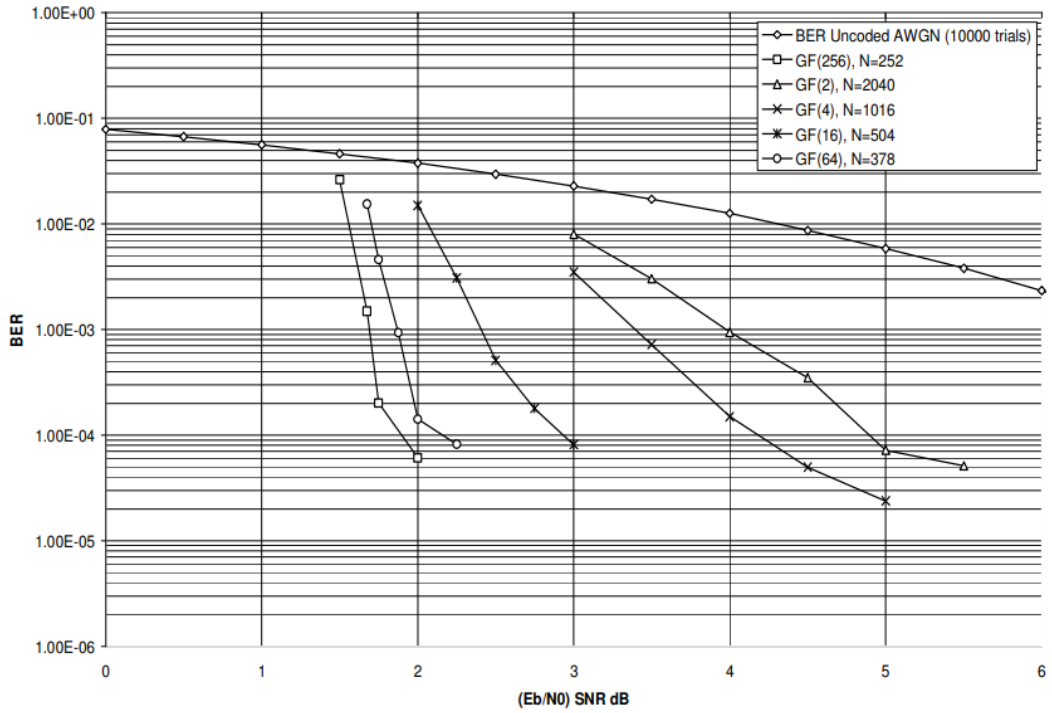
Alkim, E., Evkan, H., Lahr, N., Niederhagen, R., & Petri, R. (2020). ISA Extensions for Finite Field Arithmetic Accelerating Kyber and NewHope on RISC-V. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, *2020* (3), 219-242

E. Karabulut and A. Aysu, "RANTT: A RISC-V Architecture Extension for the Number Theoretic Transform," *2020 30th International Conference on Field-Programmable Logic and Applications (FPL)*, 2020, pp. 26-32

Solutions

- Crypto: not only classical but post-quantum
  - Flexibility for inside each algebraic model to support future changes

V. S. Ganepola, R. A. Carrasco, I. J. Wassell and S. Le Goff, "Performance study of non-binary LDPC Codes over GF(q)," 2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing, 2008, pp. 585-589



Solutions

Small World Communications

LCD01C CCSDS (8160,7136) LDPC Decoder

4 April 2015 (Version 1.07) — Product Specification

LCD01C Features

LDPC Decoder

- CCSDS compatible
- Rate 223/255 (8160,7136)
- Includes ping–pong input and output memories
- Up to 225 MHz internal clock
- Up to 1.6 Gbit/s with 10 decoder iterations
- 6–bit sign–magnitude input data
- Up to 64 iterations
- Scaled min–sum decoding algorithm
- Optional power efficient early stopping
- Parity check output
- Xilinx LUTs: 30.5K Virtex–4, 29.1K Virtex–5, 29.5K Virtex–6 and 7–Series, 166 18KB Block-RAMs. Altera ALUTs 26.8K, 166 M9Ks
- Free simulation software

- Available as EDIF core and VHDL simulation core for Xilinx Virtex–II, Spartan–3, Virtex–4, Virtex–5, Virtex–6, Spartan–6 and 7–Series FPGAs under SignOnce IP License. Actel, Altera and Lattice FPGA cores available on request.
- Available as VHDL core for ASICs

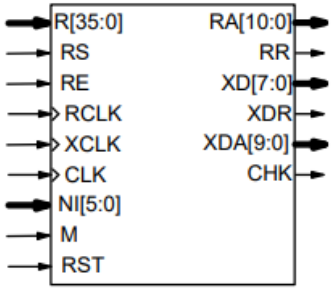
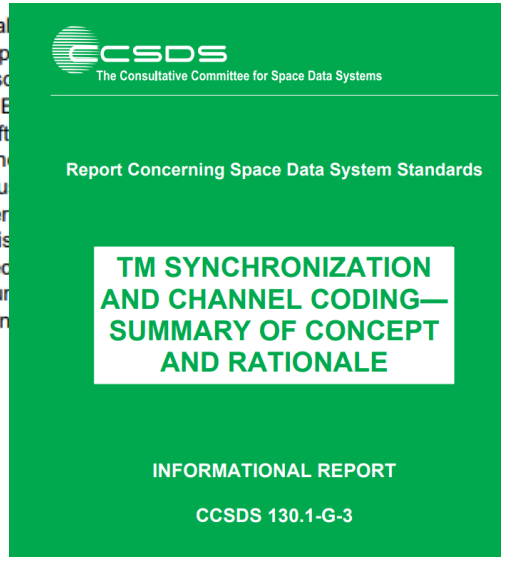
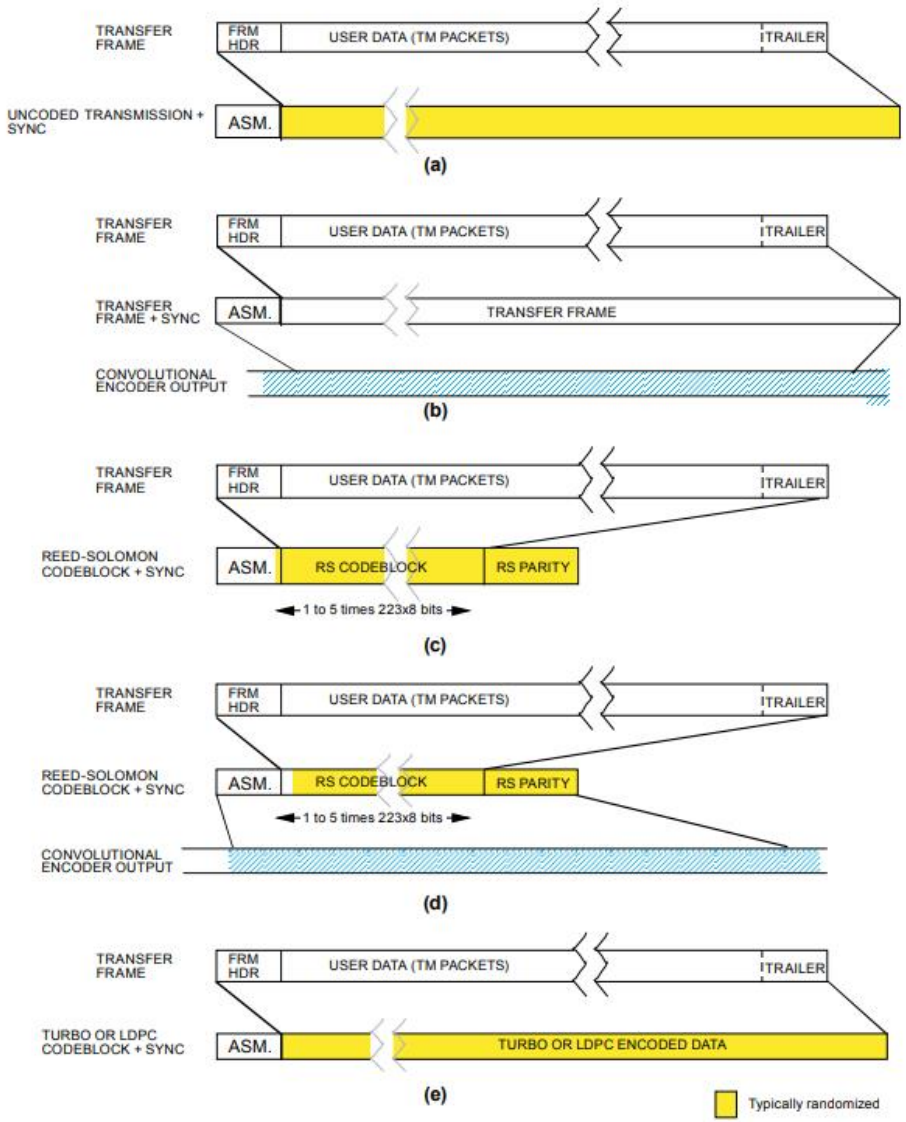


Figure 1: LCD01C schematic symbol.

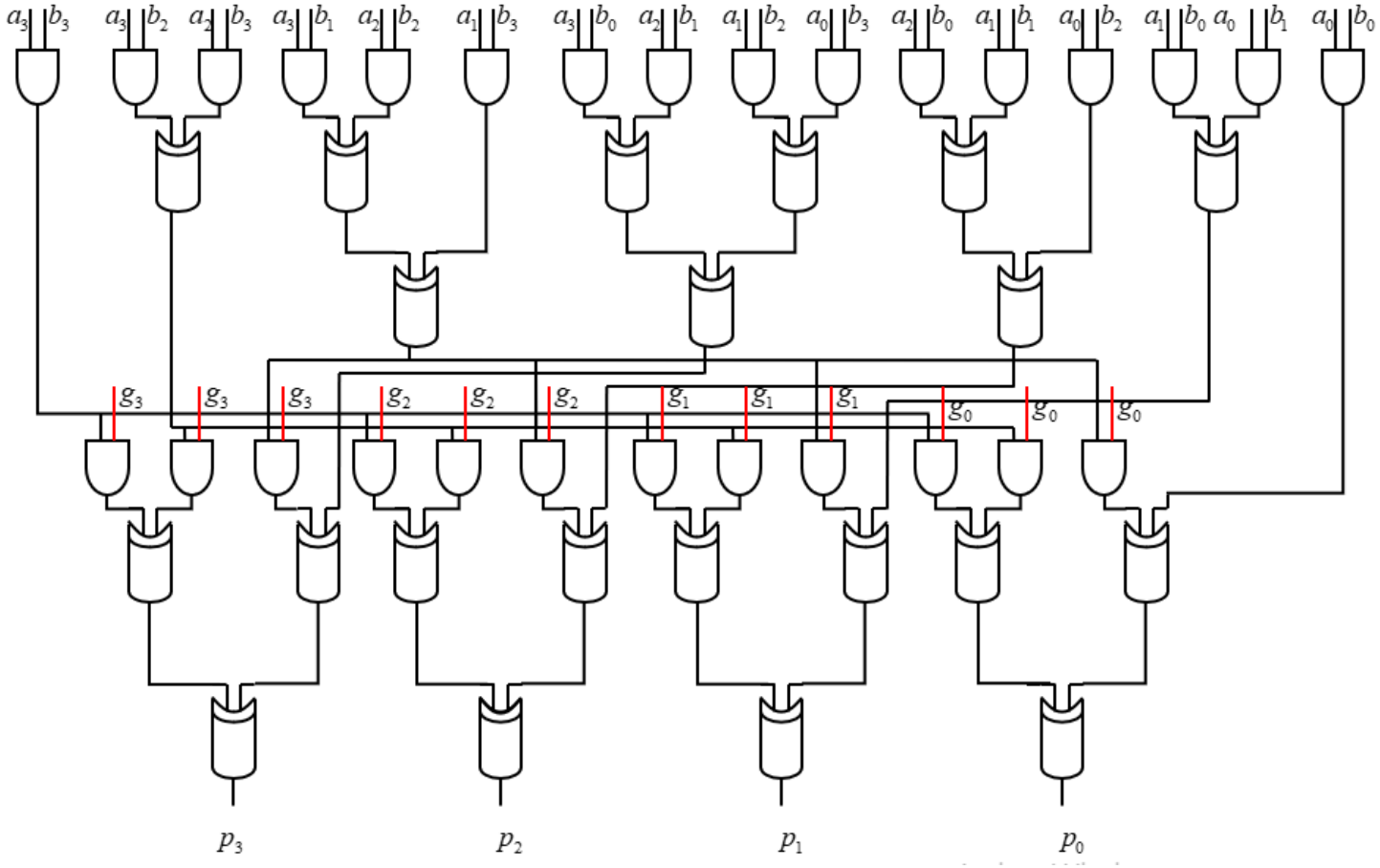
can be performed in paral
are used to buffer the inp
Figure 1 shows the sc
LCD01C decoder. The E
with Xilinx Integrated Soft
software to implement th
The VHDL core can be u
Table 1 shows the per
various Xilinx parts. T_{cp} is
riod over recommended
These performance figur
device utilisation and con





(a) uncoded transmission
(b) convolutional code only
(c) RS code only
(d) concatenated RS and convolutional
(e) Turbo or LDPC code[1]

Solutions



m	
3	$1+X+X^3$
4	$1+X+X^4$
5	$1+X^2+X^5$
6	$1+X+X^6$
7	$1+X^3+X^7$
8	$1+X^2+X^3+X^4+X^8$
9	$1+X^4+X^9$
10	$1+X^3+X^{10}$
11	$1+X^2+X^{11}$
12	$1+X+X^4+X^6+X^{12}$
13	$1+X+X^3+X^4+X^{13}$

m	
14	$1+X+X^6+X^{10}+X^{14}$
15	$1+X+X^{15}$
16	$1+X+X^{3+}X^{12}+X^{16}$
17	$1+X^3+X^{17}$
18	$1+X^7+X^{18}$
19	$1+X+X^{2+}X^5+X^{19}$
20	$1+X^3+X^{20}$
21	$1+X^2+X^{21}$
22	$1+X+X^{22}$
23	$1+X^5+X^{23}$
24	$1+X+X^{2+}X^7+X^{24}$

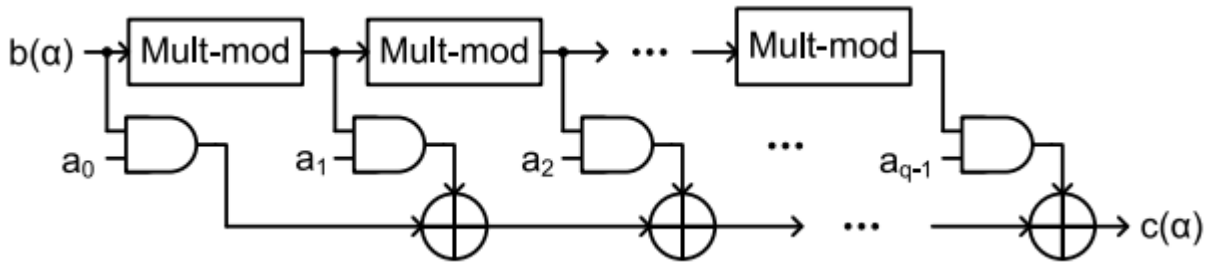
NOT GENERALIZABLE

Galois Field Multiplier GF(2^m), with m=4

Solutions

Power representation vs. polynomial representation for elements of $GF(2^4)$ constructed using $p(x) = x^4 + x + 1$

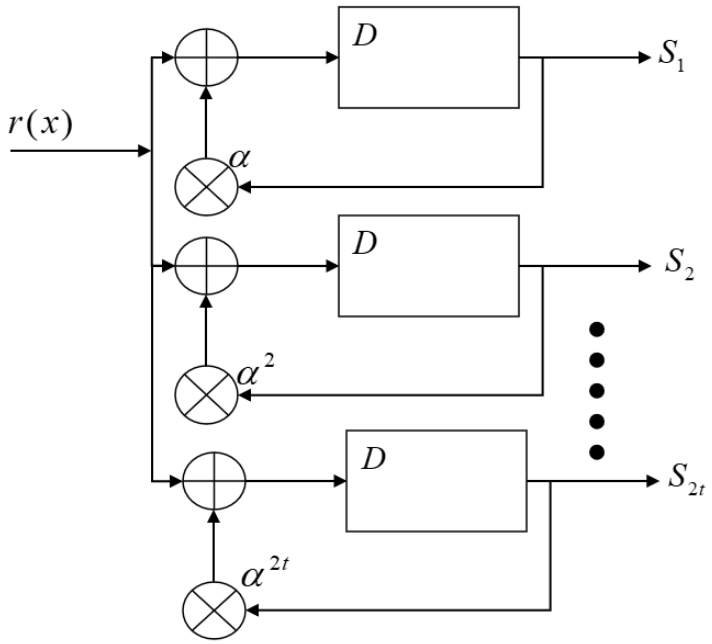
Power representation	Polynomial representation	Power representation	Polynomial representation
0	0	α^7	$\alpha^3 + \alpha + 1$
1	1	α^8	$\alpha^2 + 1$
α	α	α^9	$\alpha^3 + \alpha$
α^2	α^2	α^{10}	$\alpha^2 + \alpha + 1$
α^3	α^3	α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^4	$\alpha + 1$	α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^5	$\alpha^2 + \alpha$	α^{13}	$\alpha^3 + \alpha^2 + 1$
α^6	$\alpha^3 + \alpha^2$	α^{14}	$\alpha^3 + 1$

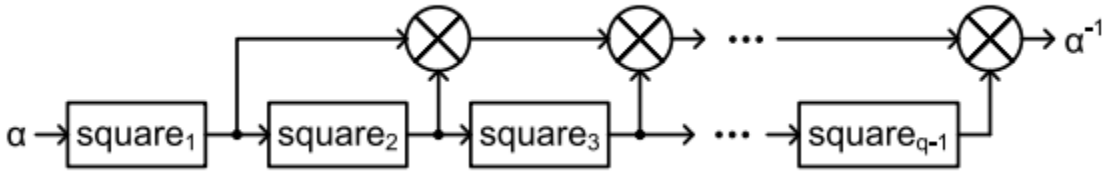


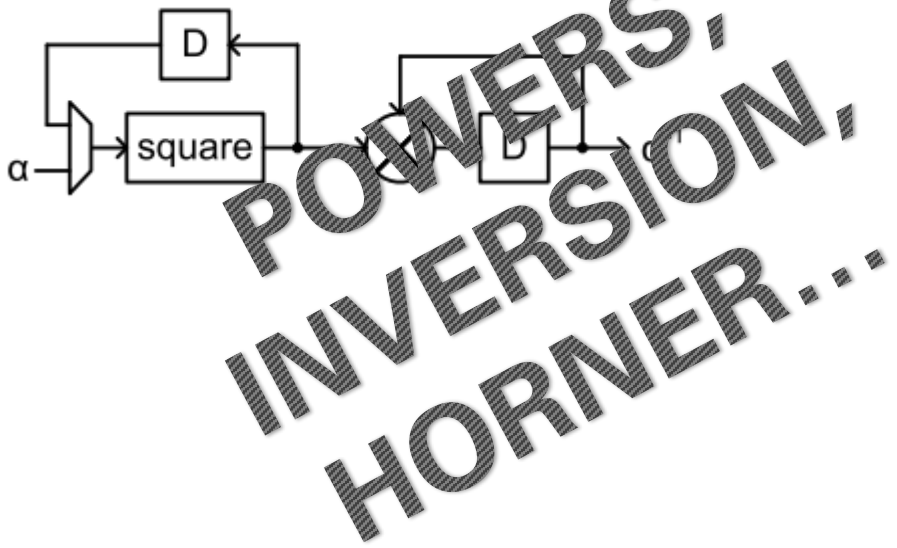
SEVERAL IMPLEMENTATIONS

Solutions

- Not only addition and product…







Solutions

National Aeronautics and Space Administration

- Co-processors vs new architecture

Assessing and Mitigating Radiation Effects in Xilinx FPGAs

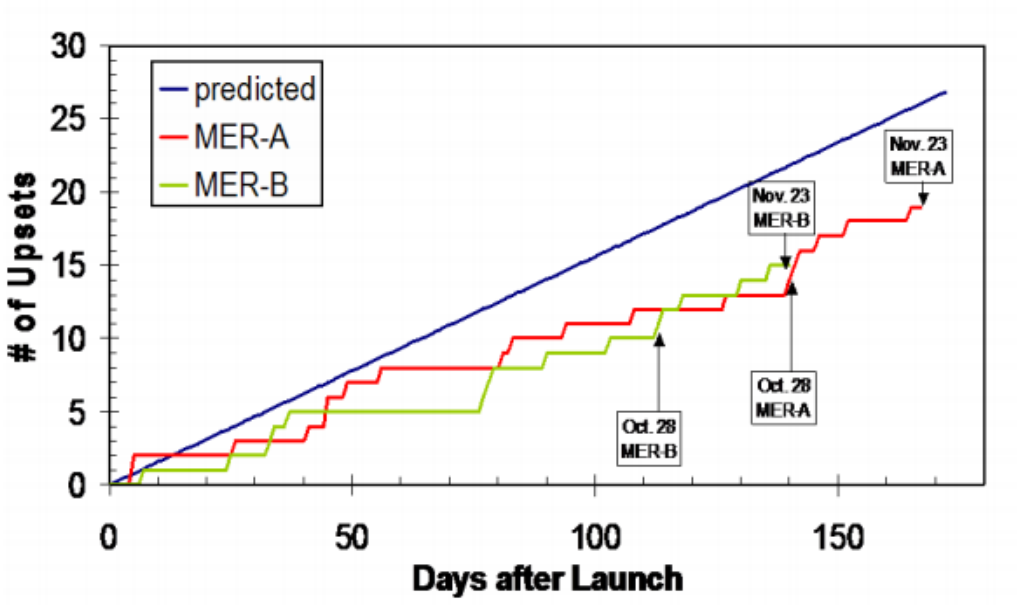


Figure 1. Pyro Control (LPSIF)—Xilinx XQR4062XL.

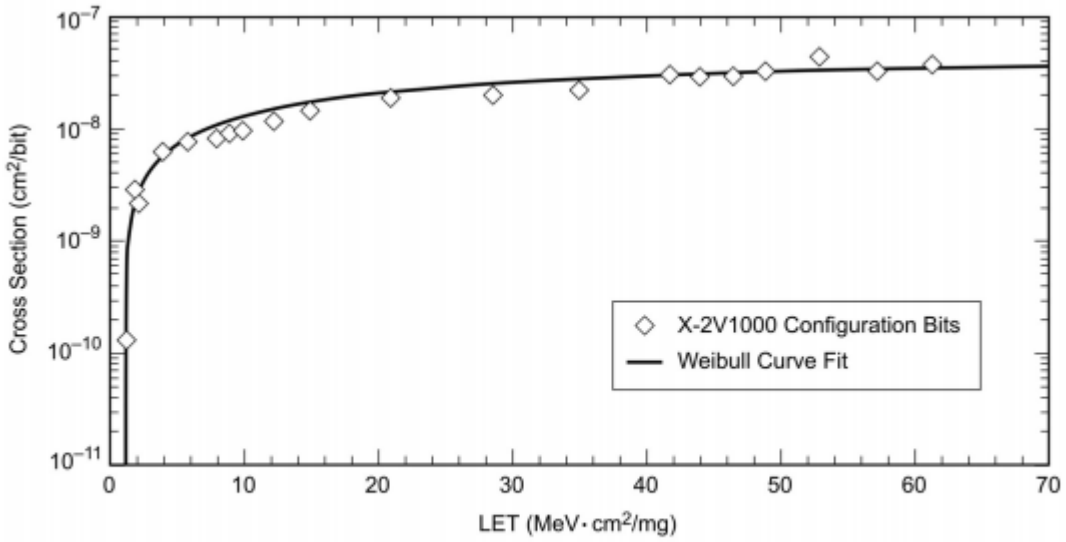
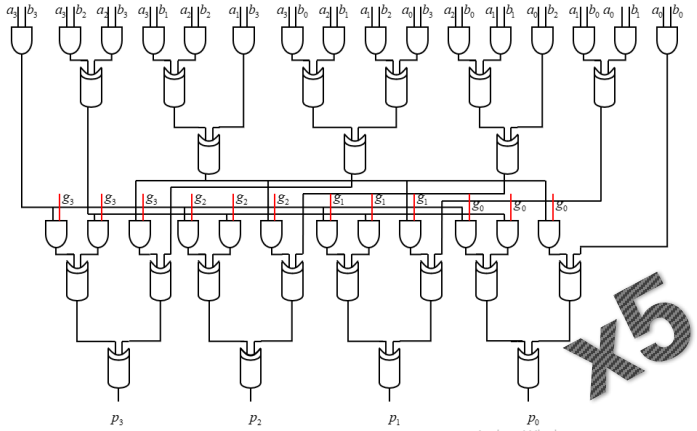


Figure 4. LET cross section for upsets in the Xilinx Virtex-II configuration SRAM [3].

Solutions

- Co-processors vs new architecture



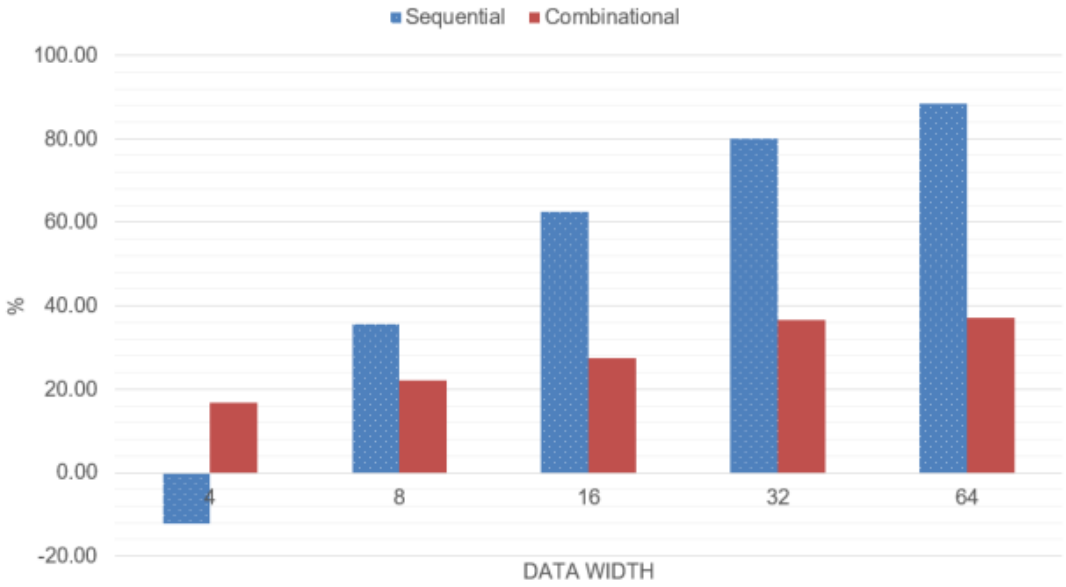
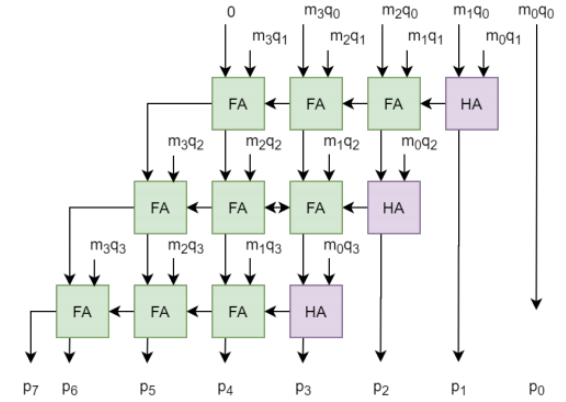
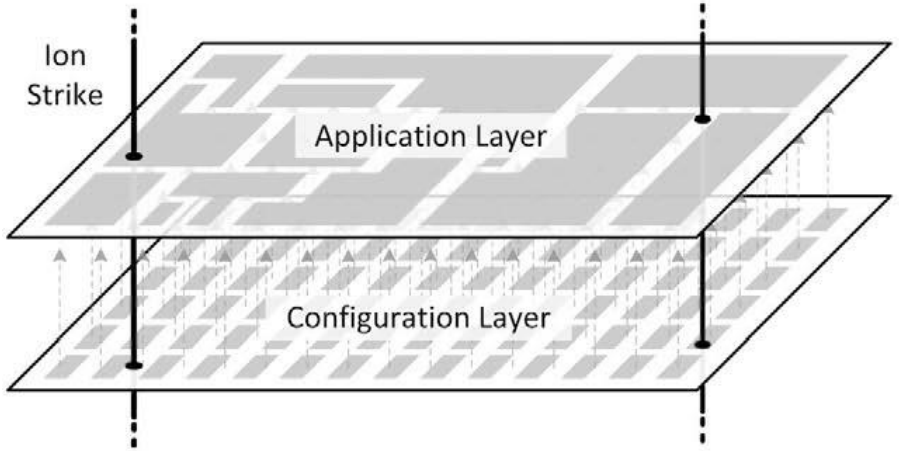


Fig. 13: Area reduction comparison between combinational and sequential architecture.

	31 ... 25	24 ... 20	19 ... 15	14 ... 12	11 ... 7	6 ... 0
clmul	0000101	rs2	rs1	001	rd	0110011
clmulh	0000101	rs2	rs1	011	rd	0110011
ffwidth	0000111	rs2	rs1	000	unused	0110011
ffred	0000111	rs2	rs1	001	rd	0110011





Solutions

- Co-processors vs new architecture

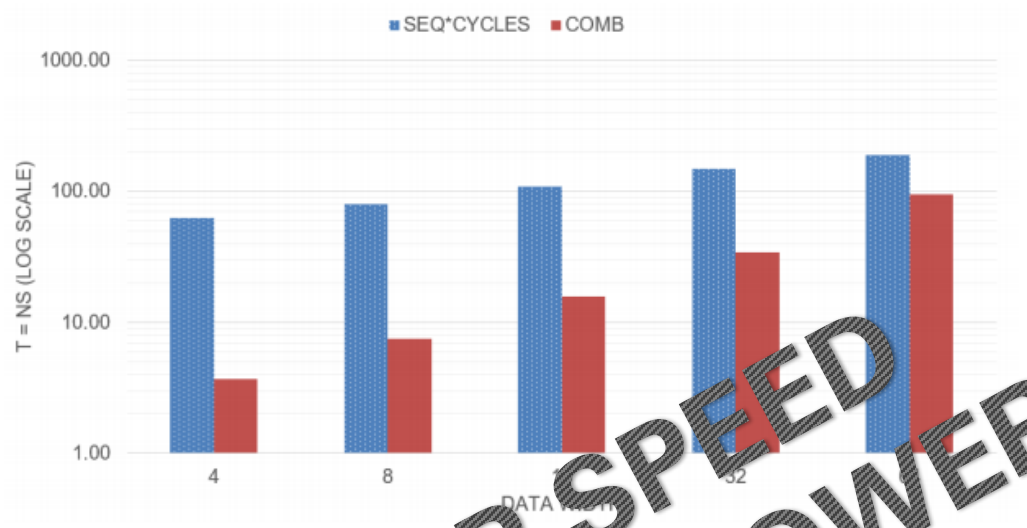
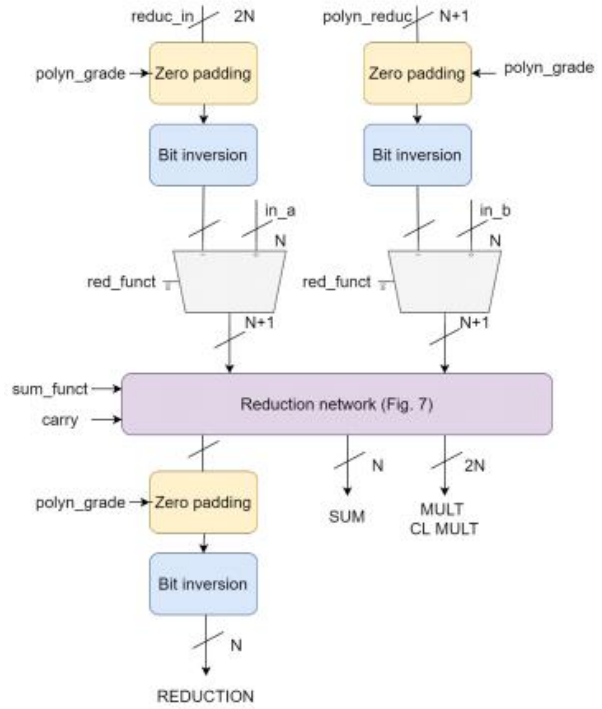
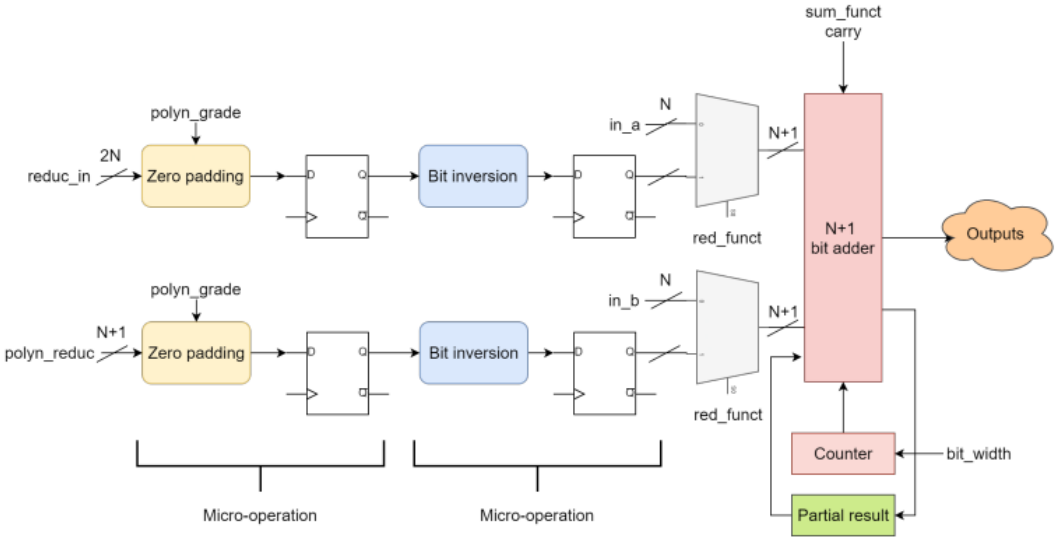


Fig. 15: CL multiplication calculation time comparison

KEEP SPEED
REDUCE POWER





Solutions

- Different algorithms, with different algebra
  - First steps GF(2^m)

AES128	CBC Enc.	CBC Dec.	CTR Enc.	CTR Dec.	ECB Enc.	ECB Dec.
RV32IMC	160626	163584	161228	161228	41475	42082
custom	22969	22759	23583	23583	7054	6917
Reduc. %	85.70	86.09	85.37	85.37	82.99	83.56

AES192	CBC Enc.	CBC Dec.	CTR Enc.	CTR Dec.	ECB Enc.	ECB Dec.
RV32IMC	196218	200144	196564	196564	50891	51836
custom	28105	27775	28719	28719	8902	8735
Reduc. %	85.68	86.12	85.39	85.39	82.51	83.15

AES256	CBC Enc.	CBC Dec.	CTR Enc.	CTR Dec.	ECB Enc.	ECB Dec.
RV32IMC	230027	234713	230897	230897	58553	59568
custom	31434	30984	32048	32048	8944	8747
Reduc. %	86.33	86.80	86.12	86.12	84.72	85.32

Crypto

SweRV-EL2	Slice LUTs	Slice Registers	F7 Muxes	F8 Muxes	Slice	LUT as logic
standard	18,605	7651	341	74	5,329	18,605
our proposal	19,974	7688	413	80	5,699	19,974
Inc. %	7.36%	0.48%	21.11%	8.11%	6.94%	7.36%

	RS(255,247)		RS(255,239)	
	Encode	Decode	Encode	Decode
standard	154,003	151,681	300,831	303,289
out proposal	29,006	22,648	58,660	45,237
Reduc. %	81.17%	85.07%	80.50%	85.08%

ECC

Solutions

- Not only for a certain application or system

pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4

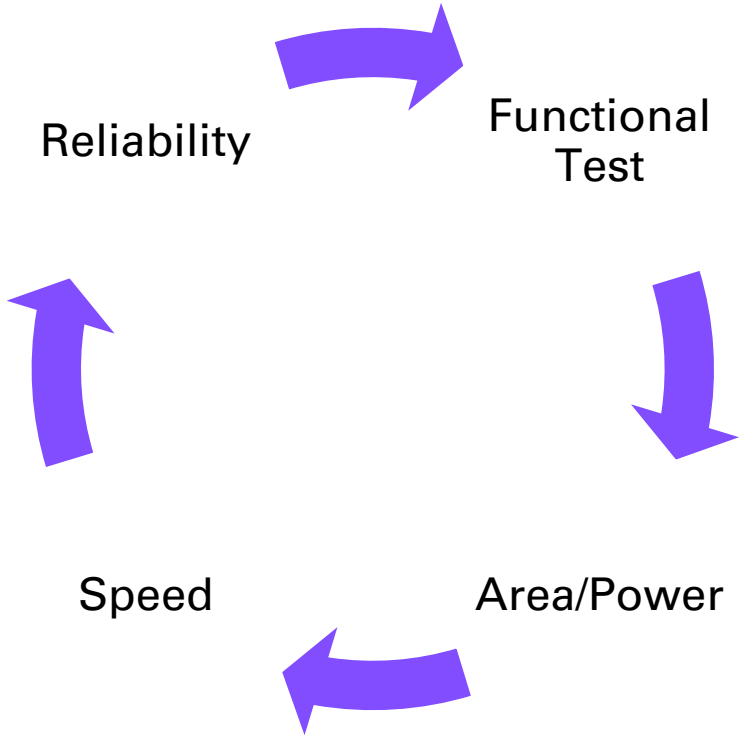
KYBER on RISC-V

Towards Reliable and Secure Post-Quantum Co-Processors based on RISC-V

OBSOLESCENCE RISK

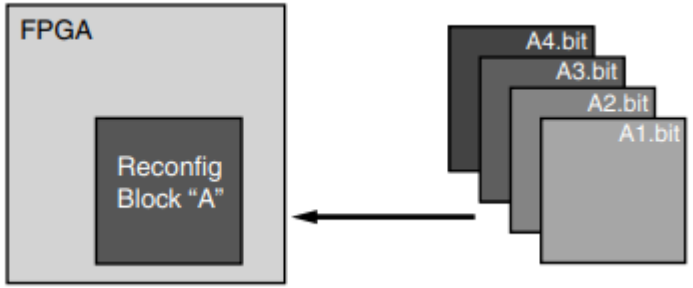
Solutions

Operation	Applications
GF(2^m) mult	Crypto, PQC, ECC
GF(2^m) inv	Crypto, PQC, ECC
GF(2^m) power	Crypto, PQC, ECC
GF(q) mult	Crypto, PQC, ECC
GF(q) power	Crypto, PQC, ECC
Ring mult, NTT	Crypto, PQC, ECC
Ring power	Crypto, PQC, ECC
mod q	Crypto, PQC



Solutions

Operation	Applications	
GF(2^m) mult	Crypto, PQC, ECC	A1
GF(2^m) inv	Crypto, PQC, ECC	
GF(2^m) power	Crypto, PQC, ECC	
GF(q) mult	Crypto, PQC, ECC	A2
GF(q) power	Crypto, PQC, ECC	
Ring mult, NTT	Crypto, PQC, ECC	A3
Ring power	Crypto, PQC, ECC	
mod q	Crypto, PQC	



There are many reasons why the ability to time multiplex hardware dynamically on a single FPGA device is advantageous.

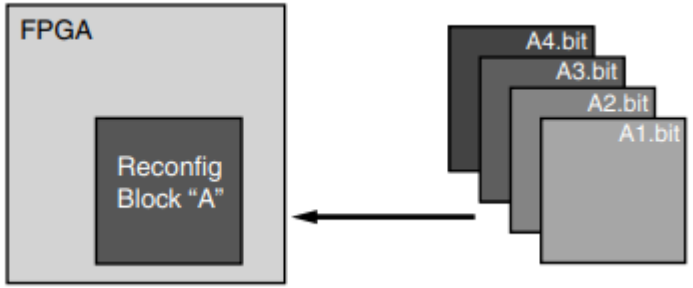
These include:

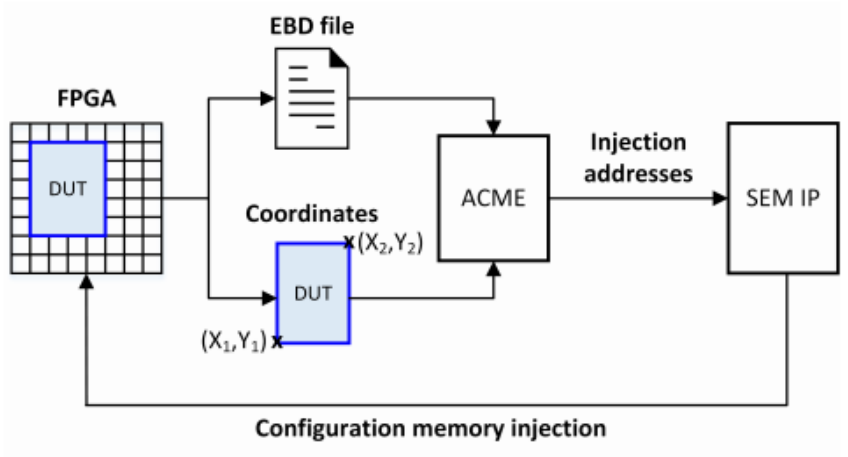
- Reducing the size of the FPGA device required to implement a given function, with consequent reductions in cost and power consumption
- Providing flexibility in the choices of algorithms or protocols available to an application
- Enabling new techniques in design security
- Improving FPGA fault tolerance
- Accelerating configurable computing

Solutions

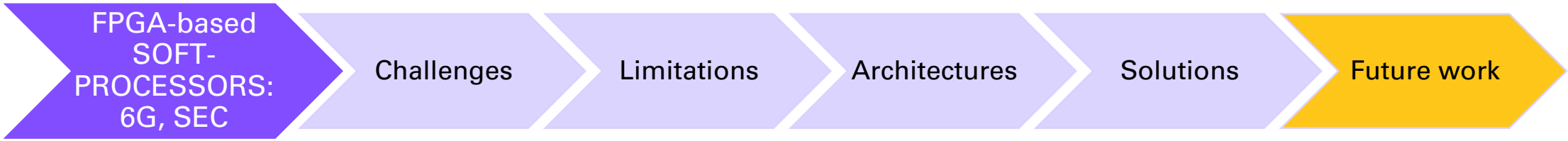
Operation	Applications
GF(2^m) mult	Crypto, PQC, ECC
GF(2^m) inv	Crypto, PQC, ECC
GF(2^m) power	Crypto, PQC, ECC
GF(q) mult	Crypto, PQC, ECC
GF(q) power	Crypto, PQC, ECC
Ring mult, NTT	Crypto, PQC, ECC
Ring power	Crypto, PQC, ECC
mod q	Crypto, PQC

A1 : m=2, q=2
A2 : m=3, q=3
A3 : m=4, q=4
A4 : m=5, q=5
…





Index


FPGA-based SOFT-PROCESSORS: 6G, SEC
Challenges
Limitations
Architectures
Solutions
Future work

Future work

- Custom instruction set for artificial intelligence applications

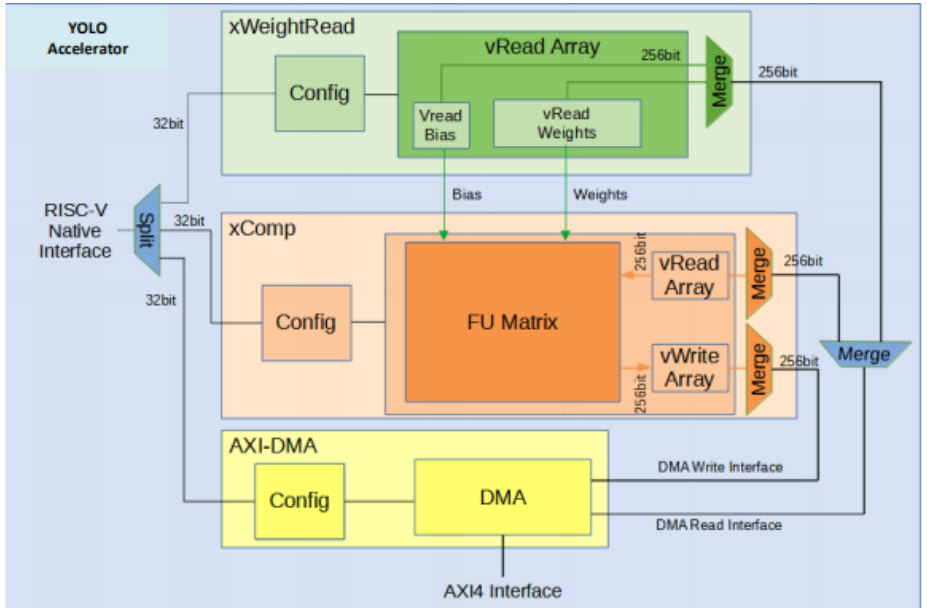
A Full Featured Configurable Accelerator for Object Detection with YOLO

DANIEL PESTANA[1], PEDRO R. MIRANDA[1], JOÃO D. LOPES[1], RUI P.DUARTE[1],(Member, IEEE), MÁRIO VÉSTIAS[2],(Member, IEEE), HORÁCIO C. NETO[1], AND JOSÉ T. DE SOUSA[1],(Member, IEEE)

[1]INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, 1000-029 Lisboa, Portuga

[2]INESC-ID, Instituto Superior de Engenharia de Lisboa, Instituto Politécnico de Lisboa, 1500-310 Lisboa, Portugal

Platform	Time (ms)	FPS
CPU (Intel i7-8700 @ 3.2 GHz)	828.3	1.2
GPU (RTX 2080 Ti)	15.4	64.9
FPGA (SoC-YOLO)	30.9	32.4



Future work

- Fault-tolerance verification for rad-hard FPGAs

Radiation-tolerant rugged FPGA for space applications like payload signal processing introduced by Xilinx

The XQRKU060 also offers high performance machine learning and machine learning development tools that support industry-standard frameworks.

Jun 22nd, 2020

Future work

- Impact of virtualization and OS on the performance in terms

Analyzing the impact of the Operating System on the Reliability of a RISC-V FPGA Implementation

Imran Wali, *Infineon Technologies AG*, Duisburg, Germany, imran.wali@infineon.com
Alfonso Sánchez-Macián, *ARIES Research Center*, *Universidad Antonio de Nebrija*, Madrid, Spain, asanchep@nebrija.es
Alexis Ramos, *Deimos Space, SLU*, Tres Cantos, Spain, alexis.ramos@deimos-space.com
Juan Antonio Maestro, *ARIES Research Center*, *Universidad Antonio de Nebrija*, Madrid, Spain, jmaestro@nebrija.es

A First Look at RISC-V Virtualization from an Embedded Systems Perspective

Bruno Sá, José Martins, Sandro Pinto
Centro ALGORITMI, Universidade do Minho, Portugal
bruno.vilaca.sa@gmail.com, {jose.martins, sandro.pinto}@dei.uminho.pt

A Comprehensive Survey on 6G Networks: Applications, Core Services, Enabling Technologies, and Future Challenges

Amin Shahraki, *Member, IEEE,* Mahmoud Abbasi, *Member, IEEE,* Md. Jalil Piran, *Member, IEEE* Mingzhe Chen *Member, IEEE* and Shuguang Cui *Fellow, IEEE*

Virtualization capability encourages diverse enterprise business models with a considerable degree of flexibility, more profits for the service provider, and lessen operational costs

VIRTUALIZATION BEYOND 5G

fgarciahe@nebrija.es