Raffaele Martino

Tutor: prof. Alessandro Cilardo

XXXII Cycle - III year presentation

Exploring the SHA-2 Design Space

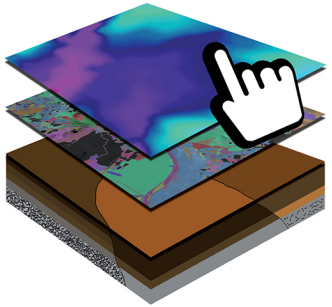
Outline

- Introduction
  - Background
  - III Year Training Activities
- Overview of the collaboration with CRISP[1]
  - Motivation
  - System Overview
  - Contributions
  - Publications
- PhD Thesis
  - Overview
    - Motivation with Examples
    - Problem Statement and Thesis Contributions
  - Discussion of specific aspects
    - Framework architecture and architectural exploration methodology
    - Experimental results
  - Publications

[1] Interdepartmental Research Centre on the Earth Critical Zone for Supporting the Landscape and Agroenvironment management

Background

- Master's Degree in Computer Engineering in 2016, magna cum laude
- PhD in Computer Architectures
- No fellowship
- Collaboration with CRISP[1]
  - From March 2018
  - Under grants from the Campania Region



[1] Interdepartmental Research Centre on the Earth Critical Zone for Supporting the Landscape and Agroenvironment management

III Year Training Activities

	Year 1	Year 2	Credits year 3									
				1	2	3	4	5	6			
	Summary	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Total	Check
Modules	**29.6**	**3.6**	**0**	1.2	6	0	0	0	0	**7.2**	**40.4**	**30-70**
Seminars	**5**	**5.6**	**0**	0	0.3	0	0	0	0	**0.3**	**10.9**	**10-30**
Research	**25.4**	**50.8**	**60**	8.8	3.7	10	10	10	10	**52.5**	**128.7**	**80-140**
	60	**60**	**60**	10	10	10	10	10	10	**60**	**180**	**180**

- Currently attending the preparation course for the Cambrigde C2 Proficiency certification at CLA

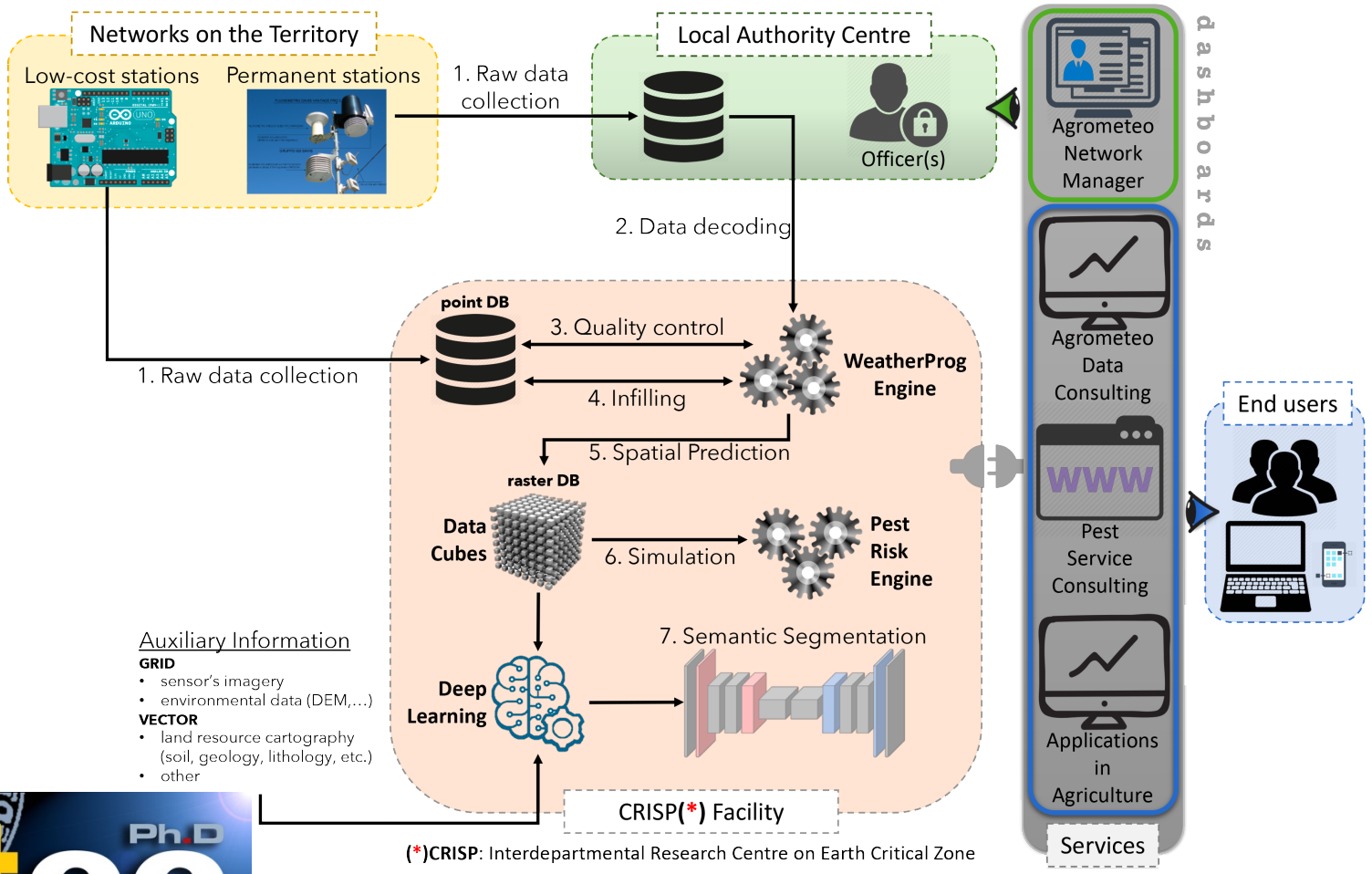
Collaboration with the Department of Agriculture of the University of Naples Federico II under subsequent grants from the Regione Campania programme “URCoFi – Unità Regionale di Coordinamento Fitosanitario”

AN INTEGRATED PLATFORM FOR AGRICULTURAL METEREOLOGY MANAGEMENT AND PLANNING

Motivation

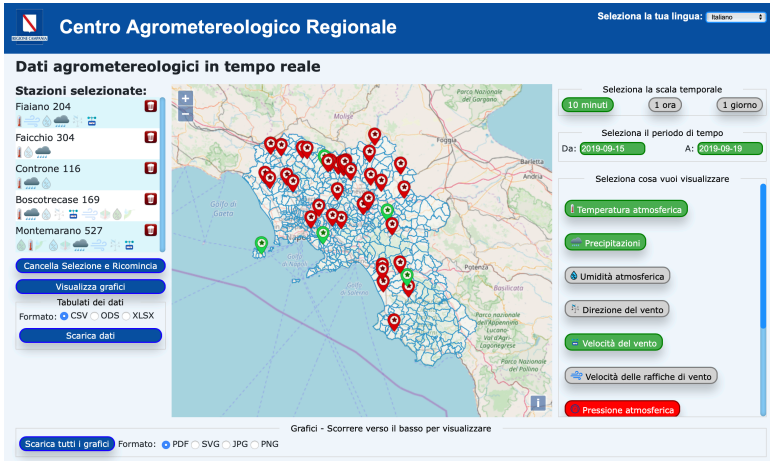
- DSS for Precision Agriculture requires timely available data
- Example: pest risk models
  - Can forecast pest diffusion in order to optimise pesticide usage
    - Statutory obligation under EU Directive 2009/128/EC
  - Require supply of weather data
- **There is currently no integrated platform from data collection to forecasts production!**

Overall System Overview



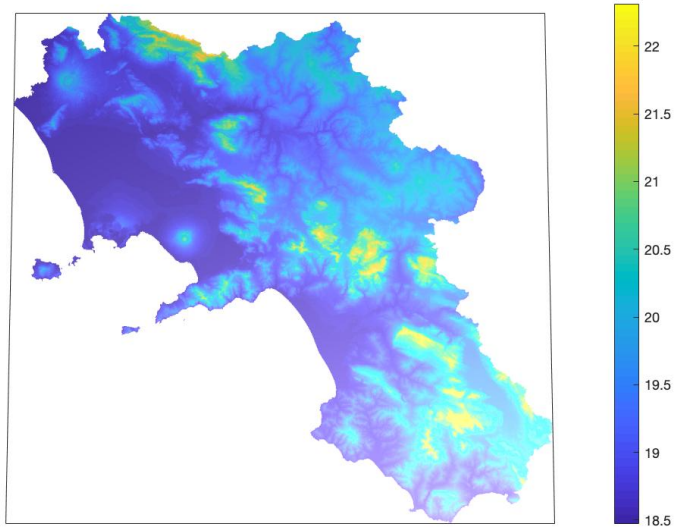
Contributions

- Data management
  - Data collection
  - Data base architecture
  - Access data policies
- End-user interface design
- Low-cost stations validation
- GPU-based acceleration of spatial interpolation algorithms

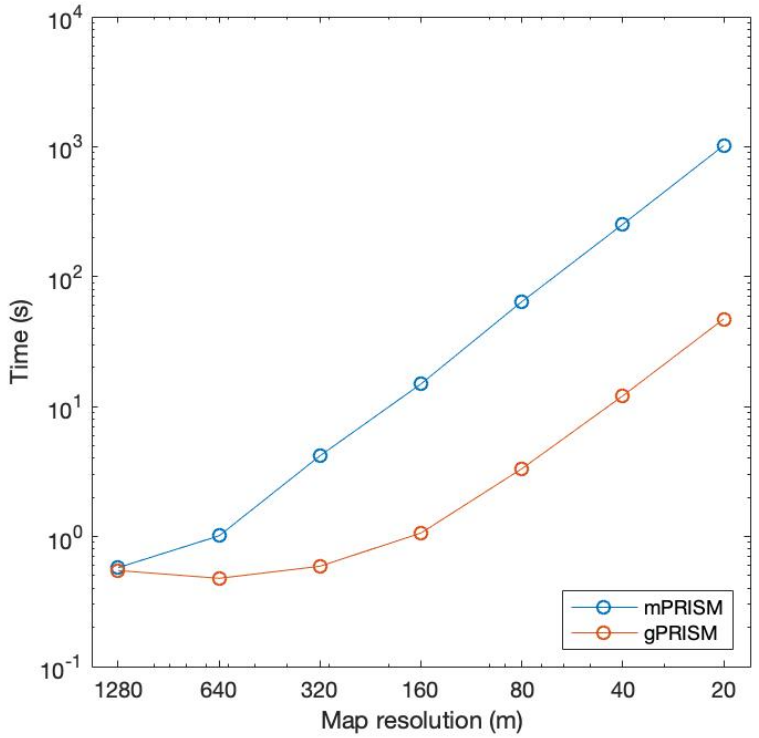


gPRISM: accelerating spatial interpolation algorithms with GPU

Produced air temperature map for June 09th, 2019



Multi-processor scaling



Publications

International Conference Papers:

- **R. Martino**, M. Nicolazzo, M. Crimaldi, G. Langella, "A low-cost movable station for fast and effective agroclimatic monitoring". *Proceedings of the 2nd International Workshop on Metrology for Agriculture and Forestry (METROAGRIFOR 2019)*, Portici, Italy, Oct. 24-26, 2019, DOI: 10.1109/MetroAgriFor.2019.8909248.
- **R. Martino**, M. Nicolazzo, G. Langella, "Towards efficient production of digital climatic maps for the Campania Region". *Proceedings of the 2nd International Workshop on Metrology for Agriculture and Forestry (METROAGRIFOR 2019)*, Portici, Italy, Oct. 24-26, 2019, DOI: 10.1109/MetroAgriFor.2019.8909232.
- **R. Martino**, M. Nicolazzo, G. Langella, "A full integrated system for agroclimatic and pest monitoring at farm and landscape scales in Campania Region", *Proceedings of the 1st International Workshop on Metrology for Agriculture and Forestry (METROAGRIFOR 2018)*, in IOP Conference Series: Earth and Environmental Science, 2019, vol. 275, nº 12007, DOI: 10.1088/1755-1315/275/1/012007.

➢ Journal papers are in preparation!

PhD Thesis

EXPLORING THE SHA-2 DESIGN SPACE

Introduction

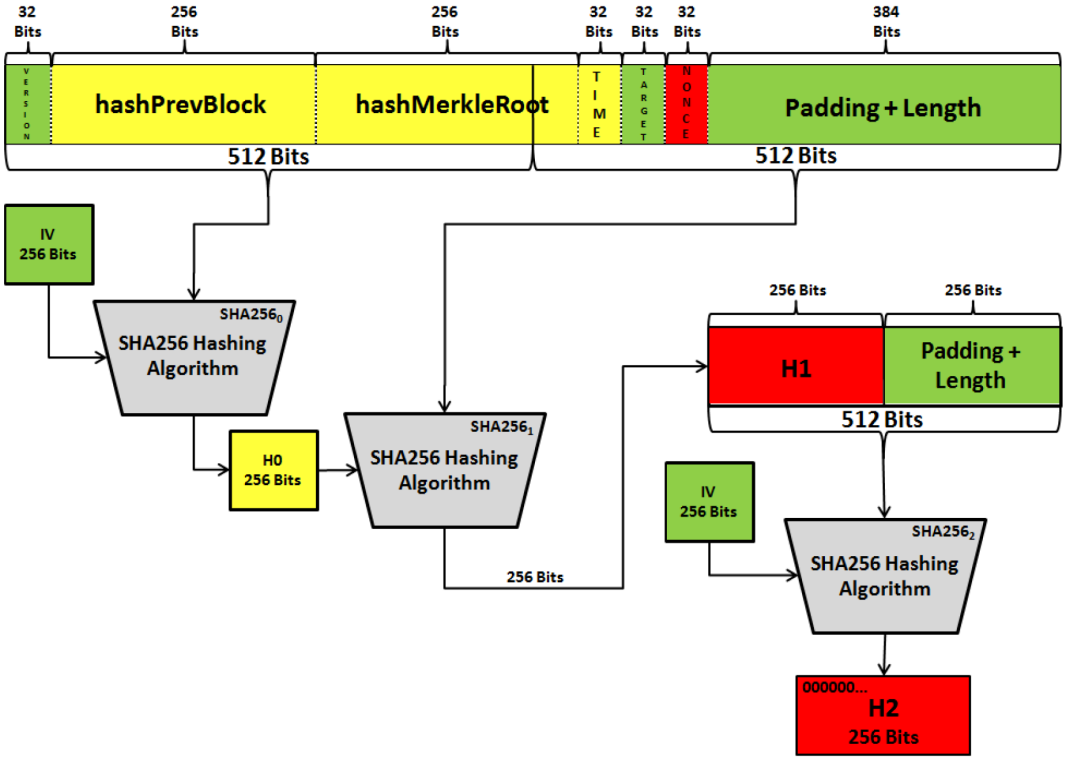
- Cryptographic hash functions underlie many aspects of our life
  - Used whenever there is the need of securing message integrity or the sender's identity
- The phasing out of other hash functions due to their breaking left SHA-2 as the most commonly used one
- Traditional application domain has been network security
  - Communicating parties can be assumed to be capable of performing hash computations

Motivation

- Emergence of innovative applications:
  - Blockchains
  - IoT
- More stringent set of requirements
  - Throughput
  - Area
  - Energy
  - Power
- Each application has its own set of requirements

Bitcoin: A Motivating Example

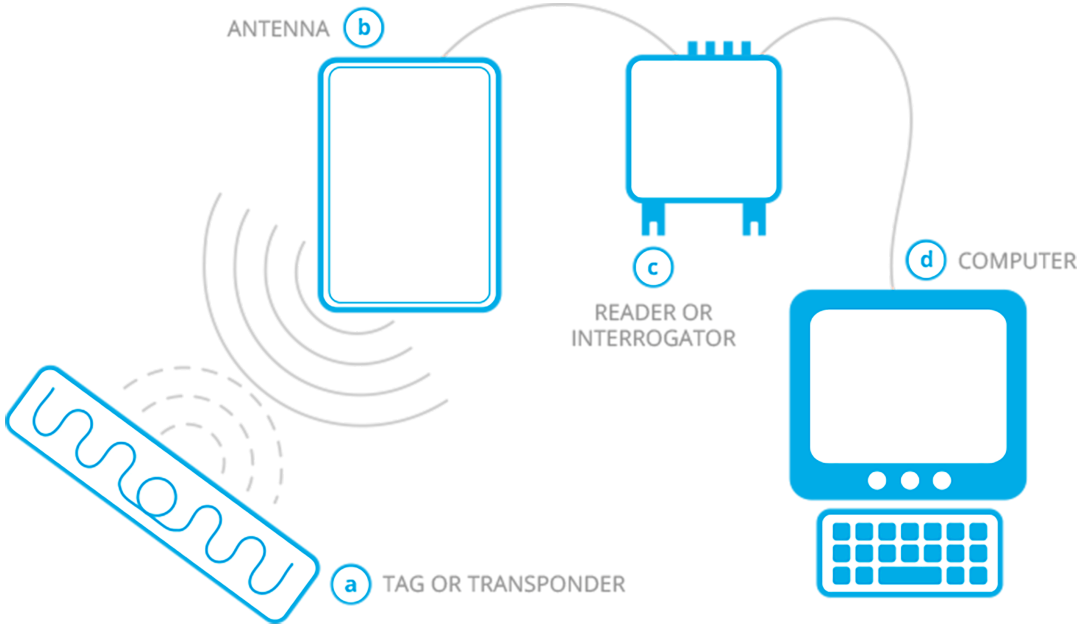
- Throughput
  - Competitive process
  - Required for profitability
- Area
  - Mass integration
- Energy
  - Cost
  - Impacts profitability



Another Example: RFID

Constraints on the **tag** side

- Area
  - Constrained environment
- Power
  - Passively powered devices



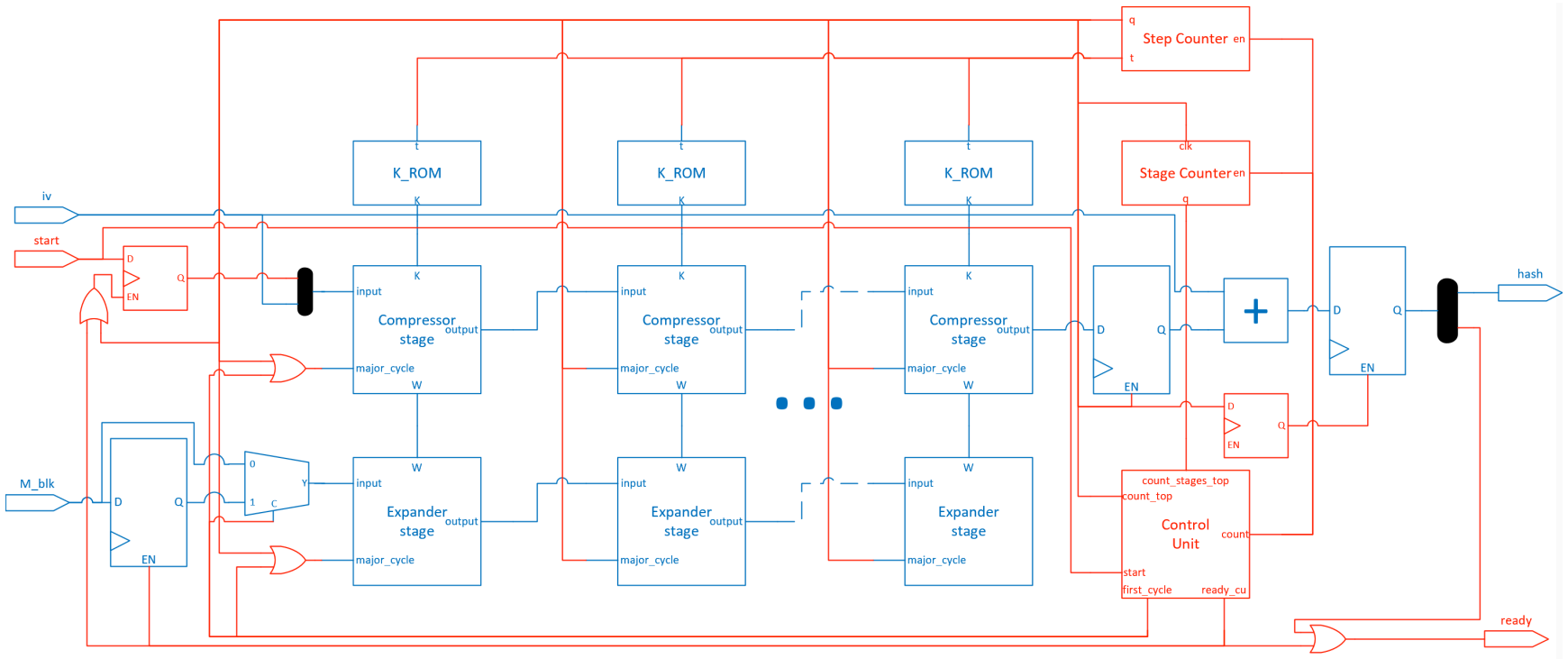
Issues when Comparing Different SHA-2 Architectures

- Designs are evaluated on specific targets
  - Cannot compare **results from different targets**
  - Hard to isolate **the contribution of the design** to the final implementation figures
- A design might have been proposed for a specific application
  - Need for **a fair comparison**
- This called for:
  - A **framework** for fair, comprehensive evaluation
  - A systematic, evidence-based **analysis**

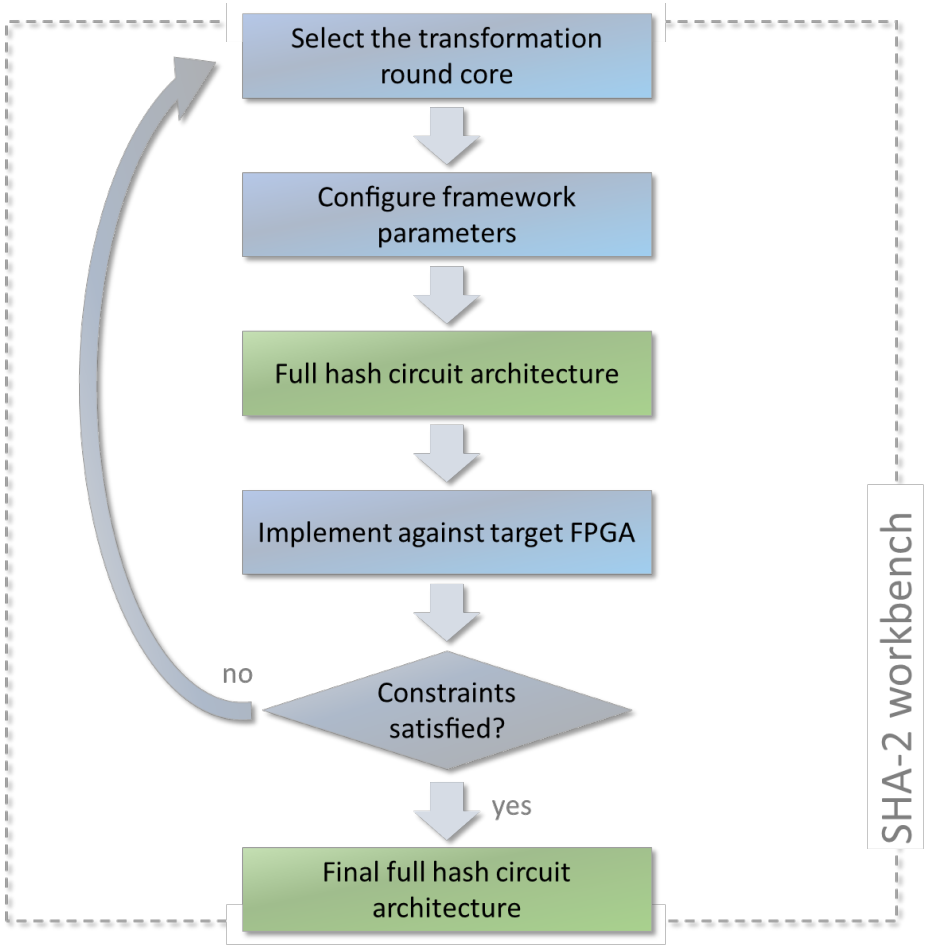
Thesis Contributions

- Systematic, evidence-based analysis of the various design techniques proposed for SHA-2
- A framework for the fair and fast evaluation of different alternatives for a SHA-2 hardware accelerator
- A newly introduced SHA-2 design, targeted to a specific FPGA, which outperforms existing literature approach

Framework Architecture



Exploration methodology



Implementation Results

Architectural Exploration

SHA-256 without final stage

(a) Base architectures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
1	2.398	6.516	1578	1875	0.451	0.122	0.573	1.057	2.911
5	3.004	5.201	1619	1866	0.451	0.115	0.566	0.822	2.353
7	2.297	6.802	1485	1640	0.451	0.131	0.582	1.173	2.992

(b) Pipelined architectures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
3	2.745	22.769	5314	4302	0.453	0.412	0.865	1.097	6.738
6	3.050	20.492	5385	4314	0.454	0.430	0.883	0.974	5.941
9	2.646	23.621	4986	4312	0.454	0.434	0.887	1.213	6.817

(c) Unrolled architectures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
2	7.750	8.065	2793	1960	0.451	0.099	0.550	0.739	3.754
8	5.146	6.073	2907	2194	0.452	0.164	0.616	0.535	2.524

(d) Unrolled and pipelined architecures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
4	9.012	27.741	9316	4188	0.453	0.347	0.800	1.097	8.877
10	5.607	22.294	8670	5184	0.455	0.581	1.036	0.658	5.509

SHA-256 with final stage

(a) `Reordered_UF1`, without pipelining

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
7	2.297	6.802	1485	1640	0.451	0.131	0.582	1.173	2.992
7'	2.250	6.944	1487	1898	0.451	0.134	0.585	1.196	3.039

(b) `Reordered_UF2`, without pipelining

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
8	5.146	6.873	2907	2194	0.452	0.164	0.616	0.535	2.524
8'	4.935	6.332	2914	2451	0.452	0.164	0.616	0.556	2.632

(c) `Reordered_UF1`, with 4-stage pipelining

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
9	2.646	23.621	4986	4312	0.454	0.434	0.887	1.213	6.817
9'	2.502	24.980	5088	4570	0.454	0.427	0.881	1.257	7.259

(d) `Reordered_UF2`, with 4-stage pipelining

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
10	5.607	22.294	8760	5184	0.455	0.581	1.036	0.658	5.509
10'	5.607	22.294	8649	5455	0.455	0.576	1.030	0.660	5.541

Implementation Results

Changing the Target Technology

(a) Base architectures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
1	6.273	2.491	1593	1865	0.122	0.063	0.185	0.400	3.447
5	8.214	1.902	1565	1866	0.122	0.054	0.176	0.311	2.767
7	6.274	2.490	1412	1642	0.122	0.070	0.192	0.452	3.321
7'	6.500	2.404	1422	1900	0.122	0.062	0.184	0.433	3.344

(b) Pipelined architectures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
3	7.002	8.926	4923	4302	0.122	0.223	0.346	0.464	6.604
6	9.290	6.728	4971	4301	0.122	0.188	0.311	0.346	5.541
9	7.103	8.799	4795	4299	0.122	0.210	0.332	0.470	6.785
9'	7.449	8.390	4754	4557	0.122	0.202	0.329	0.452	6.629

(c) Unrolled architectures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
2	20.262	3.085	2767	1960	0.122	0.048	0.170	0.285	4.645
8	13.709	2.280	2895	2195	0.122	0.086	0.208	0.202	2.808
8'	13.988	2.234	2897	2452	0.122	0.080	0.202	0.197	2.831

(d) Unrolled and pipelined architecures

Nº	Critical Delay	Hash rate (Mhash/s)	Area LUT	Area FF	Power Consumption (W) Static	Dynamic	Total	Efficiency Area	Power
4	21.563	11.594	9072	4188	0.122	0.183	0.305	0.327	9.731
10	15.494	8.068	8566	5185	0.122	0.123	0.407	0.241	5.074
10'	15.494	8.068	8468	5455	0.122	0.122	0.397	0.244	5.202

Artix-7 data

- The target change affect different architectures disproportionately
- The final stage is no longer useful

SHA-2 Optimised Design

Implementation Results

Proposal	FPGA	Slices	Frequency (MHz)	Cycles per hash	Throughput (Mbit s^{-1})	Area Efficiency
This one	Kintex-5	233	285.71	65	2250.55	9.66
[125]	Virtex-6	197	354	129	1405.02	7.13
[53]	Virtex-5	387	202.54	65	1595.39	4.12
[50]	Virtex-5	2796	179.08	64	1432.64	0.51
[82]	Virtex-5	N/D	N/D	N/D	1539.60	1.13
[78]	Virtex-7	1402	204	32	3264	2.33
[41]	Virtex-5	139	64.45	280	117.85	0.85
[4]	Virtex-2	1149	114.55	65	902.30	0.79
[81]	Virtex-6	1831	172	8	11008	6.01

Publications

International Journal Papers:

- **R. Martino**, A. Cilardo, "SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey". *IEEE Access* (accepted for publication), DOI: 10.1109/ACCESS.2020.2972265.
- **R. Martino**, A. Cilardo, "A Flexible Framework for Exploring, Evaluating, and Comparing SHA-2 Designs", *IEEE Access*, vol. 7, 2019, DOI: 10.1109/ACCESS.2019.2920089.

International Conference Papers:

- **R. Martino**, A. Cilardo, "A Configurable Implementation of the SHA-256 Hash Function'", *Proceedings of the 14th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2019)*, in Advances on P2P, Parallel, Grid, Cloud and Internet Computing, in Lecture Notes in Networks and Systems, vol. 96, 2020, pp. 558-567, DOI: 10.1007/978-3-030-33509-0_52.

Questions?

THANK YOU FOR THE ATTENTION

UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II