Application-Specific Processor Design for Low-Complexity & Low-Power Embedded Systems

Jeremy Constantin, TCL, EPFL, Switzerland; Advisor: A. Burg (TCL); Collaboration: D. Atienza (ESL)

Low-Power Embedded Systems

Portable, autonomous devices:

- Highly resource constrained systems
- Wireless (sensor) nodes
- Limited battery life-time
- Application-specific use cases
- Flexibility & programmability desired

Embedded systems require…
Low power consumption through
- Low computational complexity
- Low memory footprint

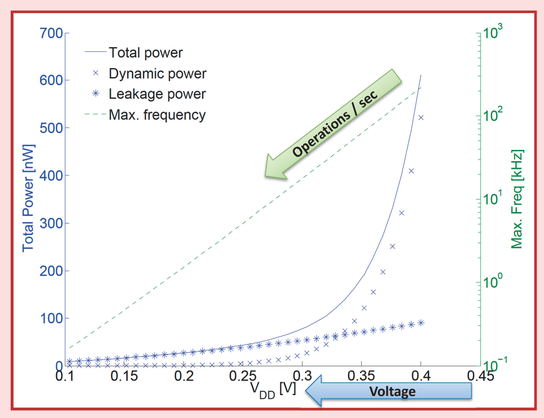
Power Savings through Voltage Scaling

Supply voltage down-scaling:

- Active power: $P_A = C \cdot V_{DD}^2 \cdot f$
- Drastic power savings

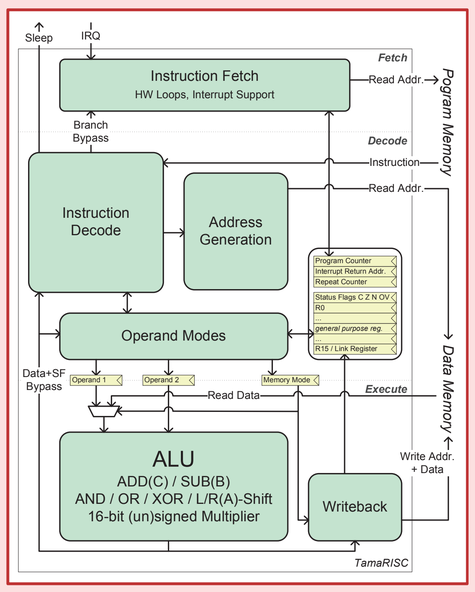
Near- and sub-V_T operation:

- Reliability issues (solvable with circuit-level techniques and custom embedded memories)
- Strong **performance degradation**



To enable aggressive voltage scaling, alleviate the performance degradation using **application-specific instruction set processors (ASIPs)**

Custom Low-Power Processor

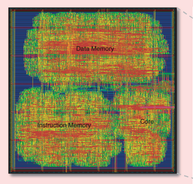


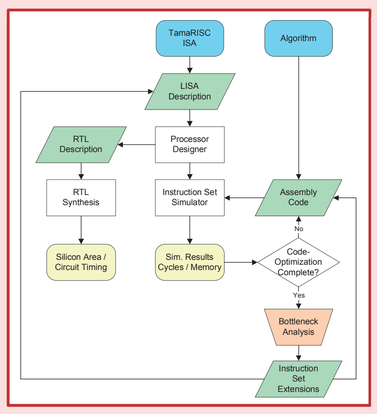
TamaRISC: custom RISC MCU

- Baseline processing core (< 10 kGE)
- 16-bit Harvard architecture
- 3-stage pipeline
- 24-bit instruction word
- 14 single word, single cycle instructions
- Minimalistic 16-bit ALU
- Addressing modes for efficient execution of signal processing applications
- Sleep mode, Interrupt, and basic HW-loop support
- Embedded real-time OS support
- Custom C-compiler

Design & Evaluation Flow

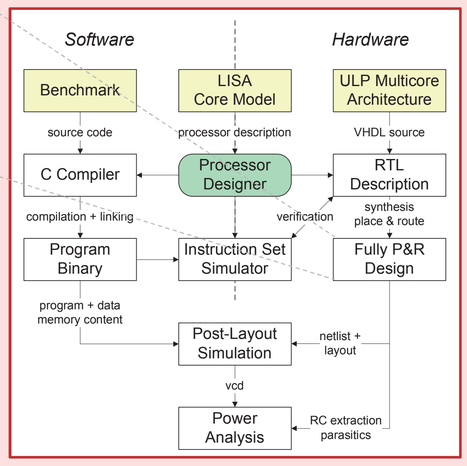
Rapid design space exploration based on single **golden processor model**





ASIP core architecture described in LISA (PD)
Automatic generation:

- Software tool-chain
- Cycle-accurate ISS
- Synthesizable HDL



Accurate power analysis using vcd-based **post-layout** gate-level simulations

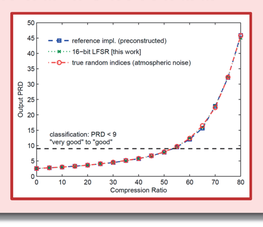
Application to Compressed Sensing

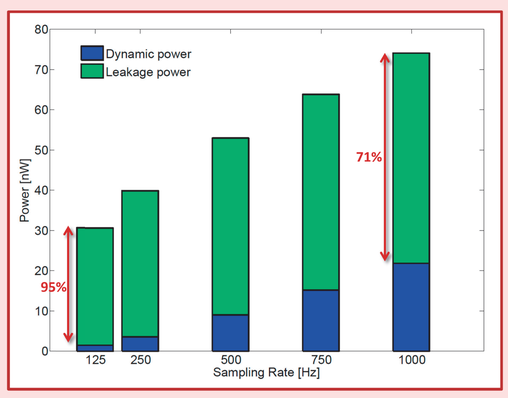
Ultra-low-power ASIP: TamaRISC-CS [1]

- Low-complexity CS algorithm
- Instruction set extension (ISE) enables efficient random index generation
- 16-bit multi-step LFSR-based PRNG
- Drastically **reduced memory** footprint
- CS application **speedup**: **62x**
- Improved **power** consumption: **11.6x**
- ISE induces less than 3% area overhead

```
for i := 1 → n do
    sample := getSample()
    for j := 1 → I do
        index := getRandomIndex(1..k)
        buffer[index] :=
                buffer[index] + sample
    end for
end for
```

Pseudocode of Reduced Complexity CS Algorithm



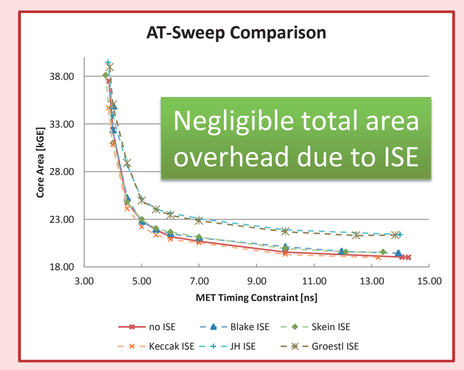


Instruction set extensions are key for sub-V_T operation

Application to Cryptography

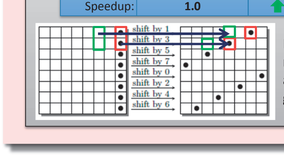
Cryptographic Hash Functions (SHA-3) [2,3]

- Individual ASIP cores, algorithm-specific ISE
  - Extension of computational units
  - Finite state machines for data address generation
  - Lookup table integration
- Average **speedup**: **172%**
- Average **memory** savings: **40%**
- Maximum core area overhead: 10%



ISE example: state row rotation memory to memory (64 bytes)

	Reference ISA	ISE
Instructions:	124	2
Cycles:	126	37
Speedup:	1.0	3.4



FSM-based memory address pattern generation

Algorithm	PIC24 [cycles/byte]	PIC24 + ISE [cycles/byte]	Speedup	Area Overhead
BLAKE	155.2	**102.9**	1.51	~ 0%
Grøstl	462.3	**57.6**	**8.03**	+10%
JH	463.8	**383.5**	1.21	+10%
Keccak	188.3	**131.7**	1.43	~ 0%
Skein	157.6	**112.6**	1.40	~ 0%

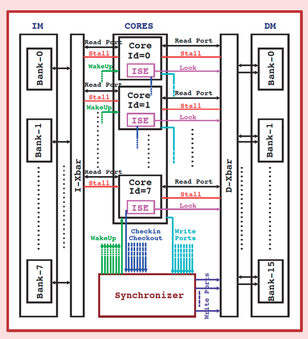
Algorithm	Data PIC24 [byte]	Data +ISE	Text PIC24 [byte]	Text +ISE
BLAKE	488	-59%	1,028	-20%
Grøstl	982	-78%	2,619	-69%
JH	1,550	-87%	4,649	-53%
Keccak	448	-21%	3,480	-31%
Skein	242	0%	5,734	-18%

No significant additions to the processor **datapath** necessary

Application to Biomedical Signal Analysis

Wearable Online Health Monitoring Systems [4,5,6]

- TamaRISC integrated into single- and multi-core architectures for multi-lead ECG signal analysis
- Custom processor optimizations and extensions tailored to ultra-low-power multi-core operation



- Banked shared memories
- Crossbar interconnects
- Virtual addr-space, MMU
- Data & instr. broadcast
- Core synchronization for efficient SIMD execution

Parallel computing architectures provide better **power efficiency** for medium to high workloads (> 2 MOp/s)

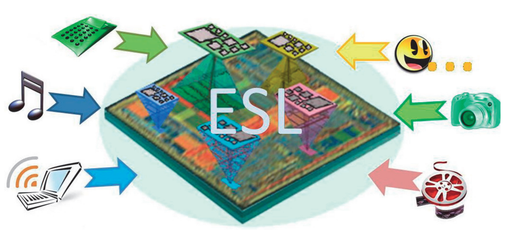
Conclusion

Considerable speedup, memory footprint reduction and in turn power-savings, enabled by small but dedicated instruction set extensions with extremely low hardware overhead.

Operation in near- and sub-V_T regime is feasible, even for more demanding online real time signal processing tasks, when combined with custom tailored ASIP systems.

[1] Constantin, J., et al., "TamaRISC-CS: An Ultra-Low-Power Application-Specific Processor for Compressed Sensing," 20th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), 2012
[2] Constantin, J., et al., "Instruction Set Extensions for Cryptographic Hash Functions on a Microcontroller Architecture," 23rd IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2012
[3] Constantin, J., et al., "Investigating the Potential of Custom Instruction Set Extensions for SHA-3 Candidates on a 16-bit Microcontroller Architecture," Cryptology ePrint Archive, 2012
[4] Dogan, A., et al., "Low-power Processor Architecture Exploration for Online Biomedical Signal Analysis," IET Circuits, Devices & Systems, 2012
[5] Dogan, A., et al., "Multi-Core Architecture Design for Ultra-Low-Power Wearable Health Monitoring Systems," Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012
[6] Dogan, A., et al., "Synchronizing Code Execution on Ultra-Low-Power Embedded Multi-Channel Signal Analysis Platforms," Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE



Telecommunications Circuits Laboratory