Instruction Set Extensions for Accelerating SNOW 3G on a Multithreaded Software Defined Radio Platform

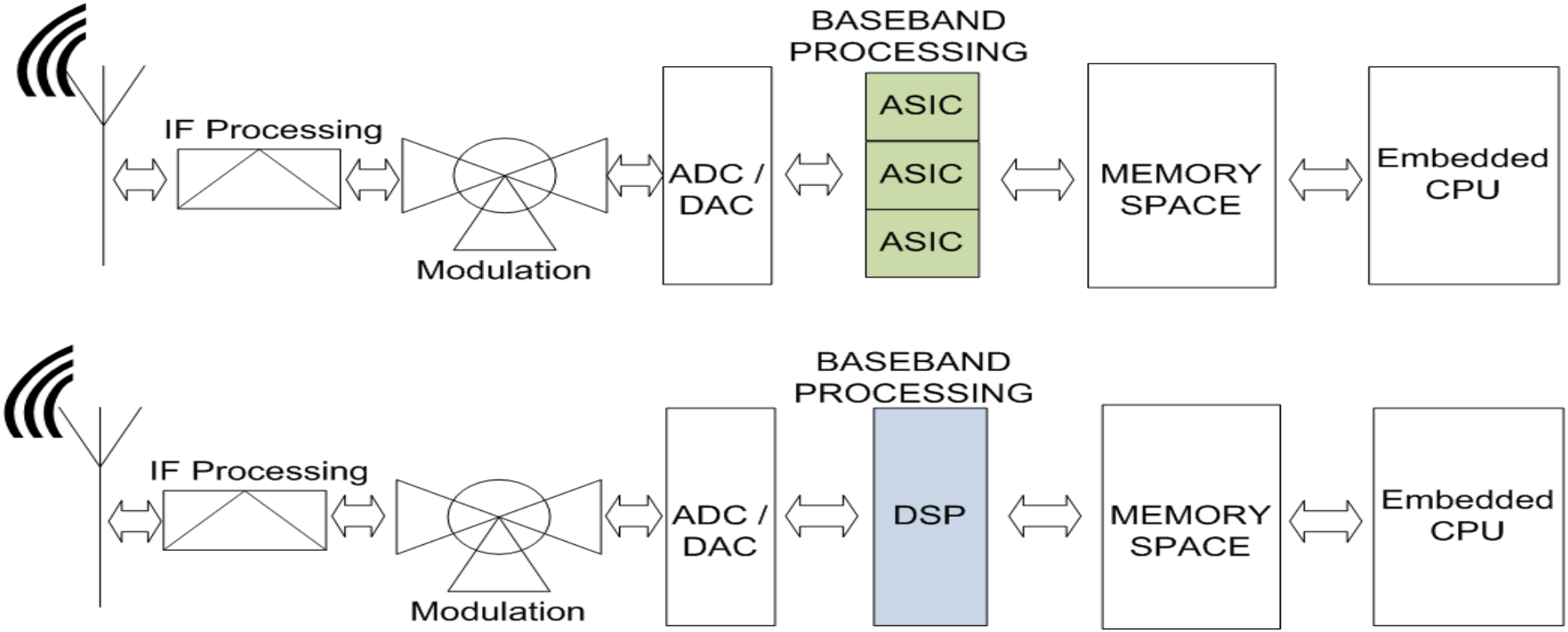
Chris Jenkins
University of Wisconsin-Madison
Mike Schulte
AMD, Inc. Research and Advanced Development Labs
John Glossner
Sandbridge Technologies

Executive Summary

- Background
  - SDR efficiently implements diverse set of wireless communication algorithms
- Problem
  - Cryptography performance/energy usage
- Hypothesis
  - Implement crypto in SIMD unit of SDR platforms
- Evaluation
  - Custom instructions on a SDR platform

THE UNIVERSITY of WISCONSIN MADISON

What is software defined radio (SDR)?

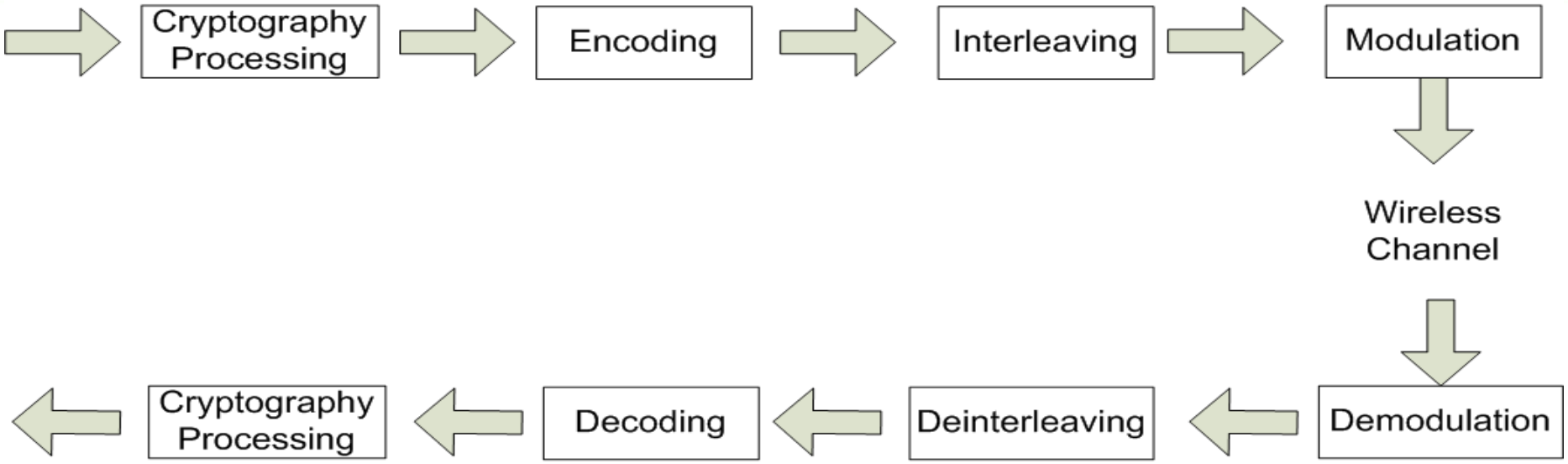


- Wireless Protocols
  - Bluetooth, GPS
  - 802.11 a/b/g/n
  - GSM, EDGE, GPRS
  - HSDPA, HSUPA, EV-DO
  - WiMAX, LTE

- Add new standards without new hardware
- Ability to switch standards on-the-fly
- Ability to run protocols concurrently

THE UNIVERSITY of WISCONSIN MADISON

Where does cryptography fit in?

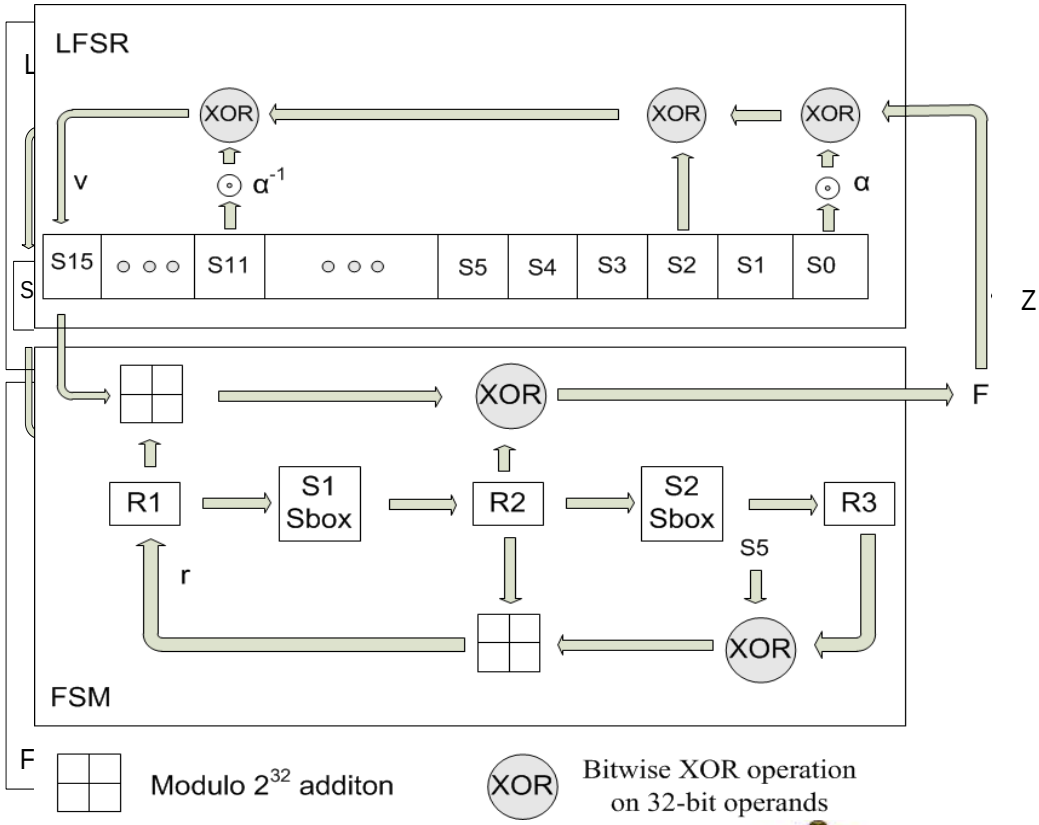


UMTS Simplified Processing Pipeline

THE UNIVERSITY of WISCONSIN MADISON

SNOW 3G: How does it work?

- General Algorithm
  - Stream cipher
  - Integrity & confidentiality
  - 2G/3G/4G networks
  - Two components
    - FSM
    - LFSR
  - 128-bit key & IV
  - 2 modes of operation
    - Initialization
    - Keystream



THE UNIVERSITY of WISCONSIN MADISON

Wireless Connectivity Speeds

Current standards

- WiMAX (70 Mbps)
- 802.11x (11 – 250 Mbps)
- HSDPA (2 – 14 Mbps)
- EV-DO (1 – 14 Mbps)
- DVB-T (1 – 31 Mbps)

Upcoming standards

- LTE (50 – 100 Mbps)
- HSPA+ (42 – 84 Mbps)
- LTE Advanced (100 - 1000 Mbps)

Can current SDR processors handle the workload?

How should processors change to accommodate the new requirements?

SDR Architectures

Processor	Throughput (Mbps)	Frequency (MHz)	Power (mW) @90nm
SODA	2 – 24	400	450
AnySP	100	300	1300
Phillips EVP	14	300	300
Sandblaster 3011	15	600	500
Sandblaster 3500	100	600	300

SB3011 Sandblaster DSP	
UEA2 (SNOW 3G) – 12.6	UIA2 (SNOW 3G) – 0.3

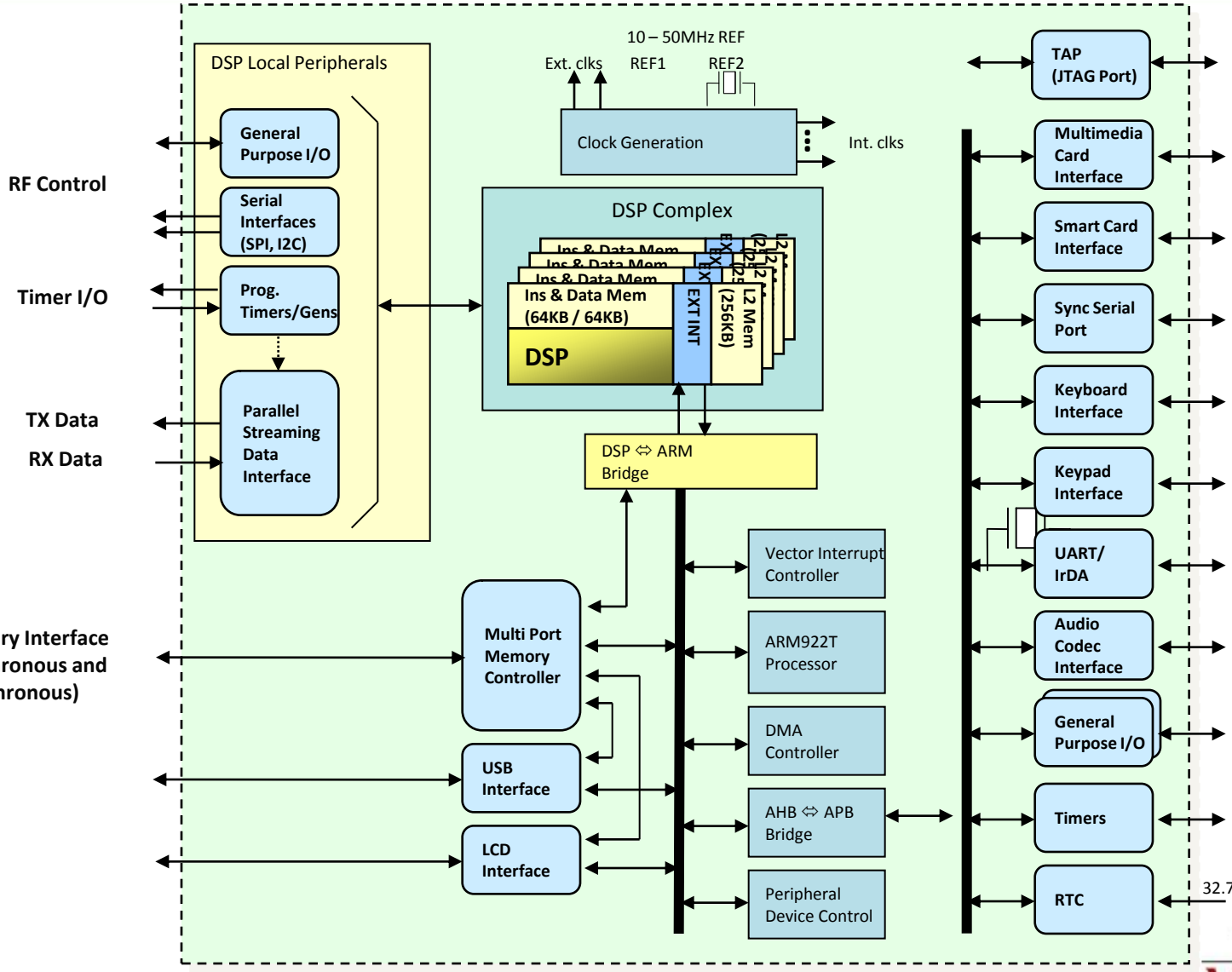
Related Research

- Product-based ASICs
  - Elliptic, 2009
  - IPCORES, 2010
- Research-based ASICs
  - First ASIC implementation (Kitsos, P., 2008)
  - S-box implementation tradeoffs (Hessel, S., 2009)
- FGPAs
  - No work found
- ISA Extensions
  - No work found

Contributions

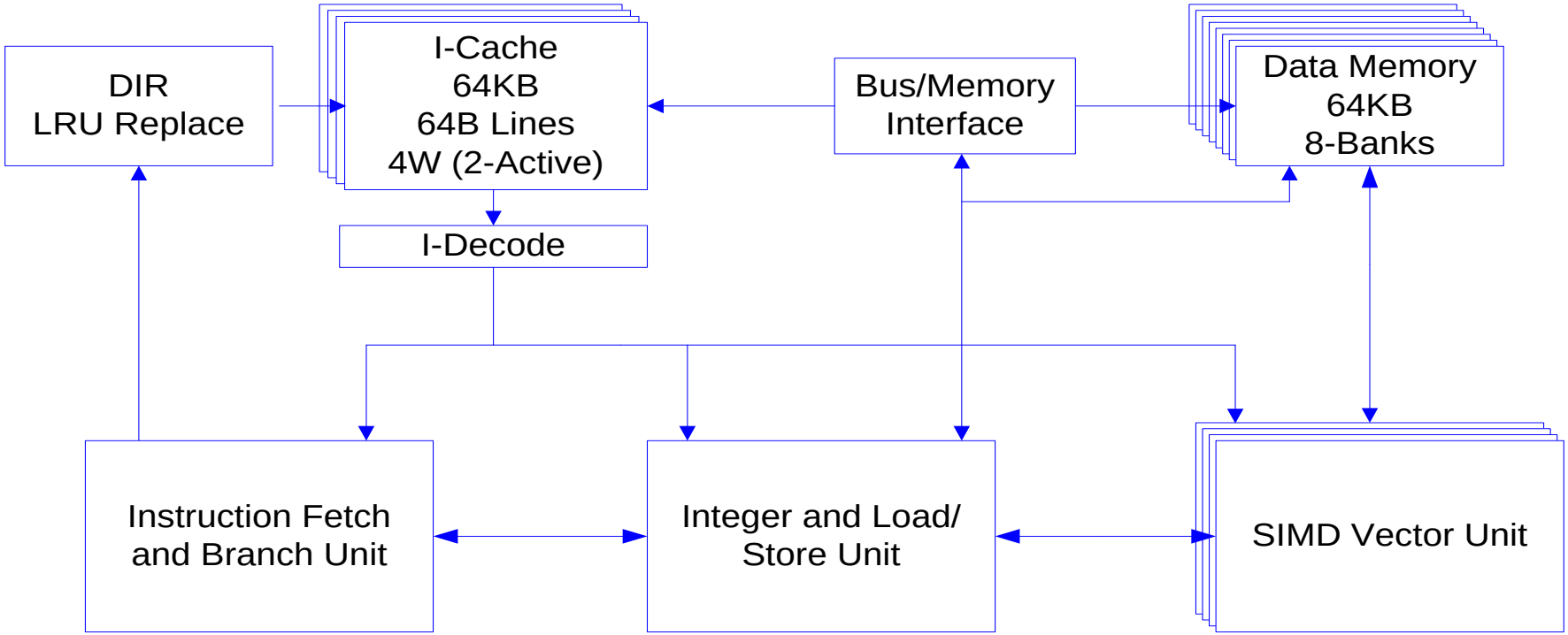
- First-known ISA extension for SNOW 3G on a SDR platform
- SDR Performance Profile
- Impact of SDR platform constraints
- Power/Energy impact
- Efficient use of ISA format

SB3011 SoC Platform



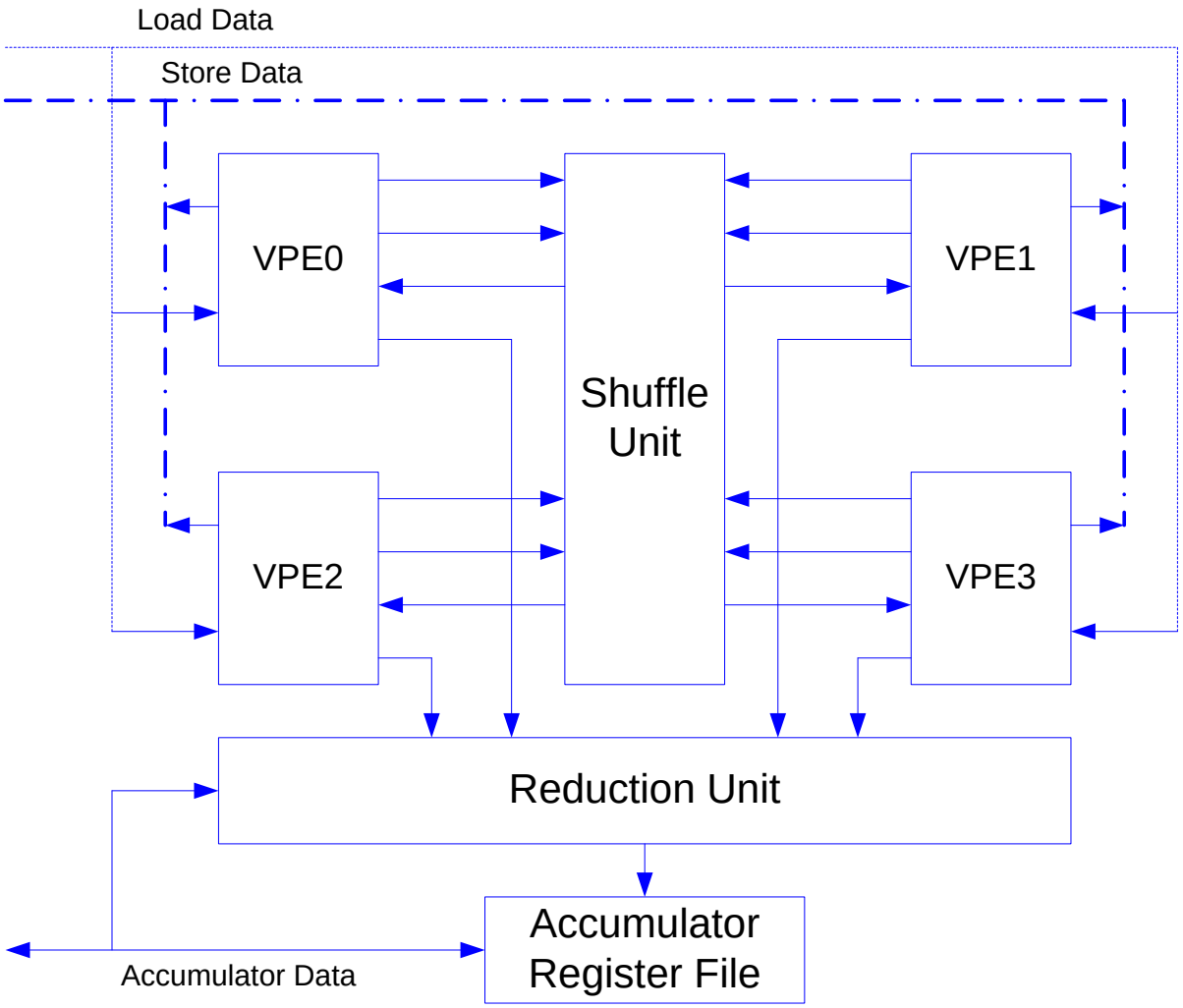
THE UNIVERSITY of WISCONSIN MADISON

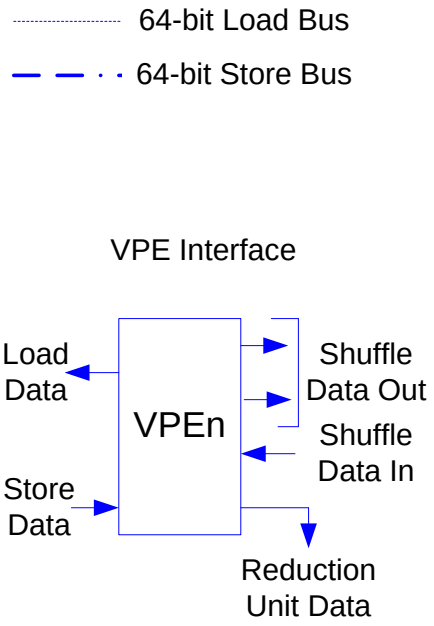
The Sandblaster™ Processor



- High Parallelism
  - Multiple operations per cycle
  - SIMD vector operations
  - Thread-level parallelism
  - Multiple processors per chip

Vector Processing Unit (VPU)



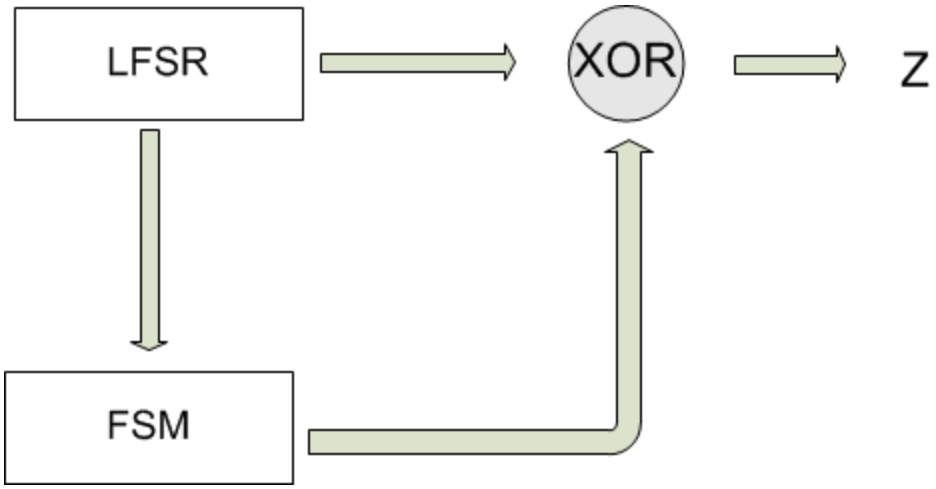


THE UNIVERSITY of WISCONSIN MADISON

ISA Extension Design Overview

Design

- 5 new instructions
- Intra-VPE reduction
- Non-traditional parallelism



SIMD Unit Benefits

- Load/store bandwidth
- RF size
- Shuffle network

THE UNIVERSITY of WISCONSIN MADISON

Proposed ISA Extensions

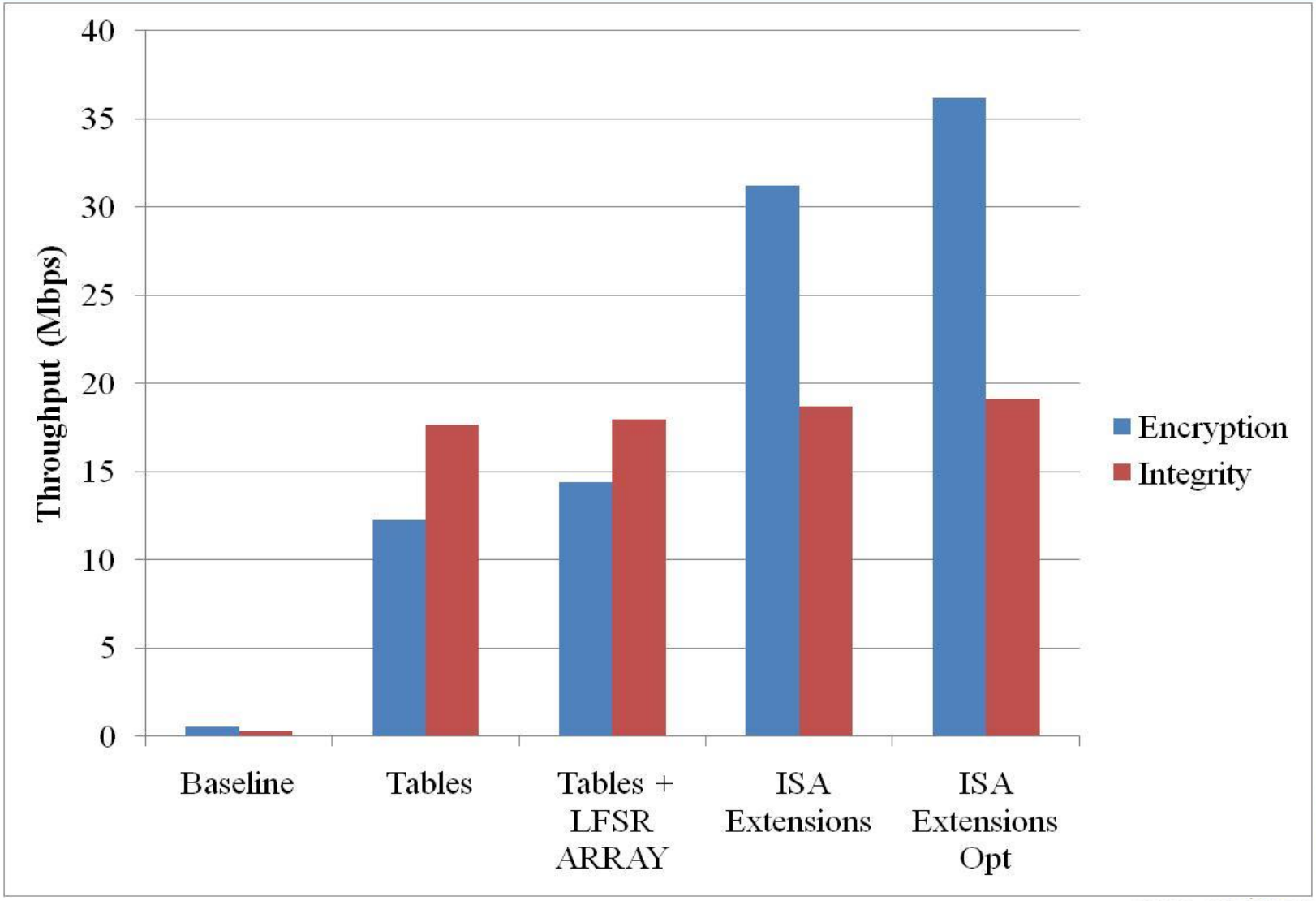
Instruction	Operand A	Operand B	Operand C	Result
snow3g_fsm	Vr1	Vr2	Vr3	Vr1
snow3g_shuffle	Vr1	X	X	Vr1
snow3g_v_f	Vr1	Vr2	Vr3	Vr1
snow3g_v	Vr1	Vr2	X	Vr1
snow3g_clmul	Vr1	Vr2	X	Vr1

Vrx = Vector Register x

Methodology

- Largest conformance data set
- SDR optimized code (supplied by Sandbridge)
- SB3011 SDR Reference Simulator
  - Determine software performance
  - Determine best location
  - Add custom instructions
  - Profile energy and speedup

ISA Extension Performance



THE UNIVERSITY of WISCONSIN MADISON

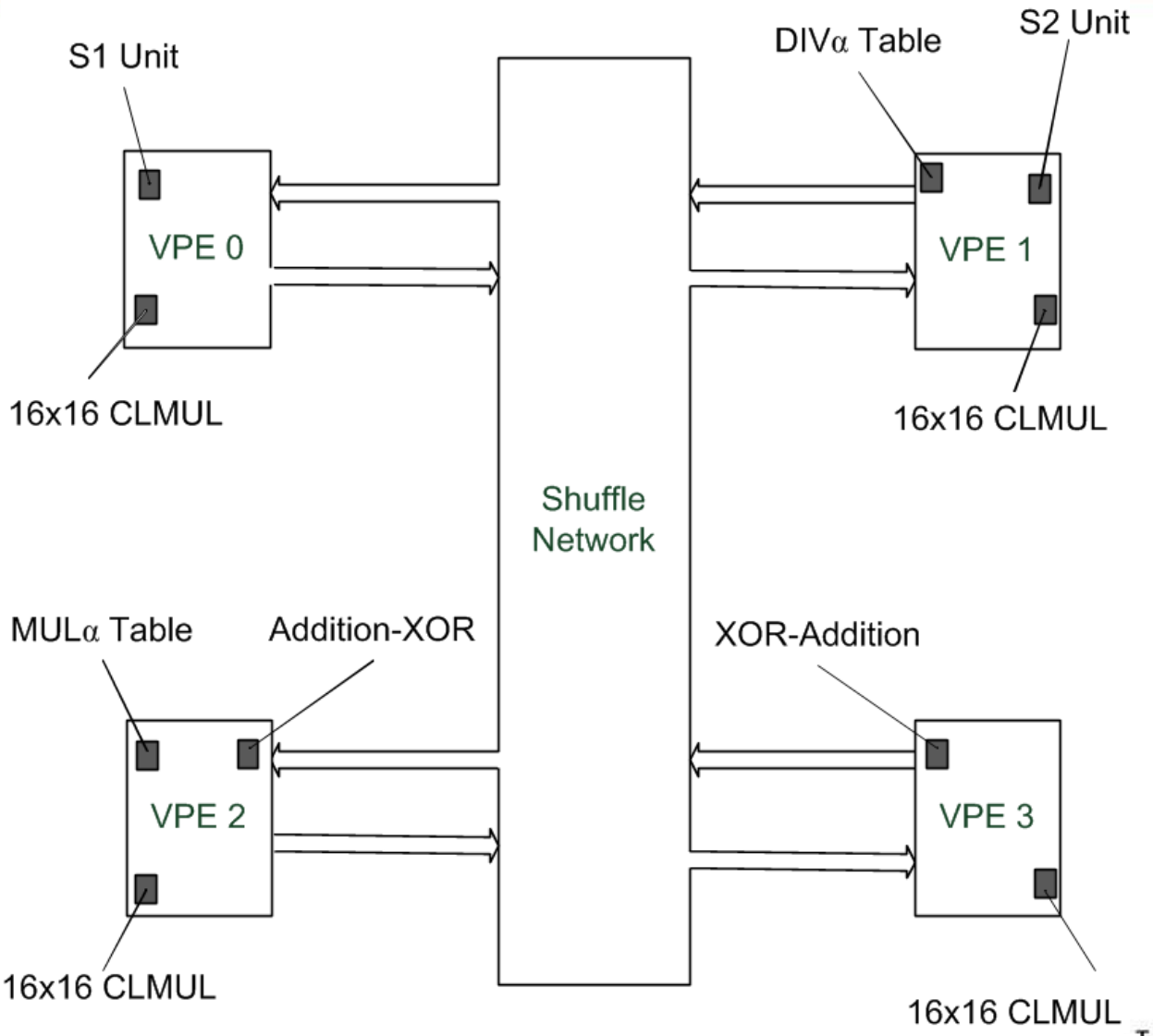
ISA Extension Performance Scaling (Mbps)

Bits to process	1000	5000	20000	Limit Estimate
Encryption (Baseline)	0.3	0.5	0.6	0.6
Encryption (Fast Software)	8.8	15.1	16.8	18.6
Encryption (ISA Extensions)	18.6	32.9	35.2	41.4
Integrity (Baseline)	0.2	0.3	0.3	0.3
Integrity (Fast Software)	1.5	7.2	22.4	88.9
Integrity (ISA Extensions)	1.6	7.5	23.3	88.9

Limitation on speed:

1) Specification limits to 20K bits / key
2) Operation Mode Re-keying

Implementation



THE UNIVERSITY of WISCONSIN MADISON

Area and Latency (600 MHz, 65nm)

Unit	Latency (ns)	Area (um^2)	Power (uW)
S1	0.93	4162	372.5
S2	1.00	4068	373.9
Addition-XOR	1.58	453	75.2
MUL_{α}	0.40	126	18.5
DIV_{α}	0.33	123	17.0
Stand-alone	1.65	16399	2992.5

Area savings = 43%

Power savings = 69%

Power Methodology

- SB3011 Hardware Platform
- DSP cores 1,2,3 and ARM shutdown
- DSP 4
  - 8 threads
  - Same instruction in endless loop
- Determine instruction mix
- Custom instruction = highest power instruction class
- Power = (Voltage drop across series resistor/0.1)*Core voltage

Speedup, Power, and Energy

Algorithm	Speedup	Normalized Power	Normalized Energy
Encryption (Fast Software)	28.7	1.04	0.04
Encryption (ISA Extensions)	62.1	1.09	0.02
Integrity (Fast Software)	61.5	1.04	0.02
Integrity (ISA Extensions)	63.9	1.05	0.02

Normalized to baseline software

THE UNIVERSITY of WISCONSIN MADISON

Conclusions

- SIMD features are beneficial to crypto
  - Load/store
  - Register File Storage
  - ISA Operand Specification
- Low opcode use
- Lower resource usage than ASIC
- Next-generation single thread speed
- Traditional SIMD arch. not ready

Questions