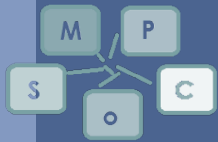# HiPAcc-LTE: An Integrated High Performance Accelerator for 3GPP LTE Stream Ciphers

Sourav Sen Gupta[1], Anupam Chattopadhyay[2], Ayesha Khalid[2]

1. *Applied Statistics Unit, Indian Statistical Institute, Kolkata, India*
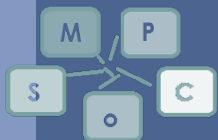2. *MPSoC Architectures, UMIC Lab, RWTH Aachen, Germany*

Indocrypt 2011, Chennai, India
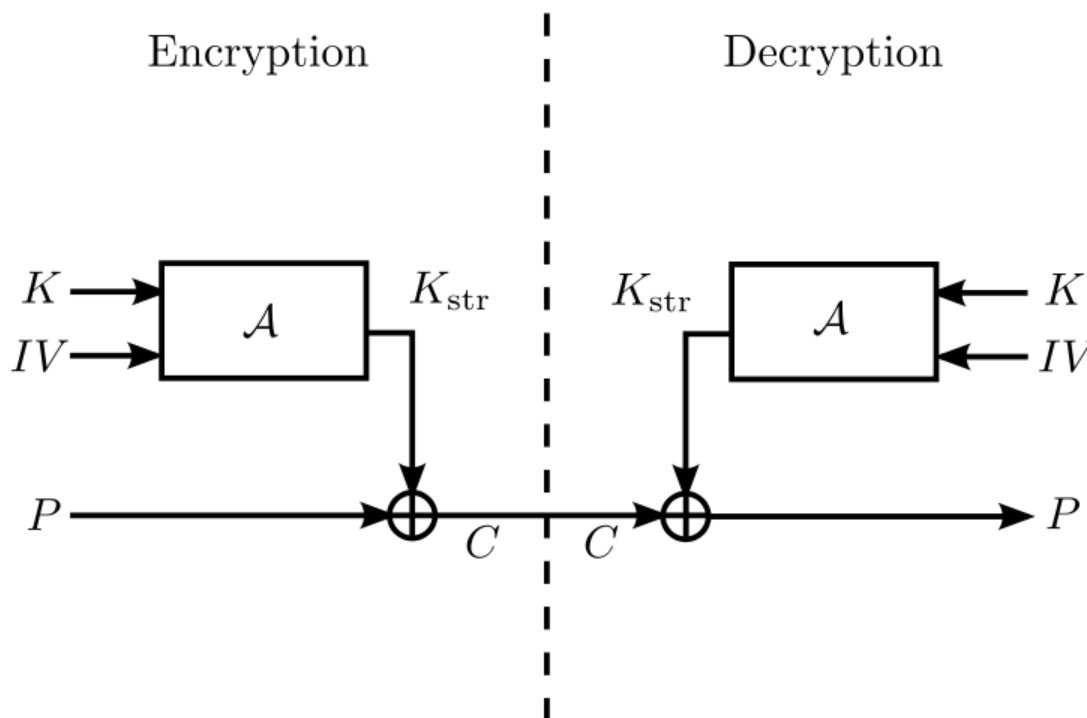
**RWTH AACHEN UNIVERSITY**

- **Enhance hardware performance of existing designs**
  - Dedicated hardware modules for high speed and low area

- **New designs targeted towards hardware performance**
  - eSTREAM profile 2 (HW): Grain v1, MICKEY v2, Trivium
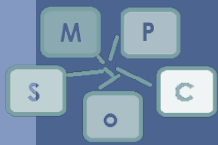
- **Enhance hardware performance of existing designs**

- **The general trend**
  - Standalone modules for individual ciphers (eSTREAM)
  - Few different ciphers put into a single package (HSMs)

- **The path not charted**
  - Fuse multiple designs together before implementation
  - Algorithm-level merger for ciphers with similar structure
 - Single base framework, rather than a package

If there is a requirement to implement an array of ciphers on the same platform, how should one approach the hardware design?
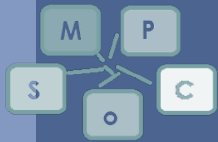
RWTH AACHEN UNIVERSITY

- **3GPP LTE Advanced – Security Suite**
    - EEA1/EIA1 – based on SNOW 3G   (same as in 3G)
    - EEA2/EIA2 – based on AES-128   (changed from KASUMI)
    - EEA3/EIA3 – based on ZUC   (brand new inclusion)

- **Observation**
    - Two similar stream ciphers in the same package
    - In general, only one will be used at any given time
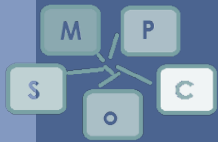
> **3GPP LTE Advanced Security Module**
>
> **HiPAcc-LTE**
> SNOW 3G + ZUC
>
> **+**
>
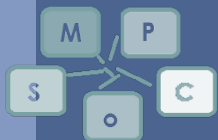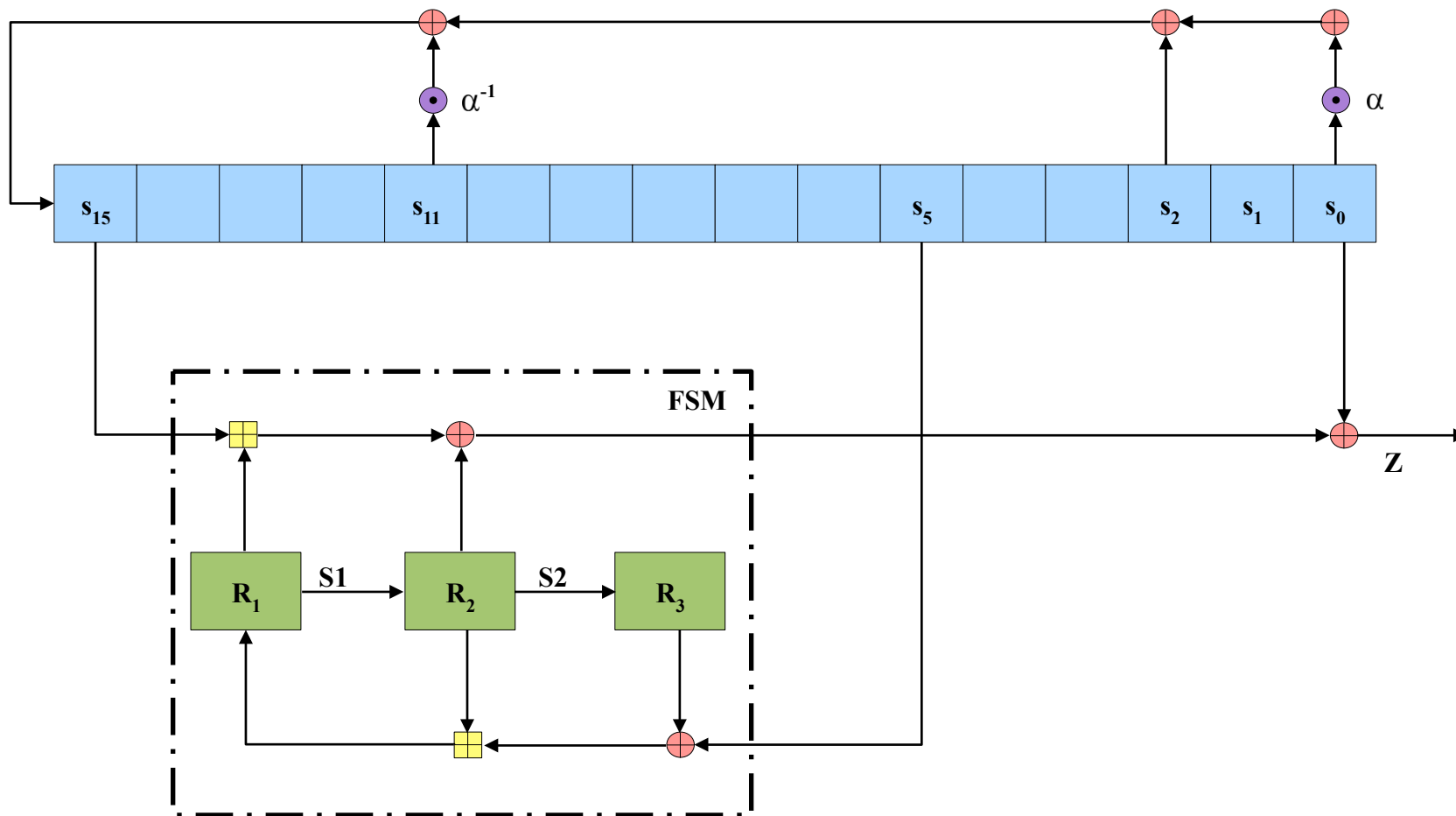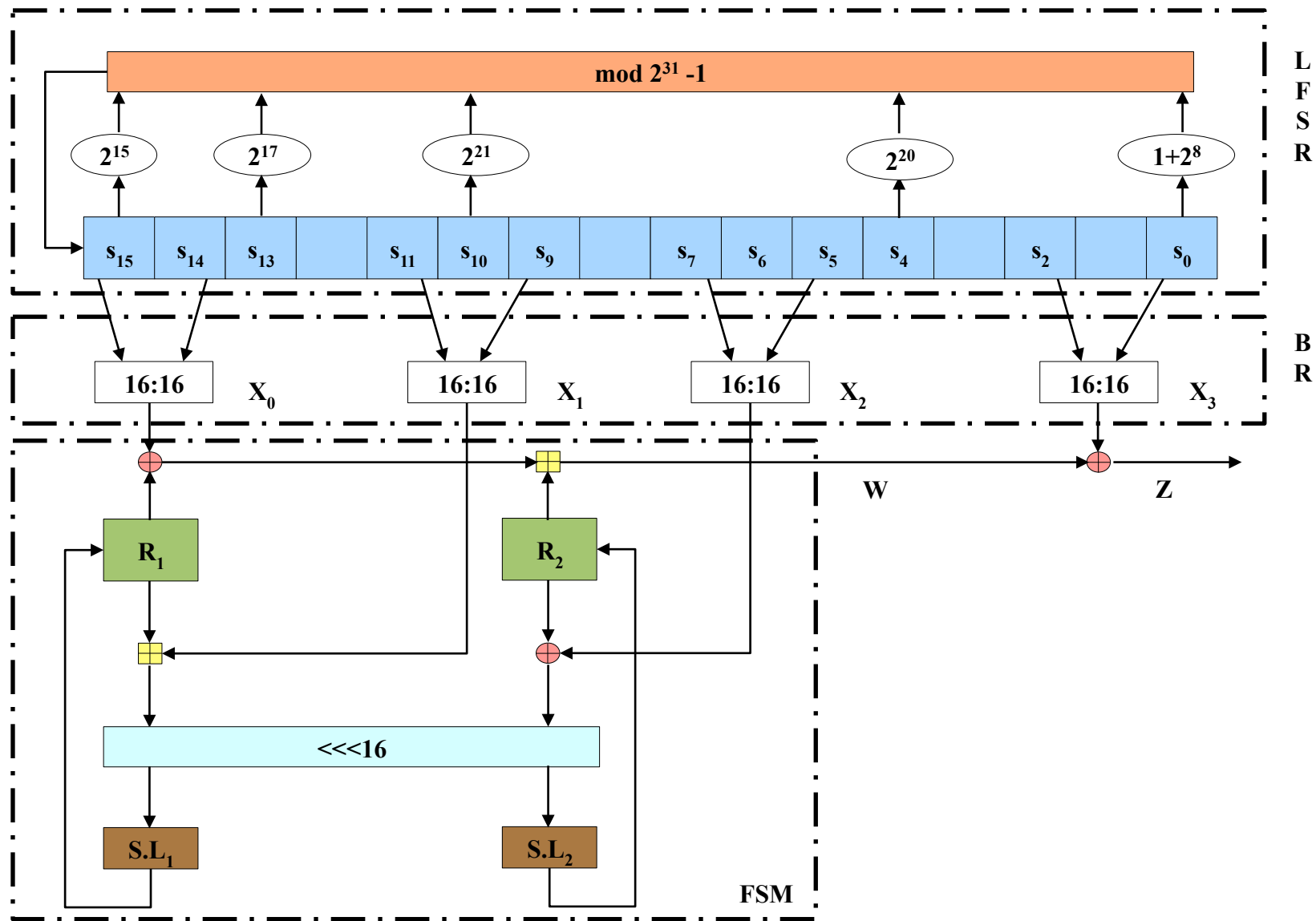> **StandaloneCore**
> AES-128

- **Fuse SNOW 3G and ZUC in hardware**
  - Sharing of resources, both storage and logic
  - Throughput vs. area optimization at the base level

- **HiPAcc-LTE: Integrated platform**
  - Integrate similarities of the individual designs
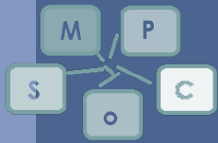 - Push the performance (speed and area) for both

RWTH AACHEN UNIVERSITY

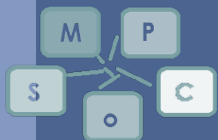- Motivation and Preliminaries

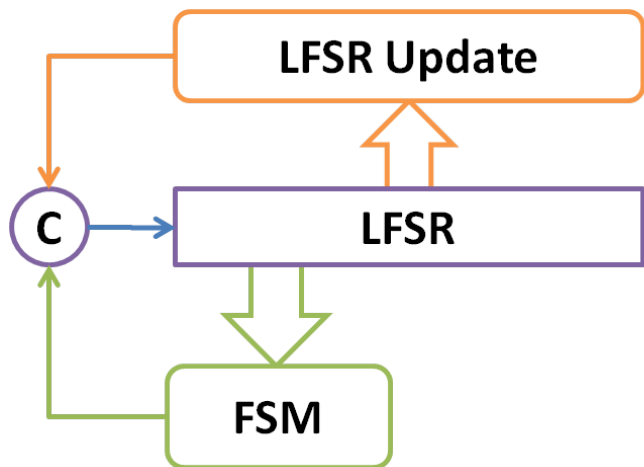- → *Design of Integrated Accelerator HiPAcc-LTE*

- Implementation and Experimental Results

- Summary and Conclusion

RWTH AACHEN UNIVERSITY
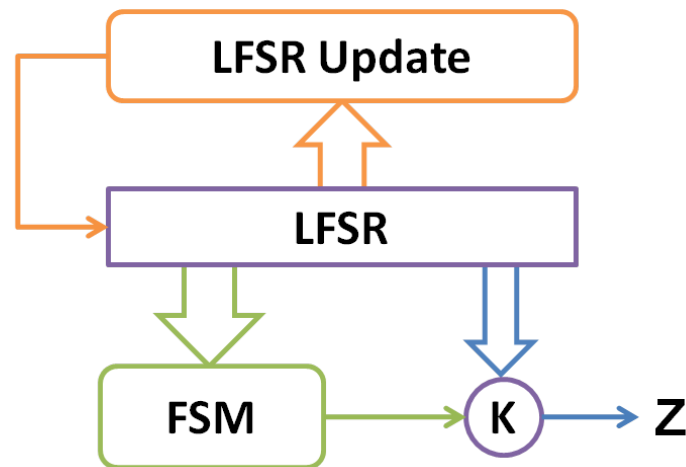
Cipher	LFSR Update	LFSR	FSM
SNOW 3G	Field Mul/Div and XOR	32 bits x 16	3 Registers and 2 S-boxes
ZUC	Modulo prime addition	31 bits x 16	2 Registers and 2 (S.L)-boxes

- **Use 16 bits x 32 LFSR structure for both**
  - SNOW 3G – just break the 32 bit blocks into halves
  - ZUC – 1 bit extra per 32 bits – duplicate the middle bit

Original LFSR Words

Modified LFSR Words

Original BR

Modified BR
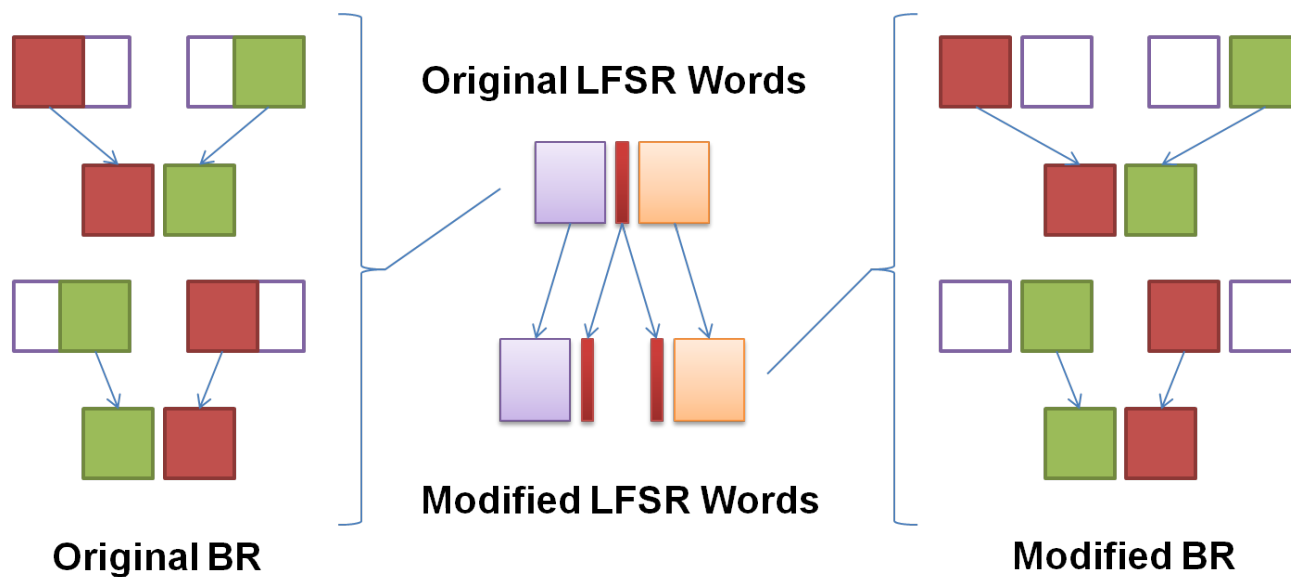
- **BR layer moved to LFSR update from FSM operation**
  - Reduces the critical path that flows through the FSM
  - Causes no significant disadvantage in LFSR update routine
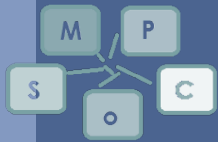
Designing the Pipeline – FSM

- **Store S-box and Mul/Div-alpha tables in Memory**
  - Allow for memory request and read time
  - Share resources: 2 registers and 8 memory tables

- **Initial design**

Stage 1

Registers → Computation for Address generation → mem request → Data Memory → mem read → Computation for Register updates → Registers
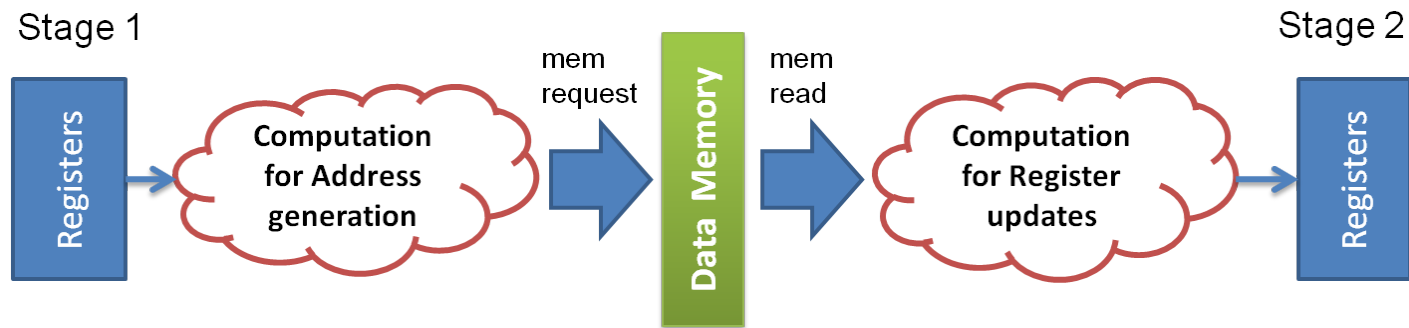
Stage 2

- **Final design**
  - Just precomputation at the first stage
  - Memory request moved to the end of second stage
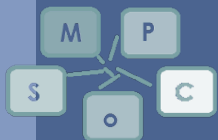
- ZUC – 6 modulo prime additions for the update

$$s_{16} = s_0 + 2^8 s_0 + 2^{20} s_4 + 2^{21} s_{10} + 2^{17} s_{13} + 2^{15} s_{15} \quad (\text{mod } 2^{31} - 1)$$

- SNOW 3G – 3 simple XORs; fits into the same structure

- **FSM: Two stages**
  - initial computations for address generation in the first stage
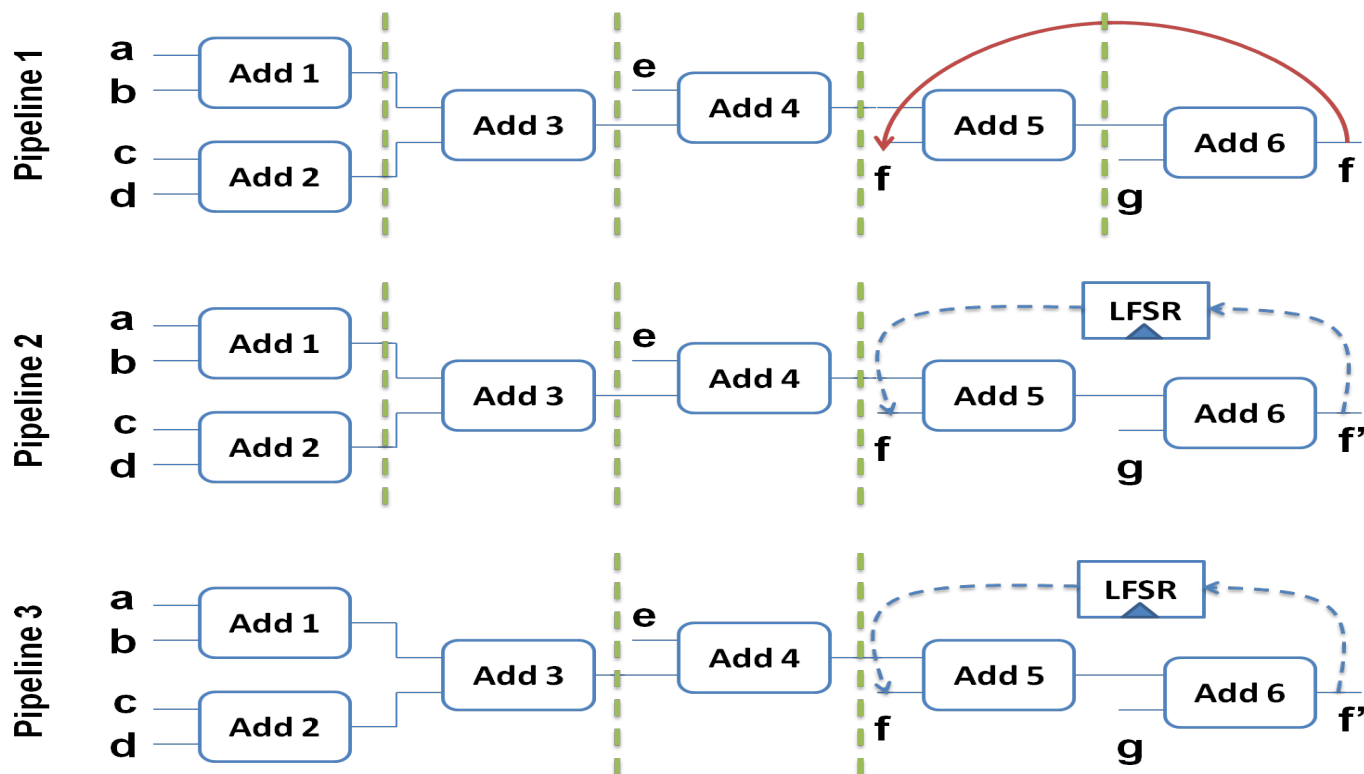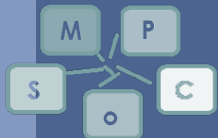 - memory access and related computations in the second stage

- **LFSR Movement: Two stages**
  - shift in first stage and s_{15} write in second stage

- **LFSR Update: Two/Three stages**
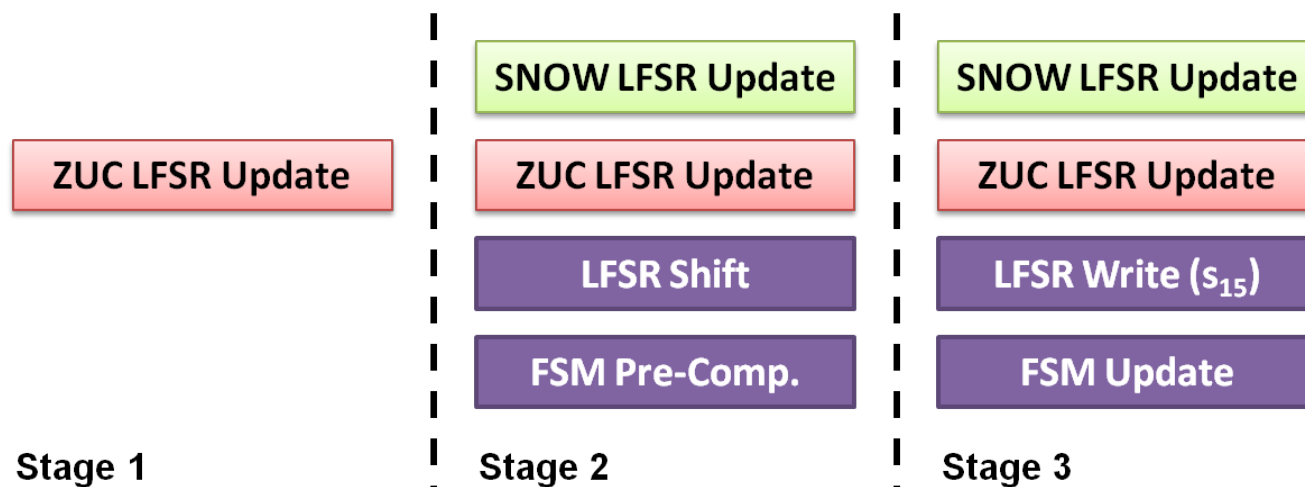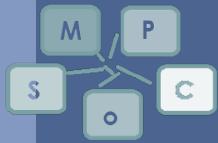
Stage 1	Stage 2	Stage 3
	SNOW LFSR Update	SNOW LFSR Update
ZUC LFSR Update	ZUC LFSR Update	ZUC LFSR Update
	LFSR Shift	LFSR Write (s_{15})
	FSM Pre-Comp.	FSM Update

- Motivation and Preliminaries

- Design of Integrated Accelerator HiPAcc-LTE

- → *Implementation and Experimental Results*

- Summary and Conclusion
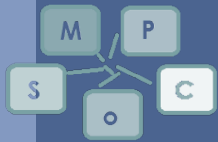
- **After the initial synthesis: In ZUC Key Initialization**

LFSR_Key_Initialization (W)

1. $v = 2^{15}s_{15} + 2^{17}s_{13} + 2^{21}s_{10} + 2^{20}s_4 + 2^8 s_0 + s_0 \pmod{2^{31} - 1}$
2. $Y = v + (W \gg 1) \pmod{2^{31} - 1}$
3. If $Y = 0$, then set $Y = 2^{31} - 1$
4. Write Y to location s_{15} of the LFSR

- **LFSR read optimization**
  - Original: Register array – access from different stages in pipeline
  - Optimized: 32 distinct 16-bit registers – placed independently
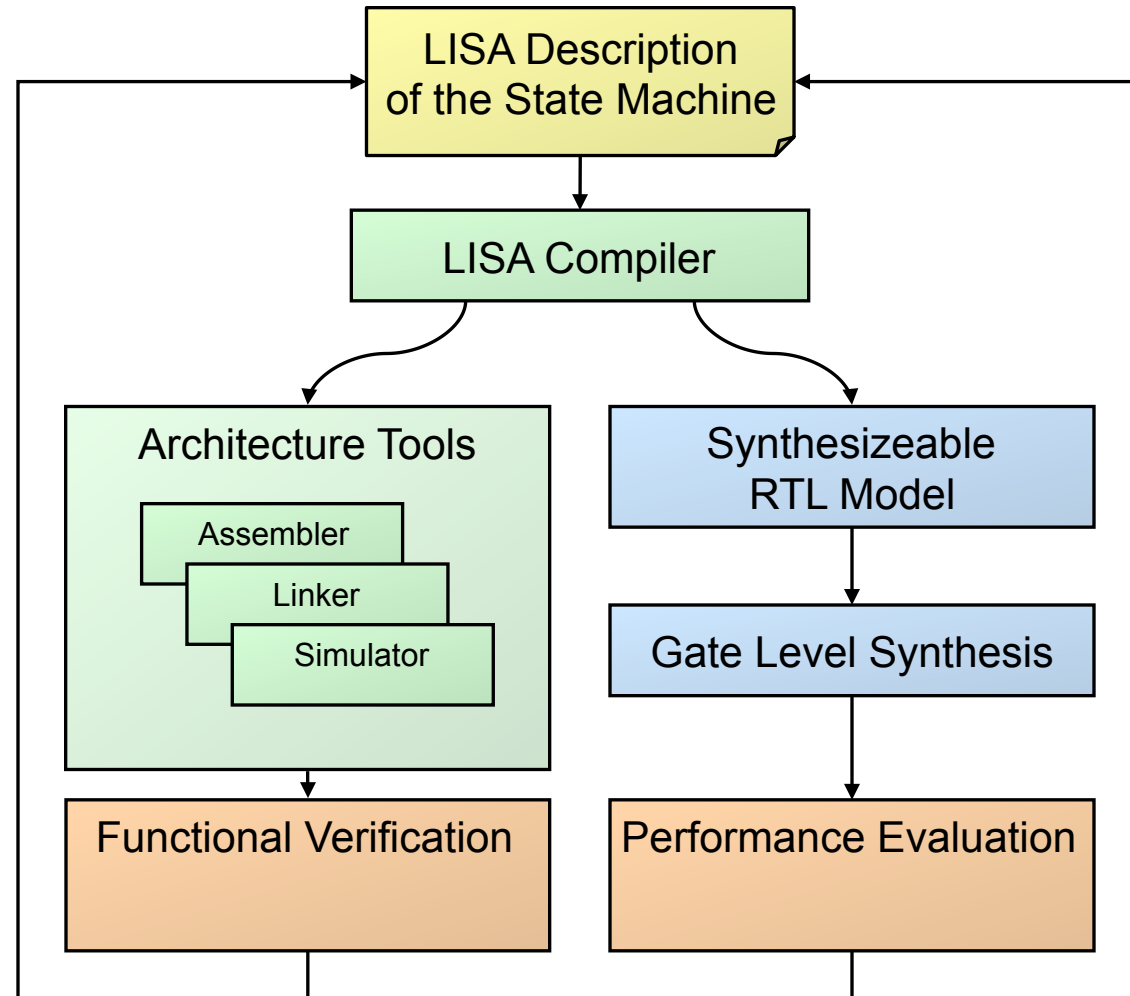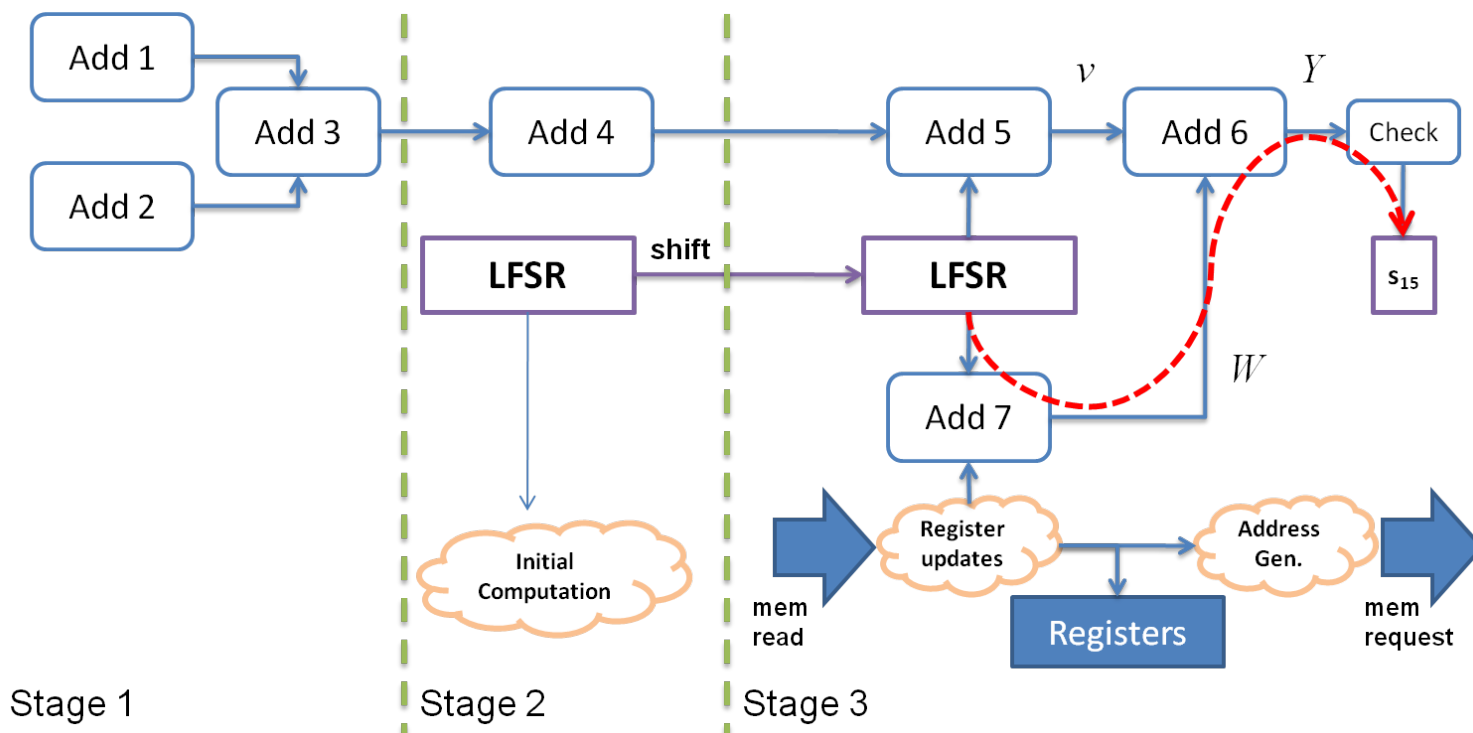
- **Modulo prime adder optimization**
  - Original: A layer of multiplexer in series with adder and increment
  - Optimized: Just increment the first adder output by the carry bit

Original Adder   Modified Adder
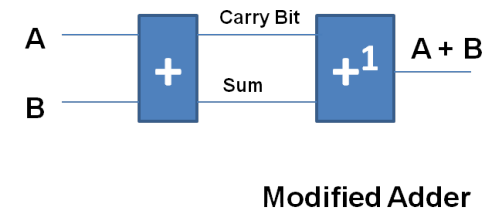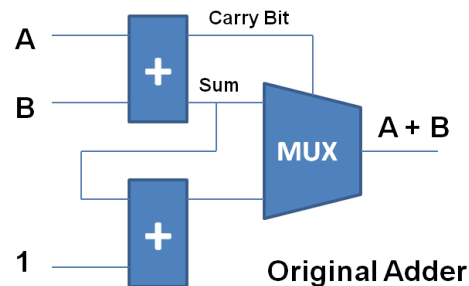
- **Check optimization**
  - Original: Check if Y = 0 where $Y = v + (W >> 1) \bmod 2^{31} - 1$
  - Optimized: Note that Y can never be 0 for proper v and W
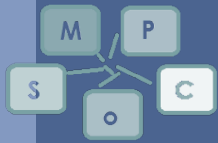
- **Standalone modes for SNOW 3G and ZUC**

  - **Academic literature** – generally 130 nm technology
    SNOW 3G: Kitsos et al, IFIP/IEEE VLSI-SOC '08
    ZUC: no attempt in ASIC till date

  - **Commercial designs** – generally 90, 65 nm technology
    SNOW 3G: IP Cores Inc., SNOW3G1 core
    ZUC: Elliptic Tech. Inc., CLP-410 core

- **Integrated mode of HiPAcc-LTE**
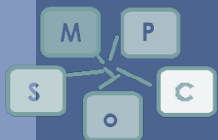
Comparison in 130 nm technology - Academic

Design	Designer	Throughput	Area	Memory
SNOW 3G	Kitsos et al	7.97 Gbps	25 Kgate	10 Kbyte
HiPAcc-LTE	- - -	24.0 Gbps	18 Kgate	10 Kbyte

Comparison in 65 nm technology - Commercial

Design	Designer	Throughput	Area	Memory
SNOW3G1	IP Cores Inc.	7.5 Gbps	8.9 Kgate	Hard Macro
HiPAcc-LTE	- - -	32.0 Gbps	7.0 Kgate	3 Kbyte
HiPAcc-LTE	- - -	52.8 Gbps	18 Kgate	Hard Macro

gate level synthesis results are obtained using Faraday 130, 90, 65 nm technology, best case performance using Synopsys DC topographical mode

RWTH AACHEN UNIVERSITY
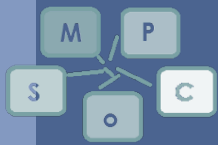
Comparison in 65 nm technology - Commercial

Design	Designer	Throughput	Area	Memory
CLP-410	Elliptic Tech	16.0 Gbps	10-13 Kgate	Hard Macro
HiPAcc-LTE	- - -	32.0 Gbps	11 Kgate	3 Kbyte
HiPAcc-LTE	- - -	29.4 Gbps	20.6 Kgate	Hard Macro

gate level synthesis results are obtained using Faraday 130, 90, 65 nm technology, best case performance using Synopsys DC topographical mode
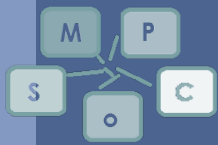
RWTH AACHEN UNIVERSITY

Performance figures for both ciphers together – 65 nm technology

Design	Frequency	Throughput	Area	Memory
HiPAcc-LTE	1090 MHz	34.88 Gbps	17 Kgate	10 Kbyte
HiPAcc-LTE	1090 MHz	34.88 Gbps	17 Kgate	3 Kbyte
HiPAcc-LTE	920 MHz	29.4 Gbps	24 Kgate	Hard Macro

Comparison in 65 nm technology - Commercial

Design	Designer	Throughput	Area	Units reqd.
SNOW3G1	IP Cores Inc.	7.5 Gbps	8.9 Kgate	4
CLP-410	Elliptic Tech	16.0 Gbps	10-13 Kgate	2
Combined	Both	30-32 Gbps	56-62 Kgate	1
HiPAcc-LTE	- - -	29.4 Gbps	24 Kgate	1

gate level synthesis results are obtained using Faraday 130, 90, 65 nm technology, best case performance using Synopsys DC topographical mode
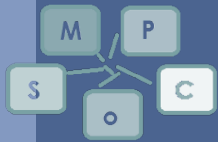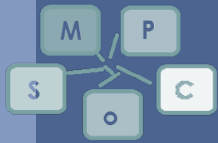
RWTH AACHEN UNIVERSITY

- Motivation and Preliminaries

- Design of Integrated Accelerator HiPAcc-LTE

- Implementation and Experimental Results

→ *Summary and Conclusion*

In a nutshell

- **Summary**
  - Multiple designs are proposed to serve similar purpose
    - varying degree of security
    - minor design choice variation
    - non-technical reasons
  - Integrated design offers significant performance improvement
  - Case study with 3GPP LTE stream ciphers presented here

- **Long term vision**
  - Design of a flexible core supporting multiple ciphers
  - Intermediate design points for individual algorithms
  - Unified platform with optimal performance for various ciphers

RWTH AACHEN UNIVERSITY

Thank You